

LimaCharlie-Tines EDR Automation Project Documentation

1. Project Overview

This project demonstrates how to set up a fully automated Security Orchestration, Automation, and Response (SOAR) system. Using LimaCharlie as the Endpoint Detection and Response (EDR) platform, combined with Tines for orchestrating automated workflows, the system detects LaZagne, a password recovery tool, and triggers alerts in Slack and email. Depending on user input, the system isolates the infected machine.

2. Project Architecture

- **LimaCharlie:** Acts as the EDR to detect threats.
 - **Tines:** Orchestrates the alerting and decision-making processes.
 - **Slack:** Used as an alert notification channel.
 - **Email:** Additional alert notification channel.
 - **Windows 10 VM:** Configured as a LimaCharlie agent for threat detection.
-

3. Steps to Setup the EDR Environment

3.1 LimaCharlie Setup

1. **Create a LimaCharlie Account:** Sign up at [LimaCharlie.io](https://limacharlie.io).
2. **Install LimaCharlie on a Windows 10 VM:**
 - Download and install the LimaCharlie agent files on a Windows 10 VM.
 - Configure the VM to act as a LimaCharlie agent, allowing it to monitor for any suspicious activity.


3.2 Detection Rule for LaZagne

1. **Download LaZagne:** Install the LaZagne tool on the same Windows 10 VM to simulate a red team scenario.


desktop-98b0o8q.lan 

Sensor Details

Hostname

desktop-98b0o8q.lan 

Network Access

Allowed  Isolate From Network


Seal Status

Not Sealed  Seal

Last Time Alive

2024-09-08 22:23:27 


External IP

104.177.1.115 


Sensor ID

00322923-c597-44cf-aeb0-961f55ec01cb 

Installer ID

66ccfdcf-c72a-4d90-a93a-26772428104b 

Platform

 Windows x86 64 bit

Kernel

Available


Enrollment Date

2024-09-08 22:23:22 


Internal IP

10.0.2.15 

Mac Address

08-00-27-90-62-7F 

Organization ID

c281bee5-ea62-426e-9502-d43ac2e5c246 

Device ID

N/A

Tags

Select tags...


Update Tags

2. Create a Detection and Response (D&R) Rule:

- In LimaCharlie, create a rule to detect LaZagne activity (such as processes or file signatures).
- Verify that LimaCharlie logs and detects the LaZagne event.


Detect

```
3 - EXISTING_PROCESS
4 op: and
5 rules:
6 - op: is windows
7 - op: or
8   rules:
9     - case sensitive: false
10     op: ends with
11     path: event/FILE_PATH
12     value: LaZagne.exe
13   - case sensitive: false
14     op: contains
15     path: event/CMDLINE
16     value: LaZagne
17   - case sensitive: false
18     op: is
19     path: event/HASH
20     value: '3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05'
```

Expand 

Respond

```
1 - action: report
2 metadata:
3   author: MyDFIR
4   description: TEST - Detects Lazagne Usage
5   falsepositives:
6     - ToTheMoon
```

Expand 

Comment

Add comment here. Comments are not included in detection content when an alert is triggered.

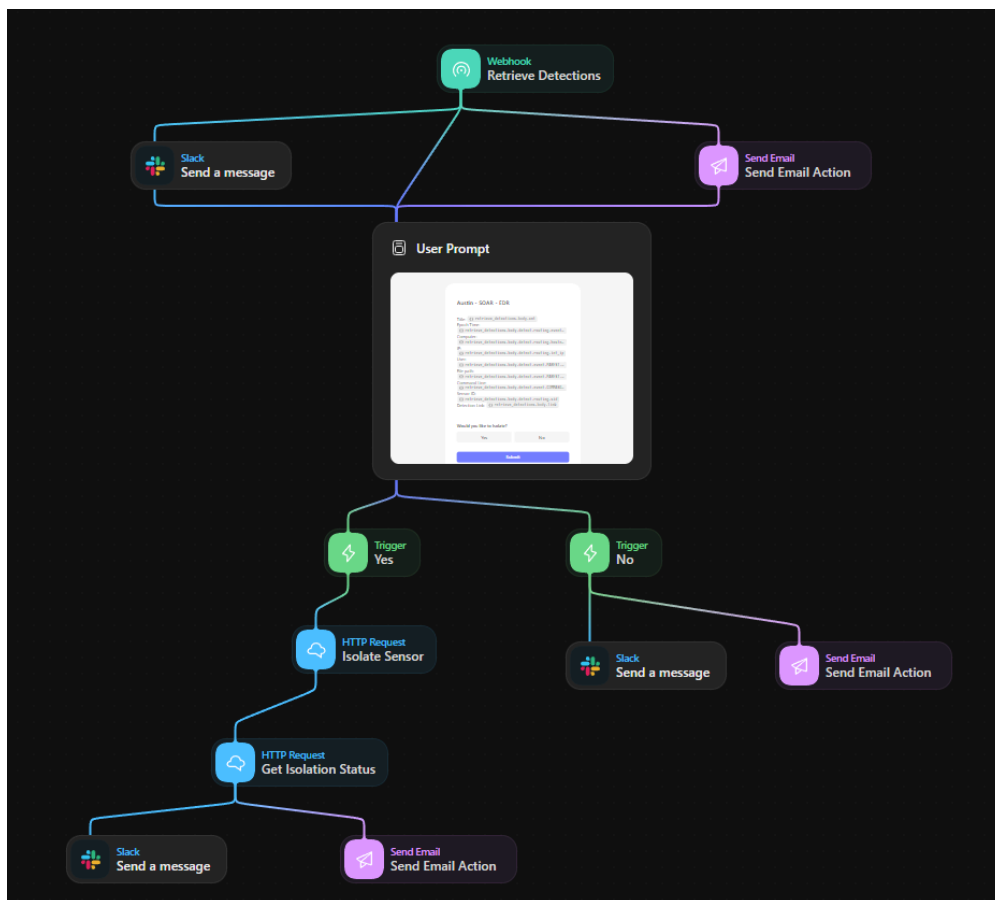
Save Rule

Discard Draft

4. Automating the Response Using Tines

4.1 Tines Integration

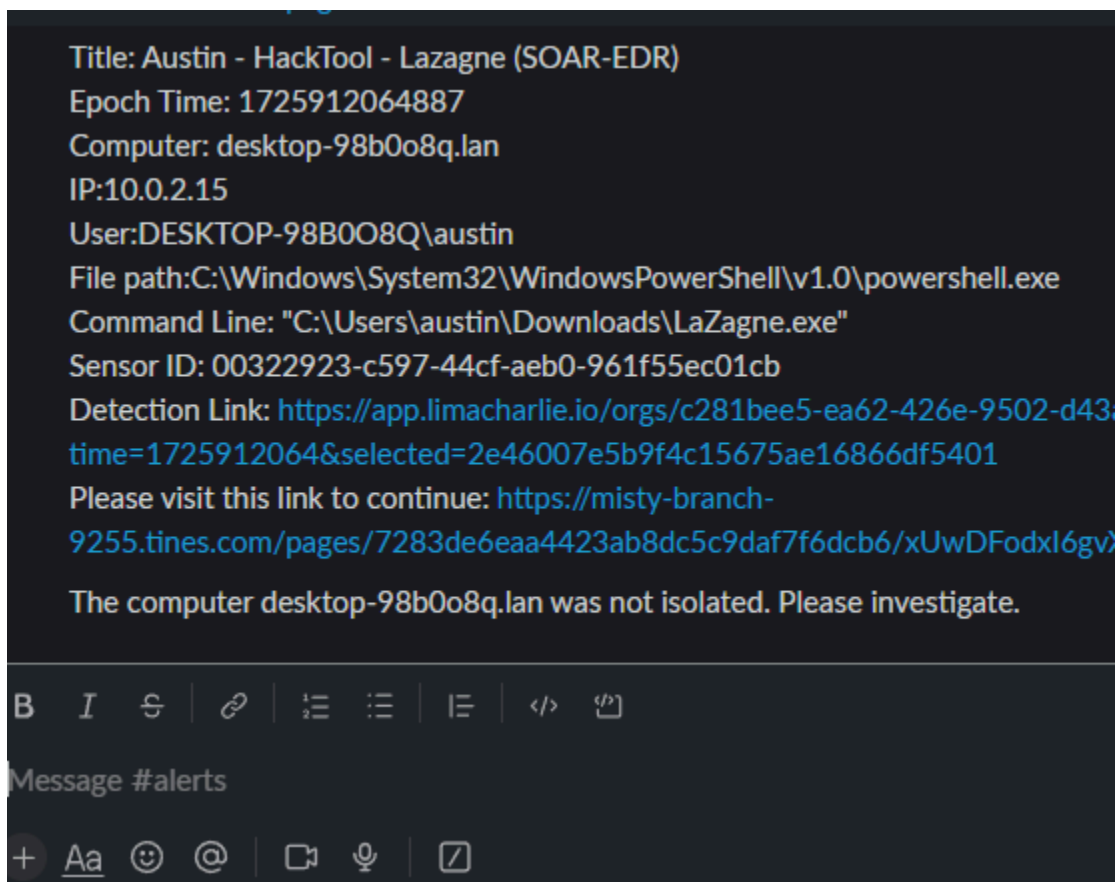
1. **Set Up Tines:**
 - Create an account in Tines.
 - Link Tines with LimaCharlie to automate alert and response workflows.
2. **Create the SOAR Workflow:**
 - Build an automation playbook in Tines that sends alerts to Slack and email when LaZagne is detected by LimaCharlie.
 - Include a user decision point: Ask the user whether they want to isolate the infected machine.



5. Alerting System

5.1 Slack Alerts

1. **Create a Slack Channel:** Set up a Slack channel to receive the automated alerts.
2. **Link Slack with Tines:** When LaZagne is detected, send detailed alert messages to Slack with the following information:
 - Time of detection
 - Computer name
 - Source IP address
 - Process and command line data
 - A link to Tines for user action



5.2 Email Alerts

1. **Configure Email Notifications:** Set up an email workflow in Tines to receive alerts along with the details outlined above.
2. **Alert Structure:** Email messages include links to Tines where users can choose to isolate the machine or investigate further.

Security Alert Inbox x



Austin <mail@tines.io>

to me ▼

Title: Austin - HackTool - Lazagne (SOAR-EDR)

Epoch Time: 1725851831080

Computer: desktop-98b0o8q.lan

IP: 10.0.2.15

User: DESKTOP-98B0O8Q\Austin

File path: C:\Users\Austin\Downloads\LaZagne.exe

Command Line: "C:\Users\Austin\Downloads\LaZagne.exe"

Sensor ID: 00322923-c597-44cf-aeb0-961f55ec01cb

Detection Link: <https://app.limacharlie.io/orgs/c281bee5-ea62-426e-9502-d43ac2ef>

Please visit this link to continue: <https://misty-branch-9255.tines.com/pages/7283de>

6. Incident Response Options

6.1 User Decision to Isolate the Machine

1. **Prompt for Isolation:** The Tines workflow asks the user if they wish to isolate the machine.
 - If **Yes**, LimaCharlie automatically isolates the infected machine.
 - If **No**, a message is sent to notify the user to investigate further.
2. **Response Update:**
 - A confirmation message is sent to both Slack and email, providing the status of the machine (isolated or not isolated).

6.2 Machine Isolation via LimaCharlie

1. **Automated Isolation:**
 - If isolation is confirmed, LimaCharlie performs the isolation, cutting off the infected machine from the network.
2. **Isolation Status Update:**
 - A message with the isolation status is sent to both Slack and email, notifying the team that the machine is now isolated.

Austin - SOAR - EDR

Title: Austin - HackTool - Lazagne (SOAR-EDR)
Epoch Time: 1725839090159
Computer: desktop-98b0o8q.lan
IP:10.0.2.15
User:DESKTOP-98B0O8Q\Austin
File path:C:\Users\Austin\Downloads\LaZagne.exe
Command Line: "C:\Users\Austin\Downloads\LaZagne.exe"
Sensor ID: 00322923-c597-44cf-aeb0-961f55ec01cb
Detection Link: <https://app.limacharlie.io/...f2>

Isolate?

Yes

No

Submit


7. Testing and Results

After setting up the system, test the integration by running LaZagne on the Windows 10 VM. Observe the following:



1. Detection of LaZagne by LimaCharlie.
2. Automated alert generation to Slack and email.
3. User prompt in Tines asking whether to isolate the machine.
4. Machine isolation (if selected) and notification of isolation status.


desktop-98b0o8q.lan ✓

Sensor Details

Hostname
desktop-98b0o8q.lan 

~~Network Access~~

 Isolated  Rejoin Network

Seal Status
Not Sealed  Seal

Alert Inbox x



A Schultz <mail@tines.io>

to me ▼

Isolation Status: true

The computer desktop-98b0o8q.lan was isolated.

8. Conclusion

This project highlights how a SOAR system using LimaCharlie and Tines can automate threat detection and incident response, providing real-time alerts and enabling quick decision-making in security operations. The combination of EDR and orchestration ensures a faster and more efficient incident response process, minimizing potential damage from security breaches.

Demo: [SOAR-EDR-DEMO](#)
