# SOAR and EDR Homelab

## Objective

The Detection Lab project aimed to establish a controlled environment for simulating and detecting cyber attacks. The primary focus was to monitor and analyze data with LimaCharlie as a Endpoint Detection and Response (EDR) system, generating test telemetry to mimic real-world attack scenarios with the HackingTool ‘LaZagne’. This hands-on experience was designed to deepen understanding of credential security, attack patterns, and defensive strategies.

### Skills Learned

- Advanced understanding of EDR concepts and practical application.

- Proficiency in analyzing and monitoring data.

- Enhanced knowledge of network protocols and security vulnerabilities.

- Development of critical thinking and problem-solving skills in cybersecurity.

### Tools Used

- LimaCharlie as an EDR.

- Tines as a SOAR.

- Slack as a communication program.

- Windows 10 2022 as a Server.

## Construction

Step 1:

Download LimaCharlie Sensor. Connect LimaCharlie over the Powershell with the Server like so:

.\hcp\_win\_x64\_release\_4.29.0.exe -i < insert here installation key from limacharlie >

Then Implement HackTool in Server.

Ein Bild, das Text, Screenshot, Diagramm, Reihe enthält.

Automatisch generierte Beschreibung

Step 2:

Create Automation rule for detecting the preferred HackTool like so:

events:

- NEW\_PROCESS

- EXISTING\_PROCESS

op: and

rules:

- op: is windows

- op: or

rules:

- case sensitive: false

op: ends with

path: event/FILE\_PATH

value: lazagne.exe

- case sensitive: false

op: ends with

path: even/COMMAND\_LINE

value: all

- case sensitive: false

op: contains

path: event/COMMAND\_LINE

value: lazagne

- case sensitive: false

op: is

path: event/HASH

value: 467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486’

Step 3:

Create a Slack Channel and a Tines Playbook. Ein Bild, das Text, Diagramm, Screenshot, Plan enthält.

Automatisch generierte Beschreibung

Step 4:

Build your Tines playbook.

Ein Bild, das Screenshot, Text, Diagramm, Design enthält.

Automatisch generierte Beschreibung

Step 5:

Connect the Tines Playbook via credentials with LimaCharlie and slack and test it in Tines.

Ein Bild, das Diagramm, Screenshot, Text enthält.

Automatisch generierte Beschreibung

Full example of Construction:

Ein Bild, das Text, Diagramm, Plan, Screenshot enthält.

Automatisch generierte Beschreibung