# ENDGAME

# An Elastic company

# User's Guide

Version 3.22

© 2021 Elasticsearch B.V.

Copyright © 2021 Elasticsearch B.V.

### **COPYRIGHT NOTICE**

The content in this document is confidential and proprietary information belonging to Elasticsearch B.V. No part of this book may be reproduced without Elastic permission. Endgame®, Endgame Resolver<sup>™</sup>, and Endgame MalwareScore® are either registered trademarks or trademarks of Elasticsearch B.V. in the United States or other countries. All rights reserved.

Elasticsearch B.V. 3101 Wilson Blvd Suite 500 Arlington, VA 22201 703-653-0361

https://www.elastic.co

# **Table of Contents**

CHAPTER 1 Getting Started	1
User's Guide Overview	2
Introduction to Endgame	3
Application Programming Interface (API) Documentation	4
Glossary Terms	5
Log in to Endgame	11
User Interface Overview	12
User Settings	15
Change Your Password	15
Change Your Time Zone	16
Log Out of Endgame	
Supported Endgame Platform Functions by Operating System	17
Platform Dashboard Overview	
CHAPTER 2 Endpoints	
Endpoints Overview	
Discover Endpoints	24
Endpoint Dashboard Overview	
Download the Endpoints List	34
Endpoint Groups Overview	
Create an Endpoint Group	
Manage Endpoint Groups	

Endpoint Details Page Overview	
Endpoint Responses Overview	
Host Isolation Overview	50
Isolate a Host	51
Release a Host	53
Allow Isolated Hosts to Connect to Other IP Addresses	
Manage the Host Isolation Exceptionlist	57
Endpoint Response Types and Advanced Configuration Options	
Delete an Endpoint	60
CHAPTER 3 Investigations	61
Investigations Overview	62
Start an Investigation	
Investigation Dashboard Overview	67
Investigation Dashboard Overview	67
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview	67 72 72
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview Archive an Investigation	67 72 72 
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview Archive an Investigation Investigation Dashboard - Archived View	
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview Archive an Investigation Investigation Dashboard - Archived View Unarchive an Investigation	
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview Archive an Investigation Investigation Dashboard - Archived View Unarchive an Investigation Hunt Types and Advanced Configuration Options	
Investigation Dashboard Overview	
Investigation Dashboard Overview	
Investigation Dashboard Overview View Investigation Results Investigation Details Page Overview Archive an Investigation Investigation Dashboard - Archived View Unarchive an Investigation Hunt Types and Advanced Configuration Options Tradecraft Analytics Overview Fileless Attacks Overview What to Look Out For	

Analyze Fileless Attacks	93
Execute an Endpoint Response	
Suspend a Thread for Memory Injection Hits	
IOC Search Overview	
Execute an IOC Search	
View IOC Search Results	97
IOC Search Types and Advanced Configuration Options	
CHAPTER 4 Alerts	
Alerts Overview	
Alert Dashboard Overview	
Alerts Page Overview	111
Sort and Filter Alerts	115
Download the Alerts List	
Alert Details Page Overview	
Alert Metadata Panel Overview	
Endgame Resolver™ Attack Visualization Overview	
Alert Commenting Overview	135
Respond to an Alert	
Dismiss an Alert	140
Resolve an Alert	141
Assign an Alert	142
Archived Alerts Page Overview	
Unarchive an Alert	144

CHAPTER 5 Artemis	
Artemis Search Overview	
About Artemis Queries	148
Sample Artemis Queries	
Execute a Search in Artemis	154
Artemis Search Optimization Tips	155
View Artemis Search Results	156
Artemis Search Results Overview	
Process Lineage Search Results Overview	162
Download Artemis Results	
Find Additional Endpoint Occurrences Using Artemis Shortcuts	167
Configure Third-Party Applications to Connect to Endgame	172
Event Query Language (EQL) Overview	
Execute EQL Queries via Artemis	
Eventing Schema	
Artemis Queries List Overview	
Archive an Artemis Query	
Verify that Logon Events are Enabled in Windows (Optional)	
Customer Support	

# CHAPTER 1

# **GETTING STARTED**

User's Guide Overview	2
Introduction to Endgame	3
Application Programming Interface (API) Documentation	4
Glossary Terms	5
Log in to Endgame	11
User Interface Overview	12
User Settings	15
Supported Endgame Platform Functions by Operating System .	17
Platform Dashboard Overview	18



### **User's Guide Overview**

This **User's Guide** is a comprehensive manual, designed to explain all features, tools and components of Endgame, version 3.22, so you can use them for maximum efficiency.

The following table lists the various icons you will see throughout the guide:

Name	lcon	Description
Info	í	Relevant, supplemental information about the aforementioned text.
Note		An important comment about the aforementioned text.
Refer to	Ē	A cross-reference to another topic or chapter in the manual.
Remember		A friendly reminder of information that appeared earlier in the manual.
Тір		A helpful, nice-to-know pointer.
Warning	$\wedge$	A critical note that should be observed.



ENDGAN

### **Introduction to Endgame**

Endgame is a centrally managed endpoint detection and response platform that operates at the earliest and all stages of the attack life cycle. Through a single agent, Endgame instantly detects and stops privilege escalation, defense evasion, malicious persistence, credential access, and propagation.

Endgame automates the hunt for next generation attacks by automating data collection and analysis across all endpoints in seconds, instantly surfacing suspicious artifacts and malicious activity with tailored Tradecraft Analytics that highlight anomalous data. This enables analysts to act with precision to stop the adversary without business disruption.

Endgame provides the following capabilities:

- Accelerated endpoint detection and response
- · In-band and out-of-band sensor deployment
- Advanced endpoint protection
- Automated hunting
- Multi-Client Management within an independent server

Endgame's advanced sensor technology allows the analyst choose to install a persistent sensor for long-term protection or a dissolvable sensor for minimal endpoint footprint.



Endgame architecture



## Application Programming Interface (API) Documentation

To view Endgame's API Documentation:

• Open a web browser and type the URL or hostname that hosts the Endgame platform followed by **/api/docs** (e.g., https://10.0.0/api/docs).

ENDGAME. An Elastic company
Endgame API Documentation
The Endgame Platform API is based on REST principles: data resources are accessed via standard HTTPS requests in UTF-8 format to an API endpoint. Where possible, the API strives to use appropriate HTTP verbs for each action.
VERB DESCRIPTION
GET Used for retrieving resources.
POST Used for creating resources.
PUT Used for changing/replacing resources.
PATCH Used for updating resources.
DELETE Used for deleting resources.
The Endgame Platform API communicates over HTTPS using JSON, and the appropriate Content-Type: application/json header must be utilized when including a request body in POST, PATCH and PUT requests. Use of other content types and failure to specify the correct content type will result in an appropriate error response
Responses
Data returned is encoded as JSON (exceptions are noted within the specific response payload). All JSON responses will be will return the requested data via the data field, and will be augmented with the metadata object. It will contain at a minimum the timestamp field informing the requester the time at which the request was fulfilled.
Standard response format
<pre>{     "data": {},     "metadata": {} }</pre>
Standard error response
<pre>{     "error": {         "code": 500,         "message": "Something terribly awry happened internally."     } }</pre>

Endgame API Documentation



## **Glossary Terms**

Before using Endgame, familiarize yourself with the following terms that are referenced in the User's Guide.

### Α

### **Activity Timeline**

A chronological list of activities that occurred on an endpoint.

### **Adversary Behaviors**

Adversary behavior alerts reflect the various behaviors attackers exhibit when executing an attack. These alerts are directly mapped to MITRE's ATT&CK<sup>™</sup> and are useful in understanding the tactics and techniques an attacker may use when carrying out an attack.

### Alert

A system-generated notification that indicates malicious activity on an endpoint.

### Artemis

Endgame's artificial intelligence-powered security mentor that provides guided alert triage and event search.

### В

### Blocklist

A list of applications and files that an end user is forbidden to run within a network. The blocklist is maintained by an administrator.

### С

### **Custom Rule**

A statement, written in EQL, that instructs Endgame's sensor to monitor suspicious or malicious activity specific to your environment. If such activity is detected, the sensor generates an alert in the Endgame platform.



### Ε

### Endgame Resolver<sup>™</sup> Attack Visualization

A visual depiction of chronological events that led up to the sensor generating an alert.

### Endpoint

Any system or host that is connected to a network and functions as a client or server in any capacity. Desktop computers, laptops, and servers are all examples of endpoints.

### **Endpoint Policy**

A policy that allows administrators to configure endpoint protections and event data collection. Policy reporting ensures compliance across all managed enterprise endpoints.

### **Endpoint Protections**

Malicious activities and behaviors that are protected by Endgame's full autonomous sensor. Endpoint protections are enabled or disabled via Endpoint Policy configuration.

### Event Query Language (EQL)

A syntax that enables you to structure more advanced queries that may be unavailable using natural language.

### Exceptionlist

A list of items that specifies the attributes for which the sensor should not trigger an alert. The exceptionlist is maintained by an administrator.

### F

### File Quarantine

A process that isolates infected files on a computer's hard disk. Files put in quarantine are no longer capable of infecting their hosting system.



### **Fileless Attacks**

An analytic and enhancement to the "Process" hunt that inspects the memory of running processes to discover potentially malicious code not backed on disk.

### G

### Group

The name given to a set of endpoints with similar attributes for easy endpoint management.

### Η

### Histogram

A chart in Investigation Details that shows the number of occurrences — according to selected variables — on a defined percentage of endpoints. The Histogram also easily identifies outliers.

### **Host Isolation**

A process that disconnects the host from the network so that adversaries are unable to move laterally and infect other systems. Isolated Hosts are only able to communicate with the Endgame platform or specific IPs that have been whitelisted.

### Hunt

A task with specific parameters, executed by the sensor, that collects a current snapshot of events occurring on specified endpoints.

### Ι.

### Investigation

A selection of one or more hunts used to identify malicious, suspicious, or anomalous behavior across endpoints.



### **IOC Search**

A targeted search on one or more endpoints for a specific indicator of compromise, such as a file hash, process name, or network connection.

### Κ

### Key Performance Indicator (KPI)

A numerical measurement that represents the total number of items (e.g., endpoints, alerts, etc.) that fall into a specific category. KPIs also act as list filters.

### Μ

### MalwareScore<sup>™</sup>

A machine learning-powered malware prevention engine that prevents the execution of both known and unknown malware. Malware is scored on a scale from 0 (benign) to 100 (malicious).

### **Multi-Client Management**

An independent server that allows an administrator to view and manage endpoint data from multiple Endgame platforms. It also serves as an entry point into those platforms.

### Ρ

### Persistence

Any access, action, or configuration change to a system that allows a persistent presence on that system. Administrators define a sensor's persistence (i.e., persistent or dissolvable) when a sensor profile is created.

### Q

### Query

A structured syntax that specifies what endpoint data Artemis, Endgame's intelligent assistant, should search.

### R

### **Reputation Score**

An objective scoring based on third-party threat intelligence.

### Response

A remediation action taken on an endpoint.

### S

### Sensor

Monitoring software deployed to an endpoint that continuously monitors it for malicious behavior and executes hunts, as tasked by a user. A sensor is also known as an agent.

### **Sensor Profile**

A profile that contains the configuration settings required to deploy a sensor. After a profile is created, an installer executable becomes available to download for use in out-of-band deployment and sensor removal.

### Т

### Threats

Threat alerts capture specific malicious activity that occurs on an endpoint. The alerts that are considered threats are Credential Dumping, Credential Manipulation, Exploit, Malicious File, Permission Theft, Process Injection, and Ransomware.

### **Tradecraft Analytics**

Unique analytics for Process, Persistence, Network, and Users hunts that show uncommon or anomalous data in the Investigation Details view.



### V

### **Visual Selector**

An interactive tool that enables the user to view the results of an investigation by selecting various data components.



### Log in to Endgame

After the Endgame platform is successfully installed, you are ready to log in.

To log in:

- 1. Open a web browser and navigate to the IP or that hosts the platform.
- 2. In the **Username** and **Password** fields, type your username and password.
- 3. Click Login.

An Elastic company
Sign in with SSO
OR
Username
admin
Password
Login
About Endgame   Contact Us   Terms of Use © Copyright 2020 Elasticsearch BV. Version 3.16.0

Endgame login screen

**NOTE:** If your administrator has configured Single sign-on, click **Sign in with SSO** and enter your login credentials in the identity provider.





### **User Interface Overview**

Endgame's user-friendly interface has two stationary toolbars which provide access to all of the platform's tools, features, and components.



Endgame user interface

**NOTE:** Depending on your user role, you may have limited access and visibility to various content pages, tools, and features.



### Left Navigation Toolbar

٢	DASHBOARD Organizational summary	ENDGAME				0	Ask Artemis     Asy 17, 2029 9.14	er 8 AM I
	ENDPOINTS Manage and take action ALERTS Triage and remediation	CALEBOARD Coperational summer Coperations Coperations Coperation	Welcome Super Admin. Select the values in the clarst to the right or they are the low to live to a the selection of the selection of the darboard. Endpoints (3) Total) • Admts (40 Total) •	Open Alerts 446 Total 410 Automations	Endpoint Status 33 Total 11 Martin 4 Ummo	e Ive sitored	Endpoint OS	idows ax
4	INVESTIGATIONS Hunts and queries at scale	Hurts and queries at scale     ADMINISTRATION     Platform management.	C Endore your data in a Kitarra Dashboard	<u> </u>	<u>^</u>	0	<u>^</u>	
à	ADMINISTRATION Platform management		Top Alerts (ly Indoorta)	Top Exploit Alerts	Top Malware Alerts		Top Fileless Alerts (By Endpoints)	
	J		C DEIXTOP-Q8550JT 199		C DESKTOP-OBBSCUT	46	C DESKTOP-G88SCUT	
				•	O MALTA	12	C DESKTOP-GBBSCUT	
			O Invanishine 34	You have no Eighalt Aberta.	<ul> <li>deepika,machine1234567 (2)</li> </ul>	10	<ul> <li>win?w64wrigts</li> </ul>	
			O WHIKAHIBONES D		🔘 win7-déwrigtp	7	<ul> <li>win7+d4-wigp</li> </ul>	
			o wirleddwigg 12		O WINKAAHSONRS	5		

The Left Navigation toolbar is the main menu on the leftmost side of the screen.

### Left Navigation toolbar

It has five buttons that each display a corresponding content page when selected:

Button	Page	Description
٢	Platform Dashboard	View an overall status of endpoint and sensor health.
	Endpoint Dashboard	View and manage endpoints.
4	Alert Dashboard	View an overall summary of current alerts in your environment.
-11	Investigation Dashboard	View and manage investigations.



Button	Page	Description
\$	Administration	View and manage all administrative functions.

**NOTE:** On all content pages besides the Platform Dashboard, the Left Navigation toolbar is a condensed version that does not display the name of each page, however, you can hover your cursor over a button to view the corresponding page name.

### **Top Navigation Toolbar**

The Top Navigation toolbar contains three menu items that provide quick access to various tools and user interface elements.



Top Navigation toolbar

### **Online Help**

Access Endgame's knowledge base to view all user documentation and print full-text print guides.

### **Artemis Chat**

The **Ask Artemis** button launches Endgame's intelligent assistant, which enables you to search for specific endpoint data via an interactive chat interface.

শি

For more information about Artemis, see "Artemis Search Overview."



### **User Settings**

The **User Settings** tab displays your name, the number or letter that corresponds to your user role status (e.g., "A" if you are an administrator, "1" if you are a Level 1 user, etc.) and the current date and time. Select the tab to display the User Settings panel, which displays your user information and allows you to change your password, change your time zone, and log out of the platform.

	<b>NOTE:</b> The option to change the current password only appears if you logged in with a local user account.
CC Ask Artemi	is Welcome, Super Apr 30, 2019 5:41 PM UTC
User Setting	IS Logout
User Information	n
Name	Super Admin
Username	admin
Role	Admin
Password Change Passwor	vrd
Time Zone	
UTC	~

User Settings panel

### Change Your Password

**NOTE:** You can only change your password if you logged in with a local account. If you need to change your username or if you forgot your password, contact your administrator.

To change your password:



- 1. Select the **User Settings** tab.
- 2. On the User Settings panel, click Change Current Password.
- 3. Complete the requirements in the Change Password section:
  - a. In the Current Password text box, type your current password.
  - b. In the New Password text box, type a new password that meets the following minimum requirements:
    - Minimum 8 characters
    - 1 uppercase character
    - 1 lowercase character
    - 1 number
    - 1 special character (e.g., ~!@#\$%, etc.)
  - c. In the **Confirm New Password** text box, type the new password again.
- 4. Click **Save** to save your changes. If the password change was successful, a "Password Changed Successfully" confirmation appears.

### **Change Your Time Zone**

By default, Endgame sets the time zone to Coordinated Universal Time (UTC). You can change your time zone from the default by selecting the appropriate time zone from the **Time Zone** drop-down list.



**NOTE:** If you are running Internet Explorer 11, UTC is the only time zone option. However, please note that UTC time zones are not displayed in the platform.

### Log Out of Endgame

• Click **Logout** in the upper-right corner of the User Settings panel.



### Supported Endgame Platform Functions by Operating System

Each of Endgame's supported operating systems provides various sensor deployment, endpoint protection, and search functionality within the platform. Refer to the following table for guidance on which functions are supported. Especially keep this information in mind when creating a new sensor profile or applying an Endpoint Policy to a group of endpoints.

	Windows	Linux	macOS	Solaris
Persistent sensor	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
Dissolvable sensor	$\checkmark$	$\checkmark$	X	$\checkmark$
Modifiable signatures	$\checkmark$	X	X	X
In-band deployment	$\checkmark$	X	X	X
Out-of-band deployment	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
Enable endpoint protection	$\checkmark$	$\checkmark$	$\checkmark$	X
Add items to the exceptionlist	$\checkmark$	$\checkmark$	$\checkmark$	X
Add items to the blocklist	$\checkmark$	X	X	X
Artemis eventing	$\checkmark$	$\checkmark$	$\checkmark$	X
Create investigations	$\checkmark$	$\checkmark$	X	$\checkmark$
Add a trusted application	$\checkmark$	X	$\checkmark$	X



### **Platform Dashboard Overview**

The Platform Dashboard is the default view when you log in to the Endgame platform. It is a summary screen that displays overall system health and sensor status.

The dashboard contains three sections:

- 1. Expanded navigation
- 2. Alert and Endpoint Key Performance Indicator (KPI) charts
- 3. Alert KPI cards



Platform Dashboard



### **Expanded Navigation**

The Platform Dashboard provides an expanded navigation view that displays the name of each content page that corresponds to the six buttons on the Left Navigation toolbar. All other content pages in the Endgame platform display a condensed view of the toolbar that only displays the page buttons.

TIP: If you are in another section of the platform, hover your cursor over a button on the Left Navigation toolbar to view the page name.

٢	DASHBOARD Organizational summary	ENDGAME				0	Ask Artemis 🔥 Welcome, Super Aug 17, 2020 3.18
	ENDPOINTS Manage and take action ALERTS Triage and remediation	Charact Linguist      Control Control      Control	Webcome Super Admin. Select the values in the charts to the right or top airsts block to bit to a filtered view. The bicrospooling automatic Selections: 03 Tinal) + Alters (440 Tinal) +	Open Alerts 4466 Total 412 Detections	Endpoint Status 33 Total 11 has 4 there	we clive onitored	Endpoint OS 33 Total 11 Data 14 Mac 15 Galaria
•	INVESTIGATIONS Hunts and queries at scale ADMINISTRATION	ADMINISTRATION Platform management	C Explore your data in a Xibana Daabboard •	40	- Lo	0	40
₽	Platform management		Top Alerts (By Endports)	Top Exploit Alerts (By Endpoints)	Top Malware Alerts (By Endports)		Top Fileless Alerts (By Endpoints)
			O DER/T0P-Q880UT     S1		0 MALTA	12	
			inumedite 34	<b>V</b>	<ul> <li>despira,machine1234567 (2)</li> </ul>	10	🔘 withdenigg
			WHAAHIONES 18	The same of Lipson Autors.	🔘 vin?vd4vrigtp	7	<ul> <li>win7+d4+origqs</li> </ul>
			<ul> <li>wn7x64wrkpp</li> <li>12</li> </ul>		O WINKAHISONES	5	

Expanded navigation view

### **Alert and Endpoint Charts**

The top of the page displays three key performance indicator (KPI) charts that summarize the overall status of alerts and endpoints within your network:

KPI Chart	Description
Open Alerts	The number of active detections, preventions, and alert notifications.
Endpoint Status	The number of endpoints that fall into one of the following categories:
	Active: An endpoint with an installed sensor that currently is communicating with the



KPI Chart	Description						
	Endgame platform.						
	• <b>Inactive:</b> An endpoint with an installed sensor that currently is not communicating with the Endgame platform.						
	Unmonitored: An endpoint that has one of the following attributes:						
	It does not have an installed sensor.						
	<ul> <li>It has not communicated with the platform in two weeks or more.</li> </ul>						
	<b>NOTE:</b> If there was a sensor previously installed but has since been installed, that endpoint also falls in the "unmonitored" status.						
	For more information about how to run an endpoint scan to discover endpoints within your network,						
	see " <u>Discover New Endpoints</u> " in Chapter 2, <i>Endpoints</i> .						
Endpoint OS	The number of endpoints running on each of Endgame's supported operating systems.						

Each numerical value in the KPI charts, called a KPI slice, represents the number of endpoints or alerts that fall into a specific category. The total count displays in the center of the chart, whereas primary (highest count), secondary, and tertiary (if applicable) KPIs display outside the chart. KPIs update in real time as new data becomes available.

~
---

### Alert and Endpoint charts. Select a KPI to filter by the selected category.

Each KPI is also an active link, that when clicked, filters the Endpoints list or Alerts list by the selected attribute. For example, to view all currently active endpoints in the Endpoints list, select the **Active** link on the Endpoint Status chart.



### Alert KPI Cards

Beneath the Endpoint and Alert charts are four Alert KPI cards — individual snapshots that highlight the top five endpoints with the most alerts in the following categories:

Alert Card Name	Alert Type	Description
Top Alerts	• All	All alert types.
Top Exploit Alerts	<ul><li>Exploit Detection</li><li>Exploit Prevention</li></ul>	Detected or blocked exploits.
Top Malware Alerts	<ul> <li>Malicious File Detection</li> <li>Malicious File Prevention</li> </ul>	Detected or blocked potentially malicious files present on disk.
Top Fileless Alerts	<ul> <li>Process Injection Detection</li> <li>Process Injection Prevention</li> </ul>	Detected or blocked malware running in memory.

**NOTE:** The Endgame platform generates alerts based on Endpoint Policy configuration. For more information, see "Endpoint Policy Overview" in the *Administrator's Guide*.



	Alert Card nam	e Top Exploit / (By Endpoir	) Alerts ots)	❶ ⊶— Cli de ca	ck to view the scription of the alert rd		
	<b>O</b> 9J0	\$1-W7X86-D		2 ⊶—Nur	nber of alerts		
	<b>9</b> jg	I-w10x64l6-d		1			
Endpoint hostname —	• <b>O</b> 9J0	\$1-W2K8R2-D		1			
	<b>9</b> jg	I-w2k12r2-d		1			
	ole 💿	31-W7X64-D		1			
$\wedge$	Ø	40	Ð	Top M	Marc Alerts	Top Fieldense Alerts	0
Top Alerts		(By Endpoints)		(Ву	Enopoints)		
Top Alerts	21	By Endpoints)	2	(By	10	© 9JG1-W7X86-P	2
9JG1-W7X86-0 9Jg1-w10x886-d	21 C	(By Endpoints) 9 JG1-W7X86-D 9 Jg1-w10x64/6-d	2	(By 9JG1-W7X86-D 9Jg1-w10x8616-d	200pounta) 10 9	(b) Sugar-W/7X86-P 9/g1-w10x886-p	2
9461-47786-0 9361-47786-0 9391-4104866-0 9391-4104866-р	21 0	Iop Exploit Alerts         (By Endoords)           9.9.01-W7X86-D         )           9.9.01-W7X86-D         )           9.9.01-W2K882-D         )	2 ( 1 ( 1 (	(By 9JG1-W7X86-D 9Jg1-w10x8616-d 9Jg1-w10x8616-p	200ponta) 10 9 6	9.01-W7X86-P 9.01-W7X86-P 9.01-W7X86-D 9.01-W7X86-D	2 2 2
9,001-W7086-0           9,001-W7086-0           9,001-W106866-0           9,001-W106866-0           9,001-W106866-0           9,001-W106866-0	21 C 19 C 16 C	10p Exploit Alerts         (g) Exploit Alerts           0 JUST-W7X86-D         0           0 sub1-W7X86-D         0           0 sub1-W7X86-D         0           0 sub1-W7X86-D         0           0 sub1-W7X86-D         0	2 ( 1 ( 1 ( 1 (	(8) 9.061-W7X86-D 9.091-w10x866-d 9.091-w10x866-p 9.091-w10x846-d	10 9 6 6	(a) GLADINA,     (b) GLADINA,     (c) GLADINA,     (	2 2 2 2

Alert KPI cards. Select an endpoint hostname to view a filtered Alerts list.

Each row displays the hostname of the affected endpoint and its alert count. Like the KPIs in the Endpoint and Alert charts, when a row is selected, those attributes are applied as filters to the Alerts list. For example, to view the top Malicious File alerts that were generated for a single endpoint, select the first row on the "Top Malware Alerts" card. The Alerts list displays the filtered data in reverse chronological order with newest alerts at the top.

 A high alert count may indicate a potential data compromise; therefore, it is recommended you view alerts with the highest count first.

(missing or bad snippet) Click the Info button ① in the upper-right corner of an Alert KPI card for a description of the alert data.

# CHAPTER 2

# **ENDPOINTS**

Endpoints Overview	24
Discover Endpoints	24
Endpoint Dashboard Overview	
Endpoint Details Page Overview	
Endpoint Responses Overview	



### **Endpoints Overview**

An endpoint is any network-connected system, piece of equipment, or host that functions as a client or server in any capacity, such as desktops, laptops, or servers. Endgame provides customized sensor configuration that enables endpoint protection against unauthorized access, changes to the environment, and other adversaries.

### **Discover Endpoints**

The first step in deploying a sensor is to run a scan to discover network-connected endpoints.

**NOTE:** This tool is only compatible with Windows. If you are deploying a sensor via out-ofband management you can skip this step. Although only administrators can deploy sensors, any user can run an endpoint scan.

For more information about in-band and out-of-band sensor deployment, see "Sensor Deployment Overview" in the *Administrator's Guide*.

To scan for new endpoints:

- 1. On the Left Navigation toolbar, click the **ENDPOINTS** button **to** display the Endpoint Dashboard.
- 2. On the Action toolbar, click **Discover Endpoints**.
- 3. Complete the requirements in the **DISCOVER ENDPOINTS** dialog window:
  - ENTER IP ADDRESS/RANGE: In the text box, type the IP address or IP range to scan. To specify a range of IP addresses, enter a Classless Inter-Domain Routing (CIDR) prefix (e.g., 10.0.6.0/24) or use a hyphen between the first and last addresses (e.g., 192.68.1.4 192.68.1.56).
  - **CUSTOM PORT (Optional):** By default, Endgame discovers Windows endpoints with port 5985 (WinRM). If you want to override the default port with a non-standard one, enter the location in the text box.
- 4. Click Start Scan. A "Scan successfully initialized" message appears to confirm the scan has begun.



DISCOVER ENDPOIN Scan your environment to find more Endpoints to	ITS deploy.
Step 1: Field a Range Discover endpoints on your network to monitor. Enter comma separated IP A your scan. Endgame will discover Windows endpoints with Port 5985 (WinRt To override the default portwith a non-standard port, specify the location in t	Addresses, Ranges or CIDRs to start M) open and autocreate those devices. the Custom Port Field.
ENTER IP ADDRESS/RANGE	CUSTOM PORT (Optional)
10.0.6.0/24	Enter Non-Standard Port
Step 2: Discover Once an IP address or range is entered, select the Start Scan button to start confirmed successful, the scan will immediately be running in the backgrour have their status marked as <i>Unmonitored</i> . Select the <b>Deploy</b> button, in the <b>Ta</b> deploying sensors on those newly discovered endpoints.	discovering endpoints. Once nd. Newly discovered endpoints will ake Action dropdown, to start Start Scan

Discover New Endpoints dialog window

5. Click **Finish**. After the scan begins, the total number of endpoints steadily increases as they are identified, and the **Scan in Progress** indicator appears in the upper-right corner of the Endpoint Dashboard.



6. When the scan is finished, a "Scan Completed" confirmation appears with two options to either download the log file or dismiss the message. To download the scan log, click **Download Log File**.





### **Endpoint Dashboard Overview**

The Endpoint Dashboard provides an overview of all endpoints in the Endgame platform, gives an overall status of sensor health, and provides options to view, execute specific actions, filter, and manage endpoints.

To view the Endpoint Dashboard, click the **ENDPOINTS** button on the Left Navigation toolbar.

Endpoint Dashboard								? 😳 Ask Artemis	A Welco May 22	me, Supe 2, 2019 8:4	HT 6 PM UTC
302 301 All Windows	Li	1 <sup>nux</sup> 1		Apply More Policy Actions All I All I							Ð
302 302 Total Active	Ina	0 ctive 🕅	0 Unmonitored	d Isolated २३							0
GROUPS	1 - 5 of 5		JII 3 end End	Create Group spoints currently selected ∽ Ipoint Status: Active ⊗						1	- <u>50</u> of 302 < 🗲
Dynamic Static				ENDPOINT NAME adt-dhcp-172-31-4-178.eng.endgames.local	IP ADDRESS	OPERATING SYSTEM	POLICY Default	SENSOR VERSION	ALERTS	AD	GROUP
Windows 10	20			Active since May 20, 2019     DESKTOP-QBBSCUT	10.6.122.9	Windows 10 (v1803)	<u>Successful</u> Default	3.51.10	34		1 Group
Windows To	22			Active since May 20, 2019     HD-04i-241f61d4	10.50 174 122	Windows Server 2012 (SP1)	<ul> <li><u>Successful</u></li> <li>Default</li> </ul>	3 51 0	0	0	1 Group
Windows 8	63			Active since May 20, 2019     HD-04v-02b74d64     Active since May 20, 2010	10.32.116.227	Windows Server 2012 (SP1)	Successful     Default	3.51.0	0	0	1 Group
Windows Server 2012	69			HD-0bn-46dfa2ca	10.0.67.35	Windows 8.1 (SP1)	• <u>Successful</u> Default	3.51.0	0	0	1 Group
				+Active since May 20, 2019 +D-0jr-57ec92c9 • Active since May 20, 2019	10.174.40.63	Windows Server 2016 (v1607)	Successful	3.51.0	0	0	0 Groups
0				HD-Opm-7420113d • Active since May 20, 2019	10.180.215.205	Windows Server 2012 (SP1)	Successful     Successful	3.51.0	0	0	1 Group
				HD-0r5-43abea0b • Active since May 20, 2019	10.181.229.120	Windows Server 2016 (v1607)	Default     Successful	3.51.0	0	0	0 Groups
				HD-0wz-cda3dd95 • Active since May 20, 2019	10.8.113.2	Windows Server 2008 R2 (SP1)	Default • Successful	3.51.0	0	0	0 Groups
				HD-104-eebd6e5b • Active since May 20, 2019	10.212.138.40	Windows Server 2008 R2 (SP1)	Default • Successful	3.51.0	0	0	0 Groups
				HD-1c0-777f17c6 • Active since May 20, 2019	10.49.167.225	Windows Server 2012 R2 (SP1)	Default • <u>Successful</u>	3.51.0	0	0	1 Group
				HD-1gc-656d8041 • Active since May 20, 2019	10.44.207.171	Windows Server 2016 (v1607)	Default • Successful	3.51.0	0		0 Groups
				HD-1kz-43f6467d • Active since May 20, 2019	10.92.240.142	Windows 8 (SP1)	Default Successful	3.51.0	0	0	1 Group

### Endpoint Dashboard

The dashboard contains three major sections:

- 1. Action toolbar
- 2. Endpoints list
- 3. Groups panel





### **Action Toolbar**

The Action toolbar enables you to execute various endpoint actions, such as start an investigation, scan, assign a group, and deploy endpoints. It also contains key performance indicators (KPIs) to narrow endpoints by specific parameters.



Action Toolbar on the Endpoint Dashboard

### **Operating System and Endpoint Key Performance Indicators**

The toolbar contains operating system KPIs that display the total number of platform-connected endpoints and the unique number of endpoints running on Windows, Linux, macOS, and Solaris.

Beneath the toolbar, a secondary set of KPIs displays the number of endpoints that fall within a specific category:

КРІ	Description
Active	Endpoints with an installed sensor that currently is communicating with the platform.
Inactive	Endpoints with an installed sensor that currently is not communicating with the platform.
Unmonitored	Endpoints with no installed sensor.
Total	The total number of endpoints that are running on the selected operating system, or the total number of endpoints across all operating systems if the <b>All</b> KPI is selected.
Isolated	The number of endpoints that are in an isolated state and, therefore, cannot communicate with other network-connected endpoints. For more information about host isolation, see "Host Isolation Overview."



i

The default Endpoint Dashboard view displays all active endpoints. KPIs update in real time when new data is available.

Each KPI in the Endpoint Dashboard is an interactive link that filters the Endpoints list by the selected category. For example, to view all endpoints that are running on Windows with an active sensor, select **Windows**, then select **Active**. Filters are useful to narrow a large number of endpoints by specific criteria to execute a task on those similar endpoints simultaneously.

 You can also sort and filter columns within the Endpoints list. For more information, see <u>"Sort and Filter Columns in the Endpoints List"</u> in this topic.

### **Endpoint Actions**

The Action toolbar also contains additional menu items that start specific endpoint procedures when selected.

**NOTE:** The set of available options depends on the selected operating system KPI.

Tab	Description						
Create an	Starts a new investigation.						
Investigation		<b>NOTE:</b> You must select at least one endpoint to enable this task. This option is not available if the <b>All</b> KPI is selected.					
Apply Policy	Applies a new Endpoint Policy to selected endpoints.						
Discover Endpoints	Runs a Windows endpoint scan to discover network-connected endpoints.						
More Actions	Displays a list of specific actions you can take on selected endpoints:						
	Action	Description					
	Deploy	Deploys a sensor to one or more endpoints.					
	Respond	Executes a specific task on the endpoint, such as deleting or uploading a file.					
	Uninstall	Uninstalls the sensor from the endpoint.					
	Upgrade	Upgrades selected endpoints to a newer sensor version.					
	Delete	Removes the endpoint from the Endgame platform.					

An Elastic company

i If a sensor deployment or endpoint scan is in progress, a status indicator appears in the upper-right corner of the page. The number indicates how many procedures currently are running. 3 Deployments 3 Scans

In Progress

### **Endpoints List**

Ð

In Progress

The Endpoints list is an enumeration of all endpoints in the Endgame platform. The list organizes all relevant endpoint details in a table and is useful to view network statistics, find targeted data, and identify abnormal patterns in sensor status. For example, if the list indicates several sensors became inactive around the same time, this could signify an attempted data breach that requires immediate investigation.

Endpoints display in alphabetical order according to their hostname.



### Endpoints list

The columns in the Endpoints list display the following endpoint and sensor data:


Column Name	Description				
ENDPOINT NAME	The hostname of the endpoint. A secondary line displays the sensor status and the amount of time it has been in that state. The sensor status falls into one of the following categories:				
	Active: The sensor has established a connection to Endgame.				
	<ul> <li>Inactive: The sensor was previously connected to Endgame but is now disconnected.</li> </ul>				
	Unmonitored: No sensor is installed on the endpoint.				
	• <b>Deployment Failure:</b> The sensor failed to deploy to the endpoint. Click the link to view the deployment error message in a pop-up window.				
	<b>NOTE:</b> It is possible for two endpoints to have the same hostname. You can distinguish the difference by the IP address, or consider assigning it to a group. For more information about endpoint groups, see "Manage Groups" in this chapter.				
IP ADDRESS	The current IP from which the endpoint is communicating to the platform.				
OS	The current operating system running on the endpoint.				
POLICY	The associated Endpoint Policy and its policy application status. Click the policy name to view the configuration, and the status link (e.g., Successful, Failed, etc.) to download the response from the sensor.				
SENSOR VERSION	The sensor version running on the endpoint. If applicable, it also displays the status of the sensor upgrade.				
ALERTS	The number of current alerts for the endpoint.				
AD	Indicates if Active Directory (AD) is configured on the endpoint. Click the <b>Info</b> button to view Active Directory information.				
	<b>NOTE:</b> If there are updates made to your AD structure, those updates are reflected in the platform within 24 hours.				
GROUPS	Displays the number of groups assigned to the endpoint. Click the link to view the group names.				



i

The Endpoints list automatically updates when new data is available; however, if you have selected endpoints to begin a procedure (e.g., sensor deployment) and the Endpoint Dashboard is inactive for several minutes, a dialog box that says, "Your endpoint list is out of date. You must refresh to continue" appears. Click the **Refresh** button to display the new data.

#### Sort and Filter Columns in the Endpoints List

You can sort columns in the Endpoints list to change the order the contents in a column appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.

**NOTE:** You cannot sort the **AD** or **GROUPS** columns, however, you can search for specific group names.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

• Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow 1 or down arrow 1.

To search the column for a particular value:

• In the text box, type the text you want to find, then click Search. The list filters to display results that match the

entry. The currently filtered column is denoted by a 🖃 symbol.



Column sort and filter



TIP: Sorting or filtering Endpoint Policies are useful to view the status of policy application. For example, to view failed policy applications, select the **POLICY** column heading, then select the **Failed** option in the **POLICY STATUS** section.



If you have applied a filter to the Endpoints list, those values appear directly above the list, providing a comprehensive view of all filter criteria. To clear a filter from the list, click the **x** on the appropriate value.

			ers a	pplied to	the Endpo	oints list.					
Selec	t a filte	er tc	) clea	r it from t	he list.						
				1							
0		0		Man Januar 1	0.0	N		The design			
Oper	ating :	Syst	em: v	Vindows I		Sensor Versi	on: 3.51 🔞	9 Endpoi	nt Statu	IS: A	ctive 🐼
				1-1	Maria						0
17	13 1 Windowa Mar		2 <sup>-</sup> 1ux Sol	1 Apply Policy	More Actions						0
17 Al 1	13 1 Windows Mar	. u	2 T	1 Apply Policy aris At F	More Actions AL►						0
17 Al 17	13 1 Windows Mar 15 0 Active Inacti	e Li	2 mux Sol	1 Apply Policy At a ated	More Actions At ►						0
17 All V Total	13 1 Windows Mee 15 0 Active baset • *	e L	2 nux Sol nitored Isol Ity 4	1 Apply Policy All b ated IP	More Actions A≣ ⊨						•
17 All T Total	13 1 Windows Mar 15 0 Active Inacti	e Li Ne Unmo	2 Sol nux Sol nitored Isol to: 4 - 111 Create Gr	1 Apply Policy laria At b Cated bp map	More Actions At ►						0
17 All Total ROUPS	13 1 Windows Mar 15 0 Active Insct 1-5 of 5	e Li	2 nux Sol nitored Isol Re 4 4 111 Create Gr 3 endpoints cu Operating Syst	1 Apply Policy At > 0 Isted by may rently selected ~ rently selected ~	More Actions A >	Active O					0 0 1-2d7
17 All Y Total ROUPS	13 1 Windows Max 15 0 Active Inacti 1 - 5 of 5	o U Ive Unmo	2 Sol	1 Apply policy area of the by mage memory solutions of the solutions of th	Mora Actions A3 P mine: 251 O Endpoint Status IE ADDR555	Ame O	POLICY	# SENSOR XIERON	ALERTS	AD	• • 1-2 of 7 < > 9800/2
17 All Y Total ROUPS Q Dynamic Stat abod	13 1 Windows Ma 15 0 Active Inact 1-5 of 5 1	a L	2 Sol nitored look by d 3 endpoints cu Operating Syst E ENDP E DESK - Acti	1 Apply Policy 2014 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	More Actions AT > Endpoint Datase (CADRES) 10.6.244.174	Active © © OCEALING SYSTEM Wordsows 10 (1902)	PSuCr rabid_Sjane	F EDUCR VIENCE 25110	ALERTS	AD -	• • 1-2 of 7 > • • • •
17 Al 17 Total ROUPS Q Dynamic Stat abod	13 1 Windows Ma 15 0 Active Insch 1-5 of 5 1 15 2	e Uness	2 nux So 2 nifored loo 10 40 Create Gr 3 endpoints cu Operating Syst 0 ENDP 2 DESK 2 DESK 2 DESK	1 Age/y Policy All 9 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	More Actions All >	Action © F 025437963 535154 Windows 10 (+102) Windows 10 (+102)	PSUCY rable_Spore * Successful rable_Spore	♥ SINSOR VIRSON 23110 23110	<u>ALETS</u> 0 0	AD -	• • • • • • • • • • • • • • • •
17 Al 17 Total Rours Q Dynamic Stat abod lg.statag Rama	13 1 Windows Ma 15 0 Active Detect 1-5or5 1 10 2 2	e L	2 So nux So 2 min So 2 min So 2 min So 3 endpoints cu 0 persting Syst LNDP DESK Action So So System So System So	Accivity Policy Poli	More Actions At p ersise: 2.51 C Endpoint Datase II: ADDRESS II: 0.6.244, 174 II: 0.6.302 II: 0.6.831.19	Admir © © 0058ATING SISTIM Windows 10 (+160) Windows 10 (+160) Windows 10 (+160)	PSNKX rahol	♥ SENSOR VIRION 3 51 10 2 51 10 3 51 10 3 51 10	ALETTS 0 0	<u>AD</u> - -	• • • • • • • • • • • • • • • • • • •
17 Ail Tradi 20 Rours C. Parante abcd igoptetag Rena	13 1 Wedows Ma 15 0 Active Detect 1-5or5 € 10 22 2 1		2 So 2 Indexed land 2 Indexed land 4 Indexe	Angly Policy All 3 and a second	More Actions         M           AT         ►           MEADOMESE         MEADOMESE           10.6.34.174         10.6.30.82           10.6.34.194         10.6.34.194	Active © F 0252A1190 5151114 Wordews 10 (+102) Windows 10 (+107) Wordews 10 (+107)	POLICY * Machanita rabid_Sjone * Baccanita Konsente * Soccanita * Soccanita	♥ 10000 VVRION 3.51.10 3.51.10 3.51.10 3.51.10	ALEXT3 0 0 0 278	AD - - 0	0 1-247 () 68002 1.0me 1.0me 1.0mes 1.0mes
17 17 Toral Q Q Q Q Q Q Q Q Q Q Q Q Q	13 1 Mondows Monor 15 0 Dect 2 1-5 of 5 2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3		2 So 2 Instand 2 Instand 2 Instand 4 Instant 4 Ins	Accol Pocky Accol and Accol Acco	More Actions         Image: Computer Statute           III         Image: Computer Statute           IIII         Computer Statute           IIII         Computer Statute           IIIII         Computer Statute           IIIII         Computer Statute           IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	(Attive ■) # GEESATING SYSTEM Windows 10 (+162) Windows 10 (+162) Windows 10 (+162) Windows 10 (+167) Windows 10 (+167)	PSASY + Machal, Sjame + Saccastal reMul, Sjame + Saccastal Passes - Saccastal - Saccastal	♥ 20000 ¥X8500 2.31.10 2.31.10 2.31.10 2.31.10 2.31.10 2.31.10	ALETTS 0 0 278 21	A2 - - - 0	0 1-247 1000 10
17 17 17 17 17 10 10 10 10 10 10 10 10 10 10	13 1 Mindows 15 0 1-5 of 5 1-5 of 5 2 2 2 3 5		2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Accolution     A	More Actions         Endpoint Statute           III 0.0401         50.0000           III 0.0401         50.0000           III 0.6401         50.0000           III 0.6402         50.0000	Justice         Image: Contract of a statistical statis statistext statistical statisti statis statistical statistical	ESUSY - Shuky Sjune - Shuky Sjune - Successful - Succe	<ul> <li>States Vision</li> <li>23.10</li> </ul>	ALETTS 0 0 378 21 0	AQ - - 0 0 0	0 0 1-247 (5) 6804 1004 1004 1004 1004 1004 1004 1004 1

Filtered columns display the criteria in the Endpoints list



#### **Filter Endpoint Groups**

Filter endpoint groups via the Groups panel. For more information about endpoint groups, see "Endpoint Groups Overview."

To filter the Endpoints list by a specific group:

• Select the appropriate group name in the Groups panel.

To search for a specific group name:

• Begin typing text in the search bar. The list of groups filters to display results that match the typed text.

SEAR Enter grou	<b>SEARCH</b> Enter text to filter the list of groups.					
C	ROUPS	1 - 8 of 8 🔇	>			
	AD DOMAIN = DC	18				
	CENTOS	3	•••			
	MACOS SIERRA	11	•••			
	UBUNTU	5				
	WINDOWS 10	12	•••			
	WINDOWS 8	22				
	WINDOWS SERVER 201	6 16	•••			
	WINDOWS SERVER 201	9 8	•••			

Filter groups via the Groups panel

#### **Page Pagination**

In the upper-right corner above the list is a range display, which displays the current number range of endpoints out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 endpoints display per page; however, you can change the number to a preferred choice:

- 1. On the range display, click the number link. For example, if the range display is 1-50, click 50.
- 2. In the Max count of text box, enter a new number between 1 and 500.
- 3. Click  $\checkmark$  to save your changes.





# **Download the Endpoints List**

You can download the current Endpoints list to a comma-separated values (CSV) file or you can download the raw JSON to an external file. Any sort and filter preferences applied to the list are retained in the downloaded file.

To download the Endpoints list:

1. In the upper-left corner of the Endpoint Dashboard, click Download JSON or Download CSV.



2. When the download is complete, open or save the file from your browser.



### **Endpoint Groups Overview**

An endpoint group is a label assigned to selected endpoints and enables users to categorize endpoints with similar attributes. Groups assist with endpoint management — especially if there is a large amount of endpoints in your organization — and are useful to execute a task on multiple endpoints simultaneously, or quickly find endpoints with the same criteria. Take the following scenario as an example:

You are an administrator and have 5,000 endpoints in the Endgame platform. You need to organize endpoints into groups by department (e.g., Sales, Marketing, etc.) and operating system so that you can install security patches on the appropriate machines when needed.

Groups are divided into two categories: static and dynamic. Static groups are based on manual endpoint selection, whereas dynamic groups are based on selected filters that determine which endpoints are included in the group. Any future endpoints added to the Endgame platform that match the filtered criteria — whether they are active or inactive — are automatically added to that dynamic group.

The list of groups appears in the "Groups" panel, located to the left of the Endpoints list. You can create a maximum of 500 groups and can manage them at any time.



Groups panel



#### **Create an Endpoint Group**

Create a new static endpoint group when you want to manually select specific endpoints to add to a new group. Create a new dynamic group when you want to select filters to control which endpoints are added to the group. Any new endpoints that match the filtered criteria are automatically added to the dynamic group.

**NOTE:** Level 2 users and up can create groups. Level 1 users can view groups.

#### **Create a Static Endpoint Group**

1. In the Endpoints list, select the box to the left of each endpoint to add to the new group.

**NOTE:** If desired, you can create an empty group and add endpoints to it later. If so, proceed to Step 3 and see "<u>Manage Endpoint Groups</u>" for information about how to add endpoints to a group.

TIP: If you are selecting endpoints now, it is highly recommended to sort or filter the Endpoints list so that all endpoints you want to group are displayed. For more information, see "Endpoint Dashboard Overview." Also, keep in mind that you can increase the number of endpoints that display per page by selecting the number link in the upper-right corner and entering the desired number, up to 500.



2. Select all the appropriate endpoints in the list to add to the group.

TIP: To select all endpoints on the current page, click the box to the left of the "ENDPOINT NAME" column heading.

- 3. Click **Create Group** to display the Create Group dialog window.
- 4. In the "Create Static Group" section, click **Select**.
- 5. In the "Group Name" text box, enter a unique name for the group.
- 6. In the "Endpoints in Group" section, ensure the number of selected endpoints is correct.
- 7. Click **Save**. A "*Group Name* has been created" confirmation appears.

ENDGAME.
An Elastic company

Create Static Group	
Group Name	
Windows 7	
Endpoints in Group (11)	
Close	Back Save

**NOTE:** If you enter a group name that already exists, an "A group with this name already exists" message appears.

8. Click **Close**. The new group appears in the Groups panel.

#### Create a Dynamic Endpoint Group

- 1. Filter the Endpoints list with all the appropriate criteria for the group you are creating.
- 2. Click Create Group to display the Create Group dialog window.
- 3. In the "Create Dynamic Group" section, click Select.
- 4. In the Group Name text box, enter a unique name for the group.
- 5. In the "Select filters" section, ensure the filters you applied are correct. Once the dynamic group is created, you cannot edit the filters unless you delete and recreate the group.

**NOTE:** If you have applied any unsupported filters (i.e., policy status, endpoint status, alerts) those appear in the "Unsupported Filters" section and are not applied to the dynamic group. However, keep in mind that unsupported filters are still applied to the current Endpoints list view; therefore, it is possible that the dynamic group will include more endpoints than what is displayed on the page.

6. Click **Save**. A "*Group Name* has been created" confirmation appears.

Create Dynamic Group	
Group Name	
Windows 8 Sensor 3.51	
Selected filters (to be applied to this dynamic group):	
Operating System: Windows 8 Sensor Version: 3.51	
Unsupported filters (will not be applied to this dynamic group):	
A Policy Status: Successful A Endpoint Status: Active	
Close	Back Save

7. Click **Close**. The new group appears in the Groups panel.

#### Manage Endpoint Groups

The Group panel provides options to add, delete, and filter groups for easy endpoint management.



**NOTE:** You cannot add or delete endpoints from dynamic groups since they are based on previously applied filters.

#### Add Selected Endpoints to a Static Group

- 1. In the Endpoints list, select the box to the left of each appropriate endpoint for which to add a group.
- 2. In the Groups panel, locate the group for which to add selected endpoints.

TIP: If you have a large number of groups, type some text in the search bar to filter the list.

3. Click the **Overflow** menu [...], then select **Add Selected Endpoints**. The new total number of endpoints in the group is reflected in the number count.

GROUPS	1 - 6 of 6 < >	
٩		
Dynamic	Static	
Centos	1	
Windows 10	1	
Windows 7	11	
Windows 8	Add Selected Endpoints Remove SeleOd Endpoints	
Windows S	Delete Group	
Windows Se	ver 2019 12 ••••	

#### Groups panel in the Endpoints list

#### **Remove Selected Endpoints from a Static Group**

Removing endpoints from a group does not delete the group in its entirety; it solely disassociates the endpoint from that group.

To remove one or more endpoints from a static group:

1. Locate the group from which to remove the endpoint, then click the group name to filter the Endpoints list by that group.

TIP: If you have a large number of groups, use the search bar to filter the list.



- 2. In the Endpoints list, select the box to the left of each appropriate endpoint to remove from the group.
- 3. On the Groups panel, click the **Overflow** menu . , then select **Remove Selected Endpoints**. The new total number of endpoints in the group is reflected in the number count.

#### **Delete an Endpoint Group**

Deleting an endpoint group removes it from the Endgame platform, and, therefore, and removes the group relation of any assigned endpoints. If you want to remove an endpoint from a group but retain the group in the platform, see "<u>Remove</u> Selected Endpoints from a Static Group" in this topic.

To delete a group:

- 1. On the row that contains the group to delete, click the **Overflow** menu . , then select **Delete Group**.
- 2. In the dialog box that says, "You are about to delete *group name*. Are you sure?" click **Delete**. A "Successfully deleted Group" confirmation appears.

Delete Group	
You are about to delete <b>WIND</b>	OWS. Are you sure?
Ormal	Delete
Ormani	Delet

3. Click Finish.



# **Endpoint Details Page Overview**

The Endpoint Details page provides comprehensive details of the selected endpoint that enable you to analyze overall sensor health, view activity that occurred on the endpoint, and find specific data. The page is composed of two panes; the left pane contains the Endpoint Overview and Activity Timeline, and the right pane displays event details.

To view an Endpoint Details page, click an endpoint in the Endpoints list.

The page has three sections:

- 1. Endpoint Overview
- 2. Activity Timeline
- 3. Activity Details pane

DESKTOP-QBBSCI	т т	ake Action 🗸 🗸	Process Mar 29, 2019 10:49:05 PM UTC					View Investigation Details Down	nload Raw Data	
IP Address: Status:	10.6.2.110  • Active since Mar 28, 2019  Mindaw 10 (-1002)	1.	PROCESS NAME	PID	PPID	PARENT PROCESS NAME	PATH	COMMAND LINE	SIGNER	AUTHE
Groups:	Windows 10	View All	conhost.exe	3200	4016		C:\Windows\System32\conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0x4	Microsoft Windows	trustec
Policy:	Default • Successful CN=ENDPOINT-W-0-01.0U-Desktops	00-	CSTSS.exe	400	392		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trustec
Activity Timeline	Workstations,OU=Computers_DEMOj endgamelabs,DC=net	DC-demo,DC-	csrss.exe	484	476		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trustec
Expand Activity reed			Registry	88	4		Registry			
Mar 29, 2019 10:49:06 PM UTC	Network Sensor Collection	2	sshd.exe	3176	4016		C:\cygwin\usr\sbin\sshd.exe	"C:\cygwin\usr\sbin\sshd.exe"		noSign
Mar 20, 2010	Process	_	System	4	0	System Idle Process				
• 10:49:05 PM UTC	Sensor Collection	- 1	L Memory Compression	n 2264	4	System	MemCompression			
Mar 29, 2019 10:49:05 PM UTC	Removable Media Sensor Collection		L <sub>smss.exe</sub>	316	4	System	C:\Windows\System32\smss.exe		Microsoft Windows Publisher	trustec
Mar 29, 2019 10:49:05 PM UTC	Applications Sensor Collection		wininit.exe	508	392		C:\Windows\System32\wininit.exe		Microsoft Windows Publisher	trustec
			L fontdrvhost.exe	724	508	wininit.exe	C:\Windows\System32\fontdrvhost.exe	"fontdrvhost.exe"	Microsoft Windows	trustec
Mar 29, 2019 5:55:25 PM UTC	Policy Response (Success) Administrator Configuration		L Isass.exe	636	508	wininit.exe	C:\Windows\System32\lsass.exe	C:\WINDOWS\system32\lsass.exe	Microsoft Windows	trustec -

Endpoint Details page



#### **Endpoint Overview**

The Endpoint Overview section displays general information about the endpoint, including the name, IP address, status, operating system, associated Endpoint Policy, and if applicable, Active Directory information and assigned groups.

The Take Action menu contains a list of options that enable you to execute one of the following endpoint tasks:

Menu Option	Description
Start Investigation	Starts a new investigation.
Respond	Executes an endpoint response.
Apply Policy	Applies a different Endpoint Policy to the current endpoint.
Uninstall	Uninstalls the sensor and the endpoint from the platform.
Delete Endpoint	Deletes the endpoint from the platform, but retains the sensor.



Endpoint Overview section



i

#### About Sensor Activity Status

If a sensor's status changes within 24 hours from the time the page is viewed, the user interface displays the time the status took effect:

```
Status: • Active since 4:05 PM UTC
```

After 24 hours have passed, the date the status took effect displays in MM DD, YYYY format:

Status: • Active since Jan 29, 2019

**NOTE:** If you want to see the exact time the status took effect after the 24-hour time period has passed, hover your cursor towards the right of the date stamp.

#### **Activity Timeline**

The Activity Timeline chronologically lists every activity that occurred on the endpoint, with the most recent activity at the top. Some endpoint activities in the timeline may include:

- Completed hunts for an investigation
- Sensor installs and uninstalls
- Alert detections and preventions
- Executed response actions (e.g., Get File, Download File, etc.)
- Administrative actions (e.g., Endpoint Policy changes)

**NOTE:** By default, the System Configuration hunt runs once an hour on all monitored endpoints.

Each timeline entry is called an **event card**. Each event card displays the activity type (e.g., collection, alert, response, etc.), a symbol that identifies the activity type, and the date and time the activity occurred.

Depending on the activity type, an event card may also display supplemental information in red or green type. For example, an event card for a detection indicates the severity level, or an event card for an executed endpoint response (e.g., kill process) indicates if it was a success or failure.





#### Activity Timeline

Scroll the timeline to view the history of all endpoint activity. It is recommended you pay close attention to any anomalies that may require further investigation. If any new activity is recorded while you scroll the timeline, a notification displays the number of new items. Click **BACK TO TOP** to go to the beginning of the timeline.



#### **Filter the Activity Timeline**

Although the timeline displays all endpoint activity, you can filter the timeline to specific criteria.

#### Filter by Category

In the timeline, endpoint activities are separated into six categories, each denoted by a distinct symbol:

Category	Symbol	Description
ALL	N/A	All activity types.
Preventions	٤	Malicious activities that were detected and blocked.



Category	Symbol	Description
Detections	ŧ	Potential malicious activities that were detected and require resolution.
Collections		Data returned from a hunt (e.g., process survey, network survey, etc.).
Responses	Q	Response actions executed on an endpoint (e.g., delete file, execute file, etc.).
Admin Configs	\$	Sensor configuration set by an administrator.

To filter the timeline by a specific category, click the **Filter By:** drop-down arrow and select the appropriate category from the list.



Activity Timeline filter



#### Filter by Date and Time

To filter the timeline by a date and time range:

1. In the **Filter By:** field, click the **Calendar** button



- 2. Select a start date from the calendar widget that appears. Use the < and > arrows to navigate to previous and following months.
- 3. To specify a starting time other than the default 12:00 AM UTC, place your cursor in each text box and enter the appropriate time in HH:MM format. Select **AM** or **PM**.
- 4. Specify an end date and time using the same procedure in steps 2 and 3.
- 5. Click Apply Filters to update the timeline.



Activity Timeline date and time filter



#### **Activity Details Pane**

The Activity Details pane displays all-inclusive details about the selected activity in the timeline. The pane also provides options to view investigation details, download the raw JSON, and, for specific hunts, execute an endpoint response.

**NOTE:** Some activities — such as IOC Search and administration configurations — display the raw JSON in the details pane. You can download this raw JSON by clicking **Download Raw Data** > **RAW TASK DATA**.

								VIEW INVESTIGATION DETAILS View results of the associated investigation on the Investigation Details page.	DOWNLOAD RA Download the ra task data or the from the sensor.	W DATA w JSON for th data returned
DESKTOP-QBBS	SCUT Take A	ction 🗸	Process Mar 29, 2019, 10:49:05 PM UTC					View Investigation Details	Download Raw Data	
IP Address:	10.6.2.110									_
Status:	Active since Mar 28, 2019	Θ	PROCESS NAME	PID	PPID	PARENT PROCESS NAME	PATH	COMMAND LINE	SIGNER	AUTHI
Groups:	Windows 10	View All	conhost.exe	3200	4016		C:\Windows\System32\conhost.e	xe \??\C:\WINDOWS\system32\conhost	exe 0x4 Microsoft Windows	trustec
Policy:	Default • <u>Successful</u>		csrss.exe	400	392		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trustec
Active Directory Distinguished Nam	Filter By: All	<ul><li>▼</li></ul>	CSTSS.exe	484	476		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trustec
		*	Registry	88	4		Registry			
Mar 29, 2019 10:49:06 PM UTC	Sensor Collection		sshd.exe	3176	4016		C:\cygwin\usr\sbin\sshd.exe	"C:\cygwin\usr\sbin\sshd.exe"		noSigr
May 20, 2010	- Process	- 1	System	4	0	System Idle Process				
• 10:49:05 PM UTC	Sensor Collection		L Memory Compression	2264	4	System	MemCompression			
Mar 29, 2019 10:49:05 PM UTC	Sensor Collection		L <sub>smss.exe</sub>	316	4	System	C:\Windows\System32\smss.exe		Microsoft Windows Publisher	trustec
Mar 29, 2019 10:49:05 PM UTC	Sensor Collection		wininit.exe	508	392		C:\Windows\System32\wininit.ex	a	Microsoft Windows Publisher	trustec
			L fontdrvhost.exe	724	508	wininit.exe	C:\Windows\System32\fontdrvho	st.exe "fontdrvhost.exe"	Microsoft Windows	trustec
Mar 29, 2019 5:55:25 PM UTC	Administrator Configuration		L Isass.exe	636	508	wininit.exe	C:\Windows\Svstem32\lsass.exe	C:\WINDOWS\svstem32\lsass.exe	Microsoft Windows	trustec

Activity Details pane



#### **View Investigation Details**

The **View Investigation Details** button in the upper-right corner navigates to the Investigation Details page to display results of the associated investigation. This button is only available when you select a hunt in the timeline.

**NOTE:** IOC Search and System Configuration hunts do not have an Investigation Details view. Although the **View Investigation Details** button is available for IOC Search collections (it is not available for System Configuration hunts), if you click it, IOC Search does not appear in the hunt type selection list. However, if IOC Search is the sole hunt in the investigation and you click **View Investigation Details**, a message that says, "View results for this Hunt in search" appears. Click this link to view IOC Search results on the general search page.

For more information, see "IOC Search Overview."

#### **Download Raw Data**

The **Download Raw Data** button enables you to either download the raw task data, which is the data for the task initiated by the sensor, or the raw response data, which is the data returned from the sensor.

To download the raw JSON:

- 1. Click **Download Raw Data** in the upper-right corner, then select **RAW TASK DATA** or **RAW RESPONSE DATA** from the menu.
- 2. Open the file in an external application or save it to a directory.

TIP: To see the advanced configuration for a specific hunt, filter the timeline by "Collections," select the appropriate activity, then download the raw task data.

#### **View Corresponding Collections**

Some hunts, which appear as collections in the timeline, have one or more corresponding collections — distinct snapshots of specific data. For example, **System Configuration** has collections that display the drives, interfaces, memory usage, DNS and patch information.

To view a corresponding collection:

• In the details pane, click the Hunt arrow (e.g., Operating System Info, Network, etc.) and select the appropriate collection from the list.





System Configuration collections view

#### **Execute an Endpoint Response**

For Process and Network hunts, which identify running processes, you can terminate a process or download a file directly from the details pane:

- 1. In the "PROCESS NAME" column, select the appropriate process for which to kill or download a file.
- 2. In the "PROCESS DETAILS" window, select Kill Process or Get File.
- In the dialog box that asks if you are sure you would like to kill the process or download the file, click Yes. If you chose Get File, a "Get File submitted" message appears to confirm the file was downloaded. If you chose Kill Process, a "Kill Process submitted" message appears to confirm the process was terminated.
- 4. Click Finish.



Kill Process response from the details pane

# **Endpoint Responses Overview**

Endpoint responses enable you to execute individual tasks for multiple endpoints simultaneously. For example, if you found a suspicious file running on a group of endpoints, you could initiate a Delete File response to remove the file from the



뇌

appropriate endpoints. Or, if you received an alert notification for a detected process injection, you could initiate a Kill Process response to terminate the malicious process.

To execute an endpoint response:

In the Endpoints list, select the box to the left of each appropriate endpoint.

1. On the Action toolbar, point to More Actions, then click Respond. An alphabetical list of response types appears.

For complete descriptions of response types, see "<u>Endpoint Response Types and</u> Advanced Configuration Options."

- 2. In the left column, click the option button to the left of the response to execute.
- 3. In the right column, enter advanced configuration for the selected response. Advanced configuration options vary according to the response type, therefore, to ensure accuracy, review all options and enter property values accordingly.
- 4. Click Create Response.

**NOTE:** If any required property values are missing, you cannot execute the response until those values are entered.

	ENDPOIN Select endpoint respon	T RESPONSE ses and configurations below.
Select and Configure Resp You have currently selected 1 End	oonse(s) Ipoint . Once configur	red, select Create Response to launch your response.
RESPONSE TYPE		ADVANCED CONFIGURATION
O Delete File	<u>COLLAPSE</u>	File Path
Execute File	ADVANCED	C'usersliphdoe'testfile txt
Get File	ADVANCED	
Isolate Host	ADVANCED	
Kill Process	ADVANCED	
Suspend Thread	ADVANCED	
Upload File	ADVANCED	
Cancel		Create Response

Delete File endpoint response

#### Additional Ways to Execute an Endpoint Response

Proprietary Elasticsearch B.V. information.



You can also initiate an endpoint response by choosing from the following options:

• On the Endpoint Details page, click **Take Action** in the upper-left corner, then select **Respond**.

Endpoint Details					
DESKTOP-QBBSCUT Take Action					
		Start Investigation			
IP Address:	10.6.176.206	Respond			
Status:	• Active since 5:48 PM UTC				
OS:	Windows 10 (v1803)	Uninstall			
		Delete Endpoint			
Groups:	V1803, WINDO				
Policy:	Default • <u>Successful</u>				
Active Directory Distinguished Name:	-				

- If you are viewing the Endgame Resolver<sup>™</sup> Attack Visualization for an alert, you can initiate the **Retrieve File** (equivalent to Get File) or **Kill Process** response. Some alerts also contain the Retrieve File, Download File, and Kill Process responses on the **Take Action** menu on the Alert Metadata panel.
- Display results of a Process or Network hunt in the Activity Details pane, select a process name, and then choose a response action in the **PROCESS DETAILS** dialog box.

Process Name		PID	PPID	Parent Process Name	Path	
csrss.exe	PROCESS DE	TAILS	010		0.000	00)
L conhost.exe	SHA 256	4fa06c	2d9ffc710	2e3c9d7afcbf06704	564bf527afd476eac4549	c6b4fbb80c3
└ conhost.exe	MD5	ce476f	23405aado	:46039ac13127df47	3	
csrss.exe	SHA1	ab5823	24df6a700	d5631ed6d47fe5cae	58e440d86	
explorer.exe		SS				GET FILE

# Host Isolation Overview

Isolating a host temporarily prevents it from communicating with all systems besides the Endgame platform until the host is released. Isolating a host is useful to prevent malicious activity from spreading, as it blocks adversaries from making lateral movement across other endpoints. However, if necessary, you can allow isolated hosts to connect to specified IP addresses. For more information, see "Allow Isolated Hosts to Connect to Other IP Addresses" in this topic.



i

Host isolation is only compatible with Windows and macOS endpoints and the following sensor versions:

1) Windows: 3.0 and above

2) macOS: 3.51.6 and above

#### Isolate a Host

**NOTE:** To protect unwanted isolation, only Level 3 and Admin users can isolate a host. In addition, you can only isolate one host at a time.

Depending on where you are in the platform, choose one of the following options:

#### If you are viewing an alert on the Alert Details page:

1. On the Alert Metadata panel, click **Take Action**, then select **Isolate Host** from the list.

**NOTE:** Ensure the alert's affected endpoint is the one you want to isolate.

2. On the dialog box that says, "You are about to isolate *endpoint hostname*. This will disconnect the endpoint from the network and only allow connectivity to the endpoint management console" click **Yes**. A "Request successful" message appears.

Isolate Host	
You are about to isolate <b>2gxa-w81x64-d</b> . This will disconnect the endpoint from only allow connectivity to the endpoint management console.	m the network and
Cancel	Yes



3. Click **Finish** to close the dialog box. To view the sensor response in the endpoint's Activity Timeline, click **Go to Endpoint**.

**NOTE:** When the sensor initially receives the isolation request, the endpoint status — which is displayed on the Alert Metadata panel and in the Endpoints list — briefly changes to "Isolation Requested" until the isolation is successful, at which point the status changes to "Isolated." For more information, see "View Host Isolation Statuses" in this topic.

#### If you are viewing the Endpoint Details page:

- 1. In the Overview section located in the left pane, click **Take Action**, then click **Respond**. An alphabetical list of response types appears.
- 2. In the left column, click **Isolate Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
- 3. Click Close.

ENDPOINT RESPONSE Select endpoint responses and configurations below.				
Select and Configure Respon	ise(s)			
You have currently selected 1 Endpoi	nt . Once configur	red, select Create Response to launch your response.		
RESPONSE TYPE		ADVANCED CONFIGURATION		
Delete File	ADVANCED	Coloring Indiate Unit will discompatible		
C Execute File	ADVANCED	endpoint from the network. Only the Endgame platform will be able to communicate with the		
Get File	ADVANCED	host.		
O Isolate Host	<u>COLLAPSE</u>			
Kill Process	ADVANCED			
Suspend Thread	ADVANCED			
Upload File	ADVANCED			
4	×			
Cancel		Create Response		

Isolate host endpoint response





#### If you are viewing the Endpoint Dashboard:

- 1. On the Action toolbar, select the **Windows** or **Mac** tab to filter the Endpoints list by those running on the selected operating system.
- 2. In the Endpoints list, select the box to the left of the endpoint to isolate. Ensure you select only one.
- 3. On the Action toolbar, point to **More Actions**, then click **Respond**. An alphabetical list of response types appears.

**NOTE:** If an operating system tab is not selected, the "Respond" option does not appear in the **More Actions** menu.

- 4. In the left column, click **Isolate Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
- 5. Click Close.

Y To filter the Endpoints list by isolated hosts, select the **Isolated** tab on the Action toolbar.

#### **Release a Host**

Releasing a host reestablishes communication between the host and other network-connected endpoints.

To release a host:

Depending on where you are in the platform, choose the appropriate option below:

#### If you are viewing an alert on the Alert Details page:

- 1. On the Alert Metadata panel, click **Take Action**, then click **Release Host**.
- 2. On the dialog box that says, "You are about to release *endpoint hostname*. This will reconnect the endpoint to the network." click **Yes**. A "Request successful" message appears.



3. Click **Finish** to close the dialog box. To view the sensor response in the endpoint's Activity Timeline, click **Go to Endpoint**.

#### If you are viewing the Endpoint Details page:

1. In the Overview section, located in the left pane, click **Take Action**, then select **Respond** from the list. An alphabetical list of response types appears.



- 2. In the left column, click **Release Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
- 3. Click Close.

ENDPOINT RESPONSE Select endpoint responses and configurations below.						
Select and Configure Respon	Select and Configure Response(s)					
You have currently selected 1 Endpoi	nt . Once configu	red, select Create Response to launch your response.				
RESPONSE TYPE		ADVANCED CONFIGURATION				
Delete File	ADVANCED	Selecting Deleges Heat will allow this and sort				
Execute File	ADVANCED	to reconnect to the network.				
Get File	ADVANCED					
Kill Process	ADVANCED					
Release Host	<u>COLLAPSE</u>					
Suspend Thread	ADVANCED					
Upload File	ADVANCED					
4	۰.					
Cancel		Create Response				

Release host endpoint response

#### If you are viewing the Endpoint Dashboard:

- 1. On the Action toolbar, select the **Windows** or **Mac** tab to filter the Endpoints list by those running on the selected operating system.
- 2. In the Endpoints list, select the box to the left of the endpoint to release from isolation. Ensure you select only one.
- 3. On the Action toolbar, point to More Actions, then click Respond. An alphabetical list of response types appears.

**NOTE:** If an operating system tab is not selected, the **Respond** option does not appear in the **More Actions** menu.

- 4. In the left column, click **Release Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
- 5. Click Close.





#### **View Host Isolation Statuses**

When the sensor receives a host isolation or release request, Endgame displays one of the following endpoint statuses throughout various places in the Endgame platform to indicate the progress:

Host Status	Description
Isolation Requested	The Endgame platform sent an 'isolate host' task to the sensor.
Isolated	The host is isolated and, therefore, can only communicate with Endgame.
Release Requested	The Endgame platform sent a 'release host' task to the sensor.
Released	The host has been released from isolation and, therefore, can communicate with network-connected endpoints.
Isolation Failed	The sensor was unable to isolate the host.
Release Failed	The sensor was unable to release the host.

The following table lists the locations in the platform where the "Released" and "Isolated" statuses are displayed:

Platform Location	Example	
Alert Metadata panel	Endpoint	^
	Name	DESKTOP-QBBSCUT
	IP Address	10.6.122.9
	Status	• Active (Isolated) since 6:06 PM UTC
	OS	Windows 10 (v1803)
	Alert Count	15
	Groups	Windows 10 View All
	Active Directory Distinguished Name:	-
	ĺ	An "Isolated" status is also denoted by a lock button next to the Endpoint section header.



Platform Location	Example
Endpoint Details page	DESKTOP-QBBSCUT Take Action
(visible in the "Overview" section and Activity Timeline)	IP Address:       10.6.122.9         Status:       • Active (tolated) • since 521 PM UTC         OS:       Windows 10 (v1803)         Groups:       Windows 10 View All         Policy:       Default • Successful         Active Directory Distinguished Name:       •         Activity Timeline Expand Activity Feed       Filter By:         May 13, 3019, UTC       •         May 13, 3019, UTC       •         May 13, 3019, UTC       •         May 13, 3019, UTC       •         Host Isolated (Successc) UTC       •         S21:H3 PM UTC       •
Endpoints list	ENDPOINT NAME         2qxa-w10x64l6-d         • Active (Isolated) as of 7 minutes ago         2gxa-w10x86l6-d         • Active (Isolated) as of 5 days ago         2gxa-w2k12r2-d         • Active (Isolated) as of 5 days ago         2GXA-W2K8R2-D         • Active as of 5 days ago

# Allow Isolated Hosts to Connect to Other IP Addresses

When hosts are in an isolated state, communication to the Endgame platform remains enabled. However, if those isolated hosts need to establish an outbound connection to other hosts within their network, administrators can specify which ones are allowed network communication by adding that IP or IP range to a host isolation exceptionlist. This enables analysts to continue to use Endgame to manage endpoints.

To allow an isolated host to connect to an IP address:

1. On the Left Navigation toolbar, click the ADMINISTRATION button



- 2. On the Administration page, select the **PLATFORM** tab.
- 3. In the "Add IP Address" text box located in the **HOST ISOLATION CONFIGURATION** section, type the permissible IP address that can allow communication from an isolated host.
- 4. In the "Add Description" text box, type a description or note to identify the IP. Ensure the description is no more than 64 characters.
- 5. Click Add.



6. Repeat steps 1-5 to add additional IP addresses. The updated host isolation exceptionlist is immediately applied to all active sensors.

POLICY RULES USER SENSOR ALERT WHITELIST BLACKLIST TRUSTED APPLICATIONS PLATFORM					
HOST ISOLATION CONFIGURATION					
Allow isolated hosts to connect to these IP addresses. Endgame platform is alway	s allowed by default and does not need to be added.				
Add IP Address (Ec: 192.168.1.4 or 192.168.1.0/24)	Add Description	Add			
				1 - 5 of 5 < >	
IP ADDRESS	DESCRIPTION		ACTION		
105.05.05	Host 5		혭		
104.40.40.40	Host 4		圃		
103.30.30.30	Host 3		圃		
101.10.10.10	Host 2		圃		
100.00.00	Host 1		圃		

Host isolation exceptionlist

#### Manage the Host Isolation Exceptionlist

If you entered an incorrect IP address or if a current IP address in the host isolation exceptionlist should no longer allow communication from an isolated host, remove it from the exceptionlist by doing the following:

1. In the host isolation exceptionlist, locate the appropriate IP address to delete. In the corresponding **ACTION** 

column, click the **Delete** button

 In the dialog box that says, "Removing this entry will block isolated hosts from connecting to this specific address. Are you sure you want to do this?" click **Confirm**. An "Entry successfully deleted" confirmation appears and the updated host isolation exceptionlist is immediately applied to all active sensors.



Remove an entry from host isolation exceptionlist

3. Click Finish.



# **Endpoint Response Types and Advanced Configuration Options**

The following table lists all endpoint response types and their advanced configuration options.

Response Name	Description	Advanced Configuration Options
Delete File	Deletes a file.	File Path: Type the path of the file to delete.  NOTE: Ensure the path is correct. The file will not delete if the path does not match the file location.
Execute File	Executes a file.	<ul> <li>File Path: Type the path of the file to execute.</li> <li>Max Time: (Seconds) Enter the maximum number of seconds the file execution process should run before collecting the output.</li> <li>Collect Output: Select this option to capture the command line output.</li> <li>Delete After Execution: Select this option to permanently delete the file after execution.</li> <li>Arguments: To enter command-line arguments to run with the executed file, type them in the text box.</li> </ul>
Isolate Host	Isolates the endpoint to prevent it from communicating with all systems.	N/A
Get File	Retrieves a file from the endpoint to the platform.	File Name: Type the path of the file to download. NOTE: After this task is executed, you must download the file from the Endpoint Details page, which is in a password-protected zip file. The password is set to "dangerous."
Kill Process	Terminates a process by process ID, name, or file path.	Enter at least one of the following: <b>Process ID: (Single Endpoint Only):</b> Enter the process ID to terminate. <b>Process Name:</b> Type the name of the executable to terminate. <b>File Path:</b> Type the full file path of the process to terminate.



Response Name	Description	Advanced Configuration Options
Release Host <sup>1</sup>	Releases the endpoint from isolation, allowing it to communicate with all systems.	N/A
Suspend Thread <sup>2</sup>	Suspends a malicious process thread by thread ID.	Thread ID: Enter the thread ID to suspend. NOTE: Thread IDs are unique to individual endpoints, therefore, you can only suspend one thread at a time.
Upload File	Uploads a file.	Select File: Click Upload File and select the file to upload from the appropriate directory. File Path: Type the file path, including the file name, to specify where the uploaded file should reside on the endpoint. NOTE: There is a maximum file size of 16 MB. Only one file can be uploaded and only one file path can be entered at a time. It is critical that the path includes the filename so that you can upload the file to a different name than what is on the local machine. For example, c:\docu- ments\uploadedfiles is an invalid path name because it is missing the filename, however, c:\docu- ments\uploadedfiles\newfile is a valid path name. If you do not upload a file or if a directory path is incorrect, an error message appears.
		<b>Overwrite:</b> Select this option to overwrite an existing file that contains the same filename.

<sup>1</sup>Release Host appears in the list only if the endpoint has been isolated.

<sup>2</sup>Suspend Thread is only compatible with Windows.



## **Delete an Endpoint**

Deleting an endpoint first uninstalls the sensor from the endpoint, then removes the endpoint from the Endgame platform.

You can uninstall the sensor but retain the endpoint in the Endgame platform. For more information, see "Uninstall a Sensor" in the *Administrator's Guide*.

To delete an endpoint(s):

i

- 1. In the Endpoints list, select the box to the left of each appropriate endpoint.
- 2. On the Action toolbar, point to More Actions, then click Delete.
- In the Delete Endpoint(s) dialog box that says, "Are you sure you would like to delete number endpoint(s)? Deleting an endpoint will first uninstall the sensor and then delete all endpoint records from the system (including alerts)." click Yes. An "Endpoints successfully deleted" message appears.
- 4. Click Finish.

To delete a single endpoint from the Endpoint Details page, click Take Action, then select Delete Endpoint.

# CHAPTER 3

# INVESTIGATIONS

Investigations Overview	62
Start an Investigation	62
Investigation Dashboard Overview	67
View Investigation Results	72
Archive an Investigation	82
Investigation Dashboard - Archived View	83
Hunt Types and Advanced Configuration Options	84
Tradecraft Analytics Overview	
Fileless Attacks Overview	
IOC Search Overview	



i

# Investigations Overview

An investigation is a custom search that collects and analyzes targeted data across multiple endpoints. It is created by assigning one or more hunts to selected endpoints. The main goals of an investigation are to identify suspicious activity and take remedial action before damage and loss occurs.

Results of the investigation are displayed on the Investigation Details page. It contains an interactive tool, similar to a pivot table, that shows all data collected across selected endpoints. It also discovers unknown IOCs (indicators of compromise) by identifying anomalies and enabling the user to filter data by tailored analytics.

> If you received an alert notification, it is recommended you start an investigation to determine if there was an attempted compromise and to identify additional areas in the current environment that also may have been compromised. You can only start an investigation for endpoints running on the same operating system.

# Start an Investigation

The procedure for starting an investigation consists of three steps:

- 1. Select endpoints to include in the investigation.
- 2. Select and configure hunts.
- 3. Launch the investigation.

NOTE: You can only create a single investigation for endpoints that run on the same operating system. For example, you cannot create an investigation that contains both Windows and Linux endpoints.

To start an investigation:

1. On the Left Navigation toolbar, click the **ENDPOINTS** button



- 2. On the Action toolbar, select an operating system tab (i.e., Windows, Linux, or Solaris) to filter the Endpoints list.
- 3. Select the box to the left of each endpoint to include in the investigation.

TIP: Apply KPI filters as necessary to narrow the Endpoints list, or click the Currently Selected drop-down arrow and choose a bulk selection option. It is also recommended you create hunts for endpoints with active sensors; select the Active KPI to filter these endpoints.

4. On the Action toolbar, click **Create Investigation**.



 You can also start an investigation from the Endpoint Details page by clicking Take Action, then selecting Start Investigation. However, if you do, please note you can only create hunts for the current endpoint.

5. Complete the requirements in the **START INVESTIGATION** dialog window:

#### Step 1: Create an Investigation Profile

This section specifies the name, assignee, and hunts for the investigation.

**NOTE:** If you have already created and saved an investigation profile, see "<u>Apply an</u> Existing Profile to an Investigation" in this topic.

INVESTIGATION NAME (Optional): In the text box, type a unique name to identify the investigation. If you do not specify a name, Endgame automatically assigns one in the following format: Username + YYYY-MM-DDtime\_time zone, where YYYY-MM-DD represents the four-digit year, two-digit month, and two-digit day it was created (e.g., Super Admin + 2016-08-31T19:30:57.661614\_utc).

It is recommended to assign the investigation a name to distinguish the current investigation from others. You can use letters, spaces, numbers, and special characters in the text box.

- ASSIGN TO: By default, the investigation is assigned to yourself. To assign the investigation to another user:
- a. Click the **Find User** option button or link. The **ASSIGN A USER** dialog window displays an alphabetical list of all registered users and their designated usernames.
- b. Choose one of the following options to locate the appropriate user:
  - In the **Search User Name** text box, begin typing the user's first or last name. The list filters to name(s) that match the entry. If no matching users are found, an "Invalid User" error message appears.
  - Scroll the list and locate the user's name.
- c. Click the option button to the left of the appropriate user's name.
- d. Click Confirm User.

i



ASSIGN A USER Find a user to assign to an investigation.				
Selecting a User Search the list below to find the User you want to assign to this particular investigation.				
<b>Q</b> admin				
NAME	USERNAME			
Super Admin	admin			
Cancel		Confirm User		

Assign a User dialog window

- SELECTED HUNTS: To add and configure hunts:
- a. Click Manage Hunt(s). An alphabetical list of available hunt types appears.
- b. In the left column, select each hunt to include in the investigation.
- c. In the right column, enter advanced configuration for the selected hunt(s). Advanced configuration options vary according to the hunt type; therefore, to ensure accuracy, select all appropriate options and enter property values accordingly.

**NOTE:** Not all hunts have an advanced configuration. For those that do, some options are selected by default; however, you can clear the selection if desired.

If a required property value is missing, an error message displays the missing property value at the top of the **ADVANCED CONFIGURATION** column. You cannot confirm your hunts until all required values are specified. For a complete list of hunt types and advanced configuration options, see "<u>Hunt Types and Advanced Configuration Options</u>" in this chapter.

TIP: Click What's this? next to an advanced configuration option to view the description.

#### d. Click Confirm Hunts.

To save the current investigation name and hunt configuration as a profile for future use:

- 1. Click Save Profile. A "Profile created" message appears.
- 2. Click **Confirm**.



#### Step 2: Launch Your Hunts

When hunt configuration is complete:

- 1. Click **Create Investigation**. A "Hunts successfully launched" message appears to confirm the investigation has begun.
- 2. Click View Investigation to go to the Investigation Details page, or click Close to close the dialog window.

	START INVESTIGATION Configure your profile and launch your hunts	CREATE A NEW INVESTIGATION 1. Investigation Name. Give the investigation a
Create Investigation Profi	le Save Profile Use Existing Profile	unique name.
You have currently selected <b>8 En</b> your investigation. You can then Investigation List.	dpoints. Once a profile is entered, select the Create Investigation button to start view progress by selecting the View Investigation link, or directly on the	2. <b>Save Current Profile.</b> Save the current hunt configuration as a profile for future use.
INVESTIGATION NAME (Optional)	New Investigation	3. <b>Use Existing Profile.</b> Apply an existing profile to import the hunt configuration.
ASSIGN TO	Me (Super Admin)     Find User	4. <b>Assign To.</b> Displays the current assignee. Click <b>Find User</b> to assign the investigation
SELECTED HUNTS What is this?	Manage Hunt(s) 4 Hunt Types Selected	to another user. 5. <b>Manage Hunt(s).</b> Add or remove hunts and
Cancel	6 Create Investigation	6. Create Investigation. Starts the investigation.

#### Start Investigation dialog window

**Remember:** After you create an investigation, each hunt you selected appears as a separate event in the Activity Timeline.


## Apply an Existing Profile to an Investigation

After you have selected which endpoints to include in the investigation, you can import the hunt configuration from a previously saved profile.

To apply a saved investigation profile:

- 1. Click Use Existing Profile.
- 2. In the Investigation Profiles list, click the option button to the left of the appropriate profile name.
- 3. Click **Confirm Profile**. The profile imports the investigation name, hunt configuration, and assignee.



### Apply an existing profile

TIP: To overwrite the existing investigation name, select the current name and replace it with new text. This is recommended if you do not want to confuse the current investigation with an existing one.

### Manage Hunt Selection and Configuration

If necessary, you can modify or reconfigure selected hunts before you start the investigation.

To remove or reconfigure a hunt(s) from the investigation:

- 1. Click Manage Hunts. In the Hunt Types list that appears, previously configured hunts are selected.
- 2. Select or clear hunt types and edit advanced configuration as necessary.
- 3. Click Confirm Hunts to update the configuration.



# **Investigation Dashboard Overview**

The Investigation Dashboard displays essential details about all created investigations, gives an overall progress status of each one, and provides options to view, filter, and manage them.

To view the Investigation Dashboard, click the Investigations button in the Left Navigation toolbar.

The dashboard contains two sections:

- 1. Action toolbar
- 2. Investigations list

	9 j Current Arc	hived	1	Archive Investigations Current	How to Start an Investigation View ▶						0
	8 Hunts Que	1 eries T & ·	9 otal •								0
3 invest	igations currently se	elected 🗸									1- <u>9</u> of 9 < >
-	INVESTIGATION NAI	ME				ASSIGNEE	INVESTIGATION BREAKDOW	'n	ENDPOINTS	DATE CREATED	
~	Kevin Qualters + 201	I7-07-12T15:41:10.	219143_utc			Kevin Qualters	100%	1 Hunt total	1	Jul 12, 2017 3:41:10 PM UTC	
*	Eric Davis + 2017-07	7-12T15:23:36.5060	l62_utc			Eric Davis	100%	4 Hunts total	8	Jul 12, 2017 3:23:36 PM UTC	
~	Eric Davis + 2017-07	7-12T15:22:59.8984	180_utc			Eric Davis	100%	5 Hunts total	1	Jul 12, 2017 3:22:59 PM UTC	
	Eric Davis + 2017-07	7-11T23:28:29.8688	19_utc		2	Eric Davis	100%	<u>2 Hunts total</u>	8	Jul 11, 2017 11:28:29 PM UTC	
	Eric Davis + 2017-07	7-11T22:57:44.0328	19_utc		-	Eric Davis	100%	1 Hunt total	1	Jul 11, 2017 10:57:44 PM UTC	
	Eric Davis + 2017-07	7-11T22:56:31.7428	163_utc			Eric Davis	100%	1 Hunt total	1	Jul 11, 2017 10:56:31 PM UTC	
	Process Lineage 201	17-07-11T17:44:47.	382402			Eric Davis	100%	1 Query total	1	Jul 11, 2017 5:44:47 PM UTC	
	Charlie Pichette + 20	017-07-11T12:32:23	3.547286_utc			Charlie Pichette	100%	1 Hunt total	4	Jul 11, 2017 12:32:23 PM UTC	
	Charlie Pichette + 20	017-07-11T12:18:0	5.570202_utc			Charlie Pichette	100%	1 Hunt total	4	Jul 11, 2017 12:18:05 PM UTC	
										Last Updated: Jul 12, 2017 5:07:	43 PM UTC (EDT+4)

### Investigation Dashboard

## **Action Toolbar**

The Action toolbar contains two KPIs that filter the Investigation Dashboard by two views: **Current**, which displays by default, and **Archived**. By default, all investigations are current until they are archived. The Action toolbar also enables you to archive selected investigations and provides guidance on how to start an investigation.







#### Action toolbar on the Investigation Dashboard

Beneath the toolbar, a secondary set of KPIs displays the number of investigations that fall within a specific category:

KPI	Description
Hunts	An investigation that includes tasks executed by the sensor to collect data across endpoints.
Queries	Search inquiries executed using Endgame's intelligent assistant, Artemis, to find process-related events on active endpoints. For more information about Artemis, see "Artemis Search Overview" in Chapter 5, <i>Artemis</i> .
Total	The total number of hunts and queries.

Each KPI in the Investigation Dashboard is an interactive link that filters the Investigations list by the selected category.

Filters are useful to narrow investigations by a specific parameter. For example, to view all current hunt investigations, select **Current**, then select **Hunts**.



## **Investigations List**

The Investigations list is an enumeration of all investigations and their relevant details, organized in a table. The list is useful to view investigation progress, and, more specifically, how many endpoints have returned data. Investigations display in reverse chronological order with the most recently created investigations at the top.

 By default, both hunts and queries appear in the Investigations list. Select the appropriate KPI on the Action toolbar if you need to view either separately.



#### Investigations list

The columns in the list provide general details about each investigation:

Column Name	Description
INVESTIGATION NAME	The user-created name of the investigation. To view results of an investigation on the Investigation Details page, click the name link.
ASSIGNEE	The name of the user assigned to the investigation.
INVESTIGATION BREAKDOWN	Displays a progress bar that indicates the investigation's or Artemis query's percentage completion across all tasked endpoints. Click the <b>Hunts total</b> or Query total link to view a breakdown of each hunt in a pop-up window.
ENDPOINTS	The number of endpoints included in the investigation. Click the number link to view those endpoints in the Endpoints list.
DATE CREATED	The date and time the investigation was created, according to Coordinated Universal Time (UTC) or your selected time zone.



**TIP:** To help manage the Investigations list, consider archiving investigations you are finished analyzing. For more information, see "<u>Archive an Investigation</u>" in this chapter.

### Sort and Filter Columns in the Investigations List

You can sort columns in the list to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

n Elastic compan

• Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

• In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the

entry. The currently filtered column is denoted by a 🖃 symbol.

COLUMN SORT	
Select the appropriate column heading and choose to sort by ascending or descending order.	-→ O Ascending Oescending
COLUMN SEARCH	COLUMN: SEARCH
Type a value in the text box and click <b>Search</b> to filter the list.	Q
	<u>Clear</u> <u>Search</u>

Column sort and filter



## **Page Pagination**

In the upper-right corner above the list is a range display, which displays the current number range of investigations out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 investigations display per page; however, you can change the number to a preferred choice:

- 1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
- 2. In the **Max count of** text box, enter a new number between 1 and 500.
- 3. Click  $\checkmark$  to save your changes.





# **View Investigation Results**

After an investigation is created, it continuously runs in the background until complete. You can view an investigation while it is still in progress or when all endpoints have returned data.

To view results of an investigation, click the investigation you want to view from the Investigations list.

**NOTE:** IOC search results do not have an Investigation Details view but display on the Search Results page instead. For more information, see "<u>IOC Search</u>" in this chapter.

# **Investigation Details Page Overview**

The Investigation Details page displays results of the selected investigation, and enables you to compare, filter, and analyze endpoint data across multiple parameters.

**NOTE:** Artemis queries have a different view than investigations with hunts. For more information, see "View Artemis Search Results" in Chapter 5, *Artemis*.

The details page has three sections:

- 1. Investigation Overview
- 2. Endpoint Breakdown
- 3. Investigation Details

Hunt Overview		Download Tasking Co	nfig						SELECT HUNT T	YPE: Process	✓ Custor	n View 🗸
Investigation Name	1											
Investigation 3							Visual Selec	tor				<b>QQ</b> Results
Assigned To	1	Process Name		AND: ME	05 Hash							JJ Shown
Super Admin		99	20% 40%	60	)%	80% 100%	PROCESS N	AME	MD5 HASH			ENDPOINT
Nov 2 2017 2:44:02 AM	UTC						S sychos	.exe	1f8434dd4907c832e6e90d6298eab85b	1		2
101 2, 2017 011100 101		8					💲 svchos	.exe	36f670d89040709013f6a460176767ec	1		2
Endpoint Breakdown	Θ	on on					💲 svchos	.exe	54a4716b5e09a77e61649109c6a08866			2
Applications		due Oo				3	S. sychos	.exe	e4ca434f251681590d0538bc21c32d2f			2
100%	10/16	- <u>1</u> 5 33 -					9 purbori	ava	d0abc231c0b3c88c6b612b28abbf734d			2
100%	16/ <b>16</b>								-2-0-105-04105-25-006-40-500-47			-
Network		0	•				Svcnos	.exe	e3a2ad05e24105b35e966c19cb36ec47			2
100%	16/ <b>16</b>	Percent of E	napoints	Data Cole	ected: Nov 2, 1	UT7 3344203 AM OTC	💲 csrss.e	æ	17141511b178b2a0664f77eab7aed9f7			2
Persistence												
100%	16/ <b>16</b>	ENDPOINT	PROCESS NAME	PID	PPID	PATH		COMMAND LINE		SIGNER	AUTHENTICODE	MALWARESCORETM
2		gvcv-w10x8616 -p	svchost.exe	504 0	576	C:\Windows\System exe	l32∖svchost.	C:\Windows\system32\svchost.exe nation	e -k LocalServiceAndNoImperso	Microsoft Windows Publis her	trusted	0
		gvcv-w10x8616 -p	svchost.exe	262 8	576	C:\Windows\System exe	i32∖svchost.	C:\Windows\system32\svchost.exe tricted	e -k NetworkServiceNetworkRes	Microsoft Windows Publis her	trusted	0
		gvcv-w10x86l6 -p	svchost.exe	145 6	576	C:\Windows\System exe	i32∖svchost.	C:\Windows\system32\svchost.exe	e -k appmodel	Microsoft Windows Publis her	trusted	0
		gvcv-w10x8616 -p	svchost.exe	684	576	C:\Windows\System exe	i32∖svchost.	C:\Windows\System32\svchost.exe	e -k utosvo	Microsoft Windows Publis her	trusted	0
		gvcv-w10x8616 -p	svchost.exe	185 6	576	C:\Windows\System exe	132\svchost.	C:\Windows\system32\svchost.exe ted	e -k LocalServiceNetworkRestric	Microsoft Windows Publis her	trusted	0

Investigation Details page



## **Hunt Overview**

The Hunt Overview section displays general information about the investigation, including the name, assignee, and the date created. It also provides options to edit the name and archive the investigation.





### **Endpoint Breakdown**

The Endpoint Breakdown displays the status of each hunt in the investigation, which includes the following information:

- Each hunt type listed in alphabetical order
- A progress bar that displays the percentage completion
- The number of endpoints out of the total selected that have returned data





#### Endpoint Breakdown

### **Investigation Details**

Investigation results are displayed within the Investigation Details area. It contains an interactive, customized tool that enables you to filter returned endpoint data by choosing a specific hunt and one or two variables. With this method, you can focus on analyzing smaller components gradually, rather than inclusive results all at once.



#### Investigation Details





For maximum efficiency, filter investigation results by following these steps:

- 1. Create your custom view.
- 2. Find unique occurrences in the Histogram.
- 3. View results in the Visual Selector.
- 4. Analyze endpoint data in the Investigation Details table.
- 5. View hunt results on the Endpoint Details page and, if necessary, execute a response action.

**NOTE:** In the Investigation Details area, you can view current results for hunts that are in progress, and if needed, respond accordingly without waiting for all data to return; however, the results may not be entirely accurate until all hunts are complete.

### **Create Your Custom View**

On the upper-right side of the Investigation Details page are two drop-down lists that enable you to either create a custom view or select one of the Tradecraft Analytics — tailored, unique views that show uncommon or anomalous data.

NOTE: Tradecraft Analytics are not available for investigations that contain Linux endpoints.

To create your custom view:

- 1. Click the **SELECT HUNT TYPE** drop-down arrow, then select a hunt from the list.
- 2. On the Histogram, click the leftmost drop-down arrow and select a variable from the list. To add a second variable, click the second drop-down arrow and select it from the list. Variables vary by hunt type.

Download Tasking Config		SELECT HUNT TYPE: Process	Custom View 🗸
Process Name V AND: MD5 Hash V	Visual Selector		99 Results Shown
20% 40% Parent Process Name 0%	PROCESS NAME	MD5 HASH	ENDPOINT
Path MD5 Hash	Svchost.exe	1f8434dd4907c832e6e90d6298eab85b	2
Commal ine Signer	💲 svchost.exe	36f670d89040709013f6a460176767ec	2
authenticode Authenticode MalwareScore™	💲 svchost.exe	54a47f6b5e09a77e61649109c6a08866	
O anthref 33 -	💲 svchost.exe	e4ca434f251681590d0538bc21c32d2f	
	💲 svchost.exe	d0abc231c0b3e88c6b612b28abbf734d	
	💲 svchost.exe	e3a2ad05e24105b35e986cf9cb38ec47	
Percent of Endpoints Data Collected: Nov 2, 2017 3:44:03 AM UTC	S csrss.exe	17141511b178b2a0664177eab7aed9f7	

Custom view: select a hunt and one or two variables to analyze data

To view results from one of the Tradecraft Analytics:



- 1. Click the SELECT HUNT TYPE drop-down arrow, then select a hunt from the list.
- 2. Click the Custom View drop-down arrow, then select an analytic from the list.

SELECT HUNT TYPE: Process	•	Custom View	v
What is this? This patent-pending capability discovers adversaries who are hiding in memory in order to evade detection or blend within legitimate system noise. Example adversary techniques identified by Memory-Hunt include injected code. process		Custom View  MalwareScore™	
hollowing, DLL side loading, module overwriting, module hiding and more. In short, this analytic will detect even the most sophisticated in-memory only adversaries and other file-less malware threats.	,	Fileless Attacks	
What should I be looking for? Memory injection, hidden module, and memory modification detections are very likely to be malicious and should be looked		Multiple Hits	I
and often flag on malware, but you can be almost certain you will have some legitimate software on your network that is packed. Look for packed processes that are unsigned or uncommon on your network as secondary indicators of	,	Filename Masquerading	I
maliciousness.		Suspicious Path	
False positives may occur even for the high confidence MemoryHunt detection types, and usually fall into two categories. First, digital rights management (DRM) technologie used by media applications, video games, or other software use stealth and anti-analysis techniques that often look quite simila to malware in memory. Second, Just-In-Time (JIT) code is	s e	Untrusted Certificates	Ŧ
generated at runtime and therefore may resemble injected cod JIT is used in a number of runtime engines such as Java, .NET, javascript, and Flash. Fortunately, MemoryHunt is by design resilient to JIT false positives.	e.		

The list of Tradecraft Analytics for the Process hunt.

i

Tradecraft Analytics are only available for Network, Persistence, Network, and Users hunts vary and by the selected hunt. For a brief description of each analytic, see "<u>Tradecraft Analytics</u>" in this chapter or hover your cursor over an analytic to display the pop-up window.

### Find Unique Occurrences in the Histogram

The Histogram is a bar graph that displays the number of unique occurrences (y-axis) —based on the selected variables — that were found on a specific percentage of endpoints (x-axis). The number scale on the y-axis is unique for each investigation; however, the x-axis always displays a number scale of 0 to 100 percent, with percentage markers at intervals of 20 (i.e., 20, 40, 60, 80, and 100).

The Histogram highlights anomalies, if any, at first glance. For example, unique occurrences on the majority of endpoints may not indicate suspicious behavior. On the other hand, occurrences on only a few endpoints may indicate a potential compromise to endpoint data.

While viewing investigation results, the recommended goal is to identify outliers by finding occurrences on a lower percentage of endpoints. As such, after you create your custom view or select one of the Tradecraft Analytics, the Histogram automatically defines unique occurrences in the bottom 20 percent.



Download Tas	sking Config						SELECT HUNT TYPE: Process	Custom View V
Process N	Name	✓ AND:	MD5 Hash		~	Visual Selector		99 Results
99 <del>-</del>	20%	40%	60%	80%	100% •	PROCESS NAME	MD5 HASH	<u>ENDPOINT</u>
						Svchost.exe	1f8434dd4907c832e6e90d6298eab85b	2
<b>2</b> 66 -						S svchost.exe	36f670d89040709013f6a460176767ec	2
Jocurrei						S svchost.exe	54a47f6b5c09a77e61649109c6a08866	2
hique C						💲 svchost.exe	e4ca434f251681590d0538bc21c32d2f	2
5						Svchost.exe	d0abc231c0b3e88c6b612b28abbf734d	2
0						💲 svchost.exe	e3a2ad05e24105b35e986cf9cb38ec47	2
Per	rcent of Endemits	De	ata Collected: Nov	2, 2017 <b>3:44:03 AI</b>	и итс	S csrss.exe	17141511b178b2a0664f77eab7aed9f7	2

The Histogram automatically defines occurrences in the bottom 20 percent. Drag the slider bar to update the Visual Selector.

To narrow results, drag the slider bar on the Histogram left or right to the desired percentage marker. Alternatively, you can select a column bar on the Histogram to view the exact percentage of unique occurrences.

**NOTE:** Although the Histogram defaults to display occurrences in the bottom 20 percent, it is possible to not see any results if there were no occurrences within that range.

### **Visual Selector**

i

On the rightmost side of the page is the Visual Selector, a summarized list that displays results according to the current view in the Investigation Details area. The list displays the following data in separate columns:

- The value of each endpoint variable
- The number of endpoints that have one or both variable values

If you select one of the Tradecraft Analytics, the corresponding endpoint variables are pre-defined, whereas with the custom view, you choose the variables.

				Total number of results
	Visual Selector			10 Results
	PROCESS NAME		PARENT PROCESS NAME	ENDPOINT
	GoogleUpdate.exe			1
Value of the first	🔓 snmp.exe	Value of the second	o services.exe	1 Number of endpoints that
variable	S Memory Compression	variable	System	have both variable values
	💲 sppsvc.exe		services.exe	2
	💲 conhost.exe		csrss.exe	3
	S ManagementAgentHost.exe		services.exe	3
	S. Ism.exe		wininit.exe	3

Visual Selector

Proprietary Elasticsearch B.V. information.



By default, the list sorts according to the least number of endpoints; however, you can change the sort order of any column by doing the following:

- 1. Select the column heading you want to sort.
- 2. To sort by increasing value, click **Ascending**. To sort by decreasing value, click **Descending**.

As you select different hunts, variables, Tradecraft Analytics, or adjust the slider bar on the Histogram, the Visual Selector updates to reflect the most recent data. Analyze results to find possible anomalies; for example, if you are comparing the process name and path variables for a Process hunt and you find a suspicious process, it is recommended you view results of the Process hunt, in its entirety, on the Endpoint Details page to further investigate.

TIP: To help identify suspicious processes, select the **Suspicious Path** analytic from the **Custom View** drop-down list.



### **View Endpoint Data**

To view endpoint data for individual occurrences, select a row in the Visual Selector. The Investigation Details table displays each occurrence on a separate row and each variable value in a separate column.

						VARIABLE VALU Endpoint variab display in separa Select a column sort or filter the	JES le values ate columns. heading to table.				
		ENDPOINT	PROCESS NAME	PID	PPID	PATH	COMMAND LINE	SIGNER	AUTHENTICODE	MALWARESCORETM	
INDIVIDUAL OCCURRENCES The selected row in the Visual	isual al		GVCV-W7X64-P	sppsvc.exe	3060	492	C:\Windows\System32\sppsvc.exe	C:\Windows\system32\sppsvc.exe	Microsoft Windows	trusted	0
Selector displays individual		GVCV-W7X86-P	sppsvc.exe	2884	496	C:\Windows\System32\sppsvc.exe	C:\Windows\system32\sppsvc.exe	Microsoft Windows	trusted	0	
occurrences in the table.		GVCV-W7X86-D	sppsvc.exe	2908	496	C:\Windows\System32\sppsvc.exe	C:\Windows\system32\sppsvc.exe	Microsoft Windows	trusted	0	
		GVCV-W7X64-D	sppsvc.exe	3036	524	C:\Windows\System32\sppsvc.exe	C:\Windows\system32\sppsvc.exe	Microsoft Windows	trusted	0	
	ENDP Click th Details	OINT NAME he name link to page and view	o go to the Endp w complete hunt	oint : results.							

#### Investigation Details table

**NOTE:** Initially, the table displays boilerplate text until you select a row in the Visual Selector.

Like most lists in the Endgame platform, you can sort the columns in the table to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering the table are also useful to find outliers.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

• Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow  $\uparrow$  or down arrow  $\downarrow$ .

To search the column for a particular value:

• In the text box, type the text you want to find, then click Search. The list filters to display results that match the

entry. The currently filtered column is denoted by a symbol.





CHAPTER 3 | User's Guide

Column sort and filter



### **View Hunt Results**

Process Nov 2, 2017 3:43:59 AM UTC						View Investigation Details	Download Raw Data	
PROCESS NAME	<u>PID</u>	<u>PPID</u>	PARENT PROCESS NAME	PATH	COMMAN	ID LINE	SIGNER	AUTHE
conhost.exe	3024	2992		C:\Windows\System32\conhost.exe	\??\C:\Wi	ndows\system32\conhost.exe 0x4	Microsoft Windows	trusted
CSTSS.eXe	384	376		C:\Windows\System32\csrss.exe			Microsoft Windows Publisher	trusted
csrss.exe	472	452		C:\Windows\System32\csrss.exe			Microsoft Windows Publisher	trusted
sshd.exe	3072	2992		C:\cygwin\usr\sbin\sshd.exe	"C:\cygwi	n\usr\sbin\sshd.exe"		noSign
System	4	0	System Idle Process					
L Memory Compression	1756	4	System					
L <sub>smss.exe</sub>	288	4	System	C:\Windows\System32\smss.exe			Microsoft Windows Publisher	trusted
wininit.exe	460	376		C:\Windows\System32\wininit.exe			Microsoft Windows Publisher	trusted
L <sub>Isass.exe</sub>	588	460	wininit.exe	C:\Windows\System32\lsass.exe	C:\Window	ws\system32\lsass.exe	Microsoft Windows Publisher	trusted
L services.exe	576	460	wininit.exe	C:\Windows\System32\services.exe			Microsoft Windows Publisher	trusted

In the **ENDPOINT** column, click the endpoint name to go to the Endpoint Details page, where you can view all-inclusive results of the completed hunt.

#### Process hunt results on the Endpoint Details page

If necessary, execute a response action from the Endpoint Details page. For example, if results from a process hunt show a suspicious process name or path, you can terminate that process by doing the following:

- 1. In the PROCESS NAME column, select a process to kill.
- 2. In the **PROCESS DETAILS** window, click Kill Process.
- 3. In the dialog box that says, "Are you sure you would like to kill the process (PID: *process ID*) on *endpoint hostname*"? click **Yes**. A "Kill Process submitted" message appears to confirm the termination.
- 4. Click Finish.

i

You can also initiate a kill process response by doing the following: Click **Take Action** on the Endpoint Details page, select **Respond** from the list, then select the **Kill Process** option button. Please note that you will have to enter the process ID.



# Archive an Investigation

Archiving an investigation moves it from the **Current** tab on the Investigation Dashboard to the **Archived** tab. To help manage the Investigations list, consider archiving an investigation after you have analyzed all returned endpoint data to distinguish it from investigations that are either still in progress or have not yet been analyzed.

To archive multiple investigations:

1. In the Investigations list, select the box to the left of each appropriate investigation.

TIP: To select all investigations on the current page, select the box to the left of the INVESTIGATION NAME column heading.

- 2. On the Action toolbar, click **Archive Investigations**.
- 3. In the **Archive Investigations** dialog box that says, "You are about to archive number Investigations. The investigations will be immediately sent to the Archive Tab and be set as Archived..." click **Archive**. A "Successfully archived investigation(s)" message appears.
- 4. Click Finish.



#### Archive an Investigation dialog window

(i) You can also archive a single investigation from the Investigation Details page by clicking the **Archive** button in the Investigation Overview section.



# Investigation Dashboard - Archived View

The Archived view is a separate view within the Investigation Dashboard that displays all investigations that have been archived. To display the Archived view, select the **Archived** tab on the Action toolbar.

The Archived view is identical to the Current view in the Investigation Dashboard, except the Action toolbar contains an option to unarchive selected investigations.

Investigation D	ashboard									
<b>4</b> Current	Archived		Unarchive Investigations Archived >	How to Start an Investigation						0
7 Hunts	0 Queries	7 Total								0
2 investigations cur	rently selected $\checkmark$									1- <u>7</u> of 7 < >
- INVESTIGA	TION NAME				ASSIGNEE	INVESTIGATION BREAKDO	OWN	ENDPOINTS	DATE CREATED	
Super Adm	in + 2017-07-11T13:	27:48.646112_utc			Super Admin	100%	1 Hunt total	1	Jul 11, 2017 1:27:48 PM UTC	
Super Adm	in + 2017-07-11T13:	01:10.542595_utc			Super Admin	100%	1 Hunt total	1	Jul 11, 2017 1:01:10 PM UTC	
Super Adm	in + 2017-07-11T12:	52:40.730966_utc			Super Admin	100%	2 Hunts total	3	Jul 11, 2017 12:52:40 PM UTC	
Super Adm	in + 2017-07-11T12:	26:08.018551_utc			Super Admin	100%	1 Hunt total	4	Jul 11, 2017 12:26:08 PM UTC	
Super Adm	in + 2017-07-10T11:	53:55.142599_utc			Super Admin	0%	1 Hunt total	1	Jul 10, 2017 11:53:55 AM UTC	
Super Adm	in + 2017-07-10T11:	53:24.690663_utc			Super Admin	0%	1 Hunt total	1	Jul 10, 2017 11:53:24 AM UTC	
Super Adm	in + 2017-07-10T11:	52:31.379414_utc			Super Admin	100%	1 Hunt total	1	Jul 10, 2017 11:52:31 AM UTC	
									Last Updated: Jul 12, 2017 5:35:39	PM UTC (EDT+4)



## **Unarchive an Investigation**

If you mistakenly archived an investigation, you can unarchive it, which moves it back to the Current view in the Investigation Dashboard.

To unarchive an investigation(s):

- 1. In the Investigations list, select the box to the left of each appropriate investigation to unarchive.
- 2. On the Action toolbar, click Unarchive Investigations.
- In the dialog box that says, "You are about to unarchive number Investigation(s). The investigation(s) will be immediately sent back to the Current Tab..." click Unarchive. A "Successfully unarchived investigation(s)" message appears.
- 4. Click Finish.



# Hunt Types and Advanced Configuration Options

A hunt is a specific task executed by the sensor to collect various endpoint data, and an investigation is a mission to analyze that data.

Before you start a new investigation, keep the following in mind:

- Not all hunt types have advanced configuration. For those that do, required fields are noted as such. The rest are optional.
- Click **EXPAND** or **COLLAPSE** on a hunt type to show or hide its advanced configuration. You can also click the same option on an advanced configuration section heading.
- As a recommendation, some advanced configuration options are selected by default, however, you can clear the selection, if desired.
- IOC Search and System Configuration hunts do not have an Investigation Details view. As such, it is recommended you create separate investigations with each of these as the sole hunt.
- To ensure accuracy, carefully review advanced configuration for each hunt type. Select all appropriate options and enter values accordingly.

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options			
Applications	A list of all installed applications.	• Windows	N/A			
File System <sup>1</sup>	A list of all directories and file names within the specified path.	• Windows	<ul> <li>Directory (Required): Type the path of the starting directory.</li> <li>Directories Only: Returns a list of directories, but no file names.</li> <li>NOTE: The following fields and options are unavailable if you select the Directories Only option.</li> </ul>			

The following table describes each hunt type and its advanced configuration options.

<sup>1</sup>You can only create this hunt for a single endpoint.



Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			<b>Search Depth:</b> Enter a number between 1 and 3 to specify the number of levels beneath the path the survey should return a list of directories and file names for.
			For example, if <b>C:\Program Files</b> is the directory path and you enter <b>1</b> in the <b>Search Depth</b> field, the survey will return a list of all subdirectories and file names one level beneath C:\ProgramFiles.
			Metadata
			Select an option(s) to return additional data:
			<ul> <li>Collect Hashes: Returns the MD5, SHA1 and SHA256 hash values.</li> </ul>
			<ul> <li>Collect Timestamps: Returns dates and times of when the directory was last created, accessed, and modified.</li> </ul>
Firewall Rules	A list of all Windows firewall rules that also indicates if they are enabled or disabled.	• Windows	N/A
IOC Search	Executes an IOC (indicators of compromise) search on selected endpoints.	<ul><li>Windows</li><li>Linux</li><li>Solaris</li></ul>	See "IOC Search Types and Advanced Configuration Options" in Chapter 3, Investigations.
Loaded Drivers	A list of all installed drivers on the system.	• Windows	N/A
Network	A list of all current network connections.	<ul><li>Windows</li><li>Linux</li><li>Solaris</li></ul>	ARP, DNS Cache, NetBIOS, & Routes: Returns Domain Name System (DNS) records, NetBios neighborhood, Address Resolution Protocol (ARP) entries, and route entries.
Persistence	A list of applications configured to launch when a	• Windows	Click <b>EXPAND</b> on each section to view the following advanced configuration options:



Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
	system reboots.		<ul> <li>Filter By (Optional)</li> <li>Select an option to filter returned results: <ul> <li>No Filter: Returns all applications.</li> <li>Only Return Unsigned: Returns applications that do not have an SSL certificate.</li> <li>Only Return not Signed by Microsoft: Returns applications that do not have a signed Microsoft certificate.</li> </ul> </li> <li>Select Categories (Required)</li> <li>Deselect any applications that should not be checked for persistence. By default, all applications in the list are selected.</li> <li>Include Metadata (Optional)</li> <li>Select an option(s) to return additional data: <ul> <li>MD5 Hash</li> <li>SHA1 Hash</li> <li>SHA256 Hash</li> <li>MalwareScore™: Returns a score on a scale of 0-100 to indicate the level of malware.</li> <li>Signer Information: Returns the</li> </ul> </li> </ul>
Process	A list of running parent and child processes.	<ul> <li>Windows</li> <li>Linux</li> <li>Solaris</li> </ul>	Select an option to indicate which processes to return: All Processes: Returns all running processes. Suspicious Processes: Returns



Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			<ul> <li>unbacked executable processes.</li> <li>Detect</li> <li>Malware with MalwareScore™: Detects potential malware files that are present on disk. If found, it returns a score on a scale of 0 (benign) to 100 (malicious) to indicate the level of maliciousness.</li> <li>Fileless Attacks: Detects potential malware running in memory. If found, it displays those processes in the Fileless Attacks analytic. 1</li> <li>Collect</li> <li>Select an option(s) to return additional data: <ul> <li>Hashes: Returns the MD5 hash value of each found process.</li> <li>Modules: Returns all loaded modules in a process.</li> <li>Handles: Returns information about open handles owned by a given process, including the type of handle.</li> <li>Threads: Returns information about threads owned by the process, including the thread ID and the starting addrese</li> </ul> </li> </ul>
Registry	Windows information from the specified registry hives.	• Windows	<b>Registry Path:</b> Type the full registry path, including the base hive, to filter survey results (e.g., HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft).

<sup>1</sup>For more information about the Fileless Attacks analytic, see "Fileless Attacks."



Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			<b>Depth:</b> Enter a number between 1 and 3 to specify the number of subkeys beneath the registry path to return.
Removable Media	A list of devices plugged into a USB port (e.g., flash drives, portable hard drives, etc.)	• Windows	N/A
System Configuration <sup>1</sup>	Operating system and configuration information, such as hostnames, system architecture, and memory usage.	<ul><li>Windows</li><li>Linux</li><li>Solaris</li></ul>	N/A
Users	A list of all users who are currently logged in.	<ul><li>Windows</li><li>Linux</li><li>Solaris</li></ul>	N/A

<sup>1</sup>System Configuration does not have an Investigation Details view.



# **Tradecraft Analytics Overview**

Tradecraft Analytics are unique views that show uncommon or anomalous data on the Investigation Details page. This differs from the custom view, which allows you to choose which endpoint variables you want to analyze. When you select a hunt and an analytic, the Visual Selector and Histogram update with the corresponding data.

The following table describes the available Tradecraft Analytics for Network, Persistence, Process, and Users hunts, and the data each returns.

**NOTE:** Tradecraft Analytics are not available for investigations with Linux endpoints, however, you can choose endpoint variables to create a custom view.

Analytic Type	Description (Data Returned)
	Network
Uncommon Connections	The least occurring remote network connections within the environment.
Listening Ports	Listeners that are actively listening for an inbound remote connection on a port that is an outlier in the environment.
Suspicious Connections	Remote connections to web ports (e.g., 80, 443, etc.) that are not linked to a web browser.
	Persistence
MalwareScore	Persistent files that exceed the set malware threshold.
COM Hijacking	Persistent files that contain COM (Component Object Model) hijacks —a technique where the adversary writes a current user COM entry in the registry corresponding to a legitimate entry in the local machine hive.
Search Order Hijacking	Persistent files that contain DLL search order hijacks — a technique where the adversary places a malicious DLL with the same name as a legitimate DLL in a location that is loaded before the legitimate DLL.
Phantom DLL Hijacking	Persistent files that contain phantom DLLs hijacks $-a$ technique where an adversary names their library to match a phantom DLL $-a$ program that attempts to load but is not present on the system. The adversary then sets an application to load the phantom DLLs to persist.
Multiple Hits	Persistent files that triggered multiple suspicious behaviors as a result of existing high and medium analytics (e.g., Fileless Attacks, Filename Masquerading, Untrusted Certificates, etc.)
Filename Masquerading	Persistent files with the same name as a well-known system or application, or running processes that do not match the correct path.



Analytic Type	Description (Data Returned)				
Filename Mismatch	Persistent files that are empty or do not match the filename on disk.				
Suspicious Path	Persistent files that are persisting out of abnormal paths.				
Untrusted Certificates	Persistent files that are unsigned or do not properly verify on the system.				
Modified Persistence	Previously observed persistent files whose hash or signer information has changed.				
New Persistence	Persistent files that are newly discovered in the environment which are not signed by trusted sources.				
Persistence Not Found	Persistent files with an execution target that does not exist on disk.				
	Process				
MalwareScore	Processes that exceed the set malware threshold.				
Fileless Attacks	Processes that are hiding in memory to evade detection.				
Multiple Hits	Processes that triggered multiple suspicious behaviors as a result of existing high and medium analytics (e.g., Fileless Attacks, Filename Masquerading, Untrusted Certificates, etc.)				
Filename Masquerading	Processes with the same name as a well-known system or application, or running processes that do not match the correct path.				
Suspicious Path	Processes that are running out of non-traditional applications or system folders.				
Untrusted Certificates	Processes that are unsigned or do not verify on the system.				
	Users				
Multiple Logons	Users who are accessing multiple endpoints.				



# **Fileless Attacks Overview**

Fileless Attacks is an analytic and enhancement to the Process hunt that inspects the memory of running processes to discover adversaries hiding in memory to evade detection. Fileless Attacks identifies evasion techniques such as injected code, process hollowing, DLL side loading, module overwriting, and module hiding. If such techniques or other fileless threats are detected in your environment, it is a strong indicator of a potential compromise that requires immediate investigation. Details of each flagged process and its modified memory are displayed on the Investigation Details page.

1 The difference between Fileless Attacks and MalwareScore<sup>™</sup> detection is that the former detects malware running in memory; the latter detects potential malware files that are present on disk. Fileless Attacks and Malware with MalwareScore<sup>™</sup> are two detection options selected by default in the Process hunt's advanced configuration.

# What to Look Out For

Fileless Attacks categorizes hidden memory techniques into four attack types: Memory Modification, Memory Injection, Hidden Module, and Software Packing. Memory Modification, Memory Injection, and Hidden Module detections are likely malicious and each process should be investigated immediately. Although packed processes often indicate malware, it is common to have some legitimate software on your network that is packed.

Depending on the packer used, legitimately packed applications may show hits for Memory Injection. As a secondary indicator of present malware, look for packed processes that are unsigned or uncommon within your network.

TIP: When viewing investigation details of a Process hunt, in addition to Fileless Attacks, select other Tradecraft Analytics — such as Untrusted Certificates and Suspicious Path — to display anomalous data.



The following table describes the four attack types and the type of malware Fileless Attacks identifies. On the Investigation Details page, each attack type is identified by a distinct symbol.

Attack Type	Description	Symbol
Memory Modification	Identifies malware that modifies or overwrites the process memory of legitimate modules to hide its presence on the system.	Ø
Memory Injection	Analyzes running threads and memory segments to find injected code and dynamic link libraries (DLLs) in memory.	$\odot$
	<b>NOTE:</b> Memory Injection hits typically require immediate attention.	
Hidden Module	Identifies malware that removes traces of itself from the Process Environment Block (PEB) and exists on disk as a DLL.	8
Software Packing	Identifies packed processes. Packing an executable changes the file signature in an attempt to avoid signature-based detection.	•
	<b>NOTE:</b> Consider investigating packed processes for other unusual behavior, such as anomalous network connections.	

## **Discover Fileless Attacks**

To discover hidden adversaries using the Fileless Attacks analytic:

- 1. In the Investigations list, click the appropriate investigation to view it on the Investigation Details page. Ensure you included the Process hunt in your investigation.
- 2. In the upper-right corner of the page, select the **Custom View** drop-down arrow, and then select **Fileless Attacks** from the list. The Histogram automatically defaults to display results in the bottom 20 percent and lists each process name in the Visual Selector. If there are no results, drag the slider bar to a different percentage marker or click a column bar.
- 3. Select a result from the Visual Selector, which populates the Investigation Details table. The table displays each process occurrence in a separate row and each variable value such as the process name, process ID and parent process ID in a separate column.
- 4. In the **Attack Type** column, click the button that represents the attack type you want details of. A pop-up window displays details of where the memory was modified.



							HUNT SELEC Click the arro Process from	TION w and select the list.	ANA Click Filel	the arrow and ess Attacks fro	TON I select om the list.	
Download Tasking C	onfig					SELECT F	HUNT TYPE: Proc	255 🗸	Fileless	Attacks	~	
Process Name	AND: N/A		50%	Visual Sele	ector					2	Results Shown	
1			•	PROCESS	<u>NAME</u> rshell.exe					ENDF	<u>°OINT</u> 1	
0 Percent of	Endpoints	HIST Drag the c	OGRAN the slid lesired p	er bar on the Histogram to ercentage marker.								Select a result from the Visual Selector to populate the Investigation Details table.
ENDPOINT	PROCESS NAME	PID	PPID	PATH	COMMAND LINE	SIGNER	AUTHENTICODE	MALWARESCORETM	ATTACK T	YPE Ø		
endpoint-w-3- 06	svchost.exe	288 0	476	C:\Windows\SysWOW64\svchos t.exe	C:\Windows\SysWOW64\svchost.exe -k n etsvcs	Microsoft Windo ws	trusted	0				
endpoint-w-3- 08	svchost.exe	348 4	476	C:\Windows\SysWOW64\svchos t.exe	C:\Windows\SysWOW64\svchost.exe -k n etsvcs	Microsoft Windo ws	trusted	0				
endpoint-w-3- 03	svchost.exe	369 6	472	C:\Windows\SysWOW64\svchos t.exe	C:\Windows\SysWOW64\svchost.exe -k n etsvcs	Microsoft Windo ws	trusted	0		$\bigcirc \bigcirc \bigcirc \bigcirc$		
	PRC Eac sep tab	DCESS D h proces arate rov e. Click t	ETAILS s occurre v in the he Endp	ence displays on a nvestigation Detail point link to view						VIEW FILEL Click the AT details of th	ESS ATTAC TACK TYPE e modified	K DETAILS : button to display memory.

Fileless Attacks view in the Investigation Details area

TIP: Click for view a description of each attack type. To filter occurrences in the Investigation Details table by attack type, click the Attack Type column heading and select the box to the left of each appropriate type. To clear the filters, click Reset.

### **Analyze Fileless Attacks**

The initial step in analyzing Fileless Attacks is to confirm whether the memory process is malicious. Each process that detected hidden memory has memory strings available to download. It is recommended you analyze those strings for artifacts such as call back URLs and harvested system information for indicators that the process is malicious.

To download the memory strings:

- 1. In the Investigation Details table, click the **Download** button in the appropriate **ATTACK TYPE** column.
- In the dialog box that says, "Are you sure you would like to download strings from process name?" Click Yes. A "Request successful" message appears.
- 3. Click **Go to Endpoint** to go to the Endpoint Details page. The initiated task is selected in the Activity Timeline.



NOTE: If the process is no longer active, a "Download Strings" failure appears in the timeline:

- 4. In the upper-right corner of the Details pane on the right, click **Download Raw Data**, then select **RAW RESPONSE DATA**.
- 5. Save the file or open it in an external application.

### **Execute an Endpoint Response**

After you have confirmed the process is malicious, as a remedial action, you can execute an endpoint response to suspend or kill the associated threads or processes.

**NOTE:** Only administrators and Level 3 users can execute an endpoint response.

To execute an endpoint response:

- 1. In the Investigation Details table, click the link in the Endpoint column to go to the Endpoint detail page. The allinclusive data returned from the Process hunt appears.
- 2. In the **PROCESS NAME** column, select the appropriate process to terminate.



- 3. In the **PROCESS DETAILS** window, click **Kill Process**.
- 4. In the dialog box that says, "Are you sure you would like to kill the process process name (process ID) on endpoint hostname? click **Yes**. A "Kill Process submitted" appears to confirm the process was terminated.
- 5. Click Finish.

**WARNING:** There is also a **GET FILE** option; however, please use caution and ensure you are analyzing the file in an isolated environment as the file is likely malicious.

### Suspend a Thread for Memory Injection Hits

For Memory Injection attack types, you can suspend the thread directly from the Memory Details window:

1. On the THREAD ID row, click **SUSPEND THREAD**.



MEMORY INJECTION			
START ADDRESS ANOMALY CAL	L STACK ANOMALY		
TOTAL SIZE	4.1 KB		
MEMORY SECTION	MEMORY ADDRESS	SIZE	PROTECTION
	0x1180000	4.1 KB	RWX
START ADDRESS ANOMALY	0x1180000		
THREAD ID	512		SUSPEND THREAD
		<u>e</u> 6	

#### Memory Injection details

- 2. In the dialog box that says, "Are you sure you would like to suspend thread thread ID from endpoint hostname?" click **Yes**. A "Request successful" message appears.
- 3. Click Finish.



# **IOC Search Overview**

IOC (indicators of compromise) Search is a type of hunt that enables you to search across selected, monitored endpoints for specific attributes that would indicate the endpoint data was compromised. There are five IOC search types: File, Network, Process, Registry, and User, each which has a set of advanced configuration options. Although each of these can be added as individual hunts within an investigation, creating an IOC search compiles them into a single hunt, and after data is returned, displays results on the Search Results page.

**NOTE:** The difference between IOC Search and Artemis — Endgame's intelligent assistant — is the former searches for current endpoint data for both Windows and Linux endpoints, and the latter searches for historical process-related events that occurred on Windows endpoints.

For more information about Artemis, see "Artemis Overview" in Chapter 5, Artemis.

## **Execute an IOC Search**

**NOTE:** IOC Search results do not appear on the Investigation Details page, but on the Search Results page. As such, it is recommended you create an investigation with IOC Search as the sole hunt.

To create and execute an IOC search:

- 1. In the Endpoints list, select the box to the left of each appropriate endpoint.
- 2. On the Action toolbar, select an operating system tab (i.e., Windows, Linux, or Mac) to filter the Endpoints list.
- 3. Select the box to the left of each endpoint to include in the search.
- 4. On the Action toolbar, click **Create Investigation**.
- 5. In the **START INVESTIGATION** dialog window, type a unique name to identify the search and assign it to a different user, if necessary.
- 6. Click Add Hunt(s). An alphabetical list of all hunt types appears.
- 7. In the left column, select **IOC Search**.
- 8. In the right column, click **EXPAND** on each category to include in the search and enter advanced configuration as necessary. After you enter a value in one of the fields, the corresponding IOC search type is automatically selected.

**NOTE:** Registry search is not available for Linux endpoints.



**NOTE:** If you are searching for a specific filename on Windows endpoints, do not use uppercase letters.

9. Proceed with creating the investigation.

**Remember:** IOC Search appears as an event in the Activity Timeline of each endpoint that was included.

	Configure your pr	ofile and launch your hunts.	
Selecting Hunt(s)			
elect the hunt type(s) you v	want to task on the endpo	ints selected.	
IUNT TYPE		ADVANCED CONFIGURA	TION
Applications		File	EXPAND
File System	<u>Multiple Endpoints</u> <u>Disabled</u>		
Firewall Rules		Process	COLLAPSE
VIOC Search	<u>COLLAPSE</u>	Find Process	How do I build this guery?
Loaded Drivers		Tild Flocess	How do't baild this gacty:
Network	ADVANCED	csrss.exe	
Persistence	ADVANCED	With MD5 Hashes	
Process	ADVANCED	010101010101010101	0101010101010101
Registry	ADVANCED		
Removable Media	*		
Cancel			Confirm Hunts

Sample Process IOC search

For a complete list of advanced configuration options, see "<u>IOC Search Types and</u> <u>Advanced Configuration Options</u>" in this chapter.

# **View IOC Search Results**

Unlike other hunts, IOC search results do not have an Investigation Details view, but display on the Search Results page instead.

To view IOC search results:



 After you launch the investigation, click the "View Investigation" link on the START AN INVESTIGATION dialog window.

IOC search results are formatted as a tabular list. The total number of results displays in the upper-right corner.

	<b>SAVED SEARCH</b> Rerun a saved se	<b>ES</b> arch.					TOTAL RESULTS The total number of IOC sea results returned.
	Search Results				COLUMN SORT AND FILTE	R	16 TOTAL RESULTS
	SAVE SEARCH QUERY 0	SAVE SEARCH QUERY Save the current IOC search to run at a later time.	1		or filter the list.		1- <u>16</u> of 16 < >
	Collection Name	Hostname	Collection Type	Status	Endpoint IP	Operating System	Date Created
	processSearchResponse	35pc-w81x64-d	collection	success	10.6.77.236	Windows 8.1	Apr 5, 2017 10:19:39 AM UTC
	processSearchResponse	35pc-w81x86-d	collection	success	10.6.77.241	Windows 8.1	Apr 5, 2017 10:19:39 AM UTC
	processSearchResponse	35pc-w81x64-p	collection	success	10.6.77.244	Windows 8.1	Apr 5, 2017 10:19:39 AM UTC
	processSearchResponse	35pc-w81x86-p	collection	success	10.6.138.70	Windows 8.1	Apr 5, 2017 10:19:38 AM UTC
ARCH RESULTS LIST	processSearchResponse	35pc-w10x64l6-p	collection	success	10.6.77.242	Windows 10	Apr 5, 2017 10:19:05 AM UTC
IOC search.	processSearchResponse	35pc-w10x86l6-d	collection	success	10.6.77.240	Windows 10	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35pc-w10x86l6-p	collection	success	10.6.77.251	Windows 10	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W7X64-D	collection	success	10.6.77.250	Windows 7	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W2K8R2-D	collection	success	10.6.153.149	Windows Server 2008 R2	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W2K8R2-P	collection	success	10.6.77.248	Windows Server 2008 R2	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35pc-w2k12r2-d	collection	success	10.6.69.197	Windows Server 2012 R2	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35pc-w2k12r2-p	collection	success	10.6.77.243	Windows Server 2012 R2	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35pc-w10x64l6-d	collection	success	10.6.77.234	Windows 10	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W7X86-P	collection	success	10.6.135.86	Windows 7	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W7X64-P	collection	success	10.6.77.252	Windows 7	Apr 5, 2017 10:19:04 AM UTC
	processSearchResponse	35PC-W7X86-D	collection	success	10.6.77.253	Windows 7	Apr 5, 2017 10:19:04 AM UTC
C TI Si	OLLECTION NAME he name of the IOC earch item. Select an	HOSTNAME The hostname of the endpoint.	COLLECTION TYPE The category of the collection item.	STATUS The status of a executed task.	n The IP address of the endpoint.	ne OPERATING SYTSEM The operating system running on the endpoint.	DATE CREATED The date and time the collection item was indexed in the search database.
0	n the Endpoint Detail						

### IOC Search Results list

 $\downarrow$  NOTE: If the IOC search does not return any results, the page says, "There are no results."

### **IOC Search Results Overview**

The columns in the IOC Search Results list provide the following endpoint data:

Column Name	Description
COLLECTION NAME	The name of the IOC Search item, e.g., processSearchResponse. (Note: This is one text string with no spaces).
HOSTNAME	The hostname of the endpoint.
COLLECTION TYPE	The category of the collected endpoint data (e.g., detection, prevention, response, etc.). All IOC searches are collections.



Column Name	Description
STATUS	Indicates whether the collected endpoint data was a success or failure.
ENDPOINT IP	The IP address of the endpoint.
OPERATING SYSTEM	The operating system running on the endpoint.
DATE CREATED	The date and time the endpoint data was indexed in the search database.

## **View Results for a Single Endpoint**

To view complete hunt details for a specific endpoint:

- 1. In the IOC Search Results list, locate the appropriate endpoint hostname or IP address.
- 2. Click the search item in the corresponding COLLECTION NAME column.
- 3. View results in the Activity Details pane on the Endpoint Details page.

IoC Search - Pro Apr 5, 2017 10:19:38 A	ess MUTC					VIEW INVESTIGAT	ION DETAILS	DOWNLOAD RAW DATA
Process N	me PID	PPID	Parent Process Name	Path	Command Line	Signer	Authenticode	1- <u>1</u> of 1 < > MalwareScore™
lsass.exe	524	424	wininit.exe	C:\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe	Microsoft Windows Publisher	trusted	

Process hunt details for a single endpoint



**NOTE:** If you included other hunts in the investigation, you can click **VIEW INVESTIGATION DETAILS** to view those results on the Investigation Details page. However, if IOC Search is the sole hunt in the investigation as recommended, if you click **VIEW INVESTIGATION DETAILS**, a message that says, "View results for this Hunt in search" appears. When selected, it redirects to the Search Results page.

## Sort Columns in the IOC Search Results List

You can sort columns in the IOC Search Results list to change the order the contents appear.

To change the sort order within a column:

- 1. Select the appropriate column heading to sort or filter.
- 2. To sort by increasing value, click **Ascending**. To sort by decreasing value, click **Descending**. The currently sorted column is denoted by an arrow.

TIP: If there is a large number of results, consider changing the range display to a higher number to avoid searching the same criteria on multiple pages.



# **IOC Search Types and Advanced Configuration Options**

The following table describes each IOC search type and its advanced configuration options. When you configure an IOC search, keep the following in mind:

- In the **ADVANCED CONFIGURATION** column, click **EXPAND** or **COLLAPSE** on an IOC Search type to show or hide the configuration settings.
- You must enter a value in at least one field of the selected IOC search type.
- To ensure accuracy, carefully review advanced configuration for each search type. Select all appropriate options and enter values accordingly.
- Click *How do I build this query?* for guidance on how to structure a query.
- For text box entries, follow the same format as the parenthetical examples, if given.

IOC Search Type	Description	Advanced Configuration		
File	Searches for running files.	<b>Directory:</b> Type the starting directory path (e.g., C:\windows\system32). <b>Find File:</b> Type the filename(s) to search.		
		<ul> <li>TIP: Type a regex (regular expression) to narrow search results. For example, to find a file that ends with test.txt, use the following regex: .*test\.txt'</li> <li>With MD5 Hashes: Type the MD5 hash(es). Separate multiple entries with a semicolon.</li> <li>Or SHA1 Hashes: Type the SHA1 hash(es). Separate multiple entries with a semicolon.</li> </ul>		
		<ul> <li>Or SHA256 Hashes: Type the SHA256 hash(es). Separate multiple entries with a semicolon.</li> </ul>		
Process	Searches for running processes.	<ul> <li>Find Process: Type the process name or file path you are looking for.</li> <li>Separate multiple entries with a semicolon.</li> <li>With MD5 Hashes: Type the MD5 hash(es). Separate</li> </ul>		
		multiple entries with a semicolon.		
		<ul> <li>Or SHA1 Hashes: Type the SHA1 hash(es). Separate multiple entries with a semicolon.</li> </ul>		
		<ul> <li>Or SHA256 Hashes: Type the SHA256 hash(es). Separate</li> </ul>		


IOC Search Type	Description	Advanced Configuration
		multiple entries with a semicolon.
Network	Searches for network	Find Remote IP Address: Type the remote IP address or range.
	connections.	Find Local IP Address: Type the local IP address or range.
		Communicating on Port
		Select one of the following options and enter the port in the text box:
		Remote Port
		Local Port
		<ul> <li>With State: Click the arrow and select which port state(s) to return.</li> </ul>
		<ul> <li>Over Protocol: Click the arrow and select which connection type(s) to return.</li> </ul>
Registry	Searches for a registry key or value	<b>Base Hive (Required):</b> Click the arrow and select all or one of the six root keys.
	name.	<b>NOTE:</b> You must enter a value in at least one of the following options:
		Enter Registry Key or Value Name Containing: Type a registry key or value name. Separate multiple entries with a semicolon.
		By Size
		<ul> <li>Max Byte Size: Enter the maximum file size of the registry key, in bytes.</li> </ul>
		<ul> <li>Min Byte Size: Enter the minimum file size of the registry key, in bytes.</li> </ul>
		<b>Registry Date Modified:</b> Specify a date and time range of when the registry was modified:
		<ol> <li>Select a start date from the calendar widget. Use the &lt; and &gt; arrows to navigate to previous and following months.</li> </ol>
		<ol> <li>To specify a starting time other than the default 12:00 AM UTC, place your cursor in each text box and enter the appropriate time in HH:MM format. Select AM or PM.</li> </ol>
		<ol> <li>Specify an end date and time using the same procedure in steps 1 and 2.</li> </ol>



IOC Search Type	Description	Adva	nce	ed	Co	onfi	gu	rati	ion
		CALE	NDA	R FI	LTE	R			
		<		Se	ер 20	18		>	From Sep 1, 2018 UTC
		S	М	т	W	т	F	S	08:15 AM PM
		26	27	28	29	30	31	1	
		2	3	4	5	6	7	8	To Sep 6, 2018 UTC
		9	10	11	12	13	14	15	11 : 30 AM PM
		16	17	18	19	20	21	22	
		22	24	25	26	27	20	20	
		25	24	20	20	21	20	29	Clear Selection
		30	1	2	3	4	5	6	Apply Filters
User	Searches the	Find Us	er:	Тур	eαι	Jser	nam	ne(s)	. Separate multiple entries with a
	network for logged in	semicol	on.						
	network for logged in	On Don	nain	: Tv	ne t	heo	dom	ain r	name.
	users.	0.1.2.01			201				

# CHAPTER 4

# **ALERTS**

Alerts Overview	106
Alert Dashboard Overview	108
Alerts Page Overview	111
Alert Details Page Overview	120
Alert Metadata Panel Overview	121
Respond to an Alert	138
Assign an Alert	142



# **Alerts Overview**

Alerts are Endgame sensor-generated notifications that detect potentially malicious activity on monitored endpoints, such as a process injection or permission theft. Alerts are a vital feature of Endgame because they identify abnormal behavioral patterns that may require an investigation.

A previously configured Endpoint Policy, which is enabled upon deployment, specifies which endpoint activities the sensor monitors and the action the sensor should take if it detects potentially malicious activity. If the sensor detects such malicious activity, it generates an alert in the Endgame platform.

Alerts are divided into two sensor action types: **preventions** and **detections**. A prevention alert is generated when the sensor blocks malicious activity on an endpoint by executing an automated response. A detection alert is generated when the sensor detects potentially malicious activity on an endpoint but does not execute a response. You can view the inclusive list of generated alerts in the Alerts list.

**NOTE:** If the sensor is offline, it locally stores recent alerts and resends them to the Endgame platform once it has reestablished a connection.

When an alert is generated, the sensor collects related endpoint metadata, stores it in the Endgame platform, and displays it in the Alert Metadata panel, located on the Alert Details page. The Alert Details page also displays the Endgame Resolver<sup>™</sup> Attack Visualization, a visual timeline that chronologically depicts the events that led up to the alert.

For more information about the Alert Details page, see "View Alert Details" in this chapter.

Alerts are also divided into two categories: **threats** and **adversary behaviors**. Threat alerts capture specific malicious activity that occurs on an endpoint. If a threat is detected, in addition to a generating an alert, the sensor displays a notification in the Endgame platform, which appears as a flashing red "Alerts" button (megaphone icon) on the Left Navigation toolbar. The button continues to flash until you select it to view the Alert Dashboard.



## New threat alert notification

피

The following alerts are considered threats:

- Malware
- Exploit
- Process Injection
- Ransomware
- Credential Manipulation
- Credential Dumping



- Permission Theft
- Blocklist alerts

Adversary behavior alerts are directly mapped to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK<sup>™</sup>) and are useful to understand the tactics and techniques an attacker may use when executing an attack.



# **Alert Dashboard Overview**

The Alert Dashboard provides a statistical summary of alert status within your environment. It consolidates qualitative alert data into a concise visualization that enables you to do the following:

- Monitor incoming alerts in real time
- Identify which alerts are unread and assigned to you
- · Identify behavioral patterns across your endpoints
- Triage alerts so you can prioritize items that may require immediate attention

To view the Alert Dashboard, click the **ALERTS** button **See 1** on the Left Navigation toolbar.

The dashboard contains two major components:

- 1. Threats and Adversary Behaviors Key Performance Indicator (KPI) charts
- 2. Most Recent Threats and Infected Endpoints

				?	Ask Artemis	Welcome, Super Jan 19, 2018 1:58 PM UTC (EST+5)
Threats <b>300</b> <u>View All</u>	<u>18</u> Unread <u>27</u> Assigned to Me	0	Adversary Behaviors <b>247</b> <u>View All</u>	<u>18</u> Unread <u>27</u> Assigne	d to Me	36 Unread Alerts 54 Alerts Assigned to Me View All Alerts
ost Recent Threats				Mo	st Infected Endpoints	
ost Recent Threats	HOSTNAME	ASSIGNEE	DATE	Ma	st Infected Endpoints	HOSTNAME
ost Recent Threats ALERT TYPE Malicious File	HOSTNAME qasr-w81x86-p	ASSIGNEE	<b>DATE</b> Mar 9, 2018 4:25:10	Ма	st Infected Endpoints ALERT COUNT 37	HOSTNAME qasr-w81x86-p
ost Recent Threats ALERT TYPE Malicious File Ransomware	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d	ASSIGNEE Unassigned Unassigned	DATE Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10		st Infected Endpoints ALERT COUNT 37 35	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d
ost Recent Threats ALERT TYPE Malicious File Ransomware Process Injection	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d 2gxa-w10x6416-d	ASSIGNEE Unassigned Unassigned Unassigned	DATE Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10	Мо РМ ИТС РМ ИТС	st Infected Endpoints ALERT COUNT 37 35 23	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d 2gxa-w10x64l6-d
ost Recent Threats ALERT TYPE Malicious File Ransomware Process Injection Exploit Protection	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d 2gxa-w10x6416-d qasr-w81x86-p	ASSIGNEE Unassigned Unassigned Unassigned Unassigned	DATE Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10 Mar 9, 2018 4:25:10	MC IPM UTC IPM UTC IPM UTC	st Infected Endpoints ALERT COUNT 37 35 23 21	HOSTNAME qasr-w81x86-p 2gxa-w2k12r2-d 2gxa-w10x64l6-d qasr-w81x86-p

Alert Dashboard

# Threats and Adversary Behaviors KPI Charts

Threats and Adversary Behaviors charts display the total number of alerts that fall into each of these categories. Threats capture specific malicious activity that occurs on an endpoint. Adversary behaviors alerts are directly mapped to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK<sup>™</sup>).

Each chart also displays the number of unread alerts and the number of alerts assigned to you. These numerical values are user-specific, and, therefore, may vary for each user. Each numerical value is also an active link that when selected, filters



the Alerts list by that attribute. For example, to view all unread threat alerts, click the "Unread" number link on the Threats KPI chart.

The Totals chart on the far right provides numerical values for the total number of unread and assigned alerts. To view a comprehensive list of Alerts, click **View All Alerts**.



Threats and Adversary Behaviors charts

# Most Recent Threats and Infected Endpoints Cards

The Most Recent Threats card lists the most recent threat alerts generated in the Endgame platform. It also lists general details about the alert, including the hostname, assignee, and date it was generated. Select an alert from this list to view inclusive details on the Alert Details page.

The Most Infected Endpoints card lists the top five endpoints with the highest alert count. Each row displays the affected hostname and alert count. The alert count value is an active link that when selected, filters the Alerts list by the alerts associated with that endpoint.

**NOTE:** The number included in the total alert count includes threats and adversary behaviors that have not been resolved (i.e., not dismissed or marked as "Resolved").



st Recent Thre	reats					Most Infected Endpoints	
ALERT TYPE		HOSTNAM	E	ASSIGNEE	DATE	ALERT COUNT	HOSTNAME
Malicious File		qasr-w81x8	6-p	Unassigned	Mar 9, 2018 4:25:10 PM UTC	37	qasr-w81x86-p
Ransomware		2gxa-w2k1	tr2-d	Unassigned	Mar 9, 2018 4:25:10 PM UTC	35	2gxa-w2k12r2-d
Process Injection	on	2gxa-w10x	416-d	Unassigned	Mar 9, 2018 4:25:10 PM UTC	23	2gxa-w10x64l6-d
Exploit Protectio	on	qasr-w81x8	6-р	Unassigned	Mar 9, 2018 4:25:10 PM UTC	21	qasr-w81x86-p
Cradantial Dump	ala a	0		the second second			
rt Dashboard	ping	zgxa-wzĸ1.	(	Ask Artemis	Mar 9, 2018 4:25:10 PM UTC	18	Zgxa-wzx12f2-d
rt Dashboard Threats 300 Yinx All	31 Unread 22 Assigned to Me	2gxa-wzx1.	Adversary Behaviors 247 2247	Ask Artemis     Ask artemis read signed to Me	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d
rt Dashboard	38 Unread 22 Assigned to Me	2gxa-wzx1	1/2-3 Meneracy Behaviors 11 Ure 247 22 As View All	Ask Anemis  read  signed to Me  Most Infected Endpoints	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d
rt Dashboard Toreats 300 Vien All Recent Threats	JI Unread 22 Assigned to Me	ASSIGNEE	Adversary Behaviors 247 547 547 557 557 557	Ask Artemis      Ask Artemis      Ask Artemis      Ask Artemis      Ask Artemis      Ask Contemportunity      Ask Co	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d
rt Dashboard Threats 300 View All Recent Threats Licker trys Licker trys Licker trys	11 Unread 22 Assigned to Me HOSTRAME correlitation	ASSIGNEE	fife-d         11 Um           Adversary Behaviors         11 Um           247         22 As           View All         11 Um           Date         11 Um           Mare 2015 4:25 10 PM UTC         11 Um	Ask Aremis      Ask Aremis      Most Infected Endpoints      Mast roour      7      7	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d
rt Dashboard	18 Unread 22 Assigned to Me w03TNAME gameTtalling 2gaw2h102-d	Assidente Unassigned	Moversary Bahasolors 247 247 647 847 847 847 847 847 847 847 847 847 8	Consisting and Consisting and Consisting and Consisting and Constructed Endpoints	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d
rt Dashboard	18 Unward 27 Assigned to Me HOSTNAME Qarantinisp Spanishipo Spanishipo Spanishipo Spanishipo	Assidue: Unassgref Unassgref	Fif2-0         11 Units           Adversary Behaviors         11 Units           247         22 As           Safe         11 Units           Mar # 2018 425 10 PM UTC         Mar # 2018 425 10 PM UTC           Mar # 2018 425 10 PM UTC         Mar # 2018 425 10 PM UTC	Ask Areenis     Ask Areenis     Ask Areenis  Most Infected Endpoints      Acta Topology      22      23      23	Mar 9, 2018 4:25:10 PM UTC	18	2gxa-w2K12f2-d

Most Recent Threats and Infected Endpoints Cards



# **Alerts Page Overview**

The Alerts page displays essential details about all alerts generated in the Endgame platform and provides options to filter, respond to, and manage them.

The Alerts page contains two major sections:

- 1. Action toolbar
- 2. Alerts list

To view the Alerts page, click the **ALERTS** button on the Left Navigation toolbar to view the Alert Dashboard, then choose one of the following options:

- Select a value on the Threats or Adversary Behaviors chart, which shows a filtered view of alerts that fall within the selected category
- Click View All Alerts on the Totals chart on the far right to view all generated alerts

Alerts Download JSON Download CSV					Archived Alerts	Ask Artemis Ask Artemis Welcome	e, Super 18 7:43 PM UTC (EDT+4)
9 7 1 All Unread	Assign Resolve Alerts Alerts Corrent ▶ Current ▶	Dismiss Unactionable Alerts Current	Mark All As Read Current ►				0
9 0 Detections Preventions To & &	9 0 0 tal Assigned To Me Quarantined 3 🗞						0
3 alerts currently selected 🗸							1 - <u>9</u> of 9 < >
ALERT TYPE	EVENT TYPE	ASSIGNEE	<u>05</u>	IP ADDRESS	HOSTNAME	DATE	
<ul> <li>Malicious File</li> <li>Detection</li> </ul>	Creation	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:41:59 PM UTC	
Ransomware Detection		Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:47 PM UTC	
<ul> <li>Ransomware</li> <li>Detection</li> </ul>		Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:43 PM UTC	
<ul> <li>Process Injection</li> <li>Detection</li> </ul>	Shellcode Injection	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:30 PM UTC	
Malicious File     Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:11 PM UTC	
Malicious File     Detection	Execution	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:00 PM UTC	
Malicious File     Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 6:40:00 PM UTC	
Malicious File Detection	Execution	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 1:43:59 AM UTC	
Malicious File     Detection	Modification	Unassigned	Windows 10 (v1803)	10.6.238.170	DESKTOP-QBBSCUT	Sep 20, 2018 1:43:53 AM UTC	
						Last Us data di Cas 20, 2010 6	10-00 D111T0 (TDT: 0

### Alerts page

# **Action Toolbar**

The Action toolbar is located at the top of the Alerts page and enables you to execute various tasks for selected alerts. It also contains various key performance indicators (KPIs) to narrow alerts by specific parameters.





Action toolbar on the Alerts page

# **Alert Key Performance Indicators**

The Action toolbar contains two main KPIs, **All** and **Unread**, that display the total number of alerts and the total number of unread alerts, respectively.

A secondary set of KPIs beneath the toolbar displays the number of alerts that fall within a specific category:

KPI	Description
Detections	Potentially malicious activities on monitored endpoints that were detected but require remediation.
Preventions	Malicious activities on monitored endpoints that were detected and blocked.
Quarantined Files	Malicious File alerts that contain quarantined files.
Assigned To Me	Alerts that are assigned to you.
Total	The total number of generated alerts.

Each KPI is an active link, that when selected, filters the Alerts list by the selected category. Filters are useful to narrow alerts by specific criteria to find targeted data. For example, to view all unread detections, select **Unread**, and then select **Detections**.





# **Alert Actions**

The Action toolbar also contains three menu options that execute specific tasks for selected alerts simultaneously:

Menu Option	Function
Assign Alerts	Assigns alerts to a specific user.
Resolve Alerts	Resolves alerts and moves them to the Archived view.
Dismiss Unactionable Alerts	Dismisses alerts and moves them to the Archived view.
Mark All As Read	Marks all alerts as read and clears the "Unread" bullet mark.

Dismissing or resolving an alert moves it to the Archived view. For more information about alert responses, see "Respond to an Alert" in this chapter.

# **Alerts List**

i

The Alerts list is an enumeration of all generated alerts and their relevant details, organized in a table. The list is useful to view the history of accumulated alerts to identify outliers or abnormal endpoint activity. For example, if the list shows several alerts for a process injection that each occurred one minute apart, this could signify an attempted data breach that requires an immediate response.

Alerts display in reverse chronological order with the most recently generated alerts at the top. Unread alerts are distinguished with a bullet mark • that disappears after the current user views the alert.

**NOTE:** The bullet mark • appears on each user's screen until they view it. Therefore, if another user is logged in to the platform and views the alert, it still appears as new to the current user.





## Columns in the Alerts list

The columns in the list provide the following information about each alert:

Column Name	Description
ALERT TYPE	The name of the alert and whether it is a detection or prevention.
EVENT TYPE	Specifies the type of activity that occurred on the affected endpoint (e.g., "Shellcode Injection" for a Process Injection alert).
	<b>NOTE:</b> If an alert was triggered by a Custom Rule, the event type is listed as the user-created rule name.
ASSIGNEE	If applicable, the name of the user assigned to the alert. If no user is assigned, the column says, "Unassigned."
	TIP: You can click the "Unassigned" link to assign a user to the current alert.
OS	The operating system running on the affected endpoint.
IP ADDRESS	The IP address of the affected endpoint.



Column Name	Description
HOSTNAME	The hostname of the affected endpoint.
DATE	The date and time the alert was generated according to Coordinated Universal Time (UTC).

**NOTE:** If you filter the list by alert type, the columns change to display data relevant to the alert type. For more information, see "Sort and Filter Alerts."

# **Page Pagination**

In the upper-right corner above the list is a range display, which displays the current number range of alerts out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 alerts display per page; however, you can change the number to a preferred choice:

- 1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
- 2. In the Max count of text box, enter a new number between 1 and 500.
- 3. Click  $\checkmark$  to save your changes.



# **Sort and Filter Alerts**

Aside from the filters on the Alert Dashboard, the Endgame platform provides other options to sort and filter alerts. Sorting and filtering are time-efficient methods to find specific information without browsing through a large amount of data. In addition, it helps prioritize which alerts require an immediate investigation or remedial action.

# Filter by Key Performance Indicator

Each key performance indicator (KPI) on the Alerts page is an interactive link that filters the Alerts list by the selected category. For example, to view all unread preventions, select **Unread**, then select **Preventions**.







KPIs on the Alerts page are also selectable filters

# Filter by Alert Type

Filtering by alert type narrows alerts by selected threats or adversary behaviors, which can identify false positives or behavioral trends. To filter by alert type, select the **ALERT TYPE** column heading, then select the box to the left of each appropriate alert type. If you select a single alert type, the columns in the Alerts list change to display data relevant to the selected type. However, if you select more than one alert type to filter by, the standard set of columns appears in the list.

**NOTE:** If you select the Threats or Adversary Behaviors numerical value on the Alert Dashboard, the alerts that fall within the selected category are automatically selected in the "ALERT TYPE" column.

	■ <b>■</b> <u>ALERT</u>	ТҮРЕ		
COL	UMN: FILTER			<u>Reset</u>
<b>~</b>	Blocklisted File		Execution	Permission Theft
	Collection		Exfiltration	Persistence
	Command and Control		Exploit Protection	Privilege Escalation
	Credential Access		Impact	Process Injection
<b>~</b>	Credential Dumping		Initial Access	Ransomware
<b>~</b>	Credential Manipulation		Lateral Movement	Registry Modification
	Defense Evasion		Malicious File	
	Discovery		Other	

### Filter by alert type

# Sort by Order

To sort by ascending or descending order:

- 1. Select the appropriate column heading. The Column Sort and Filter panel appears.
- In the COLUMN: SORT section, select the Ascending option to sort by increasing value or the Descending option to sort by decreasing value. The currently sorted column is denoted by an arrow 1.



# **Filter by Value**

You can filter columns in the Alerts list by one or more specific values by doing the following:

- 1. Select the appropriate column heading. The Column Sort and Filter panel appears.
- 2. Choose one of the following options to add filters:
  - In the **Selected Filters** section, begin typing a value in the text box. Autocomplete displays the value(s) that matches the entry. Select the appropriate value, and then click **ADD** or press **Enter**.

TIP: If you do not know the exact name, type a wildcard character (\*) anywhere in the text to help find desired values.

Select the appropriate values from the TOP 5 and/or BOTTOM 5 columns. These are auto-populated values
that display the five highest and five lowest values from the selected column, which is useful to view possible
values of interest. The numerical count of each value is also displayed in a separate column. Each added value
appears as a selectable filter.

	Sort by ascending order.	or s	elect the column ort or filter.	a to	I <u>P ADDRESS</u>
	COLUMIN: SORT	Clear all fi	ters.		
Begin typing a value to filter by in the text box. Autocomplete populates values that match the entry.	Selected Filters (1)	Clear Selection	TOP 5	COUNT BOTTOM 5 20 I Header F 9 Key Adde 6 Modifice 4 Shellood	Yrotection 2 sd 2 tion 2 e Injection 2
	Added filters appear here. Click the <b>X</b> to remove an individual filter.	Apply the to the list press <b>Ent</b>	e filter , or <b>er</b> .	Displays the top values and their Select a value to	5 and bottom 5 individual count add a filter.

### Column sort and filter panel

i

Values in the bottom 5 are less common, therefore, it is recommended you analyze alerts within this category to determine if there are any outliers.

After you sort a column by order or apply filters, the Alerts list updates with the new data. The currently filtered column is

denoted by an 🗉 symbol, and columns that are sorted and filtered are denoted by an 🖭 symbol.

**NOTE:** If you select values from the top or bottom 5, you do not have to click **ADD** – they automatically appear as filters.

# **Remove Filters**



To remove a filter from a column:

- 1. Select the appropriate column heading. The Column Sort and Filter panel appears.
- 2. Choose one of the following options:
  - In the **Selected Filters** section, click the **X** on the appropriate filter.
  - Deselect the appropriate values from the TOP 5 or BOTTOM 5.
  - To remove all filters, click Clear Selections.

TIP: To clear all column filters and the sort order, select the All tab on the Action toolbar.



# Download the Alerts List

You can download the current Alerts list to a comma-separated values (CSV) file or JSON file. Any sort and filter preferences applied to the list are retained in the downloaded file.

**NOTE:** Downloading the Alerts list to an external file is different from exporting the list to a third-party tool.

To download the Alerts list:

1. In the upper-left corner of the Alerts page, click **Download JSON** or **Download CSV**.



2. When the download is complete, open or save the file from your browser.



# **Alert Details Page Overview**

The Alert Details page provides comprehensive details about the selected alert, various user actions to respond to the alert, and it displays the Endgame Resolver<sup>™</sup> Attack Visualization, which shows the series of events that led to the alert.

The Alert Details page contains two sections:

- 1. Alert Metadata panel
- 2. Endgame Resolver™ Attack Visualization



Alert Details page



An Elastic company

# Alert Metadata Panel Overview

The leftmost side of the Alert Details page displays the Alert Metadata panel. The panel is an accumulation of alert details, comprised of multiple sections that provide details about a specific data component. When selected, each section expands or collapses to either expose or hide details.



### Alert Metadata panel

Although the information displayed in these sections varies according to the alert type, each alert contains the following sections in the metadata panel:

Section	Description
Summary	A brief synopsis that explains what malicious activity occurred to generate the alert, the hostname of the affected endpoint, and the date and time it occurred, according to Coordinated Universal Time (UTC) or your selected time zone.
Overview	General metadata about the alert, including the type, event type, status, assignee, severity level, and the date created. This section displays in an expanded state by default.
	<b>NOTE:</b> If an alert is triggered from a Custom Rule, two additional fields appear In the Overview section: "Rule Name" and "Last Edited By."



Section	Description			
	Detected Defense Evasion       Take Action         on RND-EP-wol-07 (172,31,27,17) at Jul 27, 2019 5:00:39 PM UTC       Image: Commande Enrichments         Alert       Image: Commande Enrichments         Alert       Image: Commande Enrichments         Status       Open         Assigned To       Unassigned         Severity       Medium         Date Created       Jul 27, 2019 5:00:39 PM UTC         Rule Name       RunDLL32 Loading DL suth enrichments         Description       Identifies FunDLL32 Loading DL suth enrichments         Image: Commande Enrichments       Image: Commande Enrichments         Description       Identifies FunDLL32 Loading DL suth enrichments         Description       Identifies FunDLL32 Loading DL suth enrichments         Commonly used by Advertarias or commonly used by an ordinal value commonny used by Advertarias or code.         Code to streatifie for Defense Evasion         Tectics       Defense Evasion         Technique IDs			
Related Alerts	A list of threat and behavior alerts related to the current attack. Select an alert to view general details and a list of spawned processes in the Endgame Resolver <sup>™</sup> . For more information, see " <u>Alert Details Page</u> <u>Overview</u> " in this topic.			
Comments	View and add comments about an alert, which are shared among team members who have access to Endgame. For more information, see " <u>Alert Commenting Overview</u> ."			
Enrichments	A list of unique, related MITRE ATT&CK™ techniques that provide additional contextual information about an alert.			
Endpoint	Information about the affected endpoint, including the hostname, IP address, endpoint status, operating system, the total number of generated alerts, and any assigned groups.			
(i)	The endpoint hostname appears in the "Summary" and "Endpoint" sections and is an			

The endpoint hostname appears in the "Summary" and "Endpoint" sections and is an active hyperlink that goes to the relative Endpoint Details page.

In the upper-right corner of the Alert Metadata panel is the **Take Action** menu, which contains a list of options that enable you to execute one of the following alert tasks:

Take Action Menu Option	Description
Download Alert	Downloads the raw JSON of the alert details.



Take Action Menu Option	Description	
Download Timeline	Downloads the raw JSON of the events that occurred in the Endgame Resolver™ Attack Visualization.	
Resolve	Marks the alert as resolved and moves it to the Archived view.	
Dismiss	Marks the alert as dismissed and moves it to the Archived view.	
Start Investigation	Starts a new investigation.	
Kill Process (Exploit alerts only)	Terminates the source process.	
	NOTE: This option is a pivot action on the Endgame Resolver™ Attack Visualization.	
Suspend Thread (Process Injection alerts only)	Suspends the malicious process thread by thread ID.	
Download File (Malicious File alerts only)	Downloads the malicious file.	
	<b>NOTE:</b> The file must be retrieved from the endpoint before you can download it.	
Retrieve File (Malicious File alerts only)	Retrieves the malicious file from the endpoint and sends it to the Endgame platform.	
	NOTE: If the file was previously retrieved, the "Download File" option appears instead. However, the "Retrieve File" option is a pivot action on the Endgame Resolver™ Attack Visualization.	
Delete File (Malicious File alerts only)	Deletes the file from the affected endpoint.	
Delete from Blocklist (Blocklist alerts only)	Deletes the hash from the blocklist, and, if the option is selected, restores the quarantined file to its original location.	
Unarchive Alert	Moves the alert from the Archived view to the Current view.	
	<b>NOTE:</b> This option is available only if the alert was resolved or dismissed.	
Add to Exceptionlist	Adds selected alert attributes to the exceptionlist to prevent future alerts from generating.	
Isolate Host	Isolates the endpoint to prevent it from communicating with all systems.	
Release Host	Releases the endpoint from isolation.	



**NOTE:** Options in the **Take Action** menu only execute a task for the current alert. You can execute a task for multiple alerts from the Alerts page.



# Endgame Resolver<sup>™</sup> Attack Visualization Overview

The Endgame Resolver<sup>™</sup> Attack Visualization is a visual timeline of events that led up to the alert and the events that occurred immediately after the alert. Viewing the Endgame Resolver<sup>™</sup> Attack Visualization is useful to determine the origin of the malicious activity and other areas in your environment that may be compromised once that activity is detected. The Endgame Resolver<sup>™</sup> provides process, DNS, file, network, image load, and registry data for both parent and child events, and provides one-click response actions to resolve the alert.

**NOTE:** API, CLR (Common Language Runtime), WMI ((Windows Management Instrumentation), and PowerShell currently are beta events.

# **How it Works**

Once an alert is generated, the sensor collects event data and stores it in the Endgame platform. Once you select an alert to view, the Endgame Resolver<sup>™</sup> Attack Visualization, which appears on the right-hand side of the Alert Details page, presents the collected event data as a visual timeline to display the series of events that occurred before and following the malicious activity. By default, the Endgame Resolver<sup>™</sup> centers on the malicious process that generated the alert. Related events are grouped in a hierarchical structure so you can view events in sequential order.

NOTE: Registry Monitor alerts do not have an Endgame Resolver<sup>™</sup> Attack Visualization and display a generic error message in its place.

# Endgame Resolver<sup>™</sup> Attack Visualization User Interface

The Endgame Resolver<sup>™</sup> Attack Visualization contains the following user interface components:

- 1. Event nodes
- 2. Event Metadata card
- 3. Child events
- 4. Child process event nodes
- 5. Related Alerts
- 6. Alert Enrichments
- 7. Endgame Resolver<sup>™</sup> controls
- 8. Endgame Resolver™ timeline status
- 9. Expand/Collapse





Endgame Resolver™ Attack Visualization on the Alert Details page

# **Event Nodes**

i

Each process event that occurred before and after the alert was generated is called an "event node" and is denoted by a hexagonal icon with the letter "P." A time value is displayed between each event node to indicate how much time passed between the previous and next event.

The time values are listed as milliseconds (ms), seconds (secs), minutes, (mins), hours (hrs), and weeks.

Event nodes are color-coded to indicate the status of the process:

Color	Status	Description
Blue	Benign	The sensor did not determine the file is malicious.
Red	Malicious	The sensor determined the file is malicious.
Gray	Terminated	The process was terminated via a "kill process" task.

## **Process Details**

To view details of a specific process, select the appropriate event node, which displays an Event Metadata card. The card provides the event type (e.g., process running, process created, process terminated, etc.), the date and time the process event occurred, and additional data such as the path, user, PID, domain, and MD5 hash value. The **Respond** drop-down menu contains two options to either retrieve the file or kill the process, which is a method of responding to the alert if it requires you to take action.





Select an event node to view details in the Event Metadata card. Click the **Respond** drop-down arrow to kill the process or retrieve the file.

**NOTE:** The "Process Terminated" event type appears on the Event Metadata card only if the **Kill Process** response was executed successfully. The "Retrieve File" response sends a "Get File" task to transfer the file from the endpoint to the platform. After this task is executed, you must download the file — which is in a password-protected zip file — from the Endpoint Details page. For more information, see ""Endpoint Response Types and Advanced Configuration Options.""

macOS events contain fork and exec processes:





Process fork running on a Mac endpoint

### About Terminated Processes in the Endgame Resolver™

If a process was terminated, the hexagonal borders of the event node appear gray to indicate the process was killed. If you terminate a process via the inline "Respond" option in the Endgame Resolver<sup>™</sup>, you must first retrieve the latest data before you can see it in the timeline. For more information, see "<u>Retrieve</u> New Timeline Data in the Endgame Resolver<sup>™</sup>."





A terminated process in the Endgame Resolver™

# **Child Events**

i

If there are process, DNS, network, file, or registry child events that spawned from the parent process, a group of numerical values that represent the number of child events, called Child Event KPIs (Key Performance Indicators), displays to the right of the event node. The DNS, network, file, and registry values are active hyperlinks that display an inclusive list of child events in a secondary window when selected. To view inclusive details about one of these child events, select an event from the list and view details in the secondary window that appears. To switch to a different event type, click the **View** drop-down arrow and select the appropriate option from the list.

Endpoints running on macOS do not contain DNS or registry child events.





Select one of the Child Event KPIs to view a list of child events that spawned from the parent process. Select one of the child events in the Event Metadata card to view inclusive details.

# **Child Process Events**

If there are child process that spawned from the parent process, they are denoted by a blue cylindrical button with a number, as seen in the following image:



This number indicates the total number of child processes, which you can view in the timeline by selecting the button. Viewing child process events is useful to see what activity occurred on the endpoint after the alert was generated — which is especially recommended for threat alerts. Multiple child processes display at a perpendicular angle and can be collapsed by clicking the blue button again, which, in its expanded state, appears as a small triangle inside a circle.



NOTE: By default, the Endgame Resolver<sup>™</sup> displays the first level of child process events. You can continue expanding child process events as necessary.

# **Related Alerts**

At the top of the Endgame Resolver<sup>™</sup> are Related Alert Key Performance Indicators, which display the number of threats and behaviors that are related to the same process tree on a single endpoint. Select a KPI to view a list of those alerts in "Related Alerts" tab of the Alert Metadata panel. From here, you can select an alert to view general alert details and spawned child events in the Event Metadata card.

	alerts in the Alert Metadata panel
Select an alert to view details in the Event Middle Select and Select the Control of a Middle File       RESOLVER         Select an alert to view details in the Event Middle Select Select And Select S	Image: Control of the second of the secon

### Related Alerts view in the Endgame Resolver™

Viewing related alerts is useful to see all related activity from a single location, identify attack artifacts, and respond to elements of an attack quickly and easily.

TIP: You can filter the list of alerts in the "Related Alerts" tab by selecting the Filter By dropdown arrow.

# **Alert Enrichments**

Alert Enrichments are a list of unique, related MITRE ATT&CK<sup>™</sup> techniques that provide additional contextual information about an alert. While these actions are not necessarily malicious on their own, enrichments help paint a bigger picture and facilitate the process of scoping a problem and building a response plan. Techniques appear in reverse chronological order, with the most recent events at the bottom. Each technique also contains a link to the associated MITRE page. Select a technique from the list to view the associated event in the Endgame Resolver<sup>™</sup>.





# Endgame Resolver<sup>™</sup> Controls

In the upper-right corner of the Endgame Resolver™ are four buttons that enable you to control the current view:



Their functions are as follows:

Name	Button	Description
Reset View	4 K	Resets the Endgame Resolver™ to its original view.
Expand All		Displays all available data in the Endgame Resolver™, including child process events beyond the default first level that is displayed.



Name	Button	Description
Center	-\$-	Re-centers the Endgame Resolver™ on the process at the end of the timeline.
Zoom	<	Zooms in and out of the Endgame Resolver™. NOTE: Zooming out shows a condensed view of the timeline that does not display the Child Event KPIs or the time elapsed between events.

## Other Options to Control the Endgame Resolver<sup>™</sup> View:

- **Pan:** If data in the Endgame Resolver<sup>™</sup> is hidden from view, select any area in the background and drag your cursor to pan up, down, left, or right until the desired data is visible.
- Expand/Collapse: To expand the width of the Endgame Resolver<sup>™</sup> to a full page and hide the Alert Metadata panel, click the Expand/Collapse button .

Proprietary Elasticsearch B.V. information.



# Retrieve New Timeline Data in the Endgame Resolver™

In the upper-right corner of the Endgame Resolver<sup>™</sup> is a button that displays the current timeline status. If the status button says "Retrieve New Data," you can initiate a task for the sensor to check for updates of new data.

To update the Endgame Resolver<sup>™</sup> with the latest data:

1. Click **Retrieve New Data** in the upper-right corner.

NOTE: As the sensor is checking for updates, the status changes to "Retrieving."

2. If the sensor has retrieved new data, click **View New Data** to refresh the Endgame Resolver<sup>™</sup>. If the data in the timeline is up to date, the status button changes to "Up to Date."



An "Up to Date" status in the Endgame Resolver™ indicates the timeline is displaying the most recent data

# Endgame Resolver<sup>™</sup> Attack Visualization Statuses

The following table describes the statuses you may see in the upper-right corner of the Endgame Resolver™:

Status	Definition
Loading	The user interface is loading data collected from the sensor. This occurs when the Endgame Resolver <sup>™</sup> Attack Visualization is loading for the first time.
Retrieve New Data	Initiates a request to retrieve the latest data from the sensor.
Retrieving	The sensor is currently retrieving the latest Endgame Resolver™ Attack Visualization data.



Status	Definition
View New Data	The sensor has returned the latest data. Click this option to refresh the Endgame Resolver™ Attack Visualization.
Error Retrieving Data	The Endgame Resolver <sup>™</sup> Attack Visualization user interface encountered an error while communicating with the platform. This can be the result of failing services or sensors. You cannot interact with the resolver in this state.
Node Display Limit Exceeded     Download JSON File	Due to a hard-coded limit, the Endgame Resolver™ Attack Visualization is unable to display any more event nodes.
Endpoint Offline	The endpoint is offline.

# **Alert Commenting Overview**

The Alert Details page contains an option to add free-form comments to the current alert. Alert comments are useful to share notes or findings with your team to expedite the alert triage process. All users who have access to the Endgame platform can add alert comments.

# Add an Alert Comment

To add an alert comment:

- 1. Select the **Comments** tab on the Alert Metadata panel.
- 2. In the **Comment** box, type an alert comment. Ensure it is no more than 1,024 characters. Unicode characters are supported.
- 3. Click Add Comment. The new comment appears in the Comments list.

NOTE: There is	s a maximum of 100	comments allowe	d per alert.
----------------	--------------------	-----------------	--------------



	Detected Malicious File Take Action  Endgame MalwareScore® detected the execution of a Malicious File on RND-EP-w-1-01 (172.31.27.11) on Jul 29, 2019 at 12:50:34 PM UTC. It is the security of the security o
ALERT COMMENT CARD Each Comment card displays the username of who added the comment, the date and time it was created, and the Overflow menu.	Super Admin         OVERFLOW MENU           8 days ago         Select the menu to delete the current alert comment.
	Super Admin 8 days ago Malicious File on RND-EP: 7/29/19.
	Super Admin 8 days ago Related Alert: Suspicious MS Office Descendant Process
	Super Admin     ••••       8 days ago     ••••       Related Alert: Suspicious PowerShell Downloads
	Write a comment

Alert Comments list

**NOTE:** Alerts that have been resolved or dismissed automatically get a comment added. The comment displays the name of the user who executed the alert action, the type of alert action that was executed (i.e., whether it was dismissed or resolved), and the date.

Endgame Ma on <u>DESKTOF</u> UTC.	alwareScore® detec -QBBSCUT (10.6.1)	ted the executior 94.68) on Sep 24	n of a <i>Malicious File</i> I, 2019 at 8:00:14 PM
Overview	6 Related Alerts	1 Comments	0 Enrichments
Super Admin 27 minutes ago			
Dismissed by admin			

# **Delete an Alert Comment**

**NOTE:** Level 1, Level 2, and Level 3 users can only delete comments they originally added. Admins can delete all comments. If the alert is dismissed or resolved, the comments are retained in the Archived view.



To delete an alert comment:

- 1. In the Comments list, locate the appropriate alert comment to delete.
- 2. Click the **Overflow** menu , then select **Delete Comment**.
- 3. In the dialog box that says, "Are you sure you want to delete this comment by *user*?" verify that the comment that appears is the correct one to delete, then click **Delete Comment**. A "Comment successfully deleted" confirmation appears.

Delete Comment	
Are you sure you want to delete this comment by Jane Doe?	
File has a MalwareScore of 100 (Malicious).	
Cancel	Delete Comment

4. Click Finish.


# **Respond to an Alert**

If you receive an alert notification, it is recommended you respond accordingly as soon as possible to prevent malicious activity from going unnoticed, thus preventing a possible data breach. Responding to an alert also helps manage the number of alerts that can accumulate. After you have responded to an alert, it is recommended you mark it as resolved. For more information, see "Resolve an Alert" in this chapter.

In general, once you receive an alert notification and analyze the details, you conclude that it:

- a. Requires no response and can be ignored
- b. Is a false positive that should be suppressed in the future
- c. Requires a response

You can respond to an alert from the following places in the Endgame platform:

- The Take Action menu on the Alert Metadata panel
- A pivot action on the Endgame Resolver™ Attack Visualization
- The Action toolbar on the Alerts page (recommended for multiple alerts)

NOTE: Alert response options in the Take Action menu and Endgame Resolver<sup>™</sup> Attack Visualization apply to the current alert only.

The following is a list of Take Action menu items on the Alert Metadata panel that enable you to respond to or execute a specific task for the current alert. Please note the list of options varies by alert type.

Menu Option	Description				
Download Alert	Downloads the raw JSON of the alert details.				
Download Timeline	Jownloads the raw JSON of events that occurred in the Endgame Resolver™ Attack /isualization.				
Resolve	Marks the alert as resolved and moves it to the Archived view. For more information, see "Resolve an Alert." NOTE: Resolved alerts automatically get a comment added to the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date.				
Dismiss	Marks the alert as dismissed and moves it to the Archived view. For more information, see				
	the "Comments" tab on the Alert Details page. The comment displays				



Menu Option	Description
	the name of the user who executed the alert action and the date.
Start Investigation	Starts a new investigation.
Kill Process (Exploit alerts only)	Terminates the source process. NOTE: This option is an available pivot action on the Endgame Resolver™ Attack Visualization.
Suspend Thread (Process Injection alerts only)	Suspends the malicious process thread by thread ID.
Download File (Malicious File alerts only)	Downloads the malicious file.           NOTE: The file must be retrieved from the endpoint before you can download it.
Retrieve File (Malicious File alerts only)	Retrieves the malicious file from the endpoint and sends it to the Endgame platform.          Image: NOTE: If the file was previously retrieved, the Download File option appears instead. However, the Retrieve File option is an available pivot action in the Endgame Resolver™ Attack Visualization.
Delete File (Malicious File alerts only)	Removes the file from the affected endpoint.
Add to Exceptionlist	Displays available attributes to add to the exceptionlist.

**NOTE:** Options in the **Take Action** menu only execute a task for the current alert. However, you can resolve and dismiss multiple alerts from the Alerts page.

Refer to the following scenarios for general guidance on how to respond to an alert:

- As a precautionary measure, it is recommended to always start an investigation when you receive an alert notification.
- If an alert requires no response, select **Dismiss**. This moves the current alert to the Archived view. To dismiss multiple alerts, select each appropriate alert in the Alerts list and click **Dismiss Unactionable Alerts** on the Action toolbar.
- If an alert is a false positive and you want to suppress future alerts from generating, select **Add to Exceptionlist** to add selected attributes to the exceptionlist. For more information, see "Add Threat Alerts to the Exceptionlist."



**NOTE:** When you add an item to the exceptionlist, there is a default selected option on the dialog box to dismiss all alerts that match the exception rule. It is recommended you leave this option selected.

• If an alert requires an immediate action, select the appropriate response from the **Take Action** menu. For example, if you suspect a process is malicious, you can select the **Delete File** option to remove the file from the endpoint, or to respond to an exploit detection, you can select **Kill Process** option to kill the source process.

### Additional Endpoint Responses

The Endgame Resolver<sup>™</sup> Attack Visualization also contains two pivot actions that enable you to either retrieve a file or kill a process when you select a process event node. For more information, see "Endgame Resolver<sup>™</sup> Attack Visualization Overview."

### **Dismiss an Alert**

Dismissing an alert indicates that after analyzing the alert details, the alert does not require further action — for example, if an alert is a false positive or a duplicate. You can dismiss a single alert via the **Take Action** menu on the Alert Metadata panel, or you can dismiss multiple alerts via the Action toolbar on the Alerts page. Once an alert is dismissed, the following automated actions occur:

- Alerts are moved to the Archived view
- A comment is added to the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date

To dismiss multiple alerts simultaneously:

- 1. In the Alerts list, select the box to the left of each alert to dismiss.
- 2. On the Action toolbar, click **Dismiss Unactionable Alerts**.
- 3. In the **Dismiss Alerts** dialog box that appears, select one of the following reasons for the dismissal, then click **Dismiss**.
  - Dismiss Duplicate
  - Dismiss False Positive
  - Dismiss Other
- 4. A "Successfully dismissed alert(s)" confirmation appears.
- 5. Click Finish.





To view all dismissed alerts, on the Alerts page, click the "Archived Alerts" link in the upper-right corner. The dismissal reason you selected appears in the "STATUS" column of the Alerts list.

Alerts	Contract Street						Open Alerta	Ask Artemis	Welcome, Super Jan 24, 2020 5:53 F	PM UTC
	15 All Alers 3 All Advise 3									
0 alerts	$\circ$ currently selected $\checkmark$								1-	15 of 15 < >
	ALERT TYPE	EVENT TYPE	ASSIGNEE	<u>05</u>	IP ADDRESS	HOSTNAME	DATE	s	TATUS	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:57 PM UTC	D	ismissed – False Positive	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:57 PM UTC	D	ismissed – False Positive	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:57 PM UTC	D	ismissed – Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:57 PM UTC	D	ismissed - Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:57 PM UTC	D	ismissed – Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:56 PM UTC	D	ismissed - Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:55 PM UTC	D	ismissed – Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:54 PM UTC	D	ismissed – Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:53 PM UTC	D	ismissed — Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:53 PM UTC	D	ismissed — Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:51 PM UTC	D	ismissed – Other	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:51 PM UTC	D	ismissed – Other	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:51 PM UTC	D	ismissed – Duplicate	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:50 PM UTC	D	ismissed – Other	
	Collection Detection	etw	Unassigned	Windows 10 (v1803)	10.6.36.42	DESKTOP-QBBSCUT	Jan 24, 2020 4:29:49 PM UTC	D	ismissed – Other	
									Last Updated: Jan 24, 2020 5:	.53:12 PM UTC

Archived Alerts view

# **Resolve an Alert**

After you have responded to an alert, it is recommended you mark it as resolved, which moves it to the "Archived Alerts" page. Resolving an alert keeps the Alerts list updated and distinguishes which alerts were handled from those that require a response. The difference between a resolved alert and a dismissed alert is the former indicates a response action (e.g., download file, suspend thread, etc.) was run; the latter indicates a response action was unneeded.

**NOTE:** Although prevention alerts block malicious activity, they still need to be marked as resolved.

To resolve an alert(s):

- 1. In the Alerts list, select the box to the left of each appropriate alert.
- 2. On the Action toolbar, click Resolve Alerts.



- In the Resolve Alerts dialog box that says, "You are about to resolve number Alerts. The alerts will be immediately sent to the Archived view and be set as Resolved..." click Resolve. A "Successfully resolved alert(s)" message appears.
- 4. Click Finish.

i

To resolve a current alert displayed on the Alert Details page, click **Take Action**, then select **Resolve** from the list.

Resolved alerts automatically get a comment added in the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date.

Detected Malicious File			ke Action 🗸 🗸
Endgame M on <u>DESKTO</u> PM UTC.	alwareScore® detec P-QBBSCUT (10.6.2	ted the creation 02.193) on Sep 3	of a <i>Malicious File</i> 30, 2019 at 4:52:51
Dverview	0 Related Alerts	1 Comments	0 Enrichments
Super Ad	min	Comments	Enrichments
7 seconds	ago		

# Assign an Alert

To assign an alert(s) to a specific user to investigate:

- 1. In the Alerts list, select the box to the left of each appropriate alert.
- 2. On the Action toolbar, click **Assign Alerts**. The **ASSIGN A USER** dialog window displays a list of all registered users and their designated usernames.
- 3. Choose one of the following options to locate the appropriate user:
  - In the **Search User Name** text box, begin typing their first or last name. The list filters to name(s) that match the entry. If no matching users are found, an **INVALID USER** error message appears.
  - Scroll the list and locate the user's name.
- 4. Select the option button to the left of the appropriate user's name.
- 5. Click **CONFIRM USER**. In the Alerts List, the assignee's name appears in the **ASSIGNEE** column.



ASSIGN A USER Find a user to assign to an investigation.					
Selecting a User					
Search the list below to find the User you v	want to assign to this particular investigation.				
Q super					
NAME	USER NAME				
Super Admin	admin				
CANCEL CONFIRM USER					
		5			

Assign an alert to a user

TIP: To assign a single alert to a user or to change the current assignee, either click the link in the **Assignee** column, or on the Alert Metadata panel, click the link in the **Assigned To** field.

# **Archived Alerts Page Overview**

The Archived Alerts page is an enumeration of all alerts that have been resolved or dismissed, and their relevant details, organized in a table. It also contains an option on the Action toolbar to unarchive selected alerts.

**NOTE:** If you selected a reason for an alert's dismissal, it appears in the "Status" column.

To display the Archived Alerts page, click the "Archived Alerts" link in the upper-right corner of the Alerts page.



Alerts	Alerts: Archived OpenAlerts @ Ask Artemis @ Ask Artemis @ Welcome, Super Oct 29, 2019 6:39 PM UTC Oct 29, 2019 6:39 PM UTC							
15 At Alerts A								
0 alerts	currently selected $\checkmark$							1 - <u>15</u> of 15 < >
	ALERT TYPE Maliaiana Eila	EVENT TYPE	ASSIGNEE	<u>05</u>	IP ADDRESS	HOSTNAME	DATE	STATUS
	Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:26:26 PM UTC	Dismissed
	Defense Evasion Detection	Windows File Masquerading	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:26:19 PM UTC	Dismissed
	Ransomware Detection	Encrypt File	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:25:14 PM UTC	Dismissed - Other
	Ransomware Detection	Encrypt File	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:25:11 PM UTC	Dismissed
	Process Injection Detection	Shellcode Injection	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:25:07 PM UTC	Dismissed - Duplicate
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:55 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:54 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:54 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:54 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:54 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:54 PM UTC	Dismissed
	Process Injection Detection	Process Memory Manipulation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:49 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:46 PM UTC	Dismissed
	Malicious File Detection	Creation	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:36 PM UTC	Dismissed
	Malicious File Detection	Execution	Unassigned	Windows 10 (v1803)	10.6.66.125	DESKTOP-QBBSCUT	Oct 29, 2019 5:24:36 PM UTC	Dismissed
								Last Updated: Oct 29, 2019 6:27:56 PM UTC



# **Unarchive an Alert**

If you mistakenly dismissed or resolved an alert, you can unarchive it, which moves it back to the default view on the Alerts page.

To unarchive an alert(s):

- 1. In the Alerts list, select the box to the left of each appropriate alert to unarchive.
- 2. On the Action toolbar, click Unarchive Alerts.
- In the dialog box that says, "You are about to unarchive number Alerts. The alerts will be immediately removed from the Archived view and be sent to the Current view..." click Unarchive. A "Successfully unarchived alert(s)" message appears.



4. Click Finish.

# CHAPTER 5

# ARTEMIS

rtemis Search Overview	146
About Artemis Queries	148
Execute a Search in Artemis	154
View Artemis Search Results	156
Find Additional Endpoint Occurrences Using Artemis Shortcuts	167
Configure Third-Party Applications to Connect to Endgame	172
Event Query Language (EQL) Overview	173
Artemis Queries List Overview	198
Archive an Artemis Query	200
Verify that Logon Events are Enabled in Windows (Optional)	202



# **Artemis Search Overview**

After a sensor is deployed to a Windows, Linux, or macOS endpoint, it enables collection of various events as they occur and stores the data on the endpoint. You can then search for this historical data using Artemis, Endgame's intelligent assistant that executes a precision query based on your input. You can also use Artemis to search for current endpoint data.

Endgame's sensor stores a maximum of 500 MB of event data. The time frame of how far back you can search for event data depends on how much activity occurs on the endpoint. Once the sensor has reached the maximum amount of data, the oldest data is deleted.

**NOTE:** In order for Windows to store user logon events, the "Audit account logon events" setting in Windows Local Security Policy must be configured. For more information, see "<u>Verify that Logon Events are Enabled in Windows</u>."

### **Artemis User Interface**

Artemis' interface is a narrow chat window that enables you to have an interactive conversation. Once you type the search criteria in the text box, it either asks for more details so it can formulate a precise query, or it asks you to confirm the search. The natural, conversational language enables you to find targeted event data without having to construct a query language-based search.





CHAPTER 5 | User's Guide

Artemis user interface



# **About Artemis Queries**

An Artemis query is a formulated search that enables you to search for event data. The following table describes the specific event data you can search once a sensor has been deployed and event collection is enabled.

**NOTE:** Ensure the specific events you want to collect are enabled on each operating system. Event collection is configured in an Endpoint Policy. For more information, see "Create and Configure an Endpoint Policy" in the *Administrator's Guide*.

Event Type	Data You Can Search	Supported OS
Process	A process name, hash, or process ID.	• Windows
		• Linux
		• Mac
Process lineage	A historical timeline of when and how a process was created.	• Windows
		• Linux
		• Mac
Network	IP, port, and the amount of data transmitted or received in a	• Windows
	network connection.	• Linux
		• Mac
File	A specific filename.	• Windows
		• Linux
		• Mac
Domain Name System (DNS)	The domain name of the corresponding endpoint.	• Windows
information		
Security	Dates and times of when a user logged on or off an endpoint.	• Windows

A query requires a specified search intent and value to execute successfully. Unless specified, with the exception of process lineage search — which requires an IP address — Artemis searches all active endpoints by default. Keep this in mind if you need to search endpoints running on a specific operating system.

The following example is a valid query because it specifies the process name:



### search for process calc.exe on all Windows endpoints

To search more than one value for a given entity — which is supported only for active endpoint searches — separate each value with a semi-colon:

```
search for processes calc.exe; lsass.exe
```



# **Sample Artemis Queries**

The following table lists examples of full-text queries that meet the requirements to execute a successful search in Artemis. Refer to this table for guidance when constructing a query. Also keep the following in mind:

- When searching for a file or process with no extension, include "process" or "file" before the process name.
- When searching for port, include "port" in front of the port number.
- When searching for anything by user, include "user" before the username.

For a complete list of sample queries, visit Endgame's Knowledge Base, which you can access by clicking V on the Top Navigation toolbar.

**NOTE:** Do not include the surrounding quotation marks in your query. They are solely meant to indicate the start and end of the phrase.

Search Intent	Sample Query Text				
	Process				
A specific process by name or hash	"Show me process.exe on all Windows endpoints" "Show me process.exe on all Linux endpoints" "Find process.exe on inactive endpoints" "Search process for file process.exe on active endpoints" "Search for process hash ABC1234567890 on IP 10.1.2.34"				
The lineage of a specific process	<ul> <li>NOTE: Ensure you specify an IP address in the query and precede it with "endpoint."</li> <li>"Show me the process lineage for badguy.exe on endpoint 10.1.2.34"</li> <li>"Search the process lineage for notepad.exe on endpoint 10.1.2.34"</li> <li>"Give me the process lineage for badguy.exe on endpoint 10.1.2.34"</li> <li>"Give me the process lineage for PID 123 on endpoint 10.1.2.34"</li> <li>"Show me resolver for process winword.exe and PID 2956 on hostname endpoint-1-2-03"</li> </ul>				
Network					



Search Intent	Sample Query Text
Endpoints that	"Search for any endpoint that communicated to IP 10.1.2.34"
communicated to a specific IP	"Show me any endpoint that communicated to IP 10.1.2.34"
Endpoints	"Did any Windows 10 endpoints communicate to IP 10.1.2.34"
running on a specific operating system that communicated	"Have Windows 7 endpoints communicated with 10.1.2.34"
Endpoints	"Search network data for endpoints sending more than 100MB"
sending more	"Search network communications for endpoints sending more than 100MB"
than a specific	
amount of data	<b>NOTE:</b> Ensure there is no space between the data size and unit.
Endpoints	"Search network data for process.exe sending more than 100MB"
running a	"Search network communications for process.exe sending more than 100MB"
process	
sending more	
than a specific amount of data	
Endpoints	"Search network data for endpoints sending less than 100MB"
sending less	"Search network communications for endpoints sending less than 100MB"
amount of data	
Endpoints that	"Search for any endpoints that communicated on port 123"
communicated	
port	
	User
Any endpoints a	"Search for user johndoe"
specific user	"Search logins for user johndoe"



Search Intent	Sample Query Text
logged on to	
If a user logged on to an endpoint running on a specific operating system	"Has johndoe logged on to any Windows 7 endpoints"
All processes launched by a specific user	"Search processes created by user johndoe"
	DNS
All endpoints that communicated with a specific	"Search for any endpoint that communicated with www.domain.com" "Search for www.domain.com" "Search DNS data for www.domain.com"
uomain	



### Search by Hostname or Endpoint Group

Including a hostname or group in an Artemis query is useful to narrow search results by a specific endpoint value. Refer to the examples below for guidance on how to format these queries.

To Search by	Include in the Artemis Query	Sample Query Text
Hostname	The hostname.	"Search for process.exe on hostname endpoint-hostname"
Group	The name of the assigned group(s). If the groups include spaces or semicolons, surround them with quotation marks. Separate multiple values with a semicolon.	NOTE: If a group contains a space or semi- colon, separate it with quotation marks. "Search for process.exe on endpoints with groups ABC; XYZ" "Search for process hi.exe on group ABC"



# **Execute a Search in Artemis**

The following example describes how to execute a search in Artemis.

**Scenario:** You want a historical account of every time process "badguy.exe" was run on all endpoints within your network — even on the endpoints that are inactive or were deleted.

- 1. On the Top Navigation toolbar, click
- O Ask Artemis
- 2. In the Response box at the bottom of the chat window, type **search for badguy.exe** and press **Enter**.

TIP: When you launch Artemis, the interface automatically displays the last 10 executed search queries. Place your cursor in the Response box and press the up arrow to populate the most recent response in Artemis. Press the up arrow again to see previous recent responses.

3. Artemis asks you to confirm the query. If it is correct, type **yes** and press **Enter**. If it is incorrect, type **no** or **cancel** and type a new query.

Ask Artemis Ask Artemis Oct 25, 2019 8:25 PM UTC
Artemis
Hello, I am Artemis, your intelligent assistant. What can I help you with?
Type "help" to see what I can do.
Super Admin
search for badguy.exe
Artemis
Are you sure you want to run:
Search for process badguy.exe on active endpoints?
Super Admin
yes
Artemis
Created investigation: 1fd65608-2cad-4fff-9044-7b3b0ae74bc3
View the Investigation
Oct 25, 2019 8:26:09 PM UTC
Artemis
Hello, I am Artemis, your intelligent assistant. What can I help you with?
Type "help" to see what I can do.
Ask for help

Sample process data search in Artemis



4. Artemis confirms the search has begun. To view results, click "View Search Results."

(i) Each e	executed active	endpoint query ap	pears in the	Activity Timelin	e as an "Artemis - Event
Searc	h" entry.				
Activi	ity Timeline I Activity Feed	Filter By: All	✓ 🔳		
Oct 6:51:2	19, 2017 IS PM UTC	n <mark>is - Event Search</mark> arch			

# **Artemis Search Optimization Tips**

When constructing a search query, keep the following tips in mind:

- 1. For guidance on how to construct a query, see "About Artemis Queries."
- 2. Use correct spelling. While Artemis tries to recognize misspellings, it can return an error.
- 3. Ensure the query specifies what you are searching for and the value (e.g., process lineage must have a process name or process ID). Omitting information can return an error.
- 4. When specifying the search intent and entity value, ensure you type the correct IP address, process name, etc.
- 5. If you are stuck at any time and want to start over, type **cancel** in the chat window, or click the **Reset u** button, then click **RESET QUERY**.



# **View Artemis Search Results**

After you execute a search in Artemis, it extracts the requested event data from the endpoint log file and displays the results on the Investigation Details page.

To view search results, choose one of the following options:

- After you type "yes" in the Artemis chat window to launch the search, click the link that says "Click here to view the Investigation."
- On the Investigation Dashboard, select the **Queries** tab on the Action toolbar, then click the appropriate query in the Investigations list.

Invest	igation Dashboard				🕐 😨 Ask A	rtemis Apr 1, 2019 12:32 AM UTC (EDT+4)
	163 Terretti Accive Accive How to Start an Investigations Investigation Investigation Start an Oracle 9 Oracle 9 View 9					O
	41 122 163 Iunts Queries Total ֎ ● ֎					0
0 invest	gations currently selected 🌱					1 - <u>50</u> of 122 < >
	INVESTIGATION NAME	ASSIGNEE	INVESTIGATION BREAKDOW	/N	ENDPOINTS	DATE CREATED
	Resolver 2019-03-31T21:00:03.847734	Demo0 User	100%	1 Query total	1	Mar 31, 2019 9:00:03 PM UTC
	Resolver 2019-03-31T18:53:22.196629	Super Admin	100%	1 Query total	1	Mar 31, 2019 6:53:22 PM UTC
	Resolver 2019-03-31T18:47:40.973772	Super Admin	0%	1 Query total	1	Mar 31, 2019 6:47:41 PM UTC
	Resolver 2019-03-31T18:28:35.834402	Demo0 User	0%	1 Query total	1	Mar 31, 2019 6:28:35 PM UTC
	Resolver 2019-03-30T23:52:49.266907	Super Admin	100%	1 Query total	1	Mar 30, 2019 11:52:49 PM UTC
	Resolver 2019-03-29T21:07:41.319806	Super Admin	100%	1 Query total	1	Mar 29, 2019 9:07:41 PM UTC
	Resolver 2019-03-29T20:59:50.972339	Super Admin	100%	1 Query total	1	Mar 29, 2019 8:59:51 PM UTC
	Resolver 2019-03-29T20:58:32.658124	Super Admin	100%	1 Query total	1	Mar 29, 2019 8:58:32 PM UTC
	Process Search 2019-03-29T20:52:04.893472	Super Admin	100%	1 Query total	1	Mar 29, 2019 8:52:04 PM UTC
	Resolver 2019-03-29T20:44:36.012402	Braden Preston	0%	1 Query total	1	Mar 29, 2019 8:44:36 PM UTC
	Process Search 2019-03-29T20:43:06.633735	Super Admin	100%	1 Query total	1	Mar 29, 2019 8:43:06 PM UTC
	Process Search 2019-03-29T20:41:11.396199	Braden Preston	100%	1 Query total	1	Mar 29, 2019 8:41:11 PM UTC
	Process Search 2019-03-29T20:38:31.241624	Braden Preston	100%	1 Query total	1	Mar 29, 2019 8:38:31 PM UTC
	EQL Query Search 2019-03-29T17:42:46.944702	Demo0 User	100%	1 Query total	14	Mar 29, 2019 5:42:46 PM UTC
	File Search 2019-03-29T17:37:56.196642	Demo0 User	100%	1 Query total	14	Mar 29, 2019 5:37:56 PM UTC
	File Search 2019-03-29T17:10:03.187999	Demo0 User	100%	1.Query total	14	Mar 29, 2019 5:10:03 PM UTC

Artemis Queries list on the Investigation Dashboard



TIP: You can also go directly to the search results page from the Artemis chat window. After you type "**yes**" in the Artemis chat window to launch the search, click the response link that says "View the Investigation."

# **Artemis Search Results Overview**

Search results for active endpoint searches appear on the Investigation Details page, which displays details of the selected Artemis query and provides options to edit the name and archive the query. Search results are listed in a tabular format and appear in chronological order with the first endpoint occurrence at the top.

The results page contains four sections:

- 1. Artemis Query Overview
- 2. Endpoint Breakdown
- 3. Individual search results
- 4. Filter events



### Artemis query search results

The top of the Artemis Investigation Details page displays the following data about the query:



Data	Description
Total Hits	The total number of search results.
Endpoints with Hits	The total number of events that occurred on unique endpoints.           Image: NOTE: It is possible to see a different number of "Total Hits" and "Endpoints with Hits." The former displays the total number of occurrences, even if it occurred on the same endpoint.
First Seen Last Seen	The date and time the event occurred first on the endpoint within the specified time frame. The date and time the event occurred last on the endpoint within the specified time frame.

**NOTE:** The search results page shows a maximum of 500 results per endpoint and a maximum of 1,000 results overall. If the maximum is reached, a warning that says, "Max *number* returned overall. For more results, try using the Endgame API directly or download from the CSV link below."

### **Artemis Query Overview**

The Artemis Query Overview section displays general information about the query, including the name, assignee (the user who ran the search), query type, and date it was created. In addition, you can view the details of the query, which is useful if you want to rerun the search at a later time or see if the query syntax is accurate. The Overview section also provides options to edit the name or archive the query.





Artemis Query Overview section

**NOTE:** The default name of each query is formatted as **Query Type YYYY-MM-DD:HH:MM:SS:MMSS** (e.g., File Search 2019-01-10T18:40:28.251406). You can edit this name to something unique by clicking the pencil button.

### Endpoint Breakdown

The Endpoint Breakdown summarizes the status of the Artemis query and includes a progress bar that displays the percentage completion and the number of endpoints out of the total included that have returned data.



Query Search 2019-06- 18:01:29.781356           ned To           er Admin           Created           18, 2019 6:01:29 PM UTC           Type           Fib. col	Endpoint Breakdown ① Artemis - Event Search
ned To ter Admin Created 18, 2019 6:01:29 PM UTC Type O	Endpoint Breakdown 🕧 Artemis - Event Search
Created 18, 2019 6:01:29 PM UTC	Endpoint Breakdown 🛞 Artemis - Event Search
Created	Endpoint Breakdown 🛞 Artemis - Event Search
18, 2019 6:01:29 PM UTC	Endpoint Breakdown 🛞 Artemis - Event Search
Type	Artemis - Event Search
rah ad	
Ich_eqi	<b>100%</b> 646/ <b>646</b>
Details	
. Search: process where true active endpoints	
pint Breakdown 🚯	
nis - Event Search	
<b>0%</b> 646/ <b>646</b>	



### **Individual Search Results**

Search results are displayed in a tabular format and appear in chronological order. A search result card displays comprehensive event details about each endpoint occurrence that was found, based on the requested data in Artemis. For example, if you asked Artemis to find each time an Isass.exe process was run on a group of 16 endpoints and that process was found on all 16, the Investigation Details page displays 16 results.

NOTE: The page displays a maximum of 1,000 results.

In addition to all-inclusive details, each result card contains the following columns that provide the following data:

Column Name	Description
Time	The date and time the event occurred.
Event Type	The type of event that occurred (e.g., process, network, DNS, etc.)
Event Subtype	A description of the specific event action (e.g., process created, process terminated, etc.)
Endpoint Name	The hostname on which the event occurred.



Column Name	Description
	TIP: The endpoint hostname is an active link that goes to the Endpoint Details page.
IP Address	The IP address on which the event occurred.

	<b>Inve</b> s Deta	Total number of result stigation 136 IIS Total Hits	Date and Date and 1/2 Endpoints with Hits	time of first and last en	dpoint occurrence F 17 AM UTC Filter By All	ilter by event type		
Filter events	Search	Events  EQL Search	Plain Text Search					Download all results to a CSV file
Collapse/Expand all results	• •	Time		Event Type	Event Subtype	Endpoint Name	Platform	IP Address
Collapse/Expand individual result	• ^	Sep 2, 2019 5:32:50 AM UTC		Process	Process Terminated	DESKTOP-QBBSCUT	Windows	10.6.191.161
		Process Name sw Path C: User SY Process ID 57	chost.exe Windows∖System32\svchost.e STEM 72	Domai xe MDS Parent	n NT AUTHORITY 32569e403279b3fd2edb7eb Process ID 612	1036273fa		
	1			Process details				

### A search result from a Windows process query

☆ TIP: For applicable network data queries, you can view HTTP request data in the search results, which is useful to detect and remediate incidents. ~ Time Event Type Event Subtype Endpoint Name IP Address May 17, 2019 3:48:15 PM GMT+1 HTTP Request WIN-00V4R7RVH9S 192.168.161.205 Network ~ 172.217.7.206:80 Process Name firefox.exe Destination HTTP Request GET / HTTP/1.1 Host: 172.217.7.206 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; ... Path C:\Program Files (x86)\Mozilla Firefox\firefox.exe User endgame Process ID 3372 192.168.161.205:57965 Source Protocol tcp



TIP: Copy the path or process name by clicking inside the field. It copies the text to the clipboard, which you can then paste into a new Artemis search or other application.

### **Expand and Collapse Results**

By default, each result is expanded to display event details. However, you can collapse the comprehensive list of results to a consolidated list that only includes each event type, event subtype, endpoint name, and IP address by clicking the

**Collapse** arrow **to** the left of the "Time" column heading. Click the **Expand** arrow **to** return to the expanded state. You can also collapse and expand individual results.

					Download All to CSV
•	Time	Event Type	Event Subtype	Endpoint Name	IP Address
~	Feb 1, 2018 10:51:23 AM UTC	Process	Process Created	HD-xgx-8a3ac0db	10.236.35.82
*	Feb 1, 2018 10:51:01 AM UTC	Process	Process Created	HD-xgx-8a3ac0db	10.236.35.82
~	Feb 1, 2018 10:36:56 AM UTC	DNS	DNS Lookup	HD-7na-5b5556c8	10.233.248.62
~	Dec 12, 2017 6:23:28 PM UTC	Process	Process Terminated	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:28 PM UTC	Process	Process Exec	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:28 PM UTC	Process	Process Fork	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:19 PM UTC	Process	Process Terminated	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:19 PM UTC	Process	Process Terminated	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:19 PM UTC	Process	Process Terminated	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:19 PM UTC	Process	Process Exec	HD-ggr-790b6fd2	10.72.202.89
*	Dec 12, 2017 6:23:19 PM UTC	Process	Process Fork	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:19 PM UTC	Process	Process Terminated	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:13 PM UTC	Procesa	Process Running	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:13 PM UTC	Procesa	Process Running	HD-ggr-790b6fd2	10.72.202.89
~	Dec 12, 2017 6:23:11 PM UTC	Process	Process Running	HD-ggr-790b6fd2	10.72.202.89
*	Dec 4, 2017 4:47:01 PM UTC	Process	Process Running	HD-ggr-790b6fd2	10.72.202.89
~	Dec 4, 2017 4:47:01 PM UTC	Process	Process Running	HD-ggr-790b6fd2	10.72.202.89
~	Dec 4, 2017 4:46:56 PM UTC	Process	Process Running	HD-ggr-790b6fd2	10.72.202.89



### **Process Lineage Search Results Overview**

Search results for a process lineage appear as a visual timeline of events, known as the Endgame Resolver<sup>™</sup> Attack Visualization. This view provides a more concise and efficient method to analyze which process events occurred and in what order, as opposed to the standard "result card" view. The Endgame Resolver<sup>™</sup> also displays child processes and other events (e.g., DNS, registry, network, etc.) that spawned from the parent process, related alerts, and provides options to take action on a selected process. For complete details about the Endgame Resolver<sup>™</sup>, see "<u>Alert Details Page Overview</u>."





Process lineage search results appear in the Endgame Resolver™ view

When viewing Artemis results, you can filter the data by event type, search string, or EQL Search. Filtering data is useful to find targeted data, especially if there are several results.

### Filter By Event Type

By default, the search results display all endpoint occurrences; however, you can filter by one or more event types by selecting the **Filter By** drop-down and selecting the appropriate event type(s). Once you apply a filter, the number of total hits and endpoints with hits updates to display the filtered data. Each event type is color-coded for distinction.

Filter By	All	^	
	Process	340	
	Network	0	
	DNS	0	
	Security	0	
	Files	0	
	Registry	0	
	Image Load	0	
	PowerShell	0	
g	CLR	0	
122705264	WMI	0	
132190310	API	0	

Filter by event type



### Filter by EQL (Endgame Query Language) Search

As an alternative to filtering results by event type, you can also filter Artemis results by specific EQL. Using this method of filtering leverages the full capabilities of EQL, which provides the ability to do such as the following:

- Use Boolean operators, such as **and**, **or**, **not** (**NOTE:** Boolean operators are case sensitive and must be lowercase in EQL searches)
- Use a wildcard (\*) in the search for field values
- Search for a partial match



To filter results by EQL:

- 1. In the Search Events section, select the **EQL Search** option.
- 2. In the search bar, enter an EQL query. The EQL validator validates the query as you type. If the EQL is incorrect, a validation error with a suggested fix appears beneath the query.
- 3. When the "Validated & Ready to Submit" confirmation appears, the EQL query is correct. Click **Search** or press **Enter** on your keyboard. The number of matching events out of the total displays beneath the search bar.

1. process_name == "svcho	st.exe"						
Validated & Ready to S	ubmit						
Search Clear							
Query Overview Archive Investigation Name	Investigation 500 Details Total Hits	1/2 Fi Endpoints with Hits Li	irst Seen Aug 29, 2019 <b>12:21</b> ast Seen Aug 29, 2019 <b>3:42</b> :6	:45 AM UTC Filter By All	×		
File Search 2019-08- 29T15:42:46.466499	Search Events   EQL Search	Plain Text Search					
Assigned To	1. process_name == "svchost.exe"						
Super Admin	Validated & Ready to Submit						
Date Created	Search Clear			338/500 matching events displayed from	EQL filter.		Download All to 0
Aug 29, 2019 3:42:46 PM UTC							
uery Type 🛛 🔨 Time		Event Type	Event Subtype	Endpoint Name	Platform	IP Address	
Search Process		лс	Process	Process Created	DESKTOP-QBBSCUT	Windows	10.6.240.120
Coarry Details Search for process * see on active endpoints Path C:\Windows/System32(sychost.exe User SYSTEM			MD5 22569e4032279c342eeb7eb0036273fs Parent Process ID 620 Command Line				
Endpoint Breakdown	Process ID Domain	6272 NT AUTHORITY	C:\WIND	JWS\System32\avchost.exe -k waappx -p -a ClipS	vc		
100%	Aug 29, 2019 3:42:06 PM 0	лс	Process	Process Created	DESKTOP-QBBSCUT	Windows	10.6.240.120
	Process Name Path User Process ID Domain	svchost.exe C:Windows\System32\svchost.exe SYSTEM 9712 NT AUTHORITY	MD5 Parent P Comman C\WIND	32569e403279b3Hd2edb7ebd0 rocess ID 620 d Line W9Suystem32\svchost.exe -k netavca -p -a wildar	ve		
	Aug 29, 2019 3:40:31 PM 0	лс	Process	Process Terminated	DESKTOP-QBBSCUT	Windows	10.6.240.120
	Process Name Path	svchost.exe C:\Windows\System32\svchost.exe	Domain MD5	NT AUTHORITY 32569e403279b3fd2edb7ebd0	136273fa		

Filter results by EQL

Filter by Search String



Filtering by a search string is useful if you want to look for basic, simple words within the list of search results. Before you filter events by a text string, keep the following tips in mind:

- Results are returned from prefix search strings only or the beginning of a word. For example, if you are searching for process.exe and you type pro in the search bar, any events that contain "process.exe" appear as matches. However, if you type a suffix, such as cess, "process.exe" events do not appear as matches.
- A string is defined as phrases that are split on the following characters: / \ \_ and . If the results do not show events you expect to be listed, try removing the aforementioned characters from your search string.

To filter results by a search string:

- 1. In the Search Events section, select the Plain Text search option.
- 2. In the search bar, enter the search string by which to filter. Click **Search** or press **Enter** on your keyboard. The list of results filters to display matching events, which are highlighted. The number of matching events out of the total is displayed beneath the search bar.

Query Overview Archive Investigation Name	Investigation 136 Details Total H	1/2 ts Endpoints with Hits	First Seen Sep 2, 2019 <b>4:5</b> Last Seen Sep 2 2019 <b>5:3</b> ter events search bar	7:17 AM UTC 2:50 AM UTC	Filter By All	¥		
02T05:34:34.342112	Search Events O EQL Search	Plain Text Search	er evenes search bar					
Assigned To	Q sychost							
Super Admin			The number of matchin	a overte				
Date Created	Search Clear		out of the total		80/136 matching events displa	iyed.		Download All to Cf
Sep 2, 2019 5:34:34 AM UTC								
Query Type 🛛 🕥	∧ Time		Event Type	Event Subtype		Endpoint Name	Platform	IP Address
Search Process	Sep 2, 2019 5:32:50 AM	Highlighted hits	Process	Process Termin	nated	DESKTOP-OBBSCUT	Windows	10.6 191.161
Query Details								
Search for process *.exe on active endpoints	Process Name Path User	svchost.exe C:\Windows\System32\svcho SYSTEM	Dom it.exe MD5 Pare	in nt Process ID	NT AUTHORITY 32569e403279b3fd2edb7eb 612	d036273fa		
Endpoint Breakdown 🛞	Process ID	5772						
Artemis - Event Search	A Sep 2, 2019 5:31:42 AM	UTC	Process	Process Termin	nated	DESKTOP-QBBSCUT	Windows	10.6.191.161
	Process Name	svchost.exe	Dom	in	NT AUTHORITY			
	Path	C:\Windows\System32\svchor	t.exe MD5	xe MDS 32569e403279b3fd2edb7ebd036273fa				
	User	SYSTEM	Pare	nt Process ID	612			
	Process ID	4792						
	A Sep 2, 2019 5:25:52 AM	итс	Process	Process Termin	nated	DESKTOP-QBBSCUT	Windows	10.6.191.161
	Process Name	svchost.exe	Dom	ain	NT AUTHORITY			
	Path	C:\Windows\System32\svcho	t.exe MD5		32569e403279b3fd2edb7eb	d036273fa		
	User	SYSTEM	Pare	nt Process ID	612			
	Process ID	4228						

Filter Artemis events by search string

# **Download Artemis Results**

You can download the current search results from Artemis to a comma-separated values (CSV) file by doing the following:

1. In the upper-right corner of the search results page, directly beneath the search bar, click **Download All to CSV**.



<b>In</b> De	<b>restigation</b> tails	500 1/2 Total Hits Endpoints with Hits	First Seen Oct 27, 2019 5:56: Last Seen Oct 28, 2019 5:04:	91 PM UTC 5 PM UTC	Filter By All	v				
Sea 1.	Search Events  EQL Search  Plan Test Search  Download All to CSV									
-	Time		Event Type	Event Type Event Subtype		Endpoint Name	Platform	IP Address		
	Oct 27, 2019 5:56:01 PM UTC		Process	Process T	erminated	DESKTOP-QBBSCUT	Windows	10.6.66.125		
	Process Name suchost.exe Path C:\\lindows\System32\suchost.exe User SYSTEM Process ID 5924		Domain MD5 Parent Process	Domain         NT AUTHORTY           MD5         32569e403279b3H62xeb7ebd336273fe           Parent Process ID         608						
	Oct 27, 2019 5:5	7:04 PM UTC	Process	Process T	erminated	DESKTOP-QBBSCUT	Windows	10.6.66.125		
	Process Name Path User Process ID	svchost.exe C:\Windows\System32\svchost.exe SYSTEM 1948	Domain MD5 Parent Process	NT 32: ID 601	AUTHORITY 569e403279b3fd2edb7ebd036273fa 3					

2. When the download is complete, open or save the file from your browser.





# **Find Additional Endpoint Occurrences Using Artemis Shortcuts**

When you view an alert's details, the Alert Metadata panel displays correlated endpoint data, such as a the process name, SHA1 hash, MD5 hash, or path. Artemis contains pivot actions and shortcuts that enable you to quickly search for those same values that may exist on other endpoints. These features are useful to determine if similar malicious activity has occurred elsewhere within your environment without needing to manually enter specific search criteria. As such, this can also expedite alert remediation.

### **Execute a Recommended Artemis Query**

If you are viewing details of a specific alert, you can launch Artemis to view recommended queries for guidance on what other data to search. A preceding message appears to inform you it recognizes which alert you are viewing.

Recommended queries appear in Artemis when the following alerts are displayed:

- Credential Dumping
- Credential Manipulation
- Malicious File
- Permission Theft
- Process Injection
- Ransomware



### Recommended queries for a Credential Dumping alert

When you execute a recommended query — which is contextual according to the alert type — Artemis extracts the endpoint data from the current alert.

To execute a recommended Artemis query:

- 1. View an alert that provides recommended queries (see list above).
- 2. On the Top Navigation toolbar, click
- Ask Artemis

. The recommended queries appear in the chat window.

- 3. Click the appropriate query, which then populates in the response text box.
- 4. If the query is correct, press Enter. If it is not, you can modify the query as appropriate.
- 5. When Artemis asks you to confirm the search query, type **yes** in the text box and press **Enter**.
- 6. Click **View the Investigation** to view results on the Investigation Details page.



Г

Ask Artemi	is Welcome, Super Jun 3, 2019 7:41 PM UTC	1
Artemis		
Hello, I am Ar I help you wit	rtemis, your intelligent assistant. What can h?	
Type "help" to	o see what I can do.	
l see you are some sugges	looking at a Malicious File alert, here are sted queries I can run:	
• <u>Search</u>	<u>t for this file name on all endpoints</u>	
Ask for help		
	Super Admin	
	Search for this file name on all endpoints	
rtemis		
Are you sure y	you want to run:	
Search for pro	ocess 1.exe on active endpoints?	
Ask for help		
	Super Admi	n
	yes	
Artemis		
Artemis Created inves 2834146d-c2a	itigation: a3-4a20-9730-b301474e7bcf	
Artemis Created inves 2834146d-c2a View	stigation: a3-4a20-9730-b301474e7bcf w <b>the Investigation</b>	
Artemis Created inves 2834146d-c2a View Jun 3	stigation: a3-4a20-9730-b301474e7bcf w the Investigation ), 2019 7:41:30 PM UTC	

An executed recommended query for a Malicious File alert



### Search Current Alert Metadata on Other Endpoints

When an alert's details are displayed, you can also use Artemis to search for specific values in the current metadata that may exist on other endpoints by typing "this" in the query followed by the search intent. For example, if you are viewing a Malicious File alert, you can type "search this md5" to determine if the current MD5 hash exists on other endpoints. This eliminates the need to manually type or copy or paste this metadata in the response text box.

lert Details		Ask Artemis Apr 12, 2019 8:58 PM UTC (EDT+4)
etected Maliciou	us File Take Action 💙	Artemis
ndgame MalwareSo n <u>DESKTOP-OBBSC</u>	core® detected the creation of a <b>Malicious File</b> 2UT (10.6.176.206) on Apr 12, 2019 at 8:38:00	Hello, I am Artemis, your intelligent assistant. What can I help you with?
verview Rel		Type "help" to see what I can do.
Severity	High	Super Admin
Date Created	Apr 12, 2019 8:38:00 PM UTC	search uns mos
MalwareScore®	99.99	Artemis
File Name	mimikatz_write.exe	Are you sure you want to run:
	View File Details	Search process for md5 8425d9cb947435285cce1b14ad04f4cd on active
File Status		endpoints?
File Type	Executable	Super Admin
Malware Analys	is 🗸	yes
Endpoint	*	Created investigation:
Hash	^	debee29d-f4f7-4ad5-82f6-2200a78de81a
MD5	8425d9cb947435285cce1b14ad04f4cd	View the Investigation
SHA1	233d7555806b1abfa0a3a57afe3e355ca 06e64e3	Apr 12, 2019 8:49:43 PM UTC
SHA256	80b16acf372c70365fd201059959f179c	Artemis
	369de642fcfae8f4fe3dffcf703931f	Hello, I am Artemis, your intelligent assistant. What can I help you with?
File Malicious	•	Type "help" to see what I can do.
Source Process	*	Suner Admin

This feature also enables you to search for event data that occurred solely on the current endpoint by specifying the search intent followed by "this endpoint" in the query (e.g., "search process lsass.exe on this endpoint").



A sample file search on the current endpoint using the "this" parameter

The specific metadata you can search on other endpoints using the "this" parameter varies by alert type, as illustrated in the following table:



	Credential Dumping	Credential Manipulation	Exploit	Permission Theft	Ransomware	Process Injection	Malicious File
Endpoint	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	✓
PID	X	$\checkmark$	$\checkmark$	X	$\checkmark$	X	Х
Source PID	$\checkmark$	X	X	$\checkmark$	X	$\checkmark$	X
Target PID	✓	X	X	✓	X	✓	X
Process	Х	$\checkmark$	$\checkmark$	Х	$\checkmark$	X	$\checkmark$
Source Process	$\checkmark$	X	X	$\checkmark$	X	$\checkmark$	X
Target Process	✓	X	$\checkmark$	$\checkmark$	X	✓	X
Path	X	$\checkmark$	$\checkmark$	Х	$\checkmark$	X	✓
Source Path	$\checkmark$	X	X	✓	X	$\checkmark$	X
Target Path	✓	X	$\checkmark$	$\checkmark$	X	✓	X
SHA256	Х	X	X	Х	$\checkmark$	Х	✓
MD5	Х	X	Х	X	$\checkmark$	Х	$\checkmark$
SHA1	Х	X	Х	Х	$\checkmark$	Х	$\checkmark$



### Sample Queries Using the "this" Parameter

The following table lists examples of metadata can you search on other endpoints using the "this" parameter in Artemis. Refer to the preceding table to ensure you display the appropriate alert and search for applicable data.

Search Intent	Sample Query Text				
The file or process	"Find this file on all endpoints"				
	"Does this file exist"				
	"Search for this file on all endpoints"				
	"Find this process"				
The file path	"Find this file path"				
	"Does this file path exist on other endpoints"				
	"Search for this file path on active endpoints"				
The MD5 hash	"Find this MD5 hash"				
	"Does this MD5 hash exist"				
	"Does this MD5 hash exist on Windows endpoints"				
	"Search for this MD5 hash"				
The SHA1 hash	"Find this SHA1 hash"				
	"Does this SHA1 hash exist"				
	"Search for this SHA1 hash"				
The SHA256 hash	"Find this SHA256 hash"				
	"Does this SHA256 hash exist"				
	"Search for this SHA256 hash"				
The process lineage of a file	<b>NOTE:</b> Be sure you specify an endpoint.				
	"Determine the process lineage for this file on endpoint 10.1.2.34"				
	"Find the process lineage for this file on endpoint-hostname"				
	"Show me the process lineage for this file on endpoint 10.1.2.34"				



# **Configure Third-Party Applications to Connect to Endgame**

If a third-party application is configured to connect to Endgame, you can use Artemis to pivot to that application to search for external files that contain the same metadata. This feature leverages Endgame's detection and prevention capabilities with services that can provide additional context.

For example, if you view a Malicious File alert and VirusTotal integration is configured, when you launch Artemis, a recommended query that allows you to pivot to a hash search in VirusTotal appears in the chat window:

I see you are looking at a Malicious File alert, here are some suggested queries I can run:

- Search for this file name on all endpoints
- Search for this file hash on all endpoints
- Look up this MD5 hash on VirusTotal.

If you execute this search, the results from VirusTotal display in a new tab:

0 EXE 1/65	( 5 7 8 8 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	<b>Dne engir</b> SHA-256 File name File size Last analysis	1 <b>e detec</b> 755ced6 POWER5 434.5 KE 2017-10	<b>ted this file</b> 5c2617f5fec56f025155f9f03d44c6 5HELL 3 -07 01:53:23 UTC	5c41173cf363d0742713184(	c4f0d7	
Detection	Details	Commu	nity 1				
Cylance		A	Unsafe		Ad-Aware	Ø	Clean
AegisLab		Ø	Clean		AhnLab-V3	0	Clean
ALYac		Ø	Clean		Antiy-AVL	0	Clean
Arcabit		Ø	Clean		Avast	0	Clean
Avast Mob	ile Security	<b>S</b>	Clean		AVG	Ø	Clean

To configure a third-party application to connect to Endgame:

- 1. Open a secure shell to the Endgame platform.
- 2. At the command prompt, run the following command:

configure integration add <name of application>

3. At the command prompt, type the URL of the application, including the https://, and press **Enter**. If the integration was successful, a "Successfully added integration for <company>" confirmation appears.





Sample third-party configuration for VirusTotal

# **Event Query Language (EQL) Overview**

Event Query Language (EQL) enables you to execute advanced queries via Artemis that may be unavailable using natural language. EQL is also the syntax administrators use to create **Custom Rules**<sup>1</sup>.

EQL supports equality matching and wildcard characters, basic "and", "or", "not", and "in" Boolean search operators, and process lineage relationships. It can also join multiple events for a single process and compare values of fields to strings, integers, decimal values, and against other fields.

**NOTE:** Boolean search operators are case sensitive and must be lowercase in EQL searches. To view the complete guide on EQL documentation, go to: <u>http://eql.readthe-docs.io/</u>.

### **EQL Query Examples**

The following lists supported EQL query types and search examples.

**TIP:** You can find more examples of sample EQL queries by going to: <u>https://eql-lib.readthedocs.io/en/latest/analytics.html</u>.

### Boolean

Basic Query Structure: <event\_type> where <schema\_value> [==, !=, <=, <, >, >=]
<value>

### **Query Example:**

<sup>1</sup>A statement, written in EQL, that instructs Endgame's sensor to monitor suspicious or malicious activity specific to your

environment. If such activity is detected, the sensor generates an alert in the Endgame platform.


## process where process\_name == "svchost.exe" and command\_line != "\* -k \*"

**Description:** Finds all processes named "svchost" but without the string "-k" in the command line.

**OS:** Windows, macOS, Linux.



### Event Relationships

#### **Basic Query Structure:**

<event\_type> where child of [<event\_type> where <clause>]

Query Example:

```
process where child of [process where parent_process_name == "wmiprvse.exe"]
```

**Description:** Finds grandchildren of the Windows Management Instrumentation Provider service.

**OS:** Windows.

Join

**Basic Query Structure:** 

```
join by <schema_value>
[<event_type> where <clause>]
[<event_type> where <clause>]
```

Query Example:

```
join by pid
[process where true]
[network where true][registry where true]
[file where true]
until [process where event_subtype_full == "termination_event"]
```

**Description:** Finds events that are joined until an expiration event is met.

OS: Windows, macOS, Linux.



#### Sequence

**Basic Query Structure:** 

```
sequence with maxspan=<time>
[<event_type> where <clause>]
[<event_type> where <clause>]
```

Query Example:

```
sequence with maxspan=30s
[network where destination_port==3389 and event_subtype_full="*_accept_event*"]
[security where event_id in (4624, 4625) and logon_type == 10
```

**Description:** Network logon over Remote Desktop - With a maxspan of 30 seconds, looks for an incoming network connection from a host, followed by a separate event for the remote authentication success or failure.

**OS:** Windows, macOS, Linux.

#### **Data Pipes**

**Basic Query Structure:** 

```
unique <expression> [, <expression>] ...
count
count <expression> [, <expression>] ...
filter <expression>
unique_count <expression> [, <expression>] ...
tail <int>
head <int>
```

Query Example:

```
process where true | count parent_process_name, process_name
// results look like
// {"count": 100, "key": ["explorer.exe", "cmd.exe", "percent": .4}
// {"count": 100, "key": ["cmd.exe", "cmd.exe", "percent": .4}
```

**Description:** Counts the number of times a set of values occurs.

**Query Example:** 



## security where event\_id == 4624| tail 10

Description: Retrieves the 10 most recent logon events.

**OS:** Windows, macOS, Linux.

## Supported Event Types

The following table lists the supported EQL event types by operating system:

Name	EQL Event Type	Supported OS
CLR (Common Language Runtime) (Beta)	clr	• Windows
DNS	dns	• Windows
File	file	• Windows
		• Linux
		• macOS
Image Load	image_load	• Windows
Network	network	• Windows
		• Linux
		• macOS
PowerShell (Beta)	powershell	• Windows
Process	process	• Windows
		• Linux
		• macOS
Registry	registry	• Windows
Windows API (Beta)	api	• Windows
Windows Security Logs	security	• Windows
WMI (Windows Management Instrumentation) (Beta)	etw	• Windows



## **Execute EQL Queries via Artemis**

To execute an EQL search via Artemis:

1. On the Top Navigation toolbar, click



- 2. In the response text box, type the EQL query. If the EQL syntax is correct, Artemis asks you to confirm the search.
- 3. Type yes, then press Enter to create a query investigation.

Example:



Sample EQL search using Artemis



To run an EQL search across a specific operating system, first type the query and press **Enter**, then when Artemis responds, specify which endpoints to search, as seen in the following example:





Sample EQL search across multiple endpoints using Artemis





## **Eventing Schema**

The following table lists the fields that are indexed in the Endgame platform when the sensor collects event data. You can use these fields to construct advanced searches in Artemis using Event Query Language (EQL). The ECS column shows the most recently mapped field names in Elastic Common Schema, which you can use to create searches in the Elastic Discover application.

EQL	ECS (Elastic Common Schema)	Operating System
	API	
Subtypes		
api_event		
access_timestamp	N/A	Windows (All)
acting_process_creation_time	N/A	
acting_process_id	N/A	
acting_process_name	N/A	
acting_process_path	N/A	
acting_process_unique_pid	N/A	
acting_thread_authentication_id	N/A	
acting_thread_creation_time	N/A	
acting_thread_elevation_type	N/A	
acting_thread_id	N/A	
acting_thread_impersonation_level	N/A	
acting_thread_integrity_level	N/A	
acting_thread_start_module	N/A	
acting_thread_start_time	N/A	
acting_thread_user_domain	N/A	
acting_thread_user_name	N/A	
acting_thread_user_sid	N/A	
apc_routine	N/A	
apc_routine_bytes	N/A	
apc_routine_context	N/A	



EQL	ECS (Elastic Common Schema)	Operating System
apc_routine_context_bytes	N/A	
api_name	N/A	
callstack_hash	N/A	
change_timestamp	N/A	
creation_timestamp	N/A	
delete_file	N/A	
event_message	message	
event_subtype_full	event.action	
event_type_full	N/A	
file_attributes_int	N/A	
file_attributes_string	N/A	
file_disposition	N/A	
file_name	N/A	
file_path	N/A	
getclipboard_format	N/A	
hidden_flag_set	N/A	
key_path	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
query_file_path	N/A	
rename_count	N/A	
return_value	N/A	
serial_event_id	event.sequence	
service_access	N/A	
service_bin_path	N/A	
service_display_name	N/A	



EQL	ECS (Elastic Common Schema)	Operating System
service_start_name	N/A	
service_start_type	N/A	
service_type	N/A	
system_flag_set	N/A	
target_domain_name	N/A	
target_process_creation_time	N/A	
target_process_id	N/A	
target_process_name	N/A	
target_process_path	N/A	
target_process_unique_pid	N/A	
target_thread_creation_time	N/A	
target_thread_id	N/A	
target_thread_start_module	N/A	
target_thread_start_time	N/A	
target_token_authentication_id	N/A	
target_token_elevation_type	N/A	
target_token_impersonation_level	N/A	
target_token_integrity_level	N/A	
target_token_user_domain	N/A	
target_token_user_name	N/A	
target_token_user_sid	N/A	
target_user_name	N/A	
tid	N/A	
time_stomped	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
user_domain	user.domain	



EQL	ECS (Elastic Common Schema)	Operating System
user_name	user.full_name	
user_sid	user.id	
write_timestamp	N/A	
callers	N/A	
	CLR	
Subtypes		
load_image		
load_module		
bytes	N/A	Windows (All)
event_subtype_full	event.action	
module_name	N/A	
namespace_hash	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
serial_event_id	event.sequence	
timestamp	@timestamp	
typedef_hash	N/A	
typeref_hash	N/A	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
event_message	message	
event_type_full	N/A	
tid	N/A	
timestamp_utc	N/A	



EQL	ECS (Elastic Common Schema)	Operating System
typedefs	N/A	
typerefs	N/A	
	DNS	
Subtypes		
lookup_failure		
request_event		
event_id	N/A	Windows (All)
event_subtype_full	event.action	
event_type_full	N/A	
opcode	N/A	
pid	process.pid	
process_name	process.name	
process_path	process.executable	
query_name	dns.question.name	
query_options	N/A	
query_results	N/A	
query_status	N/A	
query_type	N/A	
serial_event_id	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
File		
<u>Subtypes</u>		
file_create_event		
file_modify_event		
file_delete_event		



file\_rename\_event

## EQL

## ECS (Elastic Common Schema)

## **Operating System**

file_overwrite_event		
event_subtype_full	event.action	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
file_attributes	file.attributes	Windows, Linux, macOS
file_name	file.name	Windows, Linux, macOS
file_path	file.path	Windows, Linux, macOS
old_file_name	N/A	Windows, Linux, macOS
old_file_path	N/A	Windows, Linux, macOS
opcode	N/A	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
share_mode	N/A	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
zone_id	N/A	Windows, Linux, macOS
create_disposition	N/A	Windows
desired_access	N/A	Windows
create_options	N/A	Windows
user_domain	user.domain	Windows
user_name	user.full_name	Windows
user_sid	user.id	Windows
effective_gid	file.gid	Linux, macOS
effective_group_name	file.group	Linux, macOS
effective_uid	file.uid	Linux, macOS



EQL	ECS (Elastic Common Schema)	Operating System
effective_user_name	N/A	Linux, macOS
real_gid	N/A	Linux, macOS
real_group_name	N/A	Linux, macOS
real_user_name	N/A	Linux, macOS
real_uid	N/A	Linux, macOS
Image Load		

Endgame collects the following image names:

- System.Management.Automation.dll
- System.Management.Automation.ni.dll
- jscript.dll
- jscript9.dll
- chakra.dll
- vbscript.dll
- scrobj.dll
- scrrun.dll
- wlbsctrl.dll
- wbemcomn.dll
- WptsExtensions.dll
- Tsmsisrv.dll
- TSVIPSrv.dll
- Msfte.dll
- wow64log.dll
- WindowsCoreDeviceInfo.dll
- Ualapi.dll
- wlanhlp.dll
- phoneinfo.dll
- EdgeGdi.dll
- cdpsgshims.dll



EQL	ECS (Elastic Common Schema)	Operating System
windowsperformancerecorderco	ontrol.dll	
<ul> <li>diagtrack_win.dll</li> </ul>		
Taskschd.dll		
• wmiutils.dll		
<ul> <li>vaultcli.dll</li> </ul>		
<ul> <li>bcrypt.dll</li> </ul>		
<ul> <li>psapi.dl</li> </ul>		
• msxml3.dll		
• 7z.dll		
<ul> <li>pgpcrypt.dll</li> </ul>		
<ul> <li>pgpencrypt.dll</li> </ul>		
wbemdisp.dll		
wbemprox.dll		
<ul> <li>wbemsvc.dll</li> </ul>		
<ul> <li>fastprox.dll</li> </ul>		
• ntdll.dll		
Subtypes		
driver_load_event		
image_load_event		
event_subtype_full	event.action	Windows (All)
event_type_full	N/A	
image_name	dll.name	
image_path	dll.path	
md5	dll.hash.md5	
opcode	N/A	
pid	process.pid	
process_name	process.name, process.title	
process_path	process.executable	



EQL	ECS (Elastic Common Schema)	Operating System
serial_event_id	event.sequence	
sha1	dll.hash.sha1	
sha256	dll.hash.sha256	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
	Network	
Subtypes		
ipv4_connection_attempt_event	N/A	Windows, Linux, macOS
ipv4_connection_accept_event		Windows, Linux, macOS
ipv4_disconnect_received_event		Windows, Linux, macOS
ipv4_reconnect_attempt_event		Windows, Linux, macOS
ipv6_disconnect_received_event		Windows, Linux, macOS
ipv6_connection_accept_event		Windows, Linux, macOS
ipv6_reconnect_attempt_event		Windows, Linux, macOS
ipv4_http_request_event		Windows
ipv6_http_request_event		Windows
connection_id	N/A	Windows, Linux, macOS
destination_address	destination.address, server.address, server.ip	Windows, Linux, macOS
destination_port	destination.port, server.port	Windows, Linux, macOS
event_id	N/A	Windows, Linux, macOS
event_subtype_full	event.action	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
in_packet_count	network.packets	Windows, Linux, macOS
opcode	N/A	Windows, Linux, macOS
out_packet_count	network.packets	Windows, Linux, macOS
partial_flow	N/A	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS



EQL	ECS (Elastic Common Schema)	Operating System
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
protocol	network.iana_number	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
source_address	source.address, source.ip	Windows, Linux, macOS
source_port	source.port	Windows, Linux, macOS
task	N/A	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
total_in_bytes	destination.bytes, server.bytes	Windows, Linux, macOS
total_out_bytes	client.bytes, source.bytes	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
user_domain	user.domain	Windows
user_name	user.full_name	Windows
user_sid	user.id	Windows
effective_gid	destination/client/server/source.user.group.id	Linux, macOS
effective_group_name	destination/client/server/source.user.group.name	Linux, macOS
effective_uid	destination/client/server/source.user.id	Linux, macOS
effective_user_name	destination/client/server/source.user.name	Linux, macOS
real_gid	user.group.id	Linux, macOS
real_group_name	user.group.name	Linux, macOS
real_user_name	user.name	Linux, macOS
real_uid	user.id	Linux, macOS
PowerShell		
Subtypes		
ps_cmdlet_etw_event		
ps_scriptblock_etw_event		
event_subtype_full	event.action	Windows (All)



EQL	ECS (Elastic Common Schema)	Operating System
header	N/A	
message	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
serial_event_id	event.sequence	
timestamp	@timestamp	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
is_obfuscated	N/A	
event_message	message	
event_type_full	N/A	
tid	N/A	
timestamp_utc	N/A	
	Process	
Subtypes		
already_running	N/A	Windows, Linux, macOS
creation_event	N/A	Windows
still_running	N/A	Windows, Linux, macOS
termination_event	N/A	Windows, Linux, macOS
exec_event	N/A	Linux, macOS
fork_event	N/A	Linux, macOS
gid_change	N/A	Linux, macOS
session_id_change	N/A	Linux, macOS
still_running	N/A	Linux, macOS



EQL	ECS (Elastic Common Schema)	Operating System
uid_change	N/A	Linux, macOS
authentication_id	N/A	Windows, Linux, macOS
command_line	process.args, process.args_count, process	Windows, Linux, macOS
	command_line	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
exit_code	process.exit_code	Windows, Linux, macOS
md5	process.hash.md5	Windows, Linux, macOS
original_file_name	process.pe.original_file_name	Windows, Linux, macOS
parent_process_name	process.parent.name, process.parent.title	Windows, Linux, macOS
parent_process_path	process.parent.executable	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS
ppid	process.parent.pid	Windows, Linux, macOS
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
sha1	process.hash.sha1	Windows, Linux, macOS
sha256	process.hash.sha256	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
unique_ppid	N/A	Windows, Linux, macOS
event_subtype_full	event.action	Windows, Linux, macOS
opcode	N/A	Windows
package_name	N/A	Windows
signature_signer	process.code_signature.subject_name	Windows
signature_status	process.code_signature.status	Windows
user_domain	user.domain	Windows
user_name	user.full_name	Windows
	user.id	



		· · · · · · · · · · · · · · · · · · ·
EQL	ECS (Elastic Common Schema)	Operating System
user_sid	N/A	Windows
effective_gid	N/A	Linux, macOS
effective_group_name	N/A	Linux, macOS
effective_uid	N/A	Linux, macOS
effective_user_name	user.group.id	Linux, macOS
real_gid	user.group.name	Linux, macOS
real_group_name	user.name	Linux, macOS
real_user_name	user.id	Linux, macOS
real_uid	N/A	Linux, macOS
session_id	process.thread.id	Linux, macOS
tid		Linux, macOS
	Security	
Subtypes		
admin_logon		
explicit_user_logon		
user_logoff		
user_logon		
user_logon_failed		
workstation_unlocked		
workstation_locked		
Subtype Full	Windows Event ID	
admin_logon	4672	
explicit_user_logon	4648	
user_logoff	4634	
user_logon	4624	
user_logon_failed	4625	
workstation_unlocked	4801	
workstation_locked	4800	



EQL	ECS (Elastic Common Schema)	Operating System
channel_name	N/A	Windows (All)
computer_name	N/A	
event_id	N/A	
event_message	message	
event_subtype_full	event.action	
event_type_full	N/A	
ip_address	N/A	
logon_type	N/A	
opcode	N/A	
pid	process.pid	
privilege_list	N/A	
process_name	process.name, process.title	
process_path	process.executable	
provider_guid	N/A	
provider_name	N/A	
serial_event_id	event.sequence	
subject_domain_name	user.domain	
subject_logon_id	N/A	
subject_user_name	user.full_name, user.name	
subject_user_sid	user.id	
system_pid	N/A	
system_process_name	N/A	
system_thread_id	N/A	
target_domain_name	user.target.domain	
target_logon_id	N/A	
target_user_name	user.target.name	
task	N/A	
timestamp	@timestamp	



EQL	ECS (Elastic Common Schema)	Operating System
timestamp_utc	N/A	
unique_pid	N/A	
	Registry	
Subtypes		
registry_modify_event		
bytes_written	registry.data.bytes	Windows (All)
bytes_written_count	N/A	
bytes_written_string	registry.data.strings	
bytes_written_string_list	registry.data.strings	
bytes_written_u32	registry.data.strings	
bytes_written_u64	registry.data.strings	
event_subtype_full	event.action	
event_type_full	N/A	
key_path	registry.data.key, registry.data.path,	
key_type	registry.data.value	
opcode	registry.data.type	
pid	N/A	
process_name	process.pid	
process_path	process.name, process.title	
serial_event_id	process.executable	
timestamp	event.sequence	
timestamp_utc	@timestamp	
unique_pid	N/A	
	N/A	
	WMI	
Subtypes		
file_create_event		
file_delete_event		



EQL	ECS (Elastic Common Schema)	Operating System
file_exchange_event		
file_modify_event		
file_overwrite_event		
file_rename_event		
event_id	N/A	Windows (All)
event_subtype_full	event.action	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
provider_guid	N/A	
serial_event_id	event.sequence	
tid	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
properties.CONSUMER	N/A	
properties.ClassName	N/A	
properties.ClientMachine	N/A	
properties.ClientMachineFQDN	N/A	
properties.ClientProcessCreationTime	N/A	
properties.ClientProcessId	N/A	
properties.Commandline	N/A	
properties.ComponentName	N/A	
properties.CorrelationId	N/A	



EQL	ECS (Elastic Common Schema)	Operating System
properties.CreatedProcessId	N/A	
properties.ESS	N/A	
properties.Errorld	N/A	
properties.FileName	N/A	
properties.Flags	N/A	
properties.GroupOperationId	N/A	
properties.HostProcess	N/A	
properties.Id	N/A	
properties.ImplementationClass	N/A	
properties.lsLocal	N/A	
properties.MachineName	N/A	
properties.Message	N/A	
properties.MessageDetail	N/A	
properties.MethodName	N/A	
properties.Namespace	N/A	
properties.NamespaceName	N/A	
properties.Operation	N/A	
properties.OperationId	N/A	
properties.Path	N/A	
properties.PossibleCause	N/A	
properties.Protocol	N/A	
properties.ProviderGuid	N/A	
properties.ProviderName	N/A	
properties.ProviderPath	N/A	
properties.Query	N/A	
properties.QueryId	N/A	
properties.ResultCode	N/A	
properties.User	N/A	



EQL	ECS (Elastic Common Schema)	Operating System
properties.unique_ClientProcessId	N/A	
properties.unique_CreatedProcessId	N/A	



# **Artemis Queries List Overview**

The Artemis Queries list is an enumeration of all Artemis queries and their relevant details, organized in a table. It is displayed on the Investigation Dashboard within the **Queries** tab. The list is useful to view general search details, investigation progress, and to view results of a specific search. Queries display in reverse chronological order with the most recently executed queries at the top.

esti	selection option.				1- <u>43</u> of 43 < 3
-	INVESTIGATION NAME	ASSIGNEE	INVESTIGATION BREAKDOWN	ENDPOINTS	DATE CREATED
/	Process Search 2017-06-07T17:34:18.030521	Super Admin	100% 1.Query total	1	Jun 7, 2017 5:34:18 PM UTC
/	Process Search 2017-06-07T17:31:45.161720	Super Admin	100% 1 Query total	1	Jun 7, 2017 5:31:45 PM UTC
/	Process Search 2017-06-07T17:18:54.957757	Super Admin	100% 1 Query total	16	Jun 7, 2017 5:18:55 PM UTC
	Process Search 2017-06-07T15:34:07.199674	Super Admin	100% 1 Query total	16	Jun 7, 2017 3:34:07 PM UTC
	User Logon Search 2017-06-07T13:12:58.092214	Super Admin	100% <u>1 Query total</u>	16	Jun 7, 2017 1:12:58 PM UTC
	Process Search 2017-06-06T20:06:40.338501	Super Admin	100% <u>1 Query total</u>	16	Jun 6, 2017 8:06:40 PM UTC
	C2 Beaconing Search 2017-06-06T20:05:57.507429	Super Admin	100% 1 Query total	16	Jun 6, 2017 8:05:57 PM UTC
	User Logon Search 2017-06-06T17:22:48.651179	Super Admin	100% <u>1 Query total</u>	4	Jun 6, 2017 5:22:48 PM UTC
	Network Search 2017-06-06T17:22:25.715415	Super Admin	100% 1 Query total	4	Jun 6, 2017 5:22:25 PM UTC
	Network Search 2017-06-06T17:21:52.737518	Super Admin	100% 1 Query total	16	Jun 6, 2017 5:21:52 PM UTC
	Process Search 2017-06-06T17:20:05.936552	Super Admin	100% 1 Query total	1	Jun 6, 2017 5:20:06 PM UTC
	<b>INVESTIGATION NAME</b> The name of the search.	ASSIGNEE The name of the user who executed the search.		ENDPOINTS The number of endpoints	DATE CREATED The date and time the search was
			INVESTIGATION BREAKDOWN The number of queries included in	link to view them in the Endpoints list.	executed.
			the search and the overall completion percentage.		

#### Artemis Queries list

The columns in the list provide the following general details about each Artemis query:

Column Name	Description
INVESTIGATION NAME	The name of the Artemis query, which initially is auto-generated. You can change the name on the Investigation Details page.
ASSIGNEE	The name of the user who executed the search.
INVESTIGATION BREAKDOWN	Displays a progress bar that indicates the query's percentage completion across all endpoints in the investigation. The <b>Query total</b> link displays the number of queries in the search, which is always <b>1</b> .
ENDPOINTS	The number of endpoints included in the search. Click the number link to view those



Column Name	Description
	endpoints in the Endpoints list.
DATE CREATED	The date and time the search was executed according to Coordinated Universal Time (UTC) or your selected time zone.

## Sort and Filter Columns in the Queries List

You can sort columns in the list to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.



NOTE: You cannot sort or filter the INVESTIGATION BREAKDOWN column.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

• Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

• In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the

entry. The currently filtered column is denoted by a 🗐 symbol.



Column sort and filter



## Page Pagination

In the upper-right corner above the list is a range display, which displays the current number range of investigations out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 investigations display per page; however, you can change the number to a preferred choice:

- 1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
- 2. In the **Max count of** text box, enter a new number between 1 and 500.
- 3. Click  $\checkmark$  to save your changes.



# Archive an Artemis Query

Archiving an Artemis query moves it from the **Current** tab on the Investigation Dashboard to the **Archived** tab. Consider archiving a query after you have reviewed the search results to distinguish it from queries that have not yet been reviewed.

To archive multiple Artemis queries:

- 1. On the Investigation Dashboard, select the **Queries** tab to filter the list to Artemis queries.
- 2. In the Investigations list, select the box to the left of each query to archive.

TIP: To select all queries on the current page, select the box to the left of the **INVESTIGATION NAME** column heading.

- 3. On the Action toolbar, click Archive Investigations.
- 4. In the Archive Investigations dialog box that says, "You are about to archive number Investigations. The investigations will be immediately sent to the Archive Tab and be set as Archived..." click Archive. A "Successfully archived investigation(s)" message appears.
- 5. Click Finish.





#### Archive Investigations dialog box

í	You can also archive a single query from the Investigation Details page by clicking the
	<b>Archive</b> button in the Artemis Query Overview section.



# Verify that Logon Events are Enabled in Windows (Optional)

The "Audit account logon events" setting in Windows Local Security Policy determines whether to audit each time a user logs on or off a computer. If this setting is not configured, Endgame's sensor is unable to store those events in the platform. Consequently, any user activity searches executed via Artemis will return with no results.

To verify that the Local Security Policy in Windows can capture logon events:

- 1. Navigate to the Audit Policy setting within the Windows Local Security Policy:
  - a. Open the Control Panel, and then go to Administrative Tools > Local Security Policy.
  - b. Expand the Local Policies folder, and then select the Audit Policy folder.

**TIP:** As an alternative, you can type **secpol.msc** in the Windows search bar to go directly to the Local Security Policy panel, and then click **Local Policies** > **Audit Policy**.

2. In the right pane, verify that the security settings for Audit account logon events and Audit logon events both say, "Success, Failure." This ensures Windows captures logon events and also ensures the sensor in the Endgame platform can store these events. If the security settings do not say "Success, Failure," an administrator can modify the local security policy to change them, or the organization group policy can configure the associated endpoints to audit capture these events.



Audit Policy in Windows



# **Customer Support**

For any questions or issues using the Endgame platform, please contact Customer Success by submitting a request at <a href="https://support.endgame.com">https://support.endgame.com</a> or emailing <a href="https://support.endgame.com">support.endgame.com</a> or emailing <a href="https://support.endgame.com">support.endgame.com</a>.

Customer Success is available Monday through Friday from 9:00 a.m. – 9:00 p.m. ET.

Sign in to End	igame Customer Succes
imail	
Password	
Stav signed in	
- Stay Signed in	
	Sign in
For	got my password

# **ENDGAME** An Elastic company