Building A Sawmill: Processing Logs With Security Onion

Matt Gracie
BsidesPGH
2024

Who Am I And What Am I Talking About?

Log Types in an Enterprise

- Windows
- Linux
- Mac OS
- Network Devices
- Cloud Services
- Endpoint Agents

Log Gathering Techniques

- Endpoints – Local Elastic Agent installation
- Network Devices – Syslog Ingestion
- Cloud Services – API Retrieval

What Is Security Onion?

"Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection honeypots, log management, and case management."

Source: https://docs.securityonion.net/en/2.4/about.html

The Components Of Security Onion

Management

- Web Interface
- Configuration

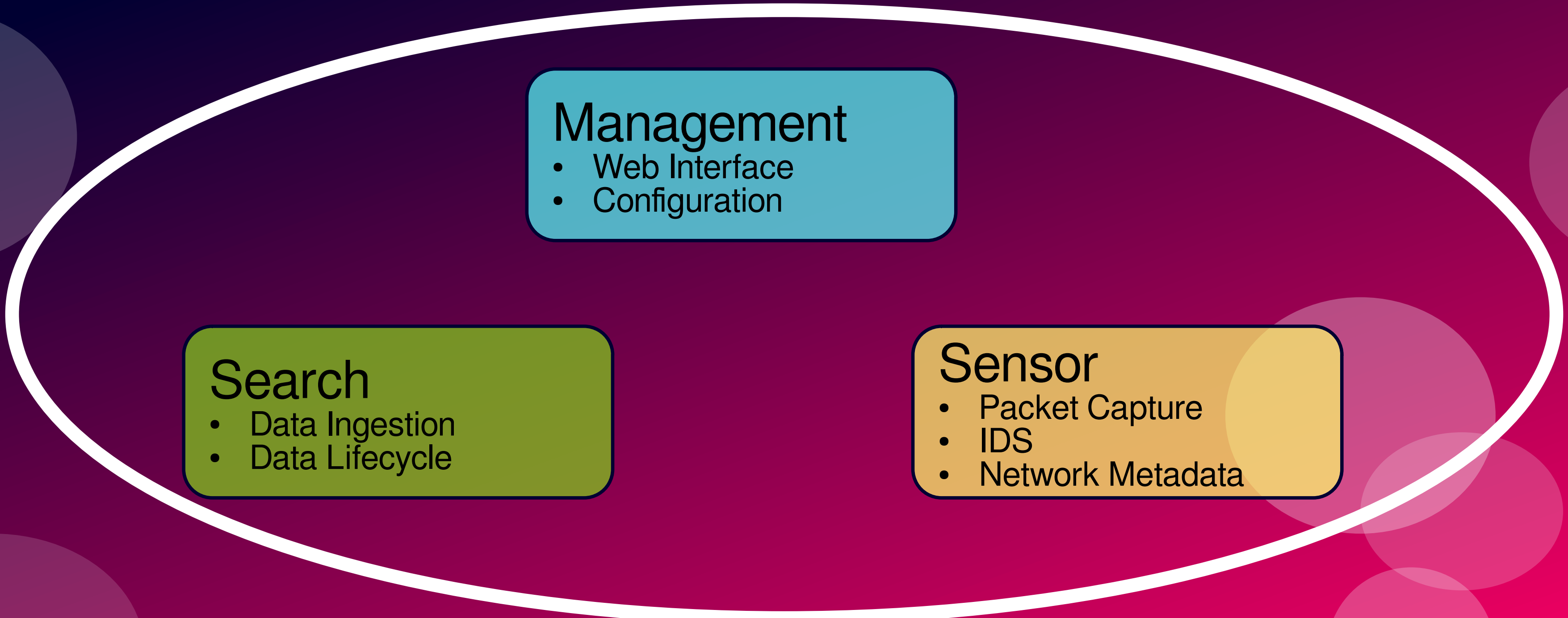
Search

- Data Ingestion
- Data Lifecycle

Sensor

- Packet Capture
- IDS
- Network Metadata

The Components Of Security Onion



Management

- Web Interface
- Configuration

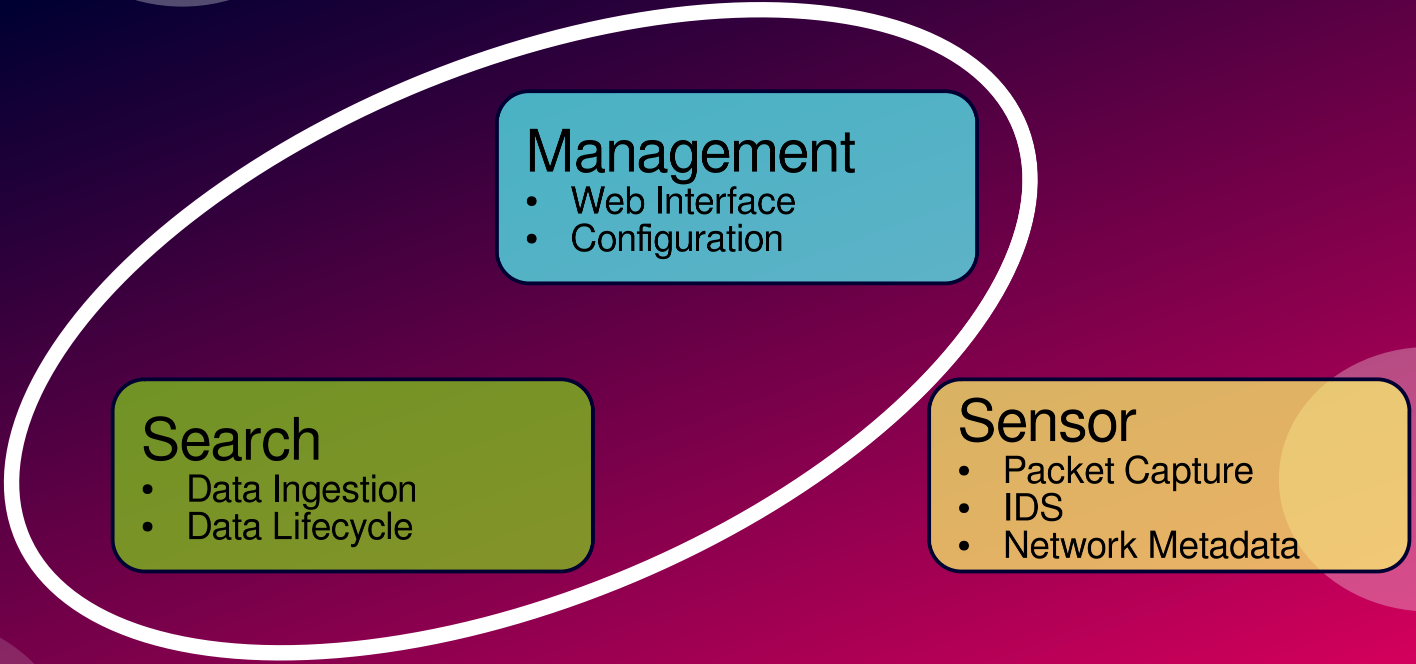
Search

- Data Ingestion
- Data Lifecycle

Sensor

- Packet Capture
- IDS
- Network Metadata

The Components Of Security Onion



Management

- Web Interface
- Configuration

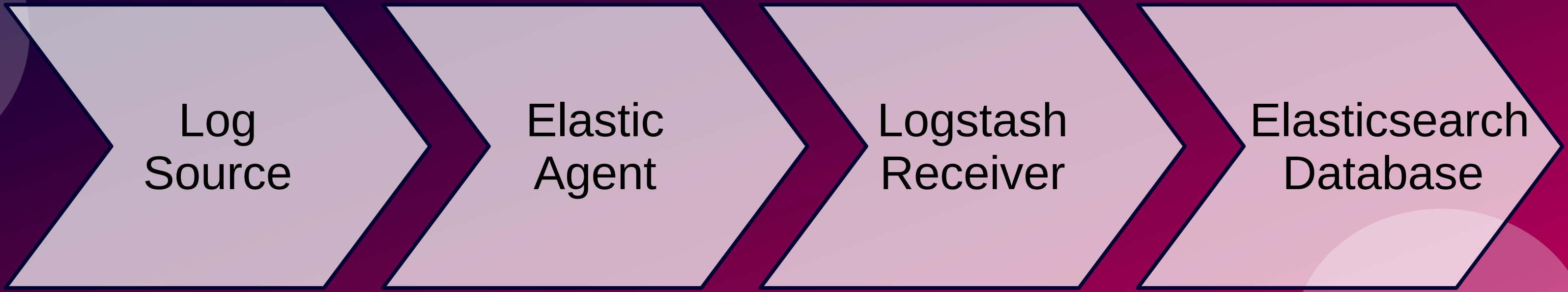
Search

- Data Ingestion
- Data Lifecycle

Sensor

- Packet Capture
- IDS
- Network Metadata

Ingestion Flow



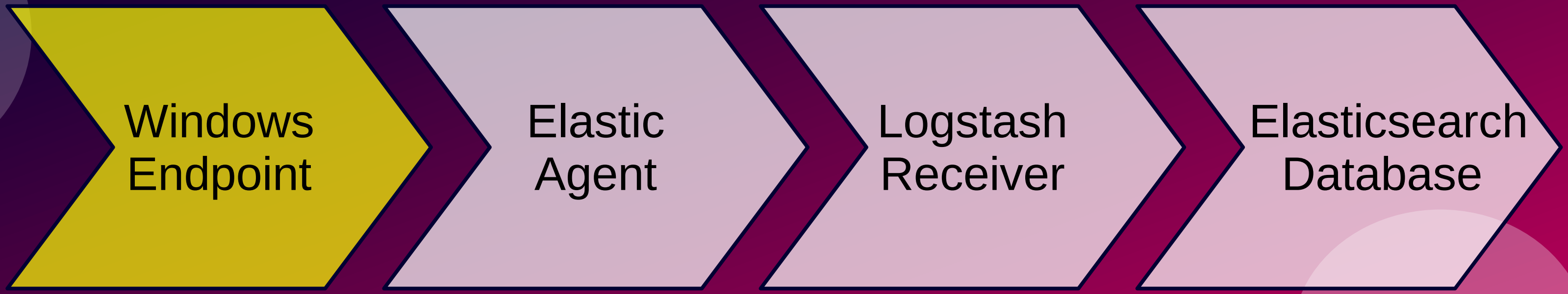
Log Source

Elastic Agent

Logstash Receiver

Elasticsearch Database

Ingestion Flow



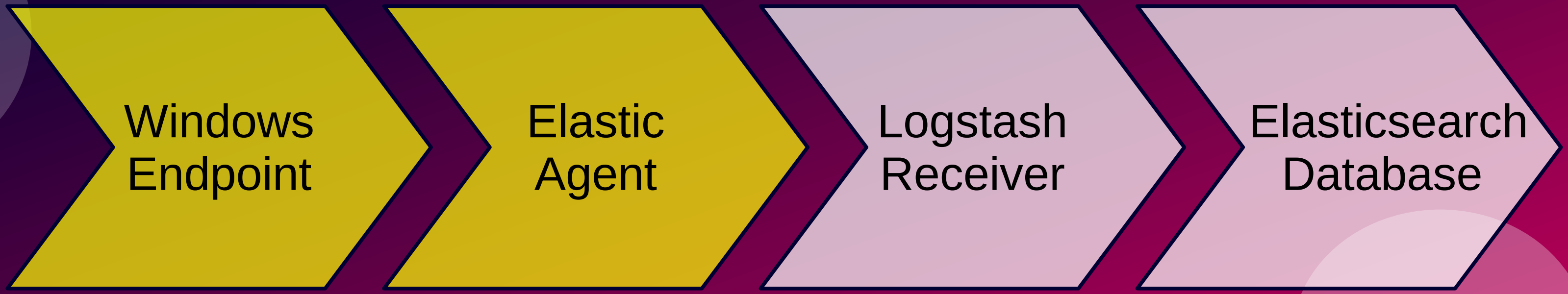
Windows Endpoint

Elastic Agent

Logstash Receiver

Elasticsearch Database

Ingestion Flow



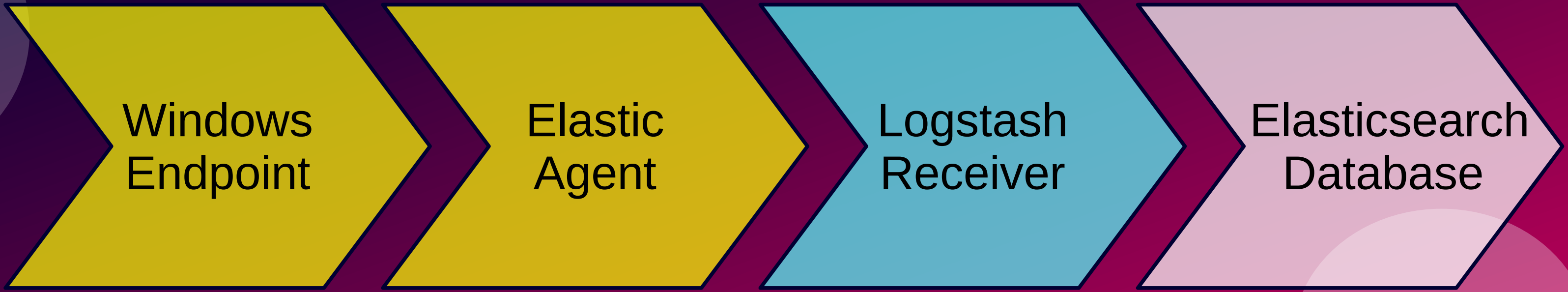
Windows Endpoint

Elastic Agent

Logstash Receiver

Elasticsearch Database

Ingestion Flow



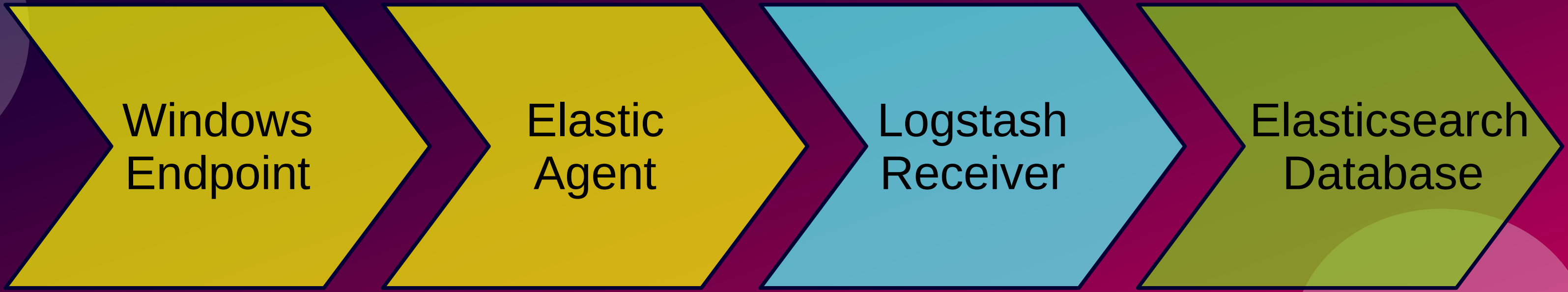
Windows Endpoint

Elastic Agent

Logstash Receiver

Elasticsearch Database

Ingestion Flow



Windows Endpoint

Elastic Agent

Logstash Receiver

Elasticsearch Database

Elastic Common Schema

“The Elastic Common Schema (ECS) is an open source specification, developed with support from the Elastic user community. ECS defines a common set of fields to be used when storing event data in Elasticsearch, such as logs and metrics...

...the goal of ECS is to enable and encourage users of Elasticsearch to normalize their event data, so that they can better analyze, visualize, and correlate the data represented in their events.”

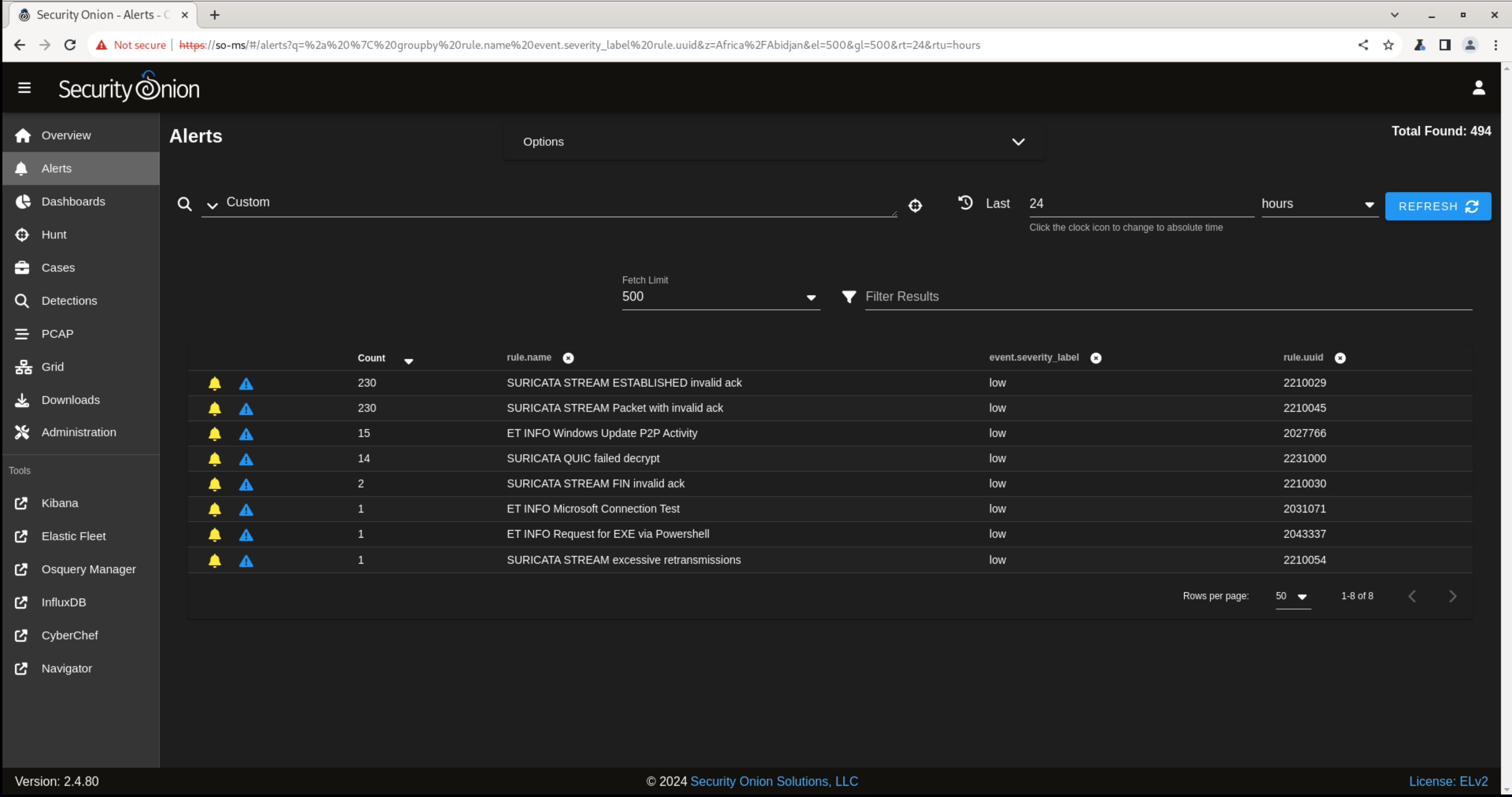
Source: https://www.elastic.co/guide/en/ecs/current/ecs-reference.html

Community ID

“When processing flow data from a variety of monitoring applications (such as Zeek and Suricata), it's often desirable to pivot quickly from one dataset to another. While the required flow tuple information is usually present in the datasets, the details of such "joins" can be tedious, particular in corner cases. This spec describes "Community ID" flow hashing, standardizing the production of a string identifier representing a given network flow, to reduce the pivot to a simple string comparison.”

Source: https://github.com/corelight/community-id-spec

So I’ve Ingested The Logs – Now What?



https://so-ms/#/alerts?q=%2a%20%7C%20groupby%20rule.name%20event.severity_label%20rule.uuid&z=Africa%2FAbidjan&el=500&gl=500&rt=24&rtu=hours

Alerts

Total Found: 494

Custom

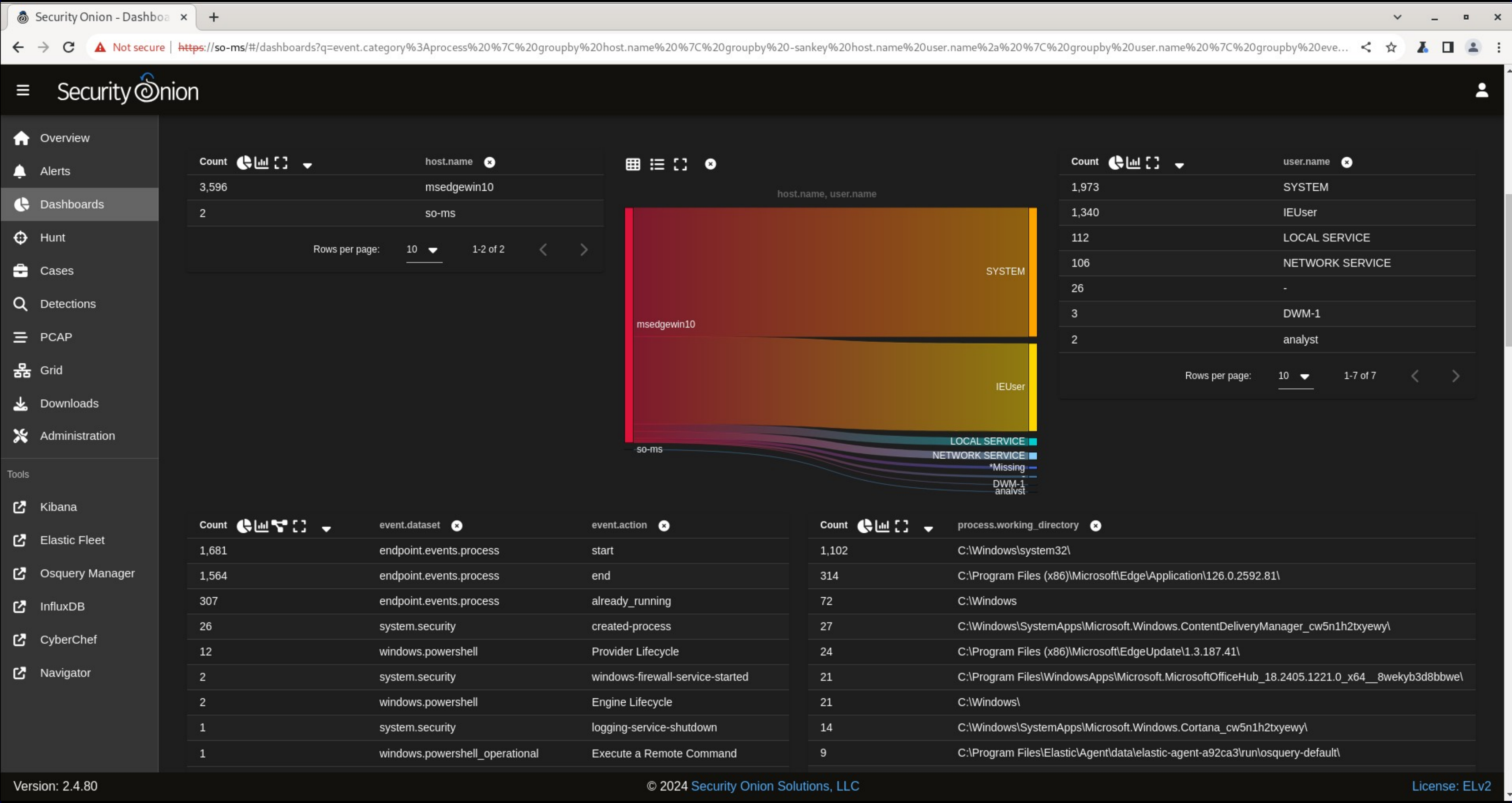
Last 24 hours

Click the clock icon to change to absolute time

Fetch Limit 500

Count	rule.name	event.severity_label	rule.uuid
230	SURICATA STREAM ESTABLISHED invalid ack	low	2210029
230	SURICATA STREAM Packet with invalid ack	low	2210045
15	ET INFO Windows Update P2P Activity	low	2027766
14	SURICATA QUIC failed decrypt	low	2231000
2	SURICATA STREAM FIN invalid ack	low	2210030
1	ET INFO Microsoft Connection Test	low	2031071
1	ET INFO Request for EXE via Powershell	low	2043337
1	SURICATA STREAM excessive retransmissions	low	2210054

Rows per page: 50 1-8 of 8



Security Onion - Dashboa
Not secure
https://so-ms/#/dashboards?q=event.category%3Aprocess%20%7C%20groupby%20host.name%20%7C%20groupby%20-sankey%20host.name%20user.name%2a%20%7C%20groupby%20user.name%20%7C%20groupby%20eve...
Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
Detections
PCAP
Grid
Downloads
Administration
Tools
Kibana
Elastic Fleet
Osquery Manager
InfluxDB
CyberChef
Navigator

Count	host.name
3,596	msedgewin10
2	so-ms

Rows per page: 10 1-2 of 2

host.name, user.name

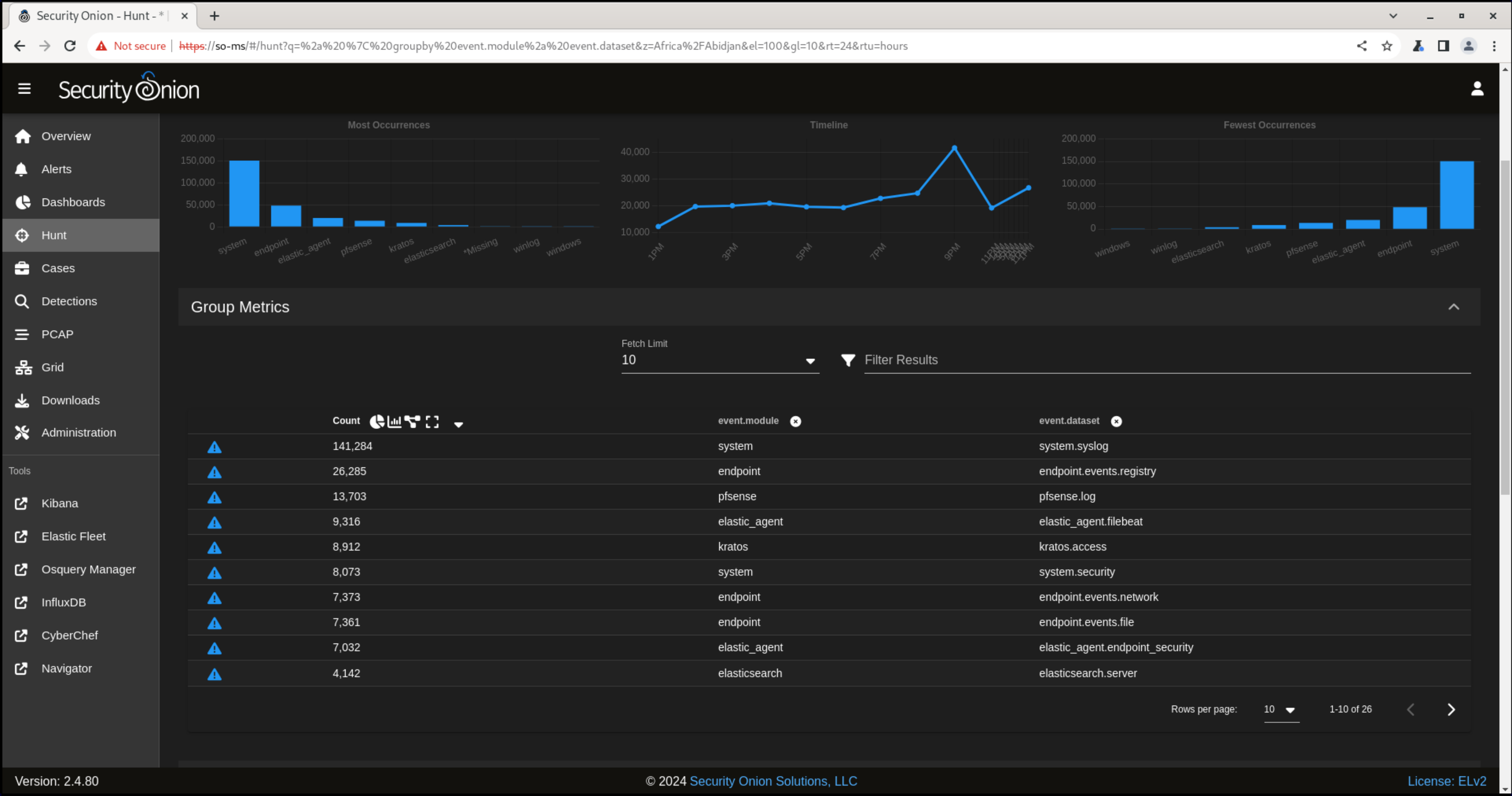
Count	user.name
1,973	SYSTEM
1,340	IEUser
112	LOCAL SERVICE
106	NETWORK SERVICE
26	-
3	DWM-1
2	analyst

Rows per page: 10 1-7 of 7

Count	event.dataset	event.action
1,681	endpoint.events.process	start
1,564	endpoint.events.process	end
307	endpoint.events.process	already_running
26	system.security	created-process
12	windows.powershell	Provider Lifecycle
2	system.security	windows-firewall-service-started
2	windows.powershell	Engine Lifecycle
1	system.security	logging-service-shutdown
1	windows.powershell_operational	Execute a Remote Command

Count	process.working_directory
1,102	C:\Windows\system32\
314	C:\Program Files (x86)\Microsoft\Edge\Application\126.0.2592.81\
72	C:\Windows
27	C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\
24	C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.187.41\
21	C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2405.1221.0_x64__8wekyb3d8bbwe\
21	C:\Windows\
14	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\
9	C:\Program Files\Elastic\Agent\data\elastic-agent-a92ca3\run\osquery-default\

Version: 2.4.80 © 2024 Security Onion Solutions, LLC License: ELv2



Group Metrics

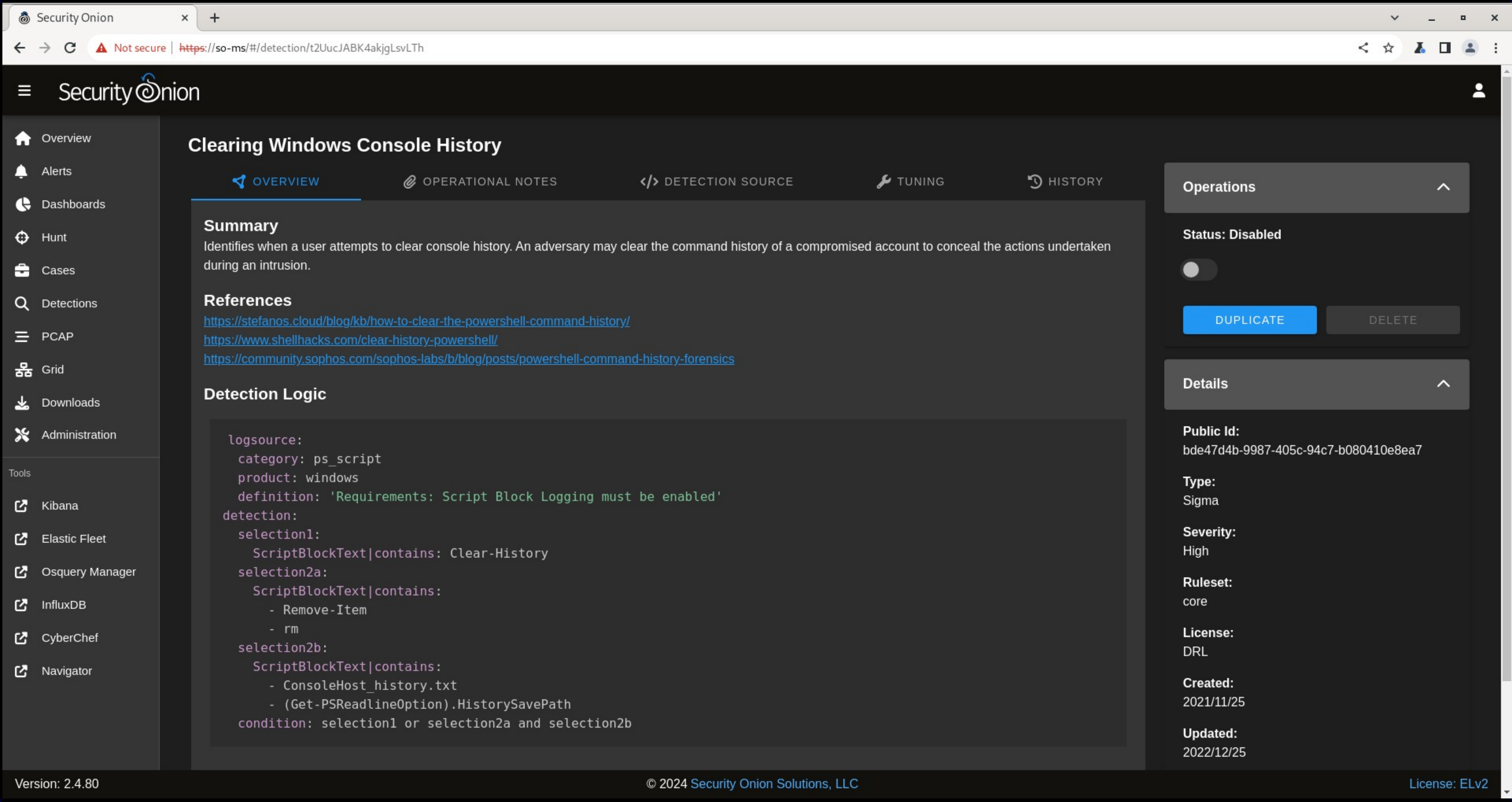
Fetch Limit
10

Filter Results

	Count	event.module	event.dataset
⚠	141,284	system	system.syslog
⚠	26,285	endpoint	endpoint.events.registry
⚠	13,703	pfsense	pfsense.log
⚠	9,316	elastic_agent	elastic_agent.filebeat
⚠	8,912	kratos	kratos.access
⚠	8,073	system	system.security
⚠	7,373	endpoint	endpoint.events.network
⚠	7,361	endpoint	endpoint.events.file
⚠	7,032	elastic_agent	elastic_agent.endpoint_security
⚠	4,142	elasticsearch	elasticsearch.server

Rows per page: 10 1-10 of 26

Version: 2.4.80 © 2024 Security Onion Solutions, LLC License: ELv2



Clearing Windows Console History

Summary

Identifies when a user attempts to clear console history. An adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion.

References

https://stefanos.cloud/blog/kb/how-to-clear-the-powershell-command-history/
https://www.shellhacks.com/clear-history-powershell/
https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics

Detection Logic

```
 logsource:
  category: ps_script
  product: windows
  definition: 'Requirements: Script Block Logging must be enabled'
detection:
  selection1:
    ScriptBlockText|contains: Clear-History
  selection2a:
    ScriptBlockText|contains:
      - Remove-Item
      - rm
  selection2b:
    ScriptBlockText|contains:
      - ConsoleHost_history.txt
      - (Get-PSReadlineOption).HistorySavePath
  condition: selection1 or selection2a and selection2b
```

Status: Disabled

Public Id:
bde47d4b-9987-405c-94c7-b080410e8ea7

Type:
Sigma

Severity:
High

Ruleset:
core

License:
DRL

Created:
2021/11/25

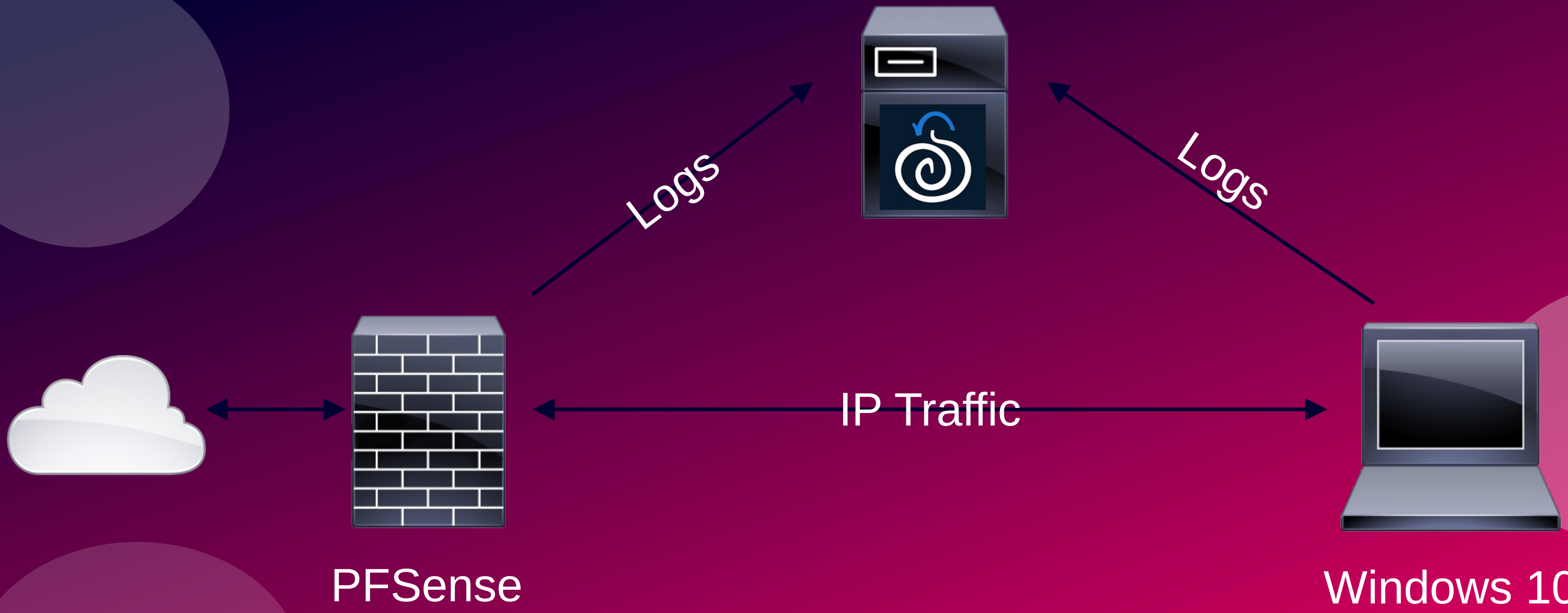
Updated:
2022/12/25

Version: 2.4.80

© 2024 Security Onion Solutions, LLC

License: ELv2

Demonstration



Conclusion

While people think of Security Onion primarily as a network monitoring solution, it’s also a very capable log management platform that can ingest the logs you’re already producing in your environment and make them available for analysis and alerting.

Questions?

@InfosecGoon

https://www.github.com/infosecgoon

infosecgoon@roadflares.org