

Module 27: Working with Network Security Data

CyberOps Associate v1.0

27.1 A Common Data Platform

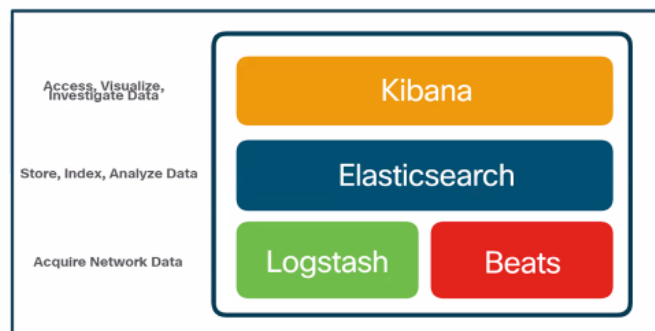
A Common Data Platform

ELK

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

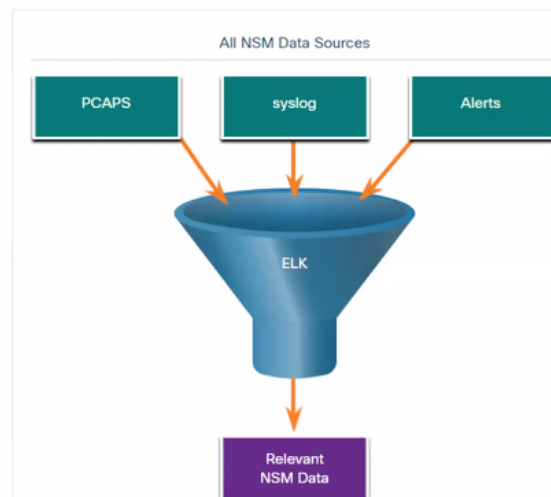
Core Components of ELK:

- **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:

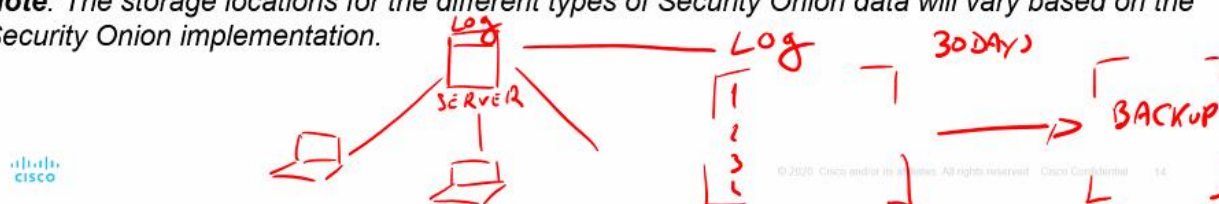
IPv6 Address Formats	Mac Formats	Date Formats
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- 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.
- Squid 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.

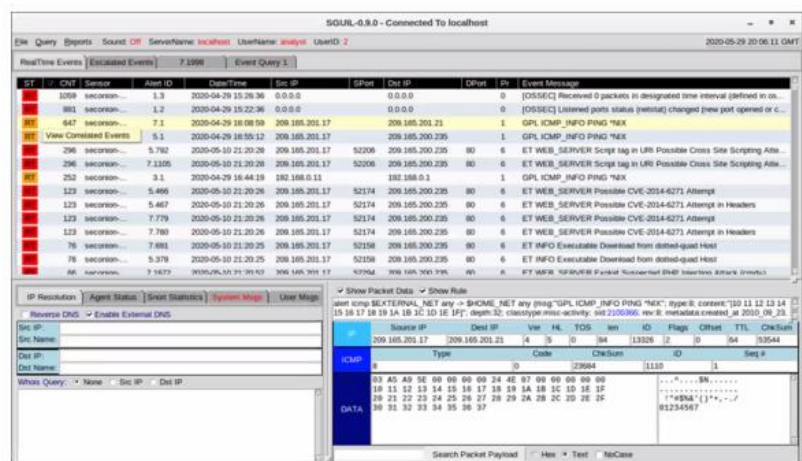
Note: The storage locations for the different types of Security Onion data will vary based on the Security Onion implementation.



27.2 Investigating Network Data

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.



Squid Alerts Sorted on CNT

INIZIO MODULO 26

Evaluating Alerts

Alert Generation

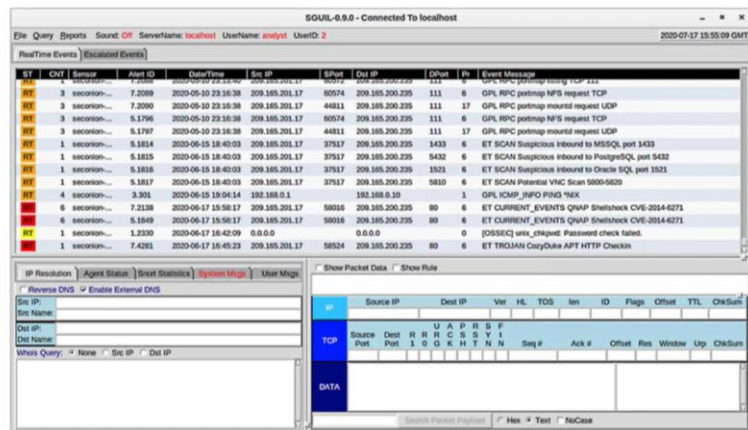
- Security alerts are notification messages that are generated by NSM tools, systems, and security devices. Alerts can come in many forms depending on the source.
- In Security Onion, Sguil provides a console that integrates alerts from multiple sources into a timestamped queue.
- A cybersecurity analyst works through the security queue investigating, classifying, escalating, or retiring alerts.
- Alerts will generally include five-tuples information, as well as timestamps and information identifying which device or system generated the alert.
 - **SrcIP** - the source IP address for the event.
 - **SPort** - the source (local) Layer 4 port for the event.
 - **DstIP** - the destination IP for the event.
 - **DPort** - the destination Layer 4 port for the event.
 - **Pr** - the IP protocol number for the event.

Evaluating Alerts

Alert Generation (Contd.)

The figure shows the Sguil application window with the queue of alerts that are waiting to be investigated in the top portion of the interface. The fields available for the real-time events are as follows:

- **ST** - This is the status of the event. The event is color-coded by priority based on the category of the alert. There are four priority levels: very low, low, medium, and high and the colors range from light yellow to red as the priority increases.
- **CNT** - This is the count for the number of times this event has been detected for the same source and destination IP address. The system has determined that this set of events is correlated.
- **Sensor** - This is the agent reporting the event. The available sensors and their identifying numbers can be found in the Agent Status tab of the pane which appears below the events window on the left.

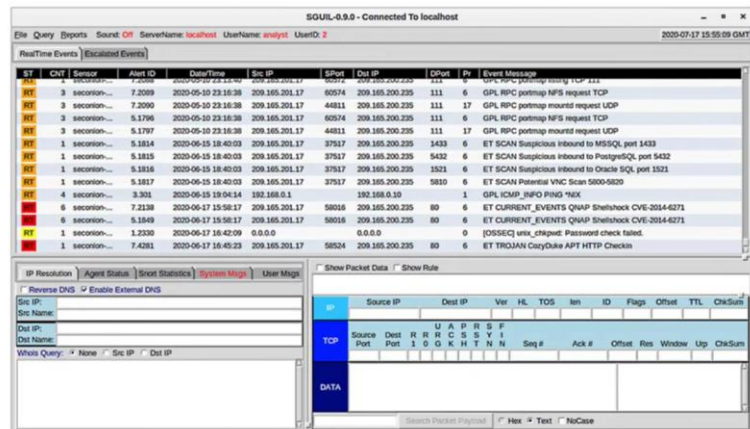


Sguil Window

Evaluating Alerts

Alert Generation (Contd.)

- **Alert ID** - This two-part number represents the sensor that has reported the problem and the event number for that sensor.
- **Date/Time** - This is the timestamp for the event. In the case of correlated events, it is the timestamp for the first event.
- **Event Message** - This is the identifying text for the event. This is configured in the rule that triggered the alert. The associated rule can be viewed in the right-hand pane, just above the packet data. To display the rule, the **Show Rule** checkbox must be selected.



Sguil Window

Evaluating Alerts

Rules and Alerts

- Alerts can come from a number of sources:
 - **NIDS** - Snort, Zeek, and Suricata
 - **HIDS** - OSSEC, Wazuh
 - **Asset management and monitoring** - Passive Asset Detection System (PADS)
 - **HTTP, DNS, and TCP transactions** - Recorded by Zeek and pcpas
 - **Syslog messages** - Multiple sources
- The information found in the alerts that are displayed in Sguil will differ in message format because they come from different sources.
- The Sguil alert in the figure was triggered by a rule that was configured in Snort.



Snort Rule Structure (Contd.)

The Rule Header

The rule header contains the action, protocol, addressing, and port information, as shown in the figure. The structure of the header portion is consistent between Snort alert rule. Snort can be configured to use variables to represent internal and external IP addresses.

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
alert	the action to be taken is to issue an alert, other actions are log and pass
ip	the protocol
any any	the specified source is any IP address and any Layer 4 port
->	the direction of flow is from the source to the destination
any any	the specified destination is any IP address and any Layer 4 port

Snort Rule Structure (Contd.)

The Rule Options

- The structure of the options section of the rule is variable. It is the portion of the rule that is enclosed in parenthesis, as shown in the figure. It contains the text message that identifies the alert. It also contains metadata about the alert, such as a URL.
- Snort rule messages may include the source of the rule. Three common sources for Snort rules are:
 - GPL** - Older Snort rules that were created by Sourcefire and distributed under a GPLv2. The GPL ruleset is not Cisco Talos certified. The GPL ruleset is can be downloaded from the Snort website, and it is included in Security Onion.
 - ET** - Snort rules from Emerging Threats which is a collection point for Snort rules from multiple sources. The ET ruleset contains rules from multiple categories. A set of ET rules is included with Security Onion. Emerging Threats is a division of Proofpoint, Inc.
 - VRT** - These rules are immediately available to subscribers and are released to registered users 30 days after they were created, with some limitations. They are now created and maintained by Cisco Talos.

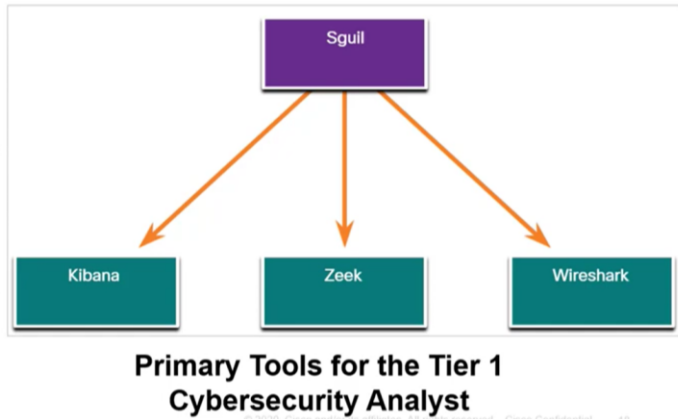
Snort Rule Structure (Contd.)

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
msg:	Text that describes the alert.
content:	Refers to content of the packet. In this case, an alert will be sent if the literal text "uid=0(root)" appears anywhere in the packet data. Values specifying the location of the text can be provided.
reference:	This is not shown in the figure. It is often a link to a URL that provides more information on the rule. In this case, the sid is hyperlinked to the source of the rule on the internet.
classtype:	A category for the attack. Snort includes a set of default categories that have one of four priority values.
sid:	A unique numeric identifier for the rule.
rev:	The revision of the rule that is represented by the sid.

The Need for Alert Evaluation

- The threat landscape is constantly changing as new vulnerabilities and threats are discovered. As user and organizational needs change, so also does the attack surface.
- Threat actors have learned how to quickly vary features of their exploits in order to evade detection.
- It is better to have alerts that are sometimes generated by innocent traffic, than it is to have rules that miss malicious traffic.
- It is necessary to have skilled cybersecurity analysts investigate alerts to determine if an exploit has actually occurred.
- Tier 1 cybersecurity analysts will work through queues of alerts in a tool like Sguil, pivoting to tools like Zeek, Wireshark, and Kibana to verify that an alert represents an actual exploit.



Evaluating Alerts

- Security incidents are classified using a scheme borrowed from medical diagnostics. This classification scheme is used to guide actions and to evaluate diagnostic procedures. The concern is that either diagnosis can be accurate, or true, or inaccurate, or false.
- In network security analysis, the cybersecurity analyst is presented with an alert. The cybersecurity analyst needs to determine if this diagnosis is true.
- Alerts can be classified as follows:
 - **True Positive:** The alert has been verified to be an actual security incident.
 - **False Positive:** The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as a benign trigger.
- An alternative situation is that an alert was not generated. The absence of an alert can be classified as:
 - **True Negative:** No security incident has occurred. The activity is benign.
 - **False Negative:** An undetected incident has occurred.

Evaluating Alerts (Contd.)

When an alert is issued, it will receive one of four possible classifications:

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

- **True positives** are the desired type of alert. They mean that the rules that generate alerts have worked correctly.
- **False positives** are not desirable. Although they do not indicate that an undetected exploit has occurred, they are costly because cybersecurity analysts must investigate false alarms.
- **True negatives** are desirable. They indicate that benign normal traffic is correctly ignored, and erroneous alerts are not being issued.
- **False negatives** are dangerous. They indicate that exploits are not being detected by the security systems that are in place.

Note: “True” events are desirable. “False” events are undesirable and potentially dangerous.

What Did I Learn in this Module?

- Security Onion is an open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution.
- Security Onion tools provide three core functions for the cybersecurity analyst: full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools.
- Security Onion integrates the data and IDS logs into a single platform through the following tools:
 - Sguil - serves as a starting point in the investigation of security alerts.
 - Kibana - It is an interactive dashboard interface to Elasticsearch data.
 - The Wireshark packet capture application is integrated into the Security Onion suite.
 - Zeek is a network traffic analyzer that serves as a security monitor.

FINE MODULO 26

Investigating Network Data

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.

ST	CNT	Sensor	Alert ID	DateTime	Src IP	DPort	Dst IP	Pn	Event Message
1	1	secmon-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	secmon-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	secmon-eth2-1	7.587	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	secmon-eth2-1	7.588	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	1	secmon-eth2-1	7.589	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

Investigating Network Data

Pivoting from Sguil

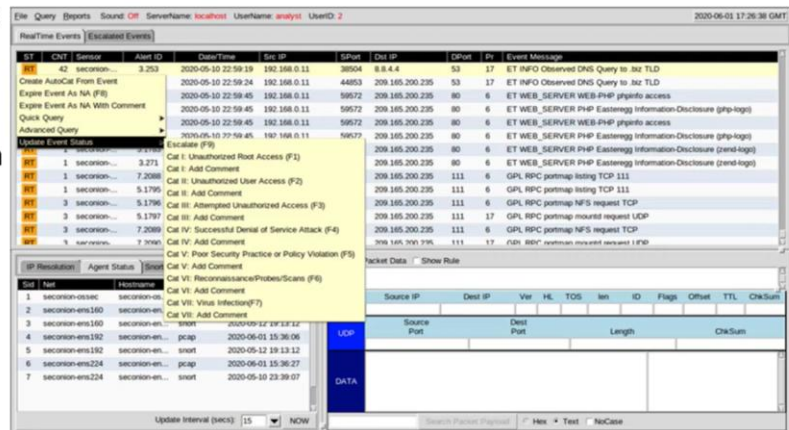
- Sguil provides the ability for the cybersecurity analyst to pivot to other information sources and tools.
- Log files are available in Elasticsearch.
- Relevant packet captures can be displayed in Wireshark.
- Sguil can provide pivots to Passive Real-time Asset Detection System (PRADS) and Security Analyst Network Connection Profiler (SANCP) information.

ST	CNT	Sensor	Alert ID	DateTime	Src IP	DPort	Dst IP	Pn	Event Message
41	1	secmon-eth1	5.1553	2020-05-10 21:20:56	209.165.201.17	52368	209.165.200.235	80	ET WEB_SERVER Possible XSS SYSTEM ENTITY in POST BODY
1	1	secmon-eth1	5.1554	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET WEB_SERVER Possible XSS SYSTEM ENTITY in POST BODY
6	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET CURRENT_EVENTS Possible Magento Directory Traversal Attempt
1	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema
2	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET WEB_SERVER Possible Joomla SQLi Attempt
2	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET CURRENT_EVENTS Possible vulnlist object injection vulnerability ...
9	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET WEB_SPECIFIC_APPS Possible Magento AdminPanel Access
2	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	ET EXPLOIT WordPress DUTV Shell UCE
1	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	ET EXPLOIT D-Link DSL-2750B - OS Command Injection
2	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET CURRENT_EVENTS Possible vulnlist object injection vulnerability ...
9	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET WEB_SPECIFIC_APPS Possible Magento AdminPanel Access
2	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	ET EXPLOIT WordPress DUTV Shell UCE
1	1	secmon-eth1	5.1557	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	ET EXPLOIT D-Link DSL-2750B - OS Command Injection

Note: The Sguil interface refers to PADS instead of PRADS.

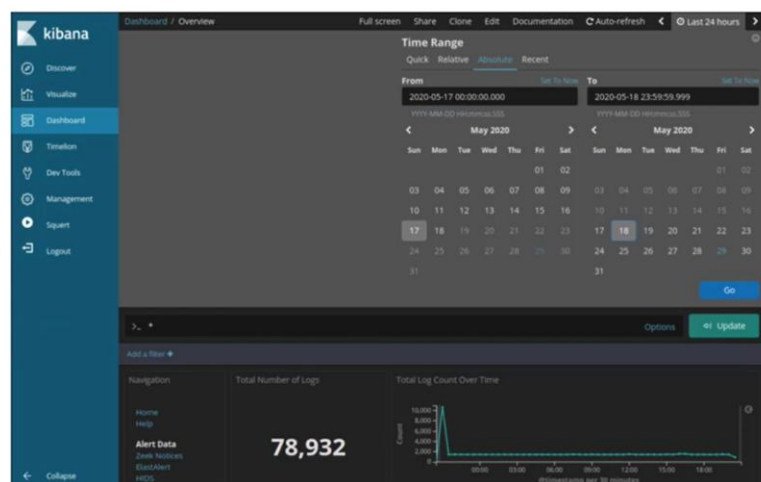
Investigating Network Data Event Handling in Sguil

- 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.



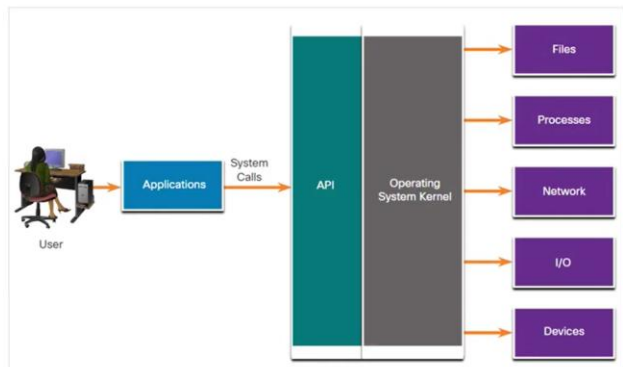
Investigating Network Data Queries in ELK

- 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 (DSL).
- Along with JSON, Elasticsearch queries make use of elements such as Boolean operators, Fields, Ranges, Wildcards, Regexp, 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.

Note: Advanced Elasticsearch queries are beyond the scope of this course. In the labs, you will be provided with the complex query statements, if necessary.

Investigating Process or API Calls

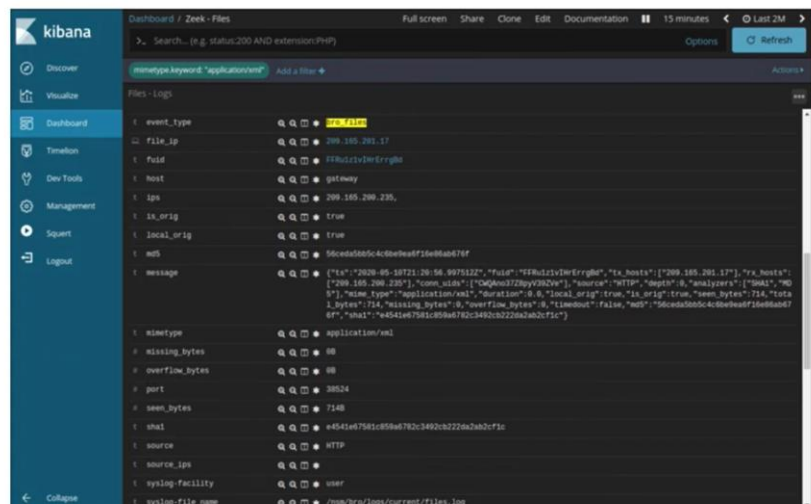
- Applications interact with an Operating System (OS) through system calls to the OS Application Programming Interface (API).
- If malware can fool an OS kernel into allowing it to make system calls, many exploits are possible.
- OSSEC rules detect changes in host-based parameters.
- OSSEC rules will trigger an alert in Squil.
- Pivoting to Kibana on the host IP address allows you to choose the type of alert based on the program that created it.
- Filtering for OSSEC indices results in a view of the OSSEC events that occurred on the host, including indicators that malware may have interacted with the OS kernel



Investigating Network Data

Investigating File Details

- In Squil, 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.

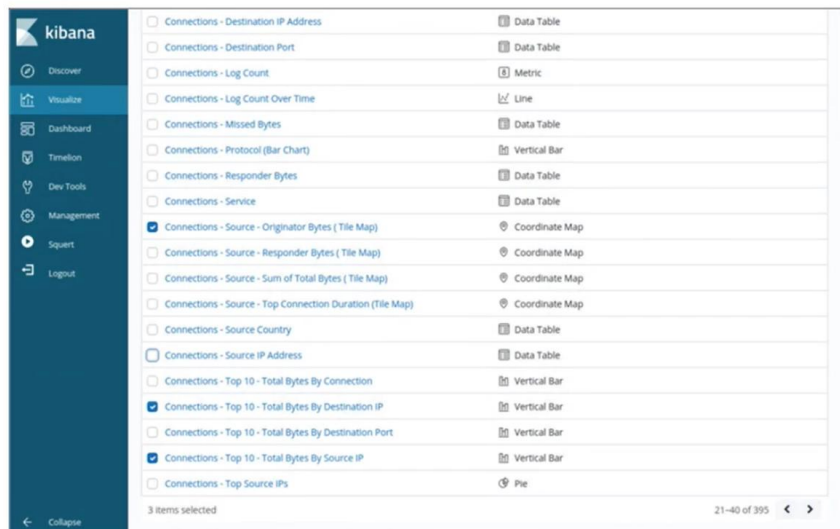


27.3 Enhancing the Work of the Cybersecurity Analyst

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.

27.4 Working with Network Security Data Summary

What Did I Learn in this Module?

- A network security monitoring platform such as ELK or Elastic Stack must unite the data for analysis.
- ELK consists of Elasticsearch, Logstash, and Kibana with components, Beats, ElastAlert, and Curator.
- Network data must be reduced so that only relevant data is processed by the NSM system.
- Network data must also be normalized to convert the same types of data to consistent formats.
- Sguil provides a console that enables a cybersecurity analyst to investigate, verify, and classify security alerts.
- Kibana visualizations provide insights into NSM data by representing large amounts of data formats that are easier to interpret.
- Workflow management adds efficiency to the work of the SOC team.