Hashtag:
#yamasec
#bsidestokyo

Learn Scalable DFIR with Velociraptor and Hayabusa

by Yamato Security

高橋福助 Takahashi Fukusuke (@fukusuket)

古市昌弘 Furuichi Masahiro (D/@hitenkoku)

Self-introduction

高橋福助　Takahashi Fukusuke　(@fukusuket)

NTT Data Group's CSIRT Team (NTTDATA-CERT)
Yamato Security member

古市昌弘　Furuichi Masahiro　(D/@hitenkoku)

Subsidiary of the NTT Group
Yamato Security member

About Yamato Security

- A ‘Yamato Spirit’ security study group that has regularly met since 2012.
- Develops two open-source security programs:

Project Leader
Zach Mathis (@yamatosecurity)
Developers
Akira Nishikawa (@nishikawaakira)
DustInDark / hitenkoku
James Takai / hachiyone(@hach1yon)
ItiB (@itiB_S144)
Kazuminn (@k47_um1n)
Garigariganzy (@garigariganzy31)
Fukusuke Takahashi / fukuseket
Yusuke Matsui (@apt773)(AD Hacking Group Leader)

Project Leader
Zach Mathis (@yamatosecurity)
Developer
DustInDark / Hitenkoku
Fukusuke Takahashi / fukusuket

connpass

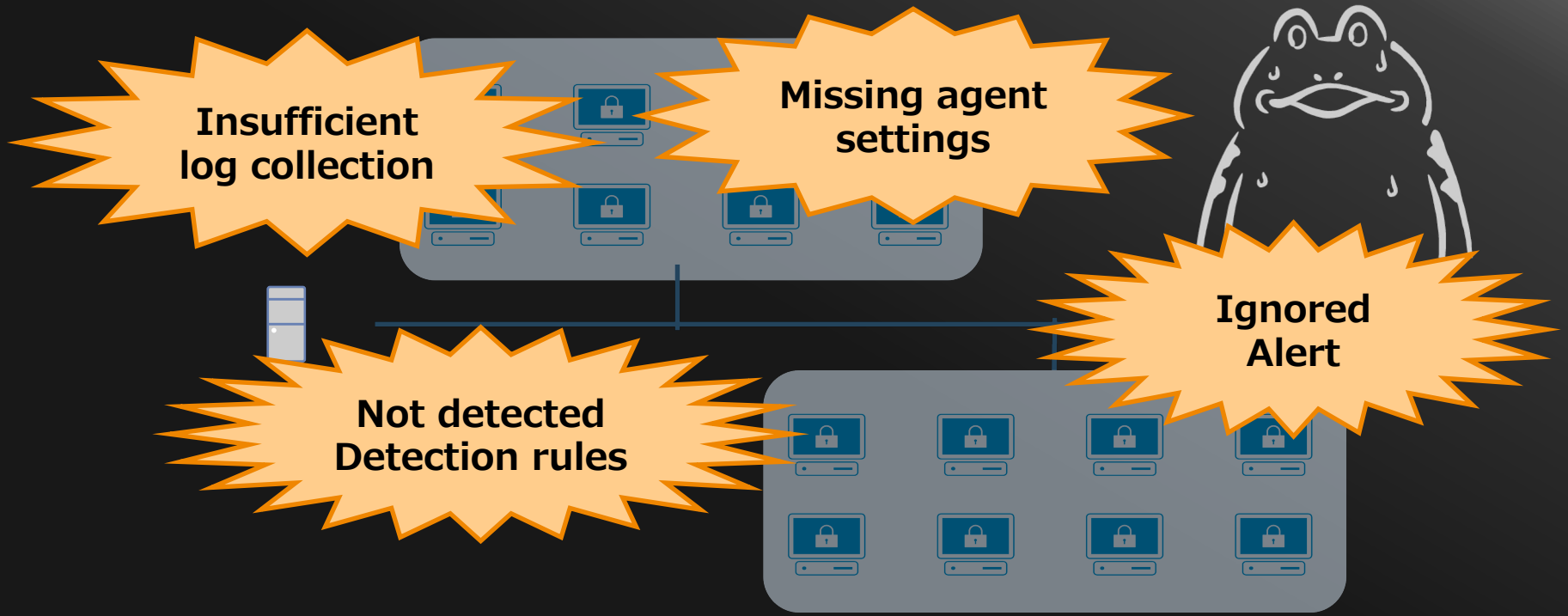
Follow:
@SecurityYamato

Agenda

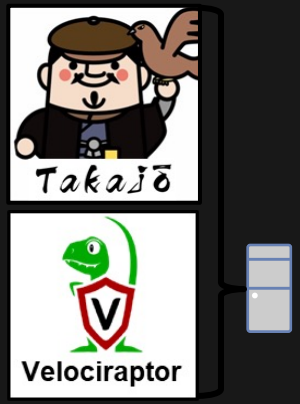
- DFIR in environments where EDR and SIEM operations are insufficient
- About Velociraptor
- About Hayabusa
- Community Knowledge
- Scalable DFIR built with Velociraptor & Hayabusa & Takajo

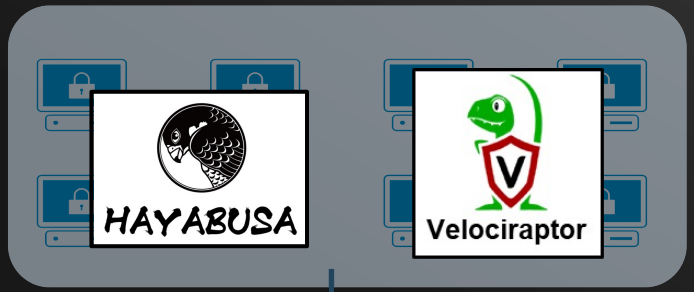
An environment where EDR and SIEM operations are insufficient?

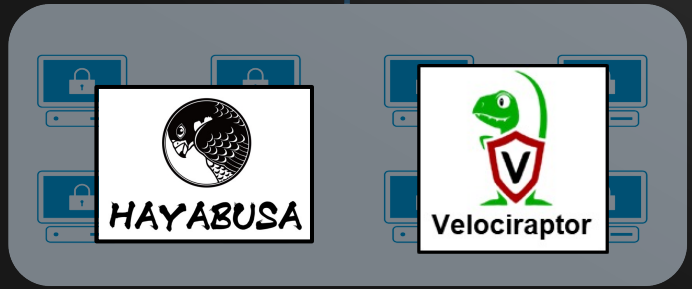
An environment where EDR and SIEM operations are insufficient?



Scalable DFIR with Velociraptor, Hayabusa and Takajo!





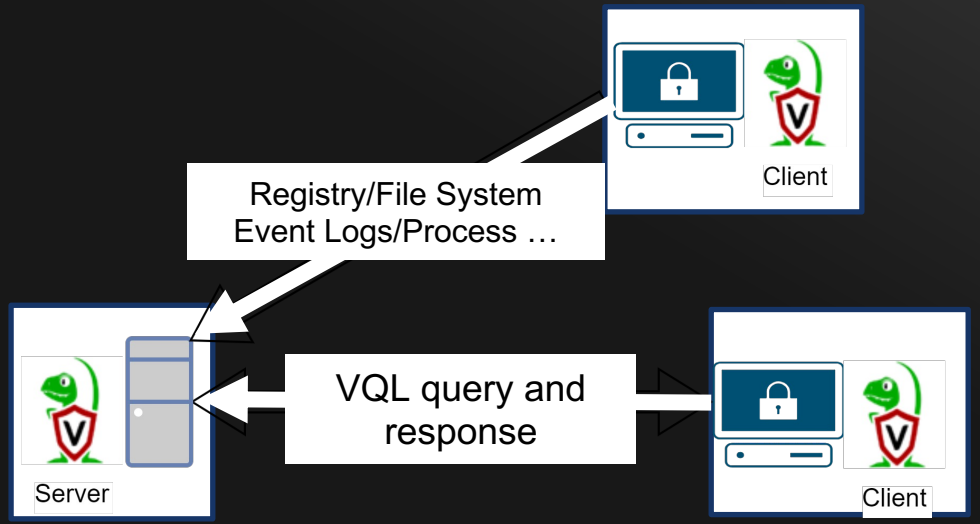


- Go back in time and recreate SIEM!
- Fast forensics on many machines!

About Velociraptor

https://docs.velociraptor.app

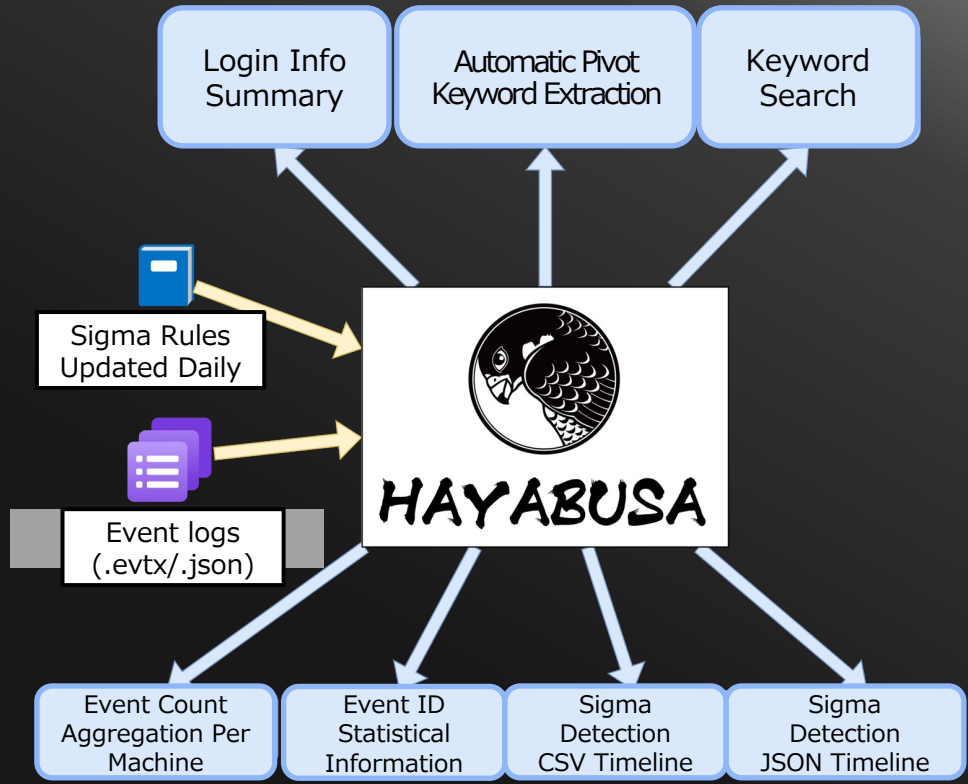
- An OSS EDR-like DFIR tool developed by Mike Cohen.
- Strength in collecting forensic artifacts.
- Can execute queries (VQL) from server-to-client and aggregate data to a server.
- Leverage knowledge by importing queries (VQL) shared by the community.



About Hayabusa

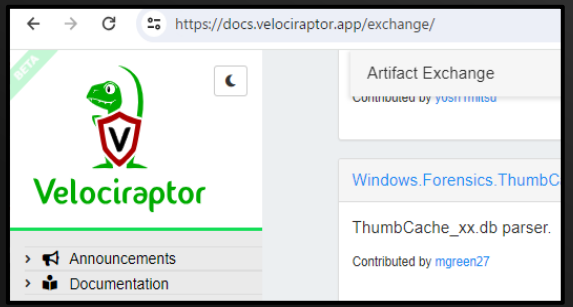
https://github.com/Yamato-Security/hayabusa

- An application that quickly analyzes large amounts of Windows event logs.
- Has various commands specialized for Windows event log analysis
- Synchronize with Sigma repository with one command. Over 4000 Sigma rules built-in

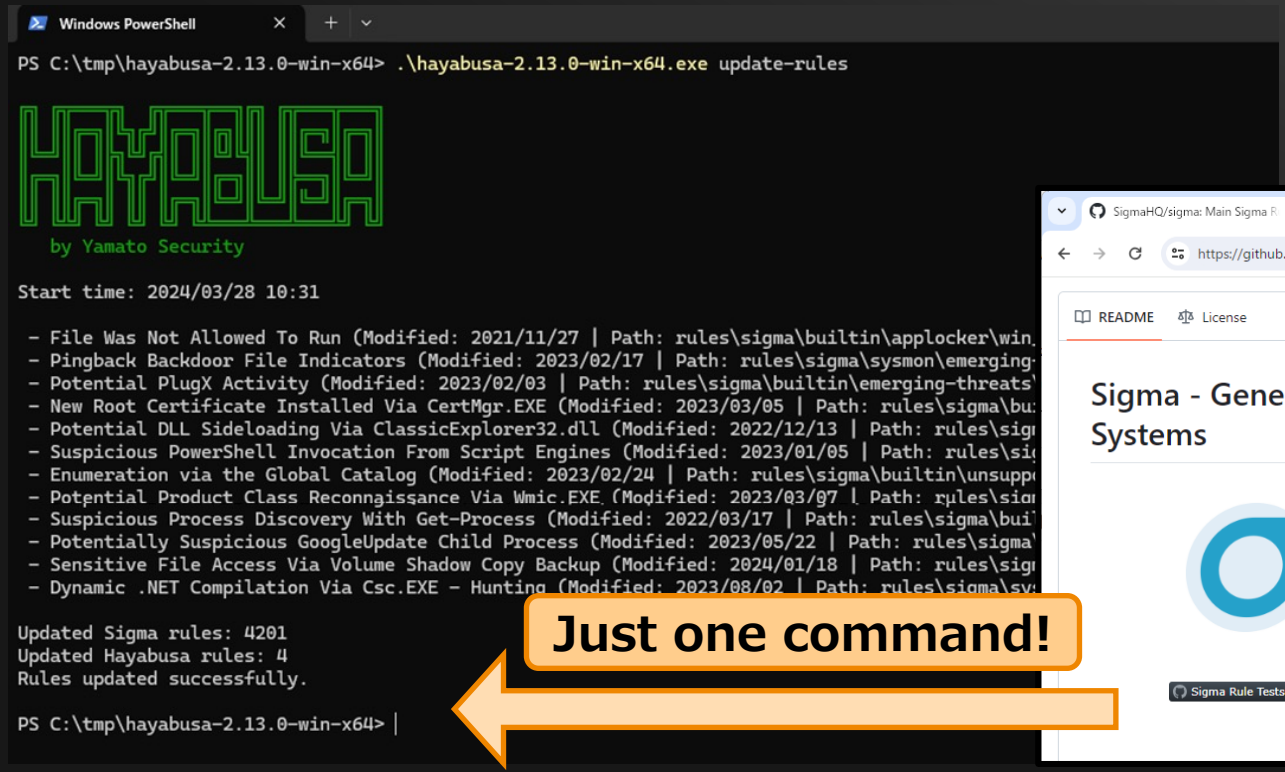


Hayabusa - Sigma - Velociraptor Community knowledge

- Hayabusa and Sigma
  - You can apply the latest rules from the Sigma repository with ‘update-rules’.
  - The Sigma repository updates rules daily and contains the latest knowledge.
- Velociraptor
  - Velociraptor Artifact Exchange
    - ~ Mechanism for sharing queries (VQL) created by the community~
  - Import Server.Import.ArtifactExchange
    - easily use community collection queries (VQL)



Hayabusa - Sigma - Velociraptor Community knowledge



Scalable DFIR environment with Velociraptor + Hayabusa + Takajo

A scalable DFIR environment?

BSides TOKYO

Scalable DFIR environment

Environment

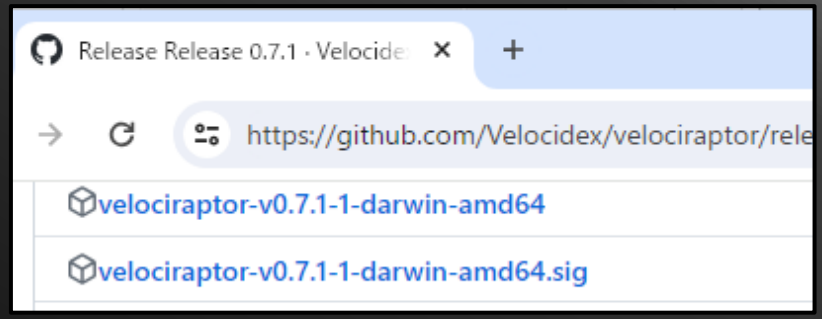
Easy to setup/distribute/collect!

Knowledge

Bulk analysis by Takajo!

Velociraptor environment setup

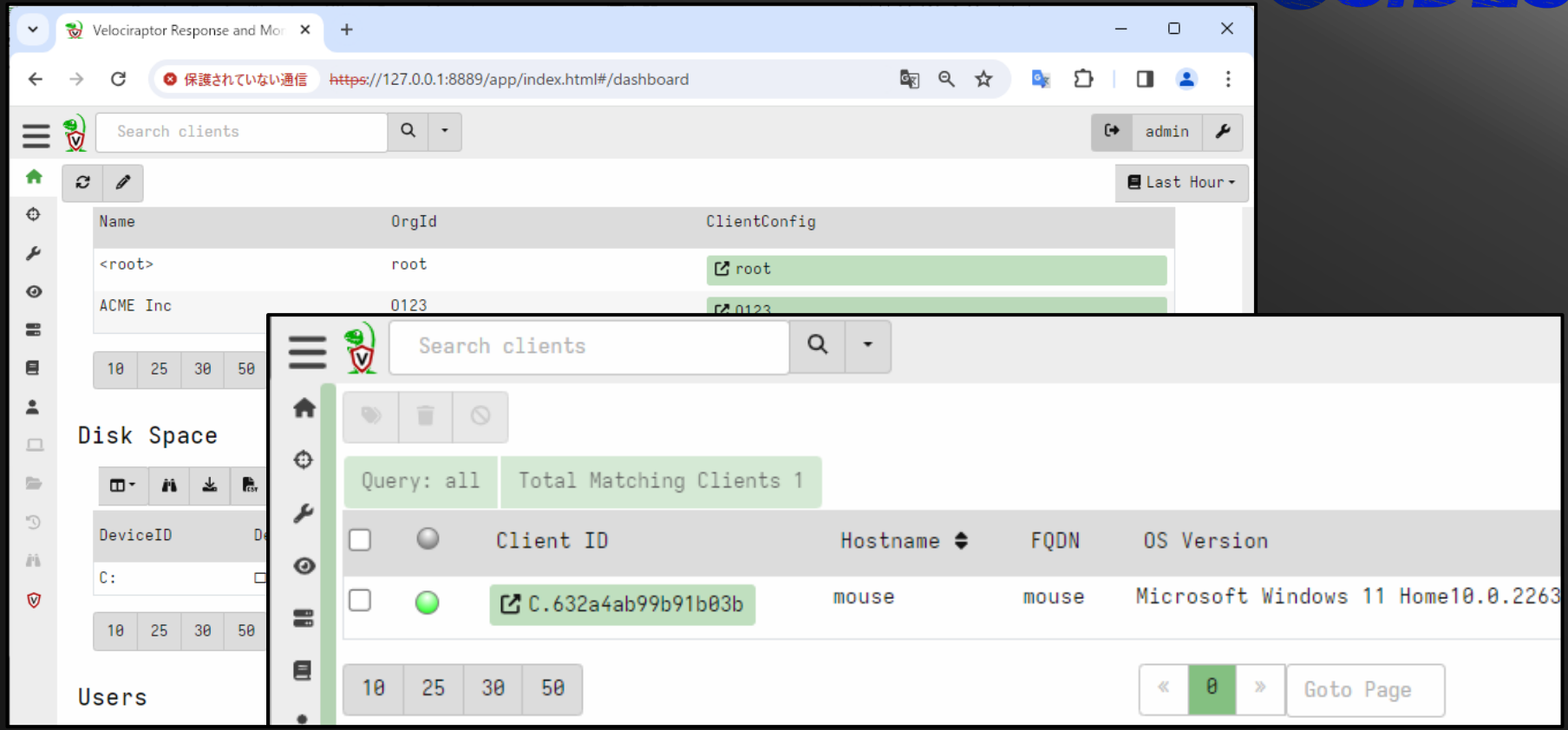
Set up in 3 easy steps:



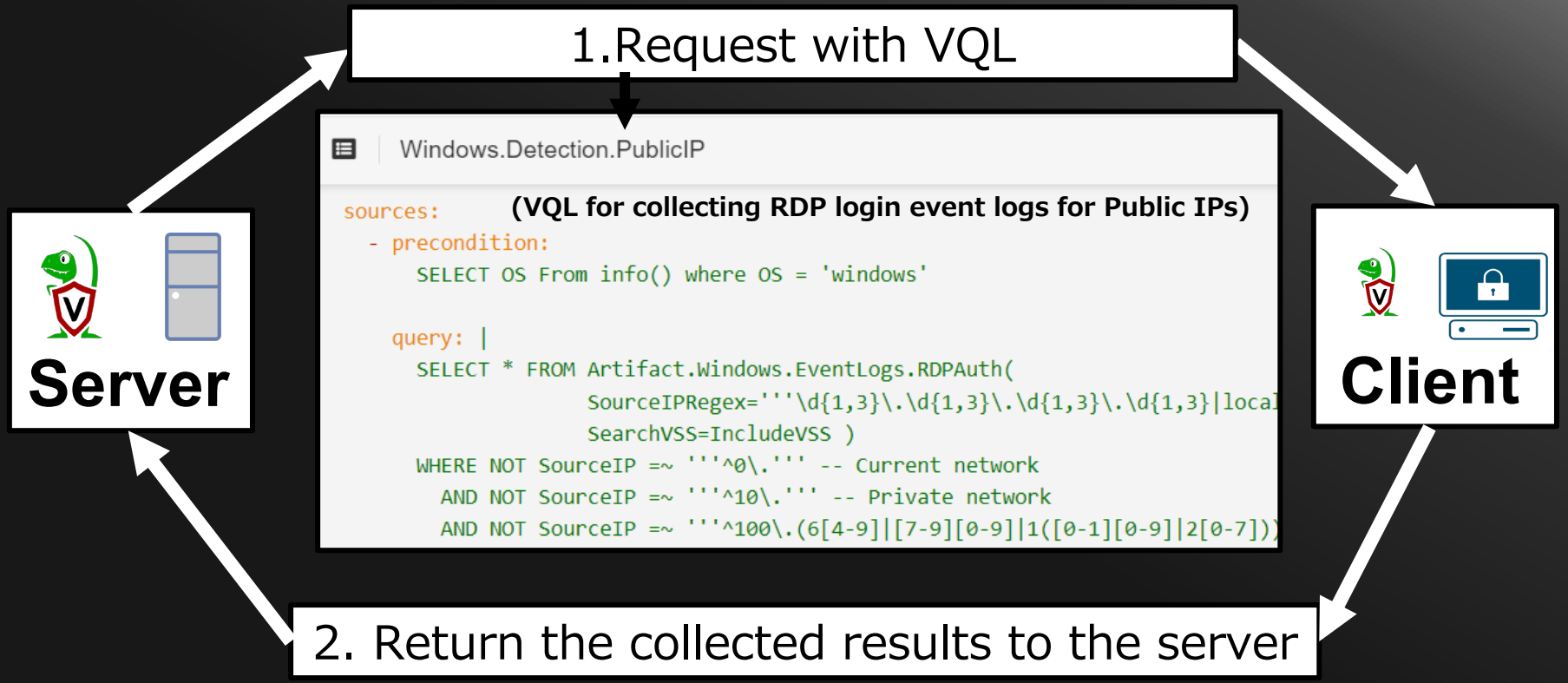
1. Server module startup
    - velociraptor gui
2. Create MSI package for distribution
    - Run Server.Utils.CreateMSI artifact
3. Distribute to client terminal
    - Distribute the MSI package created in <Step 2> using AD Group Policy, Intune, EDR, etc.

… And the setup is now complete!

Velociraptor environment setup



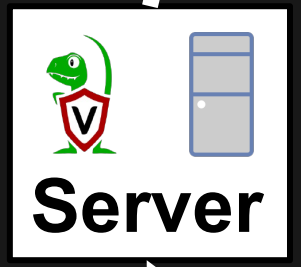
Velociraptor Basics



Distribution, execution, and collection of Hayabusa using VQL

1.Request Hayabusa distribution + execution with VQL

https://docs.velociraptor.app/exchange/artifacts/pages/windows.eventlogs.hayabusa/

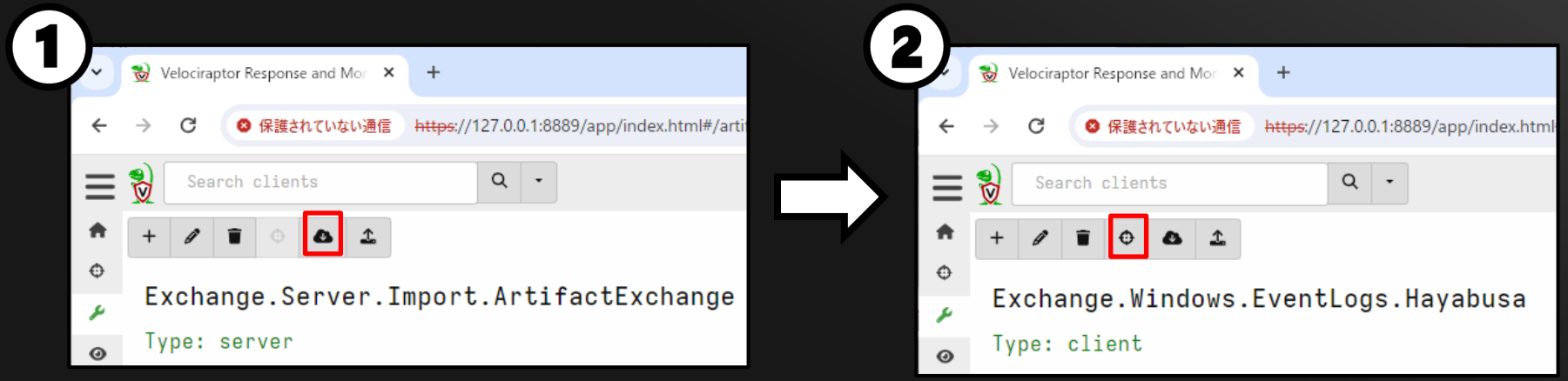


2. Return the collected results to the server

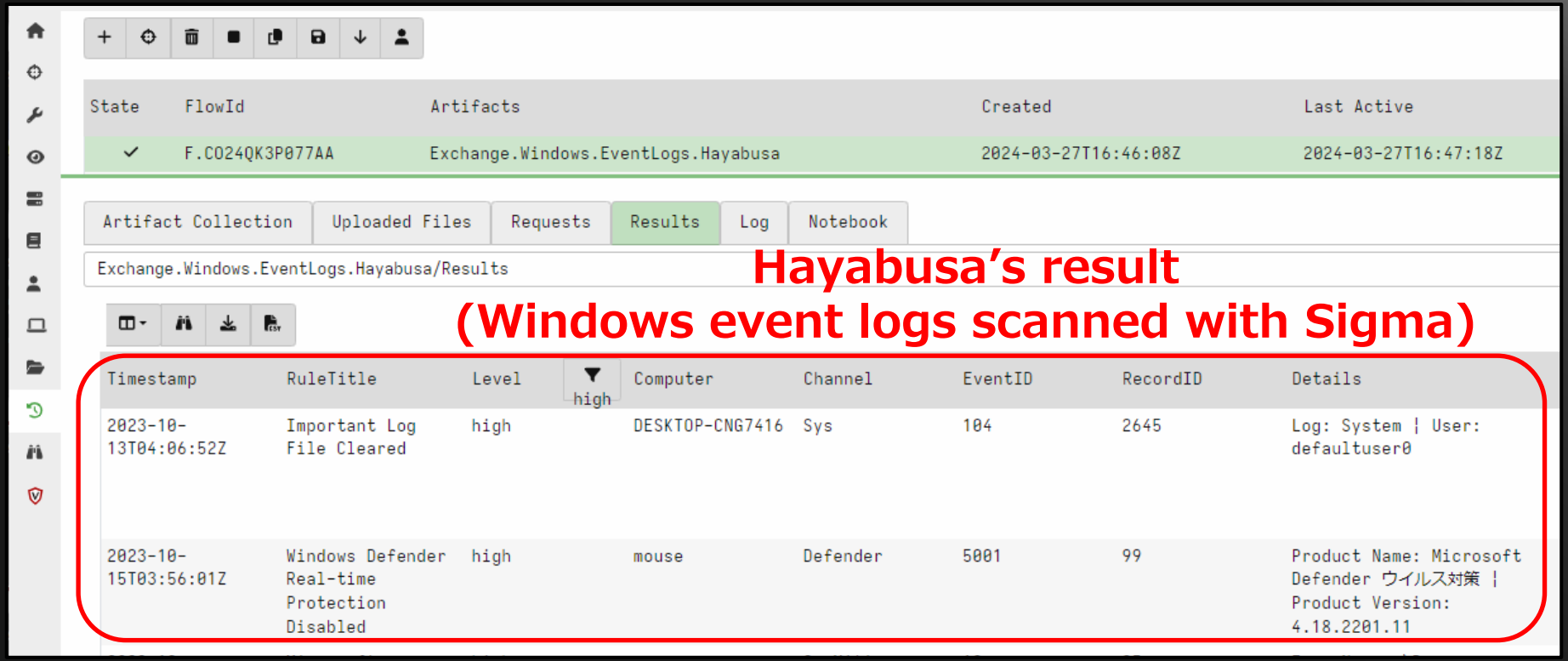
Distribution, execution, and collection of Hayabusa using VQL

Can be started in 2 easy steps!

1. Run Server.Import.ArtifactExchange. Import community VQL
2. Run Exchange.Windows.EventLogs.Hayabusa !



Collecting Windows event log timeline with Hayabusa



State	FlowId	Artifacts	Created	Last Active
✓	F.CO24QK3P077AA	Exchange.Windows.EventLogs.Hayabusa	2024-03-27T16:46:08Z	2024-03-27T16:47:18Z

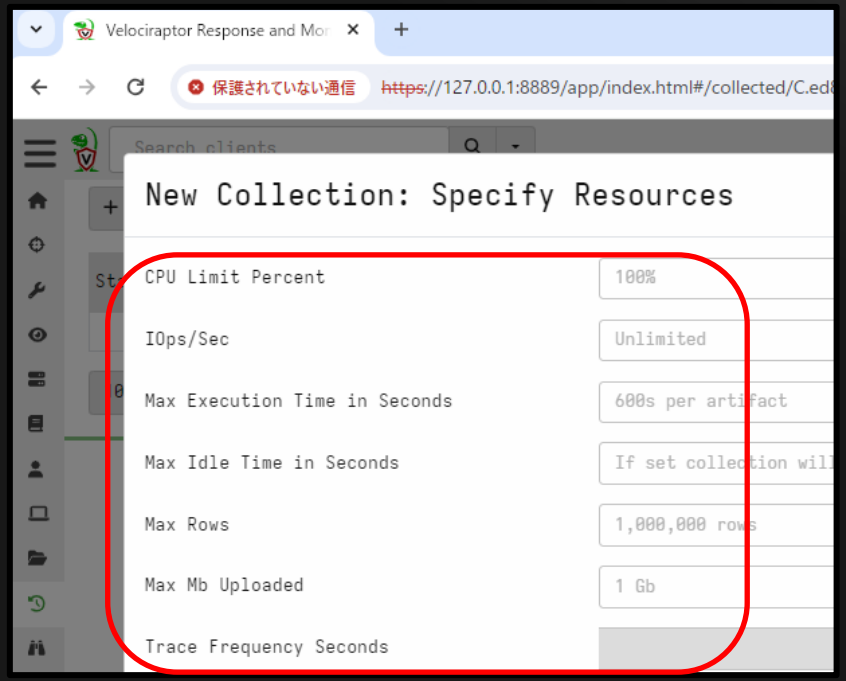
Artifact Collection | Uploaded Files | Requests | Results | Log | Notebook

Exchange.Windows.EventLogs.Hayabusa/Results

Hayabusa's result
(Windows event logs scanned with Sigma)

Timestamp	RuleTitle	Level	high	Computer	Channel	EventID	RecordID	Details
2023-10-13T04:06:52Z	Important Log File Cleared	high		DESKTOP-CNG7416	Sys	104	2645	Log: System ¦ User: defaultuser0
2023-10-15T03:56:01Z	Windows Defender Real-time Protection Disabled	high		mouse	Defender	5001	99	Product Name: Microsoft Defender ウイルス対策 ¦ Product Version: 4.18.2201.11

Tip! Specify client resource limits with Velociraptor



But it can only be used with the Velociraptor built-in module...

Resource limit specification does not work for Hayabusa, which is not built-in...

So, we are releasing new features today!

New Hayabusa features released!

--low-memory-mode!!

Special Thanks to: James Takai

Achieving advanced detection
while reducing average client load!

New Hayabusa features released!

BSides TOKYO

Analyzing Windows event logs in JSON format exported with Splunk!

Special Thanks to: DustInDark

Even in SIEM environments with insufficient detection rules, advanced Sigma scans are possible later!

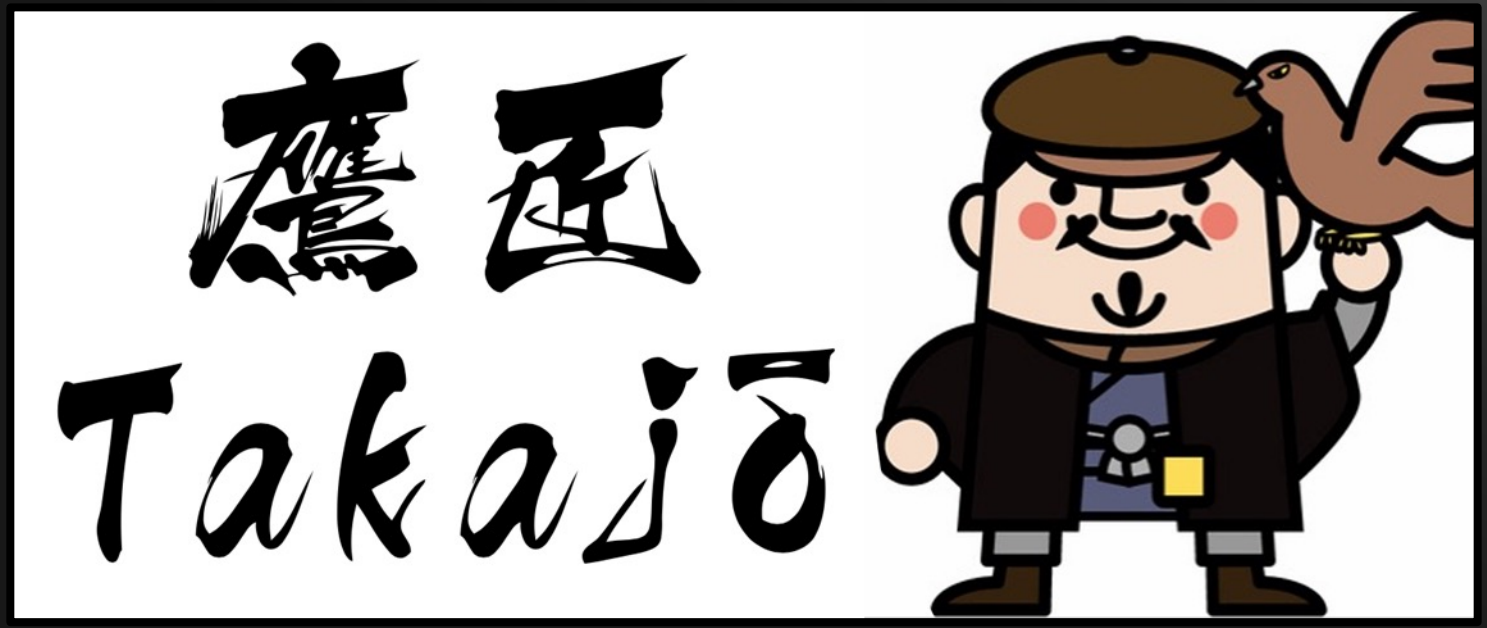
The next step...

We collected **event log analysis results** from multiple clients at once using **Velociraptor** and **Hayabusa**!

The next step is to **analyze** this all at once🤔

Knowledge scalability

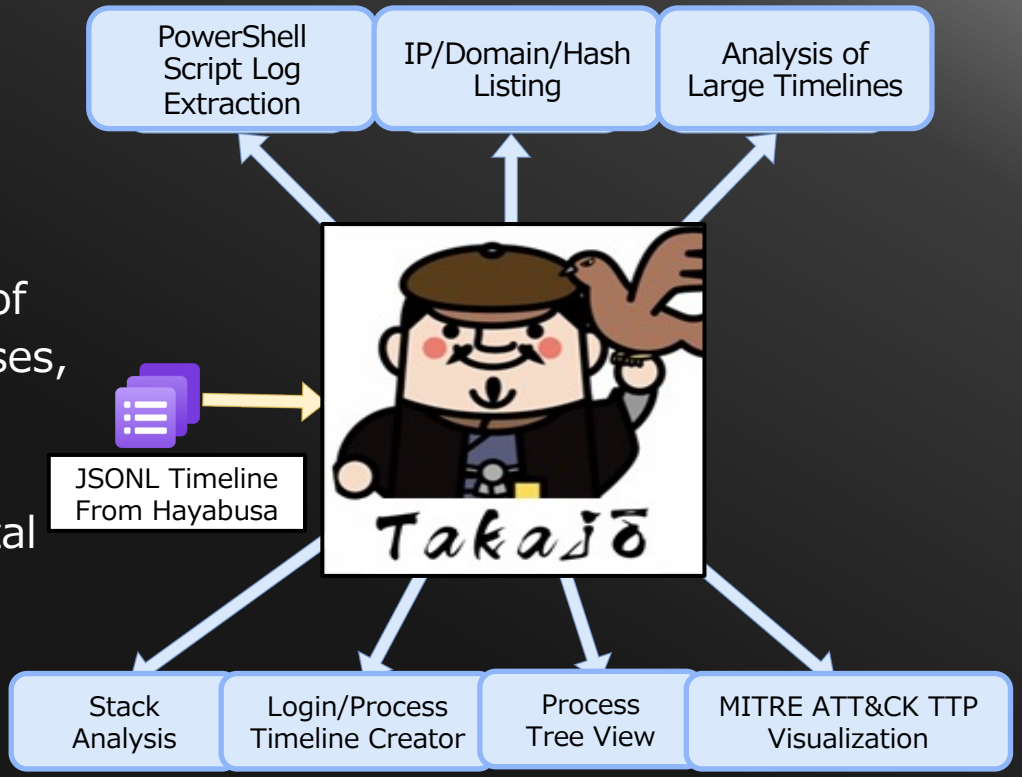
Yamato Security's analysis know-how with commands!



About Takajo

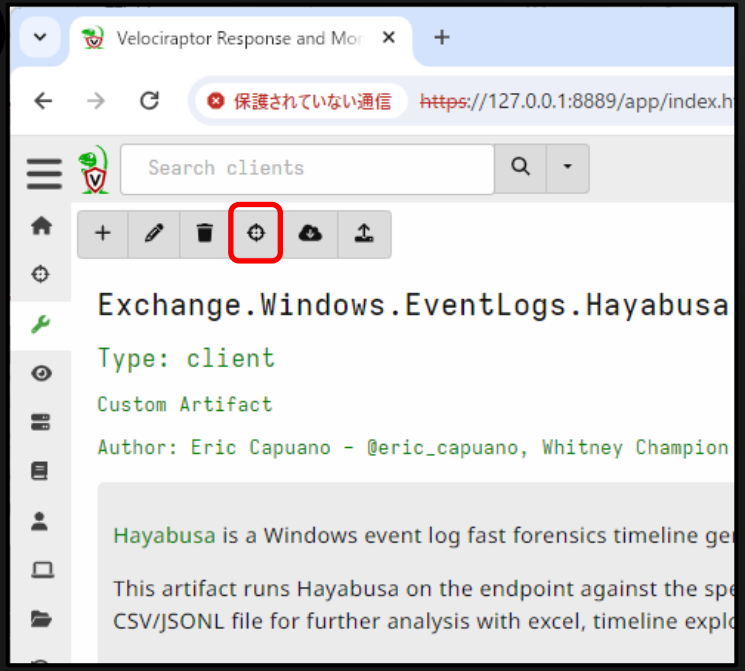
https://github.com/Yamato-Security/takajo

- Tool to analyze Hayabusa timeline (JSONL format)
- Aggregation and stacking analysis of command line, DNS, logon, processes, services, scheduled tasks, etc.
- IP/Domain/Hash lookup in VirusTotal
- MITER ATT&CK TTP visualization

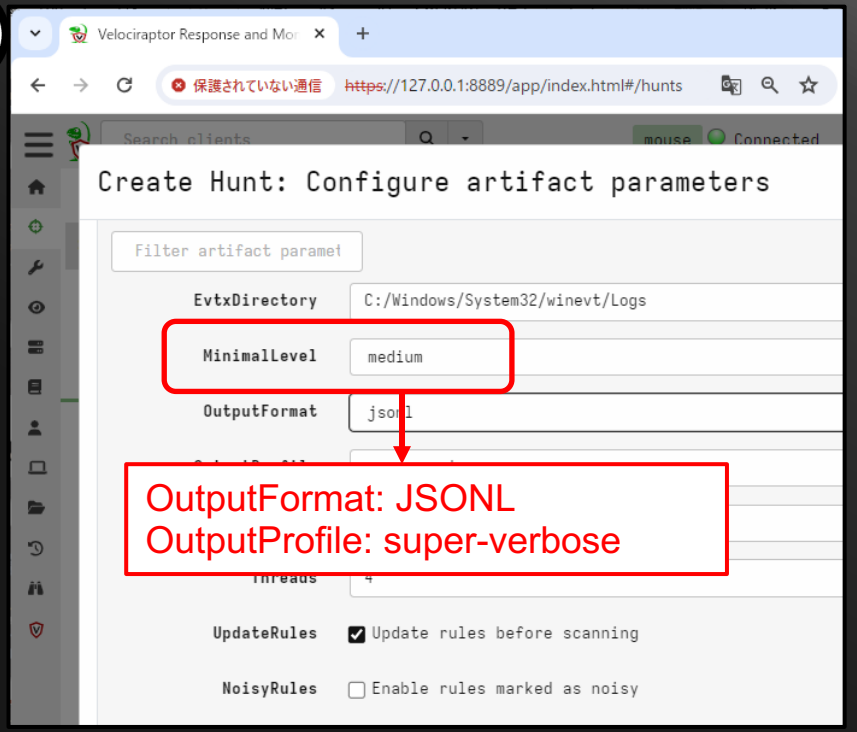


Collect Hayabusa timelines from multiple client at once

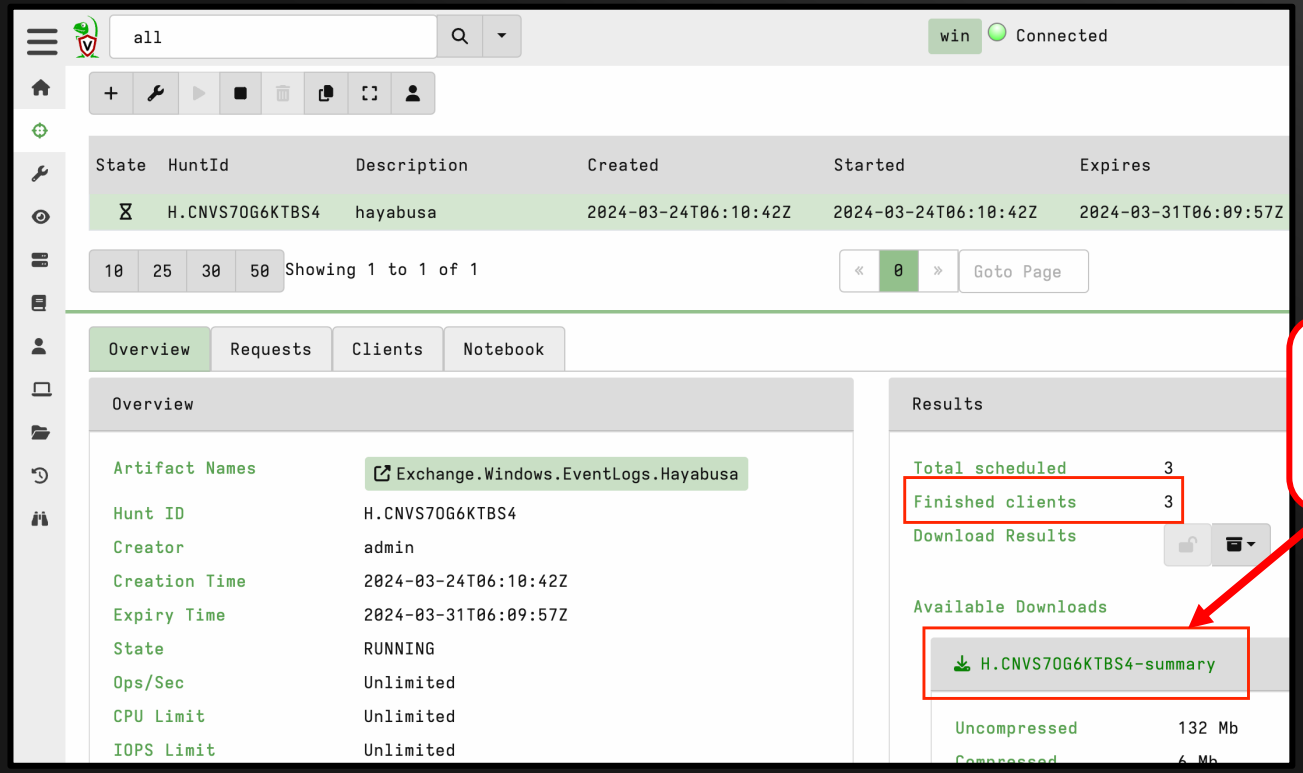
1



2



Collect Hayabusa timelines from multiple client at once



Hayabusa results for multiple clients can be downloaded in one file!

Takajo new feature released!

‘automagic’ command !

= Batch analysis of multiple files !

Takajo's various analysis commands and
Analyze multiple files in one go!

All analyzed by Takajo automagic!

Batch analysis only requires the following two steps!

1. **Download Hunt result JSON from Velociraptor GUI**
2. takajo.exe automagic –t <Step 1> .jsonl

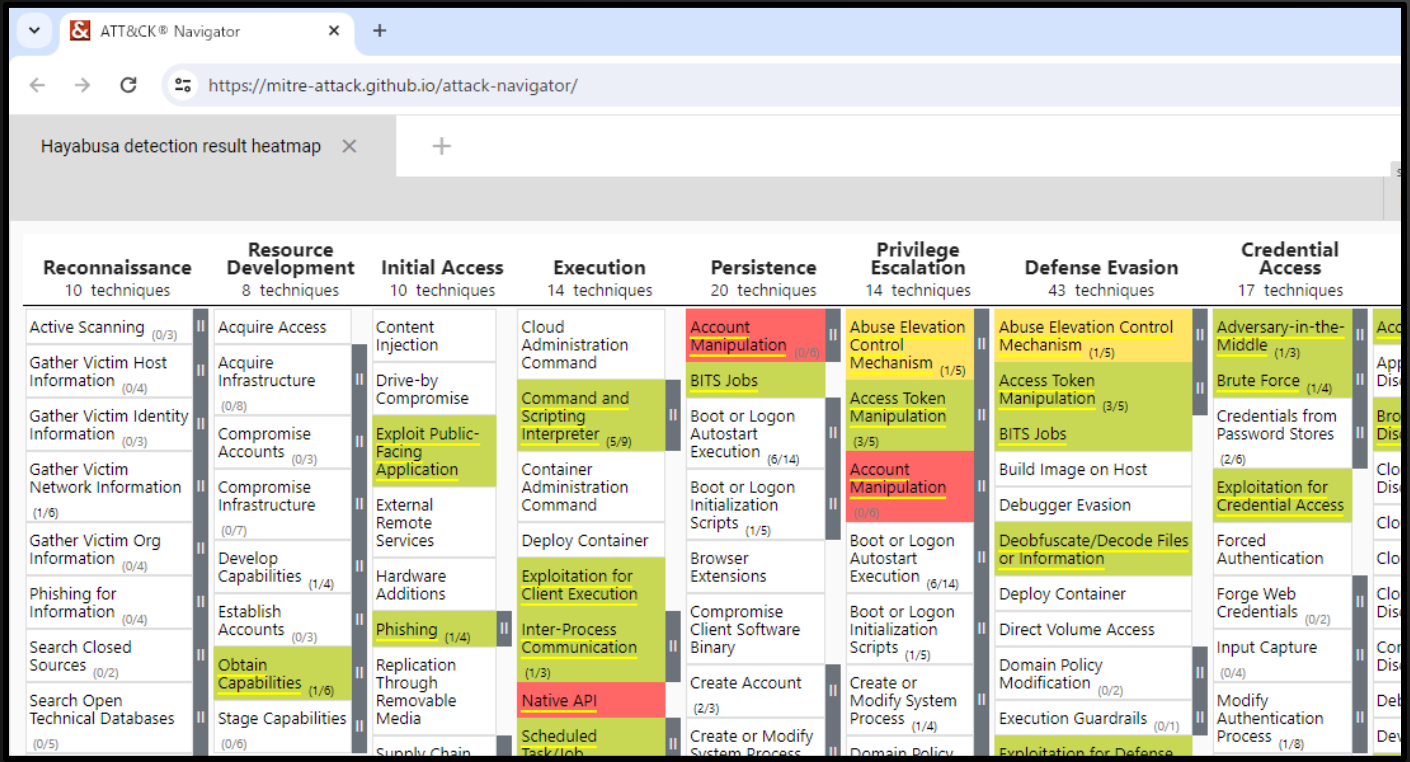
With the above,
you can analyze Hayabusa timeline results from multiple clients at once!

All analyzed by Takajo automagic!

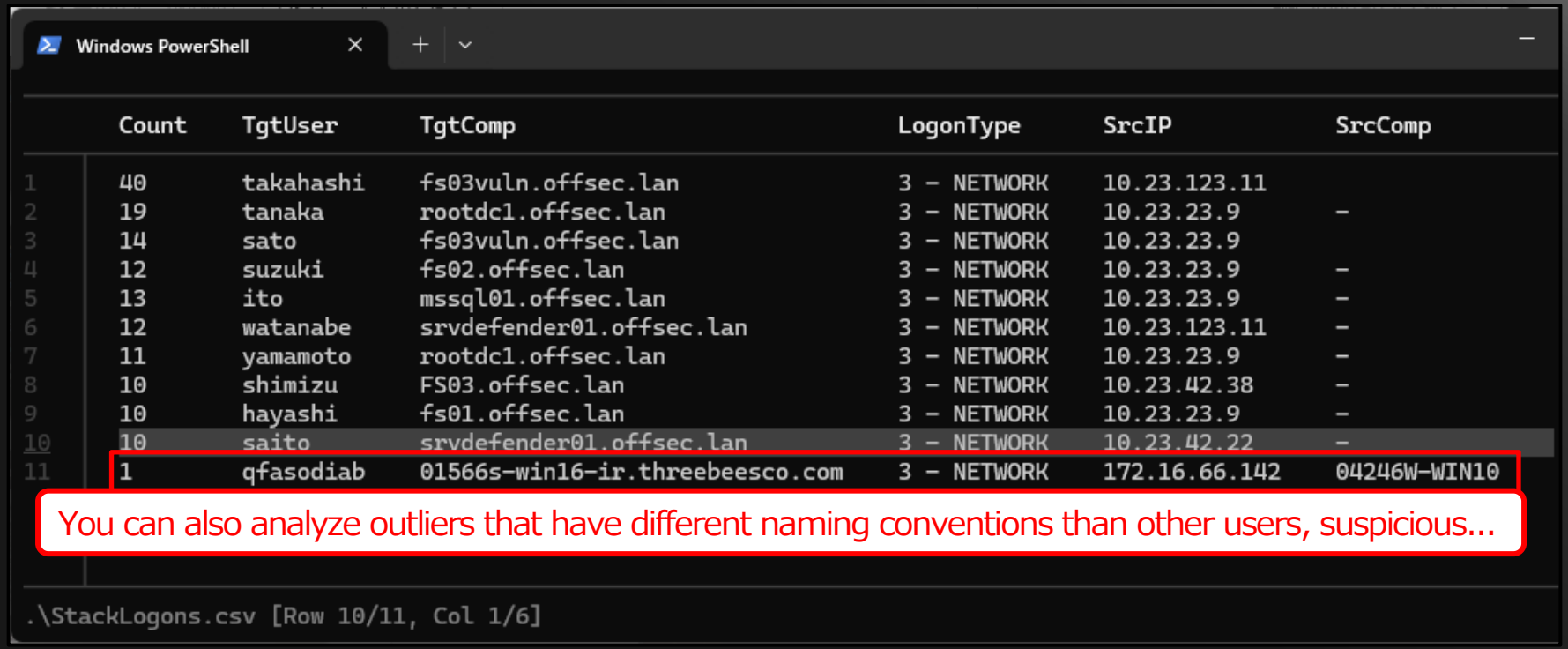
```
PS C:\tmp\takajo-2.4.0-win> .\takajo automagic -t .\timeline.jsonl -q
Started the automagic command

Automatically executes as many commands as possible and output results to a new folder.

File: .\timeline.jsonl (45.27 MB)
Counting total lines. Please wait.
Total lines: 34,940

Scanning the Hayabusa timeline. Please wait.

100%|████████████████████| 34940/34940 [ 3.0s< 0.0s,  61.55k/sec]
```

Command	Results	Saved Files
extract-scriptblocks	PowerShell logs: 108	case-1/scriptblock-logs/Summary.csv (19.92 case-1/scriptblock-logs/*.txt
list-domains	Domains: 0	case-1/ListDomains.txt (0 Bytes)
list-domains(detailed)	Domains: 2	case-1/ListDomainsDetailed.txt (16 Bytes)
list-hashes	MD5: 1,038 SHA1: 976 SHA256: 978 Import: 1,038	case-1/ListHashes-MD5.txt (4.88 KB) case-1/ListHashes-SHA1.txt (5.66 KB) case-1/ListHashes-SHA256.txt (9.02 KB) case-1/ListHashes-ImportHashes.txt (4.28 KB
list-ip-addresses	IP adddresses: 0	case-1/ListIP-Addresses.txt (0 Bytes)
stack-cmdlines	Unique cmdlines: 1,411	case-1/StackCmdlines.csv (814.13 KB)
stack-computers	Unique computers: 54	case-1/StackTargetComputers.csv (49.51 KB)
stack-computers	Unique computers: 3,571	case-1/StackSourceComputers.csv (383.32 KB)

Visualization of MITRE ATT&CK TTPs with automagic results



Stack analysis with automagic results



All analyzed by Takajo automagic!

Many other analysis results can be output with a single run of automagic:

- List Domain/IP/Hash
- Stacking Scheduled Tasks
- Stacking Users
- Stacking Service names
- Task scheduler timeline
- Logon timeline
- Process timeline
- PowerShell execution history
- MITRE ATT&CK TTPs
- …etc.

Takeaways

Velociraptor + Hayabusa + Takajo gives you two “scalables”

- Scalable environment
  - **Simply set up Velociraptor** and collect forensic artifacts via the client.
  - Analyze logs **from multiple clients with Hayabusa.**
    - You can get forensic artifacts quickly

- Scalable knowledge
  - Takajo is packed with **Yamato Security know-how**
  - Takajo can get analysis results with a **single command.**
    - Deeper analysis possible **in less time.**

Thank you so much for listening!

If you like our tools, please consider supporting us with a GitHub star!

Check out the latest release information on X!

Follow:
@SecurityYamato

Thank you for your attention!