cybereason

ENDPOINT DETECTION & RESPONSE_

Mitigate Security Threats Before They Cause Harm

KEY BENEFITS

» Get actionable threat detection without the noise

» Build detection rules across platforms for Windows, macOS, and Linux

» Create custom detection rules tailored to your organization

» Investigate attacks anywhere with Remote Shell

» Respond rapidly with built-in remediation options.

ABOUT CYBEREASON

The Cybereason Defense Platform combines managed endpoint prevention, detection, and response in one lightweight agent. It delivers multi-layer endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Combine the best platform on the market with managed services from our expert security team to receive a comprehensive defense.

CLICK HERE TO GET A DEMO →

As attackers adopt and develop increasingly sophisticated tools, techniques, and procedures, advanced threats are becoming more difficult to detect. More than 40,000 security incidents in the past year took months or longer to discover (Source: 2019 Verizon DBIR report).

As time-to-detect grows, analysts need a solution that provides automation, rapid detection, and context-rich remediation.

Cybereason EDR unifies prevention, detection, response and automated hunting capabilities in a single solution to provide complete protection against advanced threats. With Cybereason EDR, organizations can automatically detect suspicious activities, receive alerts on malicious operations, and remediate threats in real-time.

RAPIDLY DETECT & RESOLVE ADVANCED THREATS

Delivering complete endpoint protection from a single, lightweight agent, Cybereason EDR is a full-featured EDR solution designed to detect, analyze, and remediate against highly advanced threats. Cybereason allows organizations to correlate data across machines and generate contextualized alerts to monitor threats as they're discovered at any point in the attack chain.

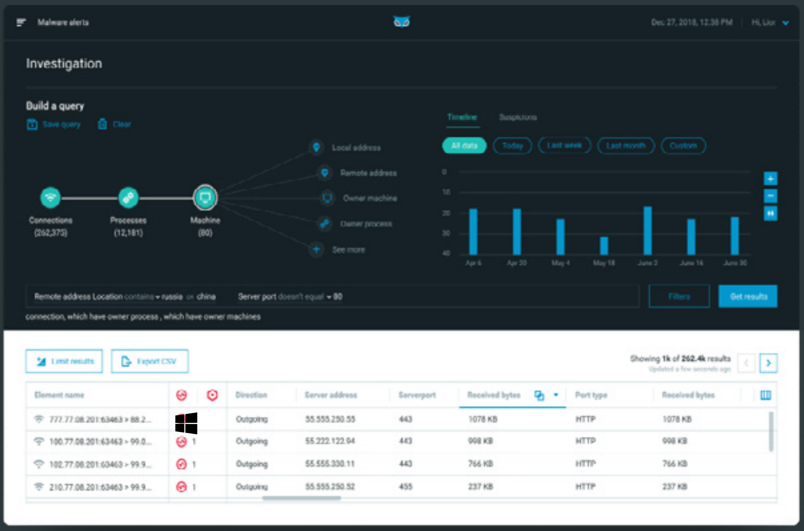
Cybereason's in-memory graph stores all event data and answers queries in seconds - across tens of millions of events.

UNDERSTAND THE FULL ATTACK

Get a complete story of the attack from start to finish with the Malop™. Within a Malop, you can easily see all related attack elements, including the root cause, all affected machines and users, incoming and outgoing communications and a timeline of the attack. The Malop gives your team full context of an incident so they can instantly be knowledgeable about the attack and remediate in seconds.

AUTOMATICALLY UNCOVER ATTACKS_

Cybereason EDR automatically detects malicious activity and presents it in an intuitive way that provides end-to-end context of an attack campaign. Our platform has a built-in threat-finder that hunts for malicious activities and tools, tactics and procedures used by attackers in real-world campaigns. You don't need to spend weeks configuring and tuning rules.



Remote address Location contains ▾ russia or china   Server port doesn't equal ▾ 80

connection, which have owner process , which have owner machines

Element name			Direction	Server address	Serverport	Received bytes	Port type	Received bytes
777.77.08.201:63463 > 88.2...			Outgoing	55.555.250.55	443	1078 KB	HTTP	1078 KB
100.77.08.201:63463 > 99.0...	1		Outgoing	55.222.122.94	443	998 KB	HTTP	998 KB
102.77.08.201:63463 > 99.9...	1		Outgoing	55.555.330.11	443	766 KB	HTTP	766 KB
210.77.08.201:63463 > 99.9...	1		Outgoing	55.555.250.52	455	237 KB	HTTP	237 KB

DETECT MALICIOUS ACTIVITY WITH FULL CONTEXT

SUPPORTED VERSIONS

WINDOWS

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, XP SP3
- Windows Vista Server 2003, Server 2003 R2
- Windows Vista Server 2008, Server 2008 R2

MACOS

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Yosemite (10.10)
- El Capitan (10.11)

LINUX

- CentOS 6 and 7
- Red Hat Enterprise Linux 6 and 7
- Oracle Linux 6 and 7
- Ubuntu 14 LTS and 16 LTS
- Ubuntu 18.04
- SLES 12
- Debian 8 and 9
- Amazon Linux AMI 2017.03

SIMPLIFY INVESTIGATIONS & RESPOND IN ONE CLICK

With Cybereason EDR, analysts with any level of experience can rapidly investigate incidents and easily respond to alerts. Your team can view the entire process tree with a complete timeline of events, for all malicious activity, across every machine and every process- all within a platform that zeroes in on what's important. Mapping alerts to the MITRE ATT&CK™ Framework allows analysts to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. Upon alerting security professionals that a malicious operation is detected, analysts can quickly remediate in a single click by killing processes, quarantining files, removing persistence mechanisms, preventing file execution, and isolating machines.

IMPROVE YOUR SECOP TEAM EFFICIENCY

With Cybereason EDR, your analysts can spend more time hunting and less time triaging. Through automation, Cybereason's dynamic database provides full context to malicious operations (Malops), all in real-time. Every alert contains all related attack elements, including a timeline of the attack, all affected users and machines, the root cause, and incoming and outgoing communication, so you can quickly understand scope and impact.