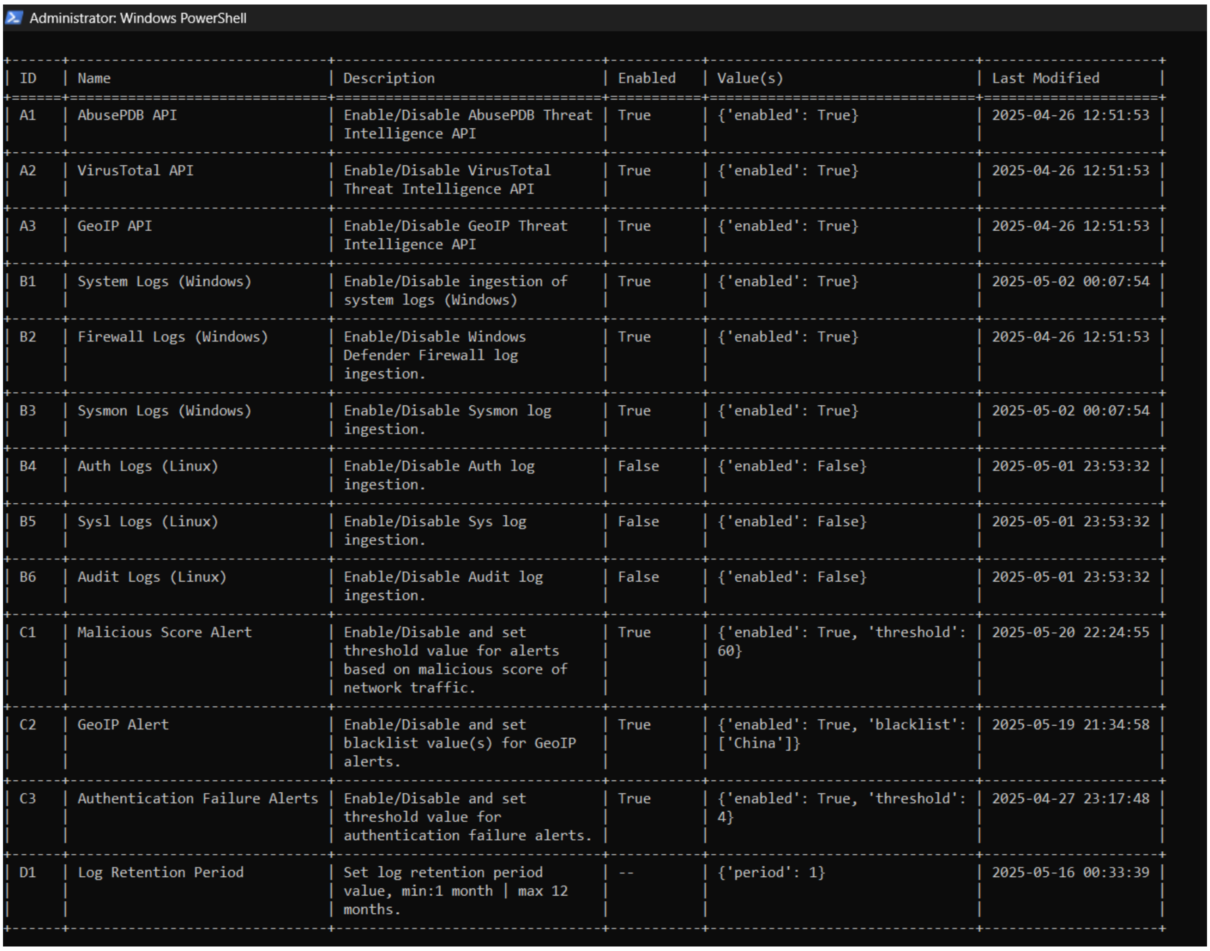
Blue Sentinel

Security Information and Event Management (SIEM)

Documentation

Features

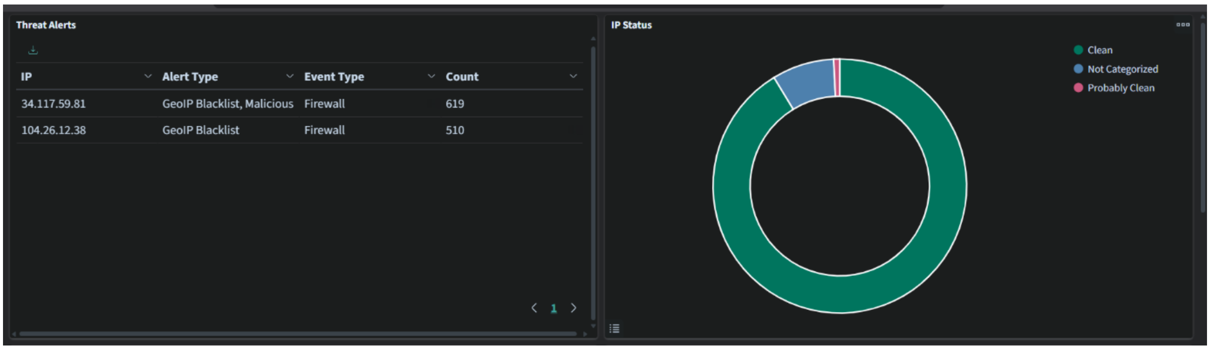
- A Security Information and Event Management System with Threat Intelligence detection and alerting.
- Event sources include: Windows System logs, Windows Defender Firewall logs and Sysmon logs.
- Technologies Used:
  - Python – Log extraction, parsing and ingestion pipeline + Threat Intelligence backend engine.
  - OpenSearch – Log database for indexing and querying
  - OpenSearch Dashboards – To provide visual insights into event's data.
- Logs from multiple sources are normalized to ECS format for easier detection and compatibility with OpenSearch (reference used: https://www.elastic.co/docs/reference/ecs/ecs-field-reference)
- Backend Config:
  - Python backend allows config editing for custom triggers like malicious alert score limit, Geo-IP blacklisting of cities, regions or countries and authentication failure alerts.
  - Config can also be modified to enable\disable threat intel API's further giving more control for customizing detection rules.
  - A screenshot of the config menu is shown below:



```
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| ID   | Name                          | Description                    | Enabled   | Value(s)                       | Last Modified       |
+======+===============================+================================+===========+================================+=====================+
| A1   | AbusePDB API                  | Enable/Disable AbusePDB Threat | True      | {'enabled': True}              | 2025-04-26 12:51:53 |
|      |                               | Intelligence API               |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| A2   | VirusTotal API                | Enable/Disable VirusTotal      | True      | {'enabled': True}              | 2025-04-26 12:51:53 |
|      |                               | Threat Intelligence API        |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| A3   | GeoIP API                     | Enable/Disable GeoIP Threat    | True      | {'enabled': True}              | 2025-04-26 12:51:53 |
|      |                               | Intelligence API               |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B1   | System Logs (Windows)         | Enable/Disable ingestion of    | True      | {'enabled': True}              | 2025-05-02 00:07:54 |
|      |                               | system logs (Windows)          |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B2   | Firewall Logs (Windows)       | Enable/Disable Windows         | True      | {'enabled': True}              | 2025-04-26 12:51:53 |
|      |                               | Defender Firewall log          |           |                                |                     |
|      |                               | ingestion.                     |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B3   | Sysmon Logs (Windows)         | Enable/Disable Sysmon log      | True      | {'enabled': True}              | 2025-05-02 00:07:54 |
|      |                               | ingestion.                     |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B4   | Auth Logs (Linux)             | Enable/Disable Auth log        | False     | {'enabled': False}             | 2025-05-01 23:53:32 |
|      |                               | ingestion.                     |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B5   | Sysl Logs (Linux)             | Enable/Disable Sys log         | False     | {'enabled': False}             | 2025-05-01 23:53:32 |
|      |                               | ingestion.                     |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| B6   | Audit Logs (Linux)            | Enable/Disable Audit log       | False     | {'enabled': False}             | 2025-05-01 23:53:32 |
|      |                               | ingestion.                     |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| C1   | Malicious Score Alert         | Enable/Disable and set         | True      | {'enabled': True, 'threshold': | 2025-05-20 22:24:55 |
|      |                               | threshold value for alerts     |           | 60}                            |                     |
|      |                               | based on malicious score of    |           |                                |                     |
|      |                               | network traffic.               |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| C2   | GeoIP Alert                   | Enable/Disable and set         | True      | {'enabled': True, 'blacklist': | 2025-05-19 21:34:58 |
|      |                               | blacklist value(s) for GeoIP   |           | ['China']}                     |                     |
|      |                               | alerts.                        |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| C3   | Authentication Failure Alerts | Enable/Disable and set         | True      | {'enabled': True, 'threshold': | 2025-04-27 23:17:48 |
|      |                               | threshold value for            |           | 4}                             |                     |
|      |                               | authentication failure alerts. |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
| D1   | Log Retention Period          | Set log retention period       | --        | {'period': 1}                  | 2025-05-16 00:33:39 |
|      |                               | value, min:1 month | max 12    |           |                                |                     |
|      |                               | months.                        |           |                                |                     |
+------+-------------------------------+--------------------------------+-----------+--------------------------------+---------------------+
```

- Threat Intelligence Enrichment
  - Windows Firewall logs are enriched with threat intel data from AbusePDB, Virus Total and IPInfo APIs for malicious score rating, IP reputation and TOR detection.
  - Tracing IP to its City, Region and Country based locations and finally enabling custom thresholds for malicious score alerts and custom blacklisting for Geo-IP tracking alerts.
- Dashboards (OpenSearch Dashboards)
  - Summarized into 8 visualizations for deep insights into system and network events of the host.
  - Threat Alerts: A table displaying the details of events which triggered alerts.
  - IP Status: A pie chart showing IP enrichment status categorized into Clean, Probably Clean, Suspicious, Dangerous and Not Categorized based on the malicious score.

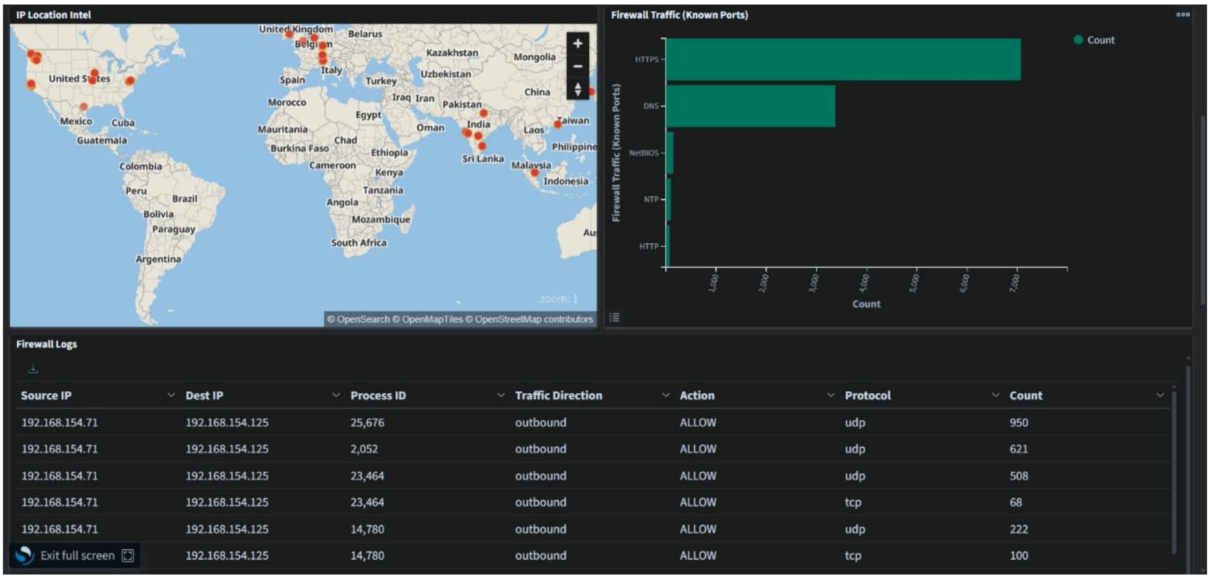
- IP Location Intel: A world map with IP locations marked to track the incoming traffic locations.
- Firewall Traffic (Known Ports): A bar chart which maps the network events traffic into know services to provide better insights into network activity.
- Firewall Logs: A table displaying the recent firewall logs summarized to include only necessary fields.
- Event Category: A bar chart mapping events to specific category based on its Event-ID.
- Event Types: A pie chart splitting events into slices based on its event type, which is derived based on its Event-ID.
- Event Logs: A table displaying recent events.
- This dashboard can be imported to your OpenSearch dashboards by going to : Dashboard Management > Saved Objects > Import > select the “Dashboard_setup.ndjson” file.
- Shown below are the screenshots for the dashboard visualizations:



Threat Alerts

IP	Alert Type	Event Type	Count
34.117.59.81	GeoIP Blacklist, Malicious	Firewall	619
104.26.12.38	GeoIP Blacklist	Firewall	510

IP Status

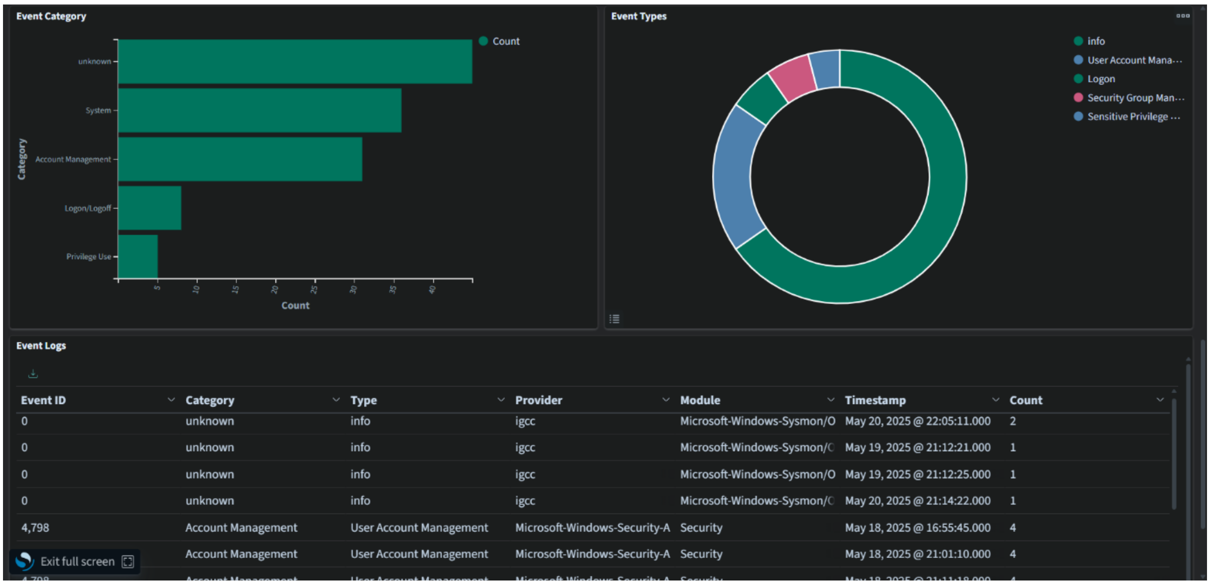


IP Location Intel

Firewall Traffic (Known Ports)

Firewall Logs

Source IP	Dest IP	Process ID	Traffic Direction	Action	Protocol	Count
192.168.154.71	192.168.154.125	25,676	outbound	ALLOW	udp	950
192.168.154.71	192.168.154.125	2,052	outbound	ALLOW	udp	621
192.168.154.71	192.168.154.125	23,464	outbound	ALLOW	udp	508
192.168.154.71	192.168.154.125	23,464	outbound	ALLOW	tcp	68
192.168.154.71	192.168.154.125	14,780	outbound	ALLOW	udp	222
	192.168.154.125	14,780	outbound	ALLOW	tcp	100



Event Logs

Event ID	Category	Type	Provider	Module	Timestamp	Count
0	unknown	info	igcc	Microsoft-Windows-Sysmon/O	May 20, 2025 @ 22:05:11.000	2
0	unknown	info	igcc	Microsoft-Windows-Sysmon/C	May 19, 2025 @ 21:12:21.000	1
0	unknown	info	igcc	Microsoft-Windows-Sysmon/O	May 19, 2025 @ 21:12:25.000	1
0	unknown	info	igcc	Microsoft-Windows-Sysmon/C	May 20, 2025 @ 21:14:22.000	1
4,798	Account Management	User Account Management	Microsoft-Windows-Security-A	Security	May 18, 2025 @ 16:55:45.000	4
	Account Management	User Account Management	Microsoft-Windows-Security-A	Security	May 18, 2025 @ 21:01:10.000	4
4,798	Account Management	User Account Management	Microsoft-Windows-Security-A	Security	May 18, 2025 @ 21:11:18.000	4

Running the Blue Sentinel System (Windows System)

- Requirements
  - Docker Desktop Application
  - WSL Enabled System
  - SysInternals-Suite
- Install OpenSearch & OpenSearch Dashboards
  - Open “docker-compose.yml” file from the script directory with a text editor.
  - Change “[YOUR-PASSWORD-HERE]” with a strong password of your choice.
  - Open PowerShell as administrator, change directory to the folder where “.yml” file is stored and run “docker compose up -d”.
  - This will download OpenSearch & OpenSearch Dashboards Docker images onto your system, create & run the containers.
  - Note: “docker compose down” can be used to stop the container.
- Initial set-up for Blue Sentinel backend script
  - While the OpenSearch container is running, change current directory to the location where the backend script is stored.

  - Create a python virtual environment, activate it. Then install all the dependencies from “requirements.txt” file. [use command: pip install -r requirements.txt]
  - Now run the script “sentinel_toolkit.py” and enter your OpenSearch username (“admin” by default) & password, then select option “Start Initial Set-up” to create necessary indices with required mappings.
  - This script also contains some additional options, for OpenSearch client operations.

- Enabling Log Sources
  - Windows Firewall:
    - Open Windows Defender Firewall with Advanced Security (run as administrator).
    - Go to Actions > Properties > Logging
    - Select Customize > select a path for saving logs (preferably somewhere you have permission to access the files.)
    - Select “Yes” for both logging successful connections and dropped packets, click ok. (enable for Domain, Private and Public profiles.)
  - SysLog:
    - Download syslog configuration file: https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml
    - Make sure that you have SysInternals-Suite extracted and ready.
    - Go to folder where SysInternals-Suite is located, open CMD as administrator, run command: Sysmon64.exe -accepteula -i "<Path to file>\sysmonconfig-export.xml"
    - Confirm that the log is being stored by running Event Viewer as administrator, and navigate to: Application & Services > Microsoft > Windows > Sysmon > Operational (shows list of logs collected.)
- Running Blue Sentinel backend script

- Modify the files “blue_sentinel.py”, “sentinel_intel.py”, populate it with your OpenSearch username, password and API keys for AbusePDB, Virus Total and IPInfo API’s.
- Run “blue_sentinel.py” to start the backend script.
- You can start the log ingestion directly with the default configurations or make tweaks to configurations by selecting option “Edit Configurations”.