SOAR-EDR Automation Project using LimaCharlie, Tines, and Slack

PROJECT TITLE:

Automated Detection and Response for Credential Access Tools (LaZagne) using SOAR-EDR

OBJECTIVE:

To design and implement a SOAR-based automated incident response system that detects credential-dumping tools using LimaCharlie EDR and performs automated alerting via Tines and Slack.

TOOLS USED:

- LimaCharlie (EDR)
- Tines (SOAR)
- Slack (Alerting)
- Email (Notification)
- Windows Endpoint (Victim Machine)

LimaCharlie (EDR)
LimaCharlie is an Endpoint Detection and Response tool.
It continuously monitors the endpoint (Windows machine) for suspicious activities like malicious processes, command execution, or credential dumping tools (e.g., LaZagne).
When a threat is detected, it generates an alert and can also perform response actions such as isolating the system.

Tines (SOAR)

Tines is a Security Orchestration, Automation, and Response platform.
It receives alerts from LimaCharlie through webhooks, processes the detection data, and automates response actions such as sending alerts, requesting analyst input, and triggering containment workflows.

Slack (Alerting)

Slack is used as a real-time alerting and communication platform.
When a security incident occurs, Tines sends a detailed alert message to a Slack channel so that security analysts can quickly view the incident details and take action.

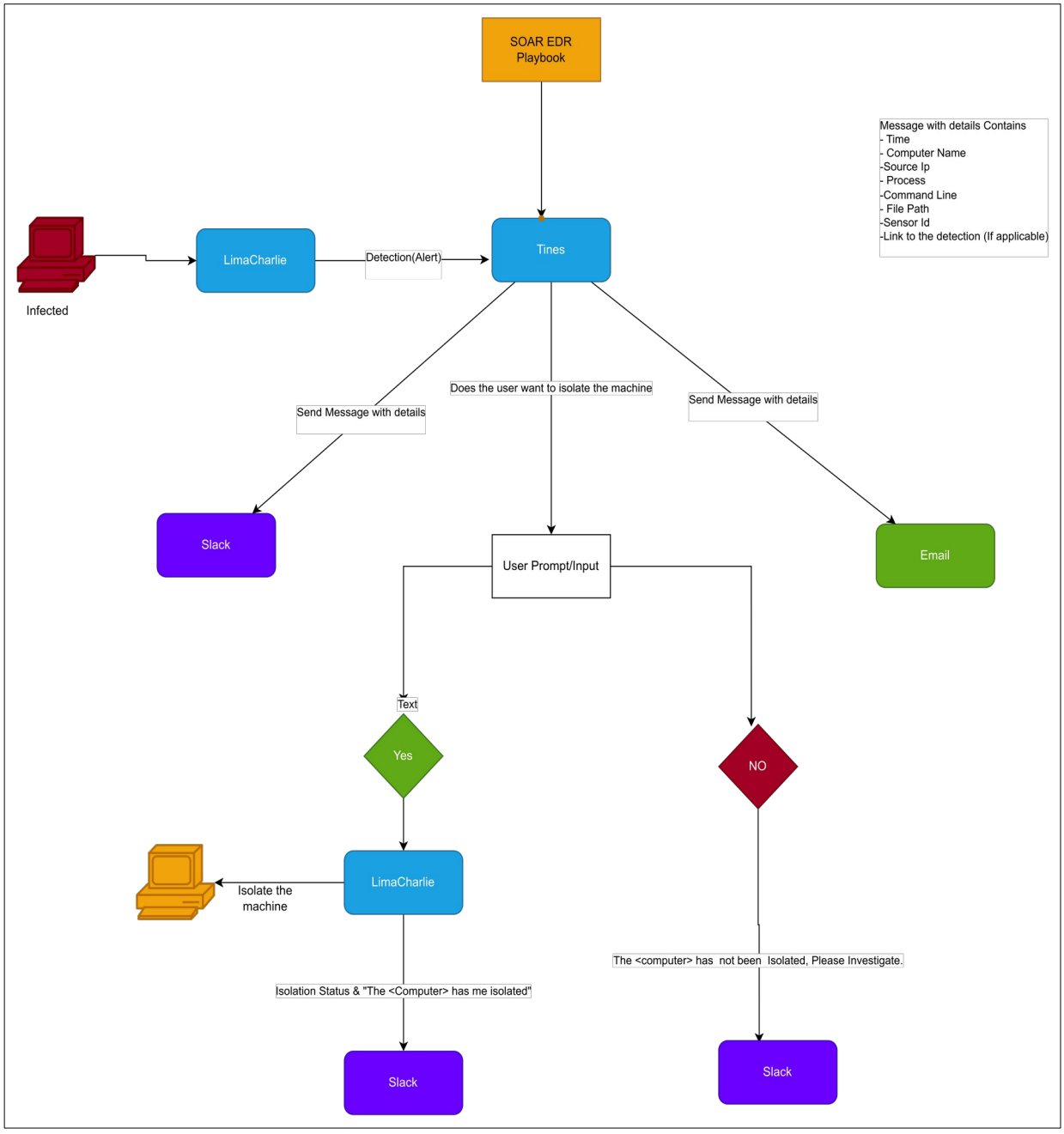
Email (Notification)

Email is used for formal and backup notification.
Tines sends an email containing incident details to ensure alerts are delivered even if Slack is missed, and for maintaining incident records or escalation.

Windows Endpoint (Victim Machine)

The Windows endpoint is the system being monitored.
It is where the malicious activity (such as running LaZagne) occurs, and where the LimaCharlie sensor is installed to detect and report suspicious behavior.

FLOW_CHART



PROJECT OVERVIEW:

This project detects the execution of LaZagne (a credential dumping tool) on a Windows endpoint. Once detected by LimaCharlie, the alert is sent to Tines via webhook, processed, and notifications are sent automatically to Slack and Email.

WORKFLOW OVERVIEW:

1. Endpoint executes LaZagne

2. LimaCharlie detects malicious behavior

3. Detection rule triggers

4. Alert forwarded to Tines via webhook

5. Tines parses detection data

6. Slack and Email notifications sent

STEP-BY-STEP IMPLEMENTATION:

STEP 1: Create LimaCharlie Account

- Sign up at https://limacharlie.io

- Create organization

- Deploy sensor on Windows machine

STEP 2: Create Detection Rule in LimaCharlie

- Detect NEW_PROCESS or EXISTING_PROCESS

- Match LaZagne.exe by file path, command line, or hash

- Set severity to HIGH

- Tag with ATTACK: Credential Access

STEP 3: Configure SOAR-EDR Output

- Enable SOAR-EDR output in LimaCharlie

- Set destination webhook (Tines webhook URL)

STEP 4: Create Tines Account

- Sign up at https://tines.com

- Create a new Story

- Add Webhook action (Retrieve Detection)

STEP 5: Parse Detection Data in Tines

- Use retrieve_detection.body fields

- Extract hostname, IP, user, file path, command line

STEP 6: Slack Integration

- Create Slack workspace

- Install Tines app

- Add Slack Send Message action

- Map detection fields into Slack message

STEP 7: Email Notification

- Add Send Email action in Tines

- Configure recipient, subject, and body

- Include detection details

ALGORITHM (DETECTION & RESPONSE):

1. Start

2. Monitor endpoint processes

3. IF process == LaZagne.exe THEN

4. Trigger detection rule

5. Send alert to Tines webhook

6. Parse JSON payload

7. Send Slack alert

8. Send Email alert

9. End

EXPECTED OUTPUT:

- Slack alert in #alerts channel

- Email notification to SOC analyst

- Logged incident in LimaCharlie

SECURITY MAPPING:

MITRE ATT&CK:

- T1003: Credential Dumping

REFERENCES:

- LaZagne Tool: https://github.com/AlessandroZ/LaZagne

- LimaCharlie Docs: https://docs.limacharlie.io

- Tines Docs: https://docs.tines.com

- Slack API: https://api.slack.com

CONCLUSION:

This project demonstrates a real-world SOAR-EDR automation pipeline that reduces incident response time, improves visibility, and standardizes alerting.