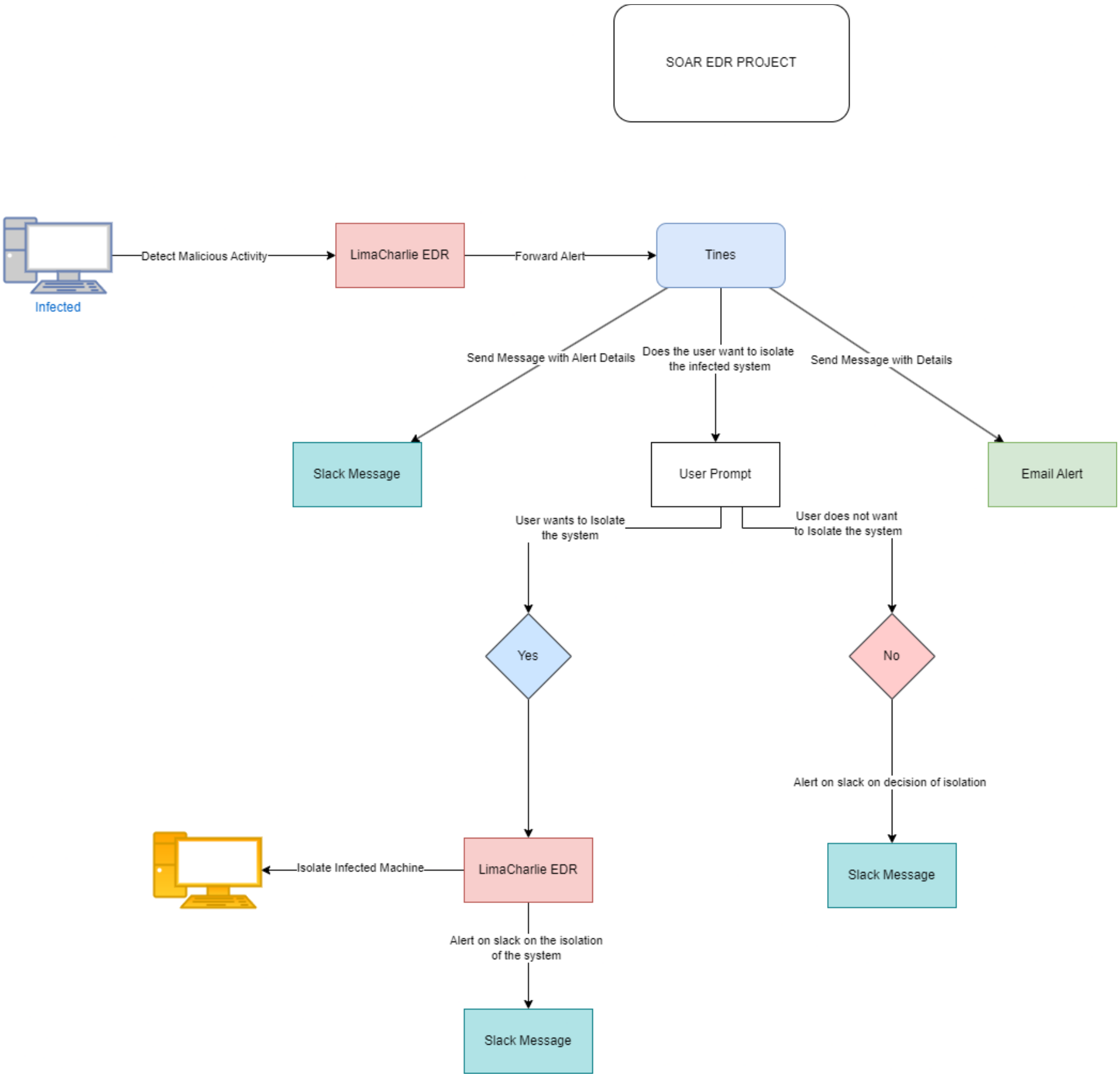
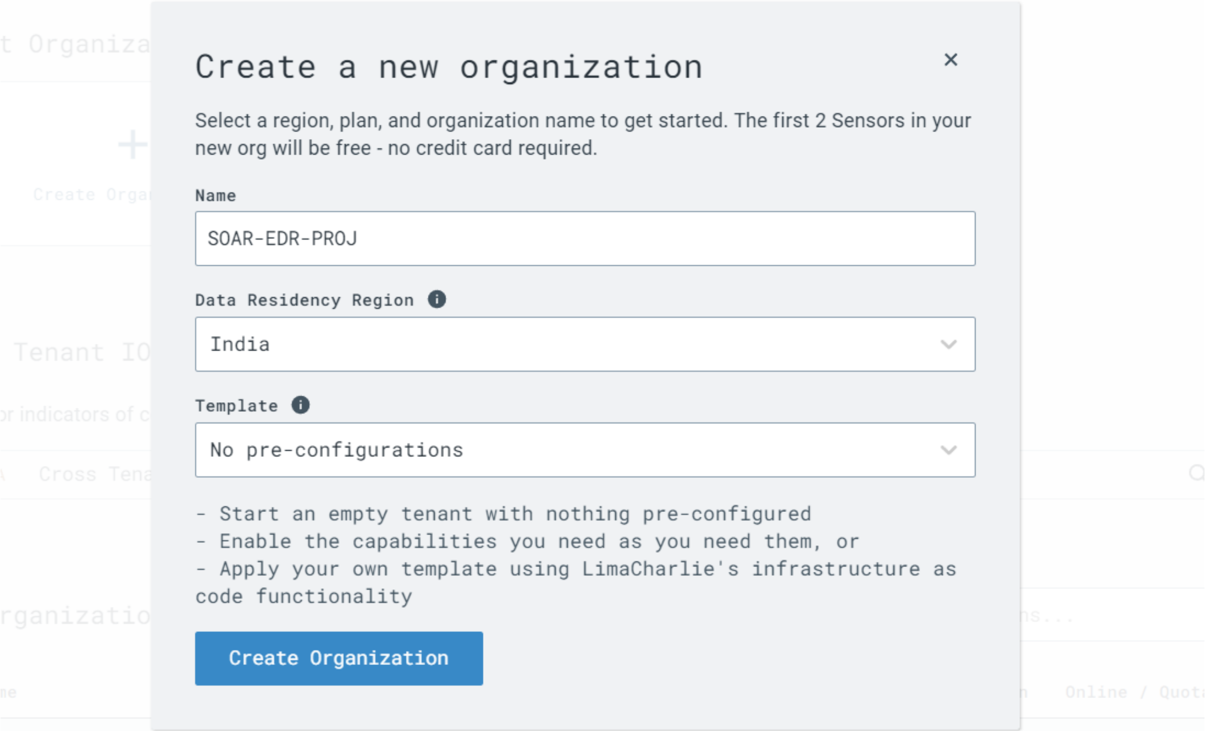
Workflow


SOAR EDR PROJECT
Infected
Detect Malicious Activity
LimaCharlie EDR
Forward Alert
Tines
Send Message with Alert Details
Does the user want to isolate the infected system
Send Message with Details
Slack Message
User Prompt
Email Alert
User wants to Isolate the system
User does not want to Isolate the system
Yes
No
Alert on slack on decision of isolation
Isolate Infected Machine
LimaCharlie EDR
Slack Message
Alert on slack on the isolation of the system
Slack Message

LimaCharlie Setup:

1. **Sign Up**: Head over to LimaCharlie and create an account using **email, Google, GitHub, or Microsoft**.
2. **Organization Creation**:
   - Set up an organization in **LimaCharlie**.



Create a new organization

Select a region, plan, and organization name to get started. The first 2 Sensors in your new org will be free - no credit card required.

Name: SOAR-EDR-PROJ

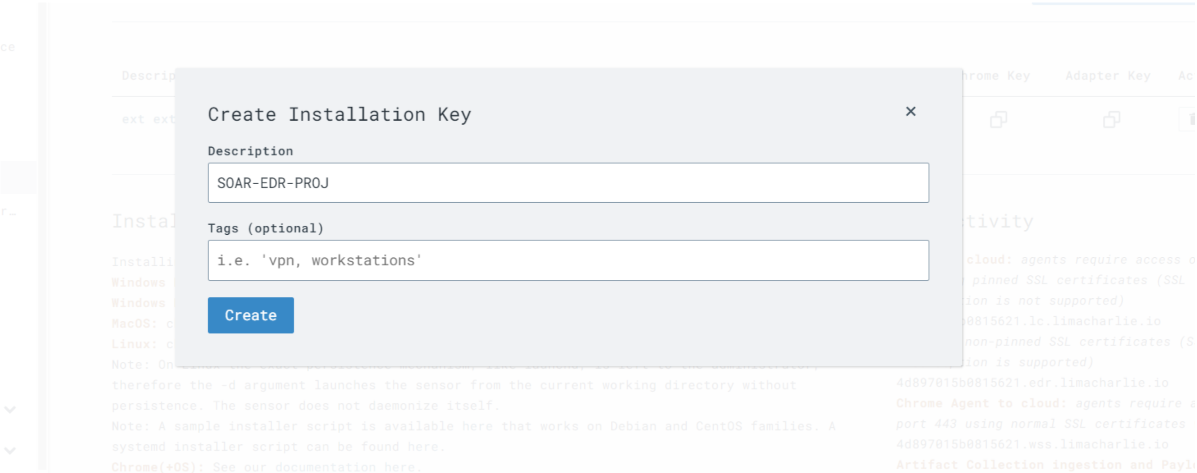
Data Residency Region: India

Template: No pre-configurations

- Start an empty tenant with nothing pre-configured
- Enable the capabilities you need as you need them, or
- Apply your own template using LimaCharlie's infrastructure as code functionality

Step 1: Download LimaCharlie

1. **Access Installation Keys**:
   - Navigate to the installation keys section on the LimaCharlie website.
   - Generate a new installation key for the project.

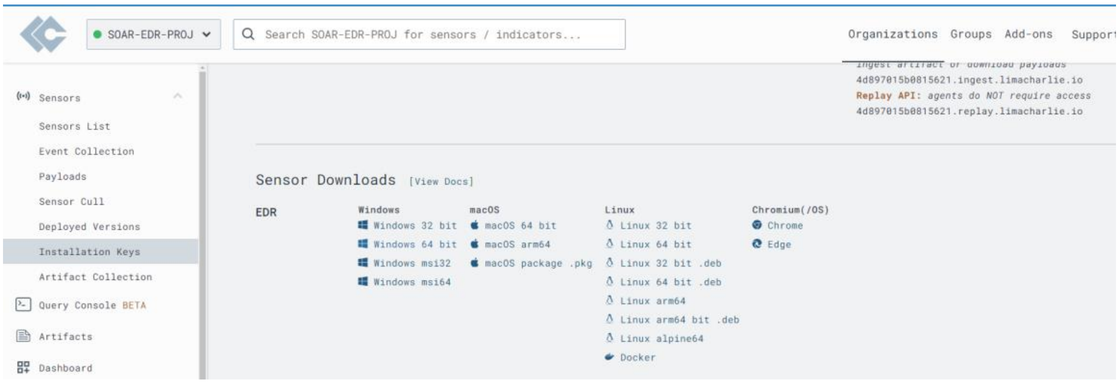


Create Installation Key

Description: SOAR-EDR-PROJ

Tags (optional): i.e. 'vpn, workstations'

2. **Download EDR**:
   - Scroll down to the "Center Downloads" section.
   - Under the EDR section, locate the download for Windows 64-bit.

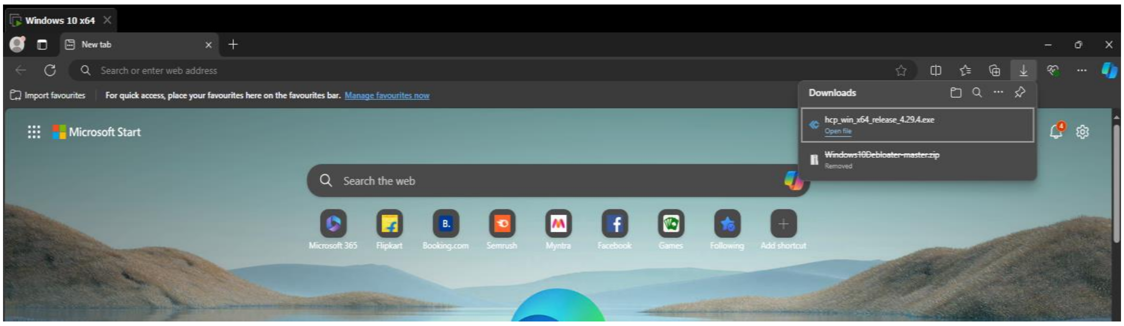


Ingest artifact or download payloads
4d897015b0815621.ingest.limacharlie.io
Replay API: agents do NOT require access
4d897015b0815621.replay.limacharlie.io

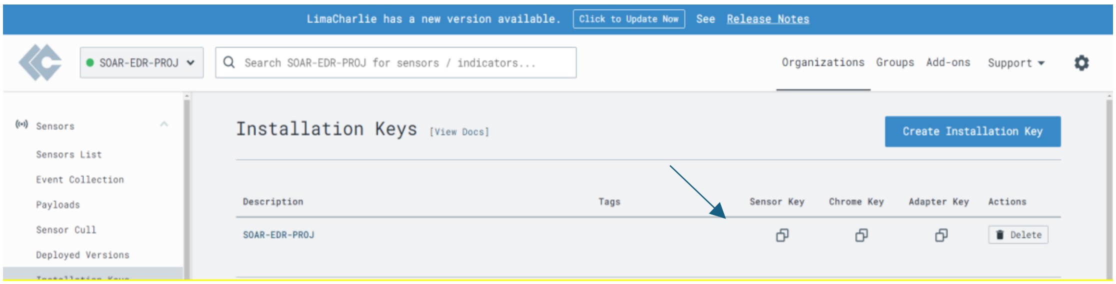
Sensor Downloads [View Docs]

	Windows	macOS	Linux	Chromium(/OS)
EDR	Windows 32 bit	macOS 64 bit	Linux 32 bit	Chrome
	Windows 64 bit	macOS arm64	Linux 64 bit	Edge
	Windows msi32	macOS package .pkg	Linux 32 bit .deb	
	Windows msi64		Linux 64 bit .deb	
			Linux arm64	
			Linux arm64 bit .deb	
			Linux alpine64	
			Docker	

- Right-click the download link and select "Copy Link Address."
- Open your server environment and paste the link to start the download.


Windows 10 x64
New tab
Search or enter web address
Import favourites
For quick access, place your favourites here on the favourites bar. Manage favourites now
Downloads
hcp_win_x64_release_4.29.4.exe
Open file
~~Windows10Debloater-master.zip~~
Removed
Microsoft Start
Search the web
Microsoft 365
Flipkart
Booking.com
Semrush
Myntra
Facebook
Games
Following
Add shortcut

3. **Copy Sensor Key**:
   - While the LimaCharlie installation is downloading, scroll up to find and copy your sensor key. This key will be used as the installation key for your server.


LimaCharlie has a new version available. Click to Update Now See Release Notes

Installation Keys [View Docs]

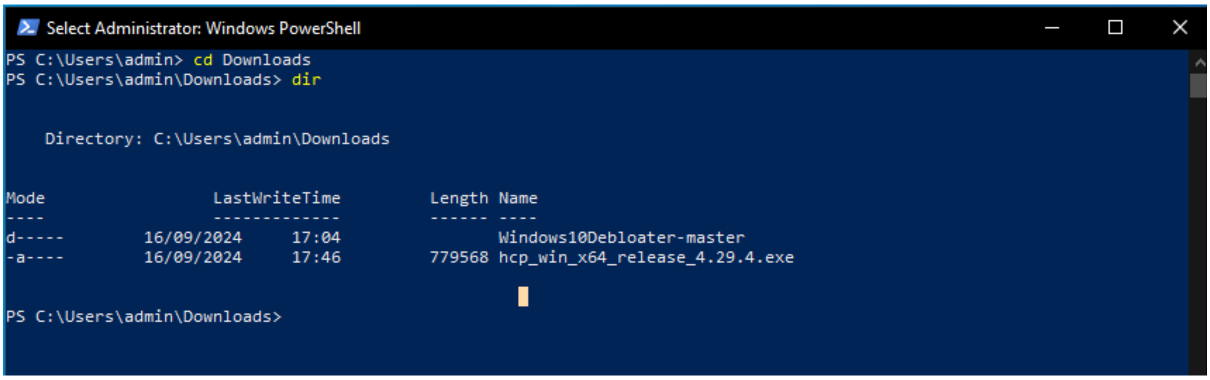
Description	Tags	Sensor Key	Chrome Key	Adapter Key	Actions
SOAR-EDR-PROJ					Delete

Step 2: Install LimaCharlie

1. **Open PowerShell**:
   - Run PowerShell as an administrator by right-clicking the icon and selecting "Run as Administrator."
2. **Navigate to Downloads Directory**:
   - Type the following commands:

     ```
     cd downloads
     dir
     ```

   - You should see the LimaCharlie executable file listed.



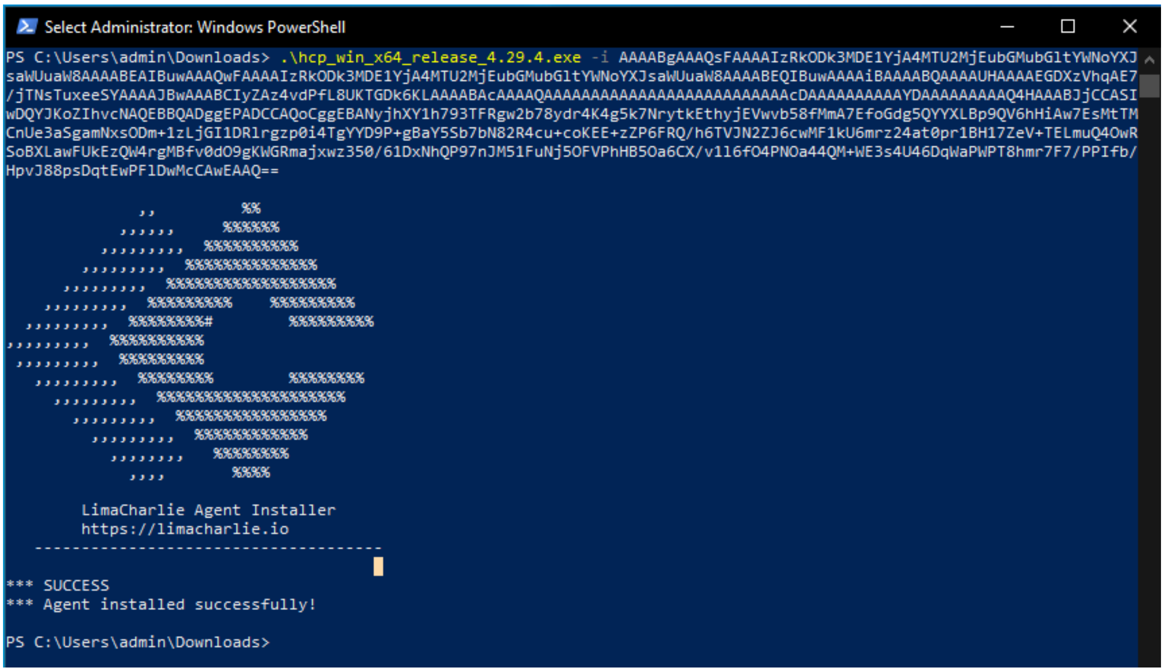
Select Administrator: Windows PowerShell

```
PS C:\Users\admin> cd Downloads
PS C:\Users\admin\Downloads> dir


    Directory: C:\Users\admin\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        16/09/2024     17:04                Windows10Debloater-master
-a----        16/09/2024     17:46         779568 hcp_win_x64_release_4.29.4.exe


PS C:\Users\admin\Downloads>
```

3. **Install the Agent**:
   - To install the agent, type:

     ```
     .\lima-charlie-executable-name.exe -i <sensor_key>
     ```

   - Replace `<sensor_key>` with the sensor key you copied earlier.
   - Press Enter to initiate the installation. A success message should appear shortly.



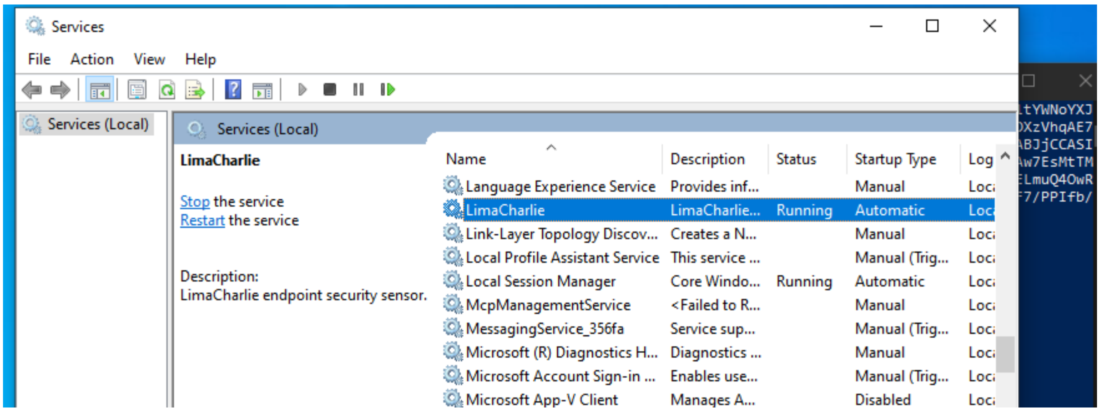
Select Administrator: Windows PowerShell

```
PS C:\Users\admin\Downloads> .\hcp_win_x64_release_4.29.4.exe -i AAAABgAAAQsFAAAAIzRkODk3MDE1YjA4MTU2MjEubGMubGltYWNoYXJ
saWUuaW8AAAABEAIBuwAAAQwFAAAAIzRkODk3MDE1YjA4MTU2MjEubGMubGltYWNoYXJsaWUuaW8AAAABEQIBuwAAAAiBAAAABQAAAAUHAAAAEGDXzVhqAE7
/jTNsTuxeeSYAAAAJBwAAABCIyZAz4vdPfL8UKTGDk6KLAAAABAcAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAcDAAAAAAAAAAYDAAAAAAAAAAQ4HAAABJjCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANyjhXY1h793TFRgw2b78ydr4K4g5k7NrytkEthyjEVwvb58fMmA7EfoGdg5QYYXLBp9QV6hHiAw7EsMtTM
CnUe3aSgamNxsODm+1zLjGI1DRlrgzp0i4TgYYD9P+gBaY5Sb7bN82R4cu+coKEE+zZP6FRQ/h6TVJN2ZJ6cwMF1kU6mrz24at0pr1BH17ZeV+TELmuQ4OwR
SoBXLawFUkEzQW4rgMBfv0dO9gKWGRmajxwz350/61DxNhQP97nJM51FuNj5OFVPhHB5Oa6CX/v116fO4PNOa44QM+WE3s4U46DqWaPWPT8hmr7F7/PPIfb/
HpvJ88psDqtEwPF1DwMcCAwEAAQ==

             ,,          %%
           ,,,,,,     %%%%%%
         ,,,,,,,,,  %%%%%%%%%%
       ,,,,,,,,,  %%%%%%%%%%%%%%
     ,,,,,,,,,  %%%%%%%%%%%%%%%%%%
   ,,,,,,,,,  %%%%%%%%%    %%%%%%%%%
 ,,,,,,,,,  %%%%%%%%#        %%%%%%%%%
,,,,,,,,,  %%%%%%%%%%
 ,,,,,,,,,  %%%%%%%%%
   ,,,,,,,,,  %%%%%%%%        %%%%%%%%
     ,,,,,,,,,  %%%%%%%%%%%%%%%%%%%%
       ,,,,,,,,,  %%%%%%%%%%%%%%%%
         ,,,,,,,,,  %%%%%%%%%%%%
           ,,,,,,,,  %%%%%%%%
             ,,,,      %%%%

        LimaCharlie Agent Installer
        https://limacharlie.io
   ------------------------------------

*** SUCCESS
*** Agent installed successfully!

PS C:\Users\admin\Downloads>
```

4. **Check for Errors**:
    - If you encounter an error stating "service installed," you can ignore it. Proceed to check if the service is running.

Step 3: Verify Installation

1. **Check Services**:
    - Open the Services management console and filter by "Lima" to confirm the LimaCharlie service is active.



LimaCharlie

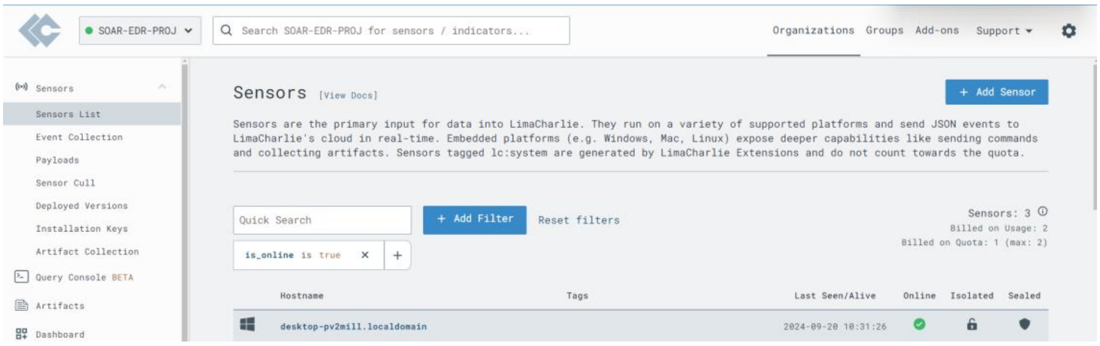
Stop the service
Restart the service

Description:
LimaCharlie endpoint security sensor.

Name	Description	Status	Startup Type	Log
Language Experience Service	Provides inf...		Manual	Loc
LimaCharlie	LimaCharlie...	Running	Automatic	Loc
Link-Layer Topology Discov...	Creates a N...		Manual	Loc
Local Profile Assistant Service	This service ...		Manual (Trig...	Loc
Local Session Manager	Core Windo...	Running	Automatic	Loc
McpManagementService	<Failed to R...		Manual	Loc
MessagingService_356fa	Service sup...		Manual (Trig...	Loc
Microsoft (R) Diagnostics H...	Diagnostics ...		Manual	Loc
Microsoft Account Sign-in ...	Enables use...		Manual (Trig...	Loc
Microsoft App-V Client	Manages A...		Disabled	Loc

```
tYWNoYXJ
XzVhqAE7
BJjCCASI
w7EsMtTM
LmuQ4OwR
7/PPIfb/
```

2. **View Sensor Information**:
    - Log into your LimaCharlie dashboard and navigate to the Sensors list.
    - Confirm that your server appears with the correct details such as hostname, network access, and sensor ID.



Sensors [View Docs]

Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts. Sensors tagged lc:system are generated by LimaCharlie Extensions and do not count towards the quota.

is_online is true

Sensors: 3
Billed on Usage: 2
Billed on Quota: 1 (max: 2)

Hostname	Tags	Last Seen/Alive	Online	Isolated	Sealed
desktop-pv2mill.localdomain		2024-09-20 10:31:26	✓	🔓	●

Key Features Explored

1. Auto Runs

- Under the **Analytics** section, you can view Auto Runs, which lists all auto-starting programs. This is crucial for identifying potential persistence mechanisms.

2. Console Commands

- The **Console** section allows you to run remote commands. For example, using `netstat` to check for active network connections can help identify suspicious processes.

3. Event Collection

- LimaCharlie collects various events from your server, providing insights into system activities.

4. File System Access

- Navigate the file system to inspect files, hashes, and timestamps. You can even perform malware analysis by downloading potentially malicious files.

5. Integrity Monitoring

- File Integrity Monitoring (FIM) enables you to detect changes in file states, which is essential for security audits.

6. Process Management

- Monitor active processes, view modules, and even kill suspicious processes. Detailed information about each process can help in investigating anomalies.

7. User Management

- The Users section displays existing users on the server, which can be useful for detecting unauthorized accounts.

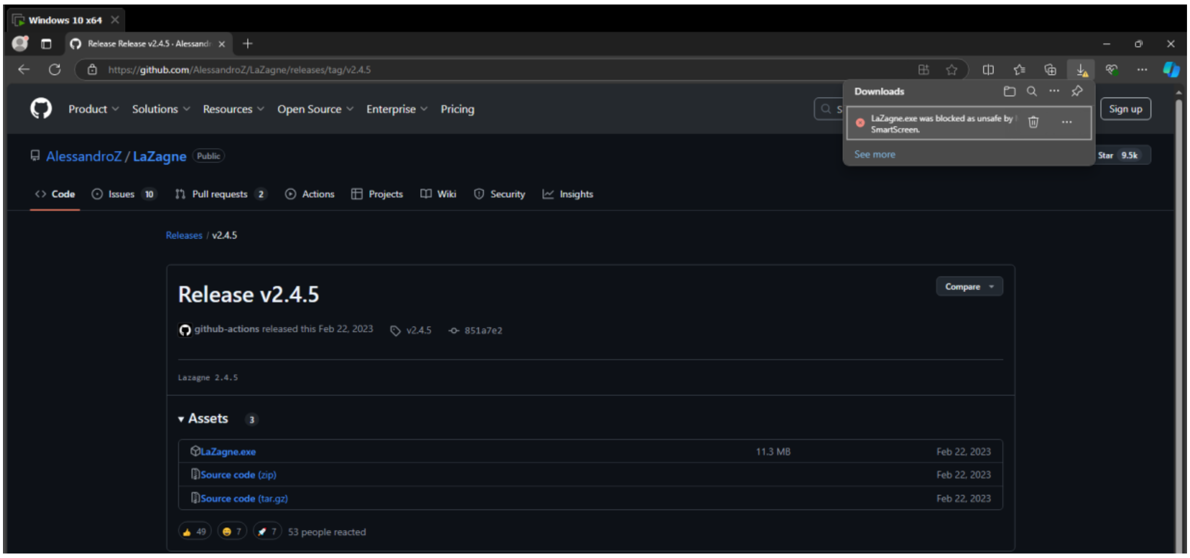
8. Timeline Analysis

- The Timeline feature allows you to track events chronologically, making it easier to investigate incidents based on user-reported issues.

Downloading and Installing Lasagna for Testing

1. **Download Lasagna**:

   - Navigate to the Lasagna GitHub.
   - Download the executable (lasagna.exe) from the "Releases" section.



https://github.com/AlessandroZ/LaZagne/releases/tag/v2.4.5

LaZagne.exe was blocked as unsafe by SmartScreen.

Releases / v2.4.5

Release v2.4.5

github-actions released this Feb 22, 2023 v2.4.5 851a7e2

Lazagne 2.4.5

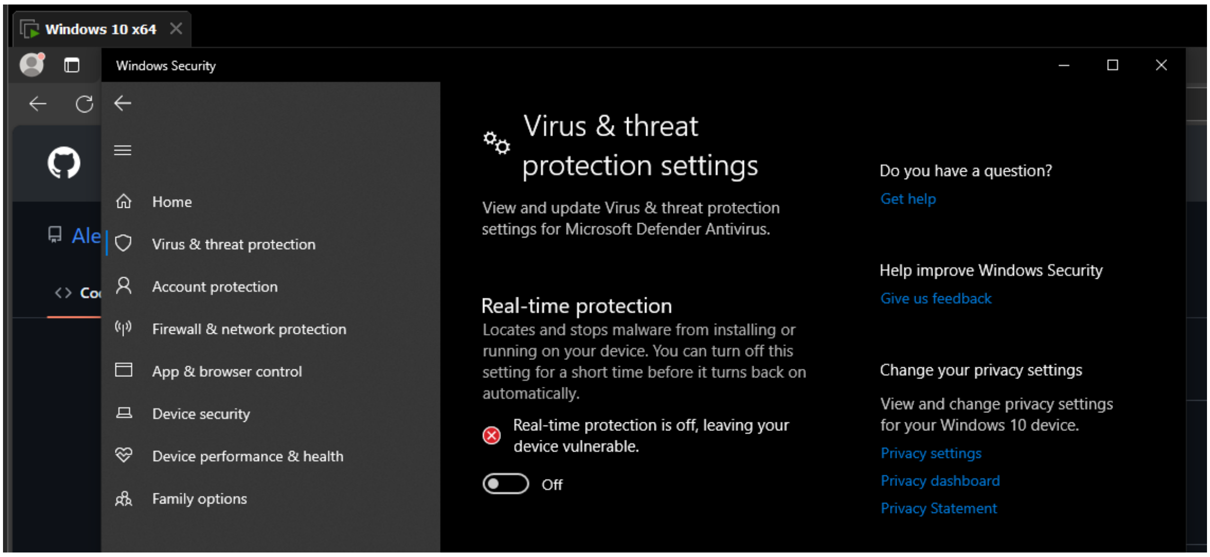
Assets 3

LaZagne.exe	11.3 MB	Feb 22, 2023
Source code (zip)		Feb 22, 2023
Source code (tar.gz)		Feb 22, 2023

49 7 7 53 people reacted

2. **Disable Windows Security**:

   - Open "Windows Security."
   - Select "Virus & Threat Protection" and click "Manage Settings."
   - Disable "Real-time protection."



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Do you have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

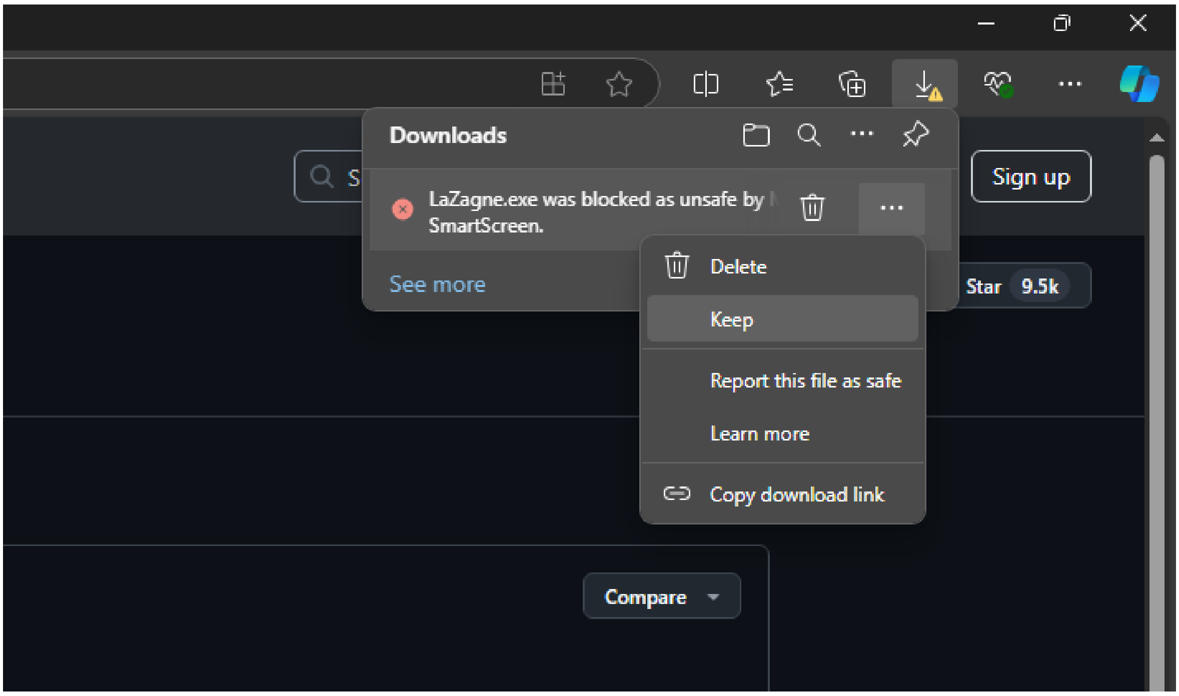
Privacy settings

Privacy dashboard

Privacy Statement

3. **Bypass Defender's Warning**:

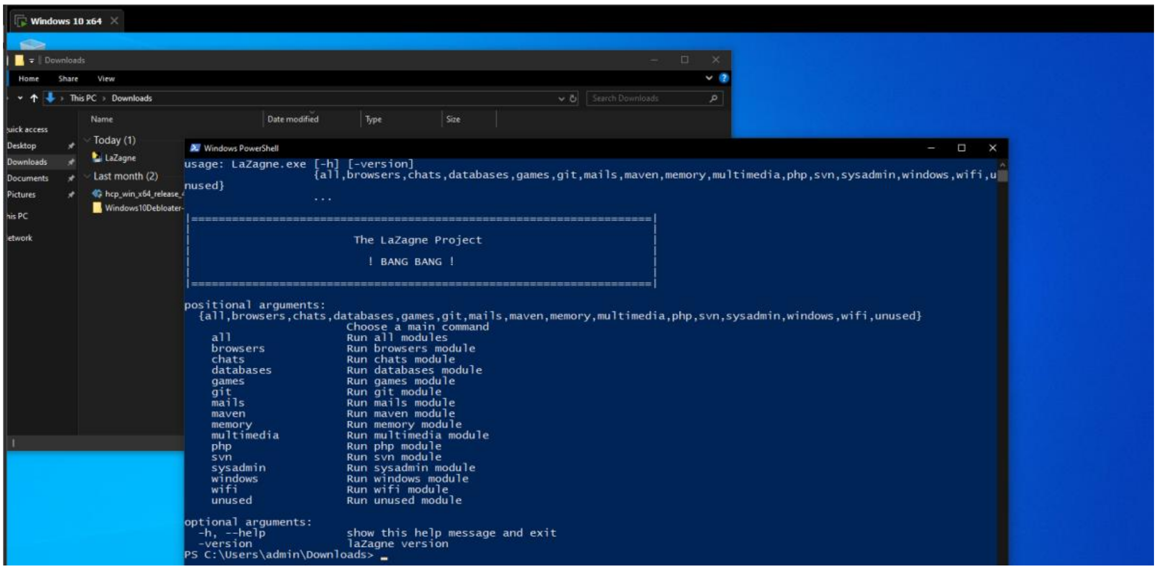
   - When Lasagna is blocked by Microsoft Defender SmartScreen, click on the three dots next to the warning.
   - Select "Keep" to download it, ignoring the warning that it is unsafe.



LaZagne.exe was blocked as unsafe by SmartScreen.

4. **Run Lasagna in PowerShell**:

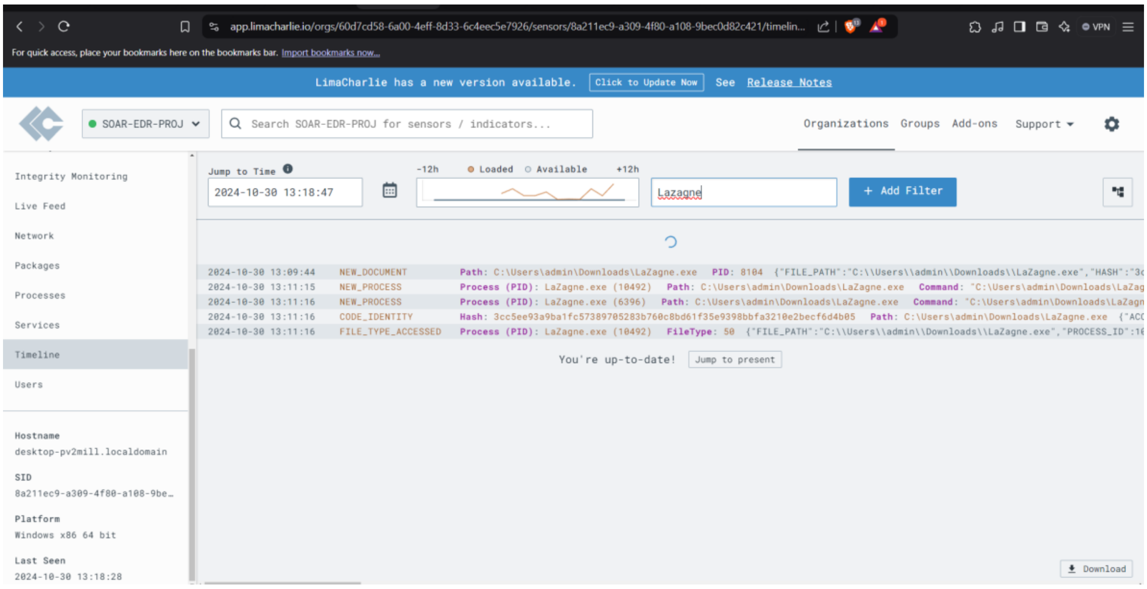
    - Open the download folder and launch PowerShell.
    - Hold **Shift + Right-click** and choose "Open PowerShell window here."
    - Execute lasagna in the terminal.



```
usage: LaZagne.exe [-h] [-version]
                   {all,browsers,chats,databases,games,git,mails,maven,memory,multimedia,php,svn,sysadmin,windows,wifi,u
nused}
                   ...

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

positional arguments:
  {all,browsers,chats,databases,games,git,mails,maven,memory,multimedia,php,svn,sysadmin,windows,wifi,unused}
                        Choose a main command
    all                 Run all modules
    browsers            Run browsers module
    chats               Run chats module
    databases           Run databases module
    games               Run games module
    git                 Run git module
    mails               Run mails module
    maven               Run maven module
    memory              Run memory module
    multimedia          Run multimedia module
    php                 Run php module
    svn                 Run svn module
    sysadmin            Run sysadmin module
    windows             Run windows module
    wifi                Run wifi module
    unused              Run unused module

optional arguments:
  -h, --help            show this help message and exit
  -version              laZagne version
PS C:\Users\admin\Downloads> _
```

5. **Verify Activity in Lima Charlie**:

   - Head over to Lima Charlie.
   - Navigate to the **Sensors List** and click on the relevant sensor.
   - Go to the **Timeline** and filter for events by typing "lasagna" to confirm its execution was detected.


app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421/timelin...
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
LimaCharlie has a new version available.
Click to Update Now
See Release Notes
SOAR-EDR-PROJ
Search SOAR-EDR-PROJ for sensors / indicators...
Organizations
Groups
Add-ons
Support
Integrity Monitoring
Live Feed
Network
Packages
Processes
Services
Timeline
Users
Jump to Time
-12h
Loaded
Available
+12h
+ Add Filter
Download

Hostname
desktop-pv2mill.localdomain

SID
8a211ec9-a309-4f80-a108-9be…

Platform
Windows x86 64 bit

Last Seen
2024-10-30 13:18:28

Jump to Time: 2024-10-30 13:18:47

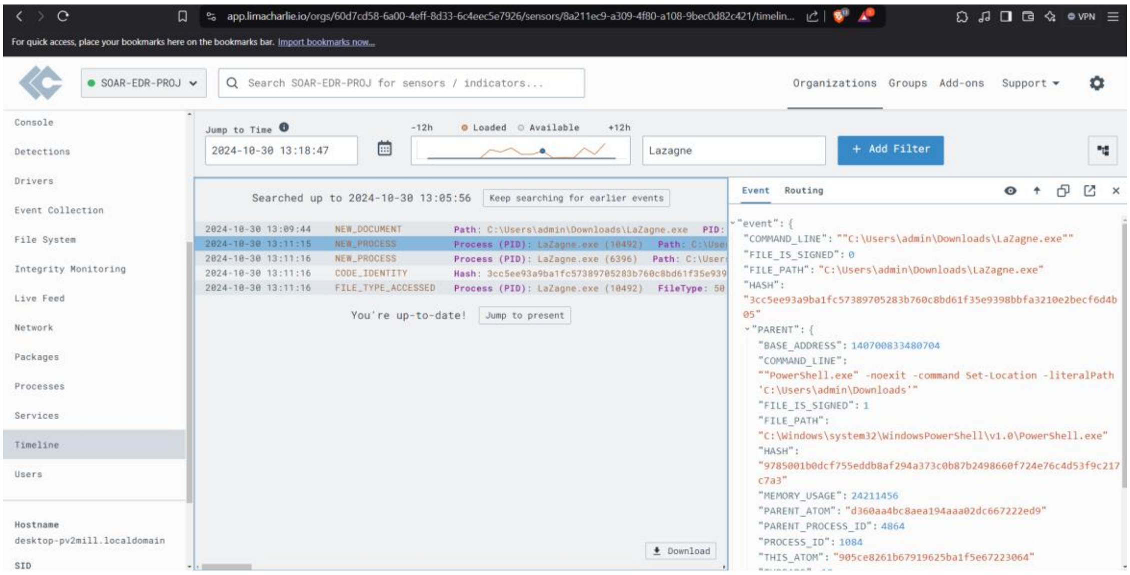
Lazagne

```
2024-10-30 13:09:44   NEW_DOCUMENT         Path: C:\Users\admin\Downloads\LaZagne.exe   PID: 8104  {"FILE_PATH":"C:\\Users\\admin\\Downloads\\LaZagne.exe","HASH":"3c
2024-10-30 13:11:15   NEW_PROCESS          Process (PID): LaZagne.exe (10492)  Path: C:\Users\admin\Downloads\LaZagne.exe  Command: "C:\Users\admin\Downloads\LaZag
2024-10-30 13:11:16   NEW_PROCESS          Process (PID): LaZagne.exe (6396)  Path: C:\Users\admin\Downloads\LaZagne.exe  Command: "C:\Users\admin\Downloads\LaZagn
2024-10-30 13:11:16   CODE_IDENTITY        Hash: 3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05  Path: C:\Users\admin\Downloads\LaZagne.exe  {"ACC
2024-10-30 13:11:16   FILE_TYPE_ACCESSED   Process (PID): LaZagne.exe (10492)  FileType: 50  {"FILE_PATH":"C:\\Users\\admin\\Downloads\\LaZagne.exe","PROCESS_ID":1(
```

You're up-to-date! Jump to present

6. **Extract Information**:

   - Examine the **new process event**.
   - Collect information like:
     - File path (C:\Users\Administrator\Downloads)
     - Process ID
     - Command-line arguments, etc.


app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421/timelin...
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
SOAR-EDR-PROJ
Search SOAR-EDR-PROJ for sensors / indicators...
Organizations
Groups
Add-ons
Support
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
Network
Packages
Processes
Services
Timeline
Users
Jump to Time
-12h
Loaded
Available
+12h
+ Add Filter
Event
Routing
Download

Hostname
desktop-pv2mill.localdomain

SID

Jump to Time: 2024-10-30 13:18:47

Lazagne

Searched up to 2024-10-30 13:05:56 Keep searching for earlier events

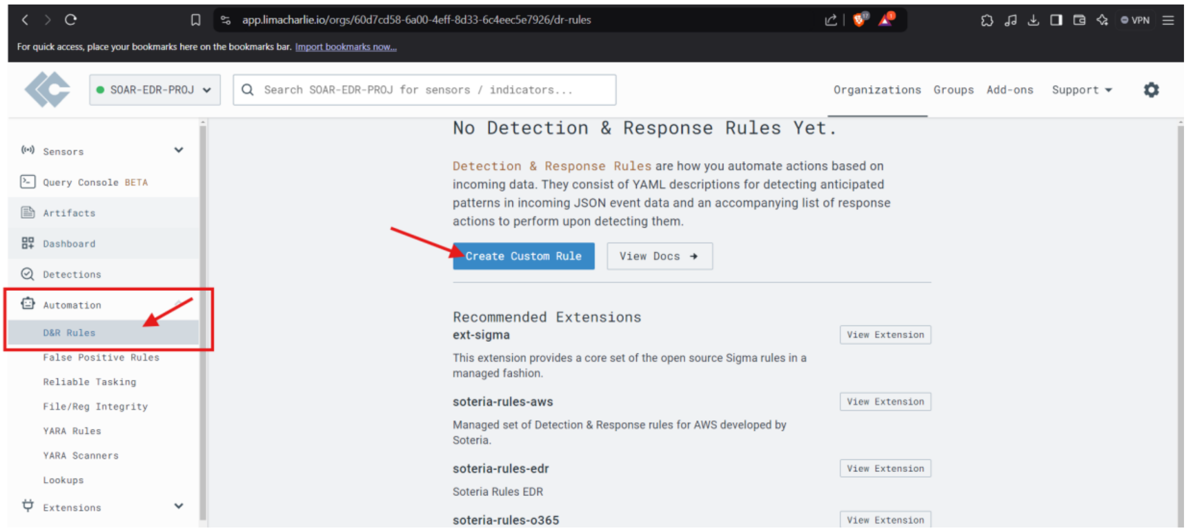
```
2024-10-30 13:09:44   NEW_DOCUMENT         Path: C:\Users\admin\Downloads\LaZagne.exe   PID:
2024-10-30 13:11:15   NEW_PROCESS          Process (PID): LaZagne.exe (10492)   Path: C:\Use
2024-10-30 13:11:16   NEW_PROCESS          Process (PID): LaZagne.exe (6396)   Path: C:\User
2024-10-30 13:11:16   CODE_IDENTITY        Hash: 3cc5ee93a9ba1fc57389705283b760c8bd61f35e939
2024-10-30 13:11:16   FILE_TYPE_ACCESSED   Process (PID): LaZagne.exe (10492)   FileType: 50
```

You're up-to-date! Jump to present

```
"event": {
  "COMMAND_LINE": ""C:\Users\admin\Downloads\LaZagne.exe""
  "FILE_IS_SIGNED": 0
  "FILE_PATH": "C:\Users\admin\Downloads\LaZagne.exe"
  "HASH":
  "3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b
  05"
  "PARENT": {
    "BASE_ADDRESS": 140700833480704
    "COMMAND_LINE":
    ""PowerShell.exe" -noexit -command Set-Location -literalPath
    'C:\Users\admin\Downloads'"
    "FILE_IS_SIGNED": 1
    "FILE_PATH":
    "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe"
    "HASH":
    "9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217
    c7a3"
    "MEMORY_USAGE": 24211456
    "PARENT_ATOM": "d360aa4bc8aea194aaa02dc667222ed9"
    "PARENT_PROCESS_ID": 4864
    "PROCESS_ID": 1084
    "THIS_ATOM": "905ce8261b67919625ba1f5e67223064"
```

7. **Create Detection Rule**:

   - In Lima Charlie, go to your organization and navigate to **Automation > DNR Rules**.
   - Click **New Rule** to begin.



No Detection & Response Rules Yet.

Detection & Response Rules are how you automate actions based on incoming data. They consist of YAML descriptions for detecting anticipated patterns in incoming JSON event data and an accompanying list of response actions to perform upon detecting them.

Recommended Extensions

ext-sigma

This extension provides a core set of the open source Sigma rules in a managed fashion.

soteria-rules-aws

Managed set of Detection & Response rules for AWS developed by Soteria.

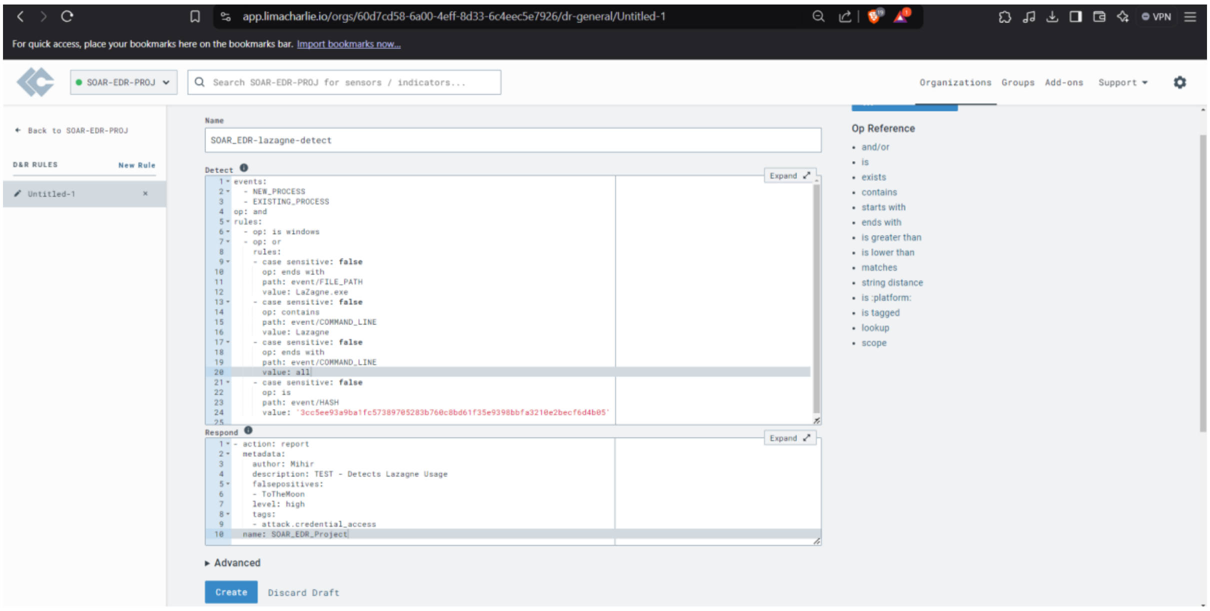
soteria-rules-edr

Soteria Rules EDR

soteria-rules-o365

8. **Write the Rules**:

   - Modify it to suit the Lasagna detection by filtering based on "process creation."



Name: SOAR_EDR-lazagne-detect

Detect

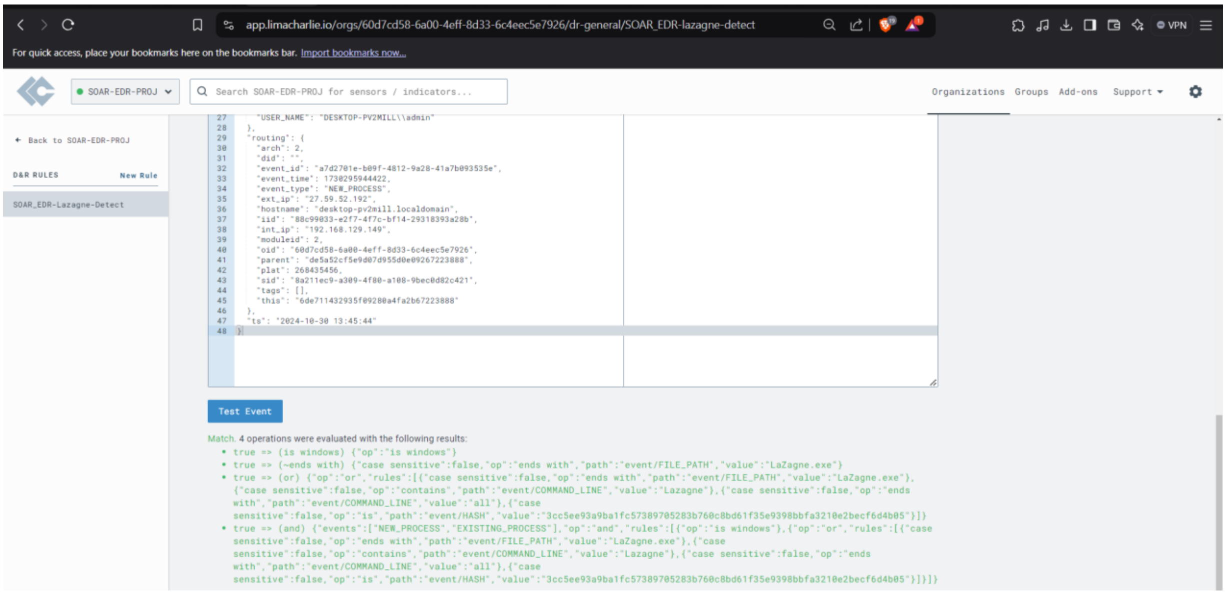
```
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - op: or
    rules:
    - case sensitive: false
      op: ends with
      path: event/FILE_PATH
      value: LaZagne.exe
    - case sensitive: false
      op: contains
      path: event/COMMAND_LINE
      value: Lazagne
    - case sensitive: false
      op: ends with
      path: event/COMMAND_LINE
      value: all
    - case sensitive: false
      op: is
      path: event/HASH
      value: '3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05'
```

Respond

```
- action: report
  metadata:
    author: Mihir
    description: TEST - Detects Lazagne Usage
    falsepositives:
    - ToTheMoon
    level: high
    tags:
    - attack.credential_access
  name: SOAR_EDR_Project
```

9. **Testing the Rule**:

   - In the rule editor, click **Target Event** to test it.
   - Paste the event and check if the rule triggers successfully.


app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/dr-general/SOAR_EDR-lazagne-detect
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
SOAR-EDR-PROJ
Search SOAR-EDR-PROJ for sensors / indicators...
Organizations
Groups
Add-ons
Support
← Back to SOAR-EDR-PROJ
D&R RULES
New Rule
SOAR_EDR-Lazagne-Detect
Test Event

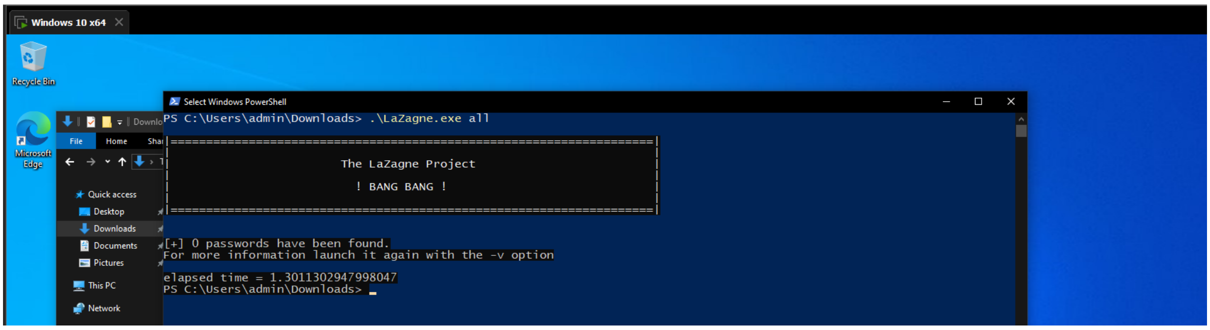
```
    "USER_NAME": "DESKTOP-PV2MILL\\admin"
  },
  "routing": {
    "arch": 2,
    "did": "",
    "event_id": "a7d2701e-b09f-4812-9a28-41a7b093535e",
    "event_time": 1730295944422,
    "event_type": "NEW_PROCESS",
    "ext_ip": "27.59.52.192",
    "hostname": "desktop-pv2mill.localdomain",
    "iid": "88c99033-e2f7-4f7c-bf14-29318393a28b",
    "int_ip": "192.168.129.149",
    "moduleid": 2,
    "oid": "60d7cd58-6a00-4eff-8d33-6c4eec5e7926",
    "parent": "de5a52cf5e9d07d955d0e09267223888",
    "plat": 268435456,
    "sid": "8a211ec9-a309-4f80-a108-9bec0d82c421",
    "tags": [],
    "this": "6de711432935f09280a4fa2b67223888"
  },
  "ts": "2024-10-30 13:45:44"
}
```

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":"contains","path":"event/COMMAND_LINE","value":"Lazagne"},{"case sensitive":false,"op":"ends
  with","path":"event/COMMAND_LINE","value":"all"},{"case
  sensitive":false,"op":"is","path":"event/HASH","value":"3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05"}]}
• 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":"contains","path":"event/COMMAND_LINE","value":"Lazagne"},{"case sensitive":false,"op":"ends
  with","path":"event/COMMAND_LINE","value":"all"},{"case
  sensitive":false,"op":"is","path":"event/HASH","value":"3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05"}]}]}
```

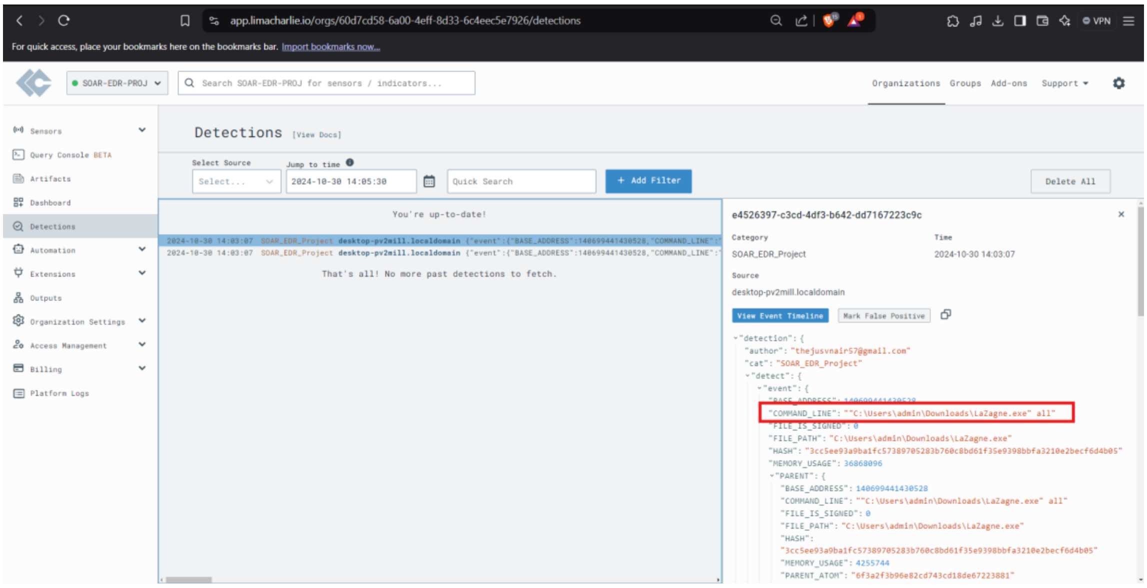
10. **Generate Detections:**

- Re-run lasagna from PowerShell with the --all flag to trigger the detection.



```
PS C:\Users\admin\Downloads> .\LaZagne.exe all
|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] 0 passwords have been found.
For more information launch it again with the -v option

elapsed time = 1.3011302947998047
PS C:\Users\admin\Downloads> _
```

- Refresh the Lima Charlie dashboard to verify the detection.



```
2024-10-30 14:05:30

You're up-to-date!
2024-10-30 14:03:07  SOAR_EDR_Project  desktop-pv2mill.localdomain  {"event":{"BASE_ADDRESS":140699441430528,"COMMAND_LINE":"
2024-10-30 14:03:07  SOAR_EDR_Project  desktop-pv2mill.localdomain  {"event":{"BASE_ADDRESS":140699441430528,"COMMAND_LINE":"
That's all! No more past detections to fetch.
```

e4526397-c3cd-4df3-b642-dd7167223c9c

Category: SOAR_EDR_Project

Time: 2024-10-30 14:03:07

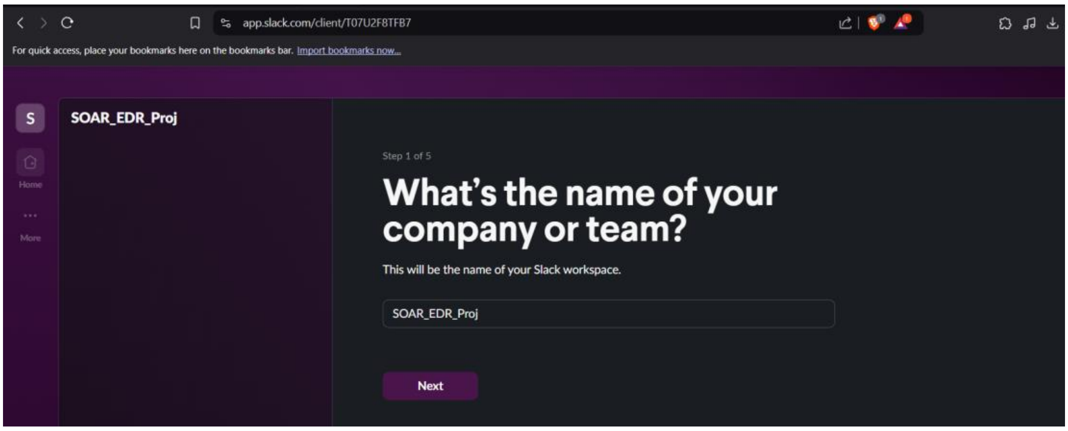
Source: desktop-pv2mill.localdomain

```
"detection": {
  "author": "thejusvnair57@gmail.com"
  "cat": "SOAR_EDR_Project"
  "detect": {
    "event": {
      "BASE_ADDRESS": 140699441430528
      "COMMAND_LINE": ""C:\Users\admin\Downloads\LaZagne.exe" all"
      "FILE_IS_SIGNED": 0
      "FILE_PATH": "C:\Users\admin\Downloads\LaZagne.exe"
      "HASH": "3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05"
      "MEMORY_USAGE": 36868096
      "PARENT": {
        "BASE_ADDRESS": 140699441430528
        "COMMAND_LINE": ""C:\Users\admin\Downloads\LaZagne.exe" all"
        "FILE_IS_SIGNED": 0
        "FILE_PATH": "C:\Users\admin\Downloads\LaZagne.exe"
        "HASH":
        "3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05"
        "MEMORY_USAGE": 4255744
        "PARENT_ATOM": "6f3a2f3b96e82cd743cd18de67223881"
```

Setting Up Slack and Tines for Automation

Step 1: Setting Up Slack

1. Visit [Slack.com]() and create an account.
2. **Create a workspace**: name it something identifiable for the project.



app.slack.com/client/T07U2F8TFB7

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

SOAR_EDR_Proj

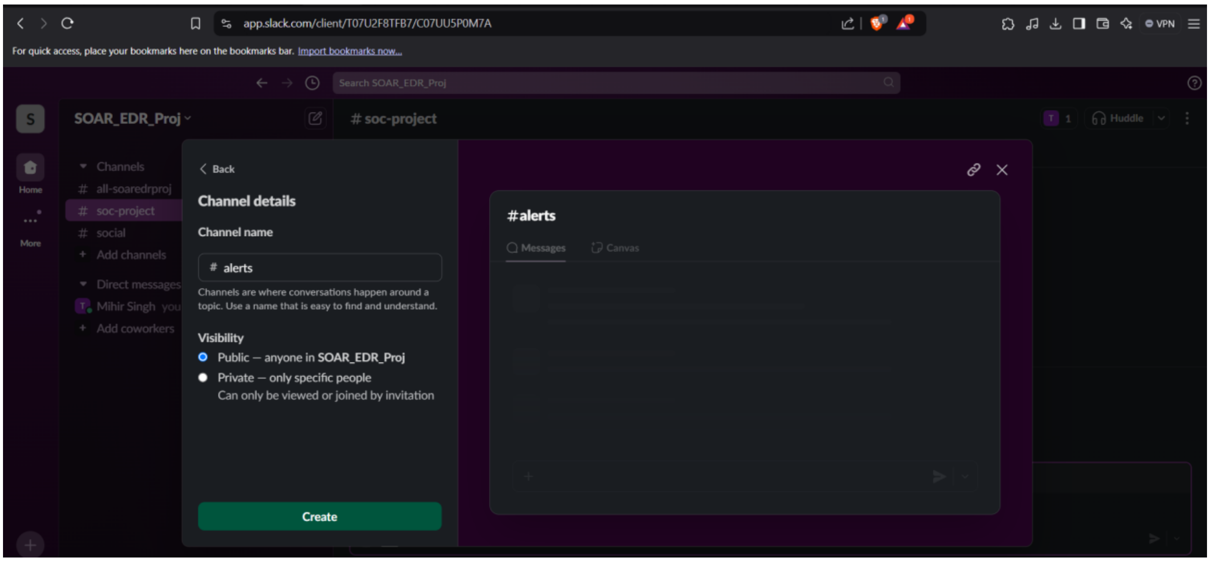
Step 1 of 5

What's the name of your company or team?

This will be the name of your Slack workspace.

SOAR_EDR_Proj

3. **Add an Alerts Channel**:
   - Click on **Add channels** > **Create a new channel** and name it **alerts**.



app.slack.com/client/T07U2F8TFB7/C07UU5P0M7A

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Search SOAR_EDR_Proj

SOAR_EDR_Proj

soc-project

Channels
# all-soaredrproj
# soc-project
# social
+ Add channels

Direct messages
Mihir Singh you
+ Add coworkers

Back

Channel details

Channel name

alerts

Channels are where conversations happen around a topic. Use a name that is easy to find and understand.

Visibility

● Public — anyone in SOAR_EDR_Proj

○ Private — only specific people
Can only be viewed or joined by invitation

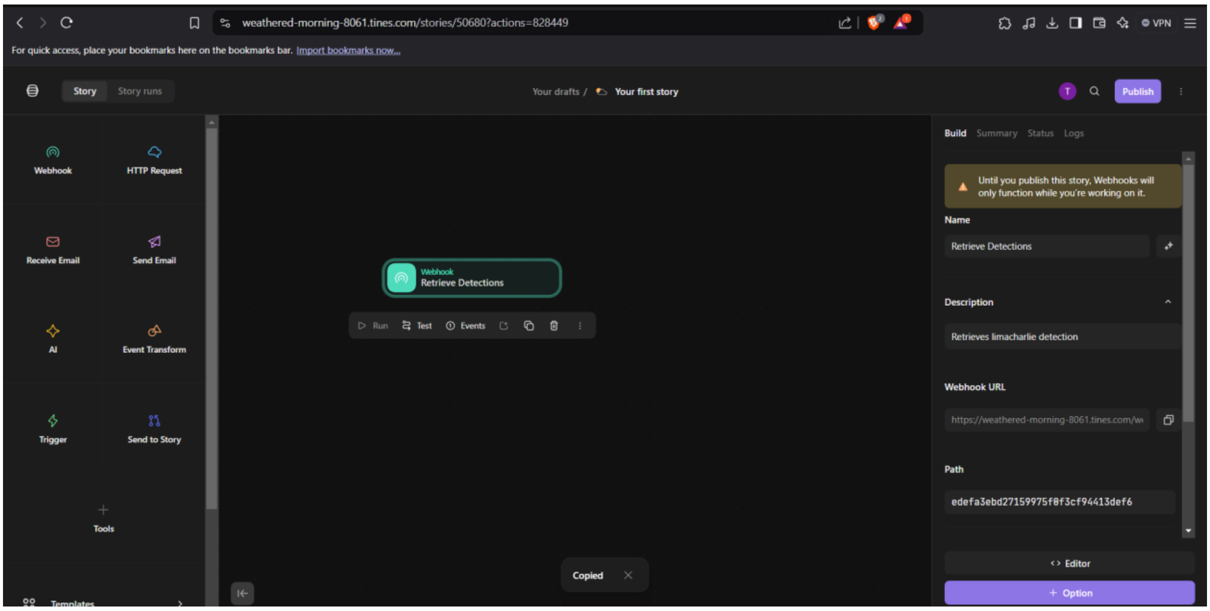
#alerts

Step 2: Setting Up Tines

1. Go to [Tines]() and **sign up** using a valid email.
2. Familiarize yourself with the **action menu** on the left side. Here, you can add:
   - **Webhooks**
   - **HTTP requests**
   - **Pre-built templates** like **VirusTotal** for hash lookups and others for common automation tasks.

Step 3: Linking LimaCharlie and Tines

1. Start by creating a **Webhook in Tines**:
   - Name it `Retrieve Detections`.
   - Set the description to `Retrieve LimaCharlie detections`.
   - **Copy the Webhook URL** generated for use in LimaCharlie.



Until you publish this story, Webhooks will only function while you're working on it.

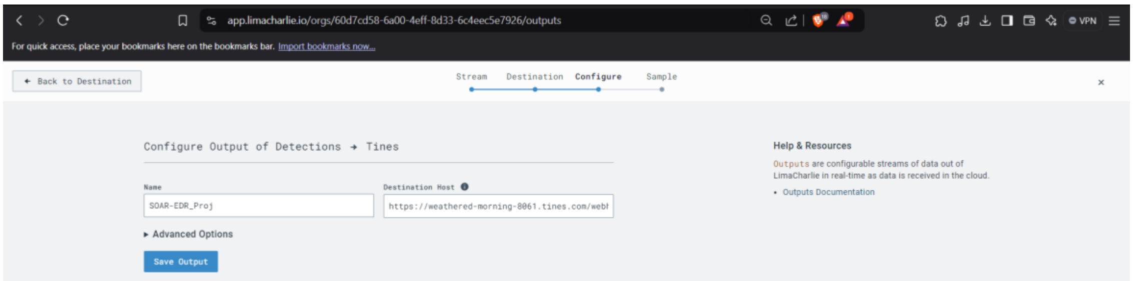
Name: Retrieve Detections

Description: Retrieves limacharlie detection

Webhook URL: https://weathered-morning-8061.tines.com/w

Path: edefa3ebd27159975f0f3cf94413def6

2. In **LimaCharlie**, configure the **Outputs**:
   - Under **Outputs**, click **Add Output** and select **Detections** (stream of detections from LimaCharlie's rule engine).
   - Select **Tines** as the output application (or Webhook if Tines isn't available).
   - Paste the Webhook URL copied from Tines.
   - Click **Save Output** to finalize.


app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/outputs
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
← Back to Destination
Stream
Destination
Configure
Sample
×
Advanced Options
Save Output

Configure Output of Detections → Tines

Name: SOAR-EDR_Proj

Destination Host: https://weathered-morning-8061.tines.com/webh

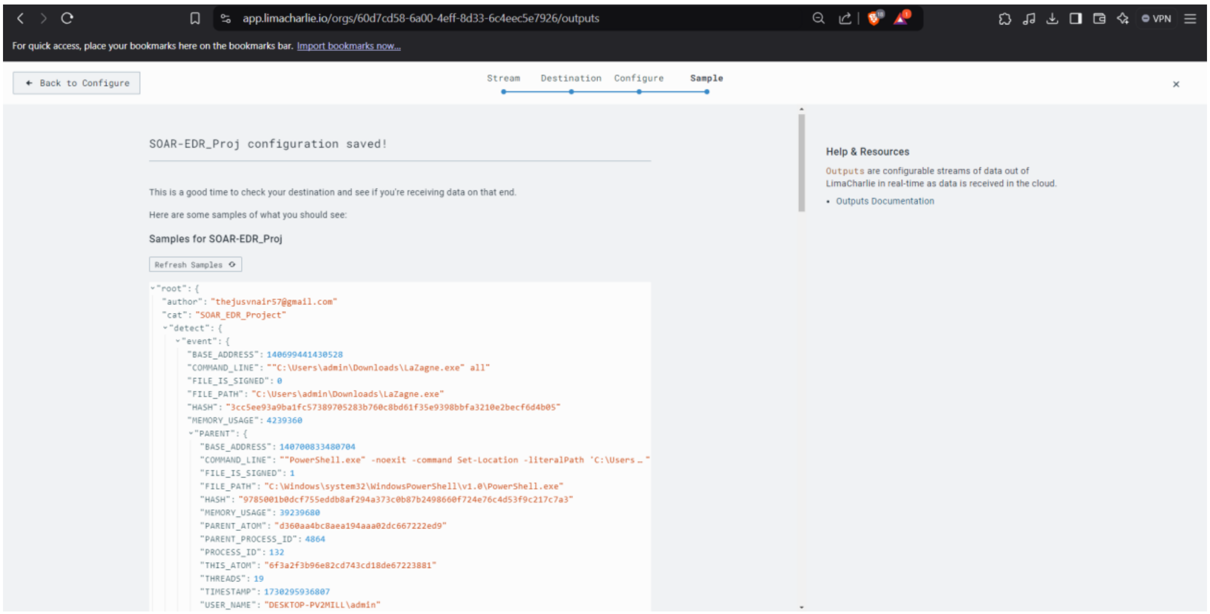
Help & Resources

Outputs are configurable streams of data out of LimaCharlie in real-time as data is received in the cloud.

- Outputs Documentation

Step 4: Testing Detection

1. **Regenerate Detection**:
   - In your server environment, simulate a detection by running `lasagna` or another known test event.
   - Go back to the **Outputs** section in LimaCharlie and **refresh**. You should see the detection appear.


app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/outputs
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
← Back to Configure
Stream
Destination
Configure
Sample
Refresh Samples ⟳
Help & Resources
Outputs Documentation

SOAR-EDR_Proj configuration saved!

This is a good time to check your destination and see if you're receiving data on that end.

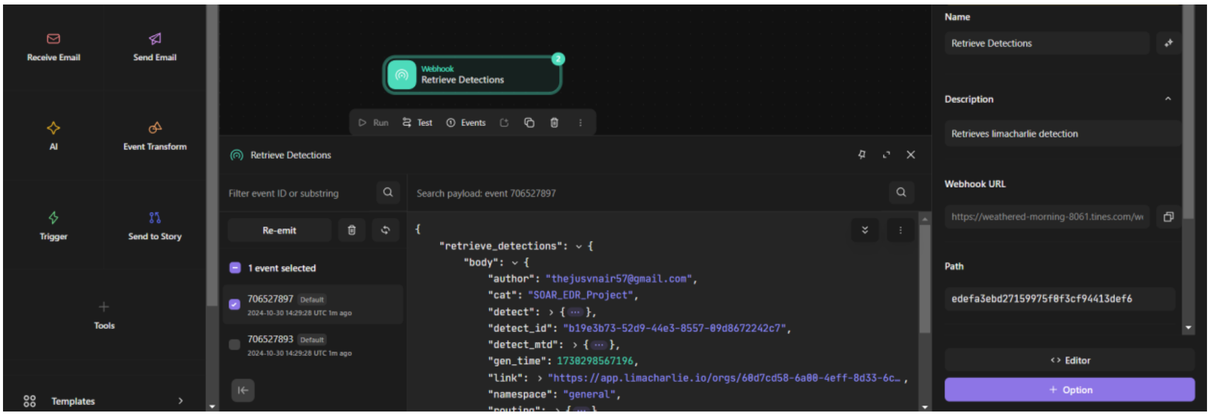
Here are some samples of what you should see:

Samples for SOAR-EDR_Proj

```
"root": {
  "author": "thejusvnair57@gmail.com"
  "cat": "SOAR_EDR_Project"
  "detect": {
    "event": {
      "BASE_ADDRESS": 140699441430528
      "COMMAND_LINE": ""C:\Users\admin\Downloads\LaZagne.exe" all"
      "FILE_IS_SIGNED": 0
      "FILE_PATH": "C:\Users\admin\Downloads\LaZagne.exe"
      "HASH": "3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05"
      "MEMORY_USAGE": 4239360
      "PARENT": {
        "BASE_ADDRESS": 140700833480704
        "COMMAND_LINE": ""PowerShell.exe" -noexit -command Set-Location -literalPath 'C:\Users_"
        "FILE_IS_SIGNED": 1
        "FILE_PATH": "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe"
        "HASH": "9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3"
        "MEMORY_USAGE": 39239680
        "PARENT_ATOM": "d360aa4bc8aea194aaa02dc667222ed9"
        "PARENT_PROCESS_ID": 4864
        "PROCESS_ID": 132
        "THIS_ATOM": "6f3a2f3b96e82cd743cd18de67223881"
        "THREADS": 19
        "TIMESTAMP": 1730295936807
        "USER_NAME": "DESKTOP-PV2MILL\admin"
```

Outputs are configurable streams of data out of LimaCharlie in real-time as data is received in the cloud.

2. In **Tines**, verify the detection:
   - Check under the `Retrieve Detections` webhook action and expand the **latest detection**.
   - Confirm detection details like **title, command line, file path, hash,** and **username**.



Name: Retrieve Detections

Description: Retrieves limacharlie detection

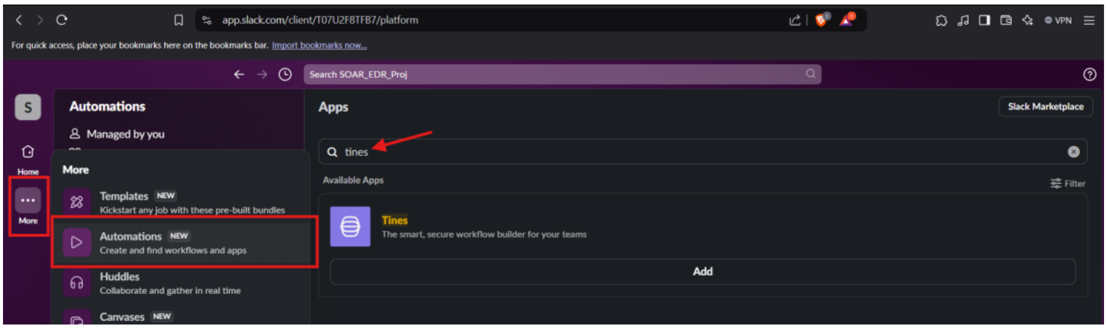
Webhook URL: https://weathered-morning-8061.tines.com/w

Path: edefa3ebd27159975f8f3cf94413def6

```
{
    "retrieve_detections": {
        "body": {
            "author": "thejusvnair57@gmail.com",
            "cat": "SOAR_EDR_Project",
            "detect": {…},
            "detect_id": "b19e3b73-52d9-44e3-8557-09d8672242c7",
            "detect_mtd": {…},
            "gen_time": 1730298567196,
            "link": "https://app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c… ,
            "namespace": "general",
```

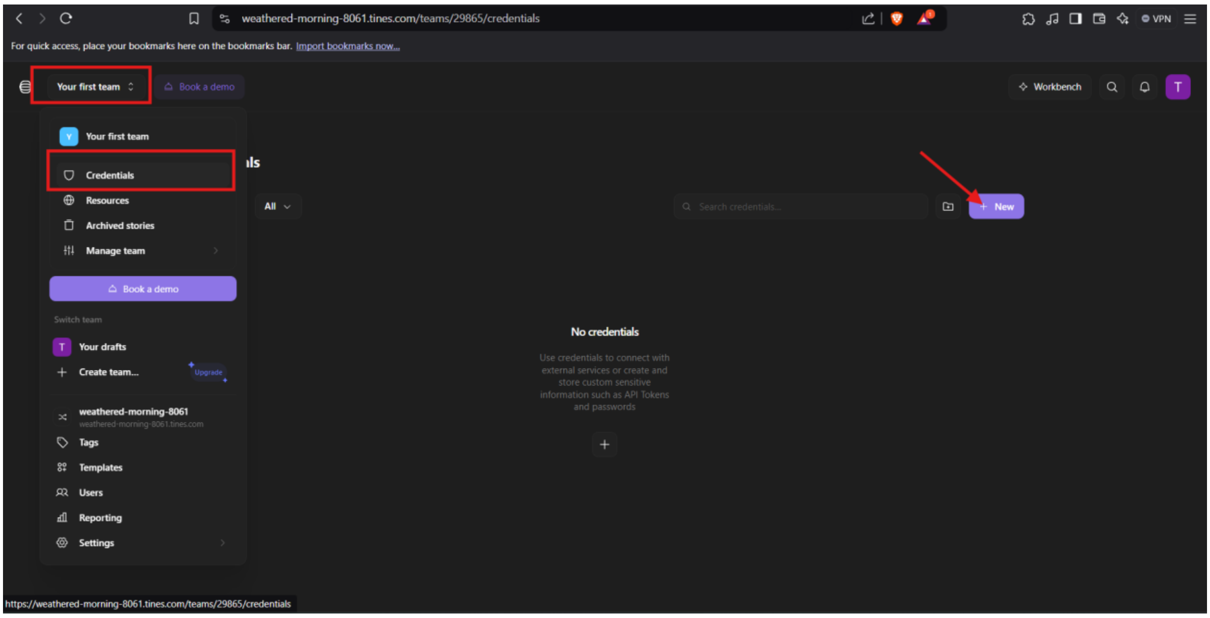
3. Add the **Tines** Application in slack:

   - Search for **Tines** in the **Slack** App Directory and add it.
   - Accept permissions for Tines to send messages and create channels.


app.slack.com/client/T07U2F8TFB7/platform
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Search SOAR_EDR_Proj
Automations
Managed by you
More
Templates NEW
Kickstart any job with these pre-built bundles
Automations NEW
Create and find workflows and apps
Huddles
Collaborate and gather in real time
Canvases NEW
Home
More
Apps
Slack Marketplace
tines
Available Apps
Filter
Tines
The smart, secure workflow builder for your teams
Add

Step 5. Setting Up Tines

1. **Establish a Link between Tines and Slack:**
   - Go to the **Credentials** section in Tines.
   - Create a new Slack credential to connect Tines and Slack.
   - Use this credential in the workflow to enable Tines to send alerts to the `alerts` channel in Slack.

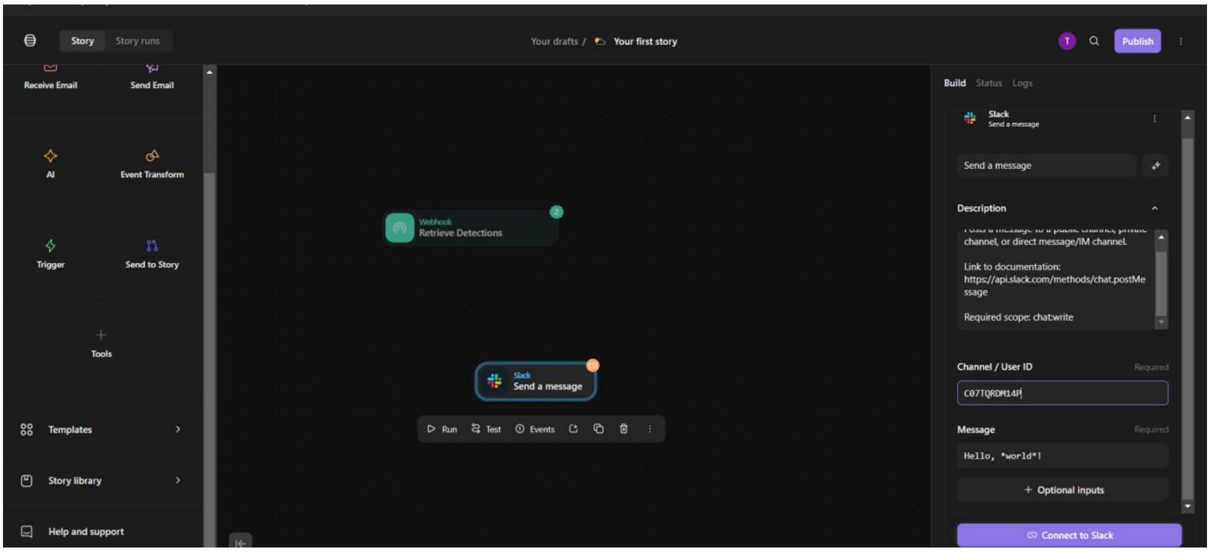

weathered-morning-8061.tines.com/teams/29865/credentials
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Your first team
Book a demo
Workbench
Your first team
Credentials
Resources
Archived stories
Manage team
Book a demo
Switch team
Your drafts
Create team...
Upgrade
weathered-morning-8061
weathered-morning-8061.tines.com
Tags
Templates
Users
Reporting
Settings
All
Search credentials...
New
https://weathered-morning-8061.tines.com/teams/29865/credentials

No credentials

Use credentials to connect with external services or create and store custom sensitive information such as API Tokens and passwords

Step 6. Connecting Slack to Tines

1. Back in **Tines**, use the **Slack template** from the **Templates Library**:
   - **Action**: Send a Message.
   - **Description**: Post a message to a public or private channel.
2. Use the channel identifier (ID) for `#alerts`:
   - Go to **Slack**, select **#alerts > Channel Details**.
   - Copy the **Channel ID** and paste it into the Tines configuration.



Send a message

Description

Posts a message to a public channel, private channel, or direct message/IM channel.

Link to documentation: https://api.slack.com/methods/chat.postMessage

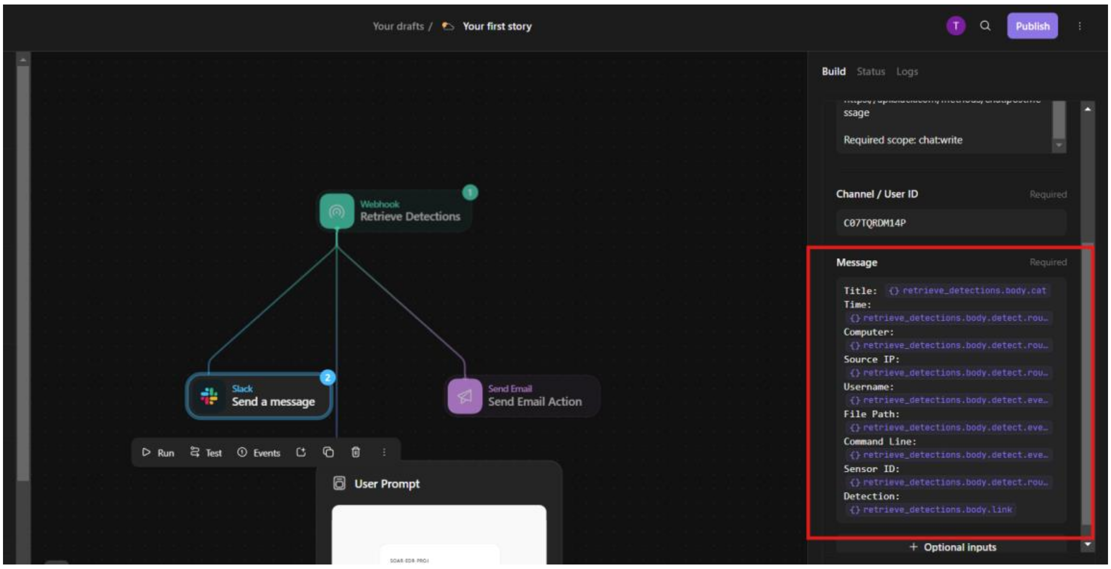
Required scope: chat:write

Channel / User ID (Required): C07TQRDM14P

Message (Required): Hello, *world*!

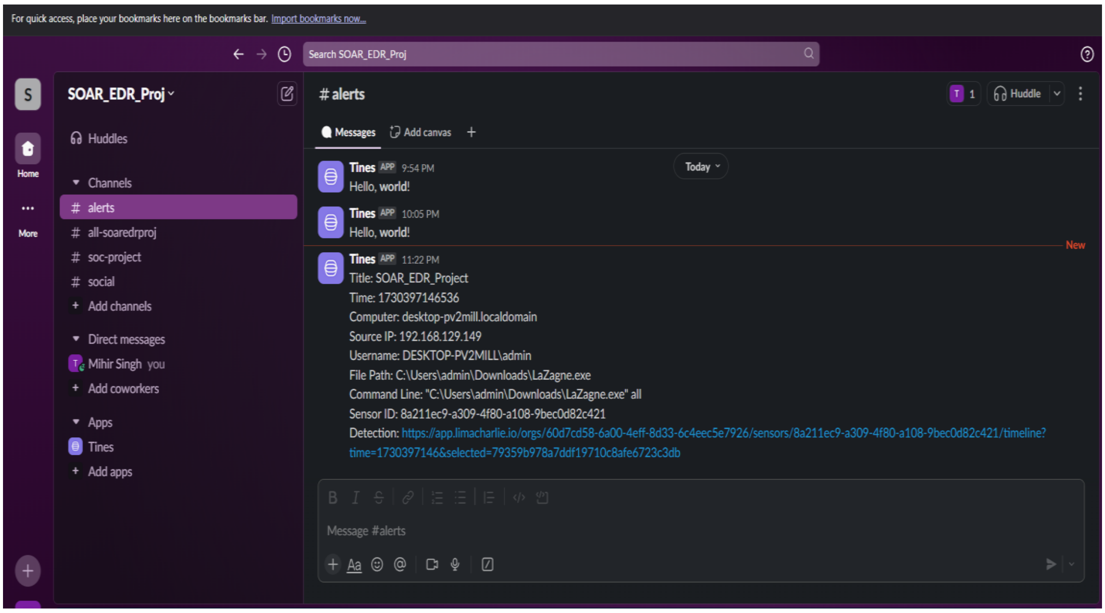
Step 7. Automating Alert Messaging in Slack

1. **Configure Slack Messaging in Tines**:
    - Use the Slack action in Tines to send a message to the alerts channel upon receiving a detection.
    - Customize the message with relevant detection details such as:
        - Detection time
        - Computer name
        - Source IP
        - Detection link for investigation



```
ssage

Required scope: chat:write

Channel / User ID
C07TQRDM14P

Message
Title: {} retrieve_detections.body.cat
Time:
{} retrieve_detections.body.detect.rou…
Computer:
{} retrieve_detections.body.detect.rou…
Source IP:
{} retrieve_detections.body.detect.rou…
Username:
{} retrieve_detections.body.detect.eve…
File Path:
{} retrieve_detections.body.detect.eve…
Command Line:
{} retrieve_detections.body.detect.eve…
Sensor ID:
{} retrieve_detections.body.detect.rou…
Detection:
{} retrieve_detections.body.link
```

2. **Test Slack Messaging**:
    - Run the detection scenario to verify that Tines successfully posts an alert to Slack, containing all relevant information.



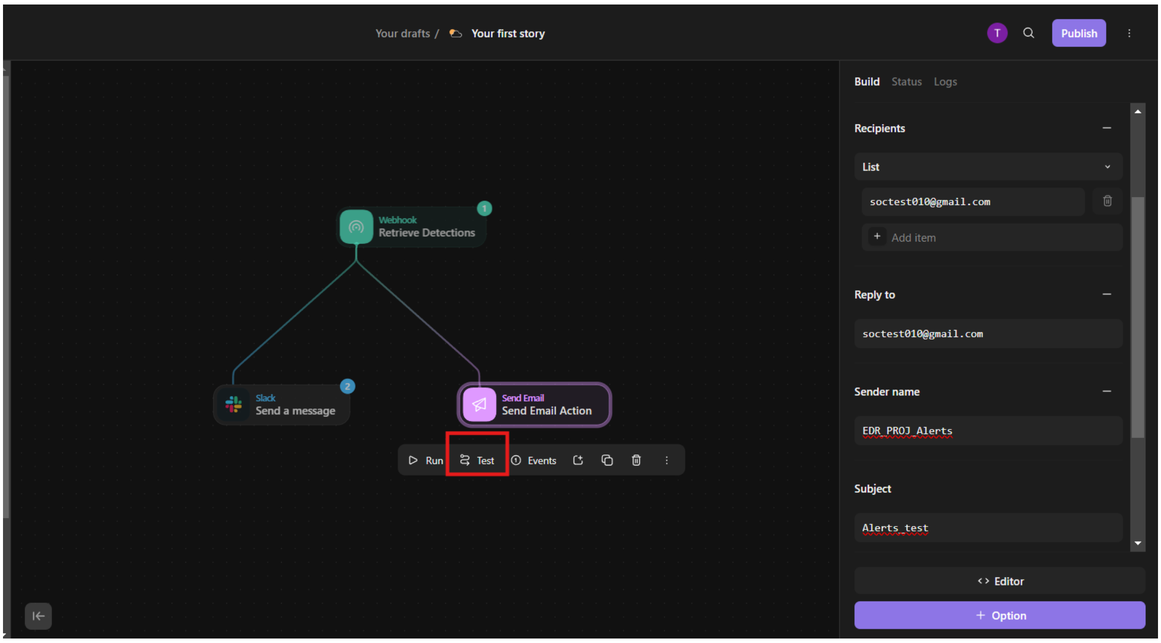
Tines APP 9:54 PM
Hello, world!

Tines APP 10:05 PM
Hello, world!

Tines APP 11:22 PM
Title: SOAR_EDR_Project
Time: 1730397146536
Computer: desktop-pv2mill.localdomain
Source IP: 192.168.129.149
Username: DESKTOP-PV2MILL\admin
File Path: C:\Users\admin\Downloads\LaZagne.exe
Command Line: "C:\Users\admin\Downloads\LaZagne.exe" all
Sensor ID: 8a211ec9-a309-4f80-a108-9bec0d82c421
Detection: https://app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421/timeline?time=1730397146&selected=79359b978a7ddf19710c8afe6723c3db

Step 8. Setting up Email Alerts in Tines

1. **Create an Email Action**:
   - ○ In Tines, add an **Email** action, using a disposable email address if necessary.
   - ○ Customize the email body with detection details similar to the Slack alert.



Recipients

List

soctest010@gmail.com

+ Add item

Reply to

soctest010@gmail.com

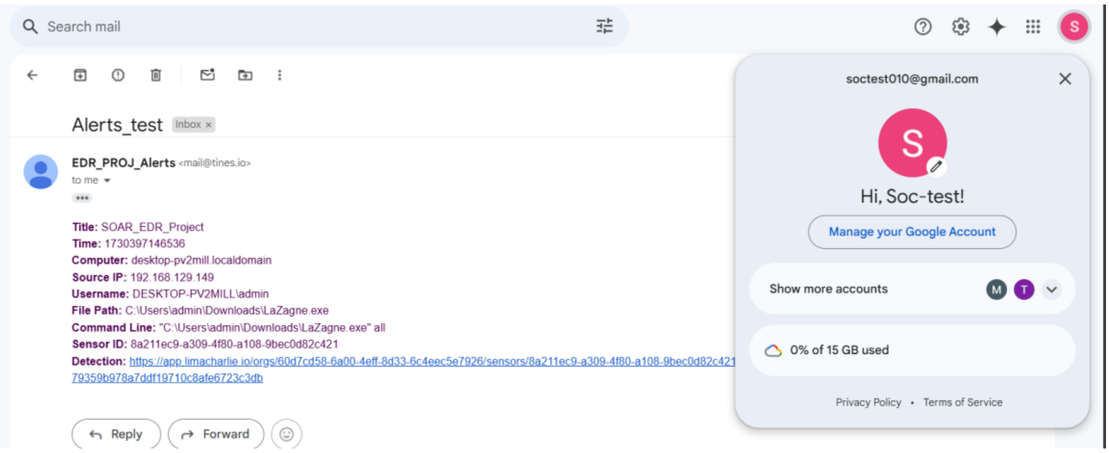
Sender name

EDR_PROJ_Alerts

Subject

Alerts_test

2. **Test Email Alerts**:
   - ○ Trigger a detection and confirm that an email is sent with the appropriate alert information.



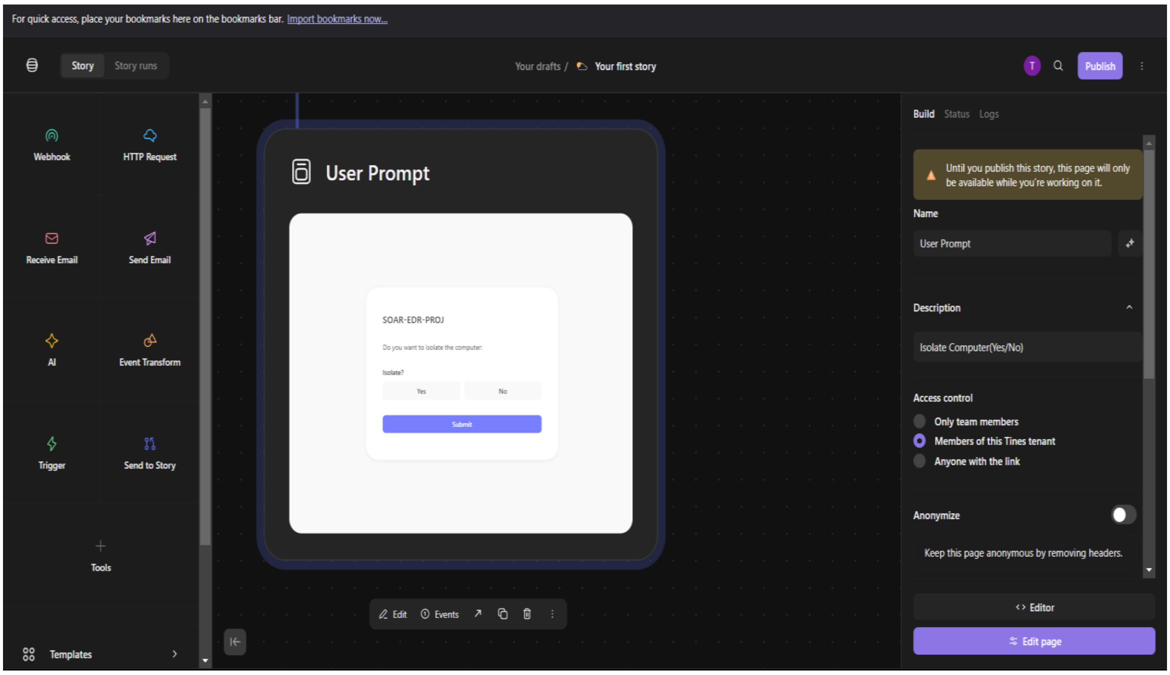
Alerts_test

EDR_PROJ_Alerts <mail@tines.io>
to me

Title: SOAR_EDR_Project
Time: 1730397146536
Computer: desktop-pv2mill.localdomain
Source IP: 192.168.129.149
Username: DESKTOP-PV2MILL\admin
File Path: C:\Users\admin\Downloads\LaZagne.exe
Command Line: "C:\Users\admin\Downloads\LaZagne.exe" all
Sensor ID: 8a211ec9-a309-4f80-a108-9bec0d82c421
Detection: https://app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421
79359b978a7ddf19710c8afe6723c3db

Step 9. Adding a User Prompt for Isolation Decision

1. **Create a User Prompt**:
   - ○ In Tines, create a **Page** action to prompt the user with a Yes/No option to decide whether to isolate the affected machine.
   - ○ Include detection details in the prompt so the user can make an informed decision.



Until you publish this story, this page will only be available while you're working on it.

Name: User Prompt

Description: Isolate Computer(Yes/No)

Access control
- ○ Only team members
- ● Members of this Tines tenant
- ○ Anyone with the link

Anonymize

Keep this page anonymous by removing headers.

SOAR-EDR-PROJ

Do you want to isolate the computer:

Isolate?

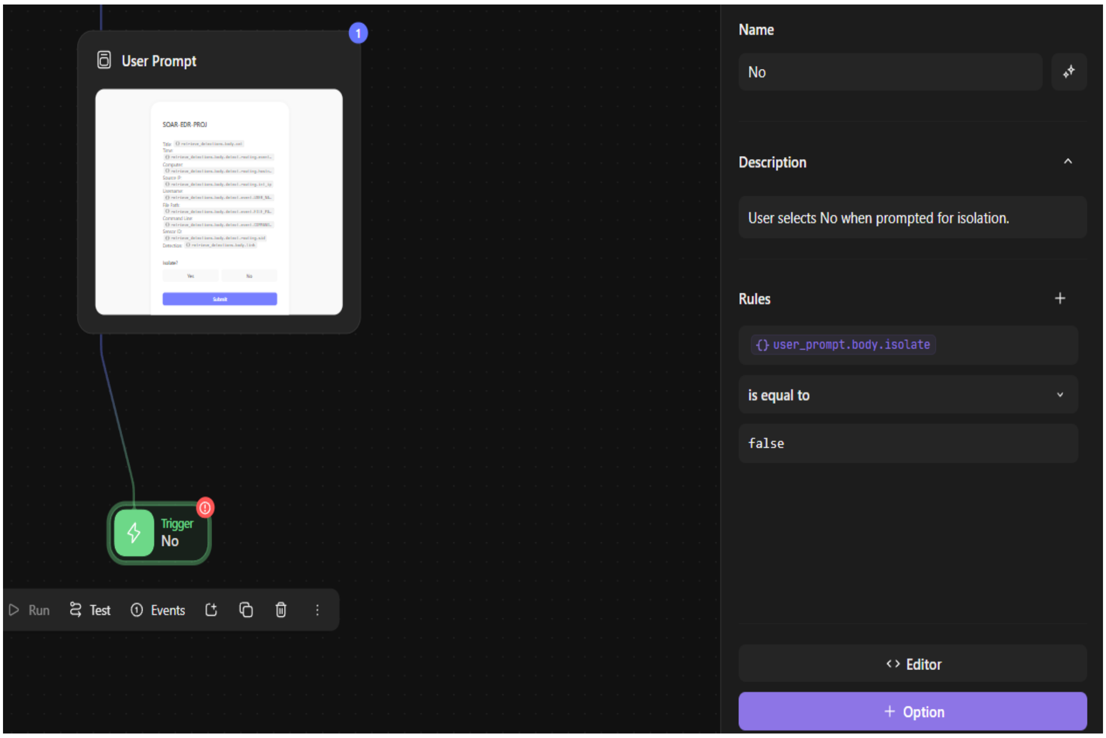
Yes No

Submit

2. **If-Else Actions for User Response**:
   - Use **If-Else** actions to handle responses:
     - If Yes, trigger isolation through LimaCharlie.
     - If No, send a Slack message to indicate that isolation was not performed.

Step 10. Handling the scenario where the user selects 'NO' for isolation

1. **Add Trigger**:
   - Add trigger in the flow chart and connect it with user prompt page.



Name: No

Description: User selects No when prompted for isolation.

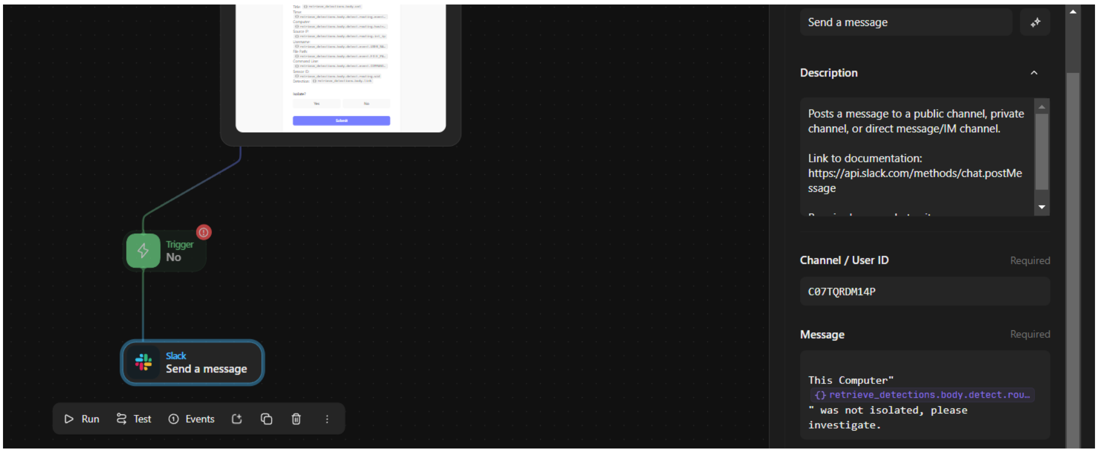
Rules

```
user_prompt.body.isolate
```

is equal to

```
false
```

- Add a new slack to send message as shown in the flow chart.



Send a message

Description

Posts a message to a public channel, private channel, or direct message/IM channel.

Link to documentation: https://api.slack.com/methods/chat.postMessage

Channel / User ID Required

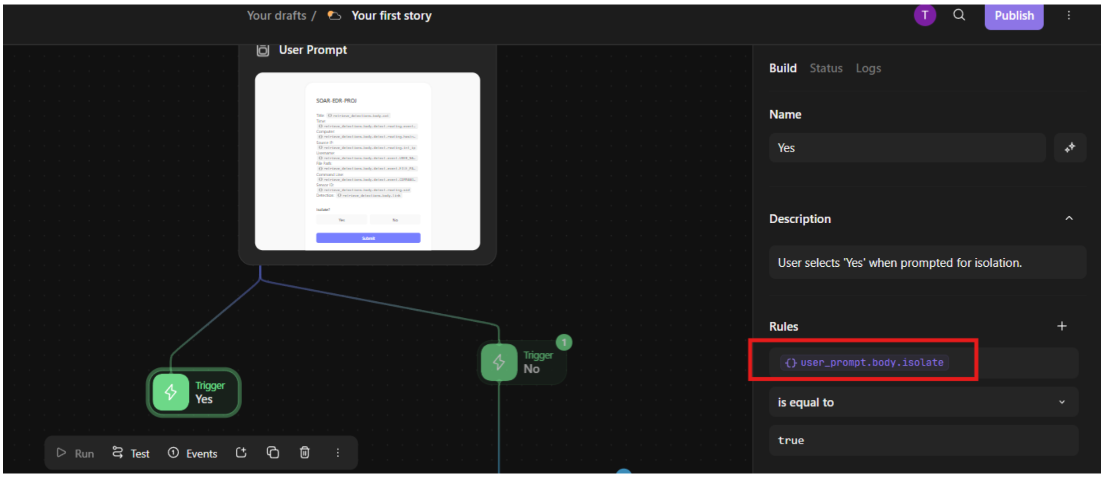
C07TQRDM14P

Message Required

```
This Computer" {} retrieve_detections.body.detect.rou…
" was not isolated, please
investigate.
```

Step 11. Automating Machine Isolation in LimaCharlie

1. **Add new Trigger Action:**
   - Add new Trigger "Yes" to the flowchart and add the isolate path from user prompt.



Build Status Logs

Name

Yes

Description

User selects 'Yes' when prompted for isolation.

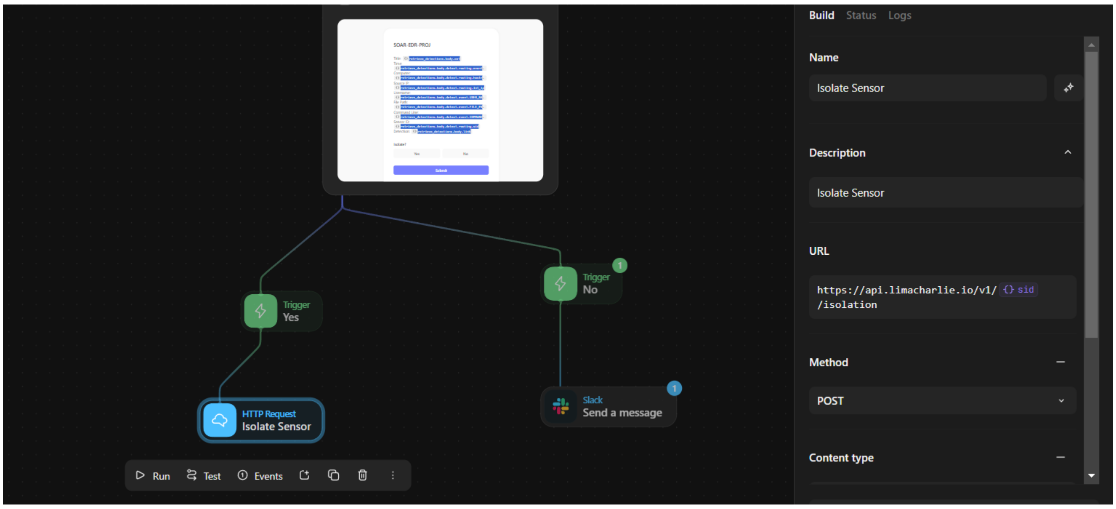
Rules

{} user_prompt.body.isolate

is equal to

true

   - Add Lima Charlie Action and connect it to Trigger "Yes" and select "Isolate Sensor" Template.



Build Status Logs

Name

Isolate Sensor

Description

Isolate Sensor

URL

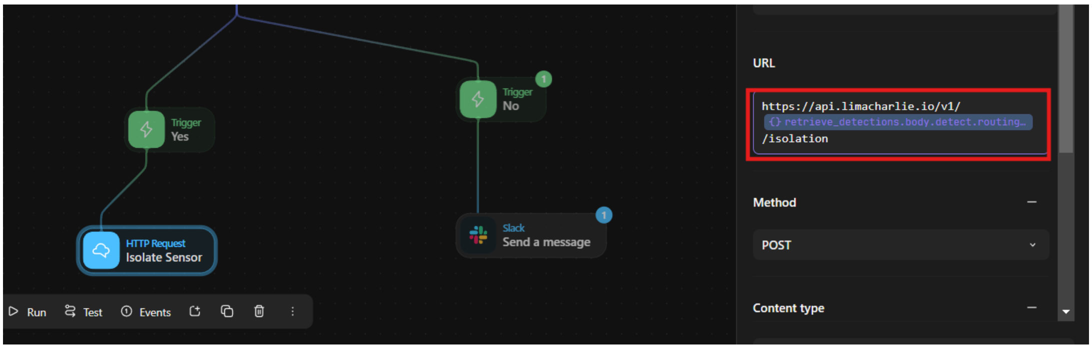
```
https://api.limacharlie.io/v1/ {} sid
/isolation
```

Method

POST

Content type

2. **Add Isolation Command**:
    - Use the **LimaCharlie action** in Tines to send an isolation command to the detected machine.
    - Use the **Sensor ID** to specify the target machine.



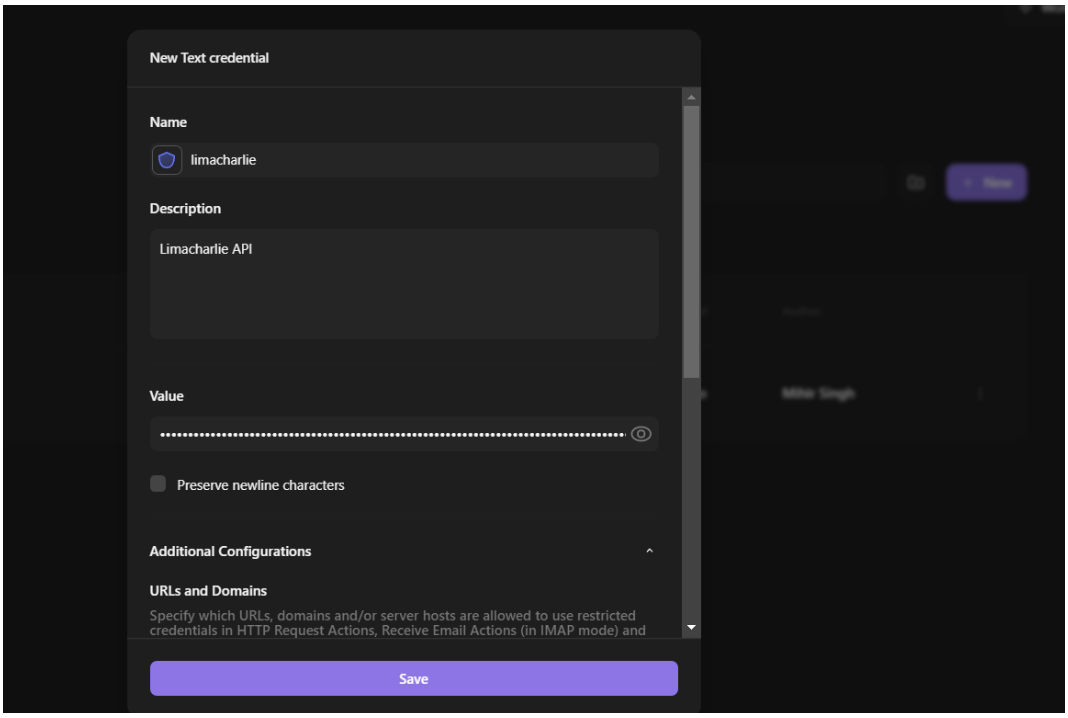
URL

```
https://api.limacharlie.io/v1/
{} retrieve_detections.body.detect.routing…
/isolation
```

Method: POST

Content type

    - Add LimaCharlie as a credential using its API



New Text credential

Name: limacharlie

Description: Limacharlie API

Value: ••

□ Preserve newline characters

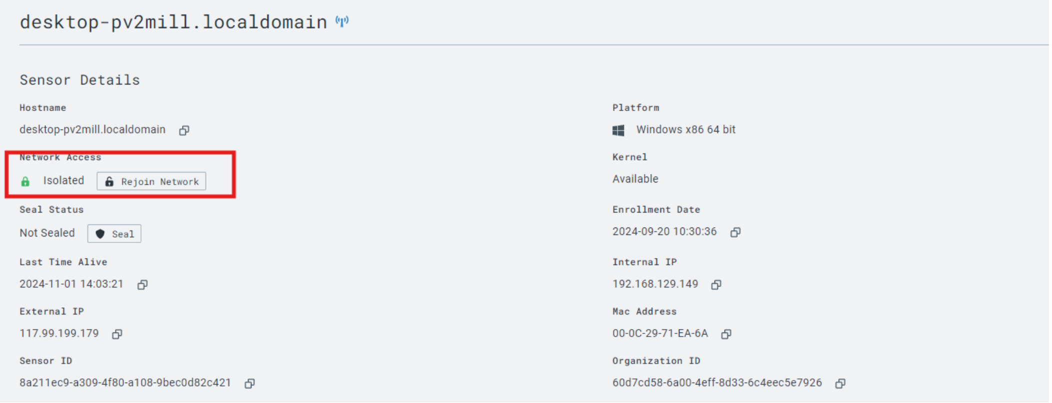
Additional Configurations

URLs and Domains

Specify which URLs, domains and/or server hosts are allowed to use restricted credentials in HTTP Request Actions, Receive Email Actions (in IMAP mode) and

Save

    - Confirm with a test that the machine is isolated successfully.

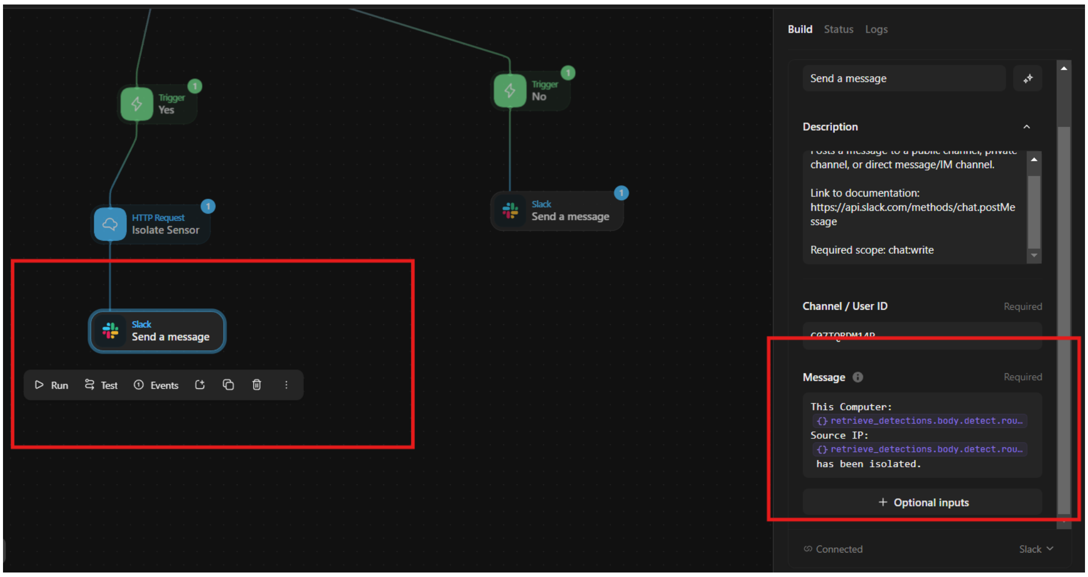


desktop-pv2mill.localdomain

Sensor Details

Hostname desktop-pv2mill.localdomain	Platform Windows x86 64 bit
Network Access Isolated Rejoin Network	Kernel Available
Seal Status Not Sealed Seal	Enrollment Date 2024-09-20 10:30:36
Last Time Alive 2024-11-01 14:03:21	Internal IP 192.168.129.149
External IP 117.99.199.179	Mac Address 00-0C-29-71-EA-6A
Sensor ID 8a211ec9-a309-4f80-a108-9bec0d82c421	Organization ID 60d7cd58-6a00-4eff-8d33-6c4eec5e7926

2. **Send Isolation Status to Slack**:
   - Once isolation is complete, send a Slack message confirming the machine's isolation status.



Send a message

Description

Posts a message to a public channel, private channel, or direct message/IM channel.

Link to documentation: https://api.slack.com/methods/chat.postMessage

Required scope: chat:write

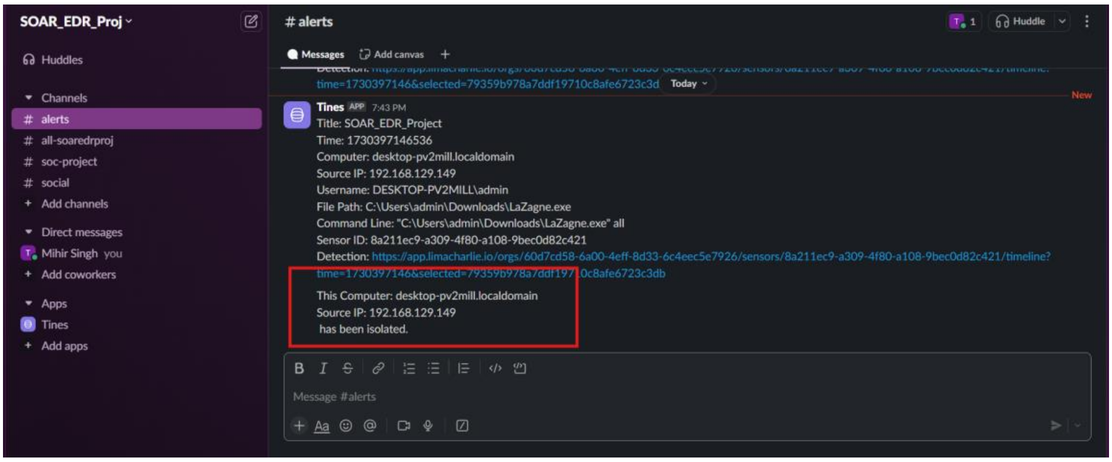
Channel / User ID — Required

C07TQBDM14P

Message — Required

```
This Computer:
{} retrieve_detections.body.detect.rou…
Source IP:
{} retrieve_detections.body.detect.rou…
 has been isolated.
```

   - Now test the slack message to check the final test.



Detection: https://app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421/timeline?time=1730397146&selected=79359b978a7ddf19710c8afe6723c3d

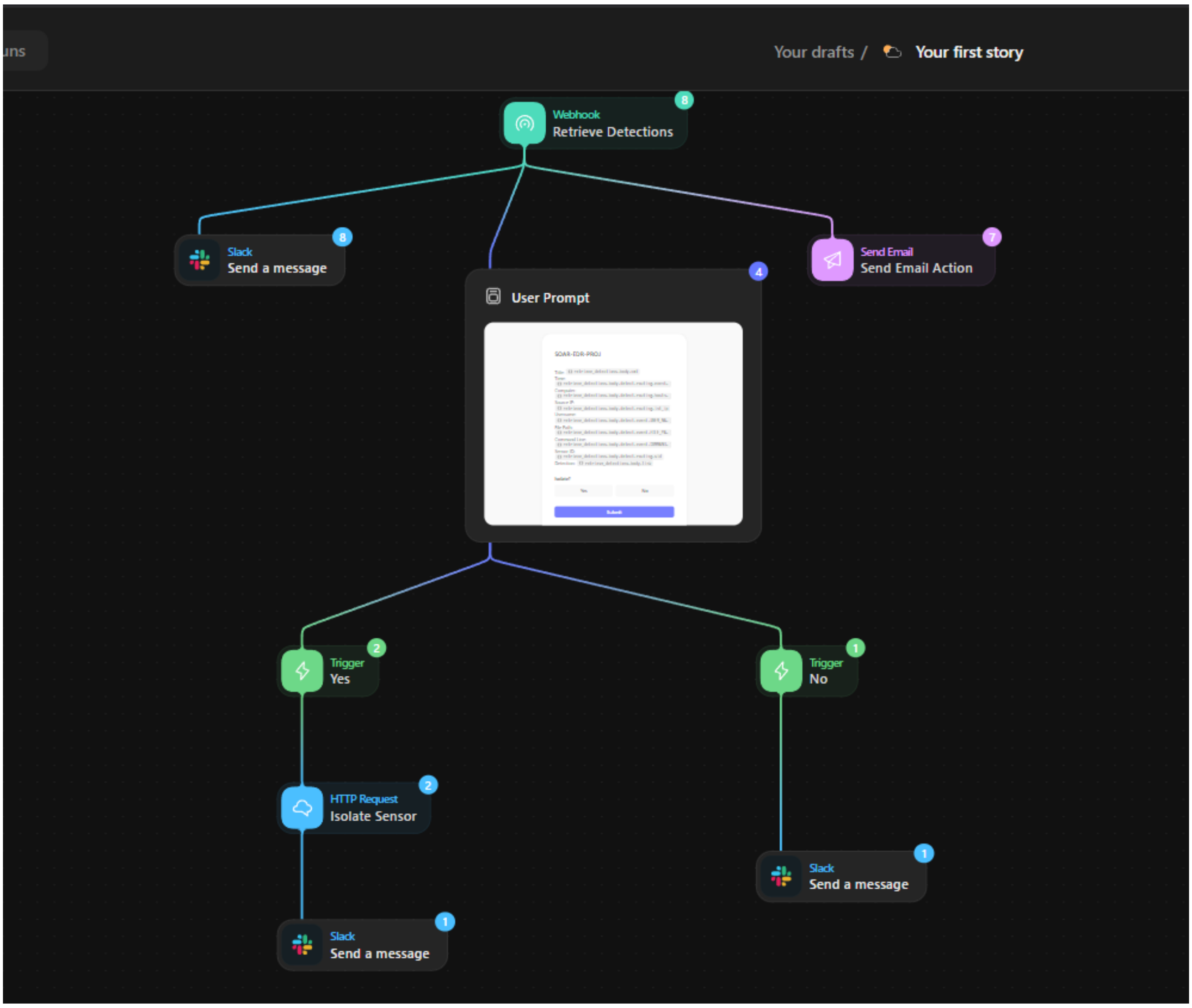
Tines APP 7:43 PM

Title: SOAR_EDR_Project
Time: 1730397146536
Computer: desktop-pv2mill.localdomain
Source IP: 192.168.129.149
Username: DESKTOP-PV2MILL\admin
File Path: C:\Users\admin\Downloads\LaZagne.exe
Command Line: "C:\Users\admin\Downloads\LaZagne.exe" all
Sensor ID: 8a211ec9-a309-4f80-a108-9bec0d82c421
Detection: https://app.limacharlie.io/orgs/60d7cd58-6a00-4eff-8d33-6c4eec5e7926/sensors/8a211ec9-a309-4f80-a108-9bec0d82c421/timeline?time=1730397146&selected=79359b978a7ddf19710c8afe6723c3db

This Computer: desktop-pv2mill.localdomain
Source IP: 192.168.129.149
 has been isolated.

With this the SOAR-EDR Automation project is completed.

Final Tines Workflow


uns
Your drafts /
Your first story
Webhook
Retrieve Detections
8
Slack
Send a message
8
Send Email
Send Email Action
7
User Prompt
4
SOAR-EDR-PROJ
Title
Time
Computer
Source IP
Username
File Path
Command Line
Sensor ID
Detection
Isolate?
Yes
No
Submit
Trigger
Yes
2
Trigger
No
1
HTTP Request
Isolate Sensor
2
Slack
Send a message
1
Slack
Send a message
1