

# Lima Charlie Detection and Response Rules Documentation

Welcome to the Lima Charlie Detection and Response Rules Documentation. This document serves as a comprehensive guide to creating, managing, and utilising detection and response rules within the Lima Charlie platform.

## 1. Introduction

Lima Charlie is a powerful security platform that enables users to detect and respond to security threats effectively. Detection and response rules are at the core of Lima Charlie's functionality, allowing users to define conditions for identifying suspicious or malicious activity and triggering automated responses. If you have missed the installation, I have provided the documentation on my [Github](#).

## 2. Getting Started

To create detection and response rules in Lima Charlie, users can access the Automation section of the platform's interface. Here, they can define rules using a simple yet flexible syntax and apply them to their environment.

The screenshot shows the 'Detection & Response Rules' interface in the Lima Charlie platform. The left sidebar contains a navigation menu with options like Sensors, Query Console, Artifacts, Dashboard, Detections, Automation, and DRR Rules. The main panel displays a list of rules with columns for Name, Last Modified, Updated By, and Tags. A search bar and filter dropdown are visible at the top of the rule list. The interface also includes a '+ New Rule' button and a 'Rules: 1926' indicator.

Name	Last Modified	Updated By	Tags
Untitled-1			
A Member Was Added to a Security-En...	2024-02-12 19:24:38	_snapattack-community	attack.persistence attack.t1098
AD Privileged Users or Groups Recon...	2024-02-12 19:24:33	_snapattack-community	attack.discovery attack.t1087.002
APT29	2024-02-12 19:24:33	_snapattack-community	attack.execution attack.g0016 attac
Abusing Findstr for Defense Evasion	2024-02-12 19:24:28	_snapattack-community	attack.defense_evasion attack.t1218
Account Tampering - Suspicious Fail...	2024-02-12 19:24:35	_snapattack-community	attack.persistence attack.defense_eva
Active Directory Replication from N...	2024-02-12 19:24:34	_snapattack-community	attack.credential_access attack.t1003

You can check the rules number and also check out the rules and explore more. There are already 1928 rules enabled by the platform.

This Documentation is all about writing the sigma rules for the detection and response with proper knowledge to trigger alerts, detection and user activity. You have knowledge about the sigma rule, here is the link to get started or you can checkout the rules: [Sigma](#)

### 3. Rule Syntax

Detection and response rules in Lima Charlie follow a straightforward syntax:

Detection and Response

25 Jan 2024 · 8 Minutes to read · Contributors

Filter

> GETTING STARTED

> TELEMETRY

> DETECTION AND RESPONSE

> LIMACHARLIE

QUERY

LANGUAGE

> MANAGED

RULESETS

> REFERENCE

DETECTING RELATED EVENTS

DETECTION ON ALTERNATE

TARGETS

DETECTION AND

RESPONSE

EXAMPLES

FALSE POSITIVE RULES

SLEEPER DEPLOYMENT

WRITING AND TESTING RULES

applying the criteria ruleset costs 30.0 per endpoint per month

the rate of false positives is much lower

Share this

## A Basic Rule

Here's a rule that detects DNS requests to `example.com` and responds by reporting them within the organization with a category name `DNS Hit example.com`.

YAML

Copy

```
# Detection
event: DNS_REQUEST
op: is
path: event/DOMAIN_NAME
value: example.com

# Response
- action: report
  name: DNS Hit example.com
```

This rule will detect and respond to requests to `example.com` within 100ms of the `DNS_REQUEST` event occurring. It uses the `is` operator to assess if the given `value` can be found inside the `event` at the given `path`.

You can checkout the official documentation of Lima Charlie for In-depth knowledge for writing rules and also checkout the various add-on they have for rulesets like sigma, soteria, Soc prime and Snapattack.

If you want to try learn about the detection and response rule writing and its format with syntaxes. Follow the documentation provided by the [lima charlie](#)

LIMA CHARLIE

Home

Search

Filter

> TUTORIALS

WHAT IS LIMACHARLIE?

LIMACHARLIE CORE

CONCEPTS

QUICKSTART

> TELEMETRY

> DETECTION AND RESPONSE

> LIMACHARLIE

QUERY

LANGUAGE

LimaCharlie Query Language

Updated on 07 Feb 2024 · 5 Minutes to read · Contributors

Print Share Dark

Beta Feature

LCQL is currently in Beta, and features may change in the future.

LimaCharlie Query Language (LCQL) provides a flexible, intuitive and interactive way to explore your data in LimaCharlie. Telemetry ingested via EDR sensors or adapters are searchable via LCQL, and can be searched en masse. Sample use cases for LCQL include:

Explore the existing rules and see how the rules are written and what format is been used

Neil Labs

Search Neil Labs for sensors / indicators...

Organizations Add-ons Support

Back to Neil Labs

MANAGED D&R RULES New Rule

Untitled-1

A Member Was Added To A Secur...

AD Privileged Users Or Groups...

APT29

Abusing Findstr For Defense E...

Account Tampering - Suspiciou...

Active Directory Replication ...

Application Whitelisting Bypa...

Backup Catalog Deleted

Cmd Stream Redirection

CobaltStrike Service Installa...

CobaltStrike Service Installa...

Credential Dumping Tools Serv...

Credential Dumping Tools Serv...

DC Shadow Copy

attack.t1000.006

attack.t1569.002

attack.s0005

Detect

6

rules:

7

- case sensitive: false

8

op: is

9

path: event/EventData/provider\_name

10

value: Service Control Manager

11

- case sensitive: false

12

op: is

13

path: event/EventData/eventid

14

value: '7045'

15

- op: or

16

rules:

17

- case sensitive: false

18

op: contains

19

path: event/EventData/imagepath

20

value: cachedump

21

- case sensitive: false

22

op: contains

23

path: event/EventData/imagepath

Expand

Op Reference

- and/or
- is
- exists
- contains
- starts with
- ends with
- is greater than
- is lower than
- matches
- string distance
- is :platform:
- is tagged
- lookup
- scope

Respond

1

- action: report

2

metadata:

3

author: >-

4

Florian Roth (Nextron Systems), Teymur Kheirkhabarov, Daniil Yugoslavskiy,

5

oscd.community

6

description: >-

You are unable to edit, delete or save a Managed Rule. Feel free to copy and edit this content within a Custom Rule.

4. Ruleset

MARKETPLACE

Featured

Extensions BETA

API

Lookups

Rulesets

Services

PERSONAL

Published

Access Token

Rulesets

Subscribe to managed rulesets in one click and start receiving detections right away.

generic-macos

Ruleset for detecting generic suspicious behaviors on MacOS.

Free

sigma

This service provides a core set of the open source Sigma rules in a managed fashion.

Free

snapattack-community

SnapAttack Community Rules

Free

socprime

Apply rules directly from content lists in SOC Prime.

Free

soteria-rules

Managed rule set by Soteria.

50¢ / vSensor / Month

Here the ruleset which you can use for detection and response, some of them are paid. By subscribing to the ruleset you can have those sets added to your alert system or DR system. All these are capable rulesets and offers a comprehensive idea about the detection and response process.

With the help of these ruleset you can have a functioning detection and response engine.

Note:- these ruleset are great they can help you to find and detect malicious activity inside the environment but they do not come with or likely don't all come with integrated response capabilities.

## 5. Managing Rules

Users can manage their detection and response rules within the Lima Charlie interface:

- **Creating Rules:** Users can create new rules by specifying conditions and actions.
- **Editing Rules:** Existing rules can be edited to update conditions or actions as needed.
- **Enabling/Disabling Rules:** Rules can be enabled or disabled based on current requirements.
- **Deleting Rules:** Unnecessary rules can be deleted to maintain a clean rule set.

## 6. Best Practices

When creating detection and response rules in Lima Charlie, consider the following best practices:

- **Be Specific:** Define precise conditions to minimise false positives and accurately identify threats.
- **Regular Review:** Regularly review and update rules to adapt to evolving threats and changes in the environment.
- **Testing:** Test rules in a controlled environment before deploying them to production to ensure they function as intended.
- **Collaboration:** Encourage collaboration among security teams to share knowledge and improve rule effectiveness.

## 7. Best Practices

When creating and managing detection and response rules in Lima Charlie, consider the following best practices:

- **Use Sigma Rules:** Leverage Sigma rules to benefit from community-developed and tested detection capabilities.
- **Regular Review:** Regularly review and update rules, including Sigma rules, to adapt to evolving threats.
- **Testing:** Test rules in a controlled environment before deploying them to production to ensure they function as intended.
- **Collaboration:** Encourage collaboration among security teams to share Sigma rule sets and improve overall threat detection.

Detection and response rules are fundamental to Lima Charlie's ability to detect and respond to security threats efficiently. By following the guidelines outlined in this documentation and leveraging the platform's capabilities, users can strengthen their security posture and better protect their assets.

---

This concludes the Lima Charlie Detection and Response Rules Documentation. After completing the installation and rules setup you're ready to go from an organisation with zero security to an organisation with 1000+ rules to detect and mitigate malware activity. For further assistance or inquiries, please refer to the Lima Charlie documentation or reach out to our support team.