Implementation of a Security Orchestration, Automation, and Response (SOAR) System

Objective: The primary goal of this project was to implement a Security Orchestration, Automation, and Response (SOAR) system using Tines as the SOAR platform and LimaCharlie as the Endpoint Detection and Response (EDR) solution. The focus was on automating the detection and response to security incidents, thereby improving the efficiency and effectiveness of the Security Operations Center (SOC).

Project Overview:

- **Tool Integration:** Tines was selected as the SOAR platform for its flexibility and ease of use, while LimaCharlie was chosen for its robust EDR capabilities. These tools were integrated to create a cohesive security automation framework.
- **Detection Rules Creation:** Custom detection rules were developed within LimaCharlie to monitor specific security events, such as unauthorized password recovery attempts on Windows machines. These rules were designed to proactively identify potential threats and trigger automated responses.
- **Playbook Design and Implementation:** Automated playbooks, referred to as "stories" in Tines, were designed and implemented to streamline the response process. These playbooks included actions such as sending real-time alerts via email and Slack, and providing the option to isolate compromised systems based on user input.

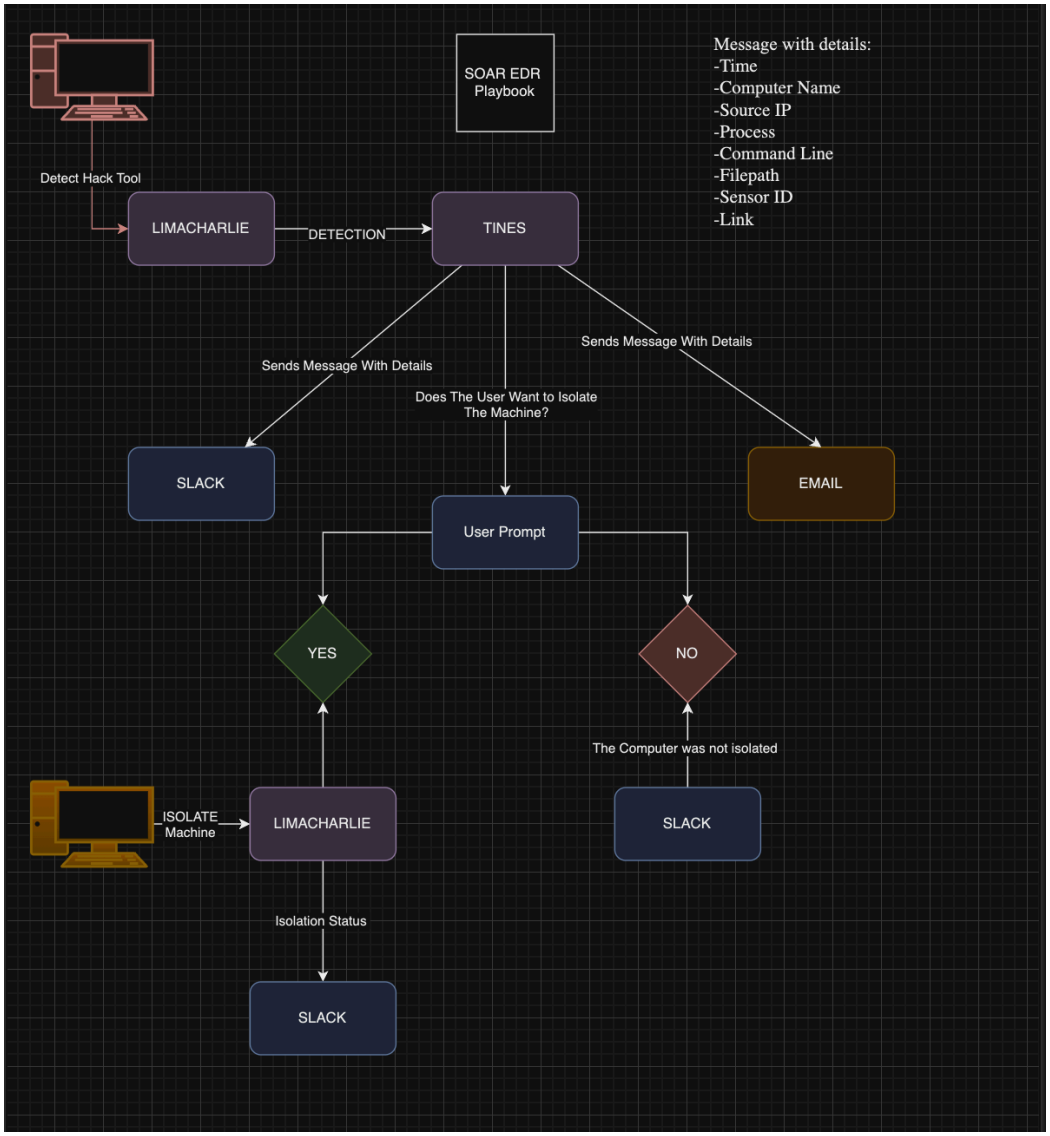
Process and Methodology:

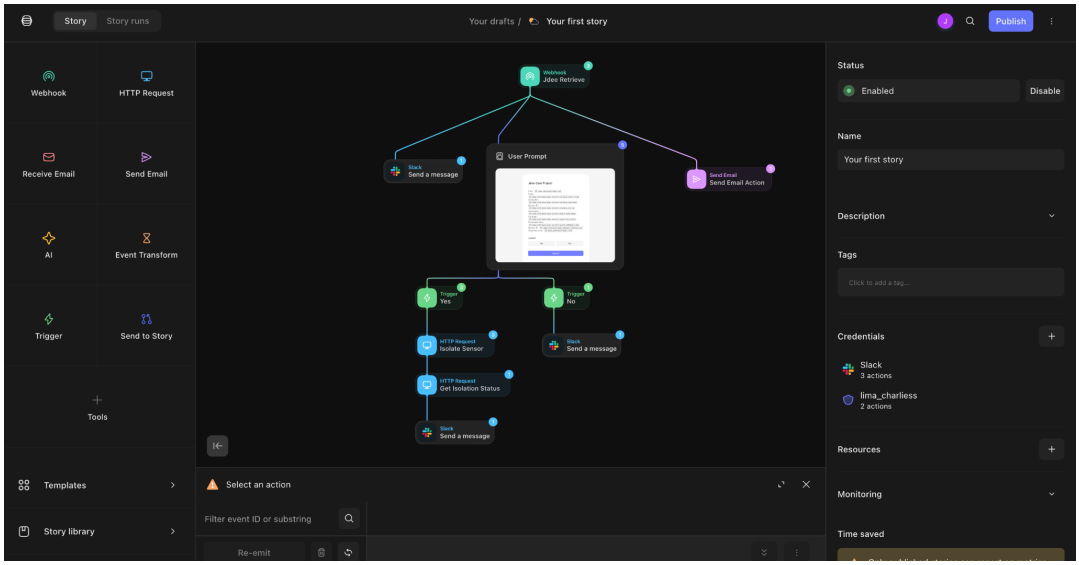
1. **Detection Rule Development:** The first step involved creating detection rules in LimaCharlie that could identify specific malicious activities. These rules were fine-tuned to minimize false positives and ensure accurate threat detection.
2. **SOAR Playbook Creation:** Once the detection rules were in place, the next step was to create automated playbooks in Tines. These playbooks were designed to execute a series of actions when a detection occurred, including sending alerts to security personnel and taking predefined remedial actions.
3. **Tool Integration and Testing:** The integration between LimaCharlie and Tines was tested extensively to ensure seamless communication between the EDR and SOAR platforms. The system was tested with various security scenarios to validate its effectiveness and reliability.
4. **Automation and Optimization:** The automated playbooks were continuously refined and optimized to improve response times and reduce manual intervention. This involved iterative testing and adjustment of the workflows to align with best practices in incident response.

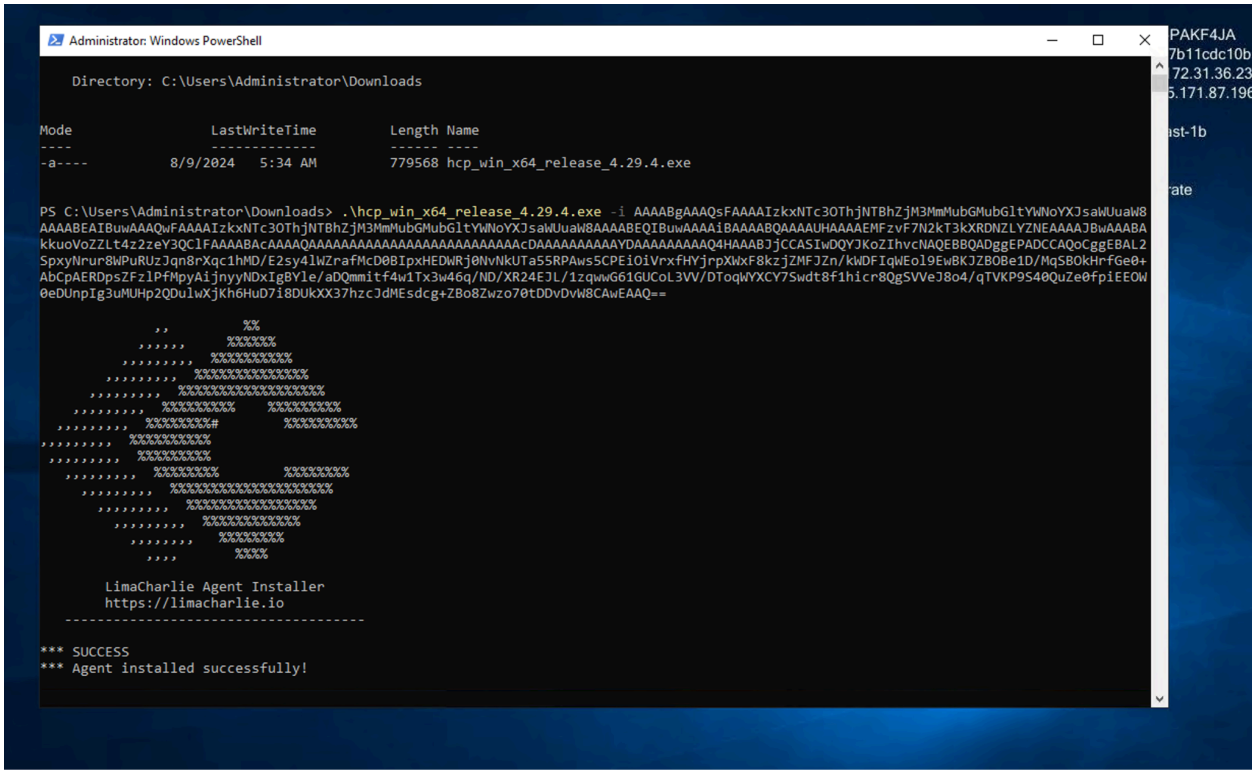
Outcomes and Benefits:

- **Enhanced SOC Efficiency:** The implementation of the SOAR system significantly reduced the time and effort required for security incident detection and response, allowing the SOC to focus on more strategic tasks.
- **Proactive Threat Management:** The custom detection rules and automated playbooks provided a proactive approach to threat management, ensuring that potential security incidents were addressed swiftly and effectively.
- **Scalability and Continuous Improvement:** The system was designed to be scalable, allowing for the addition of new detection rules and playbooks as the threat landscape evolves. Continuous improvement practices were embedded in the workflow to ensure the system remains effective over time.

Conclusion: This project successfully demonstrated the value of integrating SOAR and EDR platforms to enhance security operations. The automation of threat detection and response processes not only improved the efficiency of the SOC but also provided a scalable framework for ongoing security management. The hands-on experience gained from this project is expected to contribute significantly to the advancement of cybersecurity practices within the organization.


SOAR EDR Playbook
Message with details:
-Time
-Computer Name
-Source IP
-Process
-Command Line
-Filepath
-Sensor ID
-Link
Detect Hack Tool
LIMACHARLIE
DETECTION
TINES
Sends Message With Details
Does The User Want to Isolate The Machine?
Sends Message With Details
SLACK
User Prompt
EMAIL
YES
NO
The Computer was not isolated
ISOLATE Machine
LIMACHARLIE
SLACK
Isolation Status
SLACK


Story
Story runs
Your drafts / Your first story
Publish
Webhook
HTTP Request
Receive Email
Send Email
AI
Event Transform
Trigger
Send to Story
Tools
Templates
Story library
Webhook
Jdee Retrieve
Slack
Send a message
User Prompt
Send Email
Send Email Action
Trigger
Yes
Trigger
No
HTTP Request
Isolate Sensor
Slack
Send a message
HTTP Request
Get Isolation Status
Slack
Send a message
Select an action
Filter event ID or substring
Re-emit
Status
Enabled
Disable
Name
Your first story
Description
Tags
Click to add a tag...
Credentials
Slack
3 actions
lima_charliess
2 actions
Resources
Monitoring
Time saved



Sensor Details

Hostname
ec2amaz-pakf4ja.ec2.internal

Platform
Windows x86 64 bit

Network Access
Allowed | Isolate From Network

Kernel
Available

Seal Status
Not Sealed | Seal

Enrollment Date
2024-08-09 05:40:20

Last Time Alive
2024-08-09 05:40:26

Internal IP
172.31.36.237

External IP
35.171.87.196

Mac Address
0E-0B-B2-09-33-C5

Sensor ID
46432b13-ba07-4ea6-846b-c431799b75c4

Organization ID
c173bc5e-cdda-44f7-9174-433592d864d1

Installer ID
2492ea15-a196-4bb7-8cf6-cde637402945

Device ID
N/A

Tags
Select tags... | Update Tags

Detect

Expand

```
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: event/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"
```

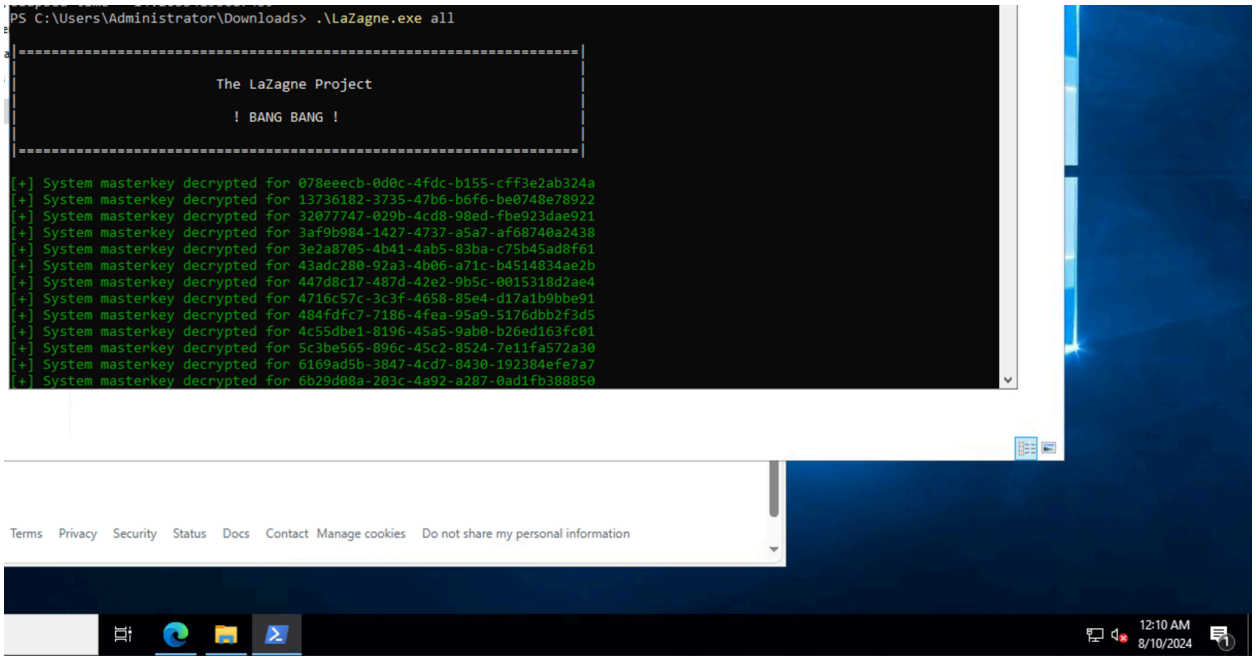
Respond

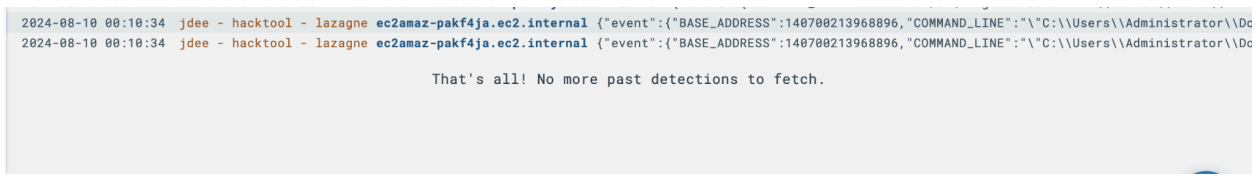
```
- action: report
  metadata:
    author: Jdee
    description: Detects Lazange(SOAR EDR TOOL)
    falsepositives:
    - To The Moon
    level: medium
    tags:
    - attack.credential_access
  name: jdee - hacktool - lazagne
```

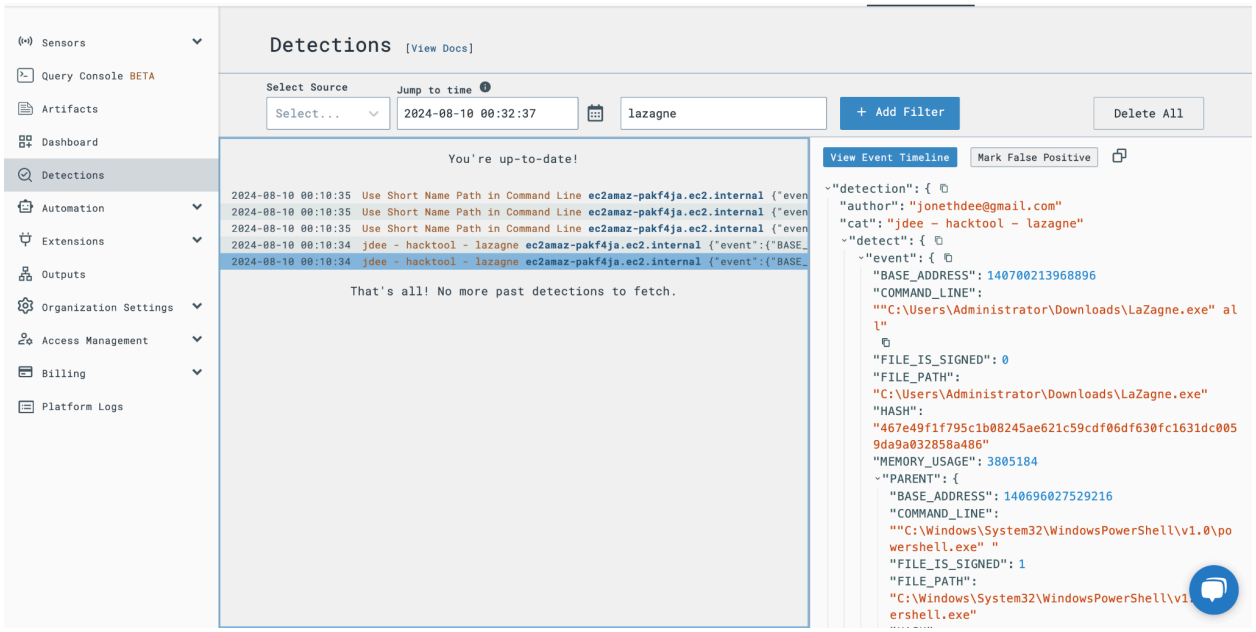
Test Event

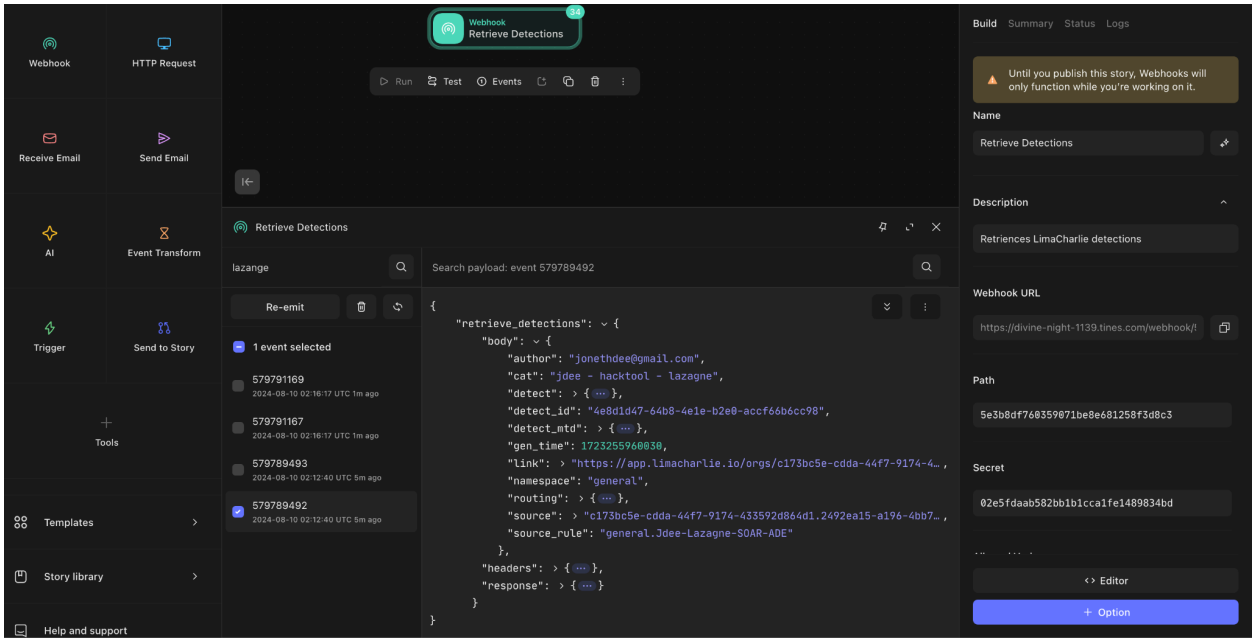
Match. 4 operations were evaluated with the following results:

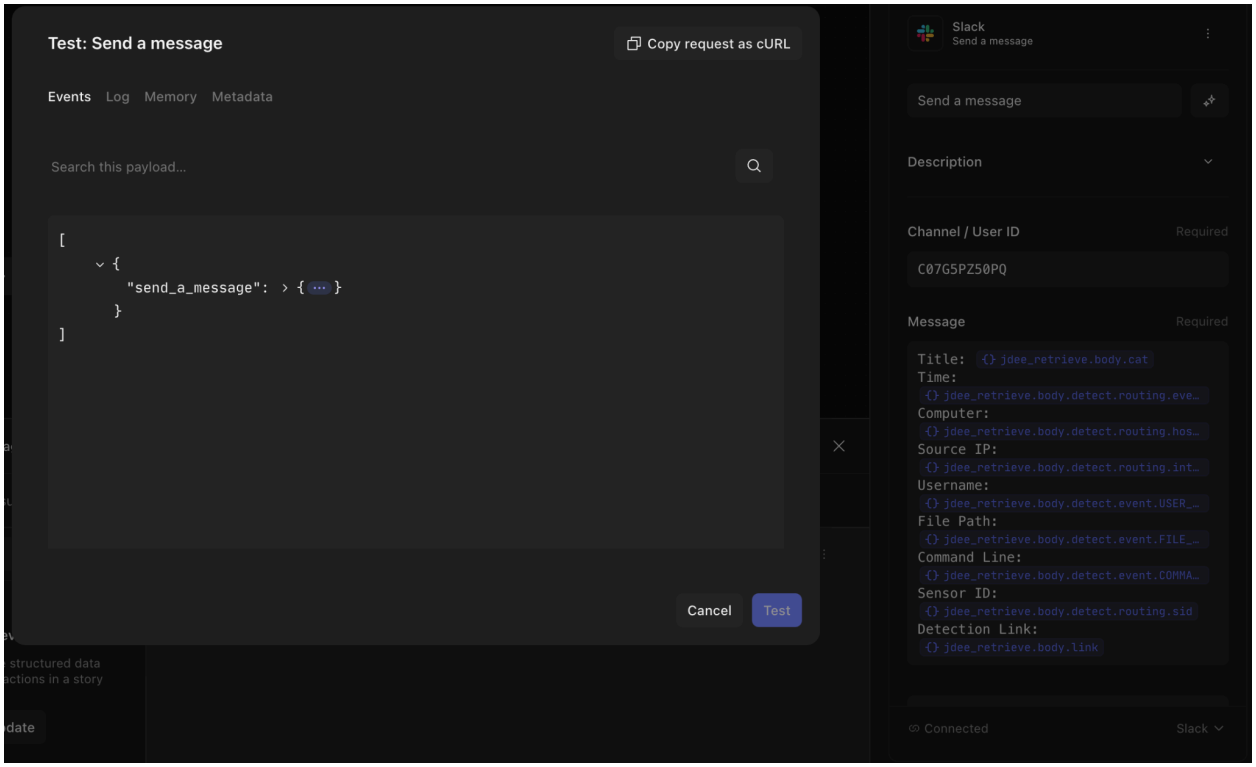
- true => (is windows) {"op":"is windows"}
- true => (~ends with) {"case sensitive":false,"op":"ends with","path":"event/FILE_PATH","value":"\\Lazagne.exe"}
- true => (or) {"op":"or","rules":[{"case sensitive":false,"op":"ends with","path":"event/FILE_PATH","value":"\\Lazagne.exe"},{"case sensitive":false,"op":"ends with","path":"event/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"}]}
- true => (and) {"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":"event/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"}]}]}

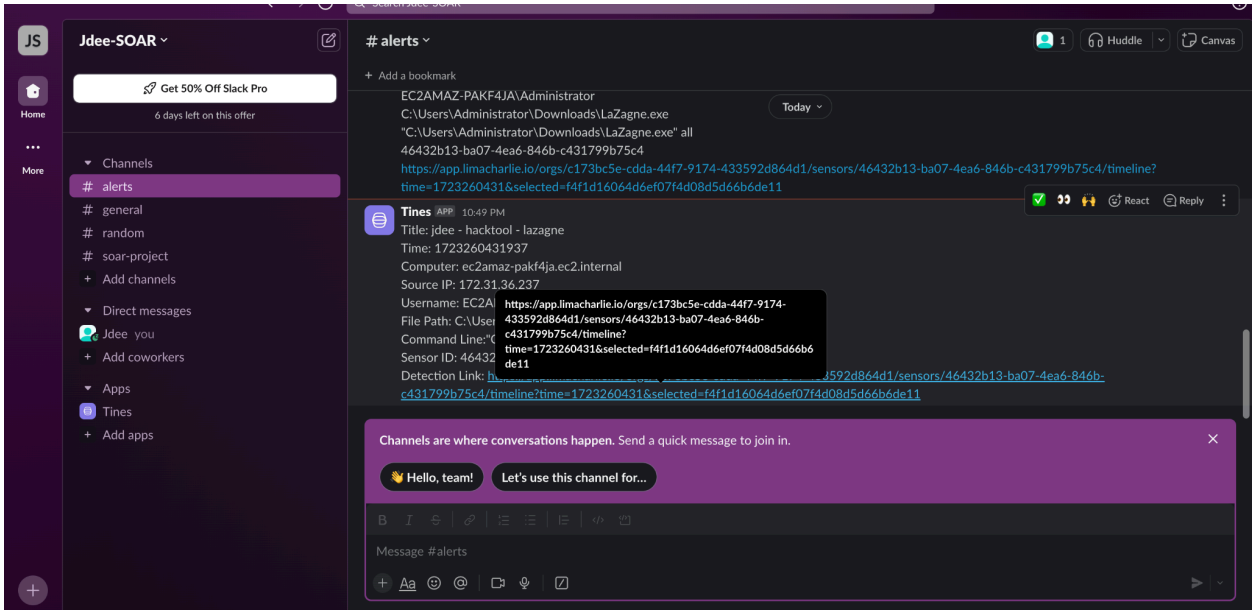

PS C:\Users\Administrator\Downloads> .\LaZagne.exe all
The LaZagne Project
! BANG BANG !
[+] System masterkey decrypted for 078eeecb-0d0c-4fdc-b155-cff3e2ab324a
[+] System masterkey decrypted for 13736182-3735-47b6-b6f6-be0748e78922
[+] System masterkey decrypted for 32077747-029b-4cd8-98ed-fbe923dae921
[+] System masterkey decrypted for 3af9b984-1427-4737-a5a7-af68740a2438
[+] System masterkey decrypted for 3e2a8705-4b41-4ab5-83ba-c75b45ad8f61
[+] System masterkey decrypted for 43adc280-92a3-4b06-a71c-b4514834ae2b
[+] System masterkey decrypted for 447d8c17-487d-42e2-9b5c-0015318d2ae4
[+] System masterkey decrypted for 4716c57c-3c3f-4658-85e4-d17a1b9bbe91
[+] System masterkey decrypted for 484fdfc7-7186-4fea-95a9-5176dbb2f3d5
[+] System masterkey decrypted for 4c55dbe1-8196-45a5-9ab0-b26ed163fc01
[+] System masterkey decrypted for 5c3be565-896c-45c2-8524-7e11fa572a30
[+] System masterkey decrypted for 6169ad5b-3847-4cd7-8430-192384efe7a7
[+] System masterkey decrypted for 6b29d08a-203c-4a92-a287-0ad1fb388850
Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information
12:10 AM
8/10/2024

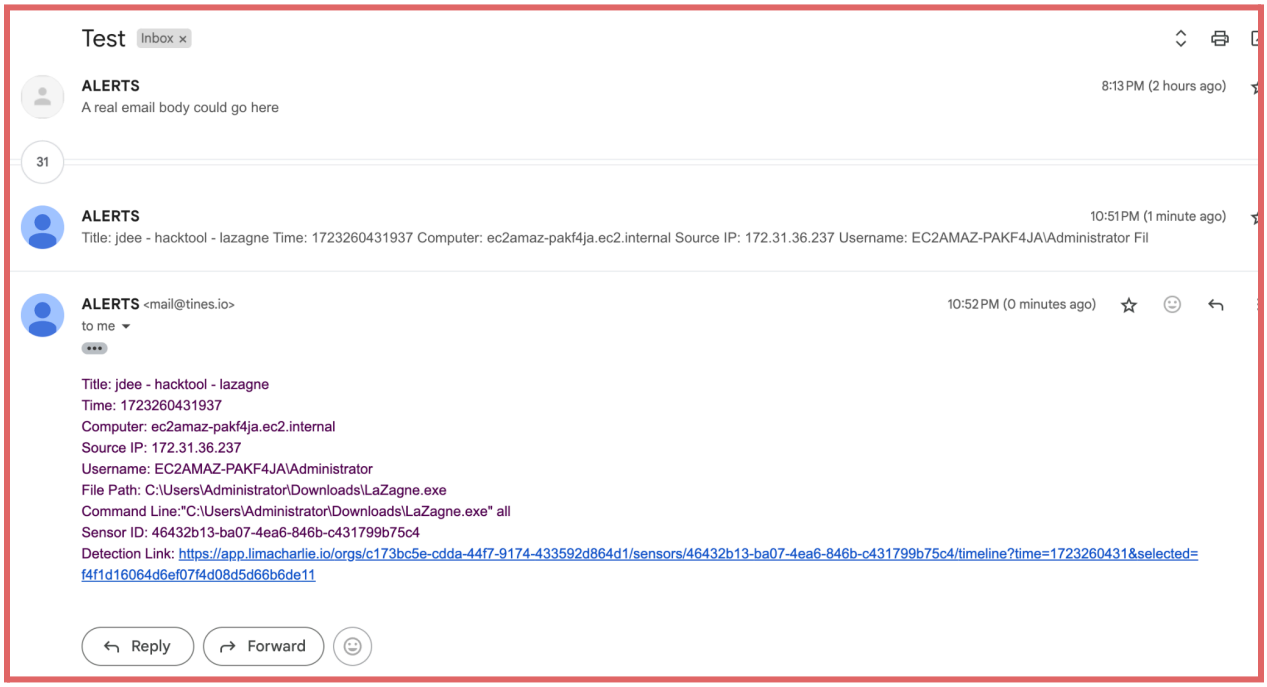

2024-08-10 00:10:34 jdee - hacktool - lazagne ec2amaz-pakf4ja.ec2.internal {"event":{"BASE_ADDRESS":140700213968896,"COMMAND_LINE":"\"C:\\Users\\Administrator\\Dc
2024-08-10 00:10:34 jdee - hacktool - lazagne ec2amaz-pakf4ja.ec2.internal {"event":{"BASE_ADDRESS":140700213968896,"COMMAND_LINE":"\"C:\\Users\\Administrator\\Dc
That's all! No more past detections to fetch.


Sensors
Query Console BETA
Artifacts
Dashboard
Detections
Automation
Extensions
Outputs
Organization Settings
Access Management
Billing
Platform Logs
Detections [View Docs]
Select Source
Select...
Jump to time
2024-08-10 00:32:37
lazagne
+ Add Filter
Delete All
You're up-to-date!
2024-08-10 00:10:35 Use Short Name Path in Command Line ec2amaz-pakf4ja.ec2.internal {"even
2024-08-10 00:10:35 Use Short Name Path in Command Line ec2amaz-pakf4ja.ec2.internal {"even
2024-08-10 00:10:35 Use Short Name Path in Command Line ec2amaz-pakf4ja.ec2.internal {"even
2024-08-10 00:10:34 jdee - hacktool - lazagne ec2amaz-pakf4ja.ec2.internal {"event":{"BASE_
2024-08-10 00:10:34 jdee - hacktool - lazagne ec2amaz-pakf4ja.ec2.internal {"event":{"BASE_
That's all! No more past detections to fetch.
View Event Timeline
Mark False Positive
"detection": {
"author": "jonethdee@gmail.com"
"cat": "jdee - hacktool - lazagne"
"detect": {
"event": {
"BASE_ADDRESS": 140700213968896
"COMMAND_LINE":
""C:\Users\Administrator\Downloads\LaZagne.exe" al
l"
"FILE_IS_SIGNED": 0
"FILE_PATH":
"C:\Users\Administrator\Downloads\LaZagne.exe"
"HASH":
"467e49f1f795c1b08245ae621c59cdf06df630fc1631dc005
9da9a032858a486"
"MEMORY_USAGE": 3805184
"PARENT": {
"BASE_ADDRESS": 140696027529216
"COMMAND_LINE":
""C:\Windows\System32\WindowsPowerShell\v1.0\po
wershell.exe" "
"FILE_IS_SIGNED": 1
"FILE_PATH":
"C:\Windows\System32\WindowsPowerShell\v1
ershell.exe"


Webhook
HTTP Request
Receive Email
Send Email
AI
Event Transform
Trigger
Send to Story
Tools
Templates
Story library
Help and support
Webhook
Retrieve Detections
Run
Test
Events
Retrieve Detections
lazange
Search payload: event 579789492
Re-emit
1 event selected
579791169
2024-08-10 02:16:17 UTC 1m ago
579791167
2024-08-10 02:16:17 UTC 1m ago
579789493
2024-08-10 02:12:40 UTC 5m ago
579789492
2024-08-10 02:12:40 UTC 5m ago
{
"retrieve_detections": {
"body": {
"author": "jonethdee@gmail.com",
"cat": "jdee - hacktool - lazagne",
"detect": { ... },
"detect_id": "4e8d1d47-64b8-4e1e-b2e0-accf66b6cc98",
"detect_mtd": { ... },
"gen_time": 1723255960030,
"link": "https://app.limacharlie.io/orgs/c173bc5e-cdda-44f7-9174-4...",
"namespace": "general",
"routing": { ... },
"source": "c173bc5e-cdda-44f7-9174-433592d864d1.2492ea15-a196-4bb7...",
"source_rule": "general.Jdee-Lazagne-SOAR-ADE"
},
"headers": { ... },
"response": { ... }
}
}
Build
Summary
Status
Logs
Until you publish this story, Webhooks will only function while you're working on it.
Name
Retrieve Detections
Description
Retrieves LimaCharlie detections
Webhook URL
https://divine-night-1139.tines.com/webhook/!
Path
5e3b8df760359071be8e681258f3d8c3
Secret
02e5fdaab582bb1b1cca1fe1489834bd
Editor
Option


Test: Send a message
Copy request as cURL
Events
Log
Memory
Metadata
Search this payload...
[
{
"send_a_message": { ... }
}
]
Cancel
Test
Slack
Send a message
Send a message
Description
Channel / User ID
Required
C07G5PZ50PQ
Message
Required
Title: jdee_retrieve.body.cat
Time:
jdee_retrieve.body.detect.routing.eve...
Computer:
jdee_retrieve.body.detect.routing.hos...
Source IP:
jdee_retrieve.body.detect.routing.int...
Username:
jdee_retrieve.body.detect.event.USER_...
File Path:
jdee_retrieve.body.detect.event.FILE_...
Command Line:
jdee_retrieve.body.detect.event.COMMA...
Sensor ID:
jdee_retrieve.body.detect.routing.sid
Detection Link:
jdee_retrieve.body.link
Connected
Slack


Jdee-SOAR
Get 50% Off Slack Pro
6 days left on this offer
Channels
alerts
general
random
soar-project
Add channels
Direct messages
Jdee you
Add coworkers
Apps
Tines
Add apps
alerts
Huddle
Canvas
Add a bookmark
Today
EC2AMAZ-PAKF4JA\Administrator
C:\Users\Administrator\Downloads\LaZagne.exe
"C:\Users\Administrator\Downloads\LaZagne.exe" all
46432b13-ba07-4ea6-846b-c431799b75c4
https://app.limacharlie.io/orgs/c173bc5e-cdda-44f7-9174-433592d864d1/sensors/46432b13-ba07-4ea6-846b-c431799b75c4/timeline?time=1723260431&selected=f4f1d16064d6ef07f4d08d5d66b6de11
Tines APP 10:49 PM
Title: jdee - hacktool - lazagne
Time: 1723260431937
Computer: ec2amaz-pakf4ja.ec2.internal
Source IP: 172.31.36.237
Username: EC2A
File Path: C:\Use
Command Line:"
Sensor ID: 4643
Detection Link:
https://app.limacharlie.io/orgs/c173bc5e-cdda-44f7-9174-433592d864d1/sensors/46432b13-ba07-4ea6-846b-c431799b75c4/timeline?time=1723260431&selected=f4f1d16064d6ef07f4d08d5d66b6de11
React
Reply
Channels are where conversations happen. Send a quick message to join in.
Hello, team!
Let's use this channel for...
Message #alerts


Test
Inbox ×
ALERTS
A real email body could go here
8:13 PM (2 hours ago)
31
ALERTS
Title: jdee - hacktool - lazagne Time: 1723260431937 Computer: ec2amaz-pakf4ja.ec2.internal Source IP: 172.31.36.237 Username: EC2AMAZ-PAKF4JA\Administrator Fil
10:51 PM (1 minute ago)
ALERTS <mail@tines.io>
to me
10:52 PM (0 minutes ago)
Title: jdee - hacktool - lazagne
Time: 1723260431937
Computer: ec2amaz-pakf4ja.ec2.internal
Source IP: 172.31.36.237
Username: EC2AMAZ-PAKF4JA\Administrator
File Path: C:\Users\Administrator\Downloads\LaZagne.exe
Command Line:"C:\Users\Administrator\Downloads\LaZagne.exe" all
Sensor ID: 46432b13-ba07-4ea6-846b-c431799b75c4
Detection Link: https://app.limacharlie.io/orgs/c173bc5e-cdda-44f7-9174-433592d864d1/sensors/46432b13-ba07-4ea6-846b-c431799b75c4/timeline?time=1723260431&selected=f4f1d16064d6ef07f4d08d5d66b6de11
Reply
Forward


Tines APP 11:03 PM
The Computer:
ec2amaz-pakf4ja.ec2.internal
was not isolated, please investigate

ec2amaz-pakf4ja.ec2.internal

Sensor Details

Hostname
ec2amaz-pakf4ja.ec2.internal

Platform
Windows x86 64 bit

Network Access
Isolated | Rejoin Network

Kernel
Available

Seal Status
Not Sealed | Seal

Enrollment Date
2024-08-09 05:40:20

Last Time Alive
2024-08-10 05:36:02

Internal IP
172.31.36.237

External IP
18.206.99.207

Mac Address
0E-0B-B2-09-33-C5

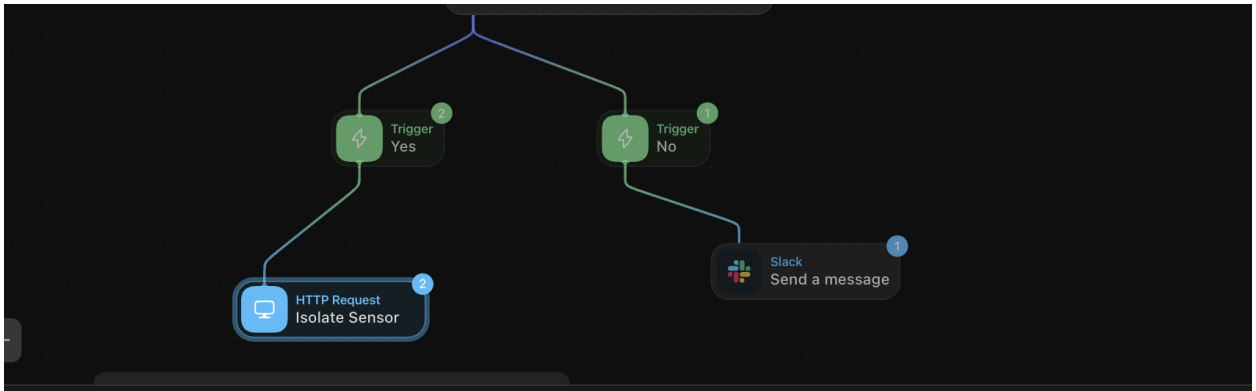
Sensor ID
46432b13-ba07-4ea6-846b-c431799b75c4

Organization ID
c173bc5e-cdda-44f7-9174-433592d864d1

Installer ID
2492ea15-a196-4bb7-8cf6-cde637402945

Device ID
N/A

Tags
Select tags... | Update Tags



Isolate Sensor

Search event ID or substring

Search payload: event 580075559

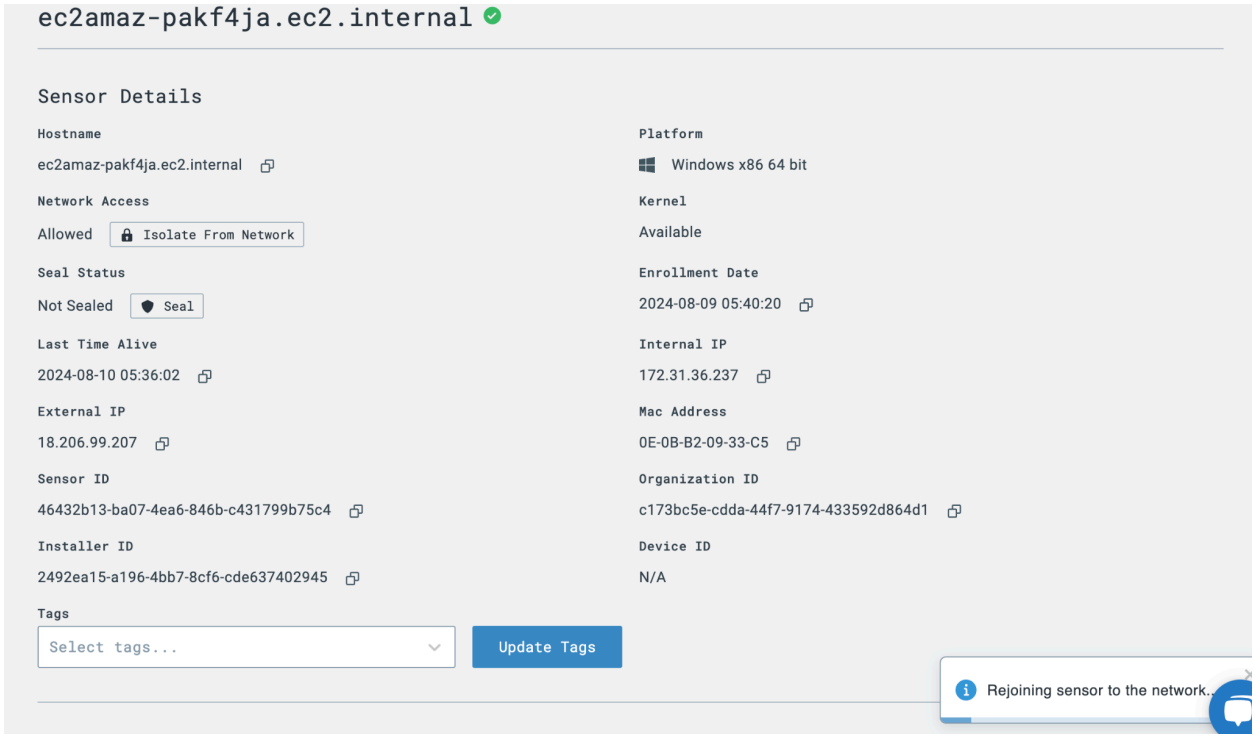
Re-emit

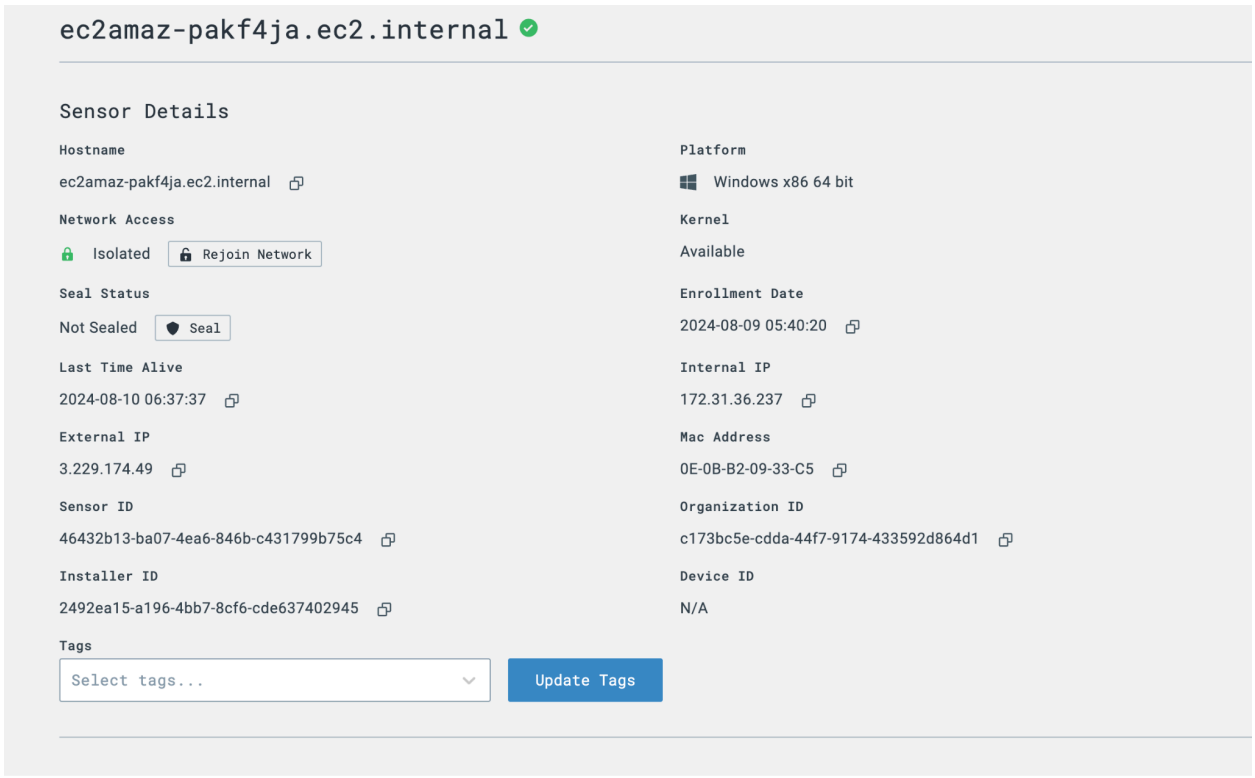
1 event selected

580075559
2024-08-10 06:19:33 UTC 1m ago

580071312
2024-08-10 06:08:15 UTC 12m ago


```
{
    "jdee_retrieve": > { ... },
    "user_prompt": > { ... },
    "yes": > { ... },
    "isolate_sensor": v {
        "body": > { ... },
        "headers": > { ... },
        "status": 200,
        "meta": > { ... }
      }
}
```


ec2amaz-pakf4ja.ec2.internal
Sensor Details
Hostname
ec2amaz-pakf4ja.ec2.internal
Platform
Windows x86 64 bit
Network Access
Allowed
Isolate From Network
Kernel
Available
Seal Status
Not Sealed
Seal
Enrollment Date
2024-08-09 05:40:20
Last Time Alive
2024-08-10 05:36:02
Internal IP
172.31.36.237
External IP
18.206.99.207
Mac Address
0E-0B-B2-09-33-C5
Sensor ID
46432b13-ba07-4ea6-846b-c431799b75c4
Organization ID
c173bc5e-cdda-44f7-9174-433592d864d1
Installer ID
2492ea15-a196-4bb7-8cf6-cde637402945
Device ID
N/A
Tags
Select tags...
Update Tags
Rejoining sensor to the network.


ec2amaz-pakf4ja.ec2.internal
Sensor Details
Hostname
ec2amaz-pakf4ja.ec2.internal
Platform
Windows x86 64 bit
Network Access
Isolated
Rejoin Network
Kernel
Available
Seal Status
Not Sealed
Seal
Enrollment Date
2024-08-09 05:40:20
Last Time Alive
2024-08-10 06:37:37
Internal IP
172.31.36.237
External IP
3.229.174.49
Mac Address
0E-0B-B2-09-33-C5
Sensor ID
46432b13-ba07-4ea6-846b-c431799b75c4
Organization ID
c173bc5e-cdda-44f7-9174-433592d864d1
Installer ID
2492ea15-a196-4bb7-8cf6-cde637402945
Device ID
N/A
Tags
Select tags...
Update Tags