

# Module 27: Working with Network Security Data

CyberOps Associate v1.0



# Module Objectives

**Module Title :** Working with Network Security Data

**Module Objective:** Interpret data to determine the source of an alert.

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.

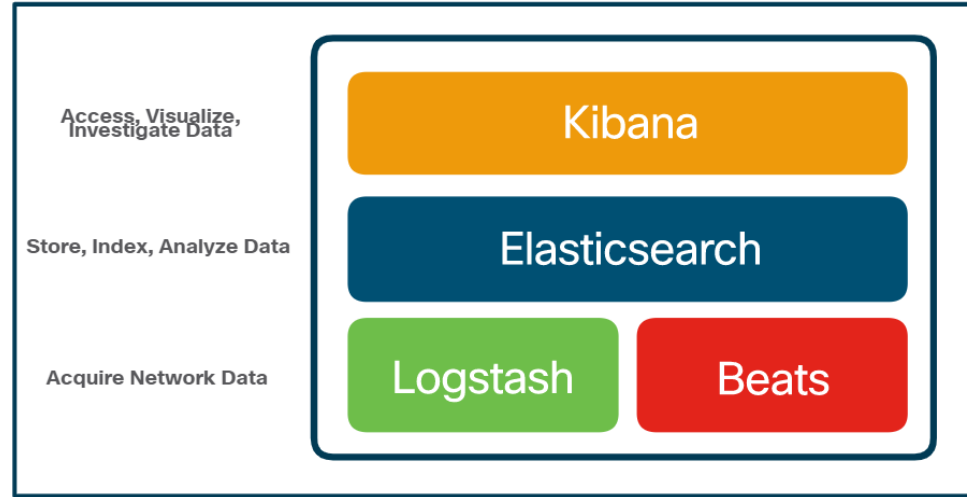
# 27.1 A Common Data Platform

# ELK

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

### Core Components of ELK:

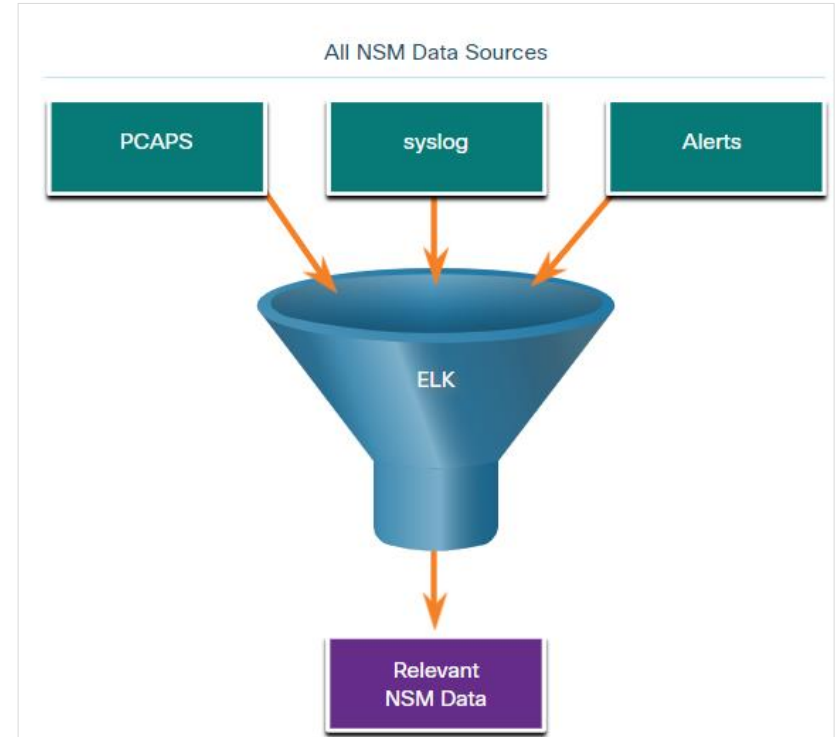
- **Elasticsearch:** An open-core platform for searching and analyzing an organization's data in near real time.
- **Logstash:** Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch.
- **Kibana:** Provides a graphical interface to data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



## A Common Data Platform

# 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.

## A Common Data Platform

# 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.*

# Lab - Convert Data into a Universal Format

In this lab, you will complete the following objectives:

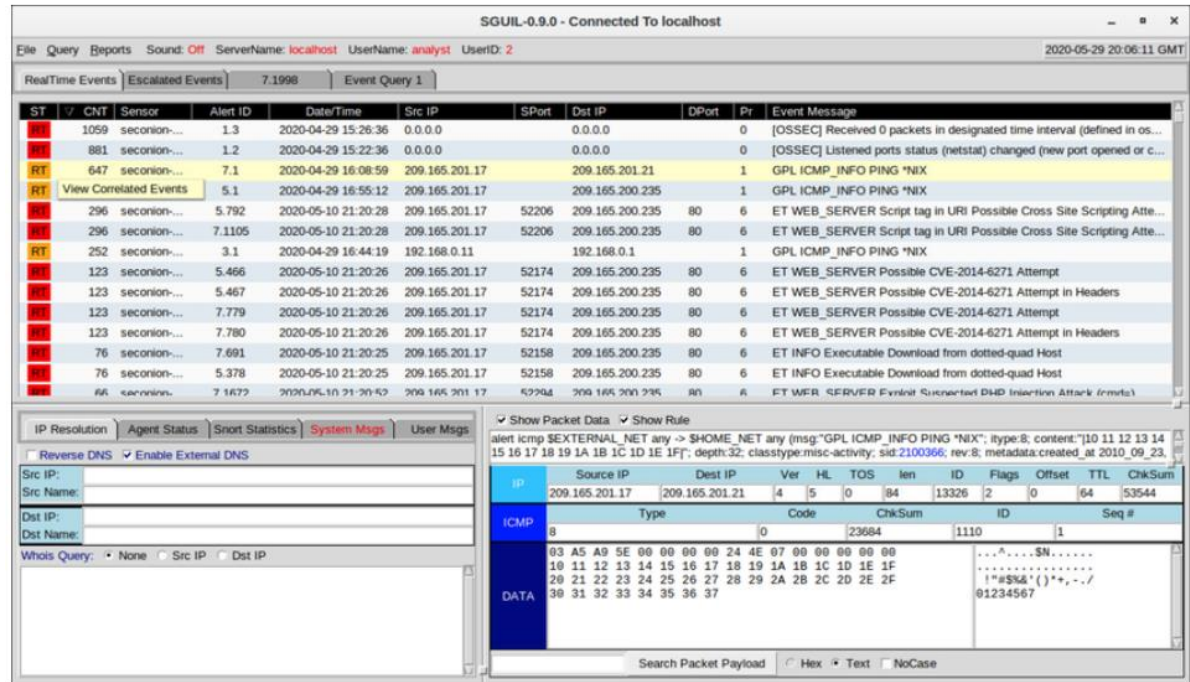
- **Part 1:** Use command line tools to manually normalize log entries.
- **Part 2:** The timestamp field must be normalized.
- **Part 3:** The IPv6 field requires normalization.



# 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.



The screenshot shows the Sguil-0.9.0 interface. The main table displays a list of alerts sorted by CNT (Count). The table has columns for ST, CNT, Sensor, Alert ID, DateTime, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The alerts are sorted by CNT in descending order, with the highest count being 11055 for Alert ID 7.1105.

ST	CNT	Sensor	Alert ID	DateTime	Src IP	SPort	Dst IP	DPort	Pr	Event Message
AL	1059	seconion...	1.3	2020-04-29 15:26:36	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in os...
AL	881	seconion...	1.2	2020-04-29 15:22:36	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports status (netstat) changed (new port opened or c...
RT	647	seconion...	7.1	2020-04-29 16:08:59	209.165.201.17		209.165.201.21		1	GPL ICMP_INFO PING *NIX
RT	51	View Correlated Events	5.1	2020-04-29 16:55:12	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
AL	296	seconion...	5.792	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
AL	296	seconion...	7.1105	2020-05-10 21:20:28	209.165.201.17	52206	209.165.200.235	80	6	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Atte...
RT	252	seconion...	3.1	2020-04-29 16:44:19	192.168.0.11		192.168.0.1		1	GPL ICMP_INFO PING *NIX
AL	123	seconion...	5.466	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
AL	123	seconion...	5.467	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
AL	123	seconion...	7.779	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt
AL	123	seconion...	7.780	2020-05-10 21:20:26	209.165.201.17	52174	209.165.200.235	80	6	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
AL	76	seconion...	7.691	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
AL	76	seconion...	5.378	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	ET INFO Executable Download from dotted-quad Host
AL	66	seconion...	7.1672	2020-05-10 21:20:52	209.165.201.17	52204	209.165.200.235	80	6	ET WEB_SERVER Evlnet Connected D&D Injection Attack (rmot)

The bottom pane shows the packet details for the selected alert. It includes a table for the packet headers and a hex dump of the payload.

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	209.165.201.17	209.165.201.21	4	5	0	84	13326	2	0	64	53544

The packet details pane also shows the packet type (ICMP) and the packet code (0). The packet length is 84 bytes. The packet ID is 13326. The packet offset is 2. The packet TTL is 64. The packet checksum is 53544.

## Sguil Alerts Sorted on CNT

# 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.

SQLUI 0.9.0 - Connected to localhost
2017-07-19 21:06:12 GMT

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2

RealTime Events Escalated Events Event Query 9

Close

SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET\_NTOA(event.src\_ip), INET\_NTOA(event.dst\_ip), event.ip.proto, event.src\_port, event.dst\_port, event.signature\_gen, event.signature\_id, event.signature\_rev FROM event IGNORE INDEX (event\_p\_key, sid\_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.src\_port = 40754 ORDER BY datetime, src\_port ASC LIMIT 1000

Submit

Export

Edit

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	1	seconion-eth1-1	5.521	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
2	1	seconion-eth1-1	5.522	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
3	1	seconion-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed
4	1	seconion-eth2-1	7.587	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
5	1	seconion-eth2-1	7.588	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap SQL Spider Scan
6	1	seconion-eth2-1	7.589	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed

IP Resolution
Agent Status
Short Statistics
System Msgs
User Msgs

Sid	Net	Hostname	Type	Last
1	seconion-osscc	seconion-osscc	osscc	2017-07-19 21:05:17
2	seconion-eth0	seconion-eth0	pcap	2017-07-19 13:44:58
3	seconion-eth1	seconion-eth0-1	snort	
4	seconion-eth1	seconion-eth1	pcap	2017-07-19 13:45:11
5	seconion-eth1	seconion-eth1-1	snort	2017-07-05 18:53:42
6	seconion-eth2	seconion-eth2	pcap	2017-07-19 13:45:22
7	seconion-eth2	seconion-eth2-1	snort	2017-07-05 18:53:42

Update Interval (secs):

15

NOW

Show Packet Data
Show Rule

Alert top \$EXTERNAL\_NET any -> HTTP\_SERVERS HTTP\_PORTS (msg: 'ET SCAN Nmap SQL Spider Scan'; flow: established to server; content: 'GET'; http\_method: content: 'OR sqlspider'; http\_ref: <http://nmap.org/nmapdoc/scripts/sql-injection.html>;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	ttl	ChkSum
TCP	209.165.201.17	209.165.200.235	4	5	0	268	33065	2	0	63	33914
DATA	40754	80									

Source	Dest	R	R	U	A	P	S	R	S	F	
1	0	G	K	H	T	N	N				
64	65	72	26	20	48	54	50	2F	31	2E	31
6F	6E	6E	65	63	74	69	6F	6E	3A	20	63

Seq#	Ack#	Offset	Res	Window	Urp	ChkSum
1692715185	667712887	8	0	229	0	50943

GET http://twiki.org/cgi-bin/edit/TWiki/7topic%2728200%20sqlspider&HTTP/1.1: connection: close

# 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.

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 this, a detailed view of the event is shown, including a table of IP Resolution and a packet capture view.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	5.1515	2020-05-10 21:20:56	209.165.201.17	52368	209.165.200.235	80	6	ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.
RT	1	seconion...	5.1556	2020-05-10 21:21:17	209.165.201.17	52406	209.165.200.235	80	6	GPL WEB_SERVER mod_gzip_status access
RT	6	seconion...	5.1557	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET CURRENT_EVENTS Possible Magento Directory Traversal Attempt
RT	1	seconion...	...	...	...	...	...	...	...	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema ...
RT	1	seconion...	...	...	...	...	...	...	...	ET WEB_SPECIFIC_APPS Possible Joomla SQLi Attempt
RT	2	seconion...	...	...	...	...	...	...	...	ET CURRENT_EVENTS Possible vBulletin object injection vulnerability ...
RT	9	seconion...	...	...	...	...	...	...	...	ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access
RT	2	seconion...	...	...	...	...	...	...	...	ET EXPLOIT MvPower DVR Shell UCE
RT	1	seconion...	...	...	...	...	...	...	...	ET WORM TheMoon.linksys.router.1
RT	1	seconion...	...	...	...	...	...	...	...	ET EXPLOIT D-Link DSL-2750B - OS Command Injection
RT	2	seconion...	...	...	...	...	...	...	...	ET CURRENT_EVENTS Possible vBulletin object injection vulnerability ...
RT	9	seconion...	...	...	...	...	...	...	...	ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access
RT	2	seconion...	...	...	...	...	...	...	...	ET EXPLOIT MvPower DVR Shell UCE
RT	1	seconion...	...	...	...	...	...	...	...	ET WORM TheMoon.linksys.router.1

Sid	Net	Hostname	Type	Last
1	seconion-ssoc	seconion-ss...	ossec	2020-06-01 17:12:29
2	seconion-ens160	seconion-en...	pcap	2020-06-01 16:43:57
3	seconion-ens160	seconion-en...	snort	2020-05-12 19:13:12
4	seconion-ens192	seconion-en...	pcap	2020-06-01 15:36:06
5	seconion-ens192	seconion-en...	snort	2020-05-12 19:13:12
6	seconion-ens224	seconion-en...	pcap	2020-06-01 15:36:27
7	seconion-ens224	seconion-en...	snort	2020-05-10 23:39:07

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

# Investigating Network Data

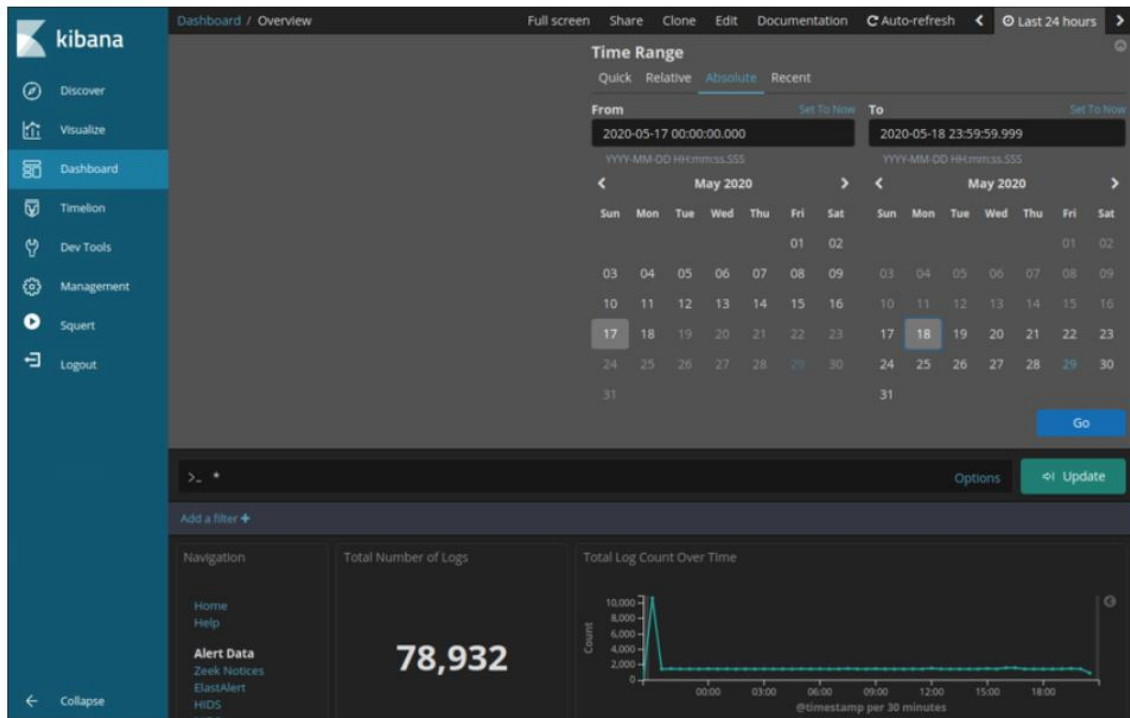
## Event Handling in Sguil

- 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.

The screenshot displays the Sguil console interface. At the top, there's a menu bar with options: File, Query, Reports, Sound: Off, ServerName: localhost, Username: analyst, UserID: 2, and a timestamp: 2020-06-01 17:26:38 GMT. Below the menu, there are tabs for 'RealTime Events' and 'Escalated Events'. The main window shows a table of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. A yellow tooltip menu is open over the 'Escalated Events' tab, showing options like 'Escalate (F9)', 'Cat I: Unauthorized Root Access (F1)', 'Cat II: Unauthorized User Access (F2)', 'Cat III: Attempted Unauthorized Access (F3)', 'Cat IV: Successful Denial of Service Attack (F4)', 'Cat V: Poor Security Practice or Policy Violation (F5)', 'Cat VI: Reconnaissance/Probes/Scans (F6)', 'Cat VII: Virus Infection (F7)', and 'Cat VIII: Add Comment'. Below the event list, there's a section for 'IP Resolution' with columns: Sid, Net, and Hostname. The bottom of the interface shows a 'Packet Data' section with a table for packet details, including Source IP, Dest IP, Ver, HL, TOS, Ien, ID, Flags, Offset, TTL, and ChkSum. The 'UDP' and 'DATA' sections are visible, showing packet details for a specific event.

# 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.





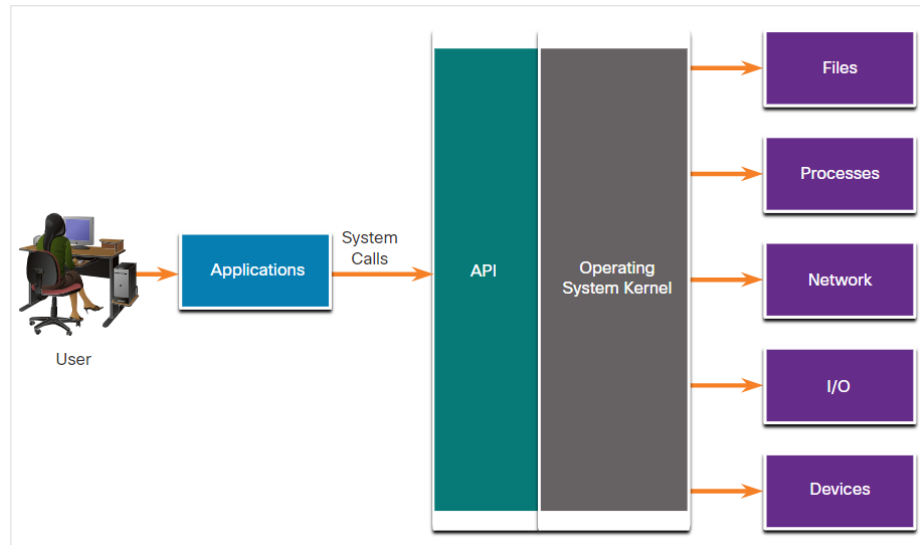
# Queries in ELK

- 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 (DSL).
- 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.

**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 Sguil.
- 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 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.

The screenshot displays the Kibana web interface. On the left is a sidebar with navigation links: Discover, Visualize, Dashboard, Timeline, Dev Tools, Management, Squert, and Logout. The 'Dashboard' link is selected. The main content area is titled 'Dashboard / Zeek - Files'. At the top of this area is a search bar with the text '>\_ Search... (e.g. status:200 AND extension:PHP)' and buttons for 'Options' and 'Refresh'. Below the search bar is a filter bar with the text 'mimetype.keyword:"application/xml"' and an 'Add a filter +' button. The main data area is titled 'Files - Logs' and contains a table of log entries. The first entry is highlighted with a yellow background and has the event type 'bro\_files' shown in a yellow box. The table columns include event\_type, file\_ip, fuid, host, ips, is\_orig, local\_orig, md5, message, mimetype, missing\_bytes, overflow\_bytes, port, seen\_bytes, sha1, source, source\_ips, syslog-facility, and syslog-file\_name.

event_type	file_ip	fuid	host	ips	is_orig	local_orig	md5	message	mimetype	missing_bytes	overflow_bytes	port	seen_bytes	sha1	source	source_ips	syslog-facility	syslog-file_name
bro_files	209.165.201.17	FFRuizivIHRerrgBd	gateway	209.165.200.235,	true	true	56ceda5bb5c4c6be9ea6f16e86ab676f	{"ts":"2020-05-10T21:20:56.997512Z","fuid":"FFRuizivIHRerrgBd","tx_hosts":["209.165.201.17"],"rx_hosts":["209.165.200.235"],"conn_uids":["CQ4no3728pyV39ZVe"],"source":"HTTP","depth":0,"analyzers":["SHA1","MD5"],"mime_type":"application/xml","duration":0.0,"local_orig":true,"is_orig":true,"seen_bytes":714,"total_bytes":714,"missing_bytes":0,"overflow_bytes":0,"timeout":false,"md5":"56ceda5bb5c4c6be9ea6f16e86ab676f","sha1":"e4541e67581c859a6782c3492cb22da2ab2cf1c"}	application/xml	0B	0B	38524	714B	e4541e67581c859a6782c3492cb22da2ab2cf1c	HTTP		user	/nsm/bro/logs/current/files.log

# Lab - Regular Expression Tutorial

In this lab, you will complete the following objectives:

- Use an online tutorial to explore regular expressions.
- Describe the information that matches given regular expressions.

## Lab - Extract an Executable from a PCAP

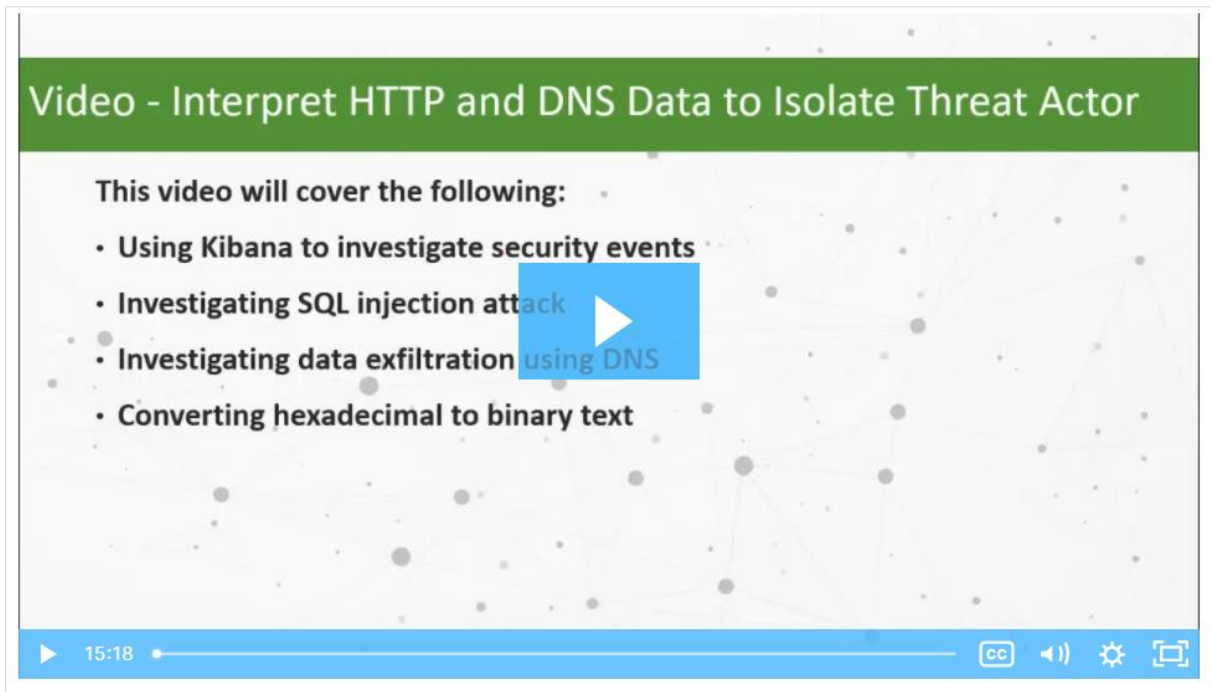
Looking at logs is very important, but it is also important to understand how network transactions happen at the packet level.

In this lab, you will complete the following objective:

- Analyze the traffic in a previously captured pcap file and extract an executable file from the traffic.

# Video - Interpret HTTP and DNS Data to Isolate Threat Actor

Watch the video to view a walkthrough of the Security Onion Interpret HTTP and DNS Data to Isolate Threat Actor lab.



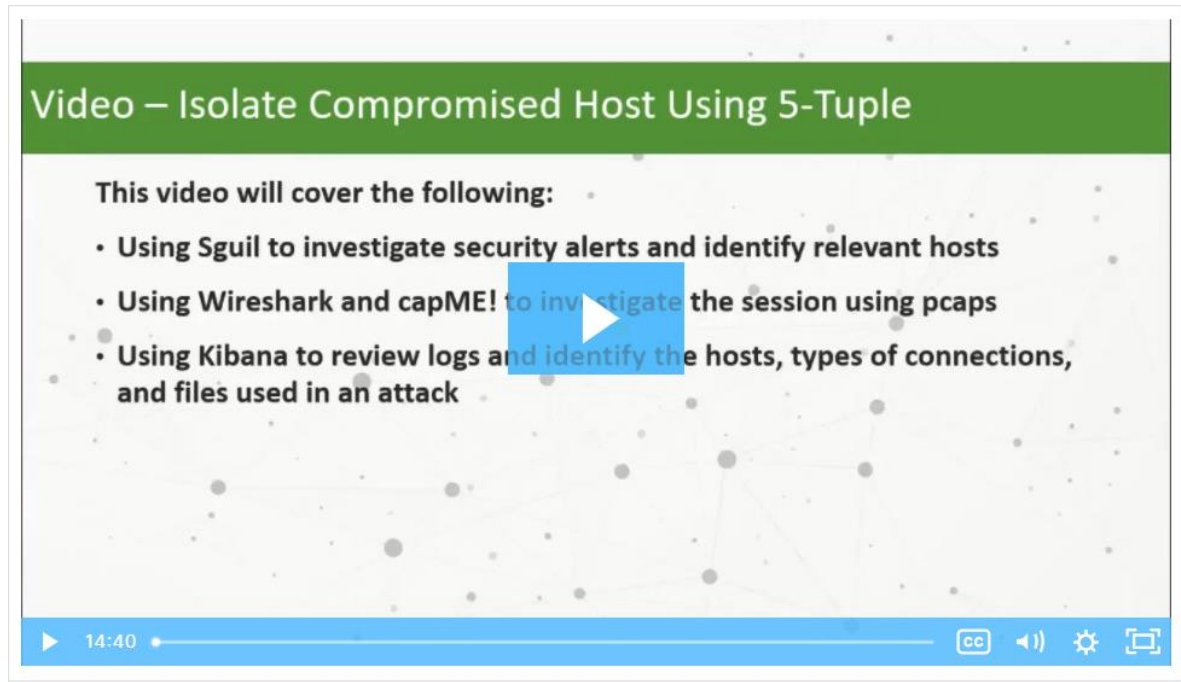
## Lab - Interpret HTTP and DNS Data to Isolate Threat Actor

In this lab, you will complete the following objective:

- Investigate SQL injection and DNS exfiltration exploits using Security Onion tools.

## Video - Isolate Compromised Host Using 5-Tuple

Watch the video to view a walkthrough of the Security Onion Isolate Compromised Host Using 5-Tuple lab.



# Lab - Isolate Compromised Host Using 5-Tuple

In this lab, you will complete the following objective:

- Use Security Onion tools to investigate an exploit.

## Lab - Investigate a Malware Exploit

In this lab, you will complete the following objective:

- Use Security Onion to investigate a more complex malware exploit the uses an exploit kit to infect hosts.



# Lab - Investigating an Attack on a Windows Host

In this lab, you will complete the following objectives:

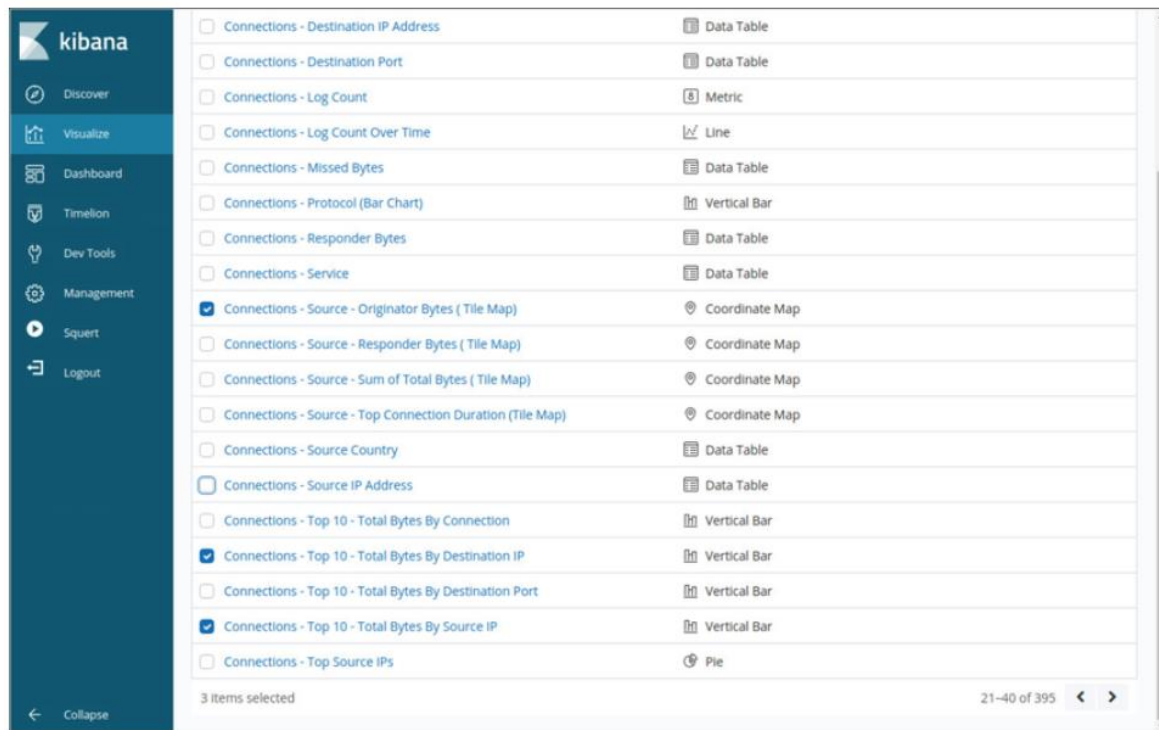
- Investigate an attack on a Windows host.
- Use Sguil, Kibana, and Wireshark in Security Onion to investigate the attack.
- Examine exploit artifacts.

# 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.



# 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.

