



# 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.

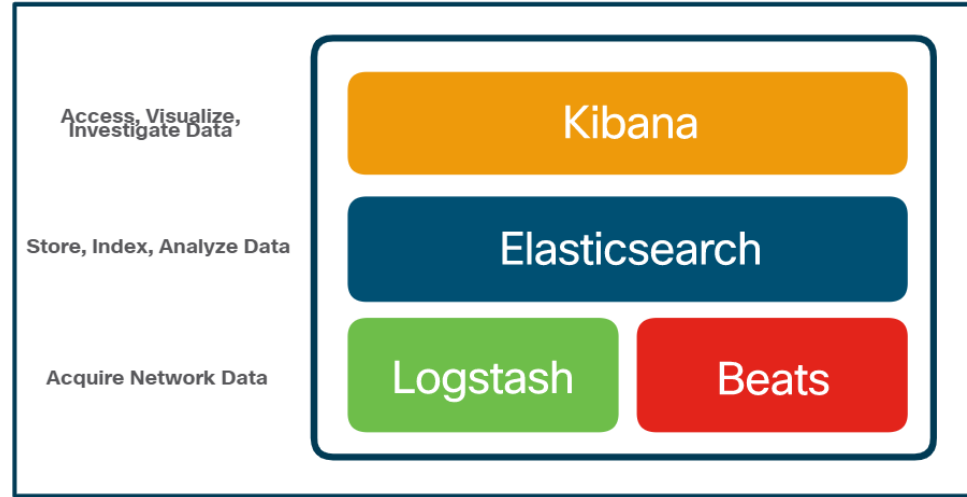
# 27.1 A Common Data Platform

# ELK

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

### Core Components of ELK:

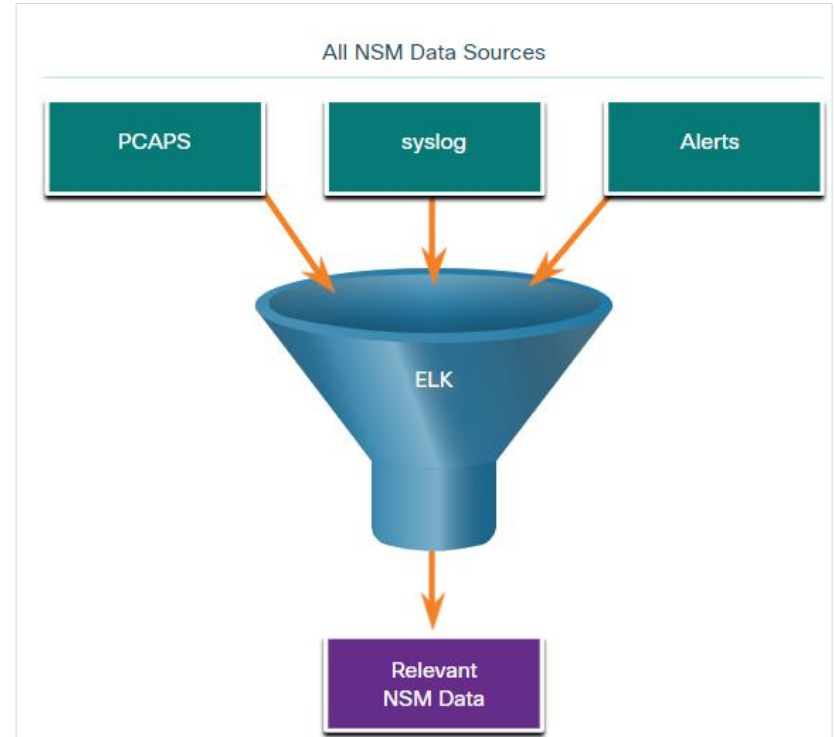
- **Elasticsearch:** An open-core platform for searching and analyzing an organization's data in near real time.
- **Logstash:** Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch.
- **Kibana:** Provides a graphical interface to data 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:

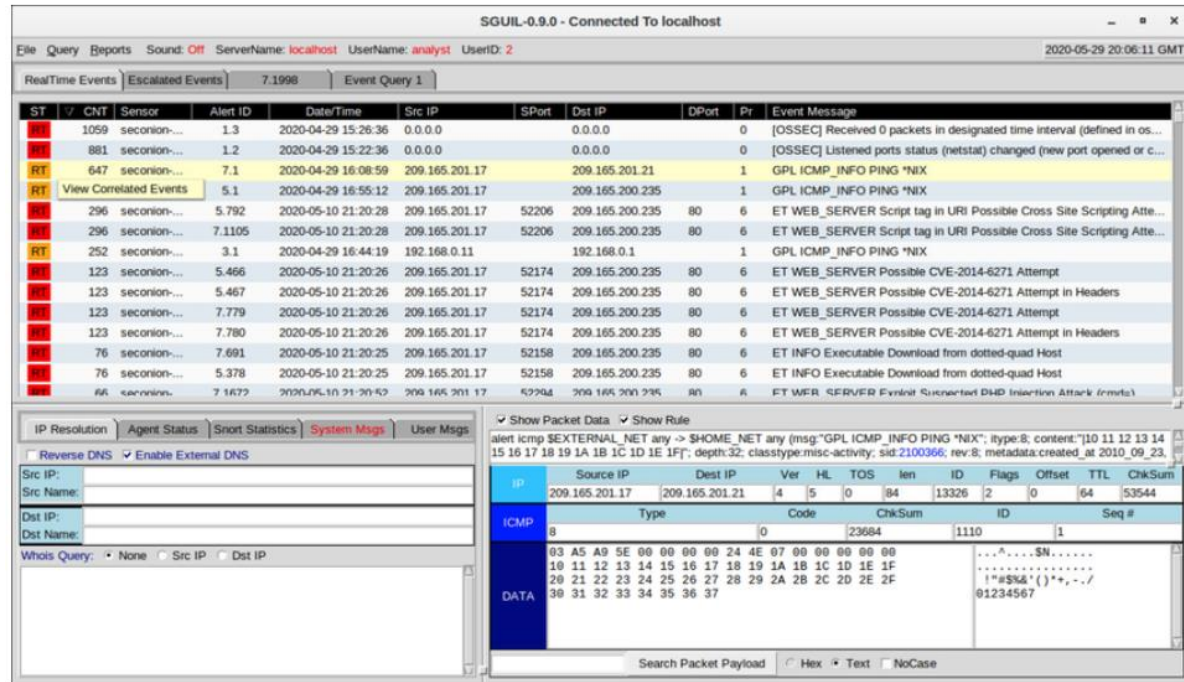
- **Part 1:** Use command line tools to manually normalize log entries.
- **Part 2:** The timestamp field must be normalized.
- **Part 3:** The IPv6 field requires normalization.



# 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 columns include ST, CNT, Sensor, Alert ID, DateTime, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The alerts are sorted by CNT, with the highest count (1672) at the bottom.

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	5.1	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 packet details pane shows the following information:

- IP Resolution: ☐ Reverse DNS ☒ Enable External DNS
- Src IP: 209.165.201.17
- Src Name: 209.165.201.17
- Dst IP: 209.165.201.21
- Dst Name: 209.165.201.21
- Whos Query: ☐ None ☐ Src IP ☐ Dst IP
- Show Packet Data: ☒ Show Rule
- Alert icmp \$EXTERNAL\_NET any -> \$HOME\_NET any (msg:"GPL ICMP\_INFO PING \*NIX"; type:s; content:"110 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F"; depth:32; classtype:misc-activity; sid:2100366; rev:8; metadata:created\_at 2010\_09\_23;
- IP: 209.165.201.17
- Source IP: 209.165.201.17
- Dest IP: 209.165.201.21
- Ver: 4
- HL: 5
- TOS: 0
- len: 84
- ID: 13326
- Flags: 2
- Offset: 0
- TTL: 64
- ChkSum: 53544
- ICMP: 8
- Type: 0
- Code: 23684
- ChkSum: 1110
- ID: 1
- Seq #: 1
- DATA: 03 A5 A9 5E 00 00 00 00 24 4E 07 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37

## 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.

The screenshot displays the Sguil-6.9.0 interface, which is connected to localhost. The top section shows a query result for 'Event Query 9'. The query is: `SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.id, 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`. The results table has columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. It lists several events related to Nmap SQL Spider Scans and User-Agent detection.

The bottom section shows the 'System Msgs' tab with a table of system messages. The table has columns: Sid, Net, Hostname, Type, and Last. It lists messages from sensors like seconion-eth0 and seconion-eth1.

Below the system messages, there is a 'Show Packet Data' section. It displays a packet capture for a TCP connection from 209.165.201.17 to 209.165.200.235 on port 80. The packet is a GET request for a URL related to Nmap SQL injection. The packet details include Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, and ChkSum. 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.
- 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 51557, which is a 'Possible Magento Directory Traversal Attempt'. Below this, the 'Event History' tab is selected, showing a list of events with columns: SId, Net, Hostname, Type, and Last. The bottom section shows a detailed view of the selected event, including a 'Show Packet Data' section with a table for packet details (Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, ChkSum) and a 'Show Rule' section with a table for rule details (Source Port, Dest Port, R R R R R R R R R R, U A P R S F, Seq #, Ack #, Offset, Res, Window, Up, ChkSum).

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

# Investigating Network Data

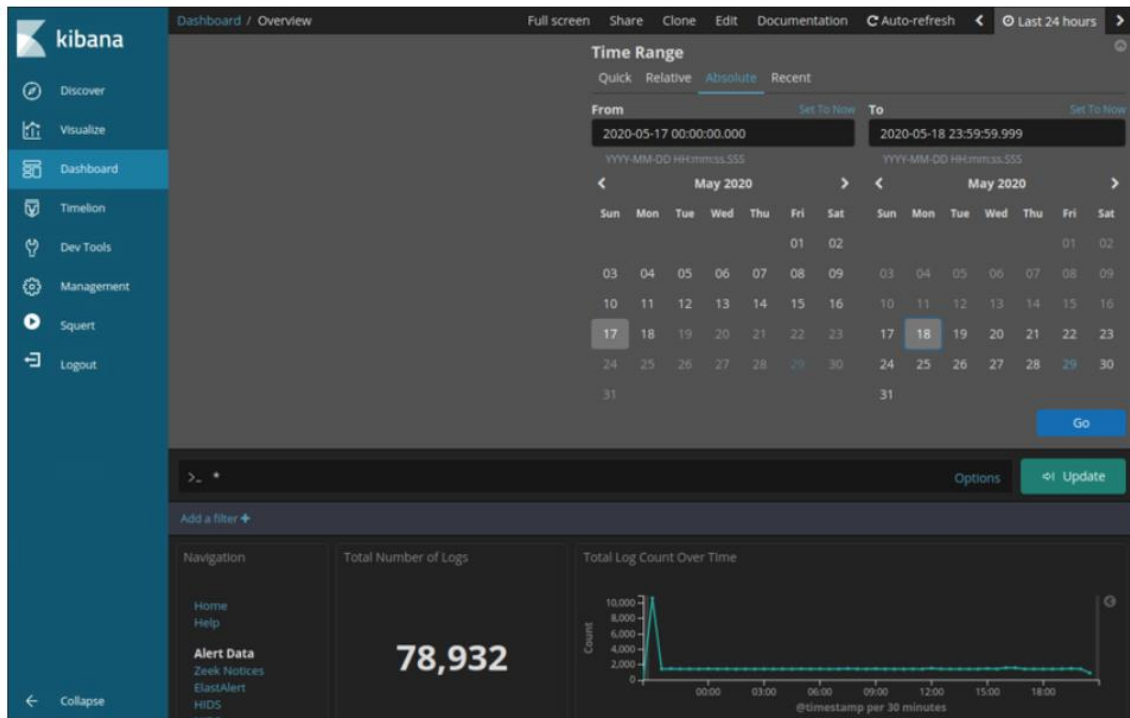
## Event Handling in Sguil

- 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 like 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 context menu is open over the table, showing options like 'Escalate (F9)', 'Cat I: Unauthorized Root Access (F1)', 'Cat I: Add Comment', 'Cat II: Unauthorized User Access (F2)', 'Cat II: Add Comment', 'Cat III: Attempted Unauthorized Access (F3)', 'Cat III: Add Comment', 'Cat IV: Successful Denial of Service Attack (F4)', 'Cat IV: Add Comment', 'Cat V: Poor Security Practice or Policy Violation (F5)', 'Cat V: Add Comment', 'Cat VI: Reconnaissance/Probes/Scans (F6)', 'Cat VI: Add Comment', 'Cat VII: Virus Infection (F7)', and 'Cat VII: Add Comment'. Below the table, there's a section for IP Resolution with columns Sid, Net, and Hostname. To the right, there's a section for Packet Data with columns Source IP, Dest IP, Ver, HL, TOS, Ien, ID, Flags, Offset, TTL, and ChkSum. The bottom of the interface has an Update Interval (secs) set to 15 and a NOW button.

# 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.





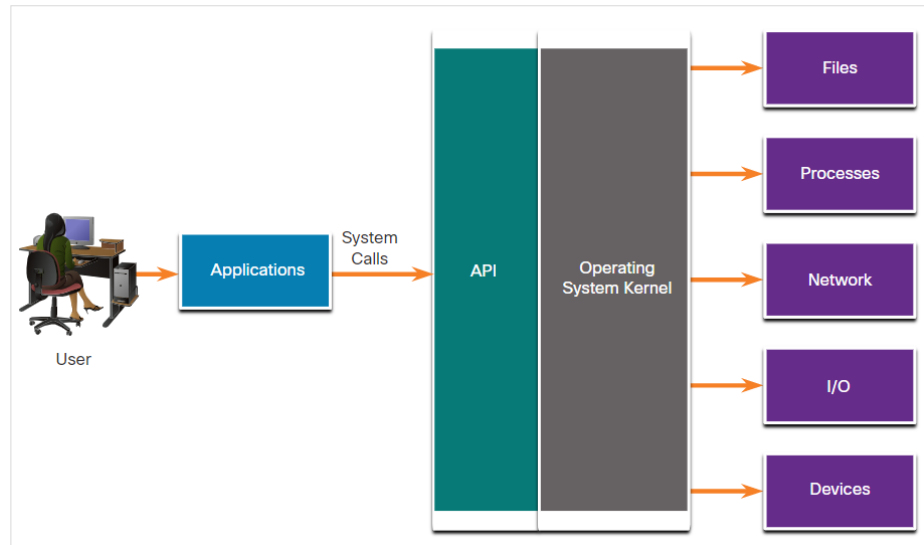
# Queries in ELK

- 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 dashboard for 'Zeek - Files'. The left sidebar shows navigation options: Discover, Visualize, Dashboard (selected), Timeline, Dev Tools, Management, Squert, and Logout. The main content area shows a search bar with the query 'mimetype.keyword:"application/xml"' and a 'Refresh' button. Below the search bar, the 'Files - Logs' section displays a list of file details. The 'event\_type' is highlighted as 'bro\_files'. Other details include 'file\_ip' (209.165.201.17), 'fuid' (FFRuizivIHRerrgBd), 'host' (gateway), 'ips' (209.165.200.235), 'is\_orig' (true), 'local\_orig' (true), 'md5' (56ceda5bb5c4c6be9ea6f16e86ab676f), and 'message' (a JSON object containing file metadata). The 'mimetype' is 'application/xml'. Other fields like 'missing\_bytes', 'overflow\_bytes', 'port', 'seen\_bytes', 'sha1', 'source', 'source\_ips', 'syslog-facility', and 'syslog-file\_name' are also listed.

Field	Value
event_type	bro_files
file_ip	209.165.201.17
fuid	FFRuizivIHRerrgBd
host	gateway
ips	209.165.200.235,
is_orig	true
local_orig	true
md5	56ceda5bb5c4c6be9ea6f16e86ab676f
message	{"ts":"2020-05-10T21:20:56.997512Z","fuid":"FFRuizivIHRerrgBd","tx_hosts":["209.165.201.17"],"rx_hosts":["209.165.200.235"],"conn_uids":["CQJqno37Z8pyV39ZVe"],"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"}
mimetype	application/xml
missing_bytes	0B
overflow_bytes	0B
port	38524
seen_bytes	714B
sha1	e4541e67581c859a6782c3492cb22da2ab2cf1c
source	HTTP
source_ips	*
syslog-facility	user
syslog-file_name	/nsn/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

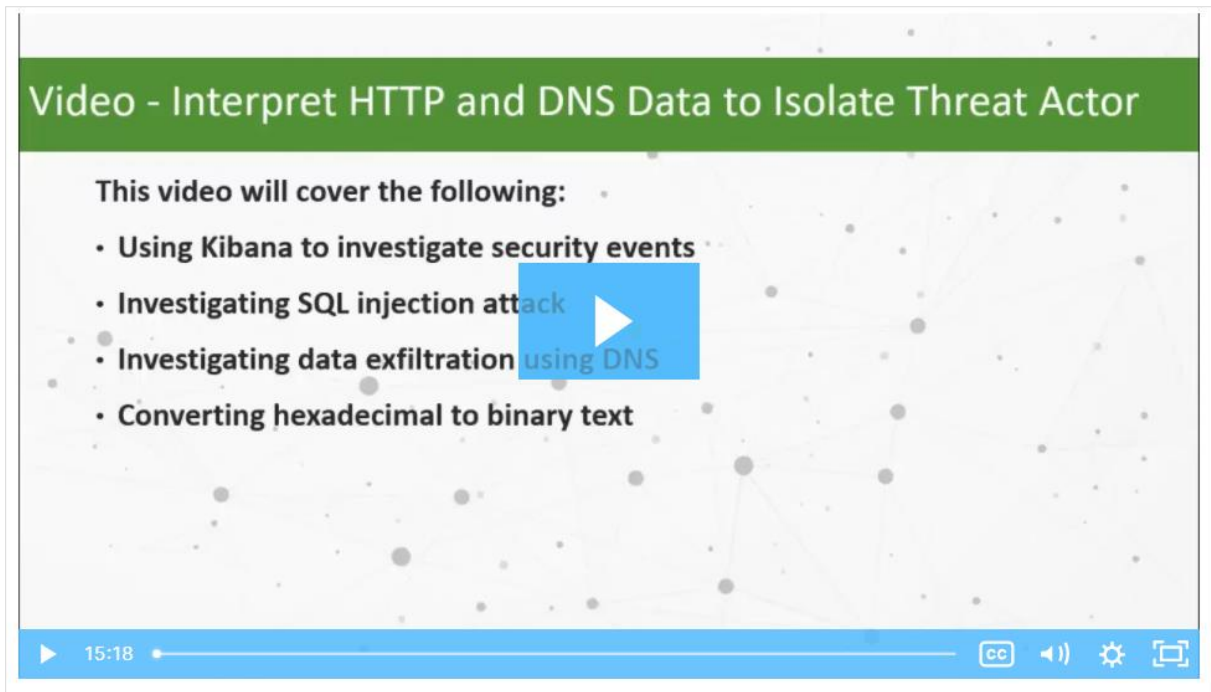
Looking at logs is very important, but it is also important to understand how network transactions happen at the packet level.

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.



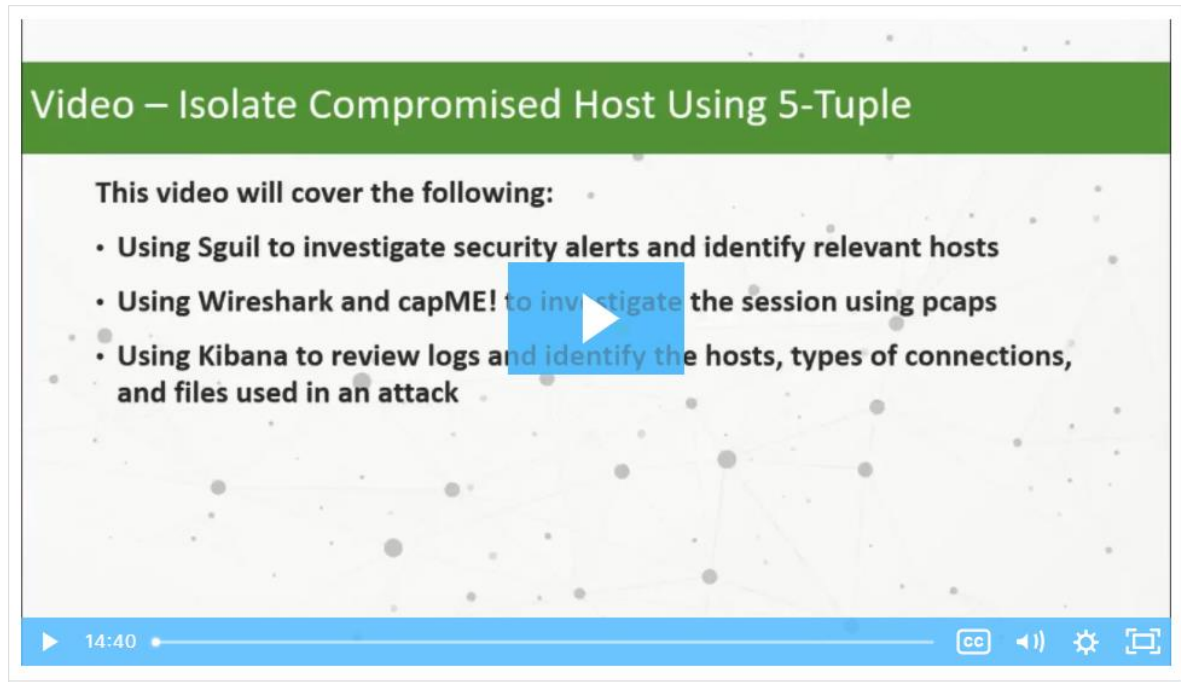
## Lab - Interpret HTTP and DNS Data to Isolate Threat Actor

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:

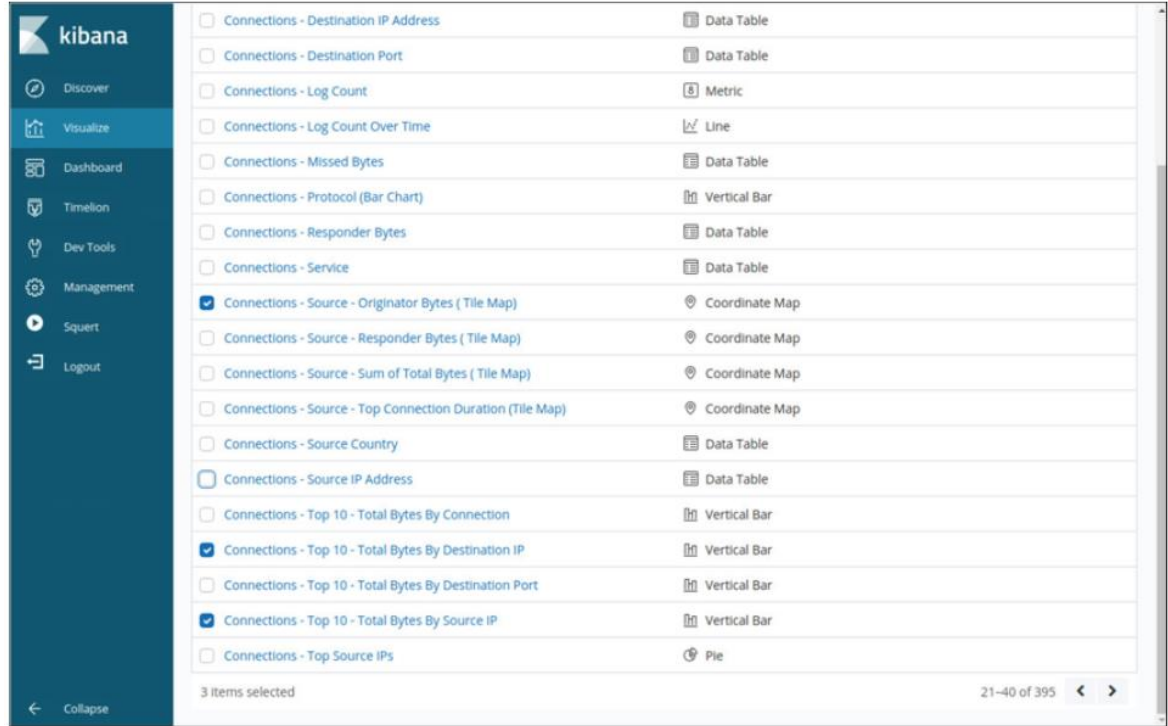
- Investigate an attack on a Windows host.
- Use Sguil, Kibana, and Wireshark in Security Onion to investigate the attack.
- Examine exploit artifacts.

# 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.

