Tool Credentials

Tool	Credentials	Data	Location
Splunk	saved	Windows, Linux, Sysmon, Squid web proxy, and Vyatta logs	http://172.16.3.20:8000
Security Onion	onion@site.lan / Simspace1!@	Network traffic logs	http://172.16.3.49
Kibana	onion@site.lan / Simspace1!@	Zeek network parsing logs, network metadata; Windows event and Sysmon logs	http://172.16.3.49/kibana

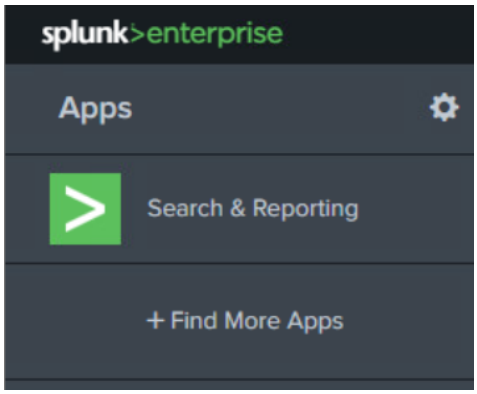
Splunk Overview

Splunk Data & Index Name

Data Source	Description	Events	Index
Suricata Alerts	Suricata IDS Alerts	IDS Alerts generated by matched strings with Suricata	‘ids’
Linux Syslog	Syslog Events	Events generated by Linux Syslog on Unix and Vyatta hosts	‘linux’
Security Onion Network Logs	Zeek/Bro Metadata parsing logs	Network protocol logs parsed by Zeek	‘onion’
Squid Web Proxy	Client web traffic logs from Squid web proxy	HTTP/HTTPS events, URLs, client address	‘proxy’
Strelka Alerts	Strelka File Extraction Info	File extraction information pulled from Zeek with Strelka	‘strelka’
Vyatta Syslog	Syslog from Vyatta Devices	Syslog from Vyatta Devices	‘vyatta’
Windows Event Logs	Forwarders are ingesting Windows logs from servers and workstations	Sysmon, Powershell, System, Security, Application	‘windows’

Utilizing Splunk Search

The Search & Reporting App is the landing page to begin threat hunting.



Commonly used modifiers:

- * – wildcard glob
- | (pipe) combine search terms or strings
- Splunk pre-built keywords (visualizations and statistics)
- Table – creates a table based on field names included
    - Ex: ‘table host, dest_ip’
- Stats – provides quick math functionality
    - Ex: ‘stats count by host’
- Uniq – deduplicate data based on field
    - Ex: ‘index=windows host=site-* | uniq’

Search Example	Description
index=* | stats count by index	List event count by index
index=windows host=site-dc	All events from domain controller *site-dc* from the *windows* index
index=wineventlog host=acc-*	All events from Windows hosts with names starting with *acc-* from the *wineventlog* index
index=* powershell	All events containing the keyword *powershell*
index=* powershell | table host	Keyword search combined with Splunk keyword visualization

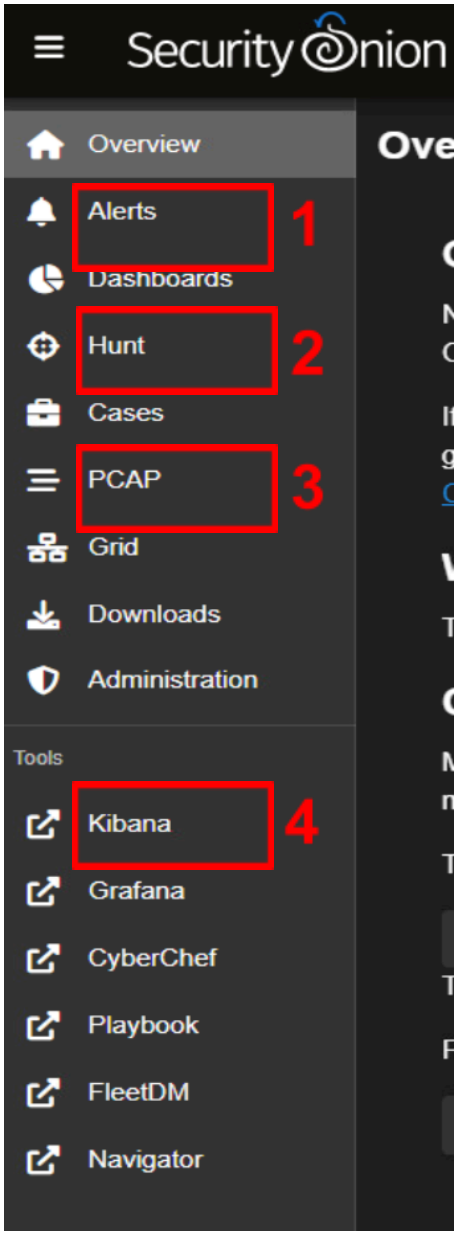
Security Onion Overview

1. Alerts – Suricata IDS alerts generated by Emerging Threats Open ruleset. Context sensitive menus can drill down into alerts and transition from IDS alerts to the alternate Hunt view.

2. Hunt – Can be used to dig through Zeek logs and IDS alerts.

3. PCAP – Can retrieve carved packet capture data for download or view within the browser. Zeek metadata logs contain a '_id' field which provides a direct link to download the associated PCAP. Session data can also be manually entered to carve packets from the PCAP page.

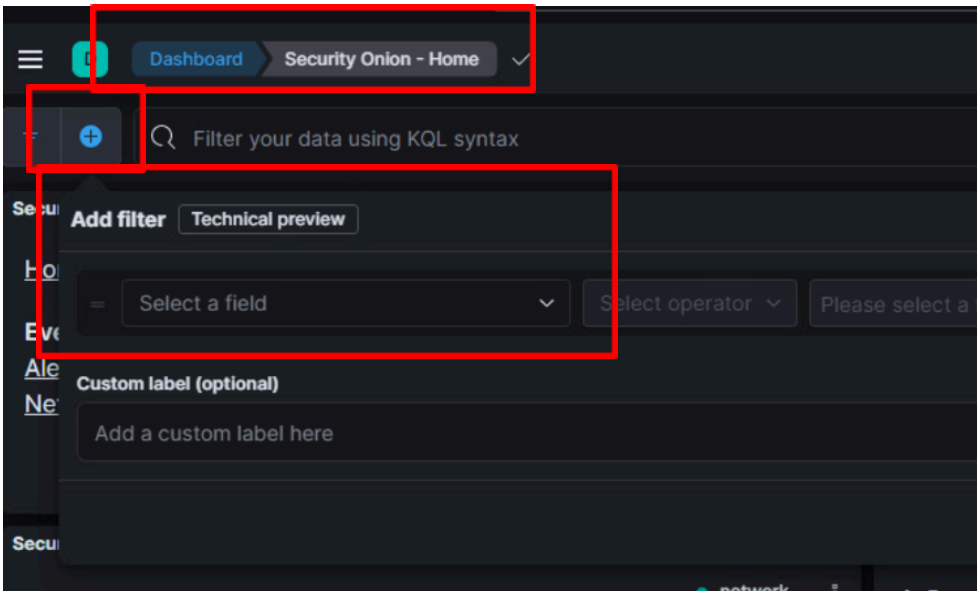
4. Kibana – Dashboards, custom views, and search interface for Zeek, IDS, Windows events and Windows Sysmon logs.



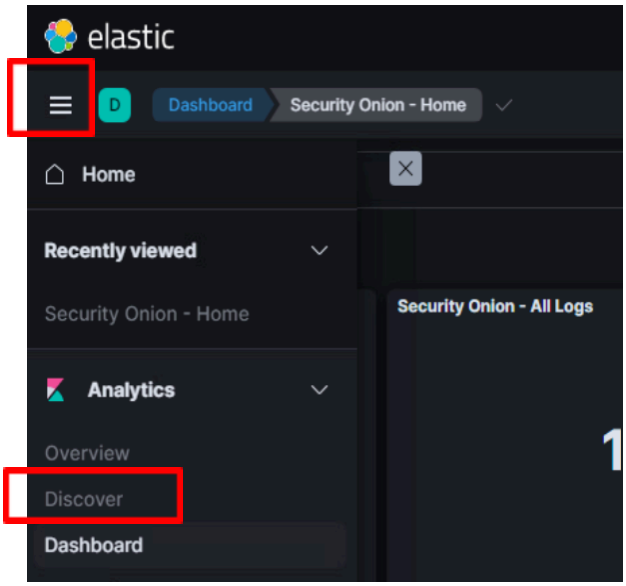
Kibana Quickstart

When accessing Kibana, “Security Onion-Home” is the first dashboard presented. This dashboard provides easy pivoting to network logs (Zeek, IDS) or host data (Windows events and Sysmon). By clicking on the plus symbol next to the search bar, field names can be as additional columns, allowing for quick viewing among multiple results.

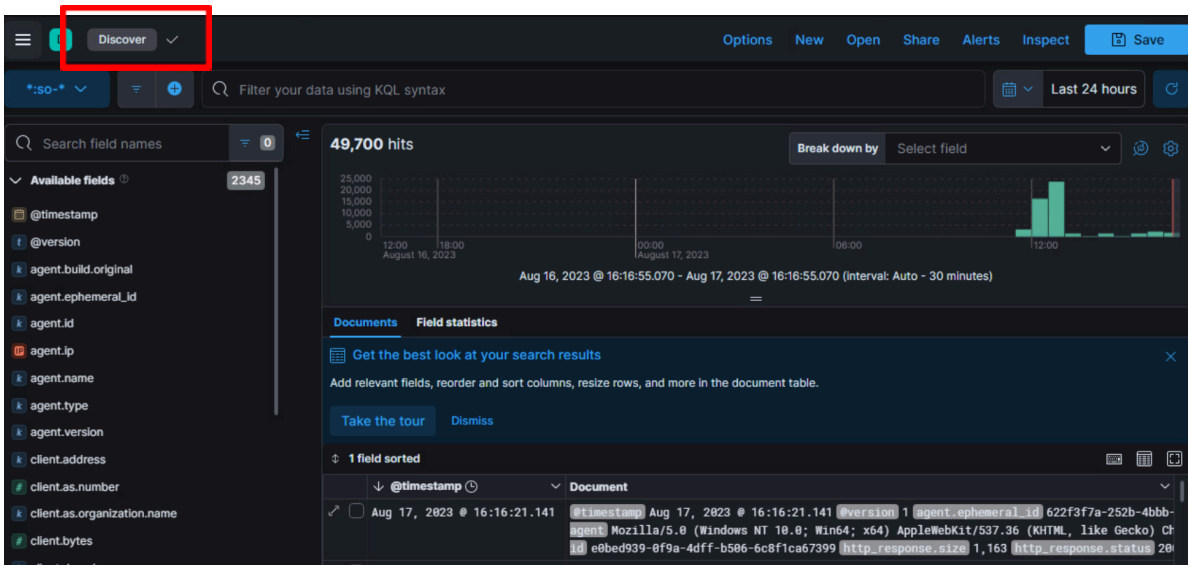
Security Onion – Home Dashboard



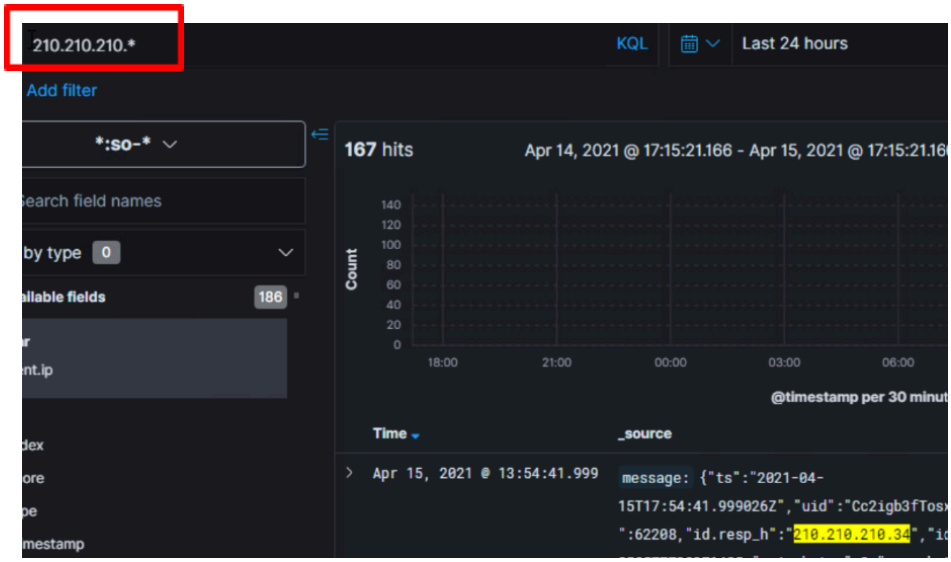
The navigation menu on the left can also be used to view additional pre-built dashboards and searches. Navigating to the Discover tab takes you to an interface similar to Splunk Search & Reporting.



Discover Dashboard



The Kibana search bar supports the Lucene search syntax. For example, entering 210.210.210* in the search bar will search and highlight all IPs within that range in events.

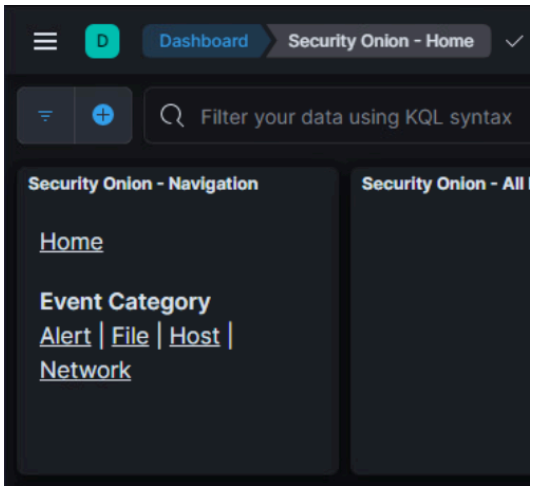


Search Modifiers:

- “literal” – quoting a string matches entire phrase
  - “google.com/update” – searches for that explicit string
- FIELD_NAME:Value – search in specific fields
  - Ex: destination_ip:155.6.3.16
- AND/OR – complex searches, AND/OR must be capitalized
  - “155.6.4.10 AND google.com/evil”
- Parentheses: (“google.com” OR “Ubuntu.com”)

Using Security Onion Dashboard

The Home dashboard can be utilized for hunting and quick visualizations of “dragnet” or generic searches. Simply typing an IP address or a host name can provide a quick high-level triage of alerts and traffic.



The example below is a hostname search and snapshot of protocols used, ports utilized (inbound and outbound) as well as Sysmon logs from the Windows OS itself.