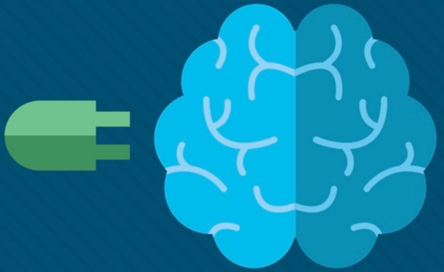


Chapter 10: Intrusion Data Analysis

Information Security

Dr. Ayman Aljarbouh

10.2 Working with Network Security Data

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.

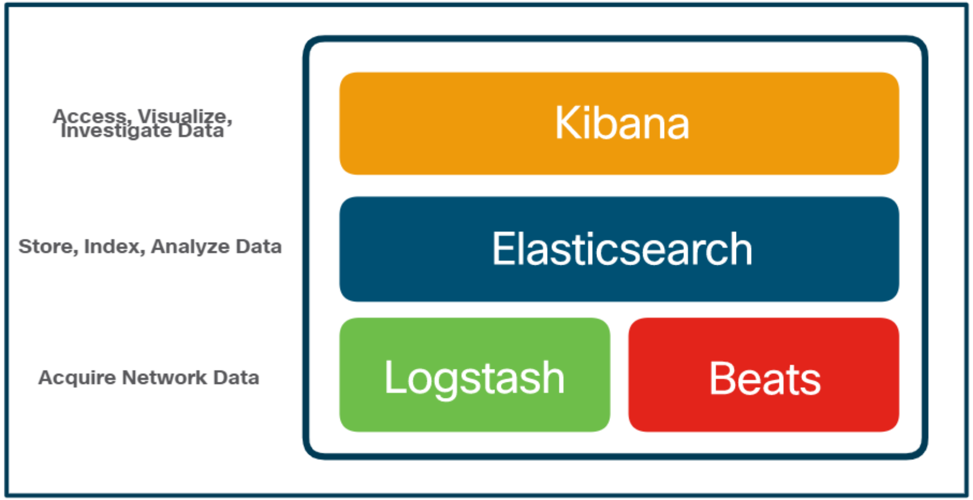
A Common Data Platform

ELK

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

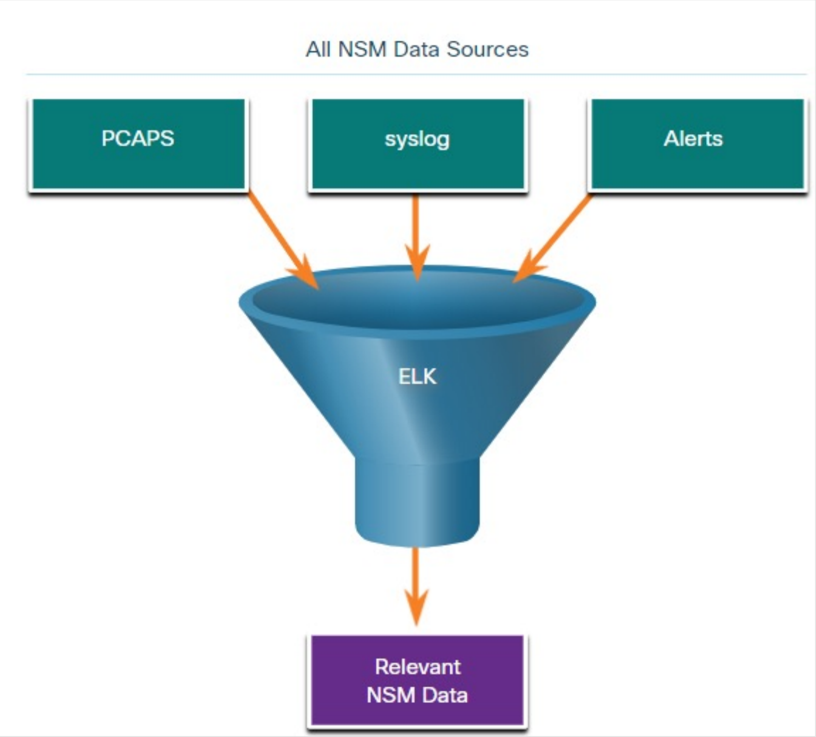
Core Components of ELK:

- **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.


Access, Visualize, Investigate Data
Kibana
Store, Index, Analyze Data
Elasticsearch
Acquire Network Data
Logstash
Beats

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.



A Common Data Platform

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.

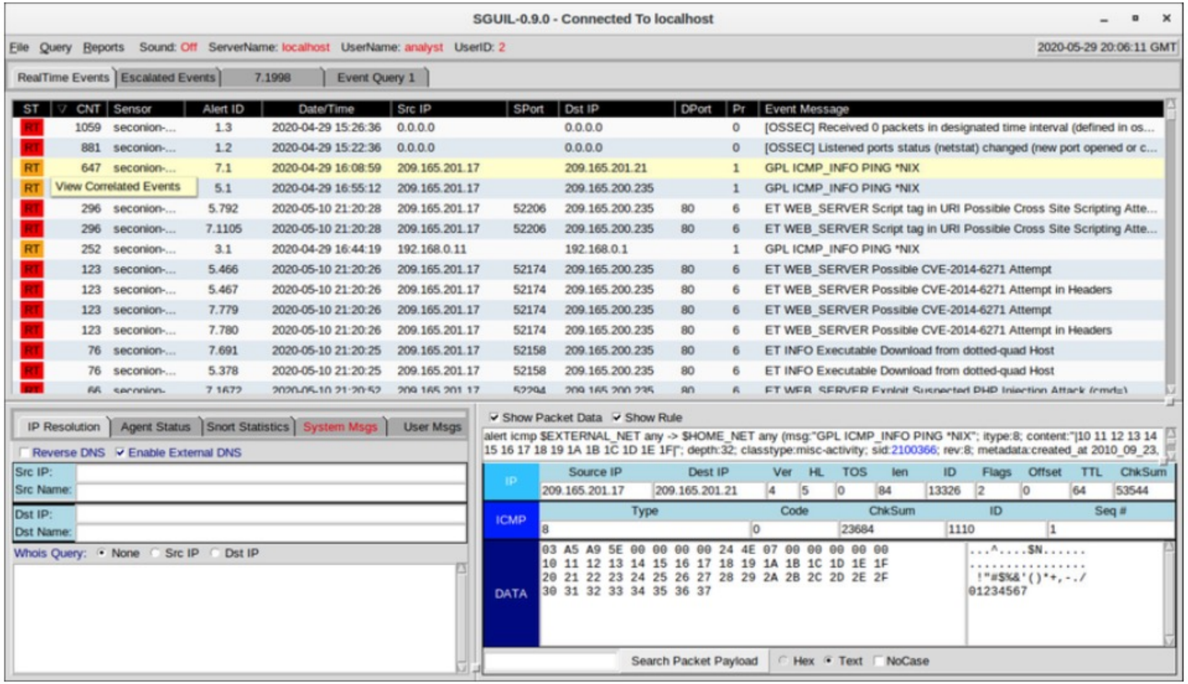
A Common Data Platform

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.

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.



Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-05-29 20:06:11 GMT

ST	▽ CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	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...
RT	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	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
RT	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...
RT	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
RT	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
RT	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
RT	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
RT	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
RT	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
RT	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
RT	66	seconion-...	7.1672	2020-05-10 21:20:52	209.165.201.17	52294	209.165.200.235	80	6	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)

□ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois 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"; itype:8; content:"|10 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	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.201.17	209.165.201.21	4	5	0	84	13326	2	0	64	53544

ICMP	Type	Code	ChkSum	ID	Seq #
	8	0	23684	1110	1

DATA

```
03 A5 A9 5E 00 00 00 00 24 4E 07 00 00 00 00 00   ...^....$N......
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F   ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F    !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                           01234567
```

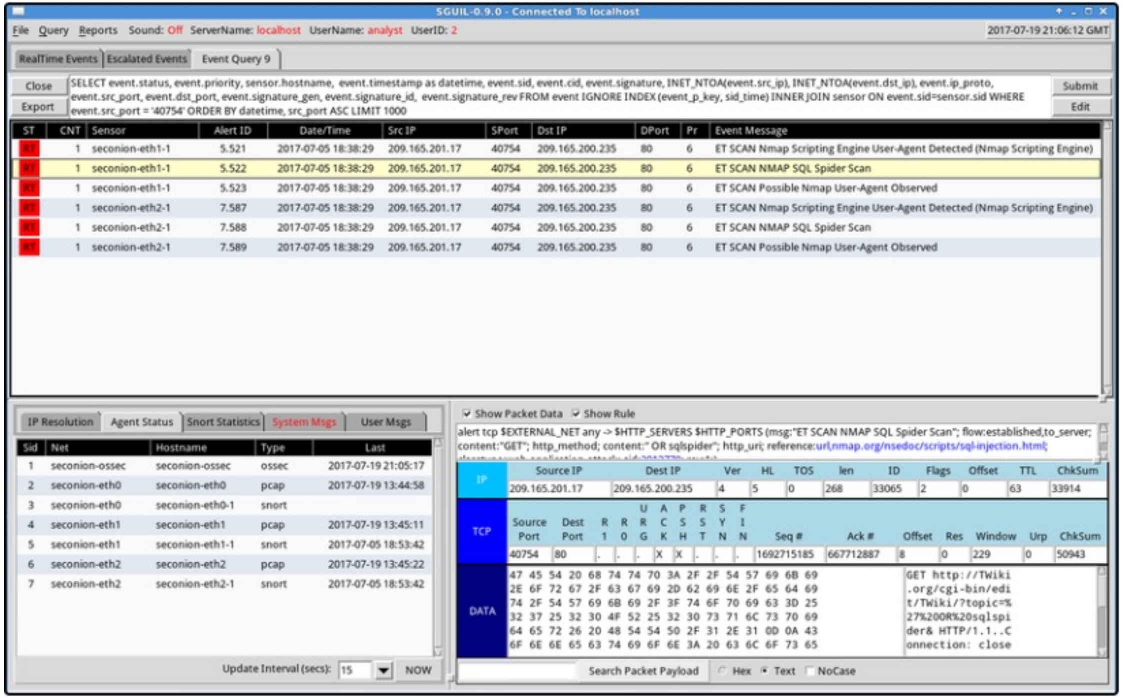
○ Hex ● Text □ NoCase

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.



```
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
```

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	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)
RT	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
RT	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
RT	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)
RT	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
RT	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

Sid	Net	Hostname	Type	Last
1	seconion-ossec	seconion-ossec	ossec	2017-07-19 21:05:17
2	seconion-eth0	seconion-eth0	pcap	2017-07-19 13:44:58
3	seconion-eth0	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

```
alert tcp $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_uri; reference:url,nmap.org/nsedoc/scripts/sql-injection.html;
```

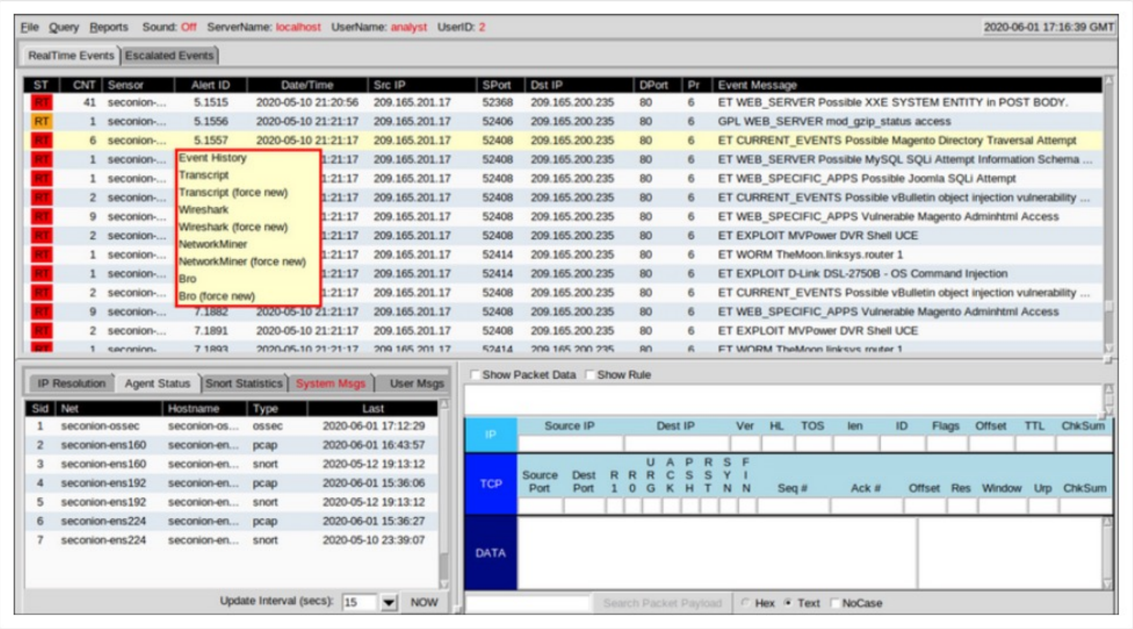
Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
209.165.201.17	209.165.200.235	4	5	0	268	33065	2	0	63	33914

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
40754	80	.	.	.	X	X	.	.	.	1692715185	667712887	8	0	229	0	50943

```
47 45 54 20 68 74 74 70 3A 2F 2F 54 57 69 6B 69    GET http://TWiki
2E 6F 72 67 2F 63 67 69 2D 62 69 6E 2F 65 64 69    .org/cgi-bin/edi
74 2F 54 57 69 6B 69 2F 3F 74 6F 70 69 63 3D 25    t/TWiki/?topic=%
32 37 25 32 30 4F 52 25 32 30 73 71 6C 73 70 69    27%20OR%20sqlspi
64 65 72 26 20 48 54 54 50 2F 31 2E 31 0D 0A 43    der& HTTP/1.1..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65    onnection: close
```

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.



Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-06-01 17:16:39 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	41	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-...		1:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema ...
RT	1	seconion-...		:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS Possible Joomla SQLi Attempt
RT	2	seconion-...		1:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET CURRENT_EVENTS Possible vBulletin object injection vulnerability ...
RT	9	seconion-...		:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access
RT	2	seconion-...		1:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET EXPLOIT MVPower DVR Shell UCE
RT	1	seconion-...		:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1
RT	1	seconion-...		1:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET EXPLOIT D-Link DSL-2750B - OS Command Injection
RT	2	seconion-...		:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET CURRENT_EVENTS Possible vBulletin object injection vulnerability ...
RT	9	seconion-...	7.1882	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access
RT	2	seconion-...	7.1891	2020-05-10 21:21:17	209.165.201.17	52408	209.165.200.235	80	6	ET EXPLOIT MVPower DVR Shell UCE
RT	1	seconion-	7.1893	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1

Sid	Net	Hostname	Type	Last
1	seconion-ossec	seconion-os...	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

Update Interval (secs): 15

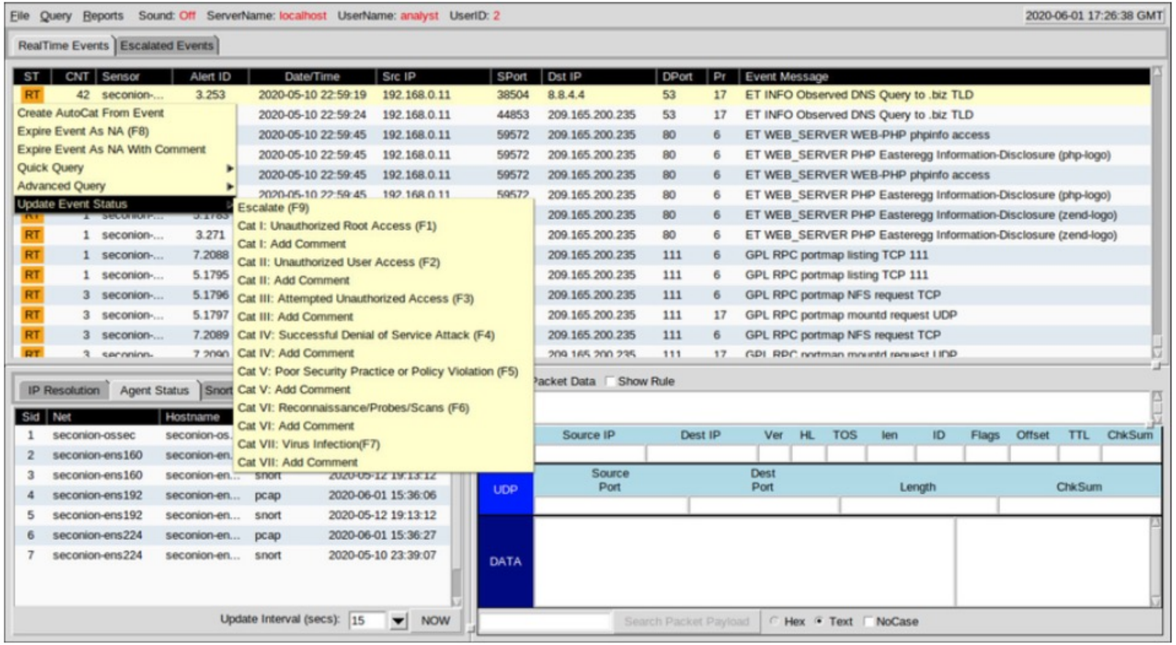
Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum

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

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 Squil 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.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	42	seconion-...	3.253	2020-05-10 22:59:19	192.168.0.11	38504	8.8.4.4	53	17	ET INFO Observed DNS Query to .biz TLD
				2020-05-10 22:59:24	192.168.0.11	44853	209.165.200.235	53	17	ET INFO Observed DNS Query to .biz TLD
				2020-05-10 22:59:45	192.168.0.11	59572	209.165.200.235	80	6	ET WEB_SERVER WEB-PHP phpinfo access
				2020-05-10 22:59:45	192.168.0.11	59572	209.165.200.235	80	6	ET WEB_SERVER PHP Easteregg Information-Disclosure (php-logo)
				2020-05-10 22:59:45	192.168.0.11	59572	209.165.200.235	80	6	ET WEB_SERVER WEB-PHP phpinfo access
				2020-05-10 22:59:45	192.168.0.11	59572	209.165.200.235	80	6	ET WEB_SERVER PHP Easteregg Information-Disclosure (php-logo)
							209.165.200.235	80	6	ET WEB_SERVER PHP Easteregg Information-Disclosure (zend-logo)
RT	1	seconion-...	3.271				209.165.200.235	80	6	ET WEB_SERVER PHP Easteregg Information-Disclosure (zend-logo)
RT	1	seconion-...	7.2088				209.165.200.235	111	6	GPL RPC portmap listing TCP 111
RT	1	seconion-...	5.1795				209.165.200.235	111	6	GPL RPC portmap listing TCP 111
RT	3	seconion-...	5.1796				209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-...	5.1797				209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	3	seconion-...	7.2089				209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-	7.2090				209.165.200.235	111	17	GPL RPC portmap mountd request UDP

Sid	Net	Hostname		
1	seconion-ossec	seconion-os...		
2	seconion-ens160	seconion-en...		
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

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum

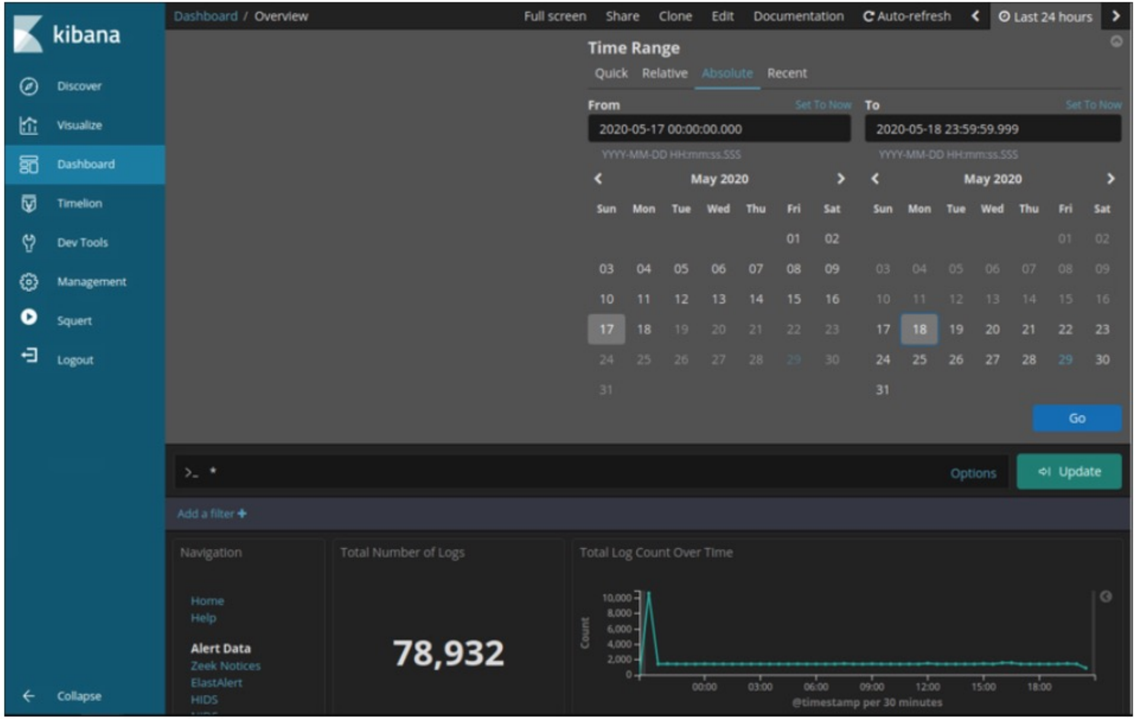
Source Port	Dest Port	Length	ChkSum

- 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.



Time Range

From: 2020-05-17 00:00:00.000

To: 2020-05-18 23:59:59.999

>_ *

Navigation

Alert Data

Total Number of Logs: 78,932

Total Log Count Over Time

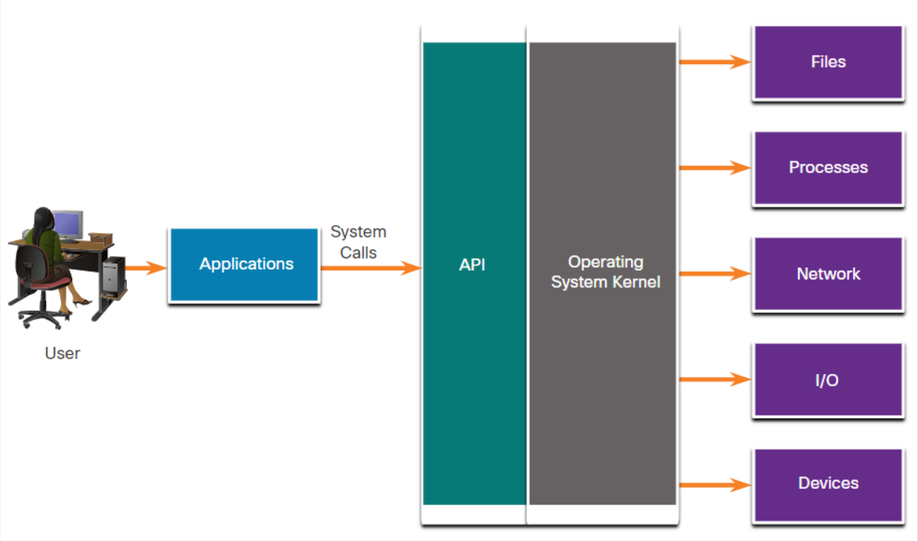
Queries in ELK

- 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

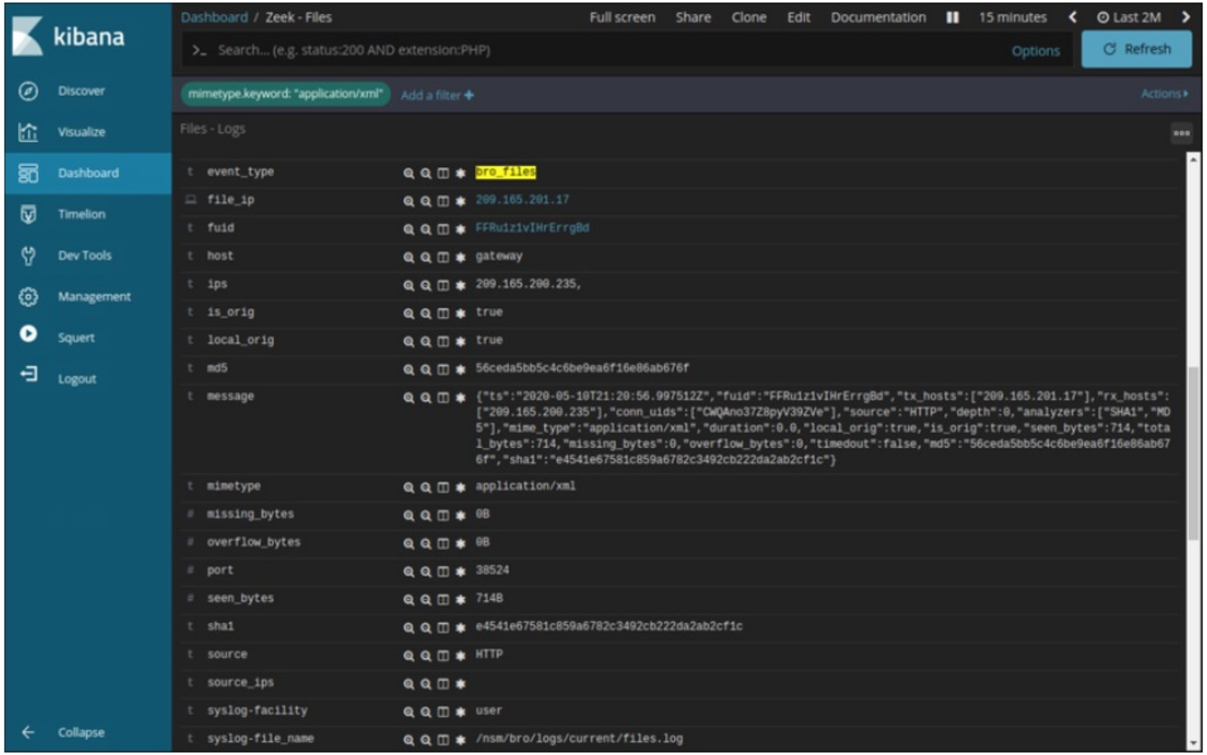
- Applications interact with an Operating System (OS) through system calls to the OS Application Programming Interface (API).
- If malware can fool an OS kernel into allowing it to make system calls, many exploits are possible.
- OSSEC rules detect changes in host-based parameters.
- OSSEC rules will 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 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.



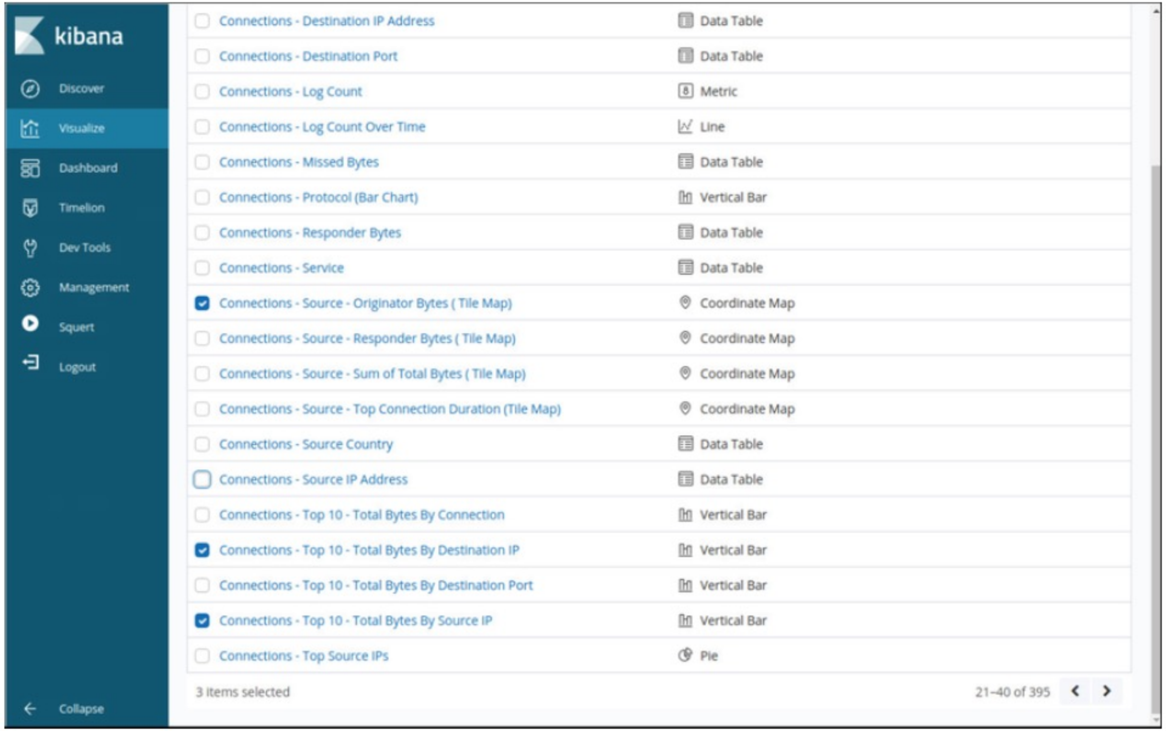
Files - Logs

```
t  event_type          bro_files
   file_ip             209.165.201.17
t  fuid                FFRu1z1vIHrErrgBd
t  host                gateway
t  ips                 209.165.200.235,
t  is_orig             true
t  local_orig          true
t  md5                 56ceda5bb5c4c6be9ea6f16e86ab676f
t  message             {"ts":"2020-05-10T21:20:56.997512Z","fuid":"FFRu1z1vIHrErrgBd","tx_hosts":["209.165.201.17"],"rx_hosts":
                       ["209.165.200.235"],"conn_uids":["CWQAno37Z8pyV39ZVe"],"source":"HTTP","depth":0,"analyzers":["SHA1","MD
                       5"],"mime_type":"application/xml","duration":0.0,"local_orig":true,"is_orig":true,"seen_bytes":714,"tota
                       l_bytes":714,"missing_bytes":0,"overflow_bytes":0,"timedout":false,"md5":"56ceda5bb5c4c6be9ea6f16e86ab67
                       6f","sha1":"e4541e67581c859a6782c3492cb222da2ab2cf1c"}
t  mimetype            application/xml
#  missing_bytes       0B
#  overflow_bytes      0B
#  port                38524
#  seen_bytes          714B
t  sha1                e4541e67581c859a6782c3492cb222da2ab2cf1c
t  source              HTTP
t  source_ips
t  syslog-facility     user
t  syslog-file_name    /nsm/bro/logs/current/files.log
```

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.



□	Connections - Destination IP Address	Data Table
□	Connections - Destination Port	Data Table
□	Connections - Log Count	Metric
□	Connections - Log Count Over Time	Line
□	Connections - Missed Bytes	Data Table
□	Connections - Protocol (Bar Chart)	Vertical Bar
□	Connections - Responder Bytes	Data Table
□	Connections - Service	Data Table
☑	Connections - Source - Originator Bytes (Tile Map)	Coordinate Map
□	Connections - Source - Responder Bytes (Tile Map)	Coordinate Map
□	Connections - Source - Sum of Total Bytes (Tile Map)	Coordinate Map
□	Connections - Source - Top Connection Duration (Tile Map)	Coordinate Map
□	Connections - Source Country	Data Table
□	Connections - Source IP Address	Data Table
□	Connections - Top 10 - Total Bytes By Connection	Vertical Bar
☑	Connections - Top 10 - Total Bytes By Destination IP	Vertical Bar
□	Connections - Top 10 - Total Bytes By Destination Port	Vertical Bar
☑	Connections - Top 10 - Total Bytes By Source IP	Vertical Bar
□	Connections - Top Source IPs	Pie

3 items selected

21-40 of 395

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.

Intrusion Data Analysis

New Terms and Commands

- Elasticsearch, Logstash, and Kibana (ELK)
- Security Onion
- Squil
- Network Security Monitoring (NSM)
- Passive Real-time Asset Detection System (PRADS)
- Security Analyst Network Connection Profiler (SANCP)
- Squert

Intrusion Data Analysis

Lab 35 - 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.

Intrusion Data Analysis

Lab 36 - 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.

Intrusion Data Analysis

Lab 37 - 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.