Lima Charlie Virtual Lab Report

By Mohammed Raseem

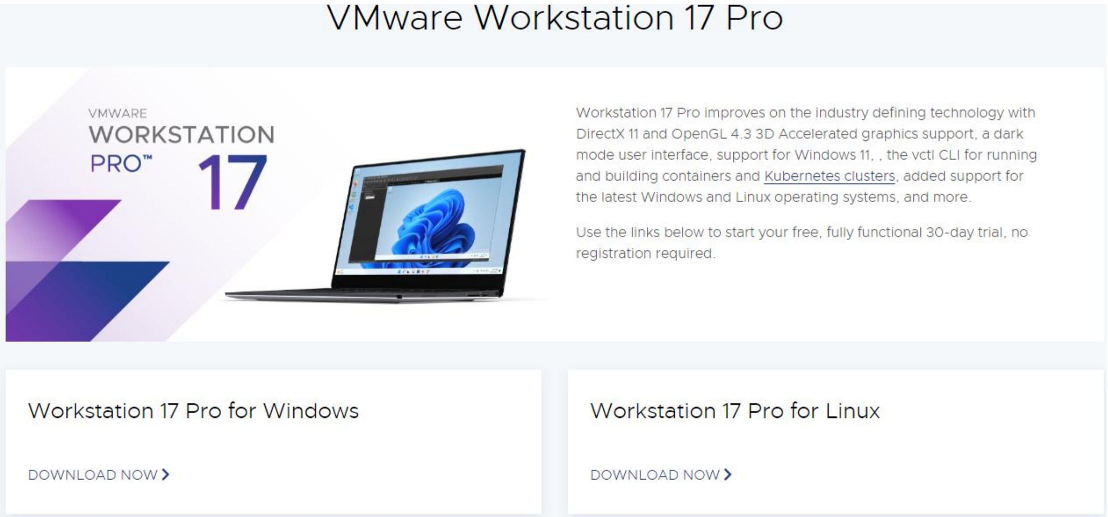
Introduction:

As I explore into the cybersecurity field and pursue my career, I'm keen on honing various tools and techniques in the field. This segment focuses on Environment Setup, LimaCharlie Configuration, and Sliver (C2) Implementation. Mastering these aspects is crucial for aspiring Security Operations Center (SOC) Analysts, requiring practical experience and hands-on expertise. Inspired by Eric Capuano insightful guides, this series delves into the foundational steps of establishing a virtual security lab. In this initial installment, we focus on creating a virtual environment and integrating essential tools while leveraging Ubuntu Server, Windows, and VMware Workstation. Additionally, we'll explore the concepts of LimaCharlie and Sliver (C2) and their significance in the Cybersecurity landscape.

Setting Up the Virtual Lab:

- ### Installing VMware Workstation:

I began by downloading and installing VMware Workstation from the official website. Following the installation instructions, I launched the software to initiate the setup process for my virtual environment.



VMware Workstation 17 Pro

Workstation 17 Pro improves on the industry defining technology with DirectX 11 and OpenGL 4.3 3D Accelerated graphics support, a dark mode user interface, support for Windows 11, , the vctl CLI for running and building containers and Kubernetes clusters, added support for the latest Windows and Linux operating systems, and more.

Use the links below to start your free, fully functional 30-day trial, no registration required.

Workstation 17 Pro for Windows

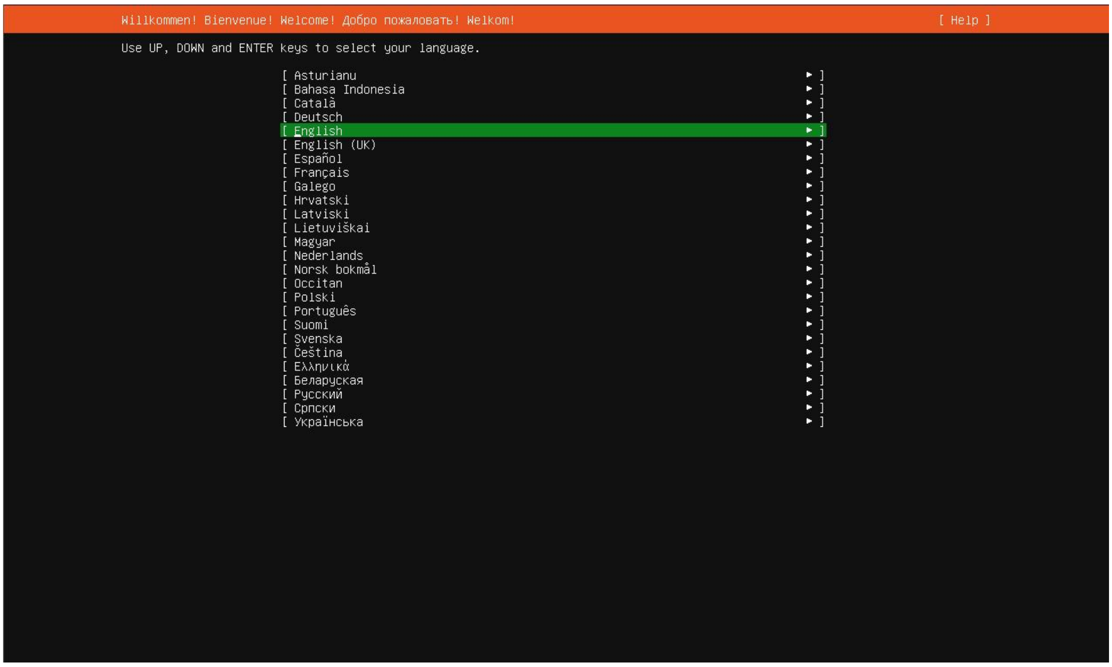
DOWNLOAD NOW ›

Workstation 17 Pro for Linux

DOWNLOAD NOW ›

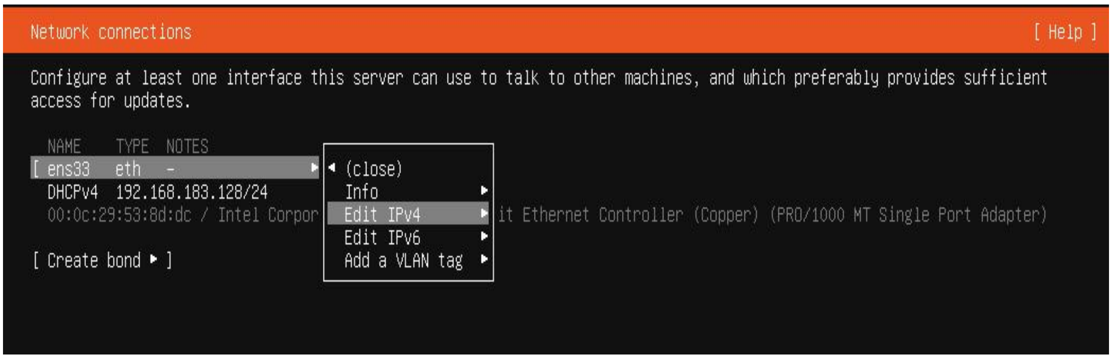
• Installing Ubuntu Server in a New Virtual Machine

With the Ubuntu Server ISO file obtained from the official Ubuntu website, I created a new VM in VMware Workstation. Using the downloaded ISO file as the installer image, I proceeded with the Ubuntu Server installation.



```
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!                    [ Help ]

Use UP, DOWN and ENTER keys to select your language.

                    [ Asturianu                                        ▸ ]
                    [ Bahasa Indonesia                                 ▸ ]
                    [ Català                                           ▸ ]
                    [ Deutsch                                          ▸ ]
                    [ English                                          ▸ ]
                    [ English (UK)                                     ▸ ]
                    [ Español                                          ▸ ]
                    [ Français                                         ▸ ]
                    [ Galego                                           ▸ ]
                    [ Hrvatski                                         ▸ ]
                    [ Latviski                                         ▸ ]
                    [ Lietuviškai                                      ▸ ]
                    [ Magyar                                           ▸ ]
                    [ Nederlands                                       ▸ ]
                    [ Norsk bokmål                                     ▸ ]
                    [ Occitan                                          ▸ ]
                    [ Polski                                           ▸ ]
                    [ Português                                        ▸ ]
                    [ Suomi                                            ▸ ]
                    [ Svenska                                          ▸ ]
                    [ Čeština                                          ▸ ]
                    [ Ελληνικά                                         ▸ ]
                    [ Беларуская                                       ▸ ]
                    [ Русский                                          ▸ ]
                    [ Српски                                           ▸ ]
                    [ Українська                                       ▸ ]
```

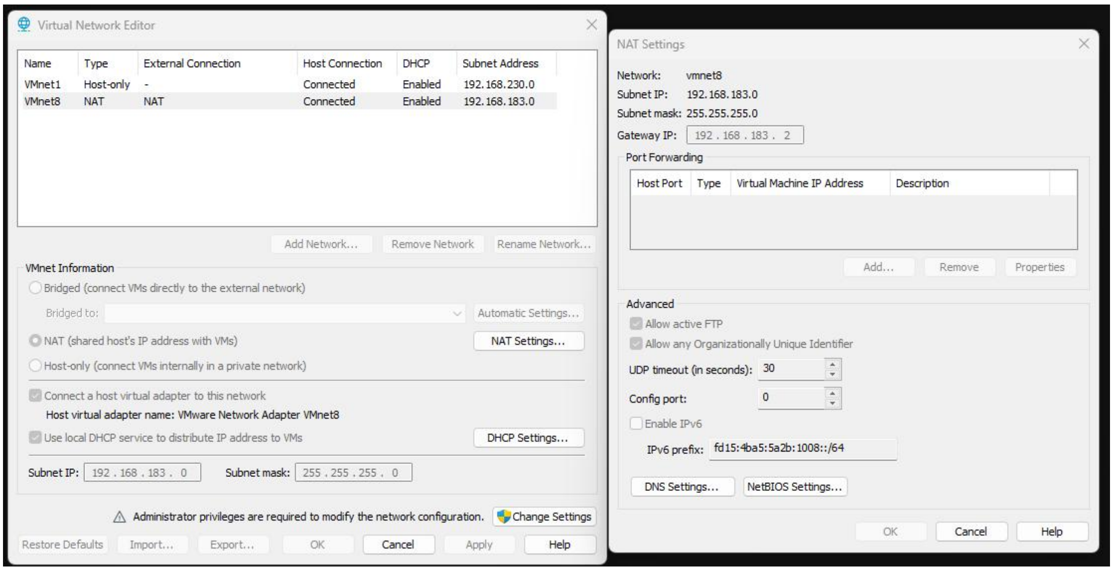
As I progressed through the Ubuntu Server installation, I reached the "**Network connections**" section where I needed to set a static IP address for the VM. To do this, I followed these steps:



```
Network connections                                                              [ Help ]

Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient
access for updates.

  NAME    TYPE  NOTES
[ ens33   eth   -              ▸ ]  ◂ (close)
  DHCPv4  192.168.183.128/24          Info         ▸
  00:0c:29:53:8d:dc / Intel Corpor    Edit IPv4    ▸ it Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)
                                      Edit IPv6    ▸
[ Create bond ▸ ]                     Add a VLAN tag ▸
```

I opened VMware Workstation and clicked on the "Edit" menu at the top to access the "Virtual Network Editor."

From there, I selected the network type as "NAT" and clicked on "NAT Settings" to proceed with the configuration.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.230.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.183.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to:

● NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 183 . 0   Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration.

NAT Settings

Network: vmnet8

Subnet IP: 192.168.183.0

Subnet mask: 255.255.255.0

Gateway IP: 192 . 168 . 183 . 2

Port Forwarding

Host Port	Type	Virtual Machine IP Address	Description

Advanced

☑ Allow active FTP

☑ Allow any Organizationally Unique Identifier

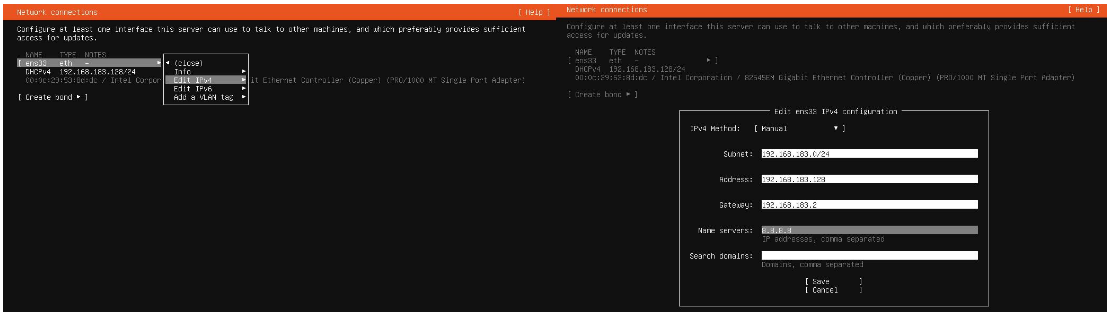
UDP timeout (in seconds): 30

Config port: 0

□ Enable IPv6

IPv6 prefix: fd15:4ba5:5a2b:1008::/64

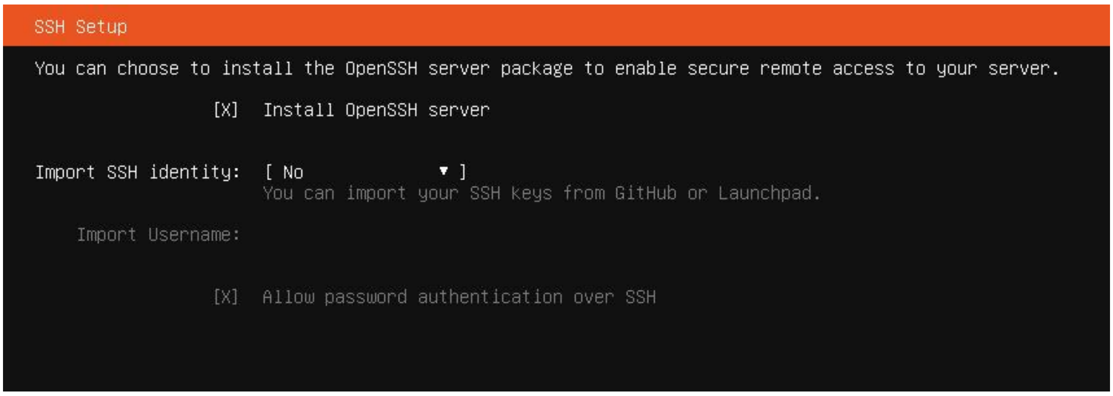
Returning to the Ubuntu installer, I proceeded to change the network interface configuration from DHCPv4 to Manual.



```
Network connections                                                              [ Help ]
Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient
access for updates.

  NAME    TYPE  NOTES
[ ens33   eth   -                 ▸ ◂ (close)
  DHCPv4  192.168.183.128/24          Info          ▸
  00:0c:29:53:8d:dc / Intel Corpor    Edit IPv4     ▸ it Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)
                                      Edit IPv6     ▸
[ Create bond ▸ ]                     Add a VLAN tag ▸
```

```
Network connections                                                              [ Help ]
Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient
access for updates.

  NAME    TYPE  NOTES
[ ens33   eth   -                 ▸ ]
  DHCPv4  192.168.183.128/24
  00:0c:29:53:8d:dc / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)

[ Create bond ▸ ]

         ──────────── Edit ens33 IPv4 configuration ────────────
          IPv4 Method:   [ Manual           ▾ ]

                Subnet:  192.168.183.0/24

               Address:  192.168.183.128

               Gateway:  192.168.183.2

          Name servers:  8.8.8.8
                         IP addresses, comma separated
        Search domains:
                         Domains, comma separated
                                [ Save      ]
                                [ Cancel    ]
```

To facilitate easy command copy/pasting, I installed the OpenSSH server on the Ubuntu machine.

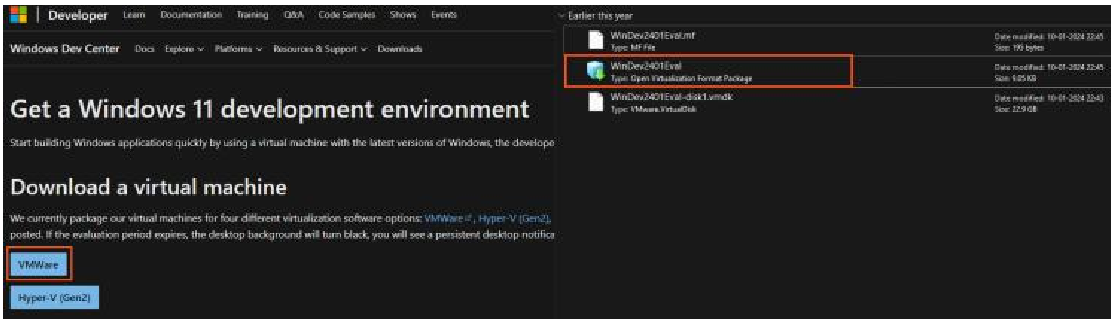


```
SSH Setup

You can choose to install the OpenSSH server package to enable secure remote access to your server.

                  [X]  Install OpenSSH server

Import SSH identity:  [ No              ▾ ]
                      You can import your SSH keys from GitHub or Launchpad.

    Import Username:

                  [X]  Allow password authentication over SSH
```

After configuring the necessary settings, I completed the Ubuntu Server OS installation.

- **Deploying and configuring the Windows Virtual Machine:**

After downloading the Windows virtual machine image from Microsoft 's official source, I imported the VM into VMware Workstation. This involved double-clicking the downloaded file "WinDev2401Eval" and following the on-screen instructions. I made necessary adjustments to the VM's settings, including RAM allocation and disk space.



Get a Windows 11 development environment

Start building Windows applications quickly by using a virtual machine with the latest versions of Windows, the develope

Download a virtual machine

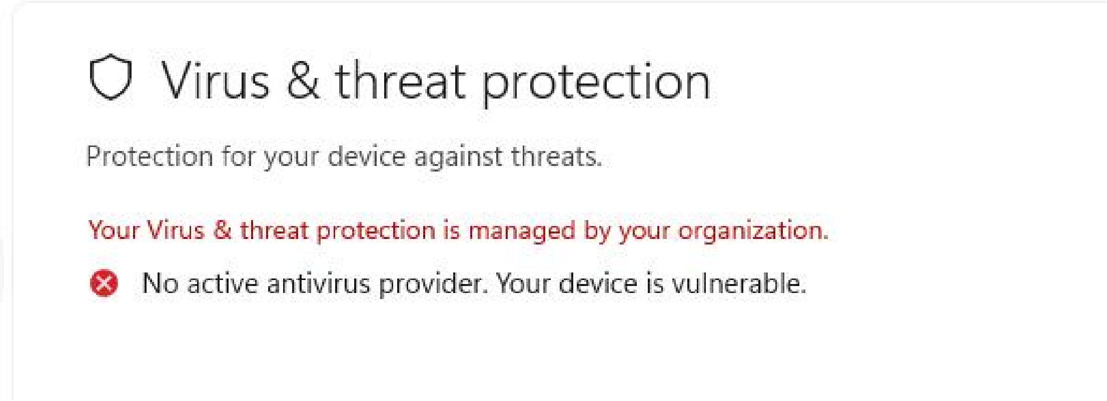
We currently package our virtual machines for four different virtualization software options: VMWare, Hyper-V (Gen2), posted. If the evaluation period expires, the desktop background will turn black, you will see a persistent desktop notifica

WinDev2401Eval.mf
Type: MF File
Date modified: 10-01-2024 22:45
Size: 195 bytes

WinDev2401Eval
Type: Open Virtualization Format Package
Date modified: 10-01-2024 22:45
Size: 9.05 KB

WinDev2401Eval-disk1.vmdk
Type: VMware.VirtualDisk
Date modified: 10-01-2024 22:40
Size: 22.9 GB

I began by starting up the VM, following Eric Capuano's instructions to fully disable Microsoft Defender. Although this action is typically discouraged in production environments, it was necessary for the purpose of this home lab setup to prevent any interference with subsequent activities.



Virus & threat protection

Protection for your device against threats.

Your Virus & threat protection is managed by your organization.

No active antivirus provider. Your device is vulnerable.

- **Install Sysmon in Windows VM**

I proceeded to install Sysmon on the Windows VM. Sysmon serves as a valuable analyst tool, providing detailed telemetry on various activities within the Windows endpoint.

To set up Sysmon on the Windows VM, I followed these steps in an administrative PowerShell session:

Downloaded Sysmon using the following command:

```
Invoke-WebRequest -Uri https://download.sysinternals.com/files/Sysmon.zip -OutFile C:\Windows\Temp\Sysmon.zip
```

Unzipped the Sysmon.zip file:

```
Expand-Archive -LiteralPath C:\Windows\Temp\Sysmon.zip -DestinationPath C:\Windows\Temp\Sysmon
```

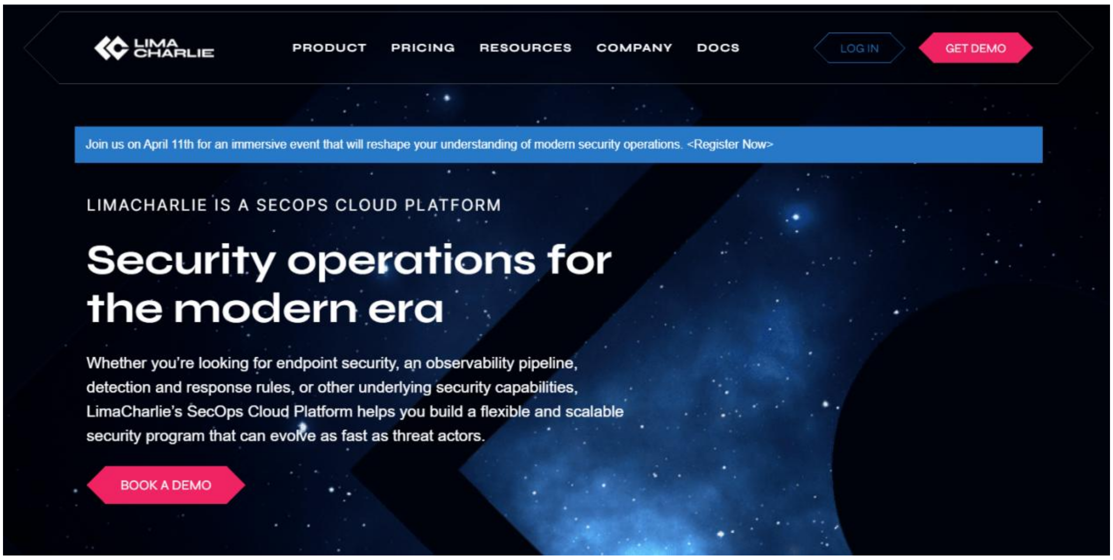
I downloaded the Sysmon configuration provided by SwiftOnSecurity. Utilizing a custom rule set from SwiftOnSecurity enhances logging on a Windows endpoint, providing optimal results when combined with Sysmon.

```
Invoke-WebRequest -Uri https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml -OutFile C:\Windows\Temp\Sysmon\sysmonconfig.xml
```

Installed Sysmon with Swift's configuration using the following command:

```
C:\Windows\Temp\Sysmon\Sysmon64.exe -accepteula -i C:\Windows\Temp\Sysmon\sysmonconfig.xml
```

Install LimaCharlie EDR on Windows Virtual Machine:



Join us on April 11th for an immersive event that will reshape your understanding of modern security operations. <Register Now>

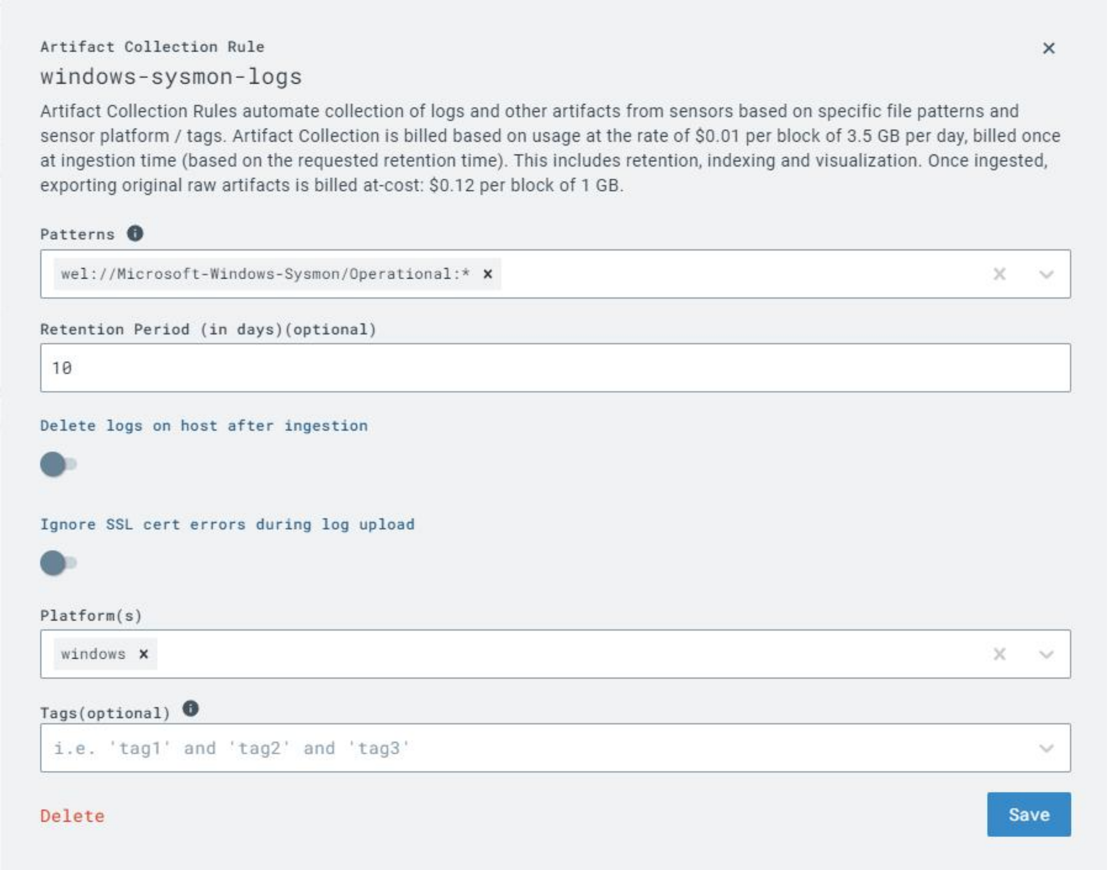
LIMACHARLIE IS A SECOPS CLOUD PLATFORM

Security operations for the modern era

Whether you're looking for endpoint security, an observability pipeline, detection and response rules, or other underlying security capabilities, LimaCharlie's SecOps Cloud Platform helps you build a flexible and scalable security program that can evolve as fast as threat actors.

LimaCharlie serves as a robust SecOps Cloud Platform, providing an extensive suite of features to bolster your cybersecurity defense. It offers a cross-platform EDR agent, robust log management capabilities, and an intelligent threat detection engine. Its comprehensive approach to security makes it akin to having a dedicated security team safeguarding your digital assets around the clock. Additionally, LimaCharlie's provision of a free tier for up to two systems enhances its accessibility for users.

- Begin by creating a free LimaCharlie account.
- After logging into LimaCharlie, proceed to create an organization



Artifact Collection Rule

windows-sysmon-logs

Artifact Collection Rules automate collection of logs and other artifacts from sensors based on specific file patterns and sensor platform / tags. Artifact Collection is billed based on usage at the rate of $0.01 per block of 3.5 GB per day, billed once at ingestion time (based on the requested retention time). This includes retention, indexing and visualization. Once ingested, exporting original raw artifacts is billed at-cost: $0.12 per block of 1 GB.

Patterns: wel://Microsoft-Windows-Sysmon/Operational:*

Retention Period (in days)(optional): 10

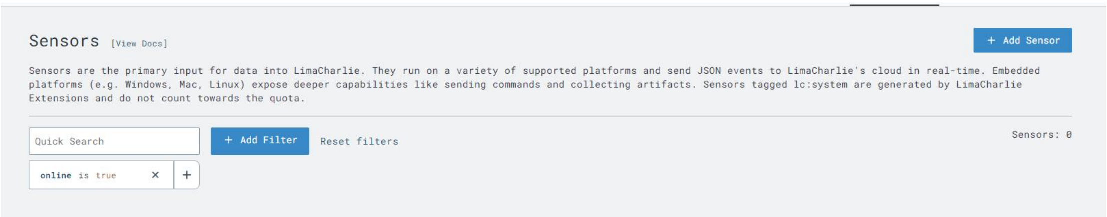
Delete logs on host after ingestion

Ignore SSL cert errors during log upload

Platform(s): windows

Tags(optional): i.e. 'tag1' and 'tag2' and 'tag3'

- After creating the organization, navigate to the "Add Sensor" option.



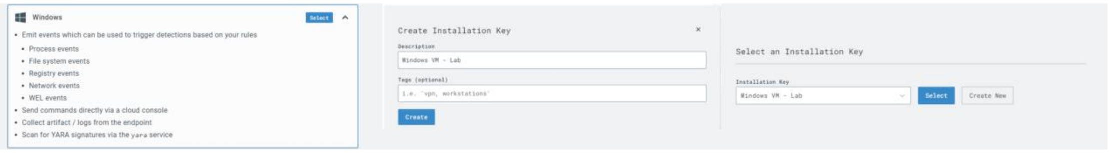
Sensors [View Docs]

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.

Sensors: 0

online is true

- After creating the organization, I proceeded to "Add Sensor," selected "Windows" as the sensor type, provided a description like "Windows VM - Lab," and chose the Installation Key generated earlier.



Windows

- Emit events which can be used to trigger detections based on your rules
  - Process events
  - File system events
  - Registry events
  - Network events
  - WEL events
- Send commands directly via a cloud console
- Collect artifact / logs from the endpoint
- Scan for YARA signatures via the `yara` service

Create Installation Key

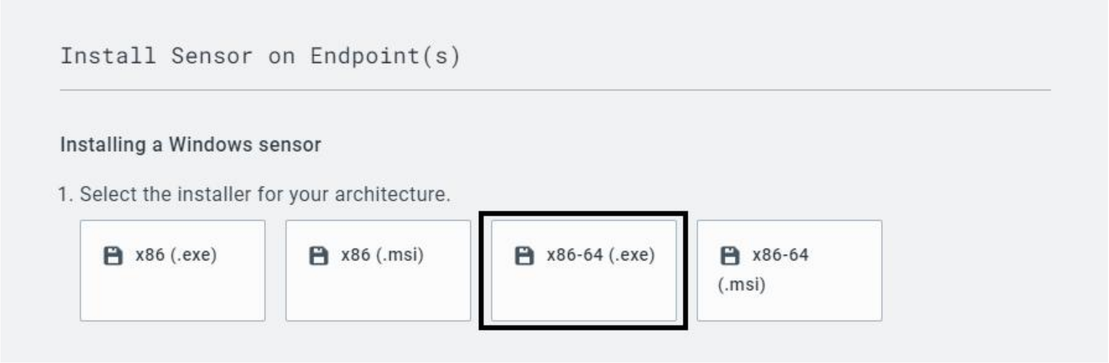
Description: Windows VM - Lab

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

Select an Installation Key

Installation Key: Windows VM - Lab

- Specify the x86-64 (.exe) sensor during the installation process.



Install Sensor on Endpoint(s)

Installing a Windows sensor

1. Select the installer for your architecture.

- In the Windows VM, I opened an Administrative PowerShell prompt and executed the following commands.

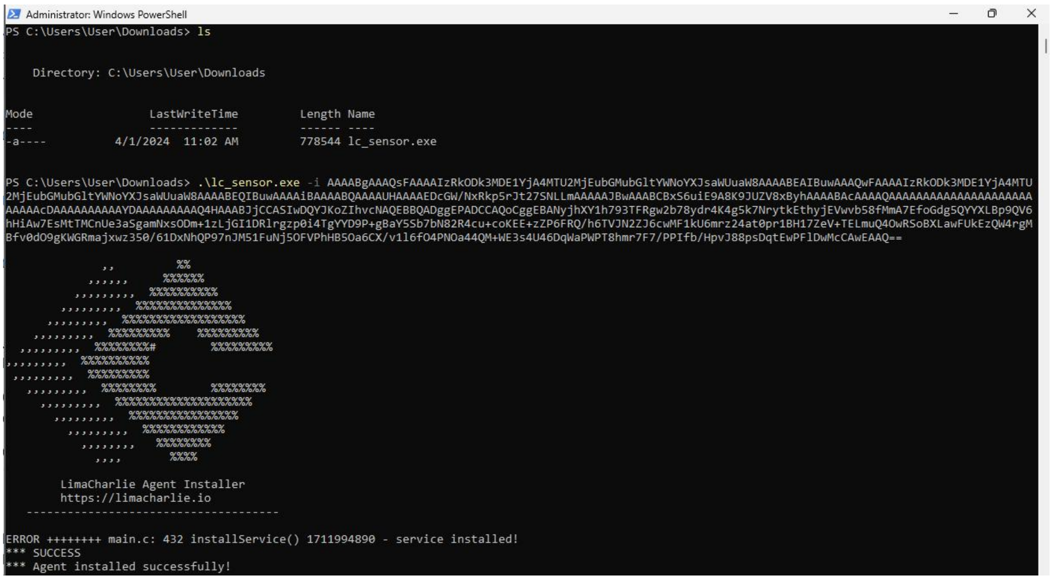
cd C:\Users\User\Downloads

cd C:\Users\User\Downloads

Invoke-WebRequest -Uri https://downloads.limacharlie.io/sensor/windows/64 -Outfile C:\Users\User\Downloads\lc_sensor.exe

- Then, I executed the following command, which contains the installation key.

lc_senser.exe -i AAAABgAAAQsFAAAAIzRkODk3MDE1YjA4MTU2MjEubGMubGltYWNoY....



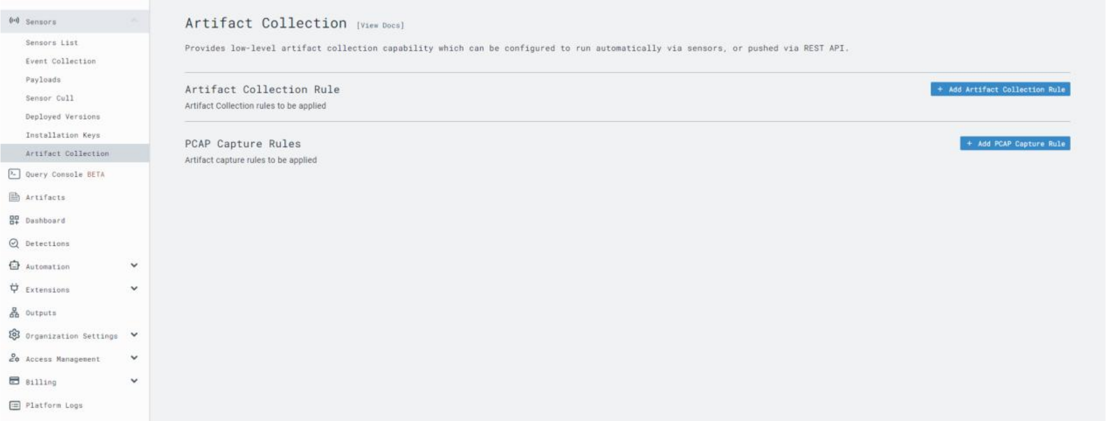
Administrator: Windows PowerShell

```
PS C:\Users\User\Downloads> ls


    Directory: C:\Users\User\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          4/1/2024  11:02 AM         778544 lc_sensor.exe


PS C:\Users\User\Downloads> .\lc_sensor.exe -i AAAABgAAAQsFAAAAIzRkODk3MDE1YjA4MTU2MjEubGMubGltYWNoYXJsaWUuaW8AAAABEAIBuwAAAQwFAAAAIzRkODk3MDE1YjA4MTU
2MjEubGMubGltYWNoYXJsaWUuaW8AAAABEQIBuwAAAAiBAAAABQAAAAUHAAAAEDcGW/NxRkp5rJt27SNLLmAAAAAJBwAAABCBxS6uiE9A8K9JUZV8xByhAAAABAcAAAAQAAAAAAAAAAAAAAAAAAAA
AAAAAcDAAAAAAAAAAYDAAAAAAAAAAQ4HAAABJjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANyjhXY1h793TFRgw2b78ydr4K4g5k7NrytkEthyjEVwvb58fMmA7EfoGdg5QYYXLBp9QV6
hHiAw7EsMtTMCnUe3aSgamNxsODm+1zLjGI1DRlrgzp0i4TgYYD9P+gBaY5Sb7bN82R4cu+coKEE+zZP6FRQ/h6TVJN2ZJ6cwMF1kU6mrz24at0pr1BH17ZeV+TELmuQ4OwRSoBXLawFUkEzQW4rgM
Bfv0dO9gKWGRmajxwz350/61DxNhQP97nJM51FuNj5OFVPhHB5Oa6CX/v1l6fO4PNOa44QM+WE3s4U46DqWaPWPT8hmr7F7/PPIfb/HpvJ88psDqtEwPFlDwMcCAwEAAQ==

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

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

ERROR ++++++++ main.c: 432 installService() 1711994890 - service installed!
*** SUCCESS
*** Agent installed successfully!
```

I observed that the LimaCharlie web UI showed the sensor reporting in.

- Next, I configured LimaCharlie to also send the Sysmon event logs along with its own EDR telemetry.

Navigate to the left-side menu and select "Artifact Collection."



Artifact Collection

Provides low-level artifact collection capability which can be configured to run automatically via sensors, or pushed via REST API.

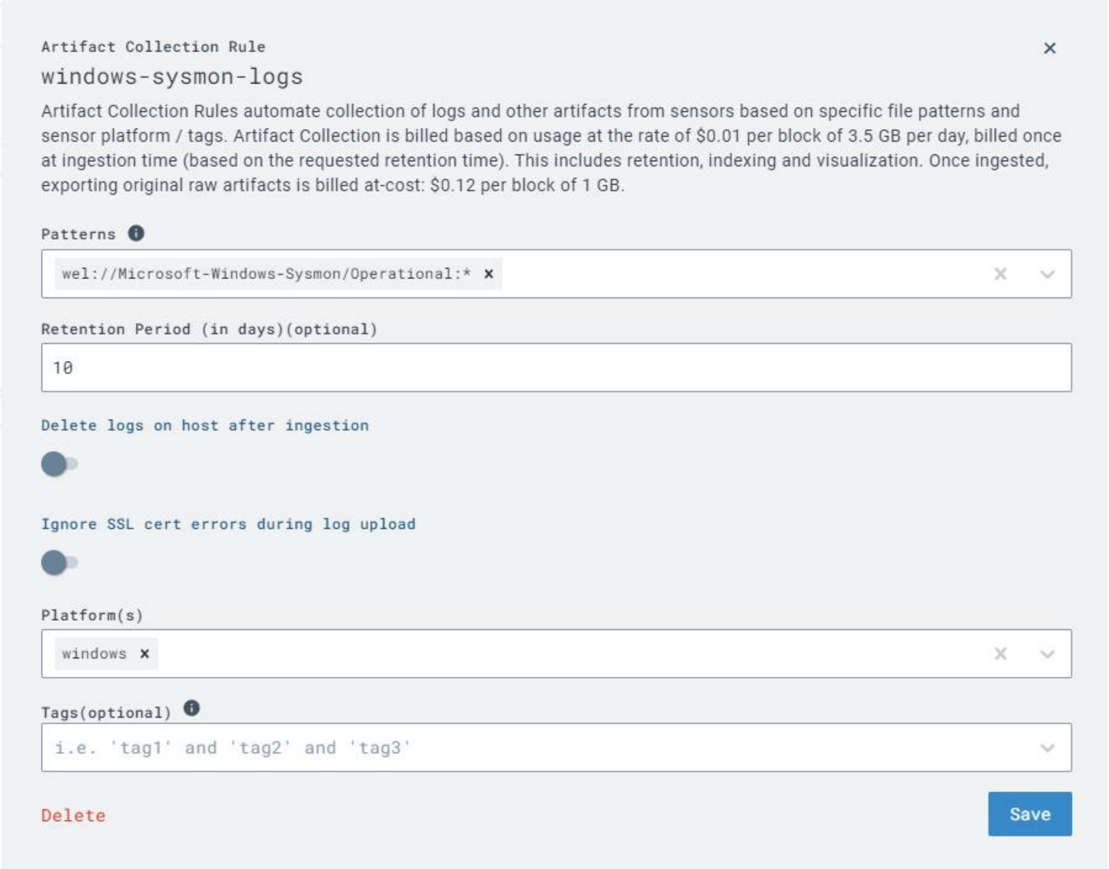
Artifact Collection Rule

Artifact Collection rules to be applied

PCAP Capture Rules

Artifact capture rules to be applied

Create a new Rule



Artifact Collection Rule

windows-sysmon-logs

Artifact Collection Rules automate collection of logs and other artifacts from sensors based on specific file patterns and sensor platform / tags. Artifact Collection is billed based on usage at the rate of $0.01 per block of 3.5 GB per day, billed once at ingestion time (based on the requested retention time). This includes retention, indexing and visualization. Once ingested, exporting original raw artifacts is billed at-cost: $0.12 per block of 1 GB.

Patterns: wel://Microsoft-Windows-Sysmon/Operational:*

Retention Period (in days)(optional): 10

Delete logs on host after ingestion: ○

Ignore SSL cert errors during log upload: ○

Platform(s): windows

Tags(optional): i.e. 'tag1' and 'tag2' and 'tag3'

Once configured, LimaCharlie will start sending Sysmon logs, offering a wealth of

EDR-like telemetry. Sysmon remains a valuable tool for visibility, working hand in hand with any EDR agent you may have in place.

Configuring the Ubuntu Attack VM:

- For smoother command copying and pasting, I chose to SSH into the Ubuntu VM. Although modern MacOS, Linux, and Windows systems have native SSH capabilities, I decided to use Putty for this home lab setup. I haven't used Putty much in the past, so it's an exciting opportunity to try something new and expand my skills.

- After establishing an SSH connection to the VM, I followed these instructions to configure our attacker C2 server. To gain root privileges, I executed the following command.

```
sudo su
```

- Next, I proceeded to download Sliver, a Command & Control (C2) framework developed by BishopFox. Sliver serves as an open-source post-exploitation C2 framework, providing an alternative to other C2 frameworks like Cobalt Strike and Merlin, or complementing them when used together.
- Obtain the Sliver Linux server binary

```
wgethttps://github.com/BishopFox/sliver/releases/download/v1.5.42/sliver-server_linux -O /usr/local/bin/sliver-server
```

- Grant executable permissions

```
chmod +x /usr/local/bin/sliver-server
```

- Install mingw-w64 to enhance functionality

```
apt install -y mingw-w64
```

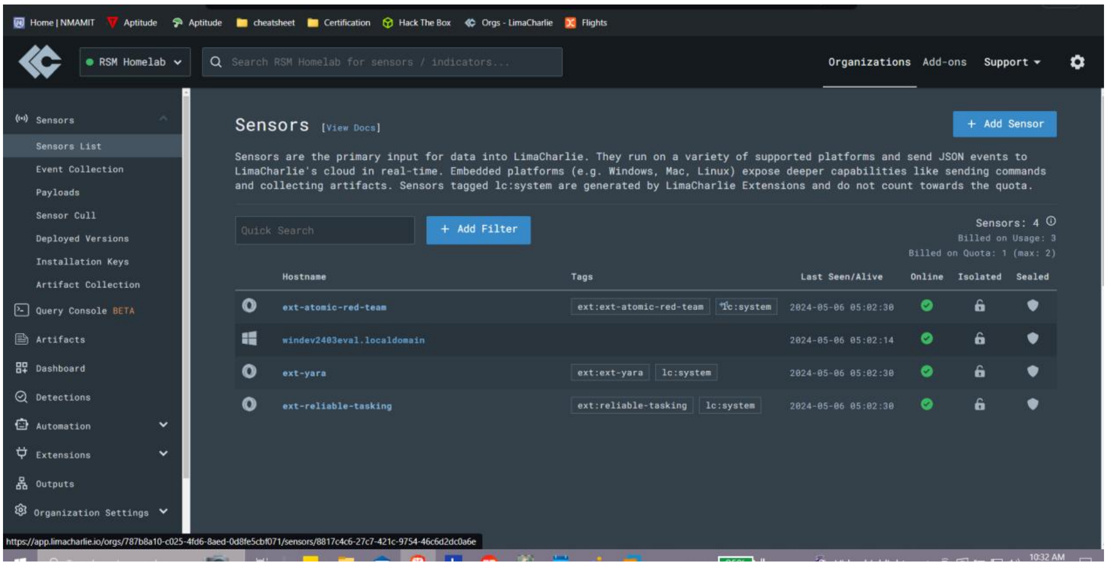
- I created a directory where I'll perform our subsequent tasks.

```
mkdir -p /opt/sliver
```

And I have successfully configured the Sliver C2 on the Ubuntu VM.

Exploring LimaCharlie Web Interface:

Let's take a closer look at the LimaCharlie web interface. I navigated to the "Sensors List" and clicked on the hostname of the sensor I was interested in exploring.



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.

Sensors: 4
Billed on Usage: 3
Billed on Quota: 1 (max: 2)

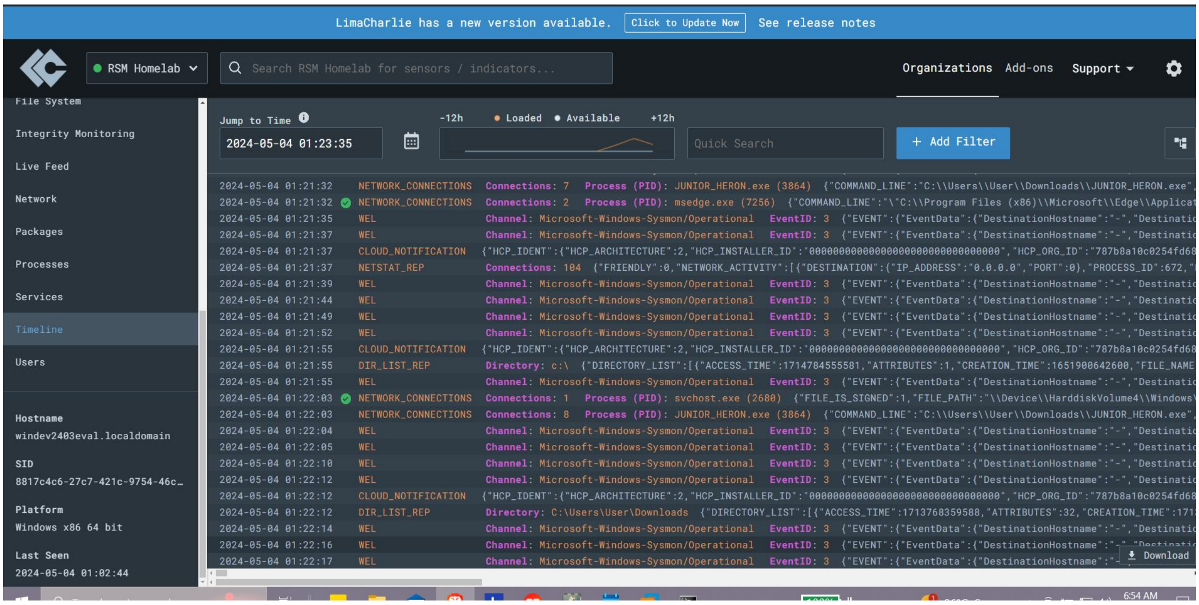
Hostname	Tags	Last Seen/Alive	Online	Isolated	Sealed
ext-atomic-red-team	ext:ext-atomic-red-team lc:system	2024-05-06 05:02:30	✓	🔓	●
windev2403eval.localdomain		2024-05-06 05:02:14	✓	🔓	●
ext-yara	ext:ext-yara lc:system	2024-05-06 05:02:30	✓	🔓	●
ext-reliable-tasking	ext:reliable-tasking lc:system	2024-05-06 05:02:30	✓	🔓	●

https://app.limacharlie.io/orgs/787b8a10-c025-4fd6-8aed-0d8fe5cbf071/sensors/8817c4c6-27c7-421c-9754-46c6d2dc0a6e

10:32 AM

- **Timeline:**

The timeline on Limacharlie EDR provides a chronological view of security events and activities on monitored endpoints, including alerts, endpoint events, incident response actions, and the progression of detected threats. It helps security analysts quickly identify and respond to potential threats.



Jump to Time: 2024-05-04 01:23:35

Hostname: windev2403eval.localdomain

SID: 8817c4c6-27c7-421c-9754-46c…

Platform: Windows x86 64 bit

Last Seen: 2024-05-04 01:02:44

```
2024-05-04 01:21:32    NETWORK_CONNECTIONS  Connections: 7  Process (PID): JUNIOR_HERON.exe (3864)  {"COMMAND_LINE":"C:\\Users\\User\\Downloads\\JUNIOR_HERON.exe",
2024-05-04 01:21:32 ✓  NETWORK_CONNECTIONS  Connections: 2  Process (PID): msedge.exe (7256)  {"COMMAND_LINE":"\"C:\\Program Files (x86)\\Microsoft\\Edge\\Applicat
2024-05-04 01:21:35    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:37    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:37    CLOUD_NOTIFICATION  {"HCP_IDENT":{"HCP_ARCHITECTURE":2,"HCP_INSTALLER_ID":"00000000000000000000000000000000","HCP_ORG_ID":"787b8a10c0254fd68
2024-05-04 01:21:37    NETSTAT_REP          Connections: 104  {"FRIENDLY":0,"NETWORK_ACTIVITY":[{"DESTINATION":{"IP_ADDRESS":"0.0.0.0","PORT":0},"PROCESS_ID":672,"
2024-05-04 01:21:39    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:44    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:49    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:52    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:21:55    CLOUD_NOTIFICATION  {"HCP_IDENT":{"HCP_ARCHITECTURE":2,"HCP_INSTALLER_ID":"00000000000000000000000000000000","HCP_ORG_ID":"787b8a10c0254fd68
2024-05-04 01:21:55    DIR_LIST_REP         Directory: c:\  {"DIRECTORY_LIST":[{"ACCESS_TIME":1714784555581,"ATTRIBUTES":1,"CREATION_TIME":1651900642600,"FILE_NAME
2024-05-04 01:21:55    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:03 ✓  NETWORK_CONNECTIONS  Connections: 1  Process (PID): svchost.exe (2680)  {"FILE_IS_SIGNED":1,"FILE_PATH":"\\Device\\HarddiskVolume4\\Windows\
2024-05-04 01:22:03    NETWORK_CONNECTIONS  Connections: 8  Process (PID): JUNIOR_HERON.exe (3864)  {"COMMAND_LINE":"C:\\Users\\User\\Downloads\\JUNIOR_HERON.exe",
2024-05-04 01:22:04    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:05    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:10    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:12    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:12    CLOUD_NOTIFICATION  {"HCP_IDENT":{"HCP_ARCHITECTURE":2,"HCP_INSTALLER_ID":"00000000000000000000000000000000","HCP_ORG_ID":"787b8a10c0254fd68
2024-05-04 01:22:12    DIR_LIST_REP         Directory: C:\Users\User\Downloads  {"DIRECTORY_LIST":[{"ACCESS_TIME":1713768359588,"ATTRIBUTES":32,"CREATION_TIME":171
2024-05-04 01:22:14    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:16    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-","Destinatic
2024-05-04 01:22:17    WEL                  Channel: Microsoft-Windows-Sysmon/Operational  EventID: 3  {"EVENT":{"EventData":{"DestinationHostname":"-
```

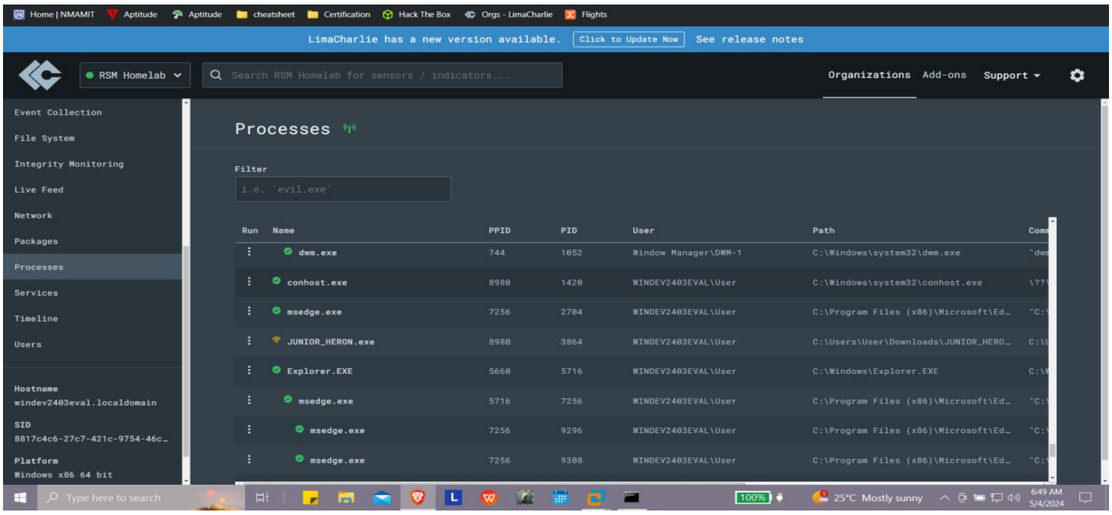
6:54 AM

I conducted an experiment by attempting to send a payload using sliver C2 from the ubuntu server to the the Windows VM where LimaCharlie EDR is installed. Now, I'll check the LimaCharlie web interface's timeline to see if the event has been registered and is available for analysis.

As observed, the ping event was successfully logged and is visible on the timeline in the LimaCharlie web interface. Furthermore, it's noted that the event was captured through the Sysmon channel, affirming that both LimaCharlie and Sysmon are functioning as expected in the setup.

- Processes:

In Limacharlie EDR, the "Processes" section provides a concise overview of the processes running on monitored endpoints, including their names, paths, IDs, parent processes, command line arguments, user context, and execution timestamps.



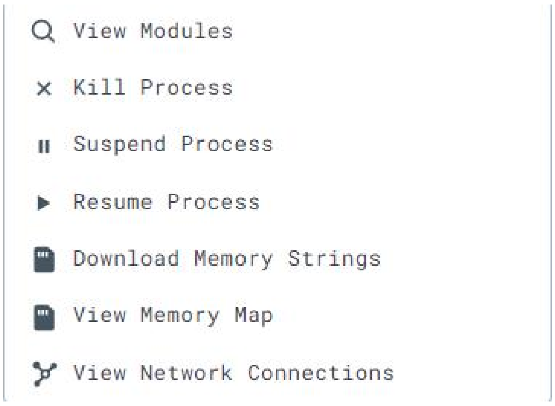
Hostname
windev2403eval.localdomain

SID
8817c4c6-27c7-421c-9754-46c…

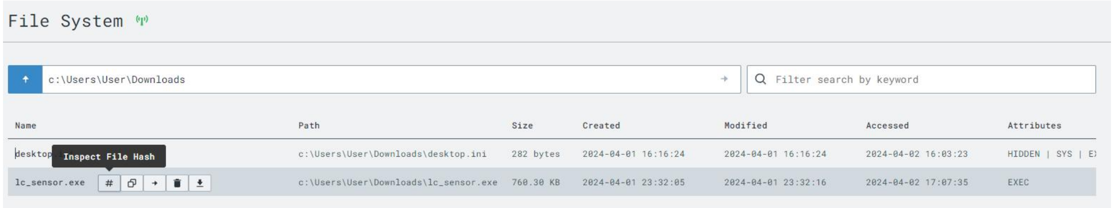
Platform
Windows x86 64 bit

Run	Name	PPID	PID	User	Path	Comm
⋮	dwm.exe	744	1052	Window Manager\DWM-1	C:\Windows\system32\dwm.exe	"dwm
⋮	conhost.exe	8980	1420	WINDEV2403EVAL\User	C:\Windows\system32\conhost.exe	\??\
⋮	msedge.exe	7256	2704	WINDEV2403EVAL\User	C:\Program Files (x86)\Microsoft\Ed…	"C:\
⋮	JUNIOR_HERON.exe	8980	3864	WINDEV2403EVAL\User	C:\Users\User\Downloads\JUNIOR_HERO…	C:\U
⋮	Explorer.EXE	5660	5716	WINDEV2403EVAL\User	C:\Windows\Explorer.EXE	C:\W
⋮	msedge.exe	5716	7256	WINDEV2403EVAL\User	C:\Program Files (x86)\Microsoft\Ed…	"C:\
⋮	msedge.exe	7256	9296	WINDEV2403EVAL\User	C:\Program Files (x86)\Microsoft\Ed…	"C:\
⋮	msedge.exe	7256	9308	WINDEV2403EVAL\User	C:\Program Files (x86)\Microsoft\Ed…	"C:\

The three dots menu for each process in Limacharlie EDR provides the following options:



These options provide various capabilities to investigate and respond to potential security threats associated with specific processes.



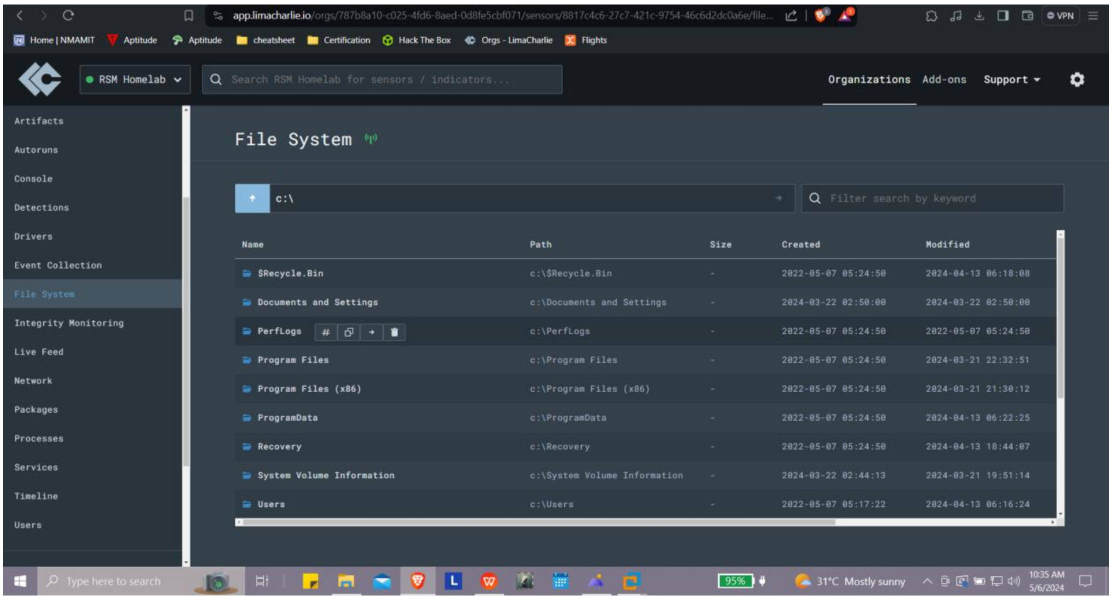
File System

c:\Users\User\Downloads

Name	Path	Size	Created	Modified	Accessed	Attributes
desktop	c:\Users\User\Downloads\desktop.ini	282 bytes	2024-04-01 16:16:24	2024-04-01 16:16:24	2024-04-02 16:03:23	HIDDEN | SYS | E
lc_sensor.exe	c:\Users\User\Downloads\lc_sensor.exe	760.30 KB	2024-04-01 23:32:05	2024-04-01 23:32:16	2024-04-02 17:07:35	EXEC

- File System:

In Limacharlie EDR, the "File System" section provides a view of the files and directories present on the monitored endpoints.

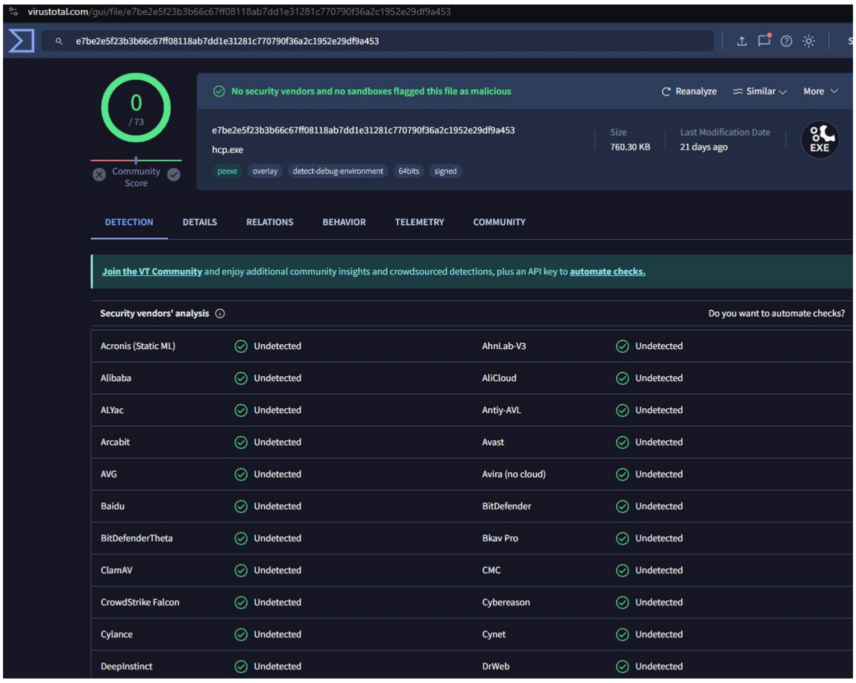


File System

c:\

Name	Path	Size	Created	Modified
$Recycle.Bin	c:\$Recycle.Bin	-	2022-05-07 05:24:50	2024-04-13 06:18:08
Documents and Settings	c:\Documents and Settings	-	2024-03-22 02:50:00	2024-03-22 02:50:00
PerfLogs	c:\PerfLogs	-	2022-05-07 05:24:50	2022-05-07 05:24:50
Program Files	c:\Program Files	-	2022-05-07 05:24:50	2024-03-21 22:32:51
Program Files (x86)	c:\Program Files (x86)	-	2022-05-07 05:24:50	2024-03-21 21:30:12
ProgramData	c:\ProgramData	-	2022-05-07 05:24:50	2024-04-13 06:22:25
Recovery	c:\Recovery	-	2022-05-07 05:24:50	2024-04-13 18:44:07
System Volume Information	c:\System Volume Information	-	2024-03-22 02:44:13	2024-03-21 19:51:14
Users	c:\Users	-	2022-05-07 05:17:22	2024-04-13 06:16:24

In Limacharlie, a standout feature is the ability to search file hash values directly with VirusTotal. This handy tool quickly checks the potential threat of files against VirusTotal's database, making it easier to assess and handle suspicious files. Integrating VirusTotal into the file explorer streamlines the analysis process, helping security analysts make better decisions and strengthen endpoint security.


virustotal.com/gui/file/e7be2e5f23b3b66c67ff08118ab7dd1e31281c770790f36a2c1952e29df9a453
e7be2e5f23b3b66c67ff08118ab7dd1e31281c770790f36a2c1952e29df9a453
0
/ 73
Community Score
Reanalyze
Similar
More
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY

No security vendors and no sandboxes flagged this file as malicious

e7be2e5f23b3b66c67ff08118ab7dd1e31281c770790f36a2c1952e29df9a453
hcp.exe
peexe overlay detect-debug-environment 64bits signed

Size: 760.30 KB
Last Modification Date: 21 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
CrowdStrike Falcon	✓ Undetected	Cybereason	✓ Undetected
Cylance	✓ Undetected	Cynet	✓ Undetected
DeepInstinct	✓ Undetected	DrWeb	✓ Undetected

CONCLUSION

In conclusion, setting up this virtual lab was both interesting and exciting. By installing tools like VMware Workstation, Ubuntu Server, Windows VMs, Sysmon, LimaCharlie EDR, and Sliver C2, I've laid a solid foundation for hands-on learning.

Exploring LimaCharlie's web interface has uncovered the power of monitoring and analyzing security events. Engaging with processes and file systems has provided me with valuable insights into threat detection and response.