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

silensec™ ISO27001 Certified

About CYBER RANGES

Cyber Range as a Service

Hosted

On Premise

Portable

silensec™
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 Launn, 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

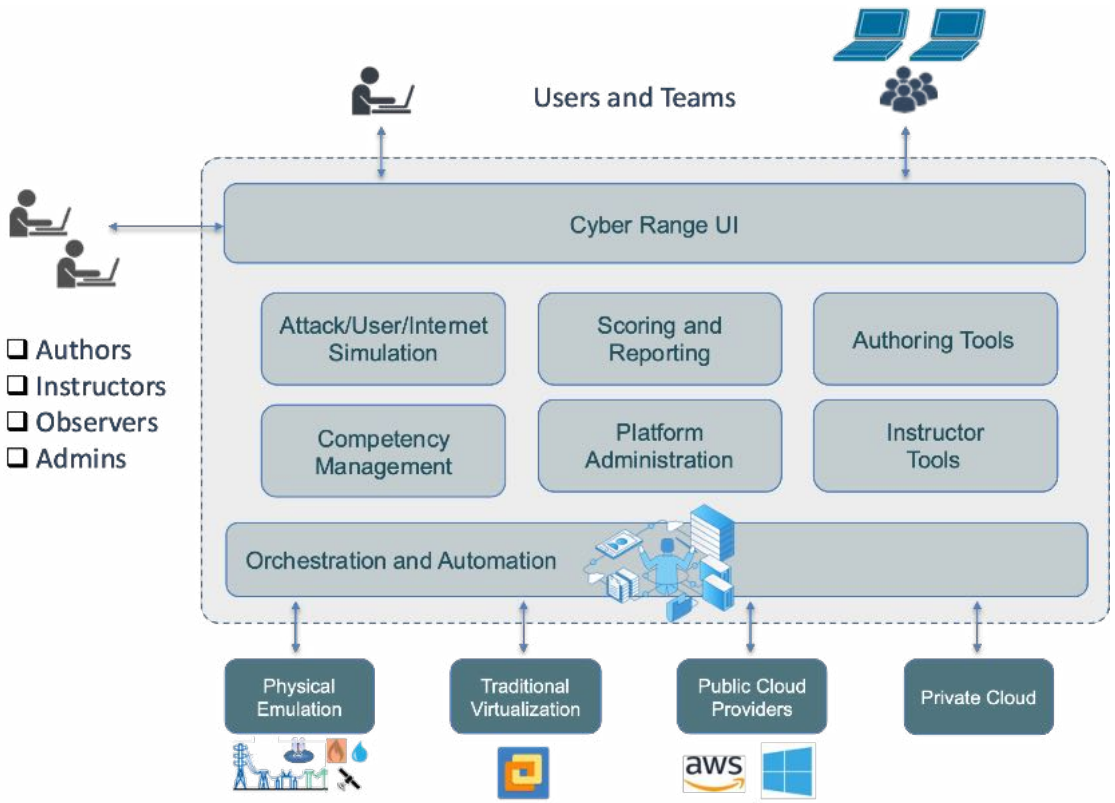
Page: 1 of 2

...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



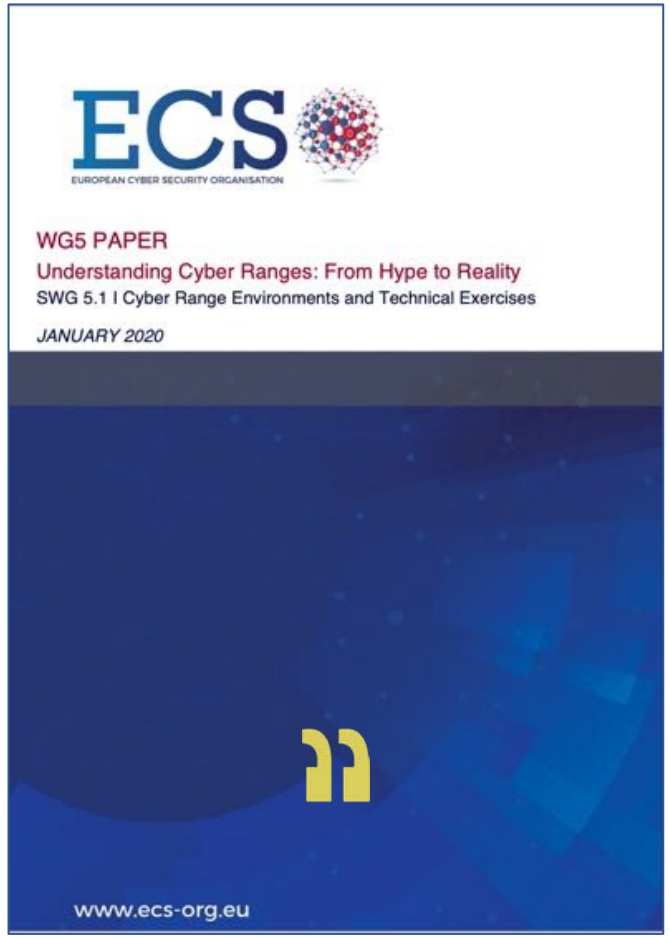
A cyber range is a platform for the development, delivery and use of interactive simulation environments.

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.

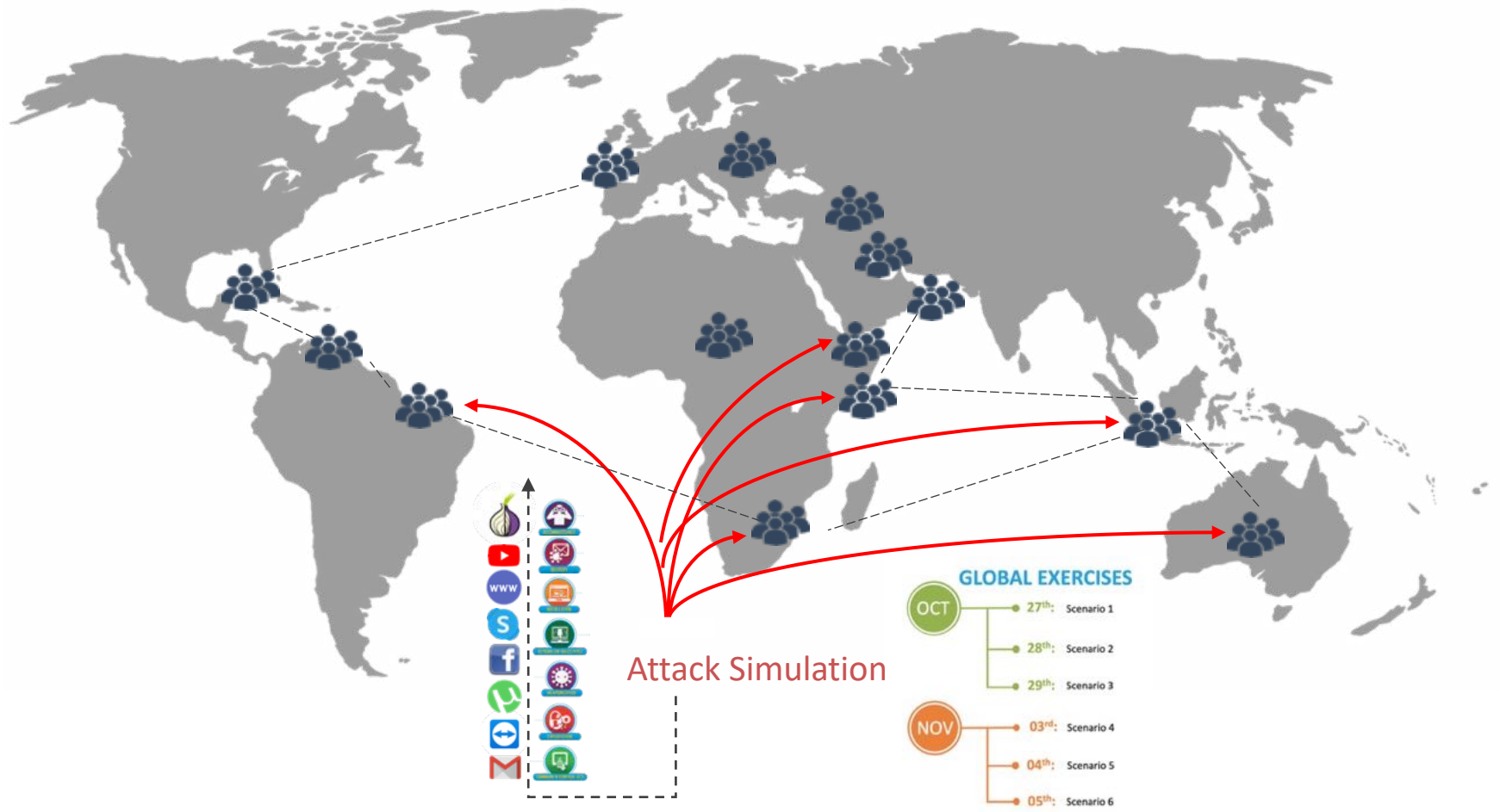
A cyber range includes a combination of core technologies for the creation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases.

Source: EUROPEAN CYBER SECURITY ORGANIZATION (ECSO)

https://ecs-org.eu

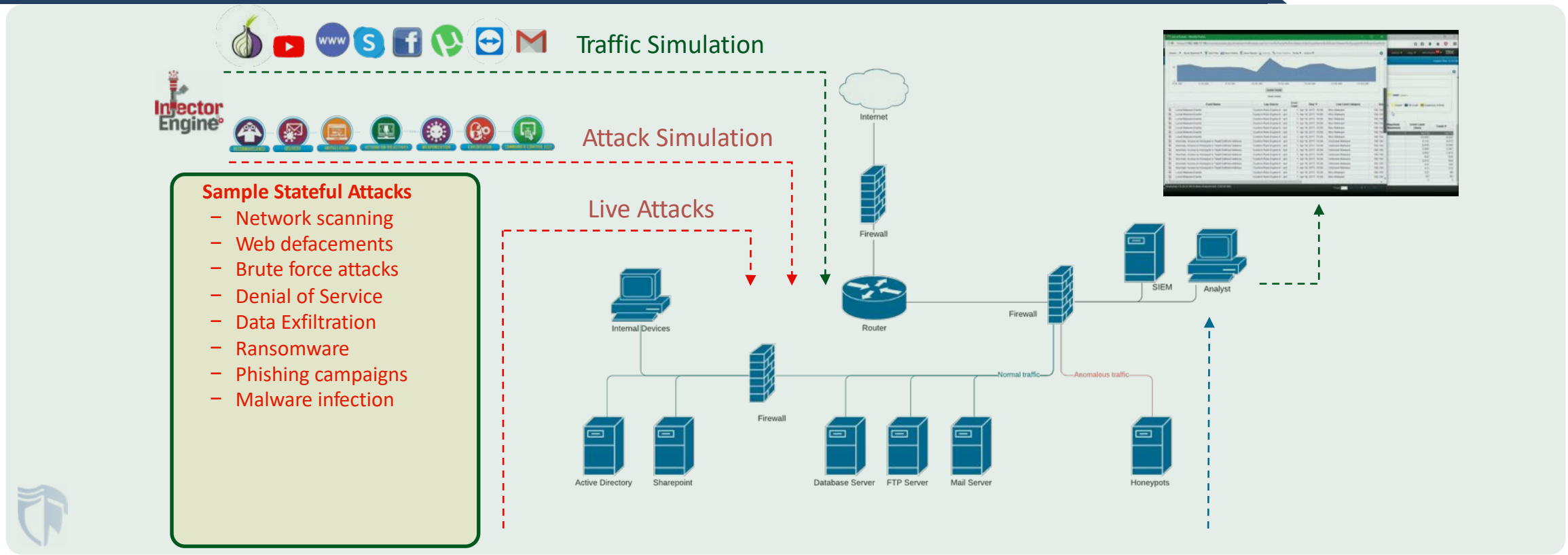


Large-Scale Cyber Exercises



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



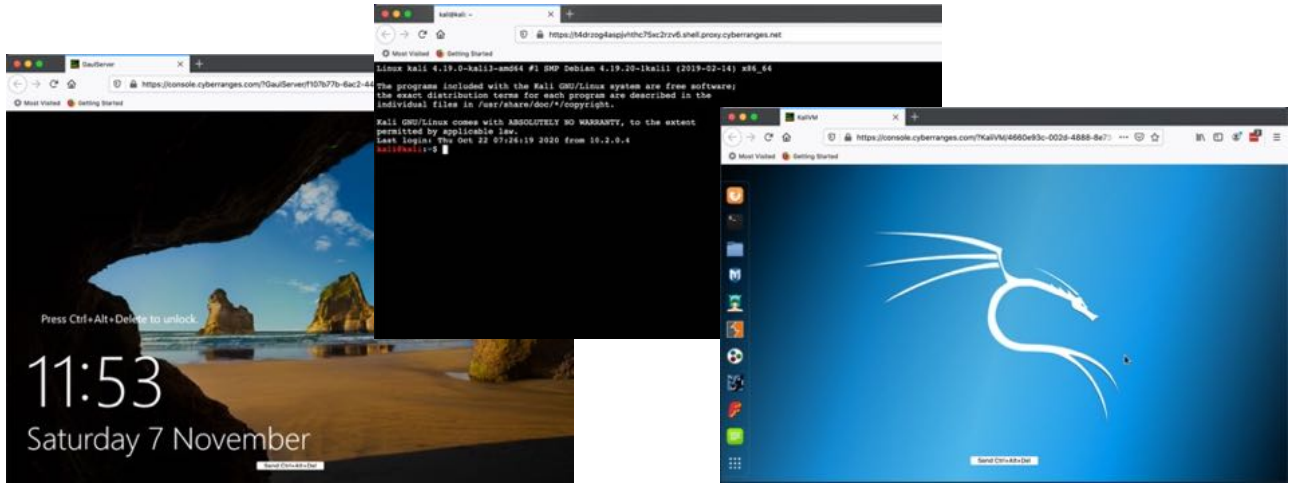
Red Team

Purple Team

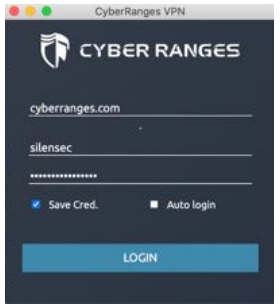
Blue Team

White Team

Using CYBER RANGES



In-Browser Access to the Simulation Environment



Access via VPN for for BYOD Engagements

Individual access to the VMs

CYBER RANGES

OCWAR-C - Ghana session - Scenario 1

CYBER RANGES

silensec
ISO27001 Certified

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 and Network IDS overview

- 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

SIEMs and LMS IDS overview

- 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.

CYBER RANGES

Integrating Zeek/Bro Events to the ELK Stack

Scenario Description

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 various 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.**

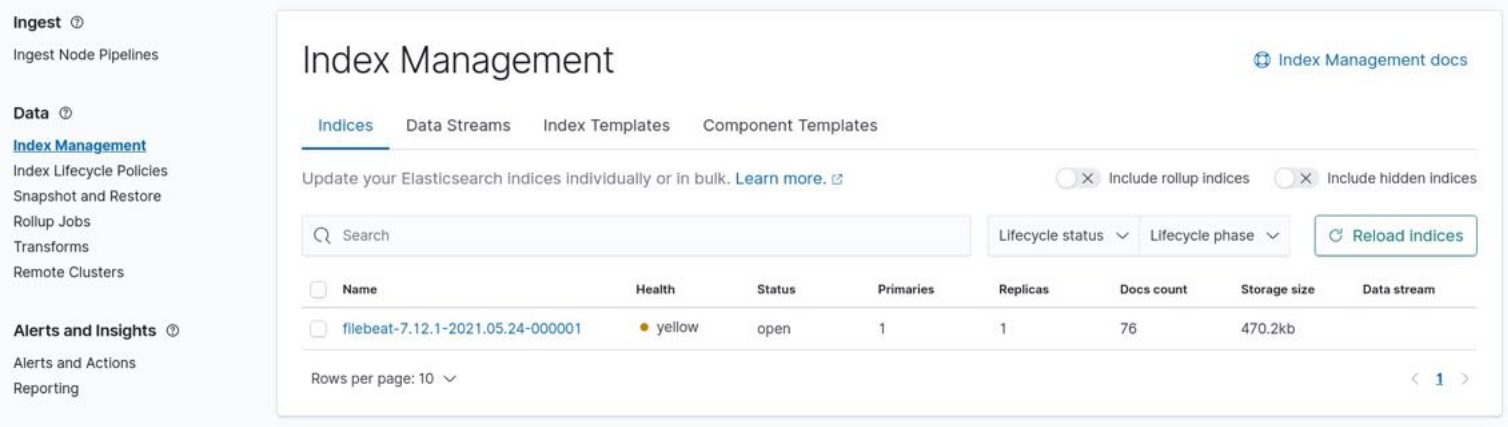
Integrating Zeek/Bro Events to the ELK Stack

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 date 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;

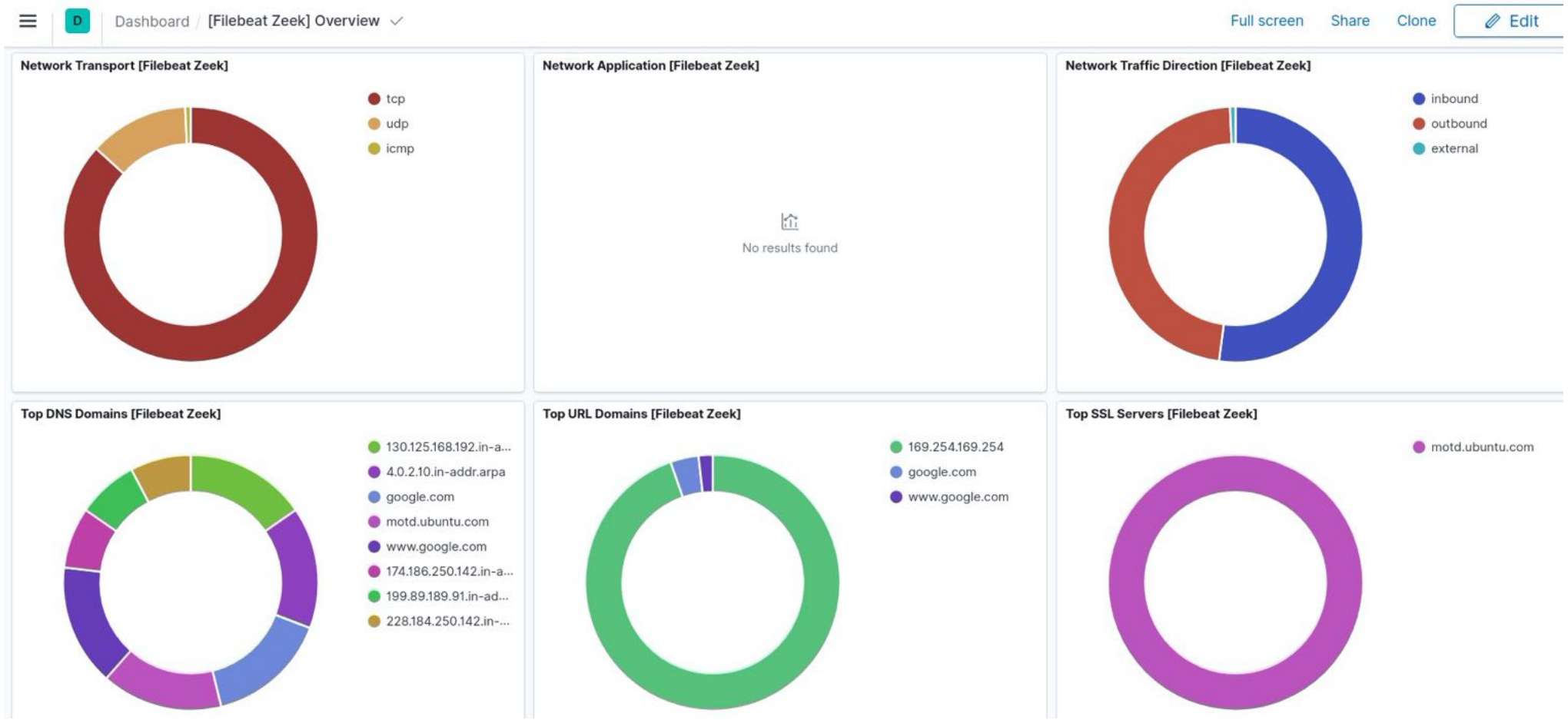


Viewing Zeek Events on Kibana

- 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

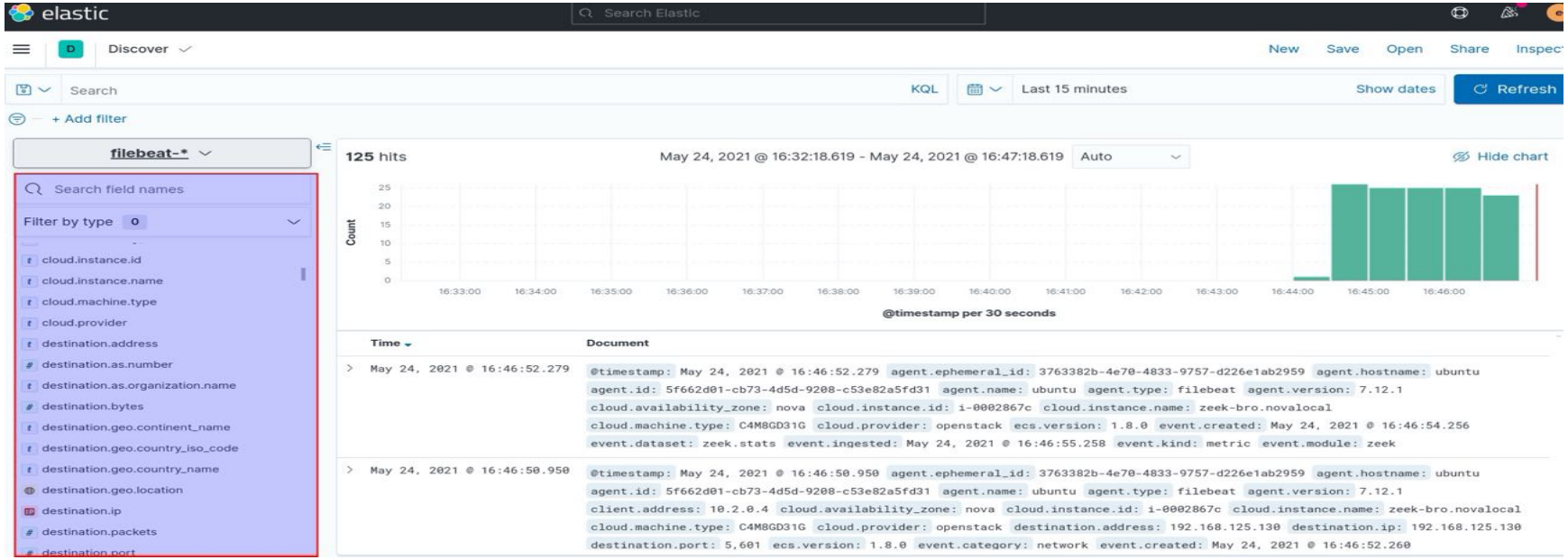
Sample Zeek ELK Dashboards



Zeek Events on ELK

Sample Zeek Events on ELK

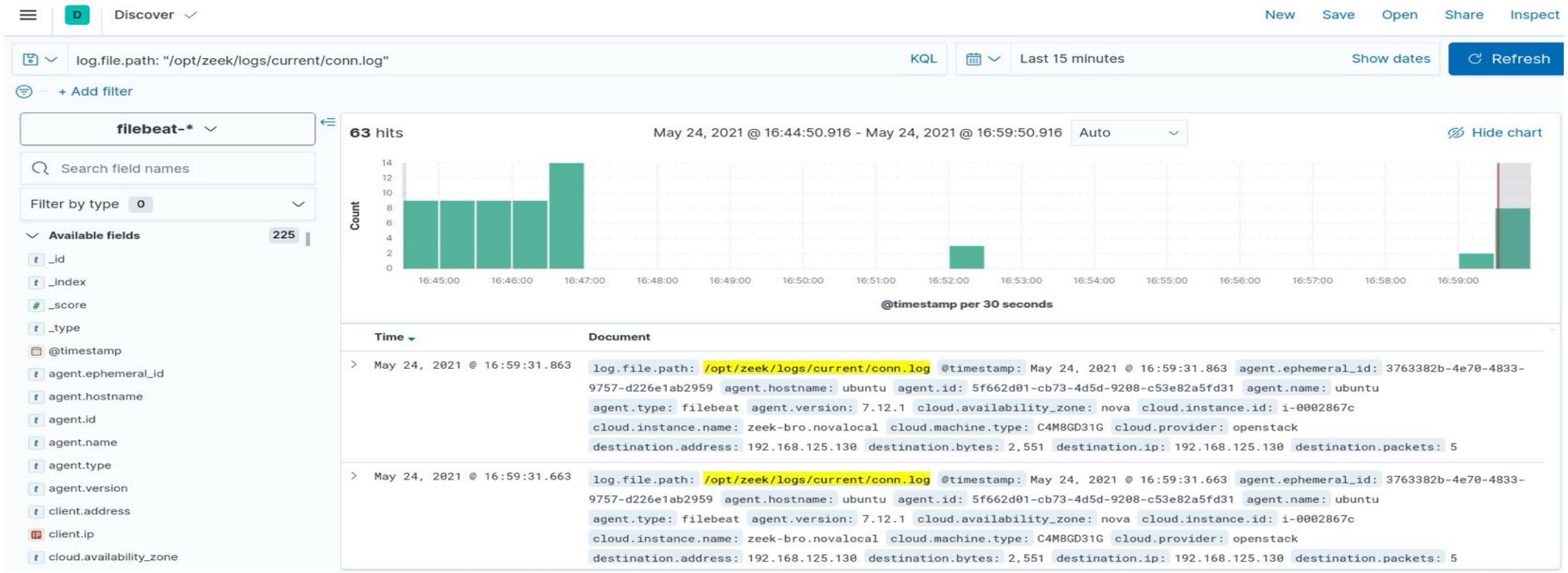
- Displays Zeek events collected from the host running Zeek.
- The events are related to traffic passing through the interface on which Zeek is configured to monitor.



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.



CYBER RANGES

OCWAR-C - Ghana session - Scenario 2

CYBER RANGES

silensec
ISO27001 Certified

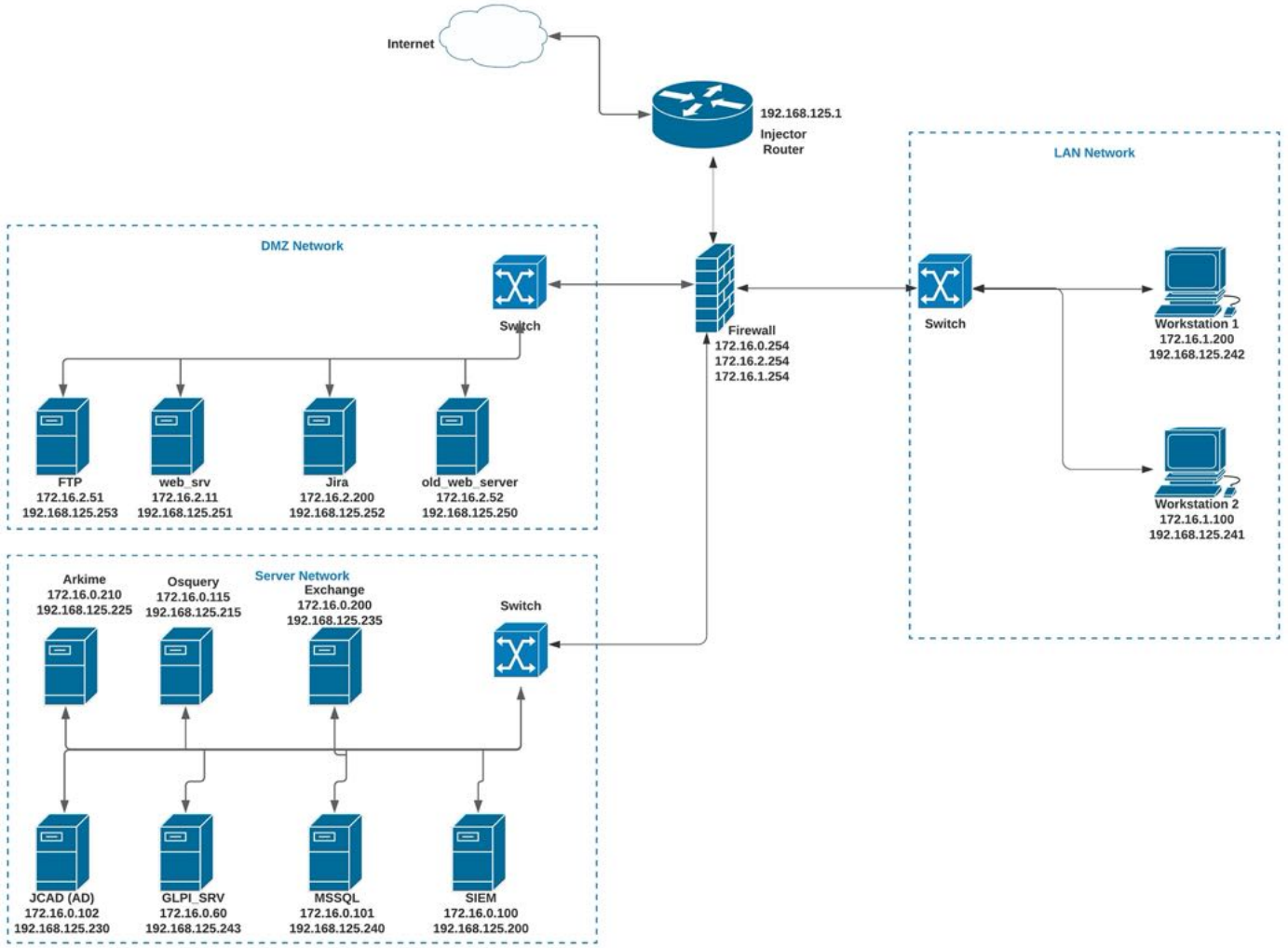
Session 2 Outline

- Arkime Netwok 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



CYBER RANGES

Network Traffic Analysis With Arkime

CYBER RANGES

silensec
ISO27001 Certified

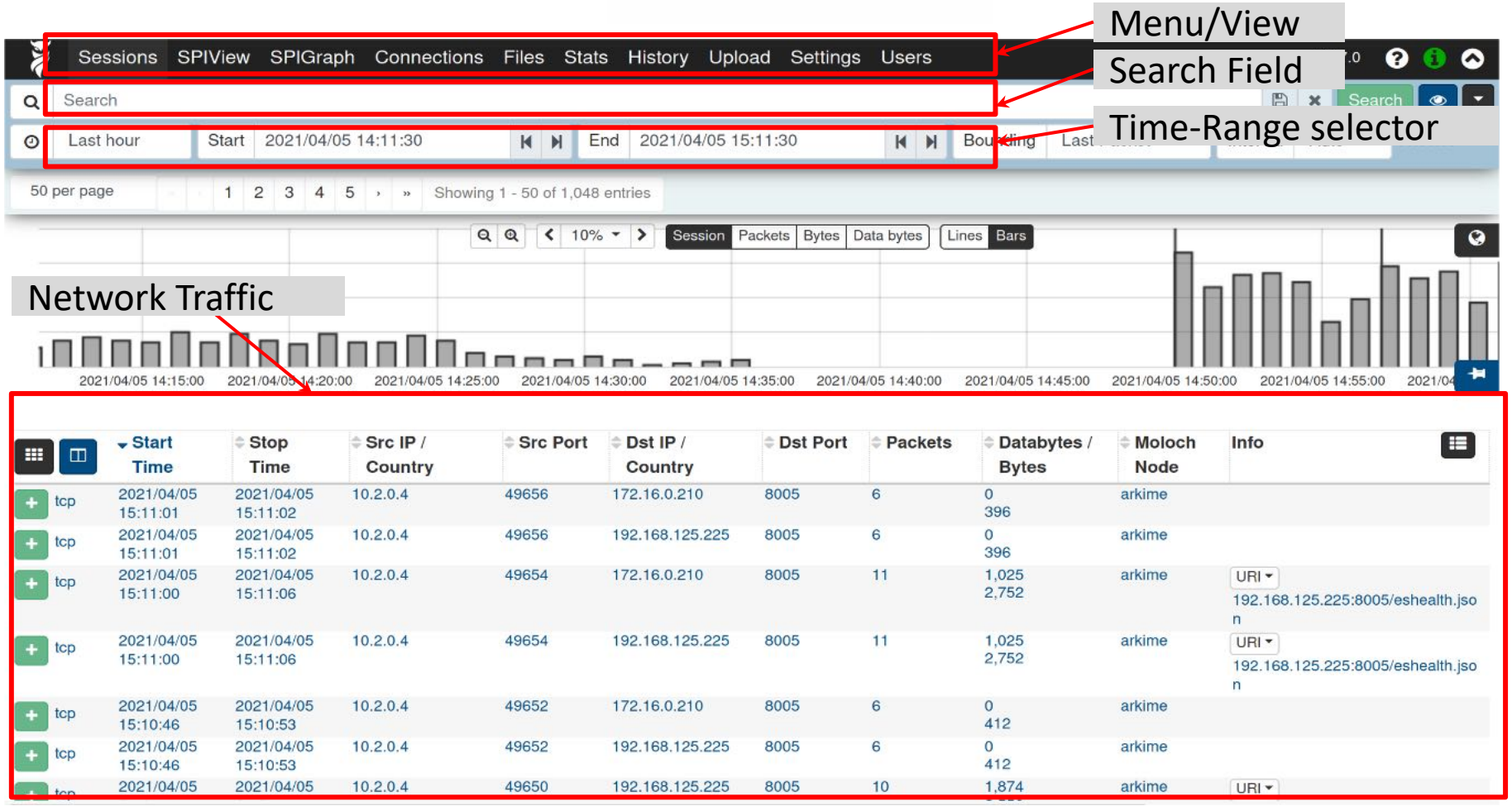
Network Traffic Analysis With Arkime

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

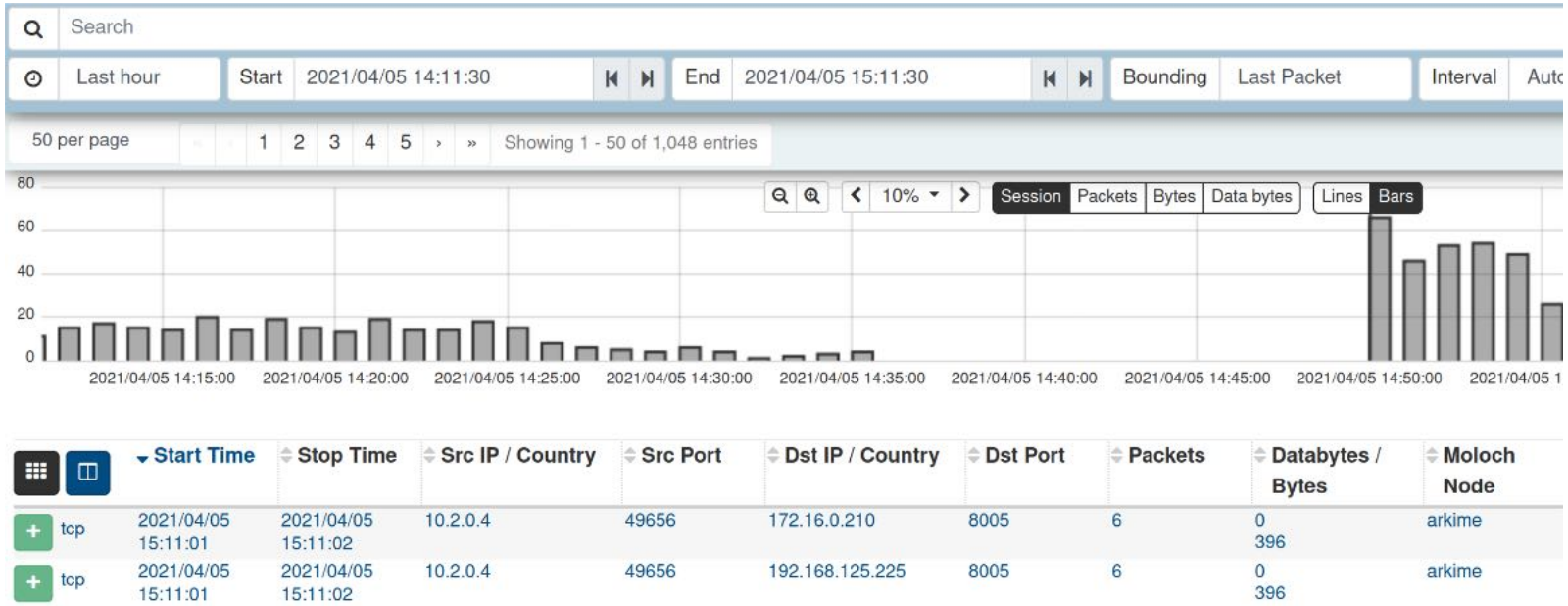


Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
tcp	2021/04/05 15:11:01	2021/04/05 15:11:02	10.2.0.4	49656	172.16.0.210	8005	6	0 396	arkime	
tcp	2021/04/05 15:11:01	2021/04/05 15:11:02	10.2.0.4	49656	192.168.125.225	8005	6	0 396	arkime	
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

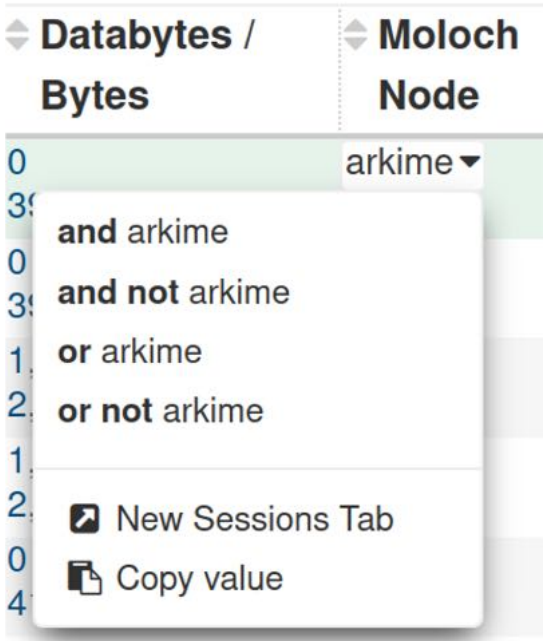
- Displays a list of indexed sessions for the selected time period and search expression
- Includes a timeline graph and map of the session results



Arkime User Interface

Sessions

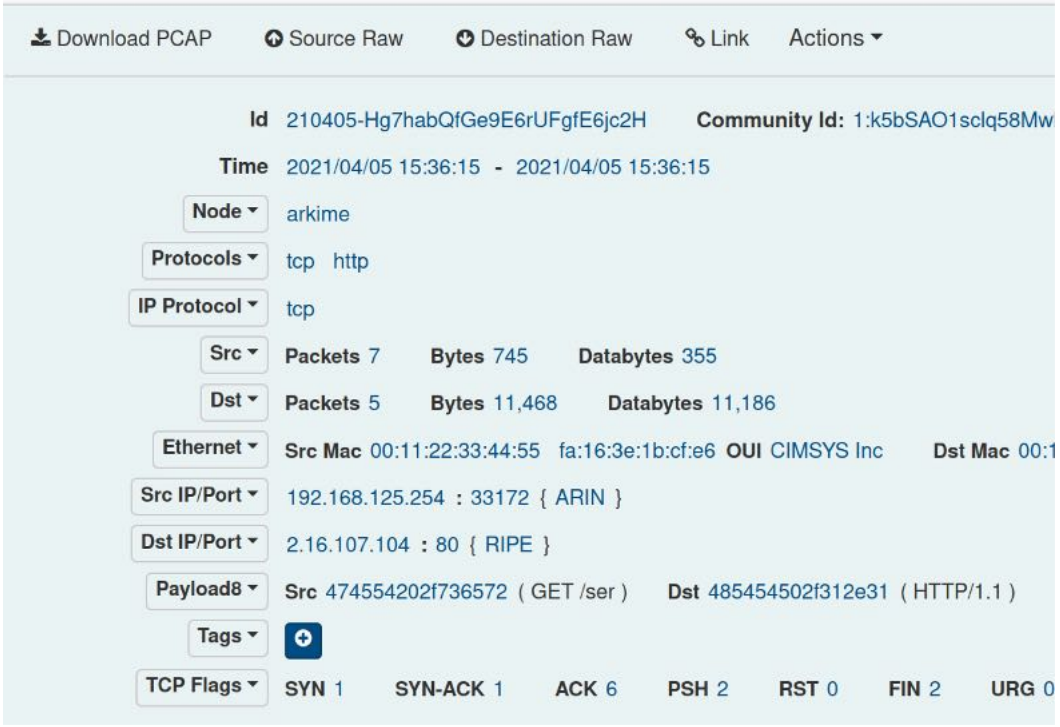
- Hovering over a value in the table gives a quick dropdown to use the values as filters

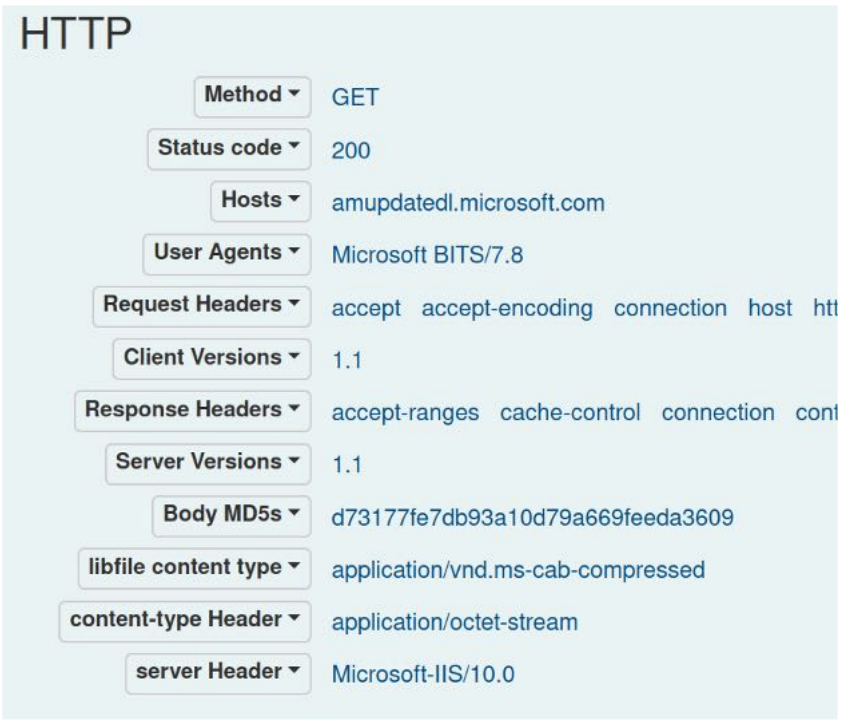


Arkime User Interface

Sessions

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





Sessions

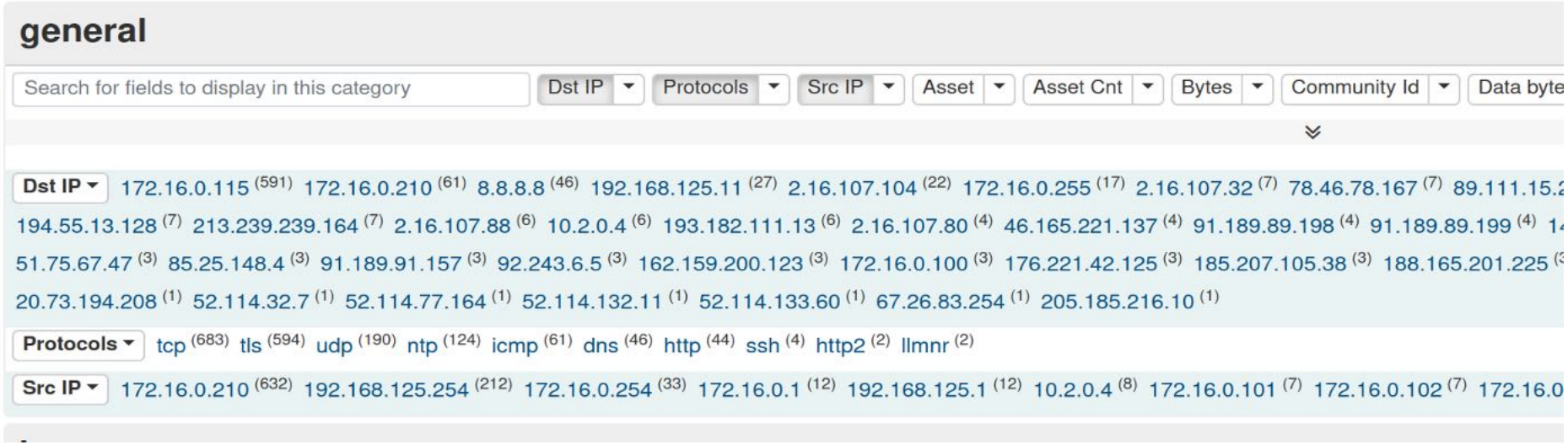
Examples of info given

- 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



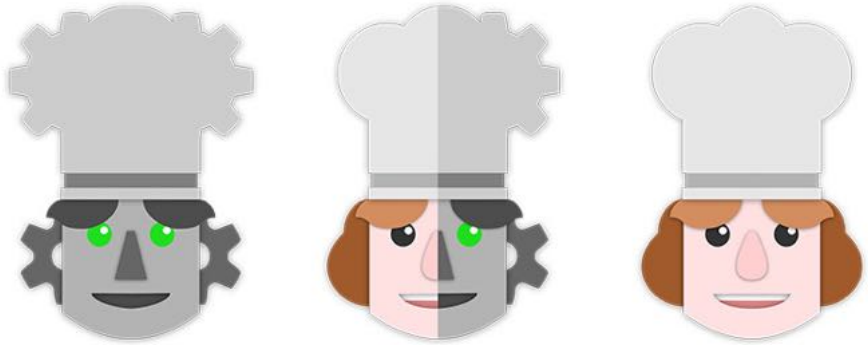
Arkime User Interface

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

CYBER RANGES

CyberChef



CYBER RANGES

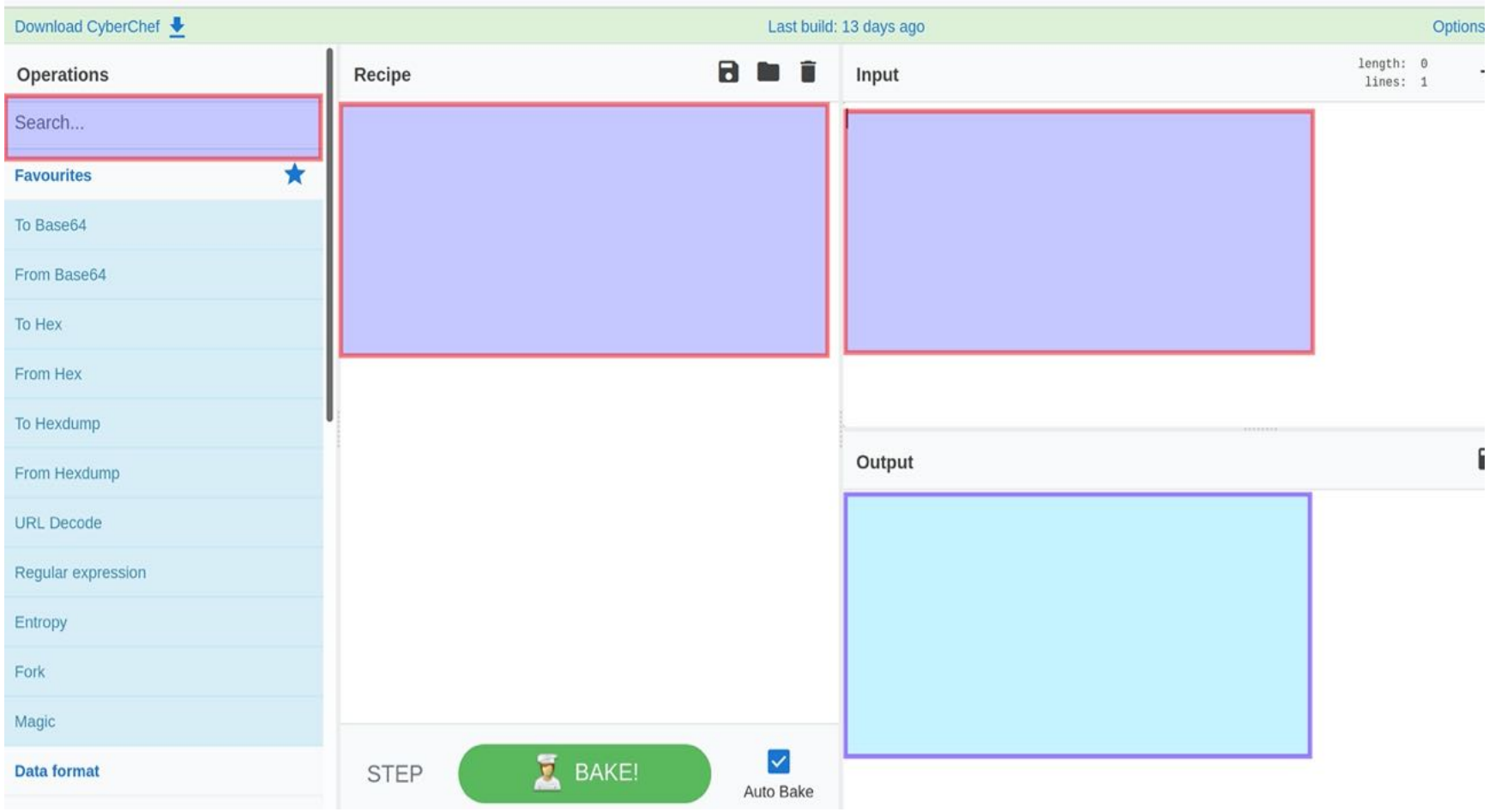
silensec
ISO27001 Certified

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



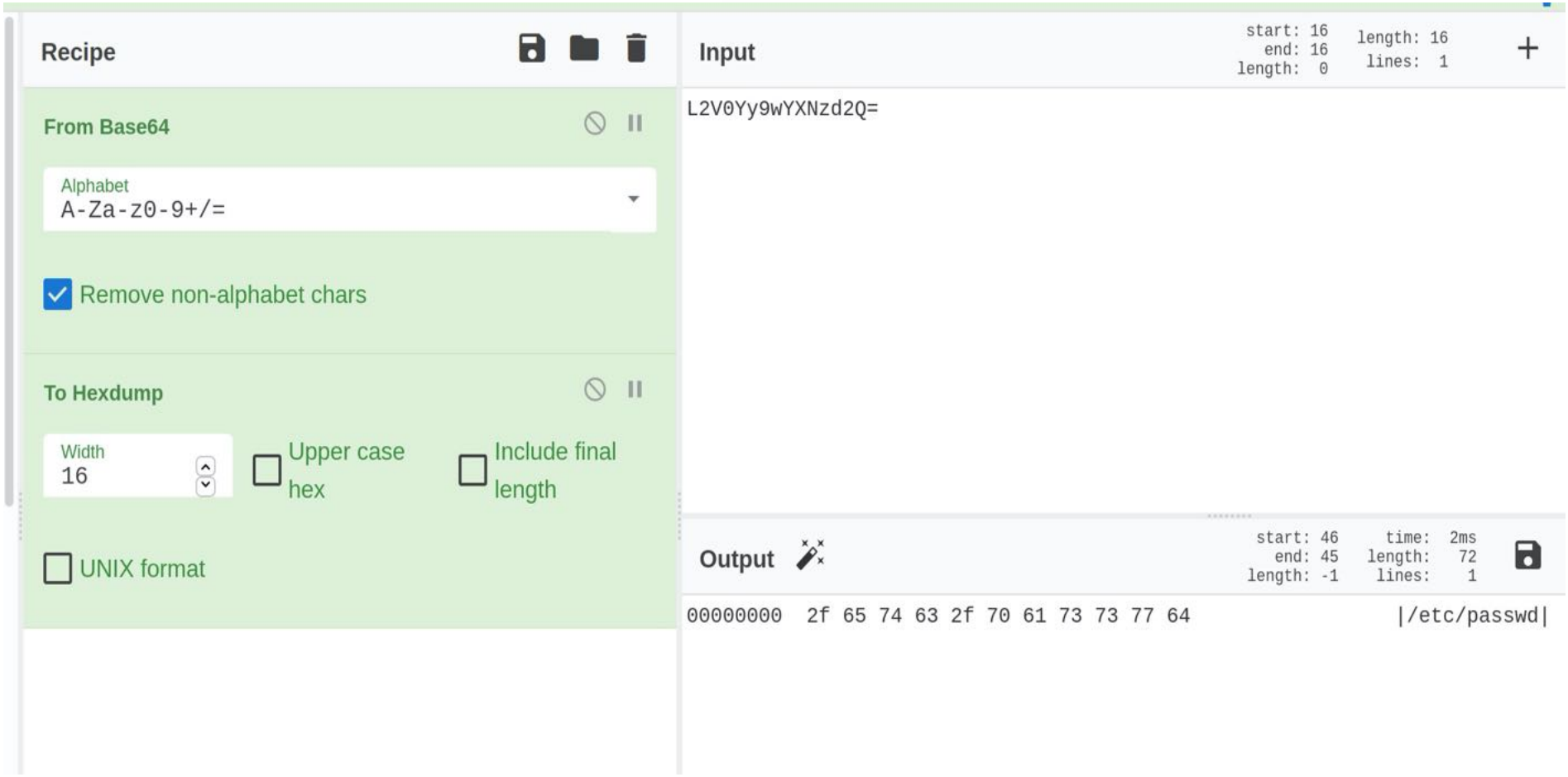
CyberChef

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

CyberChef

Chaining



CYBER RANGES

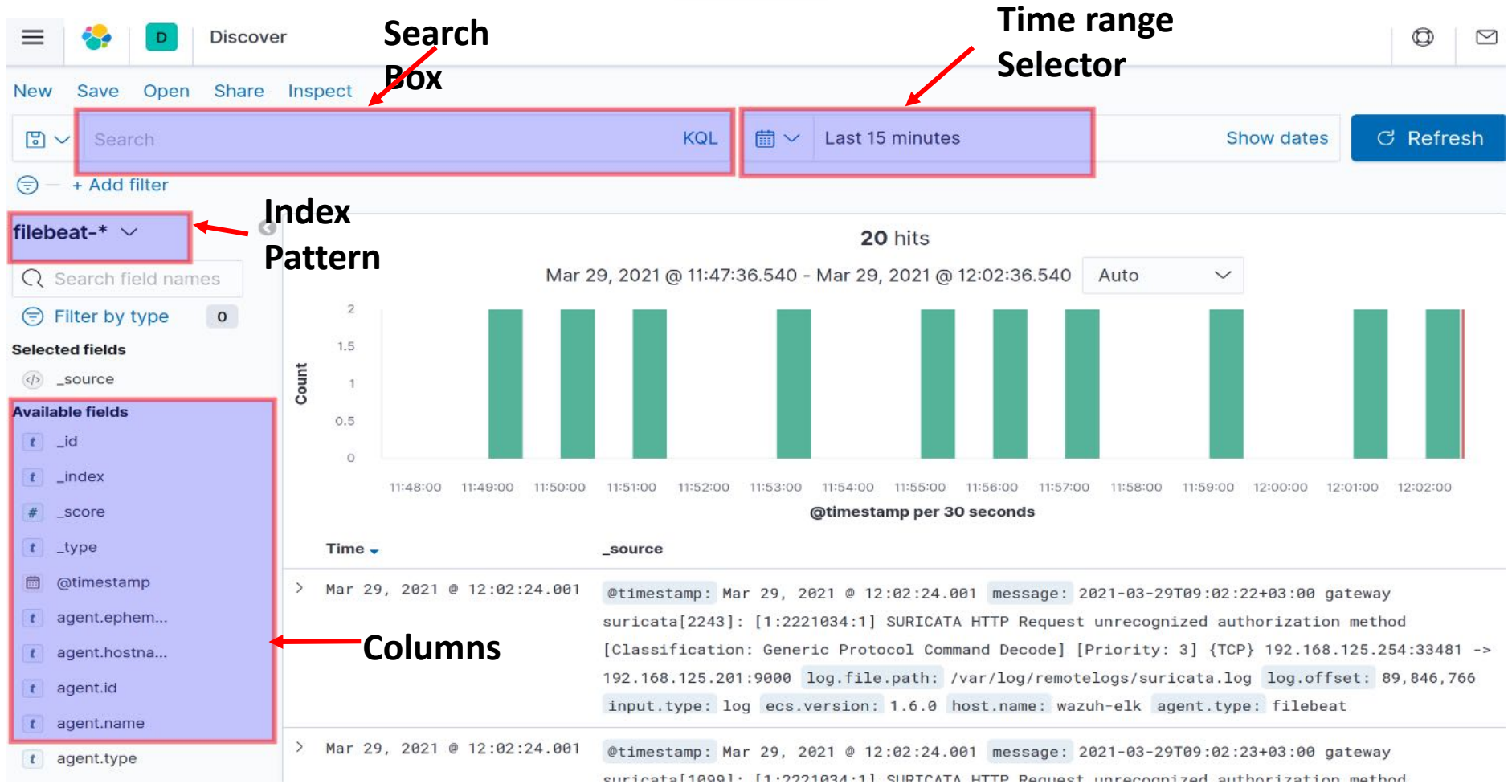
Viewing logs and log analysis with ELK and osquery

CYBER RANGES

silensec
ISO27001 Certified

Viewing Logs and Log Analysis with ELK and Osquery

ELK



ELK

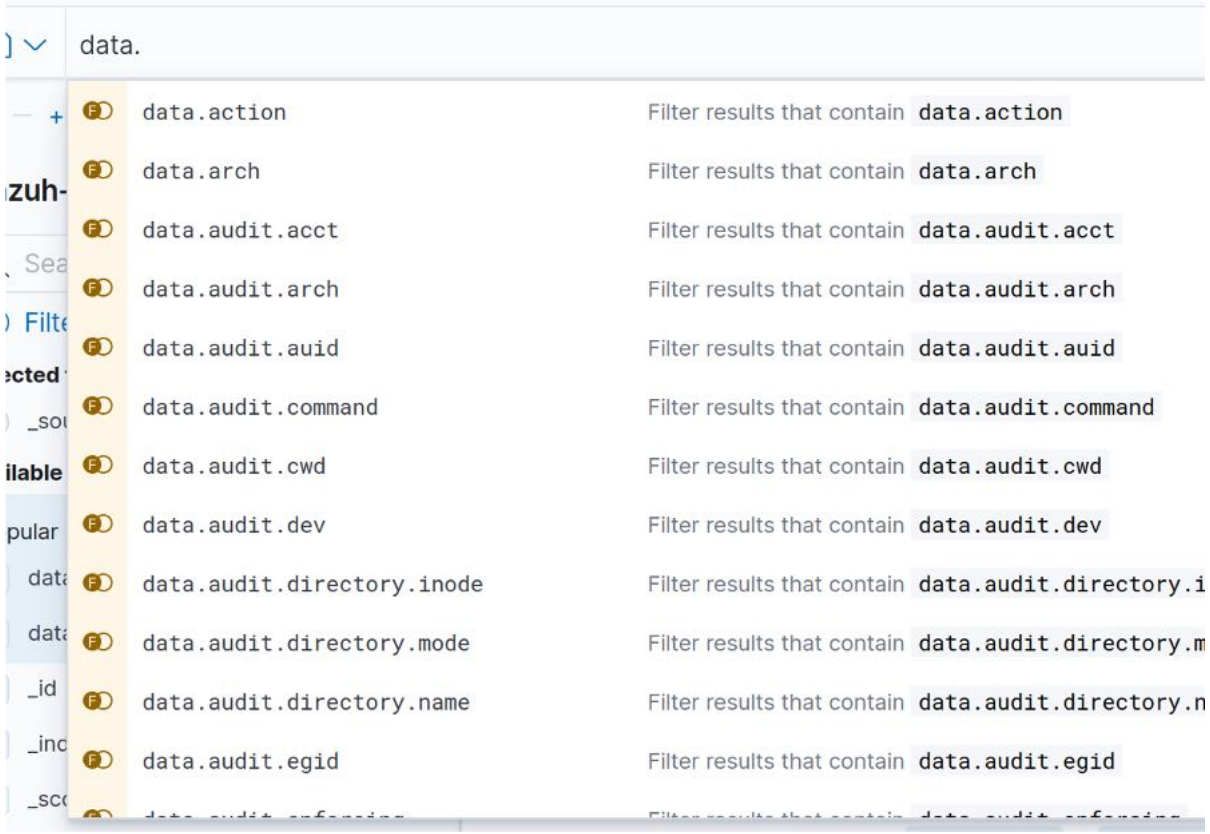
- You enter the search criteria on the Search Box
- **Always** ensure your time-range is correct
- Free text search - if keyword appears **anywhere**

```
172.16.0.102
```

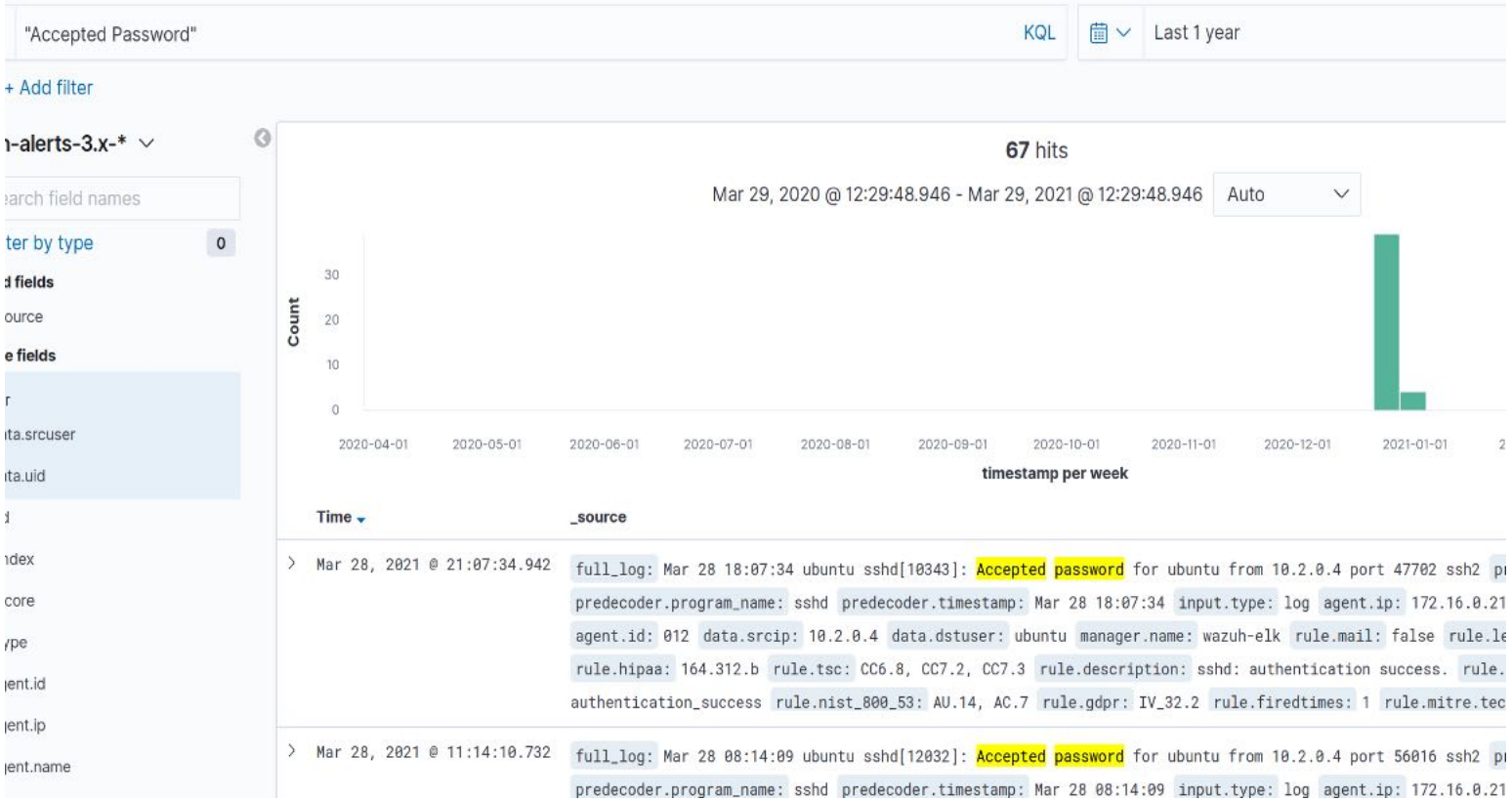
- Field-based searches

```
data.srcip:172.16.0.100
name:”Ned Stark”
age:[3 TO 10]
price:{100 TO 400}
```

- Kibana Auto-Completes fields for you

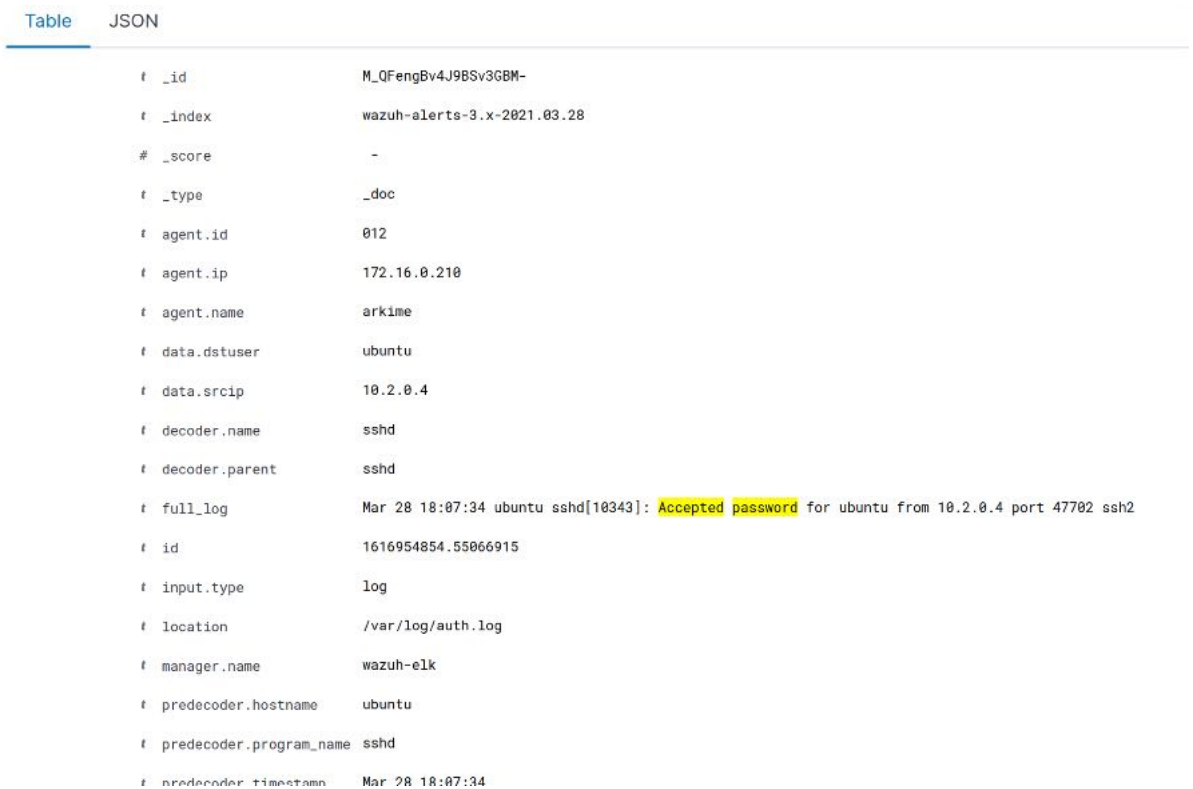


- Can search for exact text match



ELK

- Can expand individual logs to view more info



- Add more columns from the left side-bar

timestamp per week

Time	agent.name	agent.ip	data.dstuser	data.srcip	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	ftpserver	172.16.2.51	root	10.2.0.4	Valid Accounts, Remote Services
Mar 16, 2021 @ 14:51:59.152	ftpserver	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

OSQuery Analysis

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

OSQuery Analysis

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)

OSQuery Analysis

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	