VeloCON 2023

Empowering SOC Analysts with Velociraptor :

Revolutionizing Live Response and Automation

whoami

❑ 5+ years experience in the industry

❑ SOC Analyst and incident responder

❑ Product Owner @imperum.io

❑ Motivation : Help to create more effective SOCs

𝕏 semanurtg

Agenda

01 Live Response

02 Velociraptor’s Revolution

03 Velociraptor in IMPERUM

04 Integration and Automation

05 Use Cases

06 Roadmap

1 Live Response

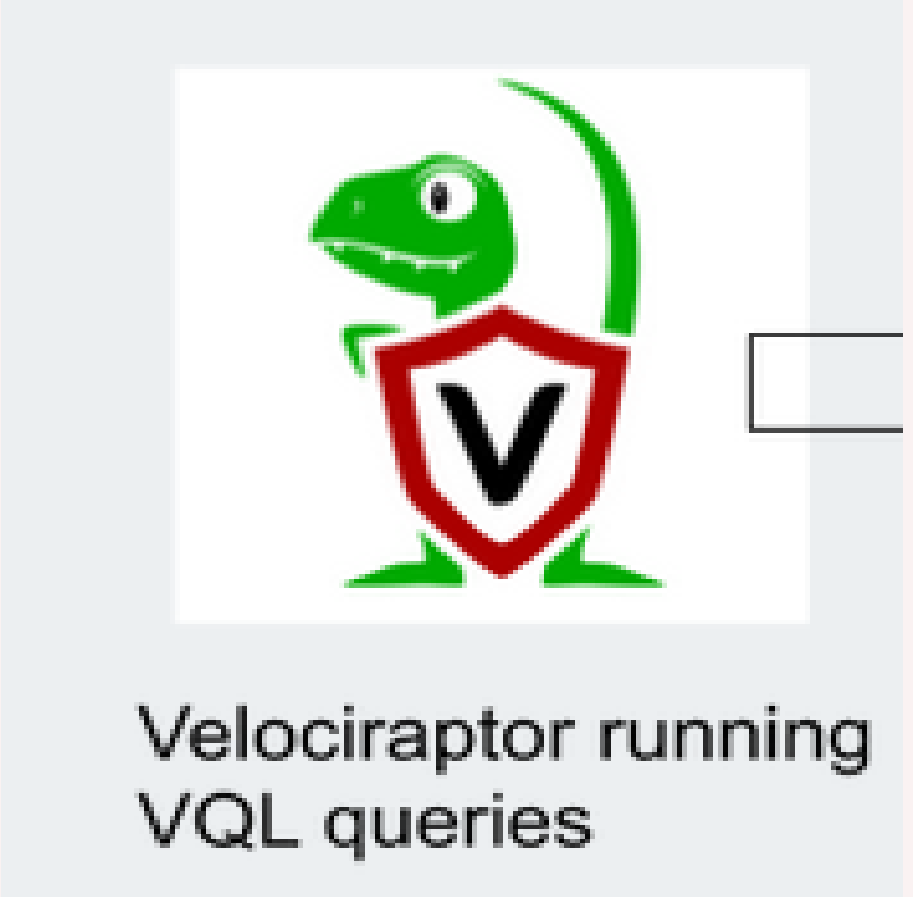
Limitations of Traditional Approaches :

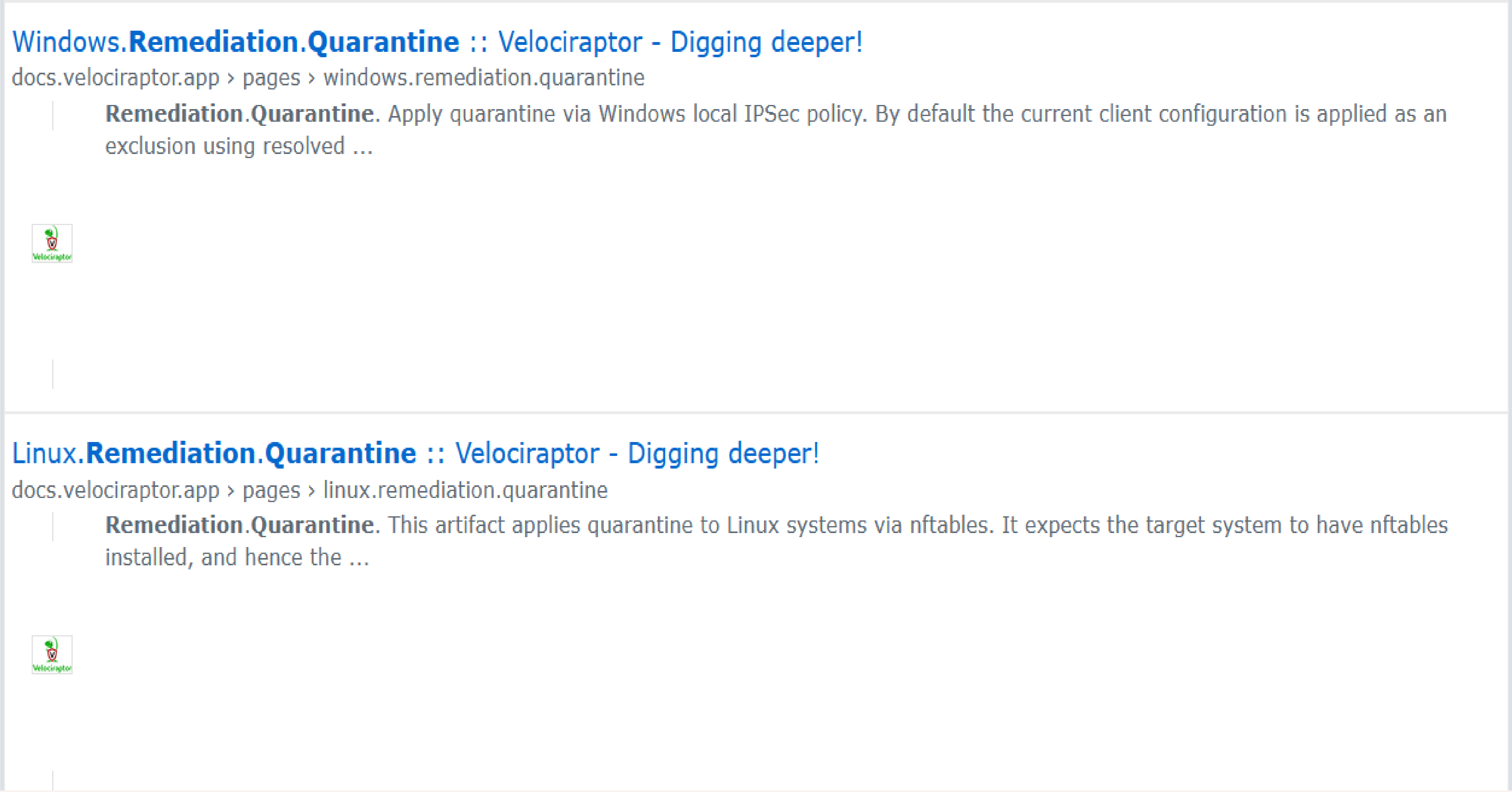
- Traditional incident response relies on predefined, static procedures.
- Often involves manual, time-consuming tasks.
- May result in delays in identifying and responding to threats.
- Limited ability to adapt to the dynamic nature of cyberattacks.

1 Live Response

- Live response is the ability to access and analyze digital evidence on endpoints in real-time.
- Live response enables proactive threat detection and rapid incident resolution.
- Empowers SOC analysts for effective incident handling.

2 Velociraptor's Revolution



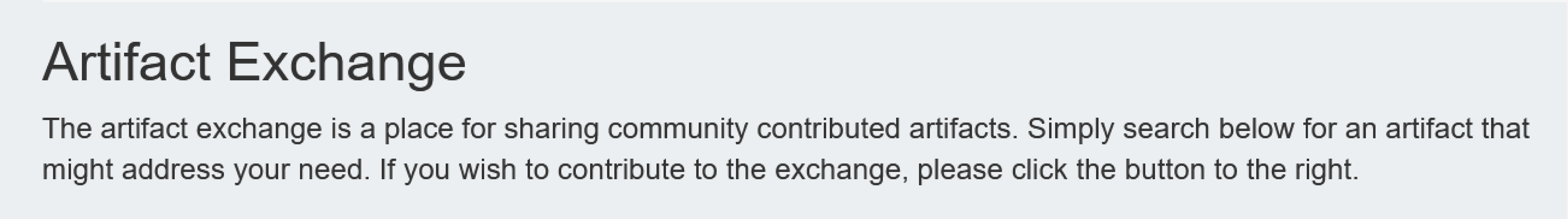


Windows.**Remediation**.**Quarantine** :: Velociraptor - Digging deeper!
docs.velociraptor.app › pages › windows.remediation.quarantine

Remediation.**Quarantine**. Apply quarantine via Windows local IPSec policy. By default the current client configuration is applied as an exclusion using resolved ...

Linux.**Remediation**.**Quarantine** :: Velociraptor - Digging deeper!
docs.velociraptor.app › pages › linux.remediation.quarantine

Remediation.**Quarantine**. This artifact applies quarantine to Linux systems via nftables. It expects the target system to have nftables installed, and hence the ...

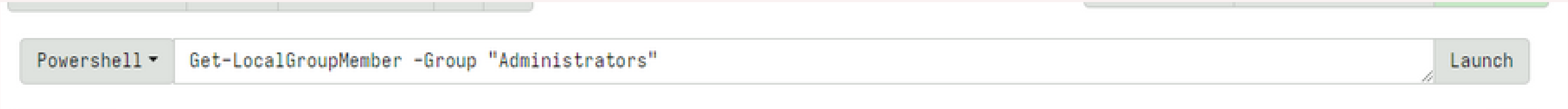


Artifact Exchange

The artifact exchange is a place for sharing community contributed artifacts. Simply search below for an artifact that might address your need. If you wish to contribute to the exchange, please click the button to the right.

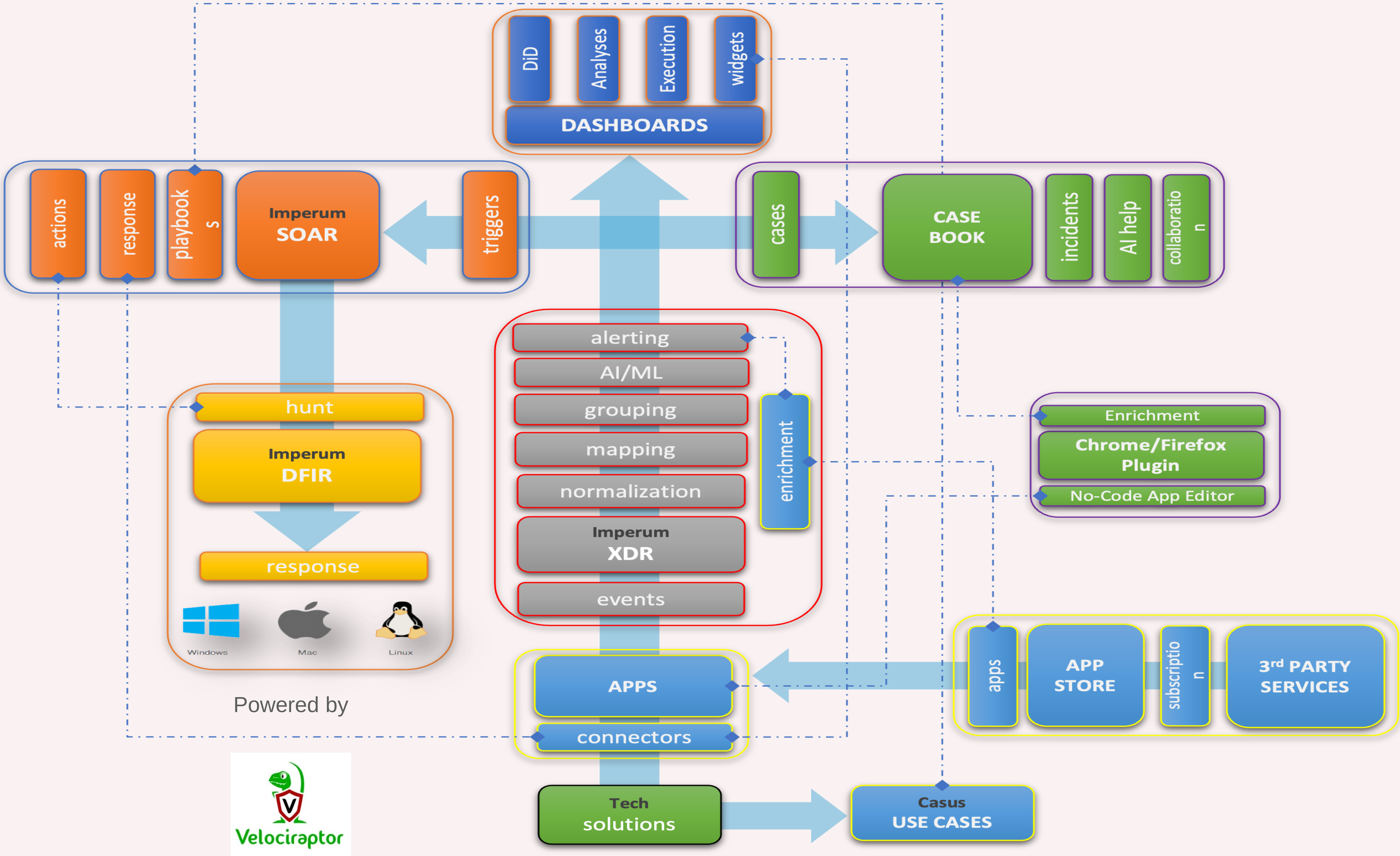
2 Velociraptor's Revolution

PowerShell



```
Get-LocalGroupMember -Group "Administrators"
```

3 Velociraptor in IMPERUM



DiD

Analyses

Execution

widgets

DASHBOARDS

actions

response

playbook s

Imperum SOAR

triggers

cases

CASE BOOK

incidents

AI help

collaboratio n

alerting

AI/ML

grouping

mapping

normalization

Imperum XDR

events

enrichment

hunt

Imperum DFIR

response

Windows

Mac

Linux

Enrichment

Chrome/Firefox Plugin

No-Code App Editor

apps

APP STORE

subscriptio n

3rd PARTY SERVICES

APPS

connectors

Powered by

Velociraptor

Tech solutions

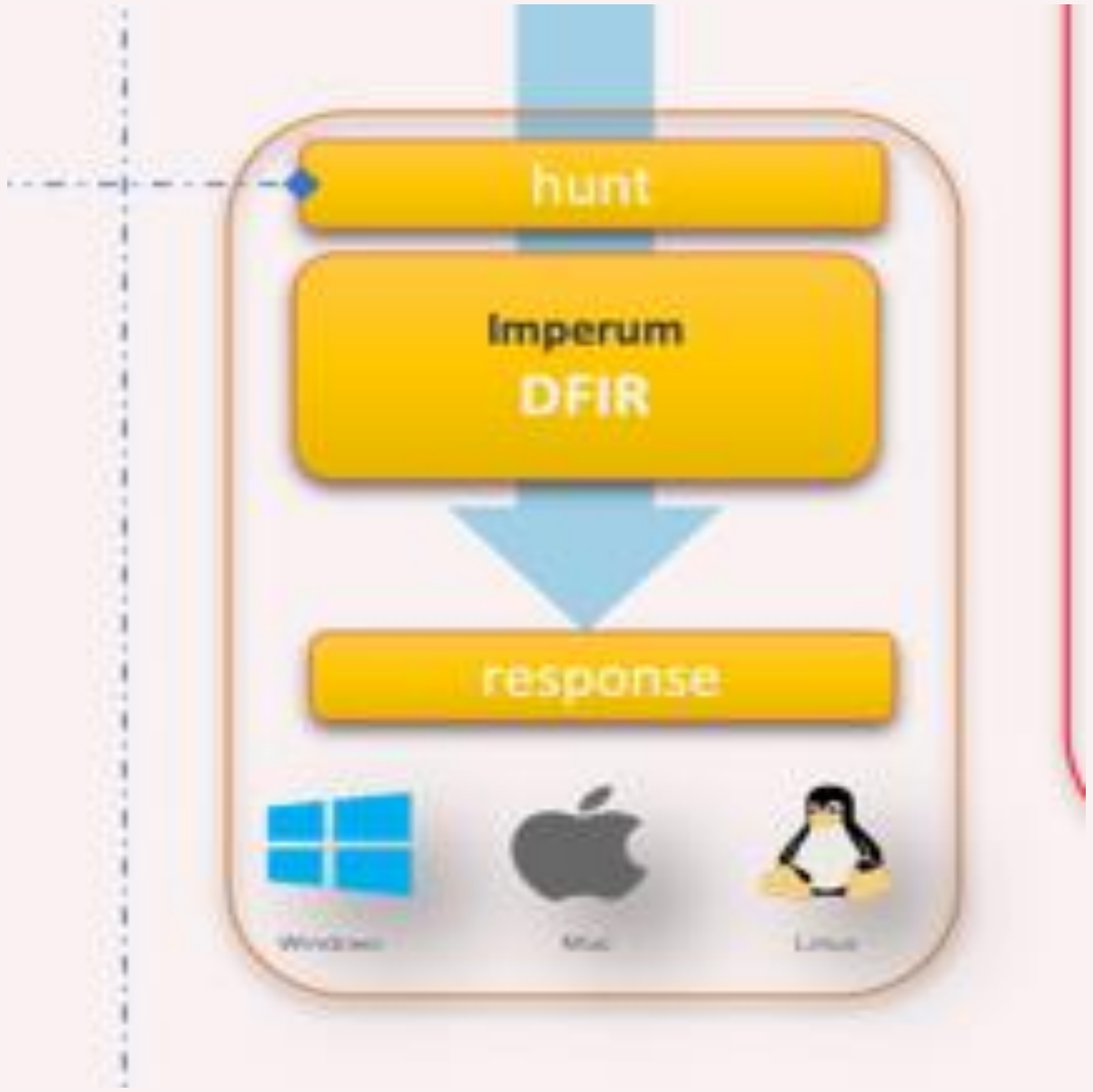
Casus USE CASES

3 Velociraptor in IMPERUM (impDFIR)

Mission

is to enable swift resolution of security incidents, minimizing their impact and ensuring business continuity.

is to close the response gap that today’s EDR’s have.



IMPERUM with Velociraptor is designed to speak with processes.

3 Velociraptor in IMPERUM (impDFIR)

search or "/" to invoke command

16 AGENTS

LAST SEEN HOSTNAME ↓

Search agents

FedoraSrv38-MacPro ONLINE
- 34 tasks

Win10-MacPro ONLINE
- 20 tasks

MacOS12-MacPro.Local... ONLINE
- 4 tasks

Senads-Mac-Pro.Local... ONLINE
- 4 tasks

Ubuntu22Desk-MacPro ONLINE
- 18 tasks

RedHat9-MacPro ONLINE
- 2 tasks

Win10-MacPro

Microsoft Windows 10 Pro10.0.19045 Build 19045 13th September 2023 4:33

Isolate Host

Last IP	Labels +	FQDN	Hostname	Arch
[redacted]		Win10-MacPro.localdomain	Win10-MacPro	amd64

Powershell Execute a terminal command Login To Activate

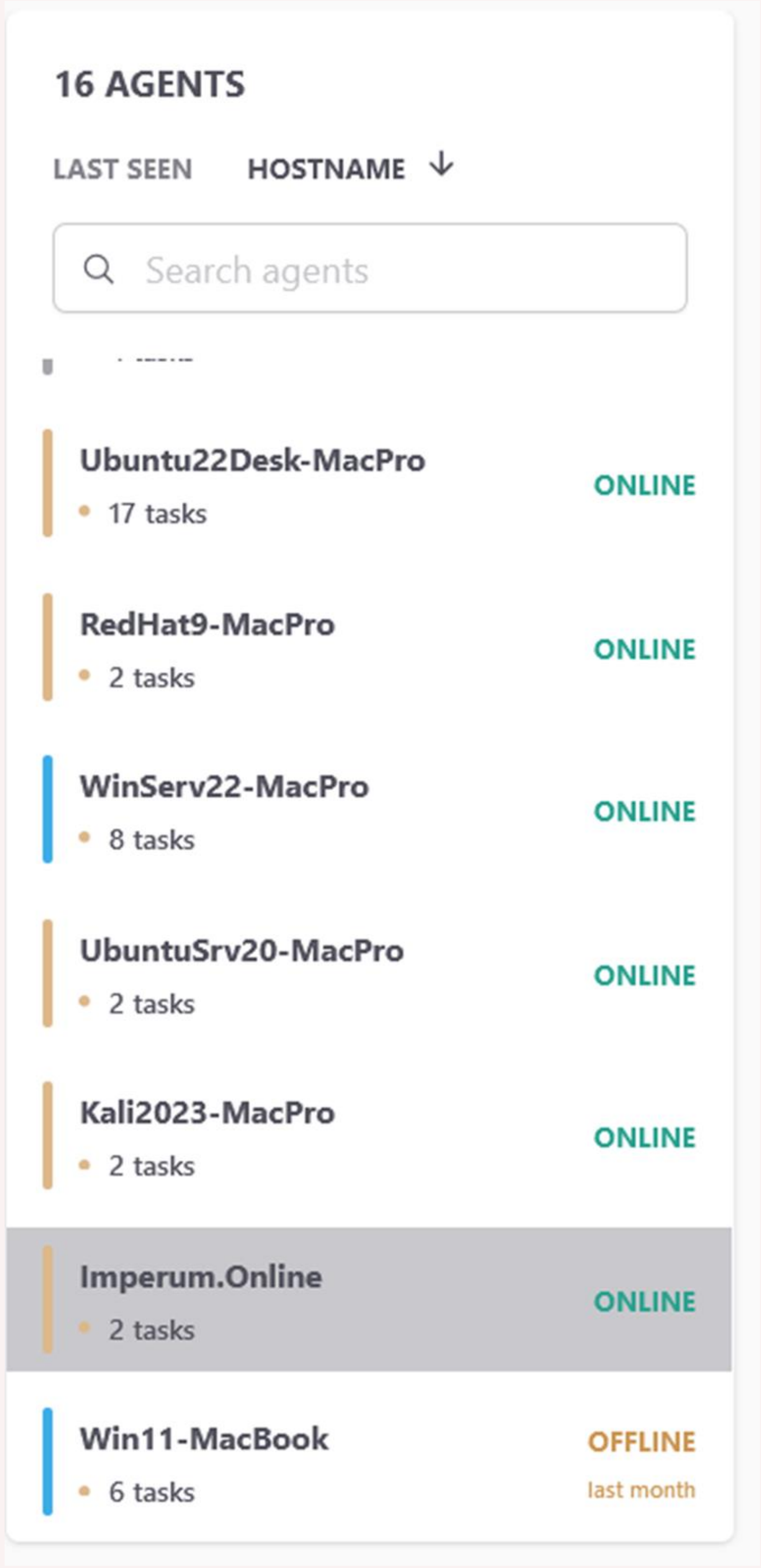
Windows.Network.ListeningPorts Windows.Sys.Users Windows.Sys.StartupItems

Not Logged in

CPU Usage

RAM Usage

3 Velociraptor in IMPERUM

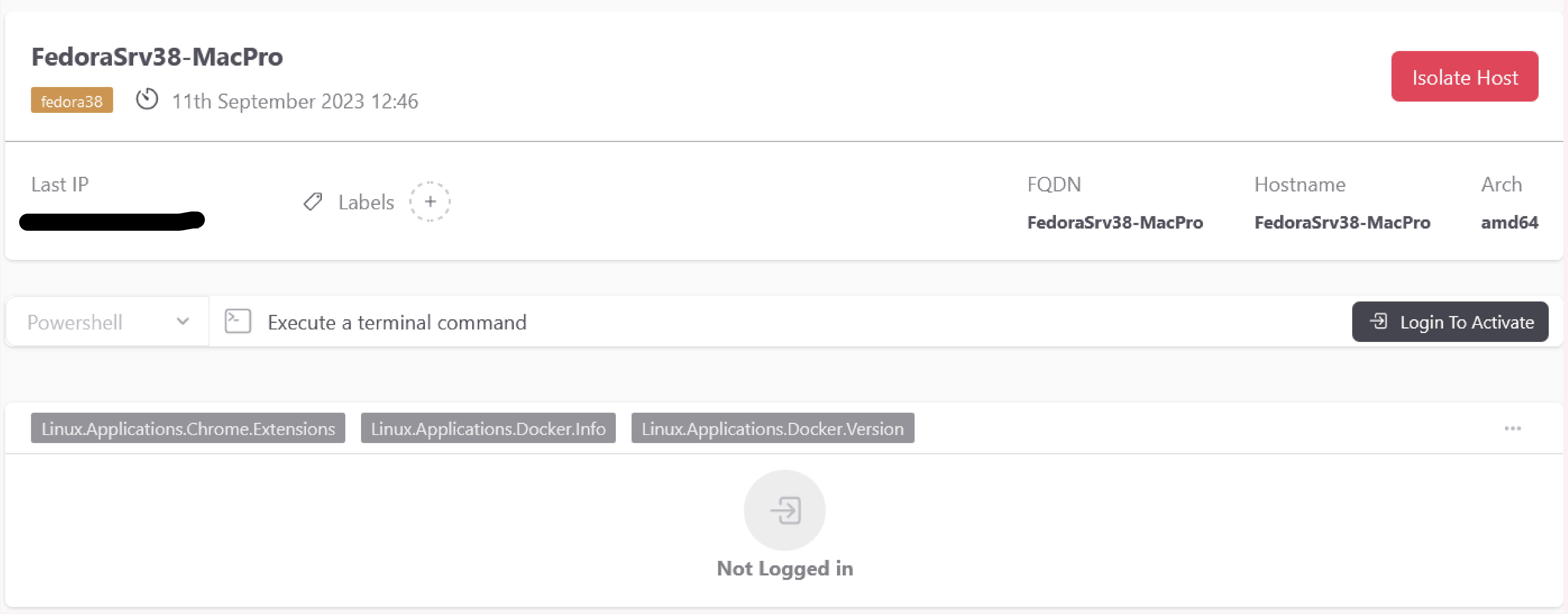


16 AGENTS

LAST SEEN HOSTNAME ↓

Search agents

Ubuntu22Desk-MacPro	17 tasks	ONLINE
RedHat9-MacPro	2 tasks	ONLINE
WinServ22-MacPro	8 tasks	ONLINE
UbuntuSrv20-MacPro	2 tasks	ONLINE
Kali2023-MacPro	2 tasks	ONLINE
Imperum.Online	2 tasks	ONLINE
Win11-MacBook	6 tasks	OFFLINE last month



FedoraSrv38-MacPro

fedora38 11th September 2023 12:46

Last IP [redacted]

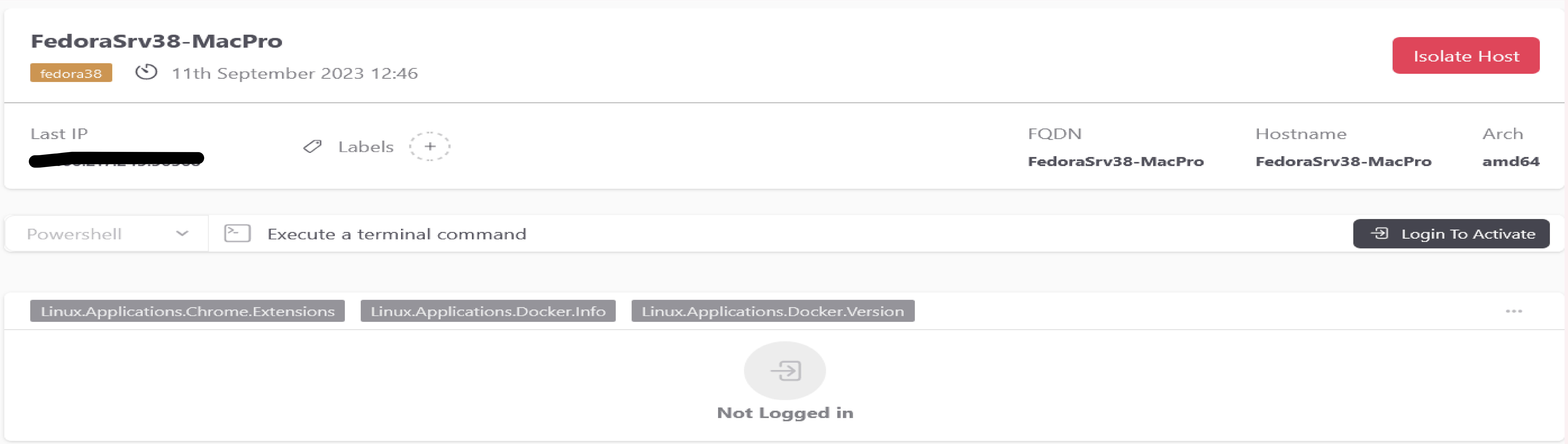
FQDN	Hostname	Arch
FedoraSrv38-MacPro	FedoraSrv38-MacPro	amd64

Powershell
Execute a terminal command
Login To Activate
Linux.Applications.Chrome.Extensions
Linux.Applications.Docker.Info
Linux.Applications.Docker.Version
...

Not Logged in

```
"SELECT os_info.system from clients() WHERE
client_id='C.{client_id}'"
```

3 Velociraptor in IMPERUM



FedoraSrv38-MacPro

fedora38 11th September 2023 12:46

Last IP: [redacted]

FQDN: FedoraSrv38-MacPro

Hostname: FedoraSrv38-MacPro

Arch: amd64

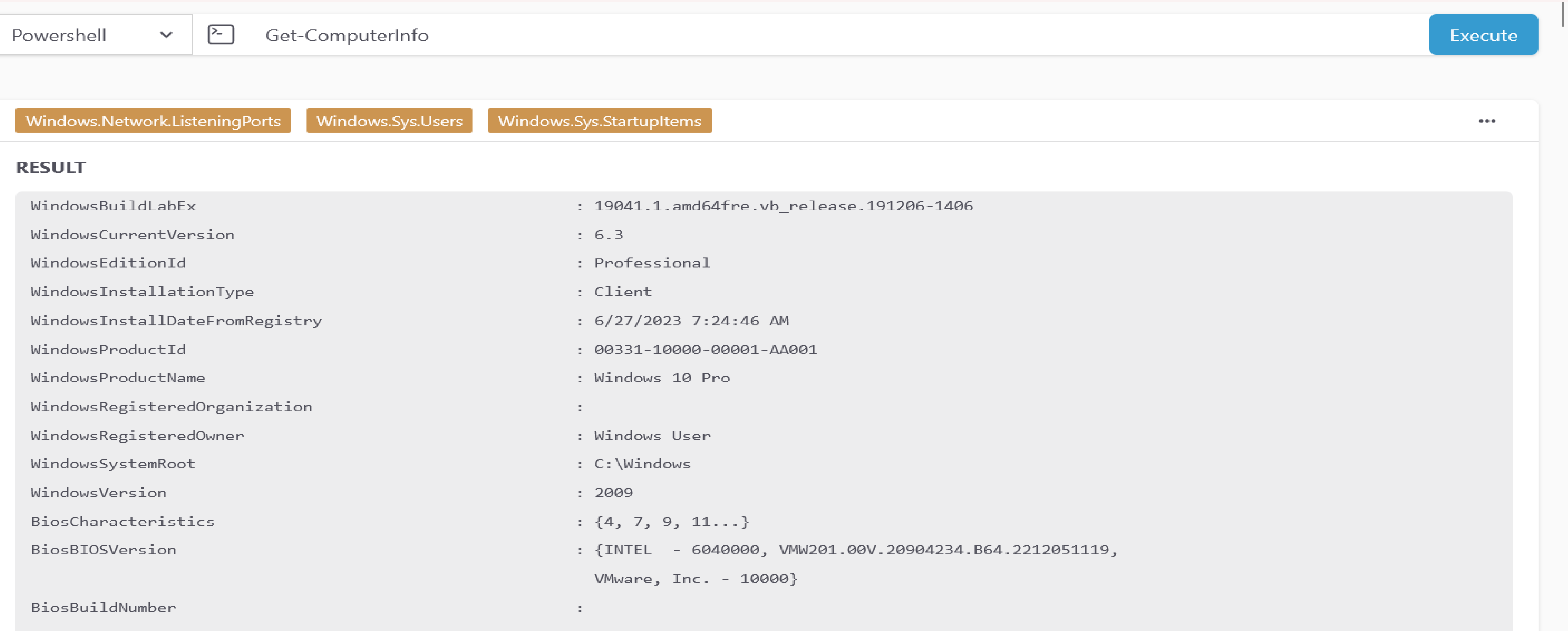
Linux.Applications.Chrome.Extensions Linux.Applications.Docker.Info Linux.Applications.Docker.Version

Not Logged in

Set Isolation Label : "LET _ <= label(client_id='C.{client_id}', labels={labels}, op='set’)”

Remove Isolation Label : "LET _ <= label(client_id='C.{client_id}', labels={labels}, op='remove')"

3 Velociraptor in IMPERUM

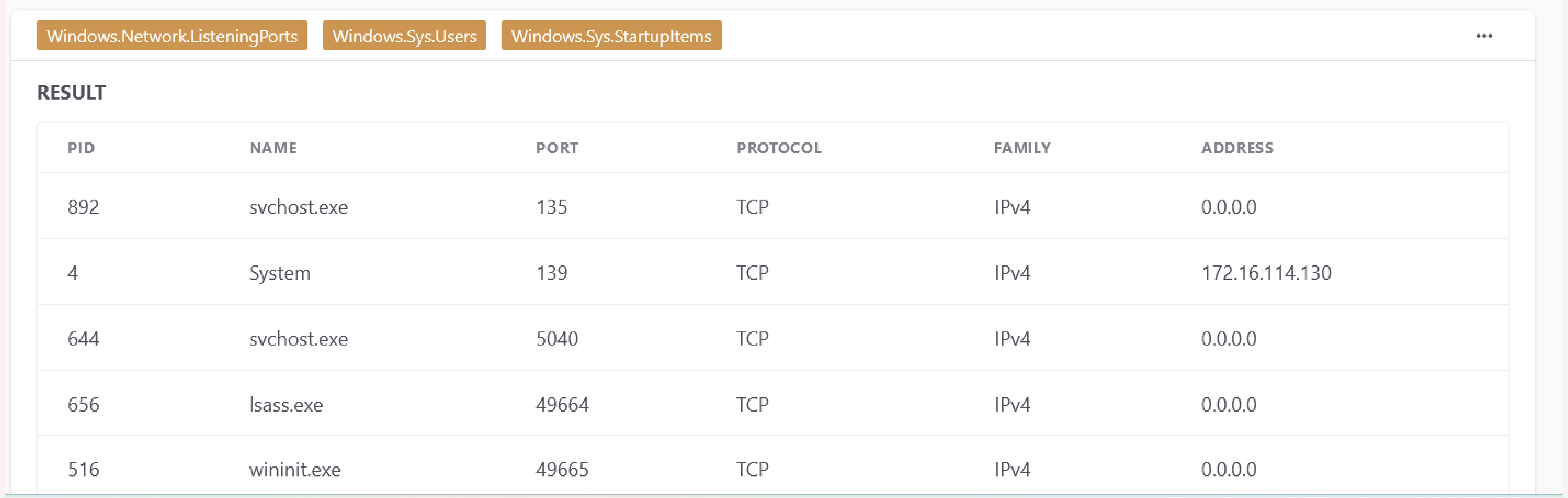


```
WindowsBuildLabEx                                        : 19041.1.amd64fre.vb_release.191206-1406
WindowsCurrentVersion                                    : 6.3
WindowsEditionId                                         : Professional
WindowsInstallationType                                  : Client
WindowsInstallDateFromRegistry                           : 6/27/2023 7:24:46 AM
WindowsProductId                                         : 00331-10000-00001-AA001
WindowsProductName                                       : Windows 10 Pro
WindowsRegisteredOrganization                            :
WindowsRegisteredOwner                                   : Windows User
WindowsSystemRoot                                        : C:\Windows
WindowsVersion                                           : 2009
BiosCharacteristics                                      : {4, 7, 9, 11...}
BiosBIOSVersion                                          : {INTEL  - 6040000, VMW201.00V.20904234.B64.2212051119,
                                                           VMware, Inc. - 10000}
BiosBuildNumber                                          :
```

```
LET collection <= collect_client(client_id='C.{client_id}', \
artifacts='{artifact}', env={env}) \

 SELECT * FROM watch_monitoring(artifact='System.Flow.Completion') WHERE \
FlowId = collection.flow_id LIMIT 1"
```

3 Velociraptor in IMPERUM

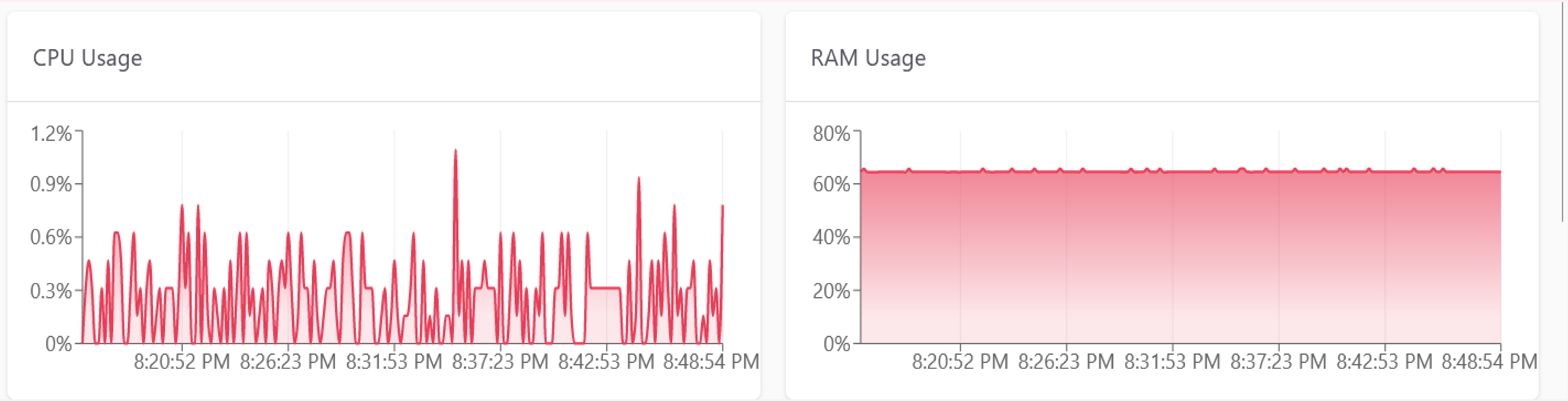


RESULT

PID	NAME	PORT	PROTOCOL	FAMILY	ADDRESS
892	svchost.exe	135	TCP	IPv4	0.0.0.0
4	System	139	TCP	IPv4	172.16.114.130
644	svchost.exe	5040	TCP	IPv4	0.0.0.0
656	lsass.exe	49664	TCP	IPv4	0.0.0.0
516	wininit.exe	49665	TCP	IPv4	0.0.0.0

```
"SELECT * FROM flow_results(client_id='C.{client_id}', flow_id='{flow_id}', \
artifact='{artifacts_with_results[0]}')"
```

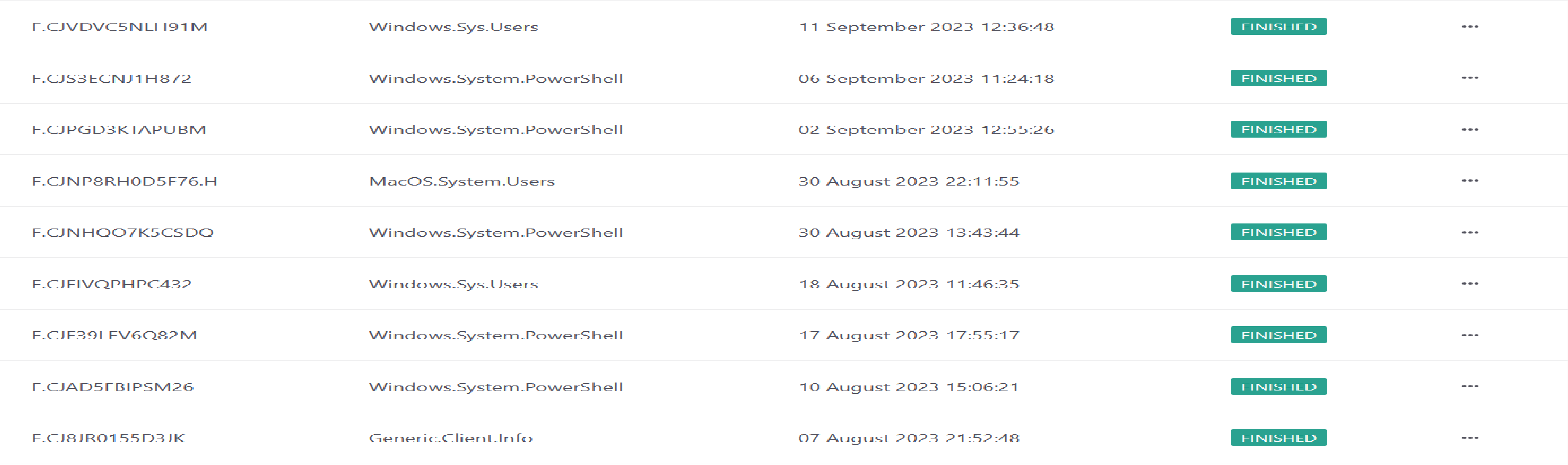
3 Velociraptor in IMPERUM


CPU Usage

RAM Usage

```
SELECT Timestamp AS timestamp, rate(x=CPU, y=Timestamp) * 100 As
cpu_percent,\                    RSS / 1000000 AS memory_use FROM
source(client_id='C.{client_id}', \                    artifact='Generic.Client.Stats')
WHERE cpu_percent >= 0"
```

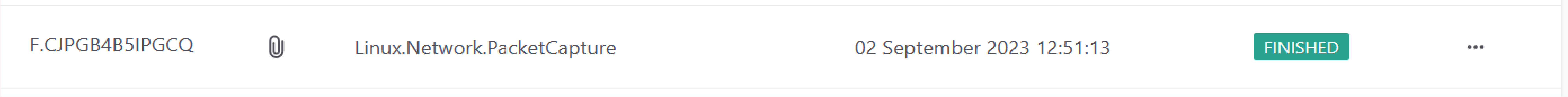
3 Velociraptor in IMPERUM



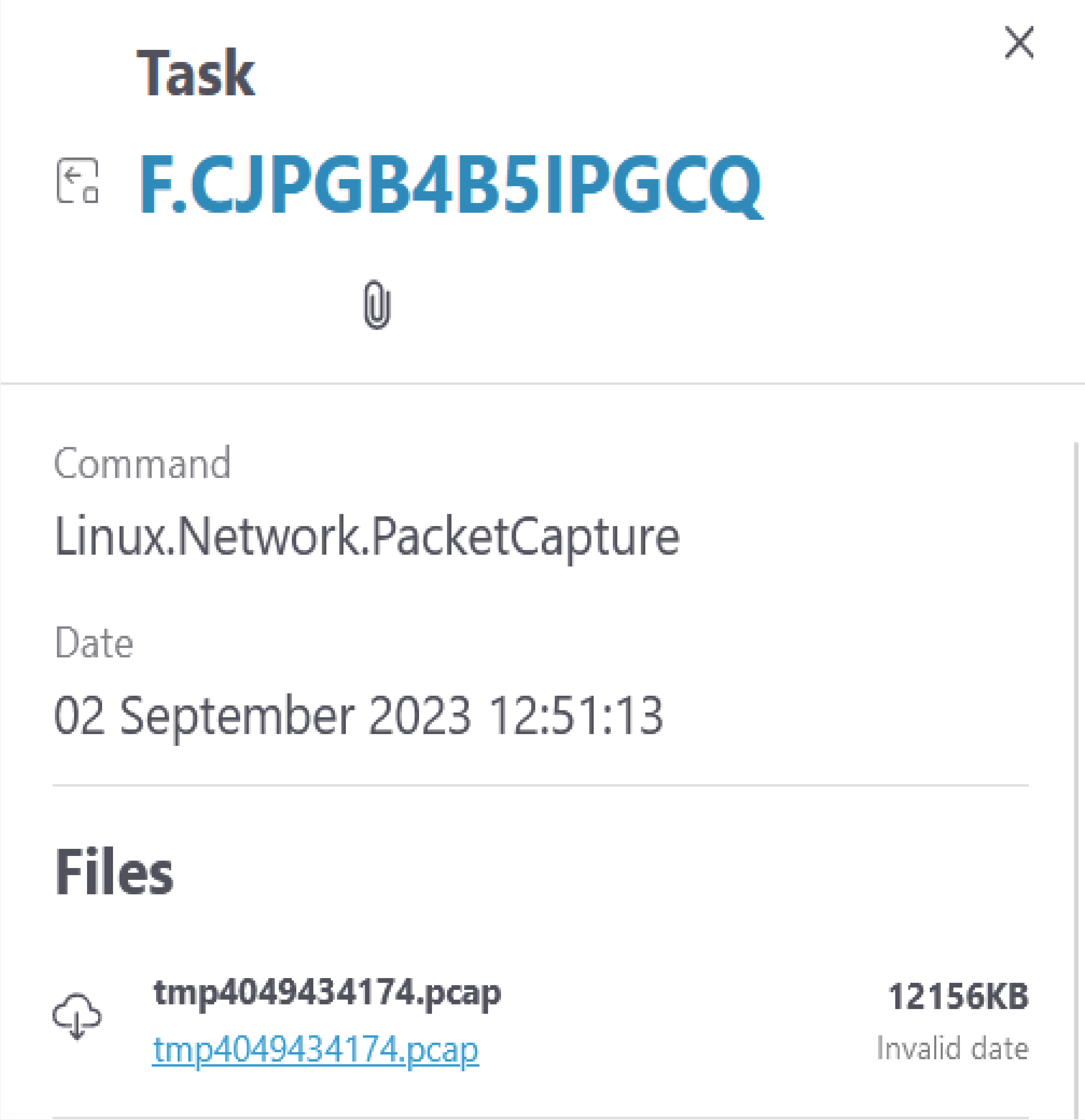
F.CJVDVC5NLH91M	Windows.Sys.Users	11 September 2023 12:36:48	FINISHED	···
F.CJS3ECNJ1H872	Windows.System.PowerShell	06 September 2023 11:24:18	FINISHED	···
F.CJPGD3KTAPUBM	Windows.System.PowerShell	02 September 2023 12:55:26	FINISHED	···
F.CJNP8RH0D5F76.H	MacOS.System.Users	30 August 2023 22:11:55	FINISHED	···
F.CJNHQO7K5CSDQ	Windows.System.PowerShell	30 August 2023 13:43:44	FINISHED	···
F.CJFIVQPHPC432	Windows.Sys.Users	18 August 2023 11:46:35	FINISHED	···
F.CJF39LEV6Q82M	Windows.System.PowerShell	17 August 2023 17:55:17	FINISHED	···
F.CJAD5FBIPSM26	Windows.System.PowerShell	10 August 2023 15:06:21	FINISHED	···
F.CJ8JR0155D3JK	Generic.Client.Info	07 August 2023 21:52:48	FINISHED	···

```
"SELECT session_id, state, request.artifacts, artifacts_with_results, \
create_time, query_stats FROM flows(client_id='C.{client_id}', \
flow_id='{flow_id}’)”
"SELECT session_id, state, request.artifacts, create_time, query_stats \
FROM flows(client_id='C.{client_id}')"
```

3 Velociraptor in IMPERUM



F.CJPGB4B5IPGCQ · Linux.Network.PacketCapture · 02 September 2023 12:51:13 · FINISHED



Task

F.CJPGB4B5IPGCQ

Command

Linux.Network.PacketCapture

Date

02 September 2023 12:51:13

Files

tmp4049434174.pcap **12156KB**

tmp4049434174.pcap Invalid date

"SELECT * FROM uploads(client_id='C.{client_id}', flow_id='{flow_id}')"

4 Integration and Automation

Velociraptor

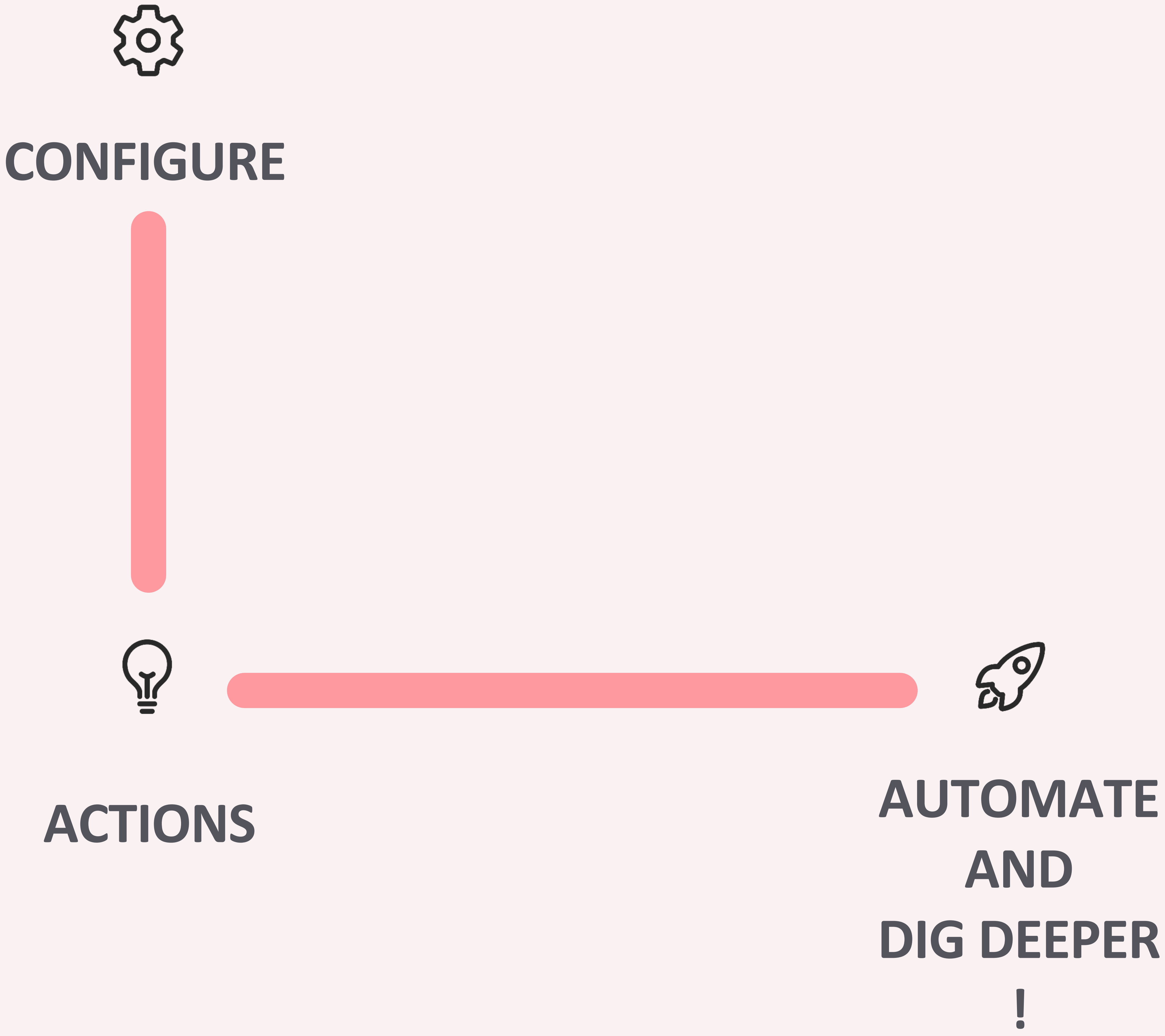
imperum

Velociraptor app in the marketplace

Integration via Velociraptor’s API

Centralized incident response and orchestration

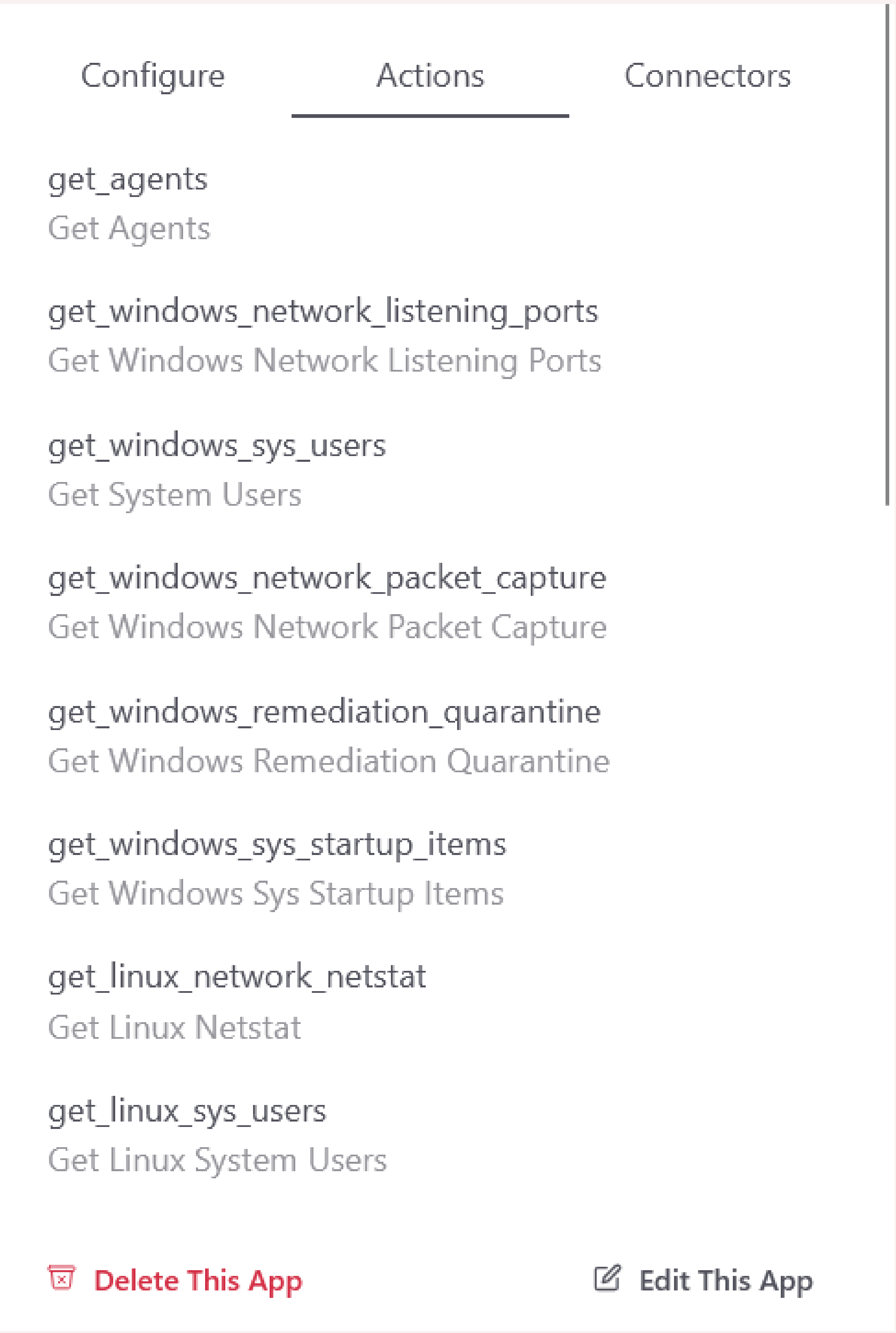
4 Integration and Automation



CONFIGURE

ACTIONS

AUTOMATE AND DIG DEEPER !



get_agents
Get Agents

get_windows_network_listening_ports
Get Windows Network Listening Ports

get_windows_sys_users
Get System Users

get_windows_network_packet_capture
Get Windows Network Packet Capture

get_windows_remediation_quarantine
Get Windows Remediation Quarantine

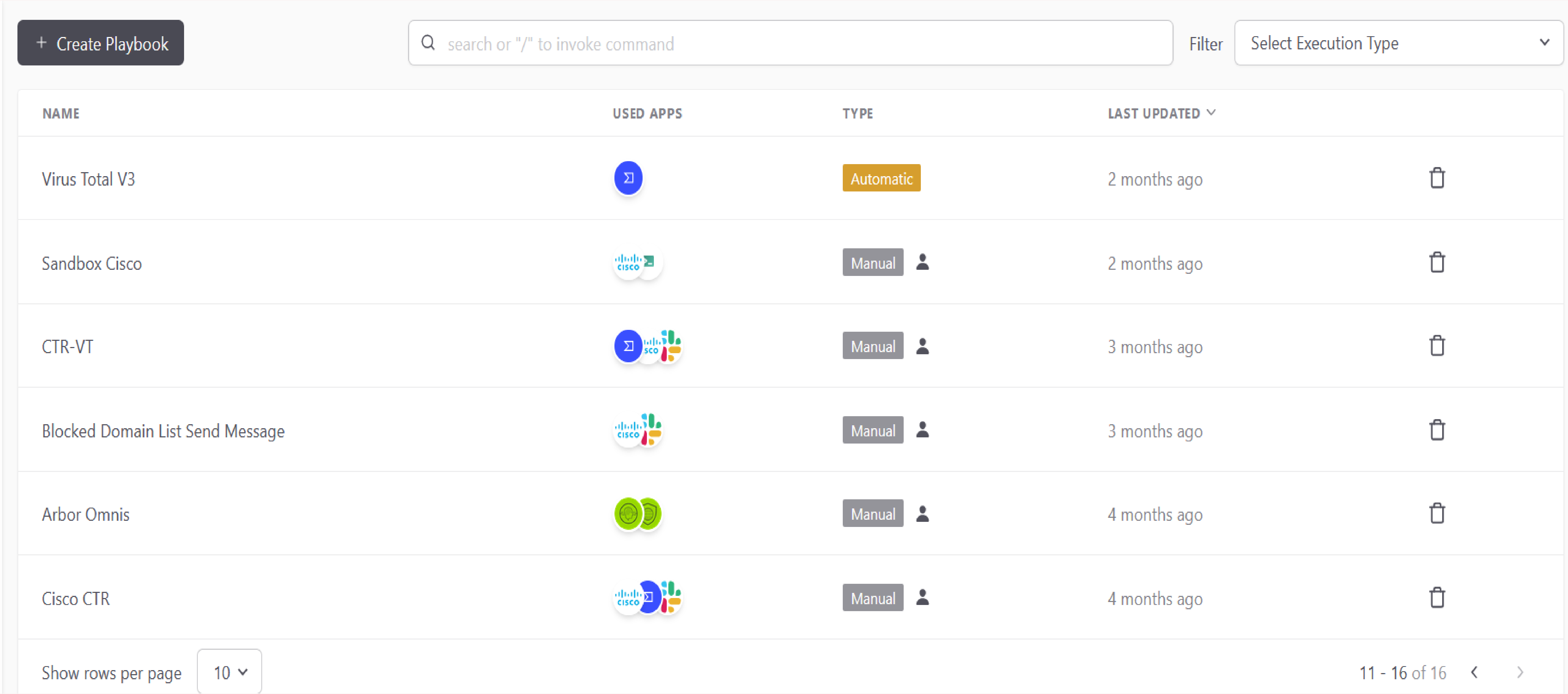
get_windows_sys_startup_items
Get Windows Sys Startup Items

get_linux_network_netstat
Get Linux Netstat

get_linux_sys_users
Get Linux System Users

4 Integration and Automation

- Manuel , automatic or semi-automatic playbooks
- Drag and drop interface
- input actions through REST-API, Webhooks, SSH, and other method
- Decision making capabilities

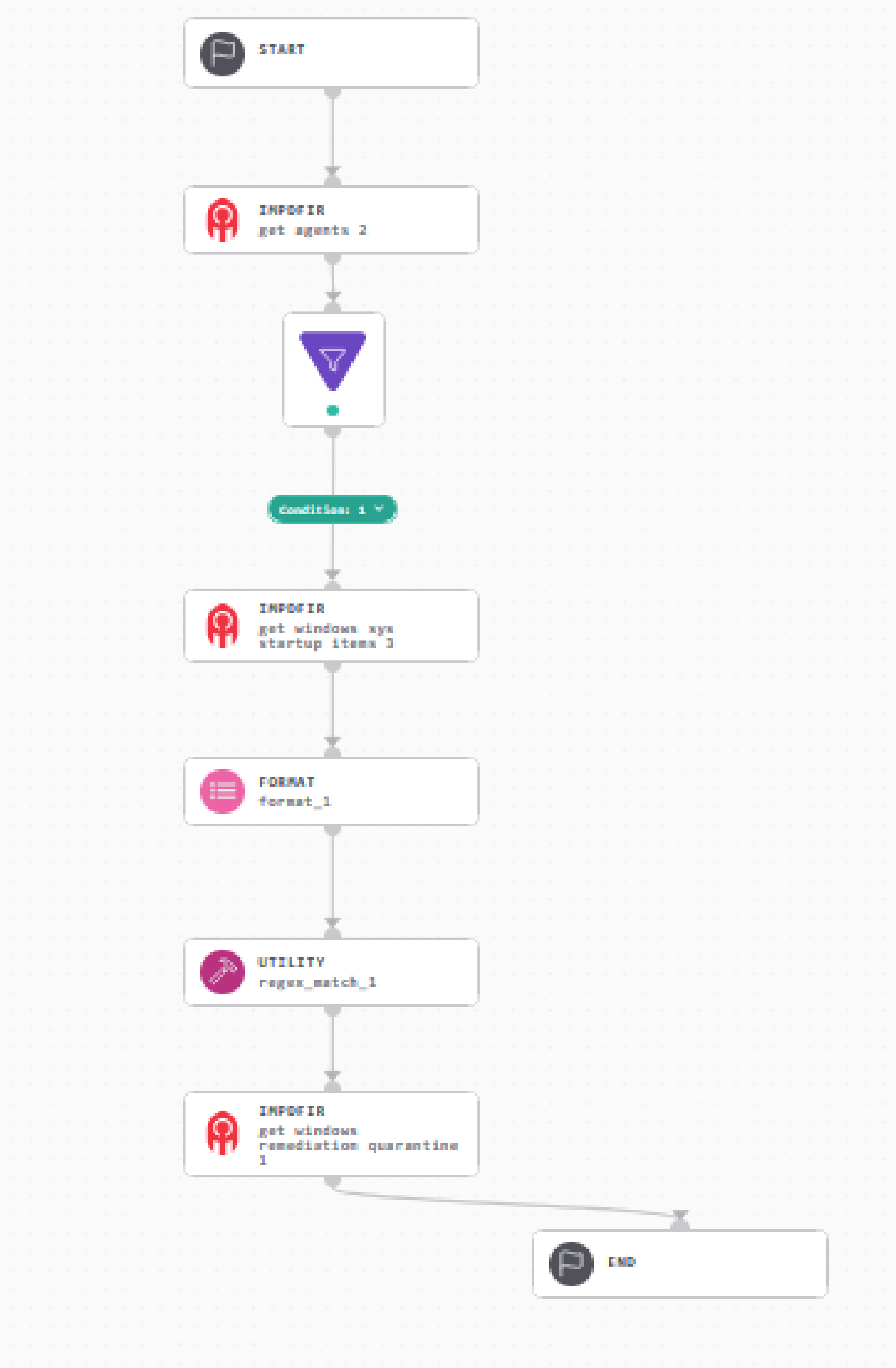


NAME	USED APPS	TYPE	LAST UPDATED
Virus Total V3		Automatic	2 months ago
Sandbox Cisco		Manual	2 months ago
CTR-VT		Manual	3 months ago
Blocked Domain List Send Message		Manual	3 months ago
Arbor Omnis		Manual	4 months ago
Cisco CTR		Manual	4 months ago

Show rows per page 10

11 - 16 of 16

4 Integration and Automation



5 Use Case - Rapid Ransomware Response

Scenario: A ransomware attack targets your network.

Velociraptor's Role:

1.Deep dive into compromised machine and collect artifacts.

2.Determine IOCs.

3.Scan IOCs for other suspected machines.

IMPERUM’s Role :

1.Automate remediation tasks for specific group of endpoints.

2.Search and correlate entities for previously events/cases may be related with compromised machines.

5 Use Case - Advanced Persistent Threat (APT) Hunting

Scenario: An APT campaign targets a tech company. You have all threat intel.

Velociraptor's Role:

1. Collect artifacts for suspected endpoints.

IMPERUM’s Role:

1.Fetch artifact results and send it to DFIR teams automatically.

2. Search and correlate entities for previously events/cases related with APT group in the Casebook.

3. Run predefined incident remediation playbooks for determined cases.

5 Use Case - Vulnerability Assessment

Scenario: An organization needs to regularly assess its critical servers for specific vulnerabilities.

Velociraptor's Role:

1. Prepare artifact for specific vulnerability.
2. Schedule hunt for critical servers.

IMPERUM’s Role :

1.Fetch results and create cases.

2.Automate communicating and patch management procedures.

3.Integrate with other vulnerability management technologies.

6 Roadmap

- ❑ Community Edition
- ❑ Design more real world DFIR use cases
- ❑ Automate repetitive tasks of forensics examiners (sub-playbooks) to make their life easier
- ❑ Add more actions for Velociraptor app
- ❑ Integrate Velociraptor with IMPERUM XDR module.
- ❑ Automatic Velociraptor deployment for critical cases

Questions & Answers

Request a Demo

Are you keen to explore how IMPERUM could enhance your cybersecurity framework?

Simply click the button below and complete the form.

Request a Demo

Our team of cybersecurity professionals will promptly get in touch to initiate your transformation journey!

Contact Me

semanur.guneysu@imperum.io

@semanurtg