limacharlie.io

Getting Started

This document outlines some recommended general configurations for those getting started with LimaCharlie's endpoint detection and response platform.

These recommendations do not constitute a comprehensive security posture but rather a general spread of capability meant to serve as an introduction to various components of the platform.

Any questions related to this document, or the LimaCharlie platform in general, can be directed to: answers@limacharlie.io

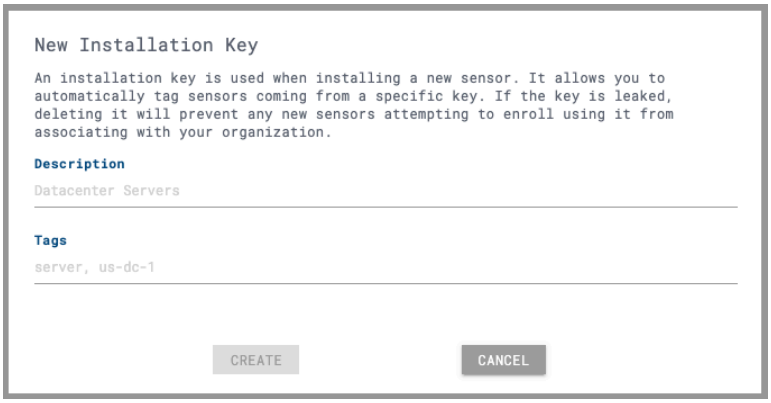
Intro

This guide is meant to help technical users new to endpoint detection and response get setup with a basic level of monitoring. If you have not familiarized yourself with the core concepts behind the LimaCharlie endpoint capability please read our Core Concepts document before proceeding.

Installing the Sensor

Before you can do any endpoint monitoring you will need to install the sensor - or agent - onto the endpoint(s) that you want to monitor. The LimaCharlie sensor is cross-platform but the installation procedure varies a little depending on which operating system you are using.

To get started you will need to create an installation key. Installation keys can be created by visiting the Installation Keys section of the web application and clicking on the plus icon in the upper right corner.



Once the key has been created copy it to your clipboard. Next visit the Sensor Downloads section of the web application and download the appropriate installer.

Once the sensor is downloaded to the endpoint you will need to give it the appropriate permissions and use the installation key when executing.

Installing the sensor requires administrator (or root) execution:

Windows: installer.exe -i YOUR_INSTALLATION_KEY

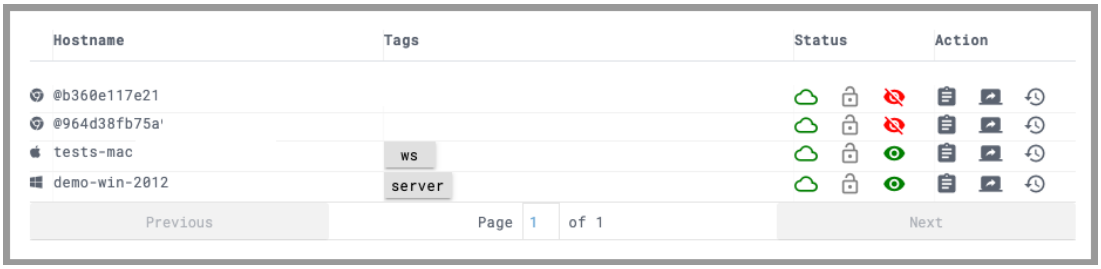
MacOS: chmod +x installer ; installer -i YOUR_INSTALLATION_KEY

Linux: chmod +x installer ; installer -d YOUR_INSTALLATION_KEY

Note: On Linux the exact persistence mechanism, like launchd, is left to the administrator, therefore the -d argument launches the sensor from the current working directory without persistence. ***The sensor does not daemonize itself***. Here is a sample script that can be used for installing the sensor in a persistent manner on Debian: Installer Script

If you wish to remove the sensor from the endpoint you can do so by running the installer with the -c flag.

Once the sensor is installed it should show up in the Sensors section of the web application.



Security Infrastructure as a Service

LimaCharlie is Security Infrastructure as a Service (SIaaS). You can think of LimaCharlie as the Amazon Web Services (AWS) or Google Cloud Platform (GCP) of information security. Our EDR capability can be thought of as the equivalent of EC2.

To enjoy the full capabilities of LimaCharlie you will need to enable the long term storage feature called Insight (the S3 to our EC2). With this feature enabled the LimaCharlie platform will store all telemetry data produced by the agents for one year. With the telemetry storage feature enabled you will be able to search for IOCs across your whole organization and utilize all of the tools available. LimaCharlie offers External Log Storage which is also indexed across IOCs and allows users to execute these same capabilities across log files

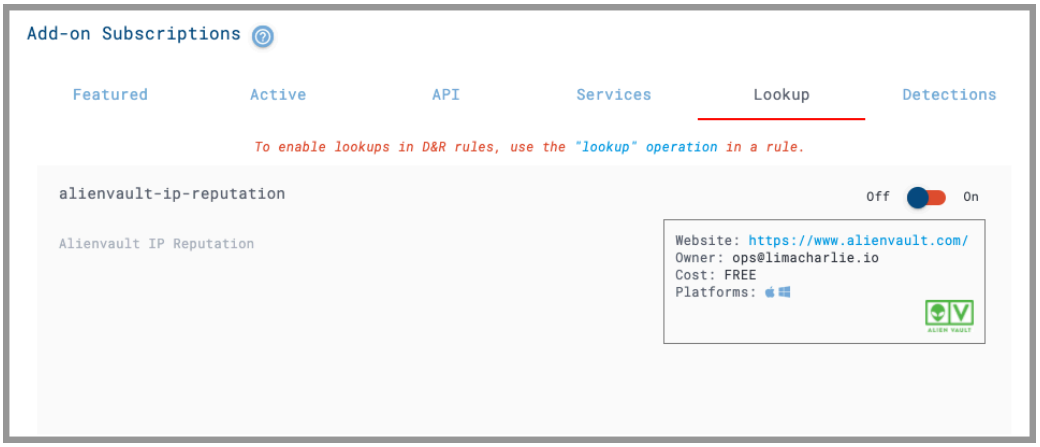
You can enable Insight be visiting the Add Ons section and clicking the toggle.

Detection and Response

LimaCharlie comes with a whole host of pre-made detections. There is no cost to the pre-made detections, but like telemetry storage, they do need to be enabled by the user.

You can go through the available detections by visiting the Add Ons section of the web application and decide on which detections you would like to enable based on their descriptions.
Threat Feed

In order to demonstrate the full process of leveraging a pre-made detection we will walk though setting up a detection and response (DR) rule based off of the AlienVault threat feed. The AlienVault threat feed is a good add on to have as a part of your initial posture and will provide good coverage for known major threats.



Start by visiting the Add Ons section, navigating to the Lookup tab and enabling alientvault-ip-reputation.

Once the Add On is enabled you will need to set up a DR rule to report if any of the listed domains are accessed. To get started go to the

D&R Rules section of the website and click on the plus icon in the upper right corner.
Click on the Advanced tab of the rule creation modal and give the detection a name. For this example we will call our rule AlienVault.

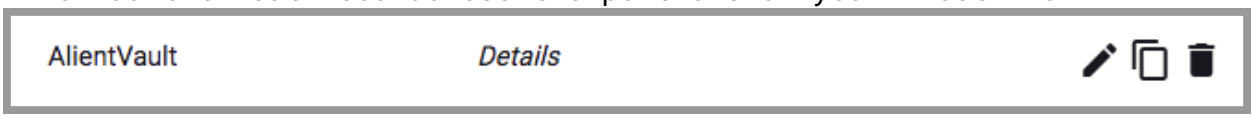
Copy the following example YAML into the detection section of the modal. This YAML example uses the AlientVault threat feed across Windows and MacOS checking all requests on TCP4, UDP4, TCP6 and UDP6. For more information on how the YAML is structured you can read the doc or work through the online course.

```
rules:
  - rules:
      - op: is windows
      - op: is mac
    op: or
  - rules:
      - path: event/PROCESS/NETWORK_ACTIVITY/?/IP_ADDRESS
        resource: 'lcr://lookup/alienvault-ip-reputation'
        event: NETWORK_SUMMARY
        op: lookup
      - path: event/?/IP_ADDRESS
        resource: 'lcr://lookup/alienvault-ip-reputation'
        events:
          - NEW_TCP4_CONNECTION
          - NEW_UDP4_CONNECTION
          - NEW_TCP6_CONNECTION
          - NEW_UDP6_CONNECTION
        op: lookup
    op: or
op: and
```

With the detection in place you will want to indicate the response. The following YAML will send an alert. Copy the YAML into the response section of the modal and click Create.

```
- action: report
  name: AlienVault
```

Having completed these steps you will now have monitoring of the AlienVault threat feed across the portions of your fleet indi



cated by the conditions in the detection rule.

Levenshtein distance

Another good starting item to get set up as part of your initial posture is Levenshtein distance. A common phishing practice employed by bad actors is to use a domain that is similar enough to the given organization that a user will not recognize the difference on a quick glance. The detection in this example will catch when a domain that is similar (but different) to the ones being watched shows up on the endpoint. This particular notification is fired when said domain is one or two characters different than one of the ones we are monitoring.

```
max: 2
case sensitive: false
value:
  - limacharlie.io
  - www.limacharlie.io
  - refractionpoint.com
  - www.refractionpoint.com
path: event/DOMAIN_NAME
event: DNS_REQUEST
op: string distance
```

The response component of this rule will be similar to the one described in the previous example and is left as an exercise for the user.

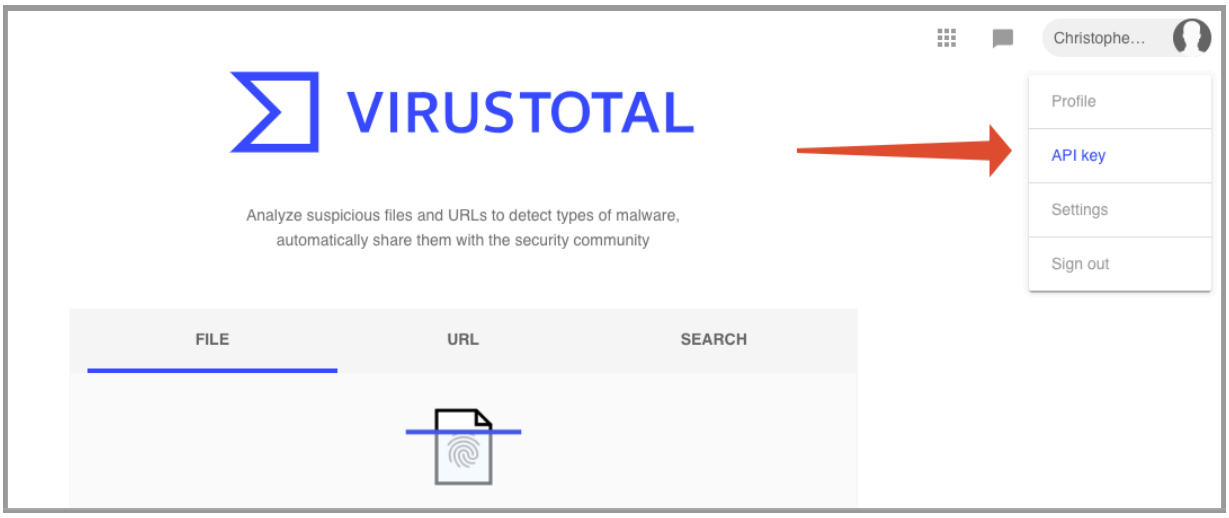
Virus Total

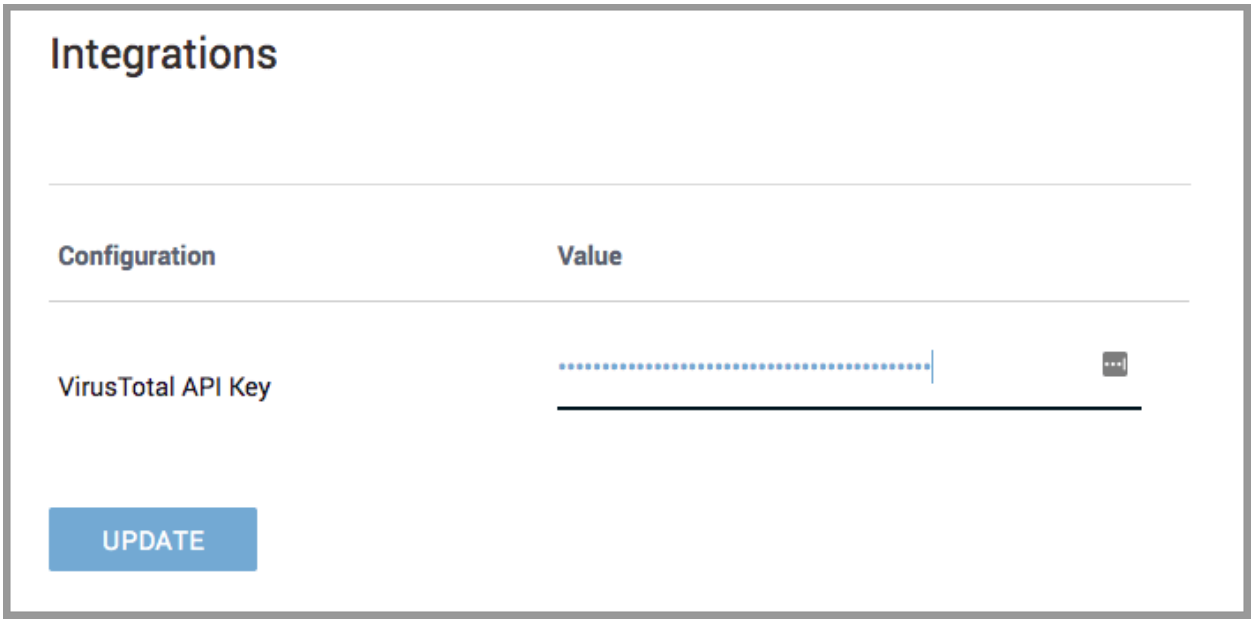
LimaCharlie also offers an integration with VirusTotal. If you do not already have an account with VirusTotal you will have to create one and get an API key.

Once you have created an account the API key can be found as follows.

The free tier of VirusTotal allows four lookups per minute via the API.

Note: LimaCharlie employs a global cache of all VirusTotal requests which should significantly reduce your costs if you are using VirusTotal at scale.





Once you have your VirusTotal API key you can go to the integrations section of the LimaCharlie web app and add your key.

Once you have entered your API key you can then create a DR rule to let you know if you get a hit from VirusTotal on a file with more than two different engines saying it is bad.

```
path: event/HASH
op: lookup
resource: 'lcr://api/vt'
event: CODE_IDENTITY
metadata_rules:
  path: /
  value: 2
  length of: true
  op: is greater than
```

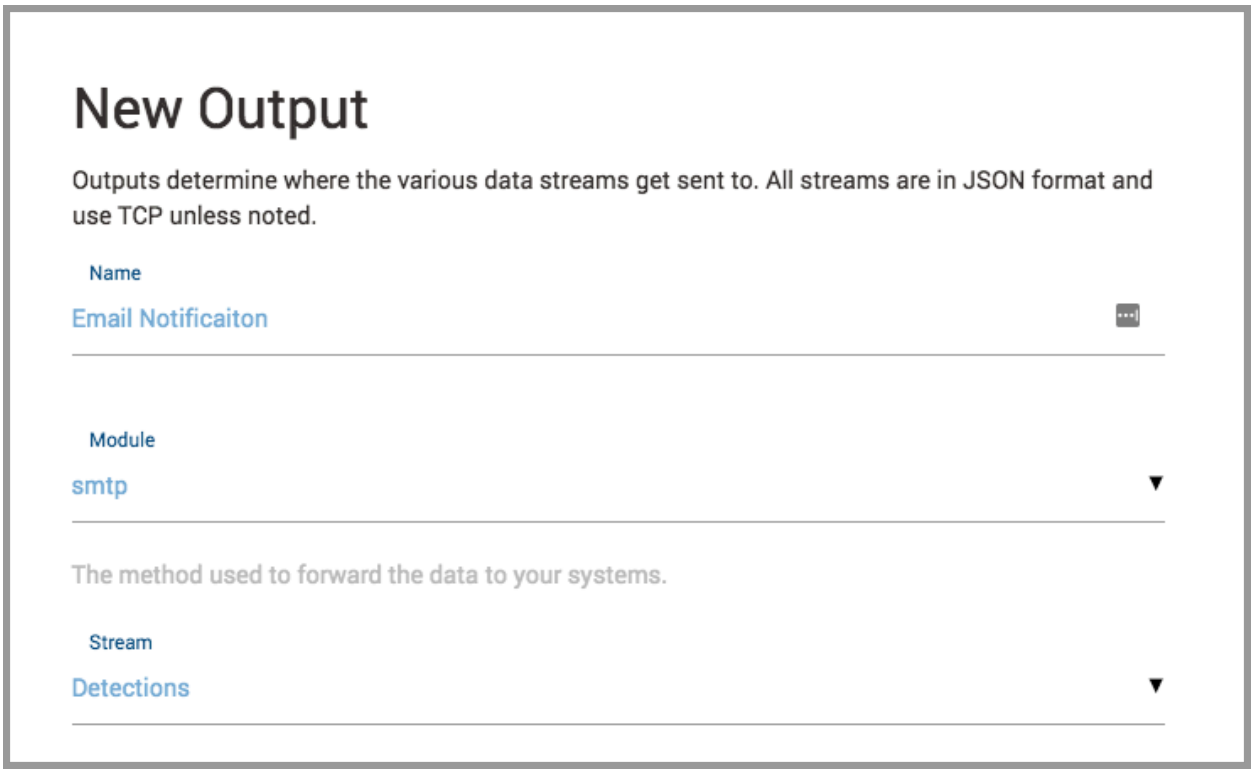
Once again the response component of this rule is left up to the user an exercise.

Notifications

LimaCharlie allows you to setup your own data lakes and send the telemetry wherever you want. With telemetry storage enabled you do not need to set up your own cold storage but you may want to get notified directly when a detection takes place.

Using the output configuration interface we can set up an SMTP module to send an email whenever a detection is caught.

You can configure the alert by visiting the Output tab and clicking the plus icon in the upper right corner. With the modal open, give the configuration a name and select smtp from the Module drop down. In order to ensure that you only get an email when a detection is triggered select Detections from the Stream dropdown.



dest_host: the IP or DNS (and optionally port) of the SMTP server to use to send the email.

dest_email: the email address to send the email to.

from_email: the email address to set in the From field of the email sent.

username: the username (if any) to authenticate with the SMTP server with.

password: the password (if any) to authenticate with the SMTP server with.

secret_key: an arbitrary shared secret used to compute an HMAC (SHA256) signature of the email to verify authenticity. See Webhook section in the doc.

Is_readable: if 'true' the email format will be HTML and designed to be readable by a human instead of a machine.

Example:

```
dest_host: smtp.gmail.com
dest_email: soc@corp.com
from_email: lc@corp.com
username: lc
password: password-for-my-lc-email-user
secret_key: this-is-my-secret-shared-key
```

There are also several optional fields that can be used to limit the alerts to particular sensors, tags or investigation IDs (you can even limit the alerts to specific event types). These optional fields should be fairly self explanatory and their configuration is left at the discretion of the user.

Full documentation can be found here: doc.limacharlie.io

REST API documentation via Swagger here: Swagger Doc

Free online course here: edu.limacharlie.io