AI & ML

IN

THREAT DETECTION

Revolutionizing Cybersecurity with Intelligent Systems

WHAT IS AI AND ML

1

Artificial Intelligence

Simulation of human intelligence in machines.

2

MACHINE LEARNING

AI subfield, enabling machines to learn from data.

3

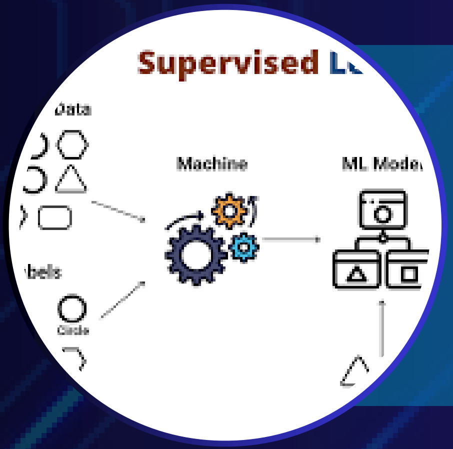
Why AI & ML...?

They bring automation, speed, and accuracy to threat detection.

Core Benefits of AI and ML in Threat Detection

- Real-time threat detection
- Reduction of false positives
- Automation of repetitive tasks
- Threat intelligence enrichment
- 24/7 monitoring with self-learning
- Predictive analytics

COMMON AI/ML ALGORITHMS USED IN THREAT DETECTION



Supervised Learning

Unsupervised Learning

Reinforcement Learning

Deep Learning

USE CASE IN THREAT (MALWARE) DETECTION

- CrowdStrike’s Falcon uses ML algorithms to detect fileless malware.
- It learns behavioral patterns of malicious code
- Detects even when traditional signature-based AV fails

AI & ML INTEGRATIONS THAT IMPROVES THREAT DETECTION

1 Explainable AI (XAI)

- Make AI decisions transparent
- Justifies why an alert was triggered
- EG. IBM’s Watson for Cyber Security provides traceable threat explanations to security teams.

2 Federated Learning

- Decentralized training without sharing raw data
- Enables organizations to share threat insights without violating data privacy
- EG. Intel and BeeKeeperAI work on federated learning in healthcare cybersecurity

3 Zero Trust Architecture Enhanced by AI

- Continuously validates users and devices
- Dynamic policy enforcement based on behavior
- EG. Microsoft Azure Active Directory uses ML to enforce adaptive access controls

4 Self-Healing Security Systems

- Systems that detect, respond, and recover autonomously
- They predict incidents and triggers responses
- EG. Darktrace uses AI to isolate infected devices automatically during an attack

AI & ML INTEGRATIONS THAT IMPROVES THREAT DETECTION

5 Multi-Modal AI Models

- Use of multiple data types (logs, text, images, audio)
- Aids in Cross-validation for stronger detection
- EG. Palo Alto Networks uses multimodal inputs to detect phishing, malware, and anomalies

6 Model Context Protocol (MCP)

7

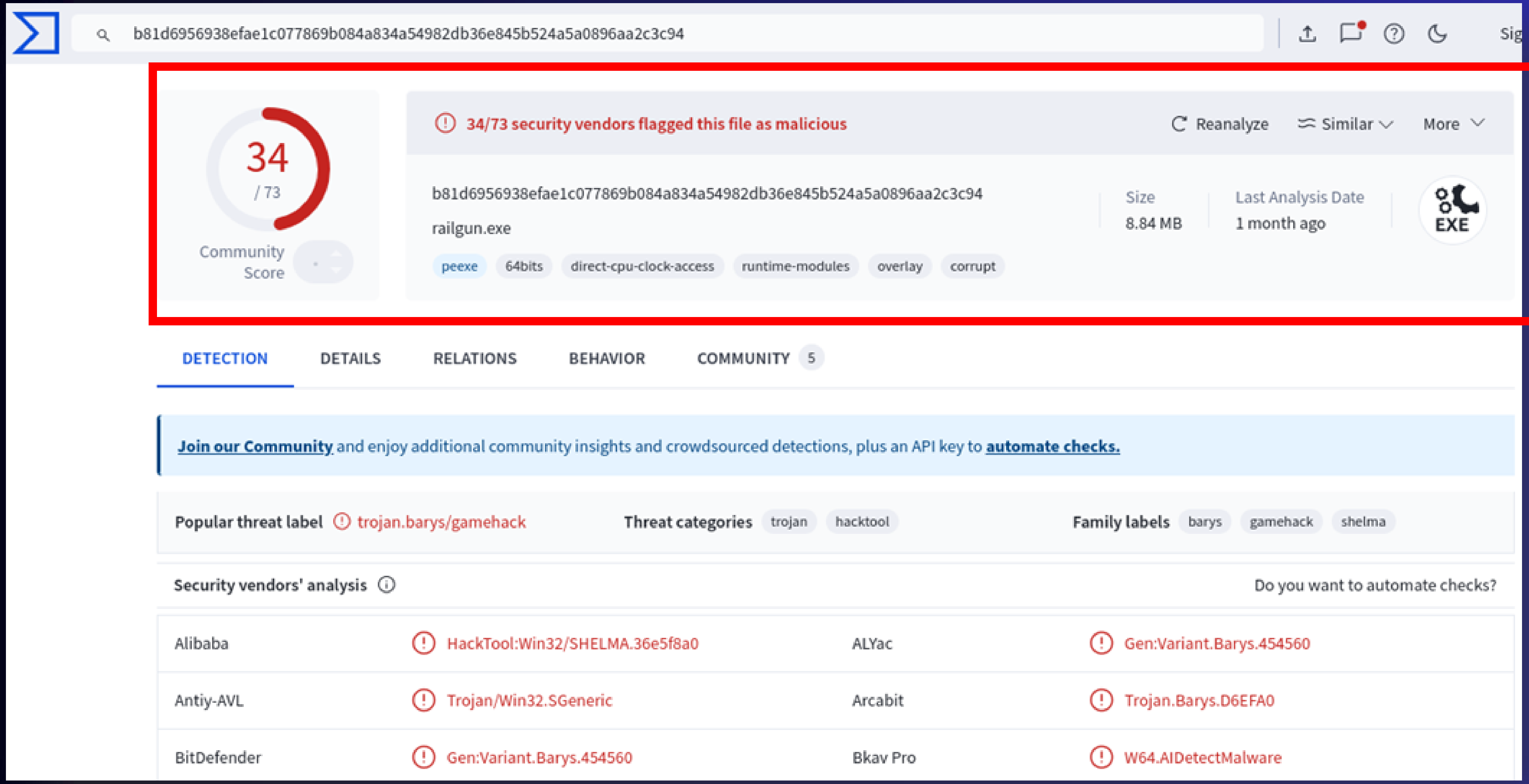
- Enables AI models to leverage external tools and data sources, providing more comprehensive understanding of security threats
- Helps the model understand surrounding conditions to make smarter decisions

7 Synthetic Data for Model Training

- Artifically generated data to train machine learning models, especially when real data is scarce/private/expensive.
- EG. AI makes synthetic financial data for fraud detection modeling

8 Agent Communication Protocol

- Enables coordination between AI agents
- Distributed AI agents can share threat signals, coordinate response
- Security Orchestration tools (like Splunk SOAR) use agent protocols for response coordination



b81d6956938efae1c077869b084a834a54982db36e845b524a5a0896aa2c3c94

34
/ 73
Community Score

34/73 security vendors flagged this file as malicious

b81d6956938efae1c077869b084a834a54982db36e845b524a5a0896aa2c3c94
railgun.exe
peexe 64bits direct-cpu-clock-access runtime-modules overlay corrupt

Size
8.84 MB

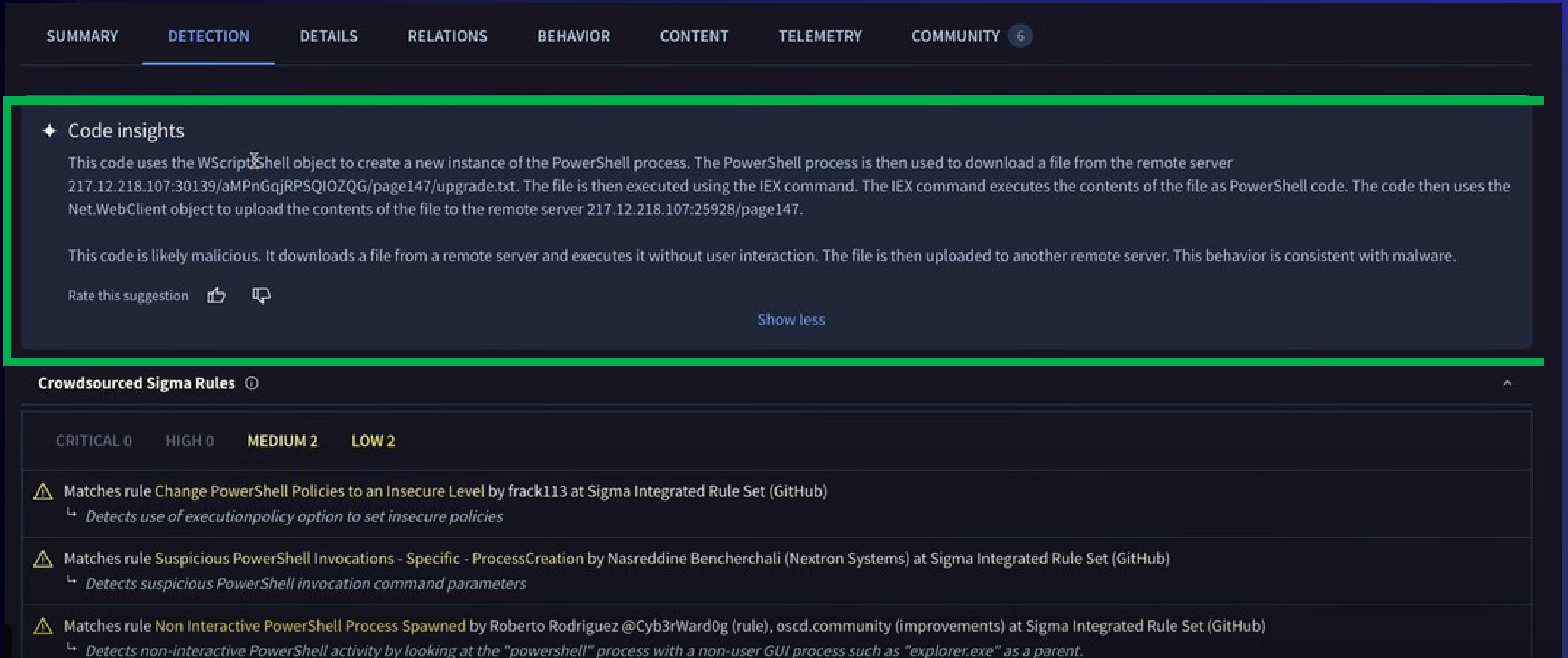
Last Analysis Date
1 month ago

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

Popular threat label trojan.barys/gamehack **Threat categories** trojan hacktool **Family labels** barys gamehack shelma

Security vendors' analysis Do you want to automate checks?

Alibaba	HackTool:Win32/SHELMA.36e5f8a0	ALYac	Gen:Variant.Barys.454560
Antiy-AVL	Trojan/Win32.SGeneric	Arcabit	Trojan.Barys.D6EFA0
BitDefender	Gen:Variant.Barys.454560	Bkav Pro	W64.AIDetectMalware



✦ Code insights

This code uses the WScript.Shell object to create a new instance of the PowerShell process. The PowerShell process is then used to download a file from the remote server 217.12.218.107:30139/aMPnGqjRPSQIOZQG/page147/upgrade.txt. The file is then executed using the IEX command. The IEX command executes the contents of the file as PowerShell code. The code then uses the Net.WebClient object to upload the contents of the file to the remote server 217.12.218.107:25928/page147.

This code is likely malicious. It downloads a file from a remote server and executes it without user interaction. The file is then uploaded to another remote server. This behavior is consistent with malware.

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 2 LOW 2

⚠ Matches rule Change PowerShell Policies to an Insecure Level by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Detects use of executionpolicy option to set insecure policies*

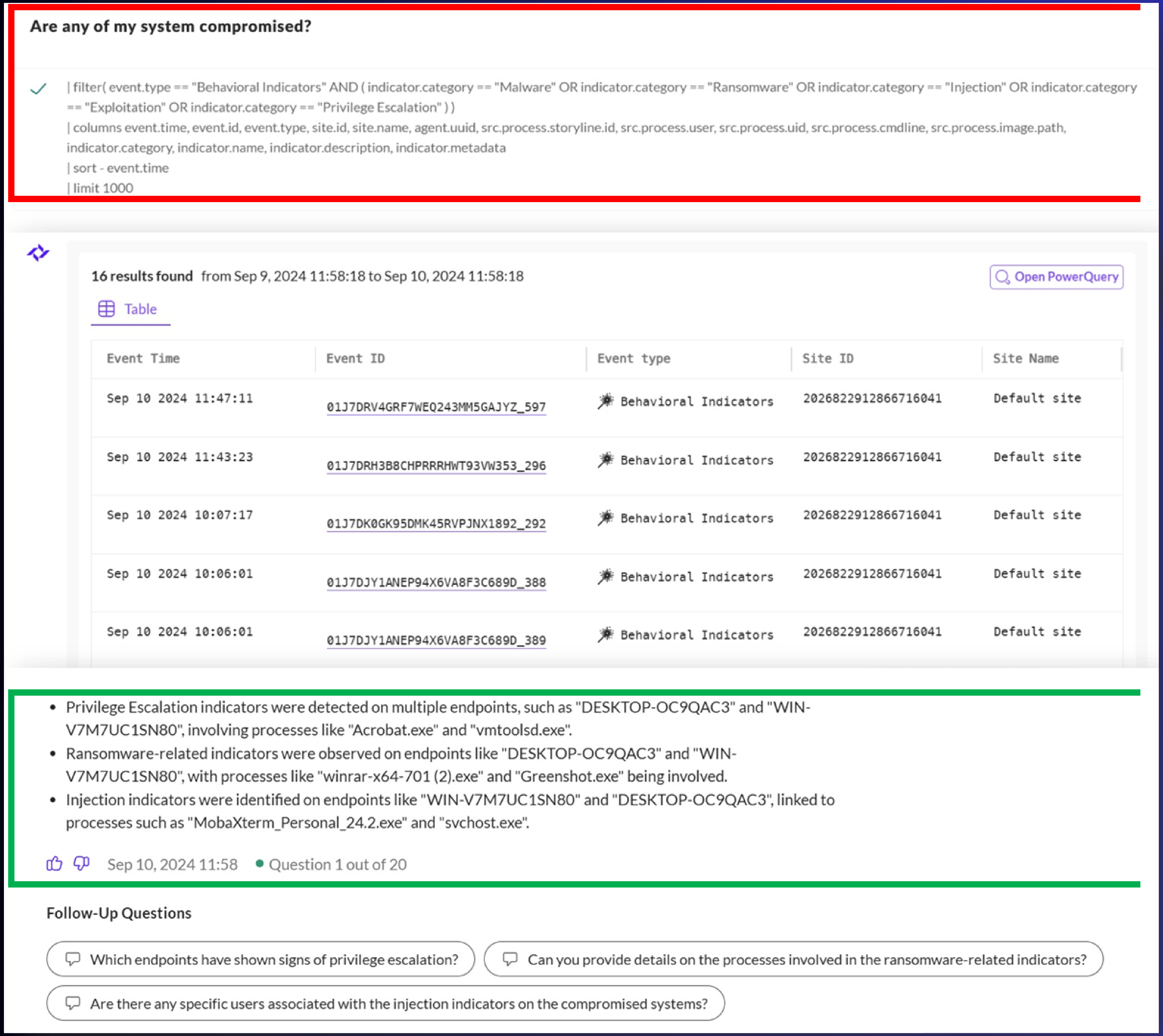
⚠ Matches rule Suspicious PowerShell Invocations - Specific - ProcessCreation by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
↳ *Detects suspicious PowerShell invocation command parameters*

⚠ Matches rule Non Interactive PowerShell Process Spawned by Roberto Rodriguez @Cyb3rWard0g (rule), oscd.community (improvements) at Sigma Integrated Rule Set (GitHub)
↳ *Detects non-interactive PowerShell activity by looking at the "powershell" process with a non-user GUI process such as "explorer.exe" as a parent.*

X **Pattern Recognition**

X **Predictive Analytics**

X **Real-time Monitoring**



Are any of my system compromised?

```
| filter( event.type == "Behavioral Indicators" AND ( indicator.category == "Malware" OR indicator.category == "Ransomware" OR indicator.category == "Injection" OR indicator.category
== "Exploitation" OR indicator.category == "Privilege Escalation" ) )
| columns event.time, event.id, event.type, site.id, site.name, agent.uuid, src.process.storyline.id, src.process.user, src.process.uid, src.process.cmdline, src.process.image.path,
indicator.category, indicator.name, indicator.description, indicator.metadata
| sort - event.time
| limit 1000
```

16 results found from Sep 9, 2024 11:58:18 to Sep 10, 2024 11:58:18

Event Time	Event ID	Event type	Site ID	Site Name
Sep 10 2024 11:47:11	01J7DRV4GRF7WEQ243MM5GAJYZ_597	Behavioral Indicators	2026822912866716041	Default site
Sep 10 2024 11:43:23	01J7DRH3B8CHPRRRHWT93VW353_296	Behavioral Indicators	2026822912866716041	Default site
Sep 10 2024 10:07:17	01J7DK0GK95DMK45RVPJNX1892_292	Behavioral Indicators	2026822912866716041	Default site
Sep 10 2024 10:06:01	01J7DJY1ANEP94X6VA8F3C689D_388	Behavioral Indicators	2026822912866716041	Default site
Sep 10 2024 10:06:01	01J7DJY1ANEP94X6VA8F3C689D_389	Behavioral Indicators	2026822912866716041	Default site

- Privilege Escalation indicators were detected on multiple endpoints, such as "DESKTOP-OC9QAC3" and "WIN-V7M7UC1SN80", involving processes like "Acrobat.exe" and "vmtoolsd.exe".
- Ransomware-related indicators were observed on endpoints like "DESKTOP-OC9QAC3" and "WIN-V7M7UC1SN80", with processes like "winrar-x64-701 (2).exe" and "Greenshot.exe" being involved.
- Injection indicators were identified on endpoints like "WIN-V7M7UC1SN80" and "DESKTOP-OC9QAC3", linked to processes such as "MobaXterm_Personal_24.2.exe" and "svchost.exe".

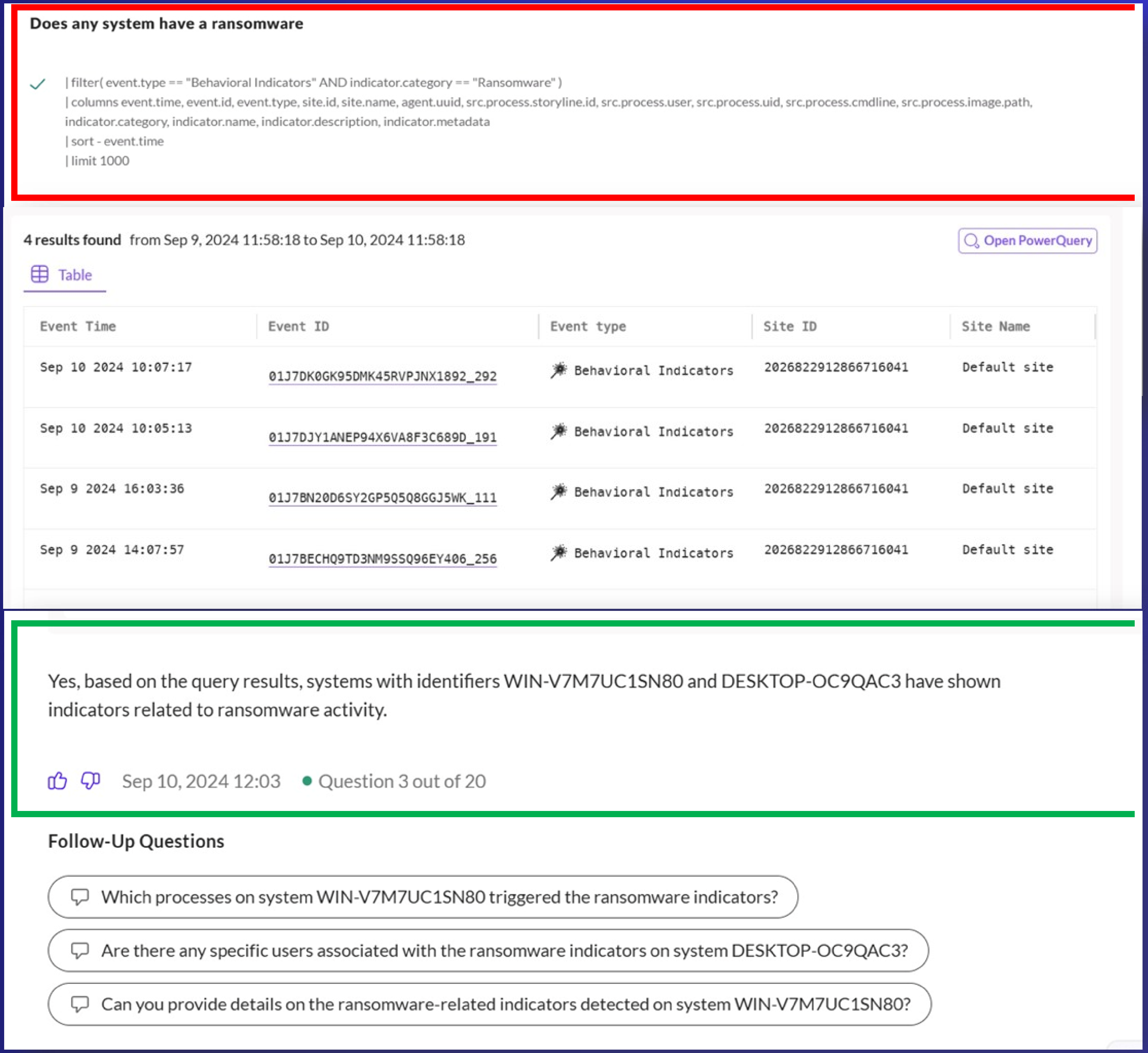
Sep 10, 2024 11:58 ● Question 1 out of 20

Follow-Up Questions

- Which endpoints have shown signs of privilege escalation?
- Can you provide details on the processes involved in the ransomware-related indicators?
- Are there any specific users associated with the injection indicators on the compromised systems?

splunk>
Azure Sentinel
RAPID7
insightIDR
?

- X **Automated Response**
- X **Enhanced Decision Making**
- X **Post-Incident Analysis**



Does any system have a ransomware

```
✓ | filter( event.type == "Behavioral Indicators" AND indicator.category == "Ransomware" )
  | columns event.time, event.id, event.type, site.id, site.name, agent.uuid, src.process.storyline.id, src.process.user, src.process.uid, src.process.cmdline, src.process.image.path,
  indicator.category, indicator.name, indicator.description, indicator.metadata
  | sort - event.time
  | limit 1000
```

4 results found from Sep 9, 2024 11:58:18 to Sep 10, 2024 11:58:18

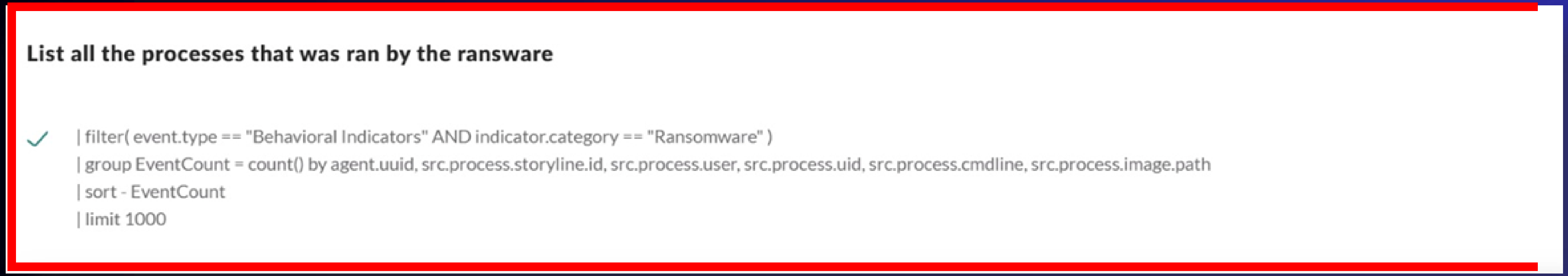
Event Time	Event ID	Event type	Site ID	Site Name
Sep 10 2024 10:07:17	01J7DK0GK95DMK45RVPJNX1892_292	Behavioral Indicators	2026822912866716041	Default site
Sep 10 2024 10:05:13	01J7DJY1ANEP94X6VA8F3C689D_191	Behavioral Indicators	2026822912866716041	Default site
Sep 9 2024 16:03:36	01J7BN20D6SY2GP5Q5Q8GGJ5WK_111	Behavioral Indicators	2026822912866716041	Default site
Sep 9 2024 14:07:57	01J7BECHQ9TD3NM9SSQ96EY406_256	Behavioral Indicators	2026822912866716041	Default site

Yes, based on the query results, systems with identifiers WIN-V7M7UC1SN80 and DESKTOP-OC9QAC3 have shown indicators related to ransomware activity.

Sep 10, 2024 12:03 • Question 3 out of 20

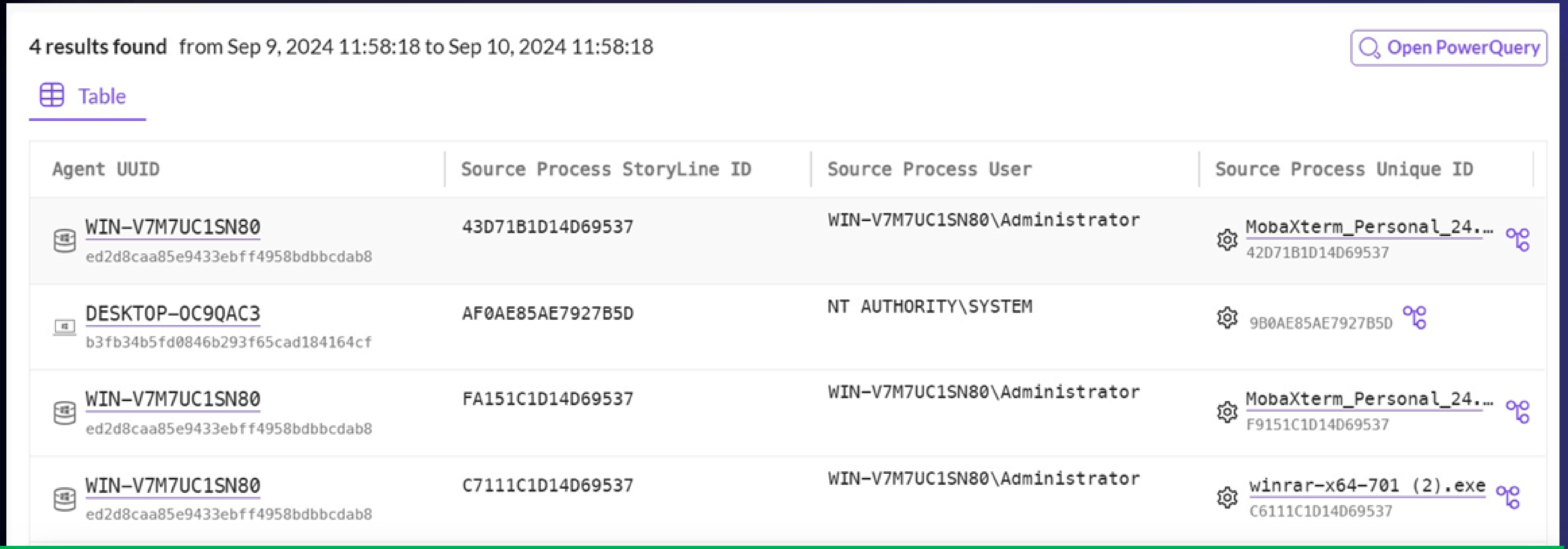
Follow-Up Questions

- Which processes on system WIN-V7M7UC1SN80 triggered the ransomware indicators?
- Are there any specific users associated with the ransomware indicators on system DESKTOP-OC9QAC3?
- Can you provide details on the ransomware-related indicators detected on system WIN-V7M7UC1SN80?



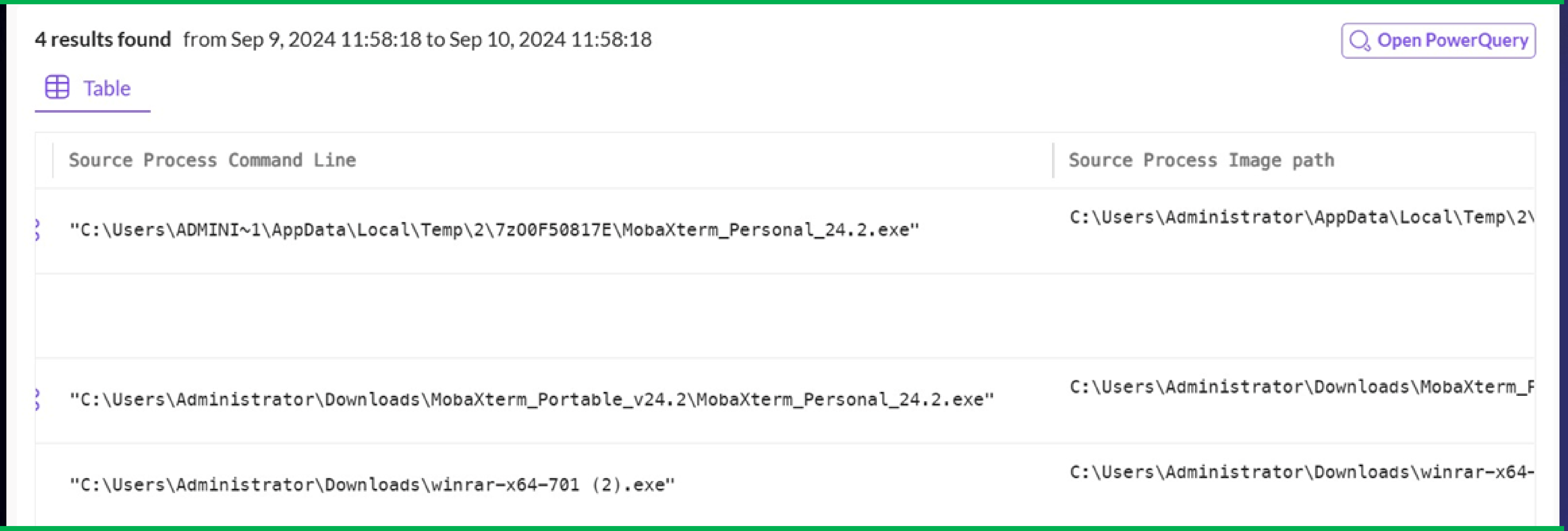
List all the processes that was ran by the ransware

```
| filter( event.type == "Behavioral Indicators" AND indicator.category == "Ransomware" )
| group EventCount = count() by agent.uuid, src.process.storyline.id, src.process.user, src.process.uid, src.process.cmdline, src.process.image.path
| sort - EventCount
| limit 1000
```



4 results found from Sep 9, 2024 11:58:18 to Sep 10, 2024 11:58:18

Agent UUID	Source Process StoryLine ID	Source Process User	Source Process Unique ID
WIN-V7M7UC1SN80 ed2d8caa85e9433ebff4958bdbbcdab8	43D71B1D14D69537	WIN-V7M7UC1SN80\Administrator	MobaXterm_Personal_24.… 42D71B1D14D69537
DESKTOP-OC9QAC3 b3fb34b5fd0846b293f65cad184164cf	AF0AE85AE7927B5D	NT AUTHORITY\SYSTEM	9B0AE85AE7927B5D
WIN-V7M7UC1SN80 ed2d8caa85e9433ebff4958bdbbcdab8	FA151C1D14D69537	WIN-V7M7UC1SN80\Administrator	MobaXterm_Personal_24.… F9151C1D14D69537
WIN-V7M7UC1SN80 ed2d8caa85e9433ebff4958bdbbcdab8	C7111C1D14D69537	WIN-V7M7UC1SN80\Administrator	winrar-x64-701 (2).exe C6111C1D14D69537



4 results found from Sep 9, 2024 11:58:18 to Sep 10, 2024 11:58:18

Source Process Command Line	Source Process Image path
"C:\Users\ADMINI~1\AppData\Local\Temp\2\7zO0F50817E\MobaXterm_Personal_24.2.exe"	C:\Users\Administrator\AppData\Local\Temp\2\
"C:\Users\Administrator\Downloads\MobaXterm_Portable_v24.2\MobaXterm_Personal_24.2.exe"	C:\Users\Administrator\Downloads\MobaXterm_F
"C:\Users\Administrator\Downloads\winrar-x64-701 (2).exe"	C:\Users\Administrator\Downloads\winrar-x64-

Real-World Integration

End-to-End Use Case

Financial organization protecting against fraud

1. AI model detects unusual login behavior
2. XAI explains decision
3. Federated learning updates model across partner banks
4. ACP triggers auto-blocking protocol

Challenges and Limitations

- Data quality and labeling issues
- Model bias and adversarial vulnerability
- Explainability and compliance
- Integration complexity

RECOMMENDATIONS

01

Combine AI with human expertise

02

Focus on model transparency (XAI)

03

Continuously monitor for adversarial attacks

04

Use synthetic data where needed

05

Ensure compliance and ethical AI practices

THANK YOU!

☎ +234 70 1470 2005

✉ hello@cyberplural.com

🌐 www.cyberplural.com