

Information Security Operations Center (Info SOC)

Lecture 9

*Analyze network intrusion data to identify
compromised hosts and vulnerabilities*

Contents

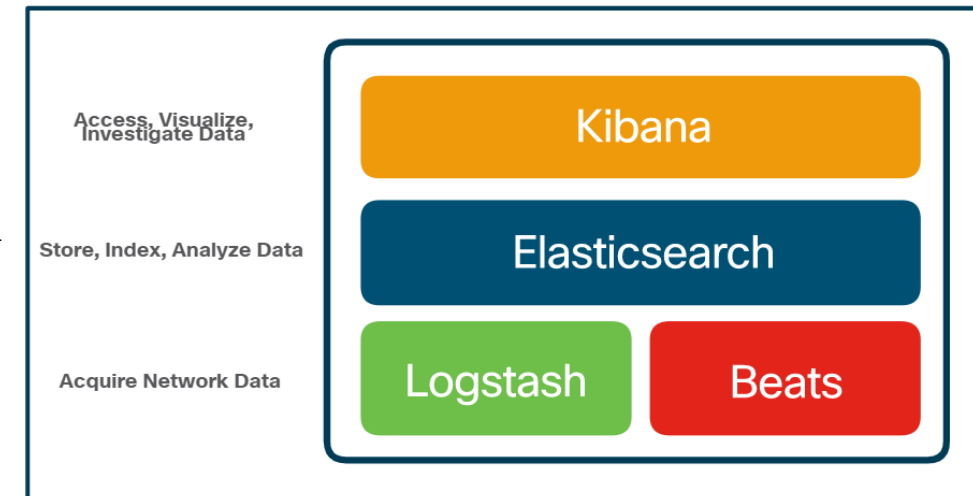
Topic Title	Topic Objective
A Common Data Platform	Explain how data is prepared for use in a Network Security Monitoring (NSM) system.
Investigating Network Data	Use Security Onion tools to investigate network security events.
Enhancing the Work of the CyberSecurity Analyst	Describe network monitoring tools that enhance workflow management.

ELK

Security Onion includes **Elastic Stack** that consists of Elasticsearch, Logstash, and Kibana (**ELK**).

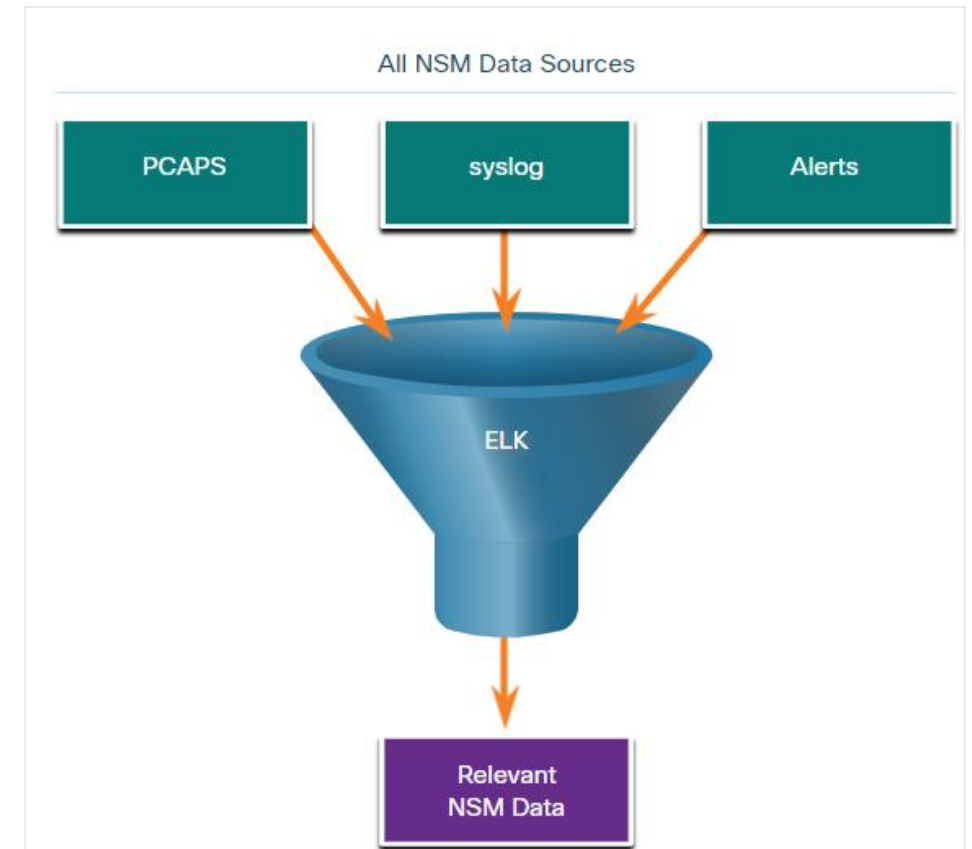
Core Components of ELK:

- **Elasticsearch**: An open-core platform for searching and analyzing an organization's data in near real time.
- **Logstash**: Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch.
- **Kibana**: Provides a graphical interface to data that is compiled by Elasticsearch.
- **Beats**: Series of software plugins that send different types of data to the Elasticsearch data stores.



Data Reduction

- To reduce data, it is essential to identify the network data that should be gathered and stored to reduce the burden on systems.
- By limiting the volume of data, tools like [Elasticsearch](#) will be far more useful.



Data Normalization

- **Data normalization** is the process of combining data from a number of sources into a common format.
- A common schema will specify the names and formats for the required data fields.
- For example, IPv6 addresses, MAC addresses, and date and time can be represented in varying formats:

IPv6 Address Formats	Mac Formats	Date Formats
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- Data normalization is also required to simplify searching for correlated events.

Data Archiving

- **Retaining** Network Security Monitoring (NSM) data **indefinitely** is **not feasible** due to **storage and access issues**.
- The retention period for certain types of network security information may be specified by compliance frameworks.
- Sguil alert data is retained for 30 days by default. This value is set in the **securityonion.conf** file.
- Security Onion data can always be archived to external storage by a data archive system, depending on the needs and capabilities of the organization.

Note: *The storage locations for the different types of Security Onion data will vary based on the Security Onion implementation.*

Investigating Network Data

Working in Sguil

- In Security Onion, the first place that a cybersecurity analyst will go to verify alerts is **Sguil**.
- Sguil automatically **correlates similar alerts into a single line** and provides a way to view correlated events represented by that line.
- To understand what is happening in the network, it may be useful to sort the **CNT** column to display the alerts with the highest frequency.

The screenshot shows the Sguil-0.9.0 interface. The main display area contains a table of alerts. The table has the following columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The alerts are sorted by CNT in descending order. The first alert has a CNT of 1059, followed by 881, 647, 296, 252, 123, 123, 123, 76, and 76. The event messages include various network-related alerts such as "OSSEC Received 0 packets in designated time interval", "OSSEC Listened ports status (netstat) changed", "GPL ICMP_INFO PING *NIX", "ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...", "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers", "ET WEB_SERVER Possible CVE-2014-6271 Attempt", "ET INFO Executable Download from dotted-quad Host", and "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers".

Sguil Alerts Sorted on CNT

Sguil Queries

- Queries can be constructed in Sguil using the **Query Builder**. It simplifies constructing queries to a certain degree.
- **Cybersecurity analyst** must know the field names and some issues with field values to effectively build queries in Sguil.
- For example, Sguil stores IP addresses in an integer representation.

The screenshot displays the Sguil 0.9.0 interface. The top section shows a query result table with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The table contains several rows of data, including alerts for 'ET SCAN Nmap Scripting Engine User-Agent Detected' and 'ET SCAN Nmap SQL Spider Scan'.

The bottom section shows packet details for a selected event. It includes a table for IP Resolution and a detailed view of the packet structure, including Source IP, Destination IP, Protocol (TCP), and various packet fields like Source Port, Destination Port, Sequence Number, and Offset. The packet data is shown in hexadecimal and ASCII format.

Investigating Network Data

Pivoting from Sguil

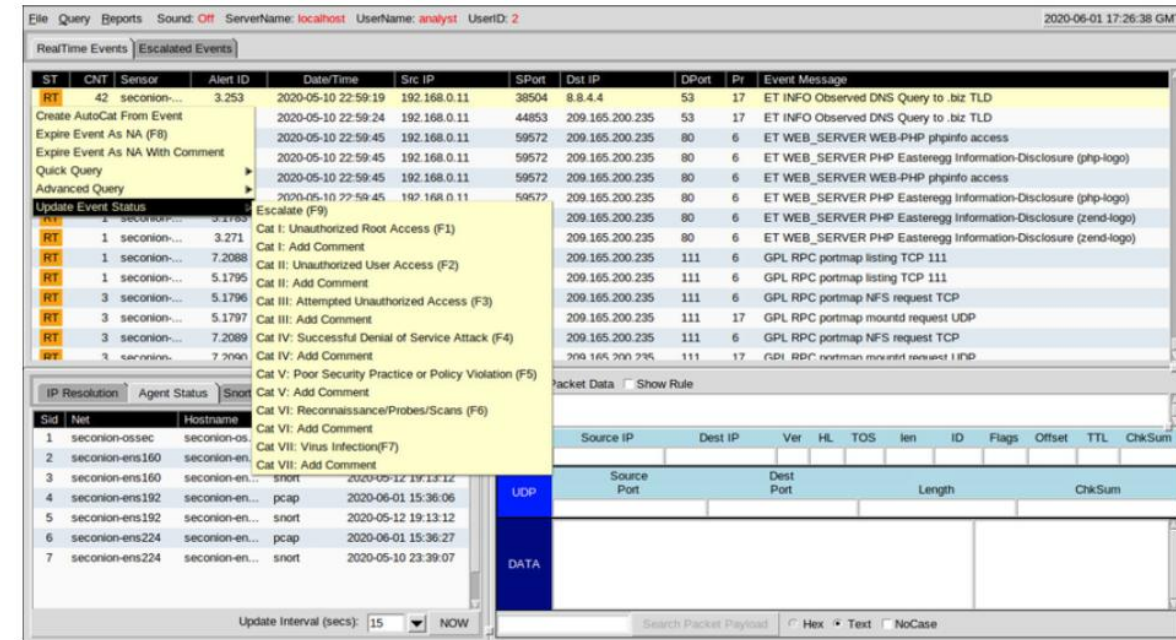
- **Sguil** provides the ability for the **cybersecurity analyst** to pivot to other information sources and tools.
- **Log files** are available in Elasticsearch.
- Relevant packet captures can be displayed in Wireshark.

The screenshot displays the Sguil interface. The top section shows a list of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. A red box highlights a specific event with Alert ID 5.1557, dated 2020-05-10 21:21:17, from Src IP 209.165.201.17 to Dst IP 209.165.200.235 on port 80. The event message is 'ET CURRENT_EVENTS Possible Magento Directory Traversal Attempt'. Below the event list, the 'System Msgs' tab is selected, showing a table with columns: Sid, Net, Hostname, Type, and Last. The bottom section shows a detailed view of the selected event, including a packet capture (pcap) and a list of related events. The packet capture details show a TCP segment from Source Port 10 to Destination Port 80, with a sequence number of 10 and a window size of 65535. The data section shows the raw packet data in hex and text format.

Investigating Network Data

Event Handling in Sguil

- Sguil is a console that enables a cybersecurity analyst to investigate, verify, and classify security alerts.
- Three tasks can be completed in Sguil to manage alerts:
 - Alerts that have been found to be false positives can be expired.
 - An event can be escalated by pressing the F9 key.
 - An event can be categorized.

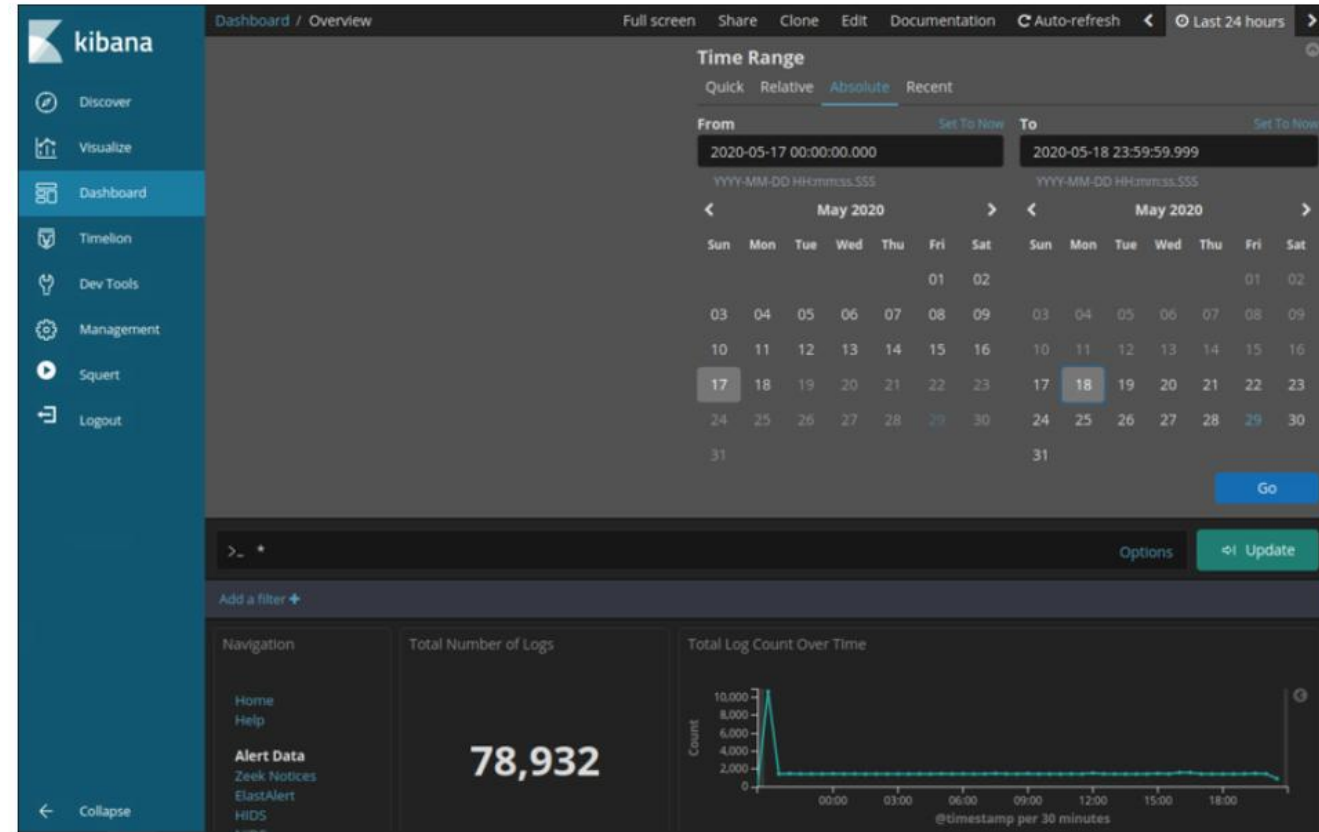


- Sguil includes seven pre-built categories that can be assigned by using a menu or by pressing the corresponding function key.

Investigating Network Data

Working in ELK

- **Logstash and Beats** are used for data ingestion in the Elastic Stack.
- Kibana, which is the visual interface into the logs, is configured to show the **last 24 hours** by default.
- Logs are ingested into Elasticsearch into separate indices or databases based on a configured range of time.
- The best way to monitor the data in Elasticsearch is to build customized visual dashboards.

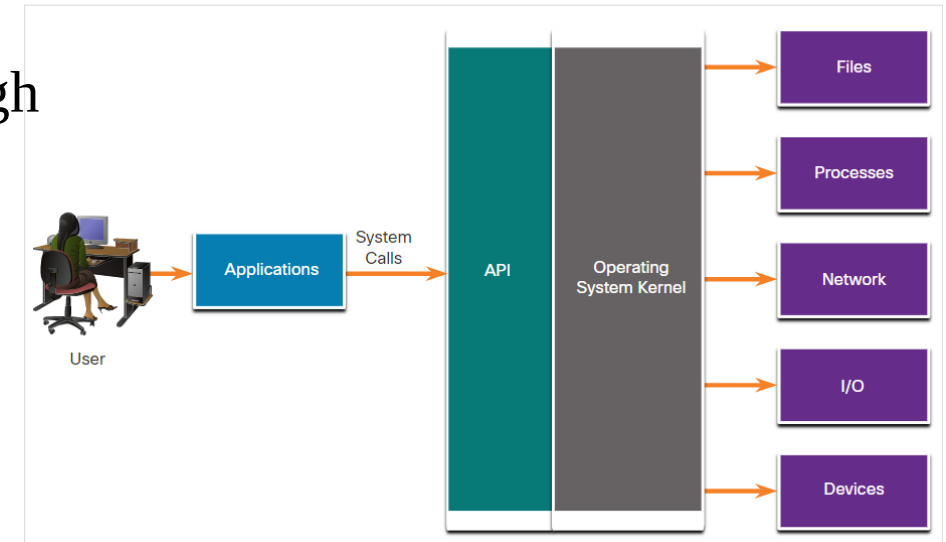


Queries in ELK

- Elasticsearch is built on [Apache Lucene](#), an open-source search engine software library featuring full text indexing and searching capabilities.
- Using Lucene software libraries, Elasticsearch has its own query language based on JSON called [Query Domain Specific Language](#) (QDSL).
- Along with JSON, Elasticsearch queries make use of elements such as Boolean operators, Fields, Ranges, Wildcards, Regex, Fuzzy Search, and Text Search.
- Elasticsearch was designed to interface with users using web-based clients that follow the HTTP REST framework.
- Methods used for executing the queries are URI, cURL, JSON and Dev Tools.

Investigating Process or API Calls

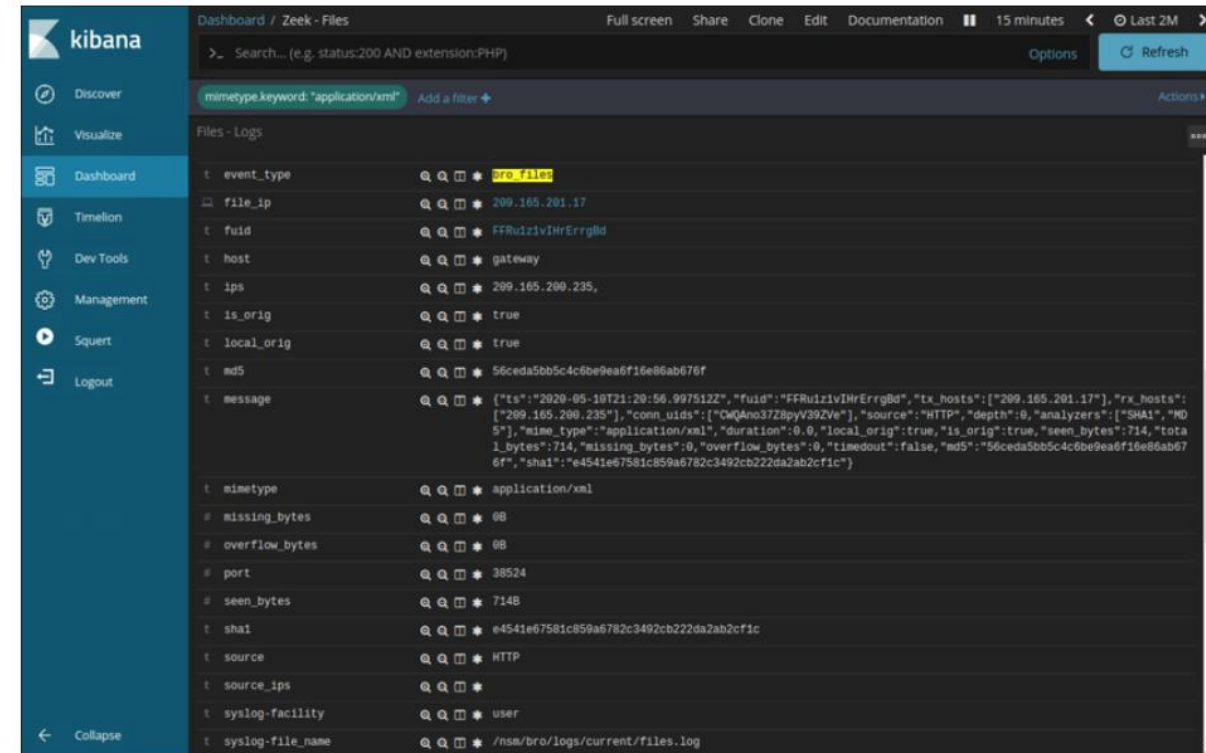
- Applications interact with an Operating System (OS) through system calls to the OS Application Programming Interface (API).
- If **malware** can **fool an OS kernel** into allowing it to make system calls, many exploits are possible.
- OSSEC rules detect changes in host-based parameters.
- OSSEC rules will trigger an alert in Sguil.
- Pivoting to Kibana on the host IP address allows you to choose the type of alert based on the program that created it.



Investigating Network Data

Investigating File Details

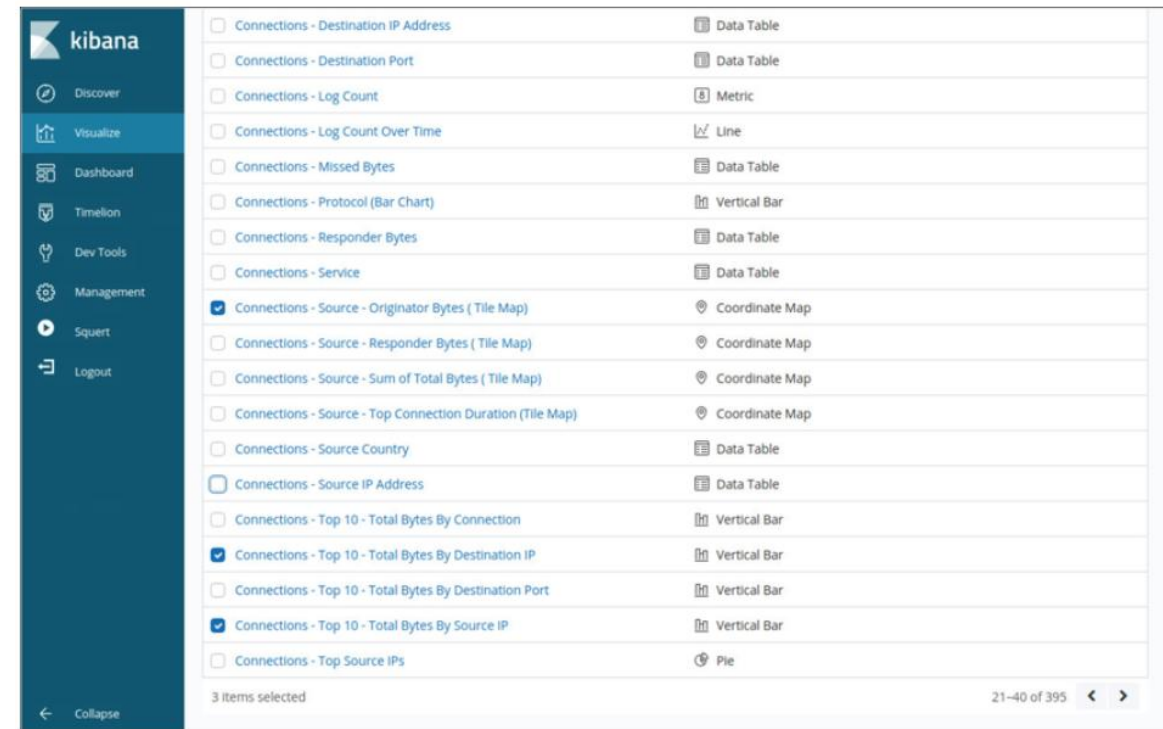
- In Sguil, if the cybersecurity analyst is suspicious of a file, the hash value can be submitted to an online site to determine if the file is a known malware.
- In **Kibana**, **Zeek Hunting** can be used to display information regarding the files that have entered the network.
- Note that in Kibana, the event type is shown as **bro_files**, even though the new name for Bro is Zeek.



Enhancing the Work of the Cybersecurity Analyst

Dashboards and Visualizations

- **Dashboards** provide a combination of data and visualizations which allows cybersecurity analysts to focus on specific details and information.
- Dashboards are usually interactive.
- **Kibana** includes the capability of designing **custom dashboards**.
- In addition, tools such as **Squert** in Security Onion provide a **visual interface** to NSM data.



Enhancing the Work of the Cybersecurity Analyst

Workflow Management

- **Workflows** are the sequence of processes and procedures through which work tasks are completed.
- **Managing the SOC workflows:**
 - Enhances the efficiency of the cyberoperations team
 - Increases the accountability of the staff
 - Ensures that all potential alerts are treated properly
- **Sguil** provides a **basic workflow management** but **not a good choice for large operations**. There are third party systems available that can be customized.
- Automated queries add efficiency to the cyberoperations workflow. These queries automatically search for complex security incidents that may evade other tools.

Activity: Isolate Compromised Host Using 5-Tuple

In this activity, you will complete the following objective:

- Use Security Onion tools to investigate an exploit.

Thanks