Security Onion:

Security Onion is a free and open source Linux distribution for Intrusion Detection, Threat Hunting, Security Monitoring, and Log Management. It includes third-party tools, such as Fleet, Playbook, TheHiva, Elasticsearch, Kibana, Suricata, Zeek, Wazuh, Stenographer, CyberChef, NetworkMiner, and many other security tools. It is an open source intrusion detection system (IDS) plus, Enterprise Security monitoring Plus, Log management solution, all-in-one package. It offers full packet capture, both network-based and host-based intrusion detection systems NIDS and HIDS, respectively, but also includes powerful indexing, search, visualization and analysis tools to make sense of those mountains of data.

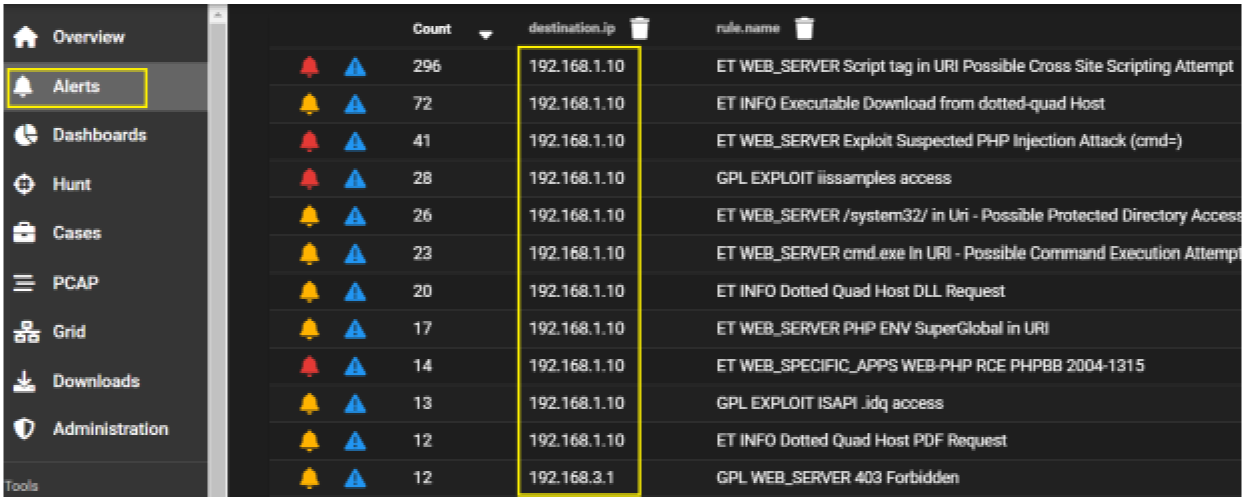
In order to enable Security Onion to monitor your network, you will need to setup either port mirroring or a basic network tap that will feed your network traffic into Security Onion.

Security Onion
SOLUTIONS

Once you have installed and configured Security Onion, you will gain access to the Security Onion Console (SOC). Upon opening the SOC, you will notice a number of menu items on the left-hand side. The upper section includes the tools which are native to Security Onion: Alerts, Hunt, PCAP, and Grid. Found in the lower section are other third-party tools which are integrated into Security Onion: Kibana, Grafana, CyberChef, Playbook, FleetDM, TheHive, and Navigator.

Alert:

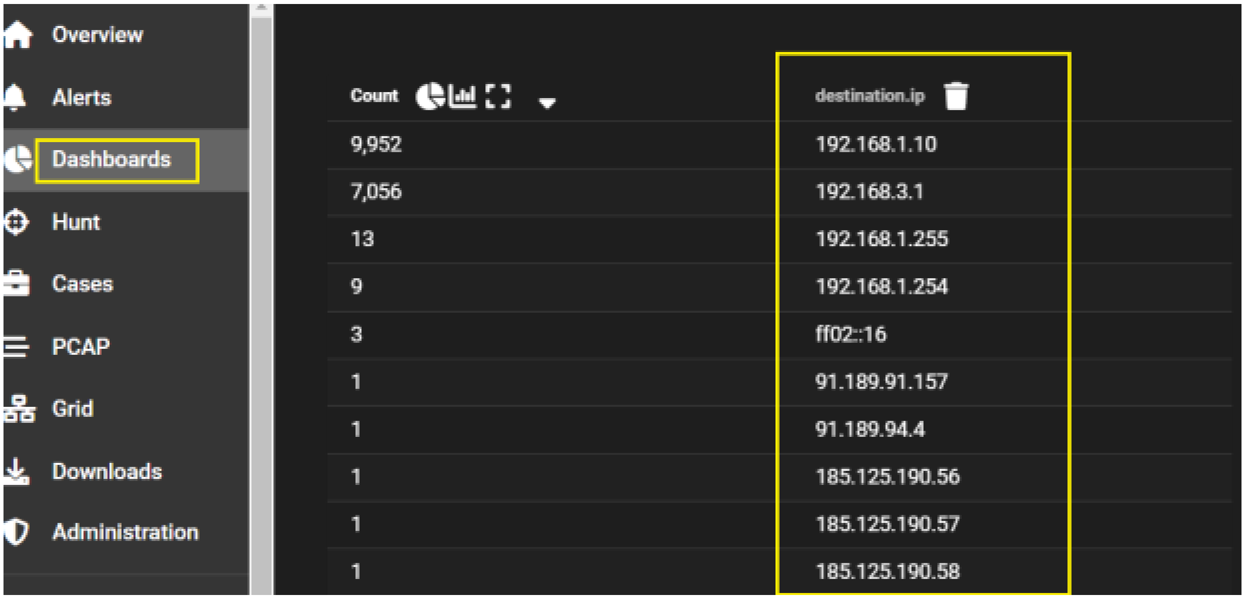
Security Onion Console (SOC) gives you access to our Alerts interface. This interface gives you an overview of the alerts that Security Onion is generating and allows you to quickly drill down into details. Alerts tab provides a centralized location for all alerts generated by Suricata or OSSEC, two open-source threat detection engines. Alerts tab allows you to sort, acknowledge, or escalate alerts should you choose to do so.



		Count	destination.ip	rule.name
🔔	⚠	296	192.168.1.10	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
🔔	⚠	72	192.168.1.10	ET INFO Executable Download from dotted-quad Host
🔔	⚠	41	192.168.1.10	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)
🔔	⚠	28	192.168.1.10	GPL EXPLOIT iissamples access
🔔	⚠	26	192.168.1.10	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access
🔔	⚠	23	192.168.1.10	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt
🔔	⚠	20	192.168.1.10	ET INFO Dotted Quad Host DLL Request
🔔	⚠	17	192.168.1.10	ET WEB_SERVER PHP ENV SuperGlobal in URI
🔔	⚠	14	192.168.1.10	ET WEB_SPECIFIC_APPS WEB-PHP RCE PHPBB 2004-1315
🔔	⚠	13	192.168.1.10	GPL EXPLOIT ISAPI .idq access
🔔	⚠	12	192.168.1.10	ET INFO Dotted Quad Host PDF Request
🔔	⚠	12	192.168.3.1	GPL WEB_SERVER 403 Forbidden

Dashboards:

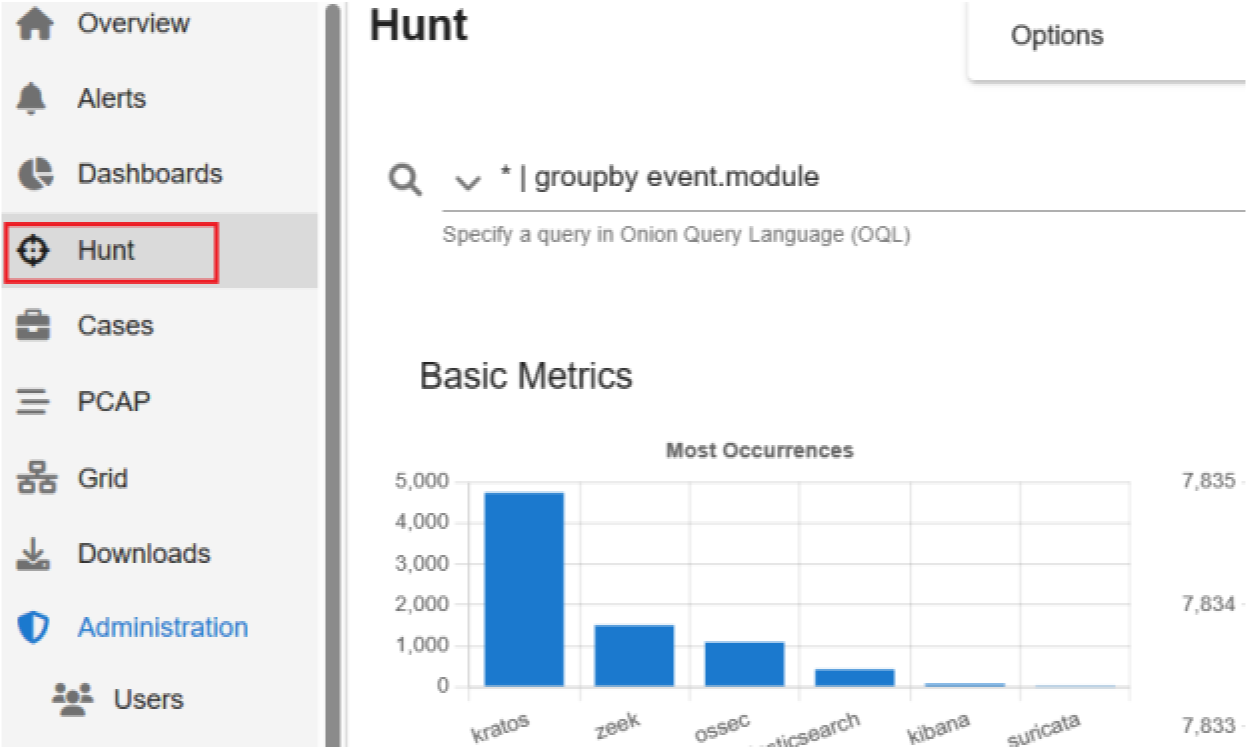
Security Onion Console (SOC) has its own Dashboards interface. This interface includes an entire set of pre-built dashboards for our standard data types. The dashboard, which shares data about the network and security status. This will visually show the analyst what events are trending within the network and traffic going through the firewall.



Count	destination.ip
9,952	192.168.1.10
7,056	192.168.3.1
13	192.168.1.255
9	192.168.1.254
3	ff02::16
1	91.189.91.157
1	91.189.94.4
1	185.125.190.56
1	185.125.190.57
1	185.125.190.58

Hunt:

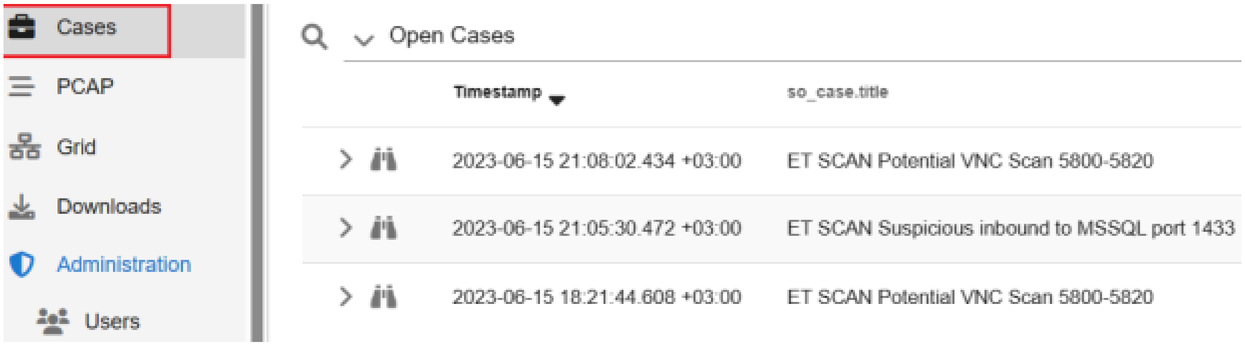
Hunt is similar to our Dashboards interface but is tuned more for threat hunting. The main difference between Hunt and Dashboards is that Hunt's default queries are more focused than the overview queries in Dashboards. Also, most of the default Dashboards queries display a separate table for each aggregated field, whereas many of the default queries in Hunt aggregate multiple fields in a single table which can be beneficial when hunting for more obscure activity. The purpose of the hunting tab is to effectively identify threats within the event.



```
* | groupby event.module
```

Cases:

Security Onion includes its own Cases interface for case management. It allows you to escalate logs from Alerts, Dashboards, and Hunt, and then assign analysts, add comments and attachments, and track observables.



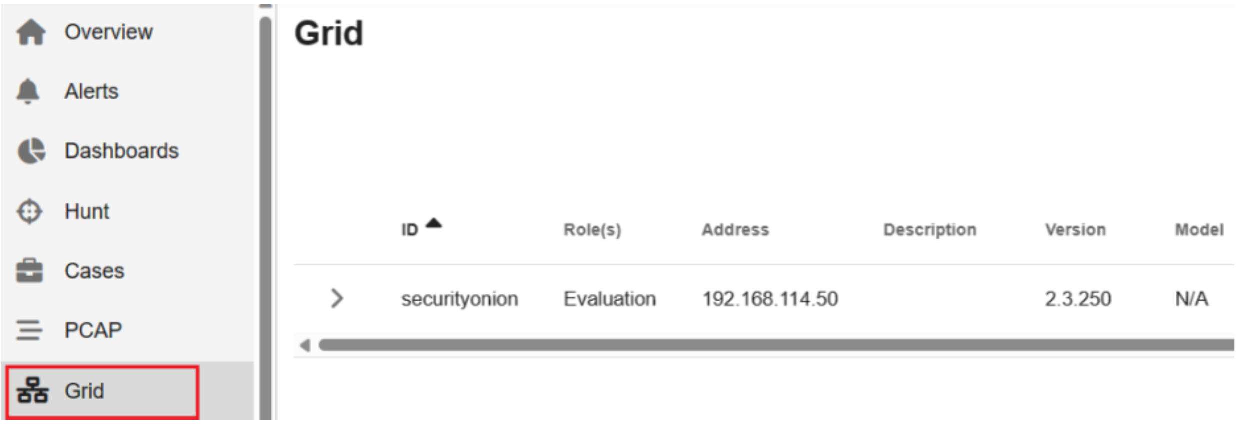
Timestamp	so_case.title
2023-06-15 21:08:02.434 +03:00	ET SCAN Potential VNC Scan 5800-5820
2023-06-15 21:05:30.472 +03:00	ET SCAN Suspicious inbound to MSSQL port 1433
2023-06-15 18:21:44.608 +03:00	ET SCAN Potential VNC Scan 5800-5820

PCAP:

Security Onion Console (SOC) gives you access to our PCAP interface. This interface allows you to access your full packet capture that was recorded by Stenographer.

Grid:

Security Onion Console (SOC) gives you access to our Grid interface. This interface allows you to quickly check the status of all nodes in your grid.

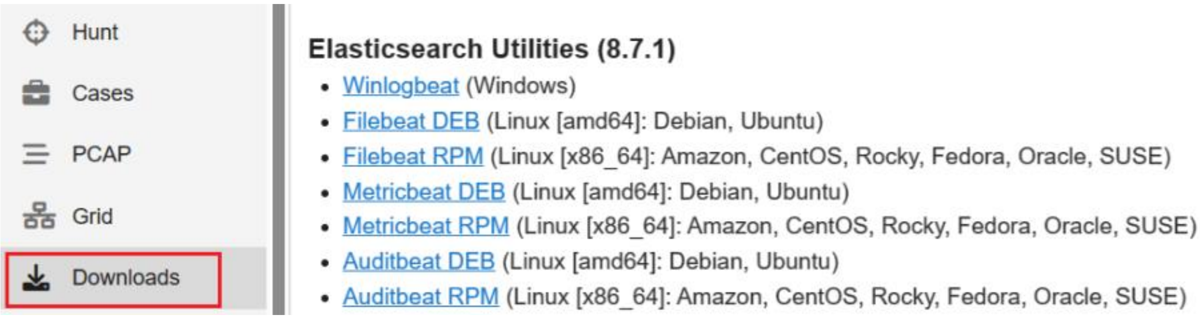


Grid

	ID ▲	Role(s)	Address	Description	Version	Model
>	securityonion	Evaluation	192.168.114.50		2.3.250	N/A

Downloads:

The Security Onion Console (SOC) Downloads page gives you access to some files that you might need to download:

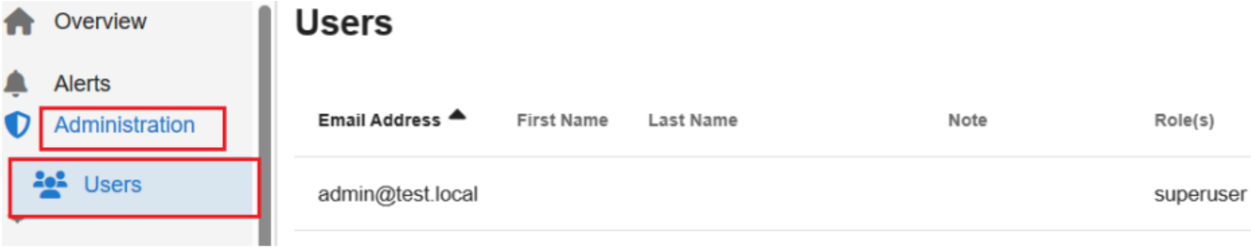


Elasticsearch Utilities (8.7.1)

- Winlogbeat (Windows)
- Filebeat DEB (Linux [amd64]: Debian, Ubuntu)
- Filebeat RPM (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- Metricbeat DEB (Linux [amd64]: Debian, Ubuntu)
- Metricbeat RPM (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)
- Auditbeat DEB (Linux [amd64]: Debian, Ubuntu)
- Auditbeat RPM (Linux [x86_64]: Amazon, CentOS, Rocky, Fedora, Oracle, SUSE)

Administration:

Security Onion Console (SOC) includes an Administration page which shows current users:

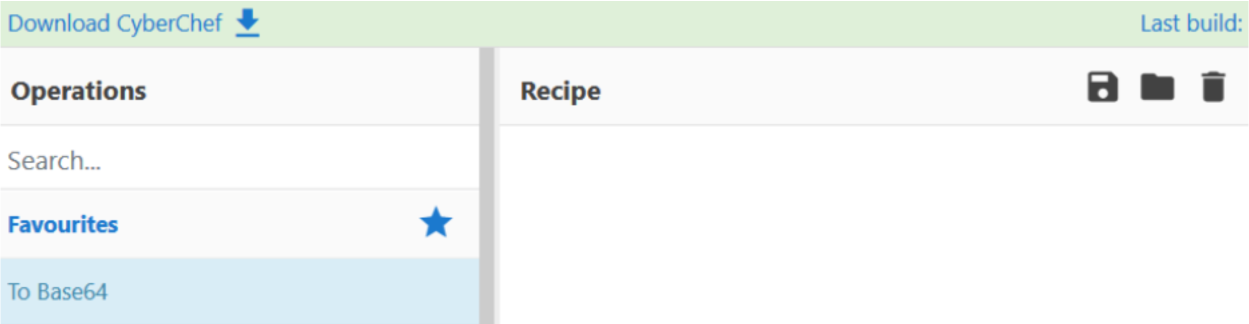


Users

Email Address	First Name	Last Name	Note	Role(s)
admin@test.local				superuser

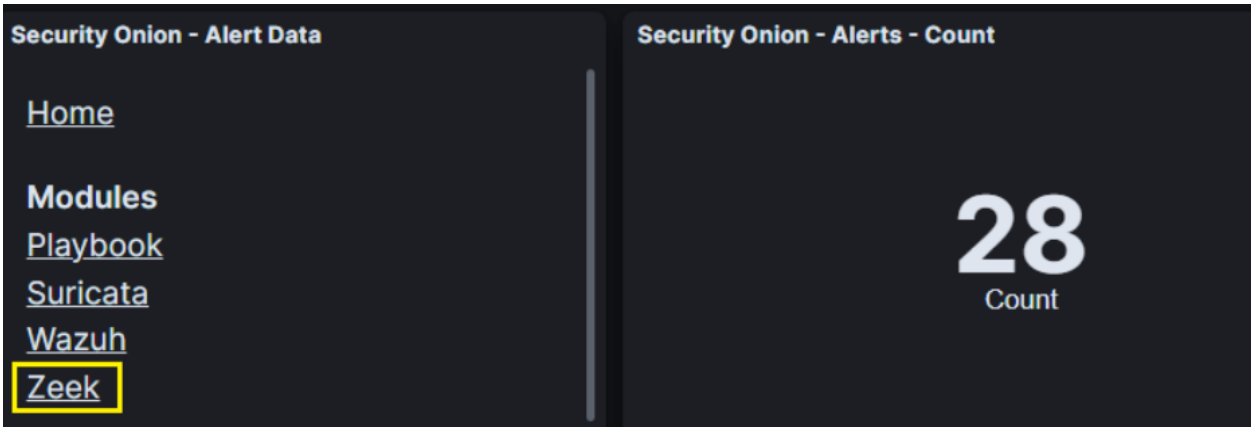
CyberChef:

This is one of the best web applications, which is around 300 operations which is quickly provide encoding, encryption, the conversation of different data, etc.



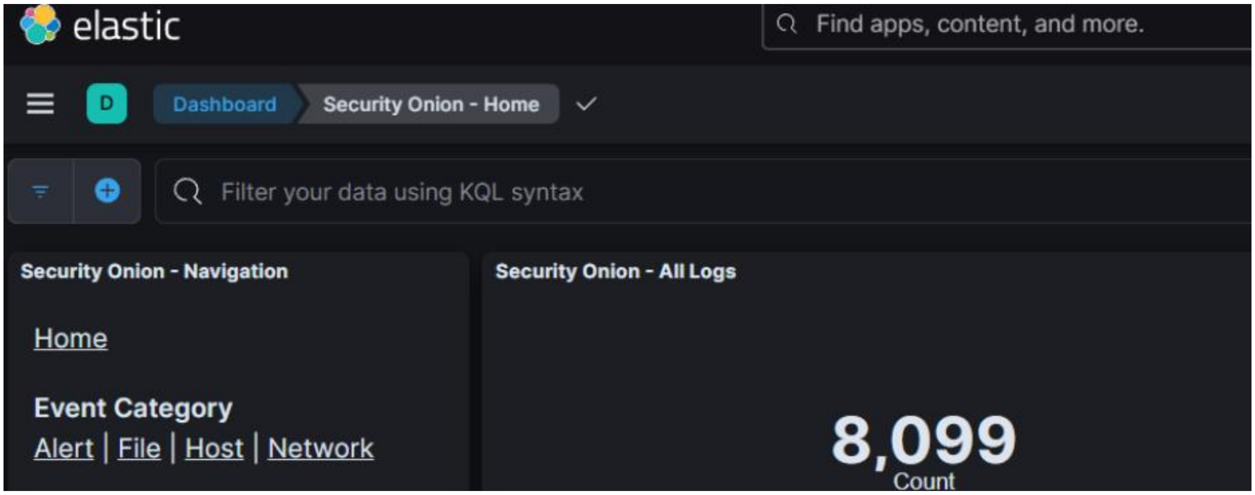
Zeek:

It has another name called Bro, and it not only an open-source platform and helps for network security monitoring. Zeek is a powerful network analysis framework. Zeek logs are sent to Elasticsearch for parsing and storage and can then be found in Dashboards, Hunt, and Kibana.



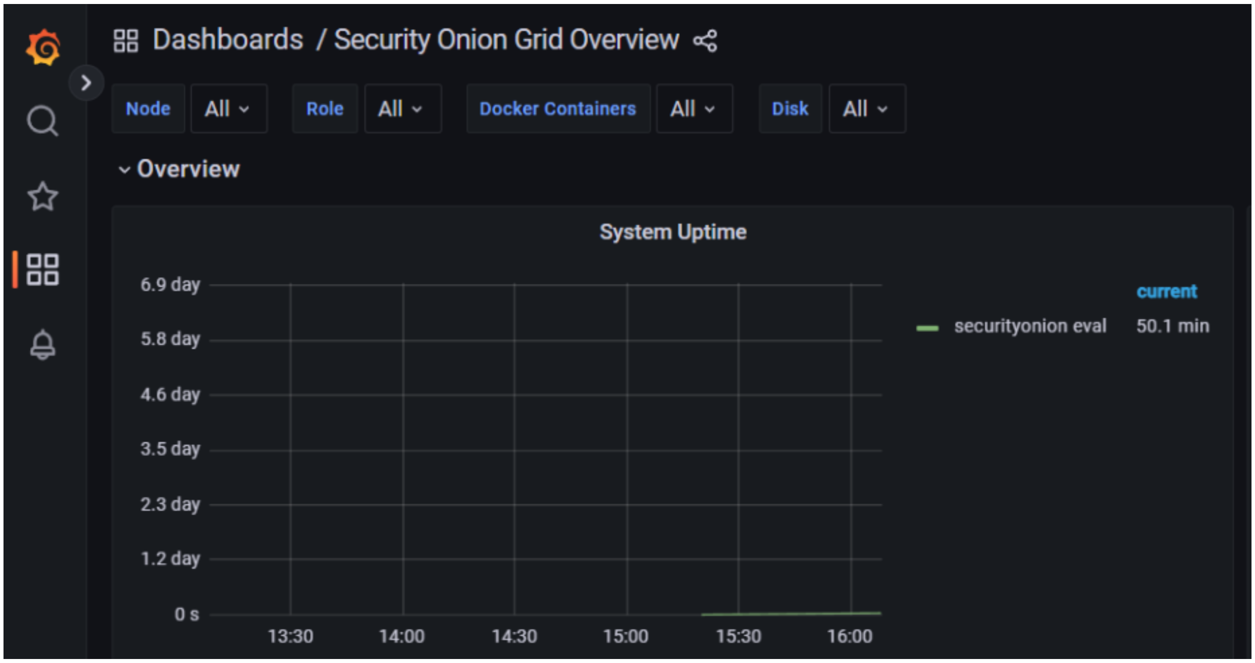
Kibana:

Kibana is a data visualization tool which allows you to analyze data generated by Elasticsearch. Kibana is a free and open user interface that lets you visualize your Elasticsearch data and navigate the Elastic Stack. you will need to log into Kibana using the same username and password that you use for Security Onion Console (SOC).


elastic
Find apps, content, and more.
D
Dashboard
Security Onion - Home
Filter your data using KQL syntax
Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Security Onion - All Logs
8,099
Count

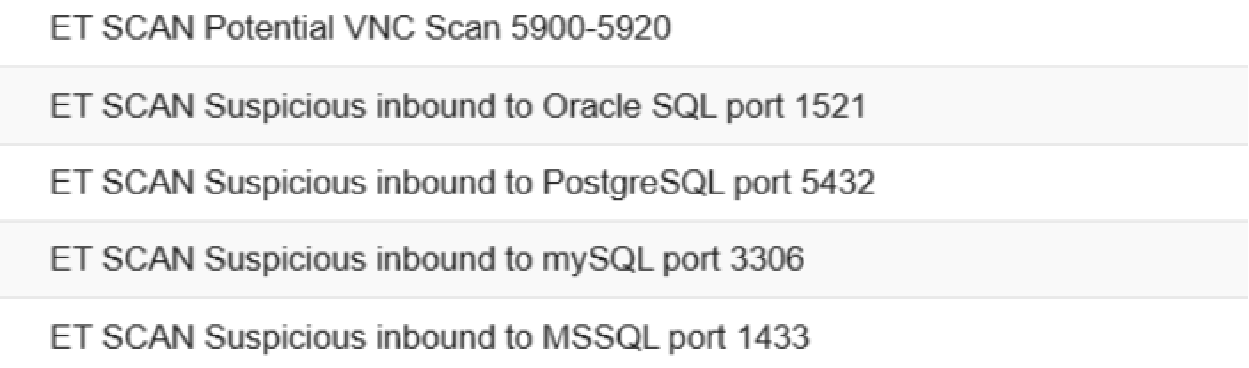
Grafana:

Once you've logged into Security Onion Console (SOC), you can then click the Grafana link to see system health information.



Suricata:

Suricata is an open-source detection engine that can act as an intrusion detection system (IDS) and an intrusion prevention system (IPS). Suricata inspects the network traffic using a powerful and extensive rules and signature language for detection of complex threats. Suricata NIDS alerts can be found in Alerts, Dashboards, Hunt, and Kibana. Suricata is a free and open source, mature, fast and robust network threat detection engine.



ET SCAN Potential VNC Scan 5900-5920

ET SCAN Suspicious inbound to Oracle SQL port 1521

ET SCAN Suspicious inbound to PostgreSQL port 5432

ET SCAN Suspicious inbound to mySQL port 3306

ET SCAN Suspicious inbound to MSSQL port 1433

Strelka:

Strelka is a real-time file scanning system used for threat hunting, threat detection, and incident response. Strelka scans files using YARA rules. If it detects a match, then it will generate an alert that can be found in Alerts, Dashboards, Hunt, or Kibana.

JUST ONE

Wazuh:

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance. Security Onion utilizes Wazuh as a Host Intrusion Detection System (HIDS) on each of the Security Onion nodes.

COUNT - 28 alerts