



PRESENTATION

Security Monitoring and Defense

Lawrence Muchilwa Graziano
SOC Manager
Silensec | CYBER RANGES

l.muchilwa@silensec.com
www.cyberranges.com
www.silensec.com

In Collaboration with
Security Brokers



About CYBER RANGES



Cyber Range
as a Service



Hosted



On Premise



Portable



silensecTM
ISO27001 Certified

bsi.



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

G & N Silensec LTD
G & N Court
41 Pafou Street
Limassol
3051
Cyprus

Holds Certificate No:

IS 616580

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The Information Security Management System applies to the provision of the Silensec CYBER RANGES products and services, information security training and consultancy services and 24/7 SOC and managed security services including the support functions of IT, Sales, Finance and Administration in accordance with the Statement of applicability, SIL_REC-008_v1.6 Date 25/06/2020.

For and on behalf of BSI:

Andrew Laurn
Andrew Laurn, EMEA Systems Certification Director

Original Registration Date: 2020-07-13
Latest Revision Date: 2020-07-27

Effective Date: 2020-07-13
Expiry Date: 2023-07-04

Page: 1 of 2



...making excellence a habit™

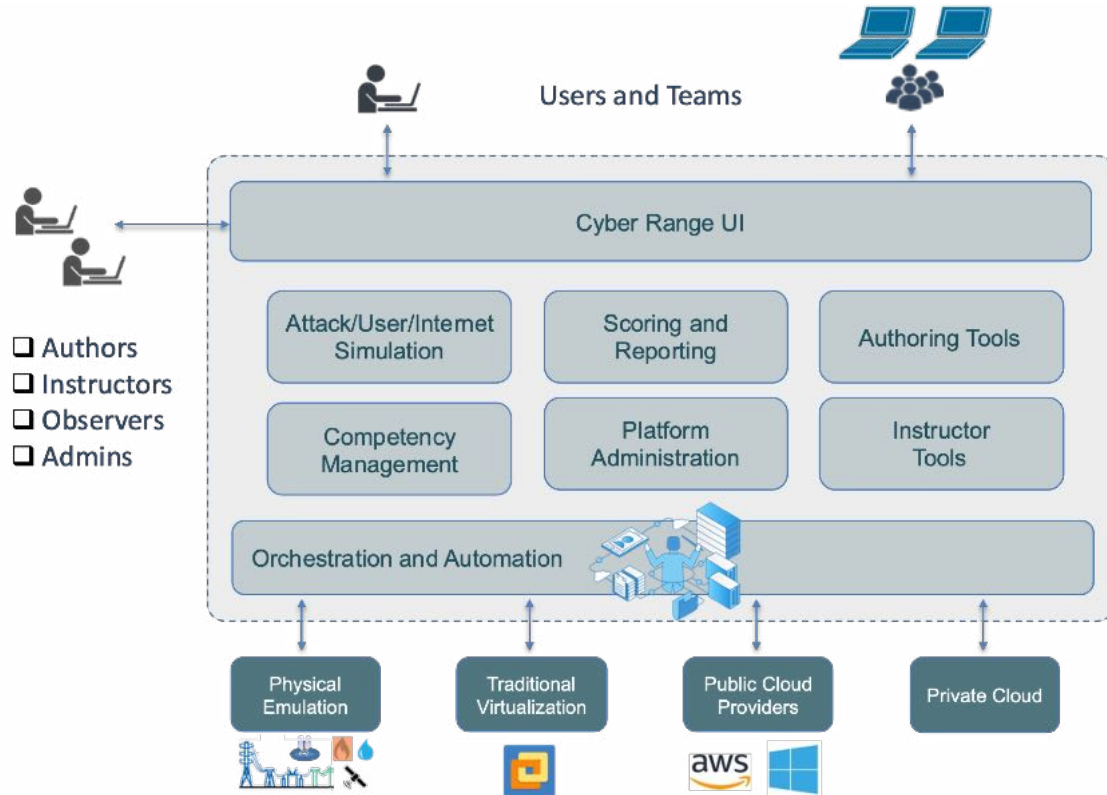
Cyprus
United Kingdom
Kenya
Canada
USA



Official platform being used by the UN for the organization of regional and national cyber drills since 2017. First ever World Cyber Drill in 2020



What is Next Generation Cyber Range



A cyber range is a platform for the development, delivery and use of interactive simulation environments.

A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon.

A cyber range includes a combination of core technologies for the creation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases.

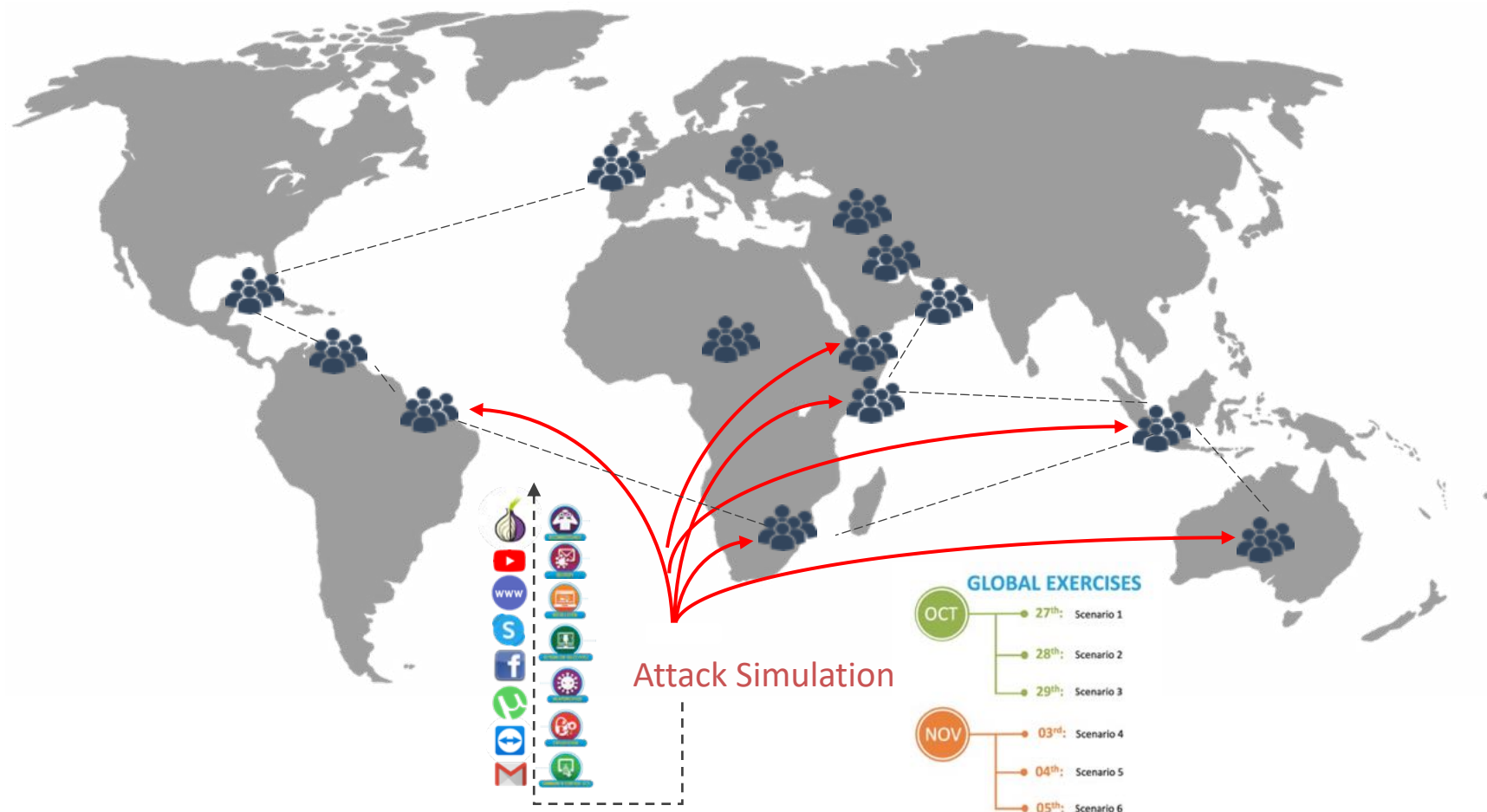
Source: EUROPEAN CYBER SECURITY ORGANIZATION (ECSO)

<https://ecs-org.eu>





Large-Scale Cyber Exercises

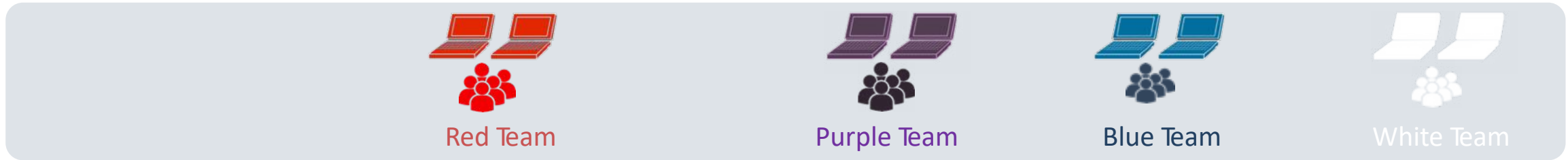
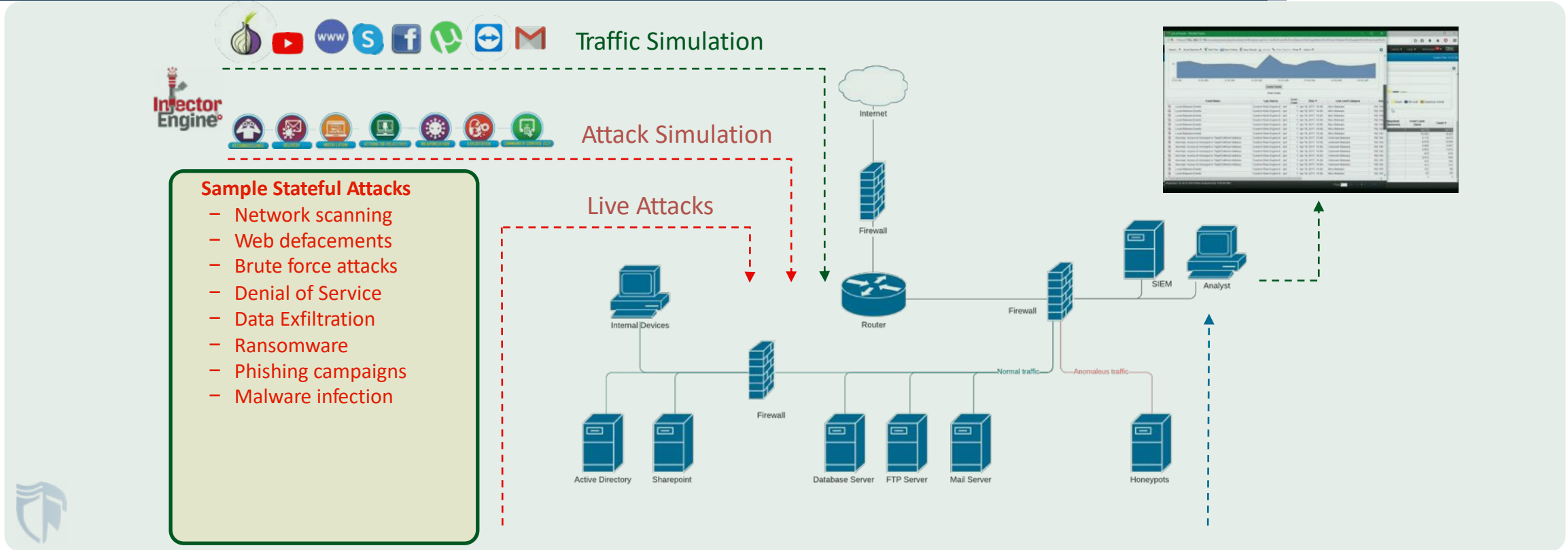


The ITU 2020 Global CyberDrill, Sep.-Nov. 2020

<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx>

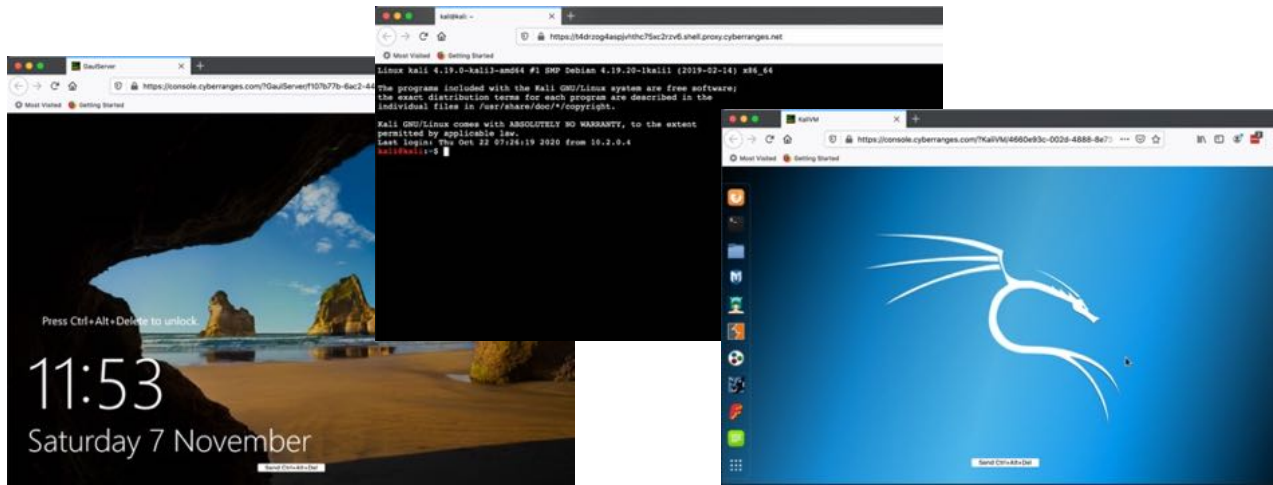


Next Generation Cyber Range Platforms

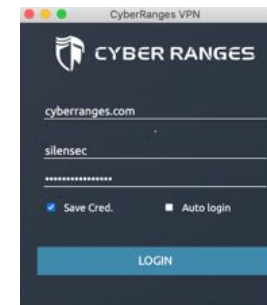




Using CYBER RANGES



In-Browser Access to the Simulation Environment



Access via VPN for for BYOD Engagements



Individual access to the VMs

OCWAR-C - Ghana session - Scenario 1



Session 1 Outline

- Windows and Linux OS logging IDS overview
- SIEMs and LMS IDS overview
- Host and Network IDS overview
- Shipping logs to ELK



Windows and Linux OS logging IDS overview

- Logs :- Application and System events being traced in a log file.
- Logs locations:
 - %SystemRoot%\System32\winevt\Logs :- Windows OS
 - Security
 - Application
 - System Logs
 - /var/log/ :- Linux Oses
 - Organized as files based on log sources eg auth, syslog
 - Logs have standard format and IDs to help you easily investigate
- Access to logs
 - Natively with EventViewer for Windows
 - Natively with Command line utilities eg Tail, Grep, Cat for Linux
 - SIEMs and LMS

- Host Intrusion Detection System
 - Mainly focused on collecting logs on each host and shipping to SIEM or LMS.
 - Will detect intrusion on the host.
 - Aggregation and correlation happens on the SIEM or LMS.
- Network Intrusion Detection System
 - Mainly focused on analyzing network traffic for intrusion detection.
 - Can be host based or Network based

- LMS :- Log Management Systems
 - Mainly focused on efficient storage, archival and searching of events.
 - Some LMS also have SIEM capabilities
- SIEMs :- Security Information and Event Management Systems
 - Mainly focused on correlation of events from various log sources.

Integrating Zeek/Bro Events to the ELK Stack



In this scenario, you will learn how to integrate Zeek/Bro events to ELK stack.

Introduction: Zeek

- Zeek is a passive, open-source network analysis framework.
- Formerly called **Bro**.
- Mostly used by security analysts as a network security monitoring (NSM) tool for the purposes of analysing and investigating suspicious network activities such as detecting SSH brute-forcing, validating SSL certificate chains etc.
- It provides an extensive set of logs describing network activity.

Introduction: Zeek

- The logs provides a comprehensive record of every activity seen on the network, HTTP sessions, DNS, DHCP, FTP, etc.
- Such security event data can be pushed to external databases or SIEM solutions to store, process, and present the data for querying.
- Zeek runs on commodity hardware and hence provides a low-cost alternative to expensive proprietary solutions.

Introduction: ELK

- ELK or Elastic Stack on the other hand is one of the top Log Management Systems (LMS).
- Incident detection and response typically begins with the collection of security data, followed by its analysis.
- ELK provides various capabilities to help IT security personnel to keep an eye on application and infrastructure performance, gather meaningful insights and make better data-driven decisions.

Introduction: ELK

- Such capabilities include:
 - Collection
 - Aggregation
 - Search and analysis
 - Monitoring and alerting

Introduction: ELK

- ELK/Elastic stack is made up of number of opensource projects;
- **Elasticsearch**: an open source, full-text search and analysis engine.
- **Logstash**: log aggregator that collects data from various input sources, transformations them stash them to various supported output destinations.
- **Kibana**: Flexible visualization tool.
- **Beats**: lightweight agents that are installed on remote hosts to collect data.

Installing ELK Stack

- In order to integrate Zeek/Bro with ELK stack, you need to have already a running ELK stack in place.
- There are different installation methods of ELK depending on the operating system of your choice.

Installing Zeek

- Once you have ELK stack installed, you can then install Zeek.
- Zeek can be installed on the network gateway depending on whether the gateway OS system supports the installation.
- Zeek can also be installed on a standalone system after which traffic is mirror to one of its interfaces.
- Zeek can then be configured to monitor the interface that provides visibility into network traffic.

Configuring Zeek

- Once you have both ELK stack and Zeek installed, you need to configure Zeek to start sending event logs ELK for visualization.
- At the very least, you will only need Kibana and Elasticsearch running on the ELK server.
- For example, you can check the status of either Kibana or Elasticsearch using the commands below;

Configuring Zeek

- Check Kibana Status
 - `systemctl status kibana`
- Check Elasticsearch Status
 - `systemctl status elasticsearch`
- Also, ensure that, from the host running Zeek, you can connect to Elasticsearch Port 9200/tcp.
- You can use telnet to confirm the connectivity to the port.
 - `telnet ES-IP 9200`

Install Filebeat on Zeek Host

- Filebeat is one of the Elastic data shippers.
- To collect Zeek events logs and push them to ELK for visualization, you need to install Filebeat.
- The installation methods for Filebeat varies from one system to another.
- Next, configure Filebeat output, which in this case is Elasticsearch output.
- **output.elasticsearch:**
- **hosts: ["localhost:9200"]**

Enable Filebeat Zeek Module

- Filebeat utilizes modules to simplify the collection, parsing, and visualization of common log formats.
- To enable Zeek Filebeat module, simply run the command below;
- `filebeat modules enable zeek`
- All modules are stored under the directory, `/etc/filebeat/modules.d/`, by default.

Collect Zeek Logs using Filebeat

- Next, you need to update the Zeek Filebeat module configuration to include all the possible Zeek log files.
- All Zeek logs are stored by default under **`/opt/zeek/logs/current/`**

Load Default Zeek Dashboards to Kibana

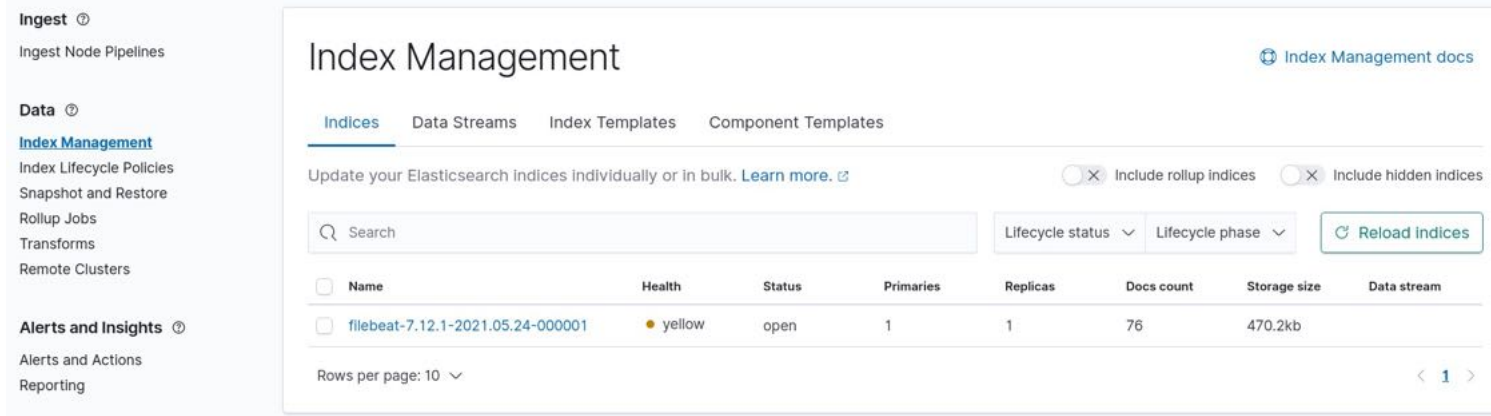
- Each Filebeat module ships with its own sample dashboards.
- To get you started, you need to load these modules on to Kibana to aid in visualizing collected event data.
- To utilize the sample visualizations, you need to create an index **filebeat-***.
- To load the modules manually, run the command below;
- **filebeat setup –dashboards**
- Restart Filebeat thereafter, **systemctl restart filebeat**.

Configure Zeek JSON Output

- You need to configure Zeek JSON output for sending to ELK.
- Stop Zeek: **zeekctl stop**
- Add the line below to Zeek config;
- `echo '@load policy/tuning/json-logs.zeek' >> /opt/zeek/share/zeek/site/local.zeek`
- Restart Zeek: **zeekctl deploy**

Create Kibana Index

- To visualize the data collected from Kibana, you need to login to Kibana interface and create an Index pattern, matching the index defined on the Filebeat Output configuration section.
- See example below;



The screenshot shows the Kibana Index Management interface. The left sidebar contains navigation options: Ingest (Ingest Node Pipelines), Data (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters), and Alerts and Insights (Alerts and Actions, Reporting). The main content area is titled 'Index Management' and includes tabs for Indices, Data Streams, Index Templates, and Component Templates. Below the tabs, there are filters for 'Include rollup indices' and 'Include hidden indices', both currently disabled. A search bar is present, along with dropdowns for 'Lifecycle status' and 'Lifecycle phase', and a 'Reload indices' button. A table displays the following index:

<input type="checkbox"/>	Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
<input type="checkbox"/>	filebeat-7.12.1-2021.05.24-000001	yellow	open	1	1	76	470.2kb	

At the bottom, it shows 'Rows per page: 10' and a pagination control for page 1.

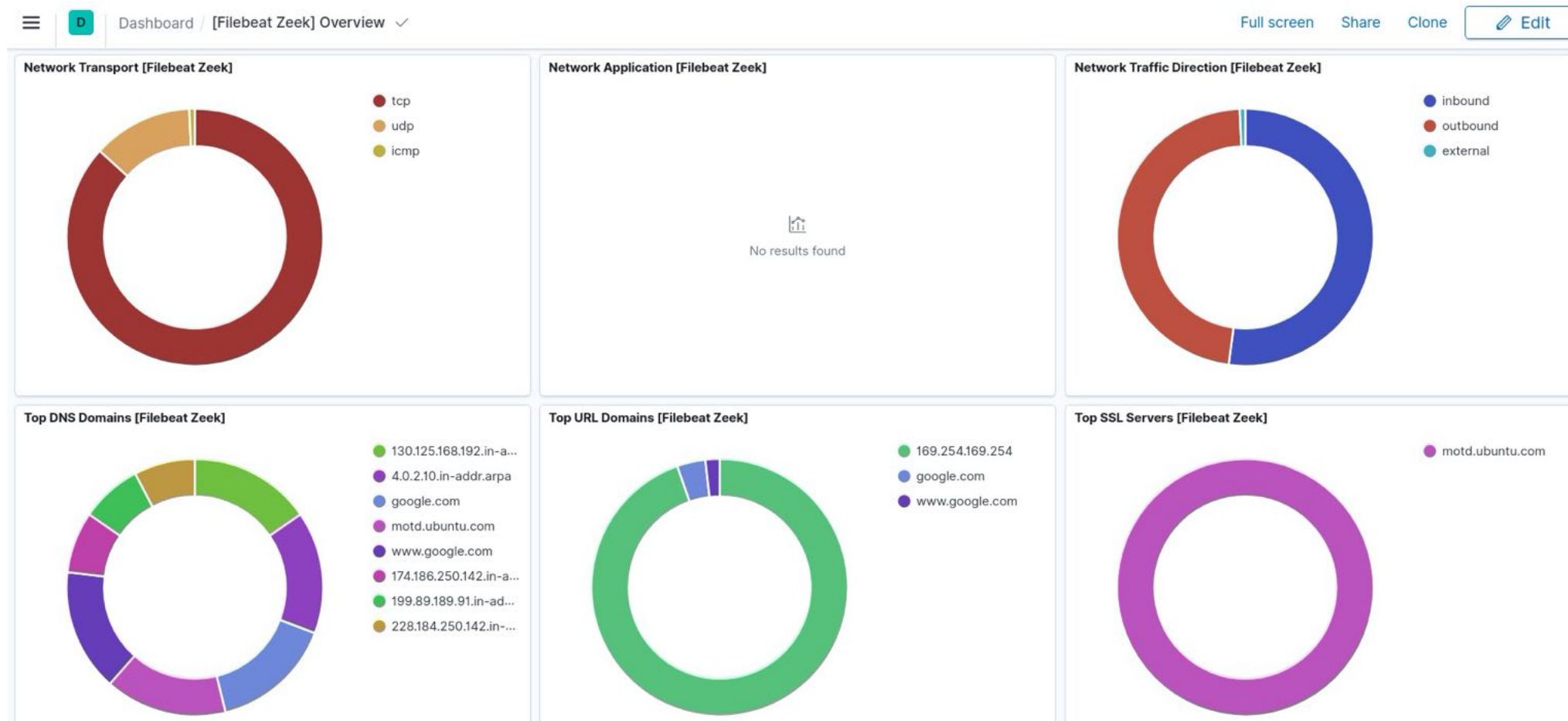
Viewing Zeek Events on Kibana

- You should now be able to view Zeek Events on ELK stack.
- Click three menu lines at the top left corner > Analytics > Discover.



Integrating Zeek/Bro Events to the ELK Stack

Sample Zeek ELK Dashboards

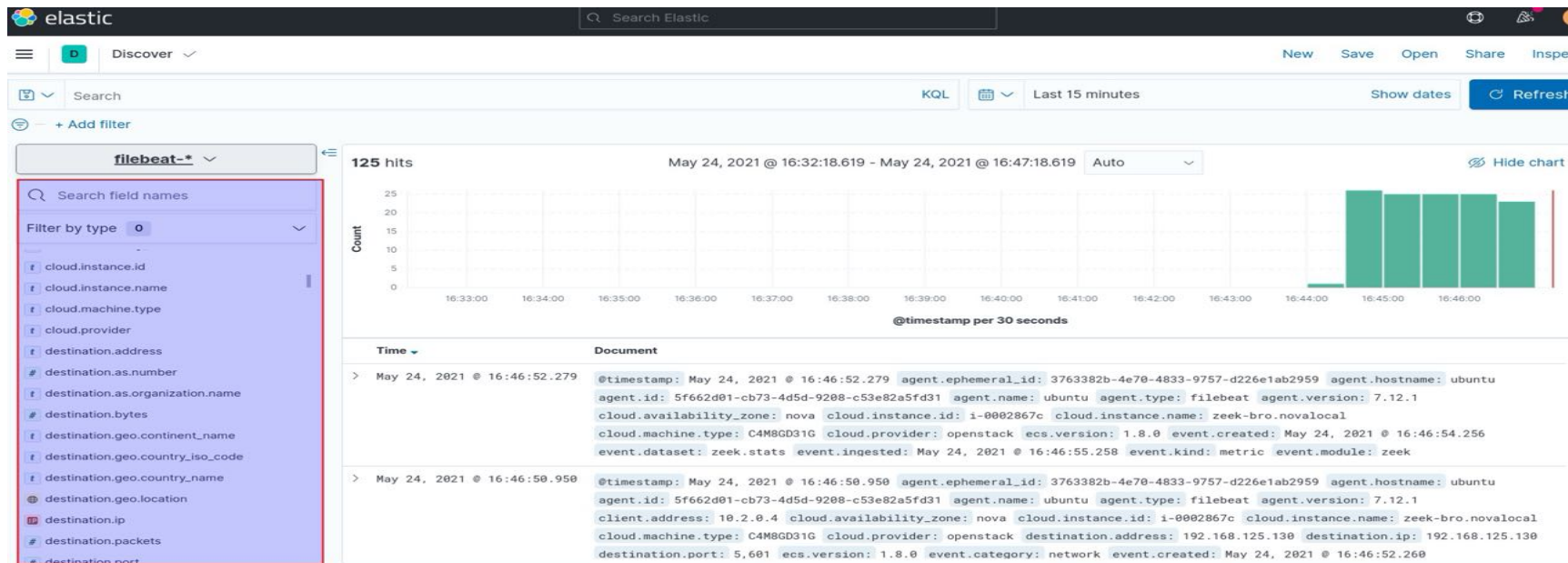




Zeek Events on ELK

Sample Zeek Events on ELK

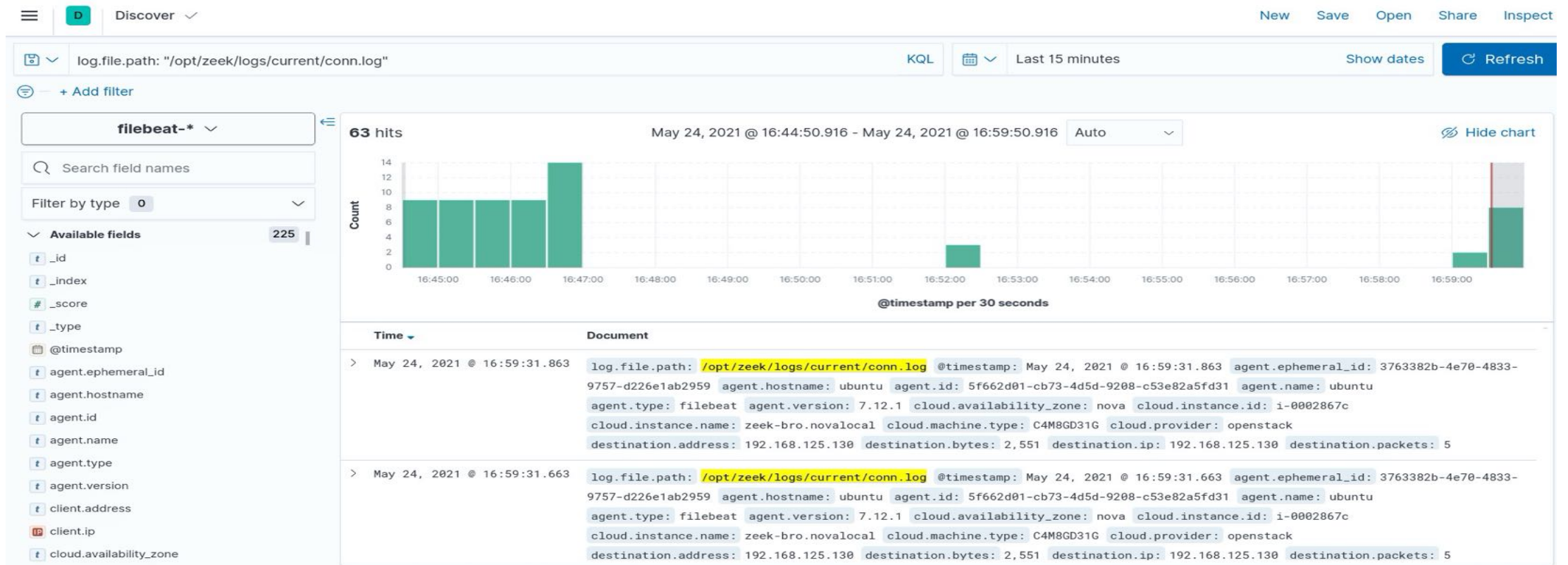
- Displays Zeek events collected from the host running Zeek.
- The events are related to traffic passing through the interface on which Zeek is configured to monitor.



Filtering Specific Zeek Events on ELK

Sample Zeek Events on ELK

- You can display specific Zeek events on ELK based on the event log files.



OCWAR-C - Ghana session - Scenario 2



Session 2 Outline

- Arkime Network Analysis Tool overview
- CyberChef Tool overview
- ELK Tool overview
- OsQuery Tool overview
- Hands on Lab

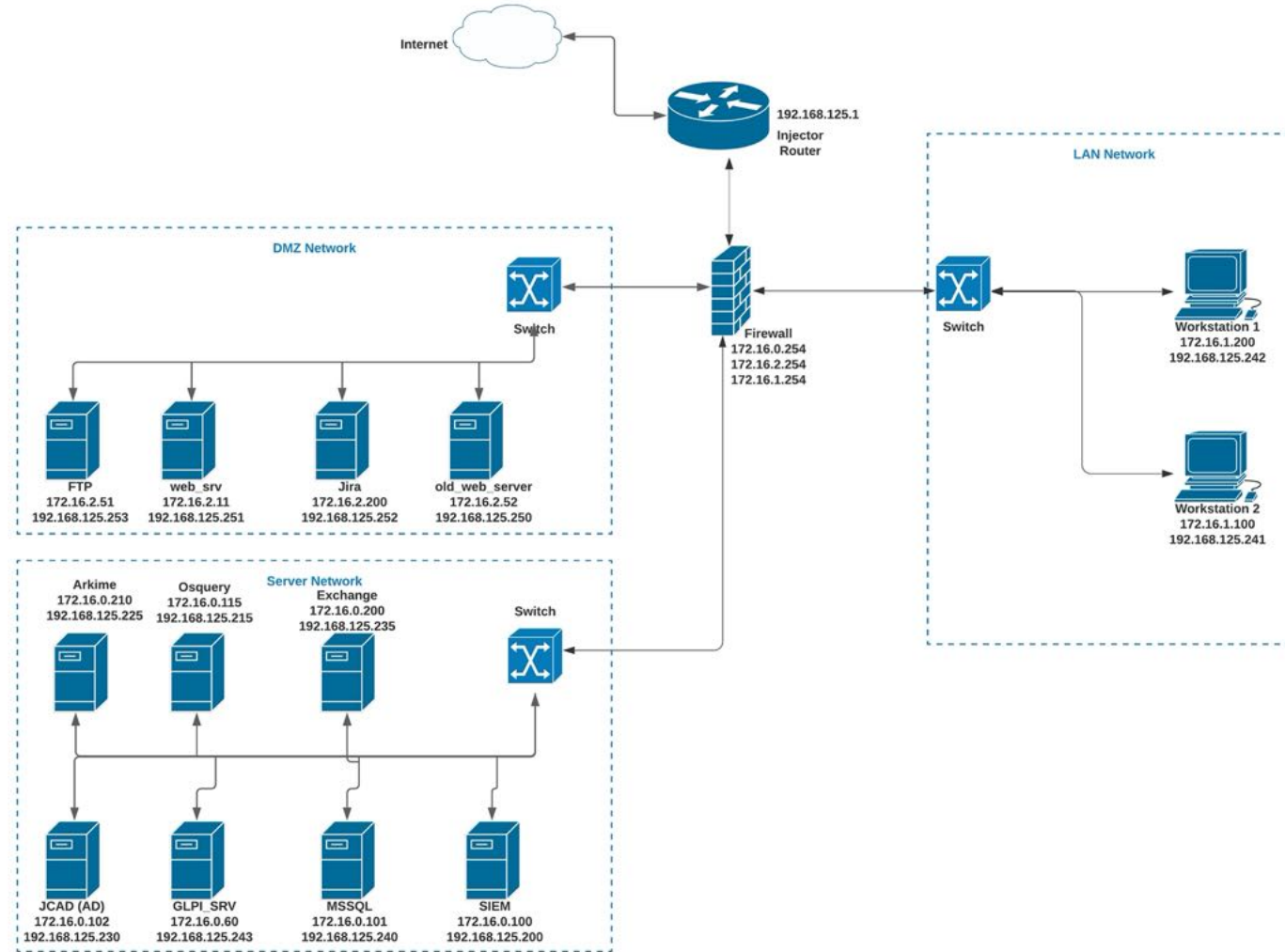


Scenario Description

- XCallCenter, has been caught off guard by constant attacks on its infrastructure
- Numerous tools have been deployed to ensure visibility
 - ELK/Wazuh
 - Arkime
 - OSQuery
- Your team has been called in to monitor the situation



Scenario Network



Network Traffic Analysis With Arkime



Network Traffic Analysis With Arkime

Introduction

- A large scale, open source, indexed packet capture and search tool
- Formerly called **Moloch**
- Arkime stores and exports all packets in standard PCAP format
 - Allows you to also use your favorite PCAP ingesting tools e.g. wireshark, during your analysis workflow
- Use of elasticsearch makes it easy to filter and view traffic

Network Traffic Analysis With Arkime

User Interface

The screenshot displays the Arkime web interface. At the top, a navigation menu includes 'Sessions', 'SPIView', 'SPIGraph', 'Connections', 'Files', 'Stats', 'History', 'Upload', 'Settings', and 'Users'. Below the menu is a search field and a time-range selector with 'Start' and 'End' time inputs. A bar chart labeled 'Network Traffic' shows traffic volume over time. Below the chart is a table of traffic entries with columns for Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, Databytes / Bytes, Moloch Node, and Info.

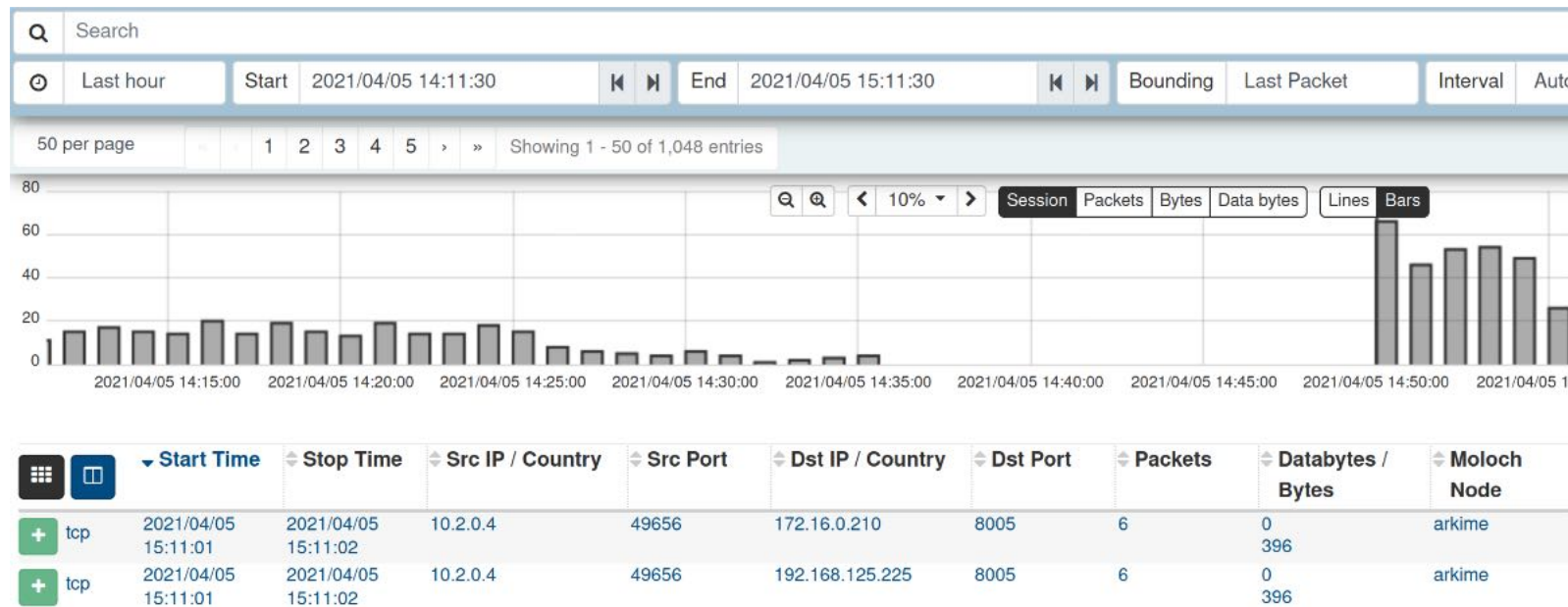
	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info	
+	tcp	2021/04/05 15:11:01	2021/04/05 15:11:02	10.2.0.4	49656	172.16.0.210	8005	6	0 396	arkime	
+	tcp	2021/04/05 15:11:01	2021/04/05 15:11:02	10.2.0.4	49656	192.168.125.225	8005	6	0 396	arkime	
+	tcp	2021/04/05 15:11:00	2021/04/05 15:11:06	10.2.0.4	49654	172.16.0.210	8005	11	1,025 2,752	arkime	URI 192.168.125.225:8005/eshealth.json
+	tcp	2021/04/05 15:11:00	2021/04/05 15:11:06	10.2.0.4	49654	192.168.125.225	8005	11	1,025 2,752	arkime	URI 192.168.125.225:8005/eshealth.json
+	tcp	2021/04/05 15:10:46	2021/04/05 15:10:53	10.2.0.4	49652	172.16.0.210	8005	6	0 412	arkime	
+	tcp	2021/04/05 15:10:46	2021/04/05 15:10:53	10.2.0.4	49652	192.168.125.225	8005	6	0 412	arkime	
+	tcp	2021/04/05	2021/04/05	10.2.0.4	49650	192.168.125.225	8005	10	1,874	arkime	URI



Arkime User Interface

Sessions

- Displays a list of indexed sessions for the selected time period and search expression
- Includes a timeline graph and map of the session results





Arkime User Interface

Sessions

- Hovering over a value in the table gives a quick dropdown to use the values as filters

◆ Src Port	◆ Dst IP / Coun
49656	172.16.0.210 ▾
and 172.16.0.210	
and not 172.16.0.210	
or 172.16.0.210	
or not 172.16.0.210	
and 172.16.0.210:8005	
and not 172.16.0.210:8005	
or 172.16.0.210:8005	
or not 172.16.0.210:8005	

◆ Databytes / Bytes	◆ Moloch Node
0	arkime ▾
and arkime	
and not arkime	
or arkime	
or not arkime	
<input checked="" type="checkbox"/> New Sessions Tab	
<input type="checkbox"/> Copy value	



Arkime User Interface

Sessions

- Expanding over a session by clicking the green plus icon on the left gives much more session info

Download PCAP Source Raw Destination Raw Link Actions

Id 210405-Hg7habQfGe9E6rUFgfE6jc2H **Community Id:** 1:k5bSAO1sclq58Mw

Time 2021/04/05 15:36:15 - 2021/04/05 15:36:15

Node arkime

Protocols tcp http

IP Protocol tcp

Src Packets 7 Bytes 745 Databytes 355

Dst Packets 5 Bytes 11,468 Databytes 11,186

Ethernet **Src Mac** 00:11:22:33:44:55 fa:16:3e:1b:cf:e6 **OUI** CIMSYS Inc **Dst Mac** 00:11:22:33:44:55

Src IP/Port 192.168.125.254 : 33172 { ARIN }

Dst IP/Port 2.16.107.104 : 80 { RIPE }

Payload8 Src 474554202f736572 (GET /ser) Dst 485454502f312e31 (HTTP/1.1)

Tags +

TCP Flags SYN 1 SYN-ACK 1 ACK 6 PSH 2 RST 0 FIN 2 URG 0

HTTP

Method GET

Status code 200

Hosts amupdatedl.microsoft.com

User Agents Microsoft BITS/7.8

Request Headers accept accept-encoding connection host htt

Client Versions 1.1

Response Headers accept-ranges cache-control connection cont

Server Versions 1.1

Body MD5s d73177fe7db93a10d79a669feeda3609

libfile content type application/vnd.ms-cab-compressed

content-type Header application/octet-stream

server Header Microsoft-IIS/10.0

Examples of info given

- All connection details e.g. hosts, port, payload
- Session flow e.g. TCP flags
- Ability to download files exchanged in session
- MD5 hashes of response
- Email body/parameters (for SMTP)
- Ability to filter traffic based on displayed parameters
- Invoke Cyberchef
- etc



Arkime User Interface

SPI View

- You can click on any value to automatically use it as a search filter
- Values are grouped into their apt categories

general

Search for fields to display in this category

Dst IP ▾ **Protocols** ▾ **Src IP** ▾ **Asset** ▾ **Asset Cnt** ▾ **Bytes** ▾ **Community Id** ▾ **Data byte**

▽

Dst IP ▾ 172.16.0.115 ⁽⁵⁹¹⁾ 172.16.0.210 ⁽⁶¹⁾ 8.8.8.8 ⁽⁴⁶⁾ 192.168.125.11 ⁽²⁷⁾ 2.16.107.104 ⁽²²⁾ 172.16.0.255 ⁽¹⁷⁾ 2.16.107.32 ⁽⁷⁾ 78.46.78.167 ⁽⁷⁾ 89.111.15.2
194.55.13.128 ⁽⁷⁾ 213.239.239.164 ⁽⁷⁾ 2.16.107.88 ⁽⁶⁾ 10.2.0.4 ⁽⁶⁾ 193.182.111.13 ⁽⁶⁾ 2.16.107.80 ⁽⁴⁾ 46.165.221.137 ⁽⁴⁾ 91.189.89.198 ⁽⁴⁾ 91.189.89.199 ⁽⁴⁾ 14
51.75.67.47 ⁽³⁾ 85.25.148.4 ⁽³⁾ 91.189.91.157 ⁽³⁾ 92.243.6.5 ⁽³⁾ 162.159.200.123 ⁽³⁾ 172.16.0.100 ⁽³⁾ 176.221.42.125 ⁽³⁾ 185.207.105.38 ⁽³⁾ 188.165.201.225 ⁽³⁾
20.73.194.208 ⁽¹⁾ 52.114.32.7 ⁽¹⁾ 52.114.77.164 ⁽¹⁾ 52.114.132.11 ⁽¹⁾ 52.114.133.60 ⁽¹⁾ 67.26.83.254 ⁽¹⁾ 205.185.216.10 ⁽¹⁾

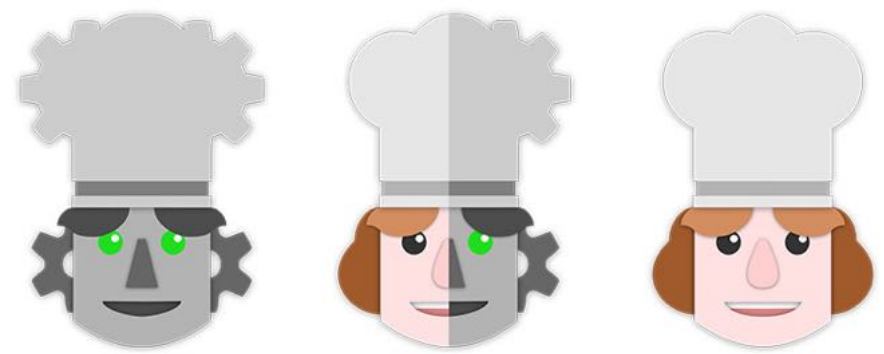
Protocols ▾ tcp ⁽⁶⁸³⁾ tls ⁽⁵⁹⁴⁾ udp ⁽¹⁹⁰⁾ ntp ⁽¹²⁴⁾ icmp ⁽⁶¹⁾ dns ⁽⁴⁶⁾ http ⁽⁴⁴⁾ ssh ⁽⁴⁾ http2 ⁽²⁾ llmnr ⁽²⁾

Src IP ▾ 172.16.0.210 ⁽⁶³²⁾ 192.168.125.254 ⁽²¹²⁾ 172.16.0.254 ⁽³³⁾ 172.16.0.1 ⁽¹²⁾ 192.168.125.1 ⁽¹²⁾ 10.2.0.4 ⁽⁸⁾ 172.16.0.101 ⁽⁷⁾ 172.16.0.102 ⁽⁷⁾ 172.16.0

Other Functionalities

- View connections and connection map
- Download pcap files for different sessions
- Upload pcap file for analysis on Arkime
- Integrate with other pcap analysis tools e.g. wireshark
- Export objects in sessions

CyberChef



Introduction

- A web app for encryption, encoding, compression and data analysis.
 - The Cyber Swiss Army Knife
- Operations can be chained on each other
- Runs purely on your browser
- Hosted on <https://gchq.github.io/CyberChef/>



CyberChef Interface

Download CyberChef Last build: 13 days ago Options

Operations

Search...

Favourites

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Data format

Recipe

Input length: 0
lines: 1




Output



STEP **BAKE!** Auto Bake

Interface

- Has 4 main areas:
 - Input – paste the text you want to work on
 - Output – Output will be put here
 - Operations – List of all possible operations
 - Recipe – Selected operations to use on input
- Command chaining
 - Convert from base64
 - Get its hexdump



Chaining

Recipe   

From Base64  

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars


To Hexdump  

Width: 16 Upper case hex Include final length

UNIX format

Input start: 16 length: 16
end: 16 lines: 1
length: 0

L2V0Yy9wYXNzd2Q=

Output 

start: 46 time: 2ms
end: 45 length: 72
length: -1 lines: 1

00000000 2f 65 74 63 2f 70 61 73 73 77 64 |/etc/passwd|

Viewing logs and log analysis with ELK and osquery



Viewing Logs and Log Analysis with ELK and Osquery

ELK

The screenshot displays the ELK Discover interface. At the top, the 'Discover' tab is active. A search bar contains the text 'Search' and is labeled 'Search Box'. To its right, a 'Time range Selector' is set to 'Last 15 minutes'. Below the search bar, the index pattern is set to 'filebeat-*'. A list of 'Available fields' is shown, including '_id', '_index', '_score', '_type', '@timestamp', 'agent.ephem...', 'agent.hostna...', 'agent.id', 'agent.name', and 'agent.type'. The main area shows a bar chart with 20 hits and a table of log entries. The table has columns for 'Time' and '_source'. The first log entry is: `> Mar 29, 2021 @ 12:02:24.001 @timestamp: Mar 29, 2021 @ 12:02:24.001 message: 2021-03-29T09:02:22+03:00 gateway suricata[2243]: [1:2221034:1] SURICATA HTTP Request unrecognized authorization method [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.125.254:33481 -> 192.168.125.201:9000 log.file.path: /var/log/remotelogs/suricata.log log.offset: 89,846,766 input.type: log ecs.version: 1.6.0 host.name: wazuh-elk agent.type: filebeat`

- You enter the search criteria on the Search Box
- **Always** ensure your time-range is correct
- Free text search - if keyword appears **anywhere**

```
172.16.0.102
```

- Field-based searches

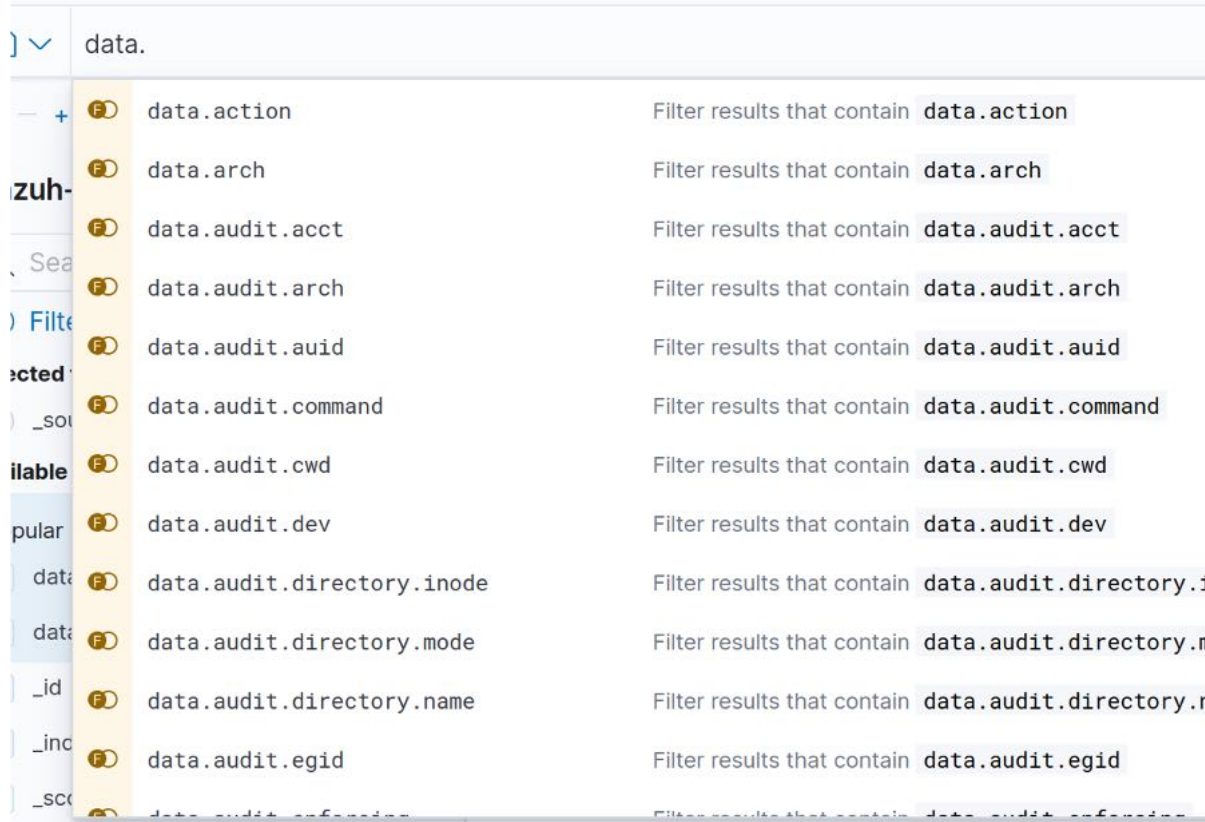
```
data.srcip:172.16.0.100
```

```
name:"Ned Stark"
```

```
age:[3 TO 10]
```

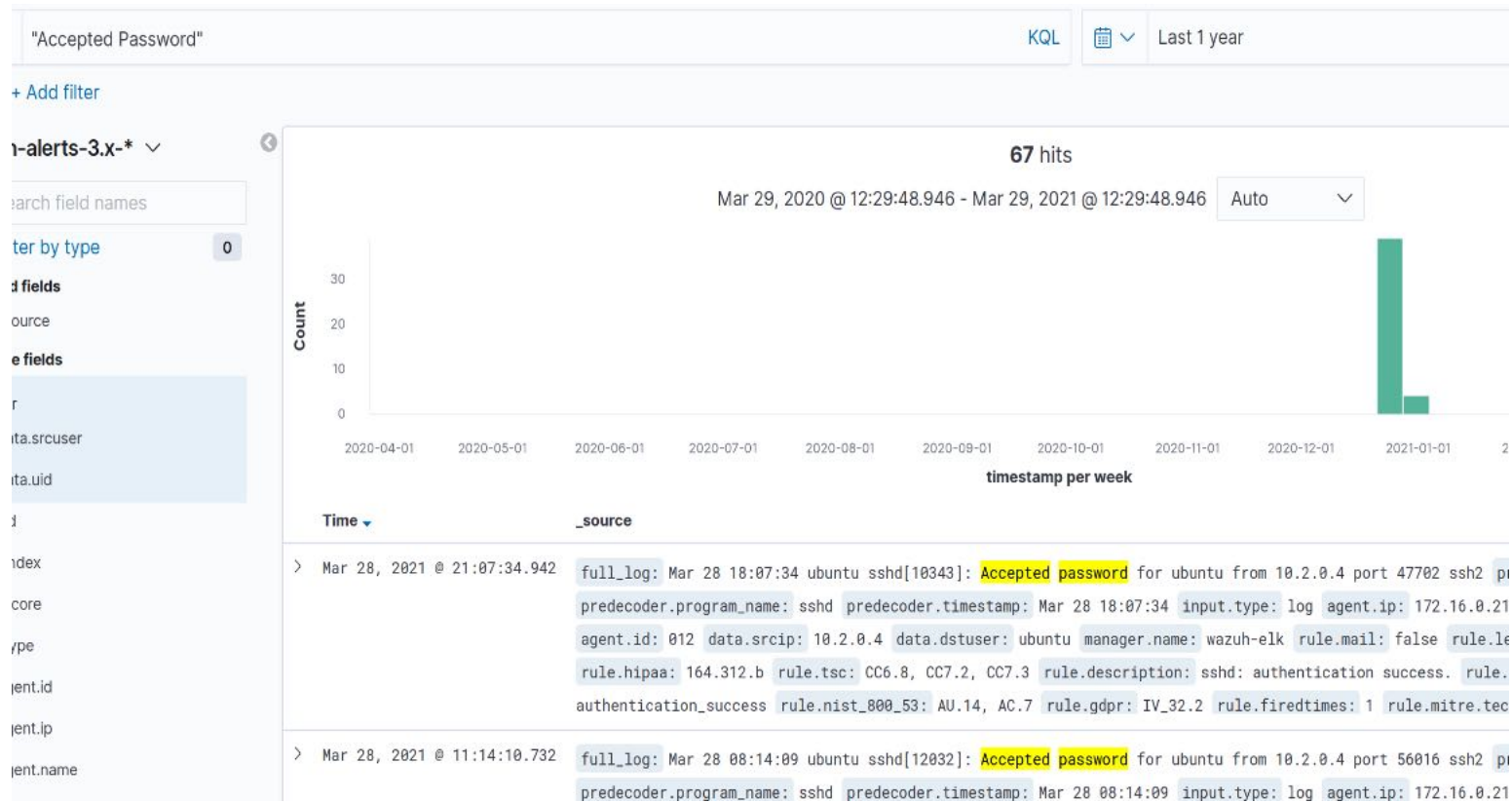
```
price:{100 TO 400}
```

- Kibana Auto-Completes fields for you



Field Name	Description
data.action	Filter results that contain data.action
data.arch	Filter results that contain data.arch
data.audit.acct	Filter results that contain data.audit.acct
data.audit.arch	Filter results that contain data.audit.arch
data.audit.auid	Filter results that contain data.audit.auid
data.audit.command	Filter results that contain data.audit.command
data.audit.cwd	Filter results that contain data.audit.cwd
data.audit.dev	Filter results that contain data.audit.dev
data.audit.directory.inode	Filter results that contain data.audit.directory.i
data.audit.directory.mode	Filter results that contain data.audit.directory.m
data.audit.directory.name	Filter results that contain data.audit.directory.n
data.audit.egid	Filter results that contain data.audit.egid
data.audit.efuid	Filter results that contain data.audit.efuid

- Can search for exact text match



- Can expand individual logs to view more info

Table	JSON
	<pre>{ "_id": "M_QFengBv4J9BSv3GBM-", "_index": "wazuh-alerts-3.x-2021.03.28", "_score": -1, "_type": "_doc", "agent.id": "012", "agent.ip": "172.16.0.210", "agent.name": "arkime", "data.dstuser": "ubuntu", "data.srcip": "10.2.0.4", "decoder.name": "sshd", "decoder.parent": "sshd", "full_log": "Mar 28 18:07:34 ubuntu sshd[10343]: Accepted password for ubuntu from 10.2.0.4 port 47702 ssh2", "id": "1616954854.55066915", "input.type": "log", "location": "/var/log/auth.log", "manager.name": "wazuh-elk", "predecoder.hostname": "ubuntu", "predecoder.program_name": "sshd", "predecoder.timestamp": "Mar 28 18:07:34" }</pre>

- Add more columns from the left side-bar

			timestamp per week		
Time ▾	agent.name	agent.ip	data.dstuser	data.scrip	rule.mitre.technique
> Mar 28, 2021 @ 21:07:34.942	arkime	172.16.0.210	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 28, 2021 @ 11:14:10.732	arkime	172.16.0.210	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 28, 2021 @ 02:18:52.037	arkime	172.16.0.210	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 23, 2021 @ 00:34:43.545	wazuh-elk	-	admin	10.2.0.4	Valid Accounts, Remote Services
> Mar 23, 2021 @ 00:34:43.545	wazuh-elk	-	admin	10.2.0.4	Valid Accounts, Remote Services
> Mar 23, 2021 @ 00:16:25.002	arkime	172.16.0.210	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 23, 2021 @ 00:16:25.002	arkime	172.16.0.210	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 16, 2021 @ 14:51:59.152	ftpsrvr	172.16.2.51	root	10.2.0.4	Valid Accounts, Remote Services
> Mar 16, 2021 @ 14:51:59.152	ftpsrvr	172.16.2.51	root	10.2.0.4	Valid Accounts, Remote Services
> Mar 16, 2021 @ 13:12:35.283	glpi	172.16.0.60	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 16, 2021 @ 13:12:35.283	glpi	172.16.0.60	ubuntu	10.2.0.4	Valid Accounts, Remote Services
> Mar 16, 2021 @ 12:51:26.637	old-web-server	172.16.2.52	ubuntu	10.2.0.4	Valid Accounts, Remote Services



OSQuery Analysis

- Osquery is an open-source security tool that takes an operating system and turns it into one giant database
 - With tables that you can query using SQL-like statements
- Use queries to monitor file integrity, check on status of services, fetch users, perform security audits of the target server, and more



OSQuery Analysis

- You can run queries on a single host or a group of hosts
- You can create Query packs to run checks at scheduled times over a host or hosts

Running Queries

```
# Fetching list of users in a specific server  
SELECT * FROM users
```

shell	uid	uid_signed	username
/bin/bash	0	0	root
/sbin/nologin	1	1	bin
/sbin/nologin	2	2	daemon
/sbin/nologin	3	3	adm
/sbin/nologin	4	4	lp
/bin/sync	5	5	sync
/sbin/shutdown	6	6	shutdown

Running Queries

```
# Fetching OS versions from multiple hosts at once  
SELECT name,platform,version FROM os_version;
```

Results

hostname	name	platform	version
WORKSTATION1.xcallcenter.com	Microsoft Windows 7 Professional	windows	6.1.7601
ubuntu	Ubuntu	ubuntu	18.04.1 LTS (Bionic Beaver)
wazuh-elk	CentOS Linux	rhel	CentOS Linux release 7.9.2009 (Core
MSSQL.xcallcenter.com	Microsoft Windows Server 2012 R2 Standard	windows	6.3.9600
msexchange.xcallcenter.com	Microsoft Windows Server 2019 Standard	windows	10.0.17763
ubuntu	Ubuntu	ubuntu	18.04.1 LTS (Bionic Beaver)
glpi	Ubuntu	ubuntu	18.04.1 LTS (Bionic Beaver)

Running Queries

```
# Fetching firewall rules on Centos servers
select chain, policy, src_ip, dst_ip from iptables ;
```

Results

hostname	chain	dst_ip	policy	src_ip
wazuh-elk	PREROUTING	0.0.0.0	ACCEPT	0.0.0.0
wazuh-elk	PREROUTING	0.0.0.0	ACCEPT	0.0.0.0
wazuh-elk	PREROUTING	0.0.0.0	ACCEPT	0.0.0.0
wazuh-elk	PREROUTING		ACCEPT	
wazuh-elk	INPUT		ACCEPT	
wazuh-elk	OUTPUT	0.0.0.0	ACCEPT	0.0.0.0
wazuh-elk	OUTPUT		ACCEPT	