# HideZeroOne
# INE – Cyber Sec
# www.hide01.ir


OUTLINE

# Table of Contents

## Module 01 | SIEM Fundamentals & Open Source Solutions

1.1 SIEM: Definition, Benefits & Solutions

1.2 SIEM Components, Architecture & Capabilities

1.3 SOC 3.0 Operations



OUTLINE

# Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ SIEM components, architecture and capabilities
- ✓ How ELK and Splunk can be used for security analytics
- ✓ SOC 3.0 operations



OUTLINE

1.1

# SIEM: Definition, Benefits & Solutions



OUTLINE

# 1.1 SIEM: Definition, Benefits & Solutions

Security Information and Event Management (SIEM) solutions provide blue teams with a complete picture of the events that take place on a network in real time.

As their name suggests SIEM solutions are able to:

- Analyze current or historical events and log data, perform event correlations and threat monitoring (Security Event Management part)
- Retrieve and index log data from disparate sources for analysis and reports (Security Information Management part)

# 1.1 SIEM: Definition, Benefits & Solutions

At this point we should mention that SIEM solutions are not only good for security monitoring purposes. They can also help an organization towards PCI DSS compliance. Specifically, a SIEM can meet the following PCI DSS requirements.

- ❑ Unauthorized network connection detection
- ❑ Search for insecure protocols
- ❑ Inspect traffic flow across DMZ

https://www.imperva.com/learn/data-security/pci-dss-certification

# 1.1 SIEM: Definition, Benefits & Solutions

Find below some benefits of using a SIEM solution:

- ✓ Extended Visibility
- ✓ Efficient Incident Identification and Handling / Response
- ✓ Reducing the impact of security breaches
- ✓ Better reporting, log analysis and retention
- ✓ IT compliance



OUTLINE

# 1.1 SIEM: Definition, Benefits & Solutions

When it comes to SIEM solutions, an organization could choose to deploy a solution like:

- ArcSight
- QRadar
- Splunk Enterprise Security

or go the open source way and utilize the ELK stack.

https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview
https://www.ibm.com/security/security-intelligence/qradar
https://www.splunk.com/en_us/software/enterprise-security.html
https://www.elastic.co/elk-stack



OUTLINE

1.2

# SIEM Components, Architecture & Capabilities



OUTLINE

# 1.2 SIEM Components, Architecture & Capabilities

SIEM solutions collect information and events from sources like:

- Host Systems / Web Servers
- Security Devices
- Routing Devices
- Applications etc.

All data are then indexed* and presented on a centralized platform.

* From Windows event and HIDS logs to proxy logs, SIEM solutions identify this data and sorts it into categories, such as malware activity, failed and successful logins, other potentially suspicious/anomalous activity etc.

# 1.2 SIEM Components, Architecture & Capabilities

In the context of this course, we will focus on two of the most effective SIEM solutions the ELK Stack and Splunk.

We chose to do so, because both require human interpretation of the collected data and in-depth knowledge of attacker TTPs in order to be effective.

Covering an automation-oriented SIEM solution would offer little in terms of incident response skillset development.

# 1.2 SIEM Components, Architecture & Capabilities

As you go through the lab manuals of the “Effectively Using Splunk” and “Effectively Using the ELK Stack” labs, you will notice that each SIEM’s components, architecture and capabilities are covered at the beginning of the respective lab manual (accompanied by pointers to important official documentation).

We did that so that you have a single point of reference.



OUTLINE

# 1.2 SIEM Components, Architecture & Capabilities

That being said let's quickly go through the architecture of an open source SIEM / Threat Hunting solution called HELK.

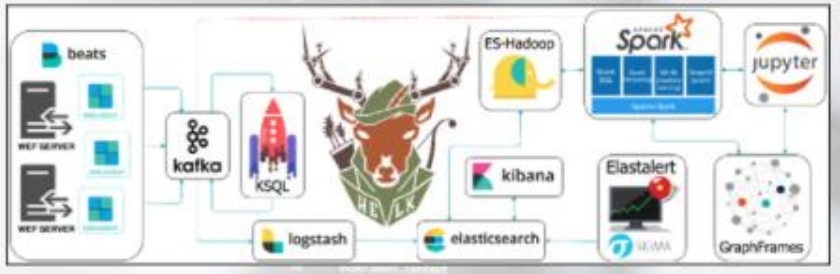
HELK is essentially a customized ELK stack with advanced analytic capabilities.

As you can see events are being sent to Logstash for filtering through Winlogbeat and Kafka brokers. Kafka was chosen due to its efficient, fast and fault-tolerant message-publishing capabilities, which are ideal for real-time data pipelines.

Events are then sent to an Elasticsearch database and from there on Kibana can come into play and visualize them.

Usage of the Apache Spark, GraphFrames and Jupyter analytics solutions is what sets HELK apart from other ELK instances. More specifically:

- Spark can subscribe to specific Kafka topics and use them to apply analytics
- Spark has a Python API (PySpark). It is possible to interact with PySpark from a Jupyter Notebook. This means that every Jupyter-created notebook will have the possibility to leverage Spark Python APIs
- GraphFrames is a package for Apache Spark which provides DataFrame-based Graphs. Its extended functionality includes motif finding, DataFrame-based serialization and highly expressive graph queries




https://github.com/Cyb3rWard0g/HELK
https://spark.apache.org/docs/latest/
https://github.com/graphframes
https://jupyter.org/



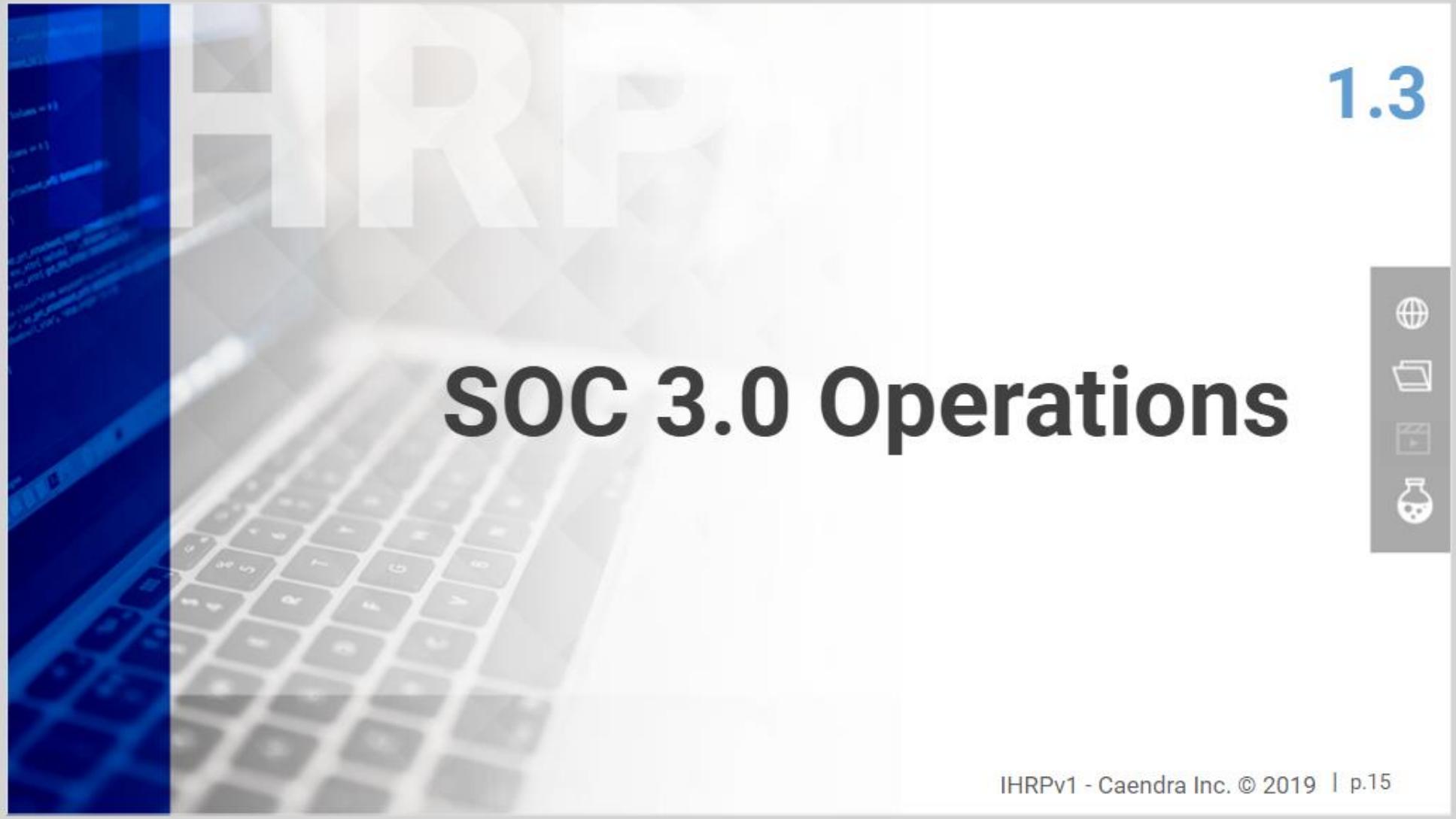
OUTLINE

# 1.2 SIEM Components, Architecture & Capabilities

"SIEM architecture" is a topic that mostly concerns security engineers. As an analyst, it is nice to have a high level understand of SIEM components and their interconnections though.



OUTLINE



1.3

# SOC 3.0 Operations



OUTLINE

# 1.3 SOC 3.0 Operations

The following is mostly about SOC architecture and mentality.

That being said SOC 3.0 operations will eventually find their way into organizations and this will affect the kind of data SIEM solutions ingest as well as the usage of SIEM solutions.

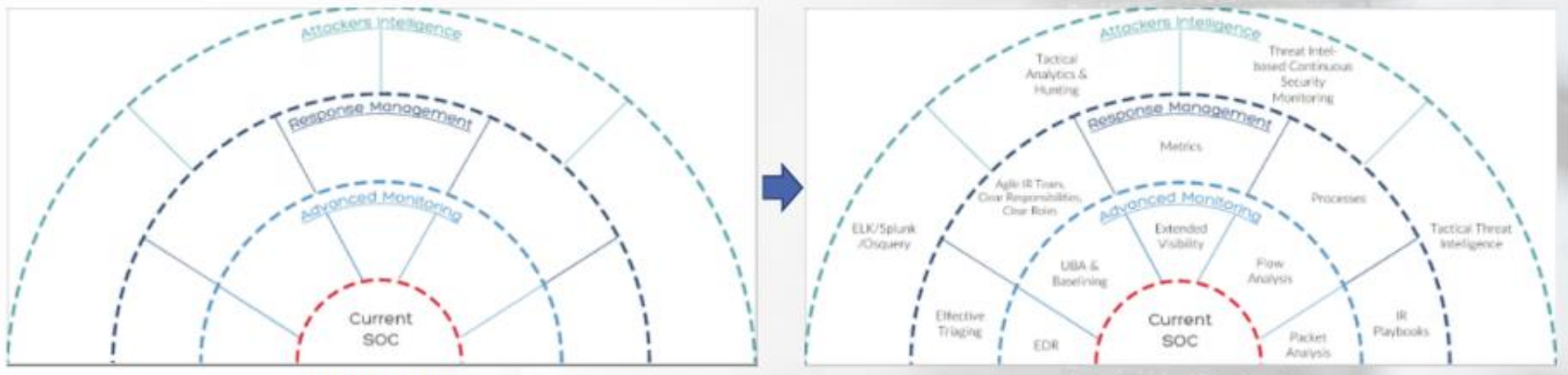
# 1.3.1 State of the SOC

Latest studies have shown that SOCs worldwide suffer from:

- Shortage of cyber security talent
- Alert fatigue
- Limited visibility
- Not being able to keep up with the ever-evolving threat landscape

# 1.3.2 SOC 3.0 Operations

For a SOC to be effective a transition should be made to SOC 3.0 operations.




Current SOC

SOC 3.0

Even if SOCs are unable to immediately transition to SOC 3.0 operations, it is imperative that they heavily analyze and utilize Tactical Threat Intelligence so they can start establishing a Tactical Analytics capability based on attacker TTPs.



OUTLINE

# 1.3.2 SOC 3.0 Operations

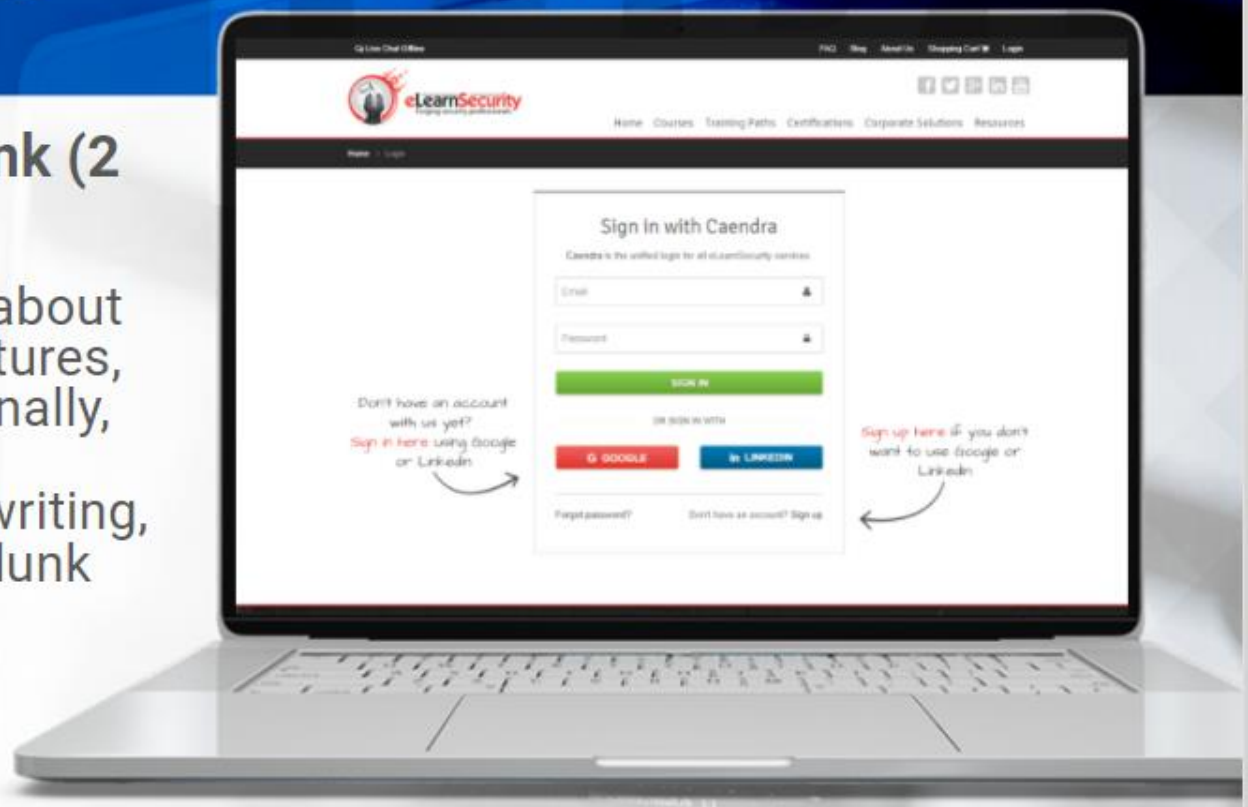
SOC 3.0 operations are not only about a shift in the utilized technology. They are also about a shift in mentality.

Organizations transitioning to SOC 3.0 operations, will adopt a proactive and threat intel-based defense approach.

# **LAB:** Effectively Using Splunk

## Effectively Using Splunk (2 Scenarios)

In this lab, you will learn about Splunk's capabilities, features, and architecture. Additionally, you will get familiar with effective Splunk search writing, so that you can make Splunk suit your detection and analysis needs.




***To access, go to the course in your members area and click the lab drop-down in the appropriate module line to access a lab, or go to the virtual labs tab on the left navigation.***

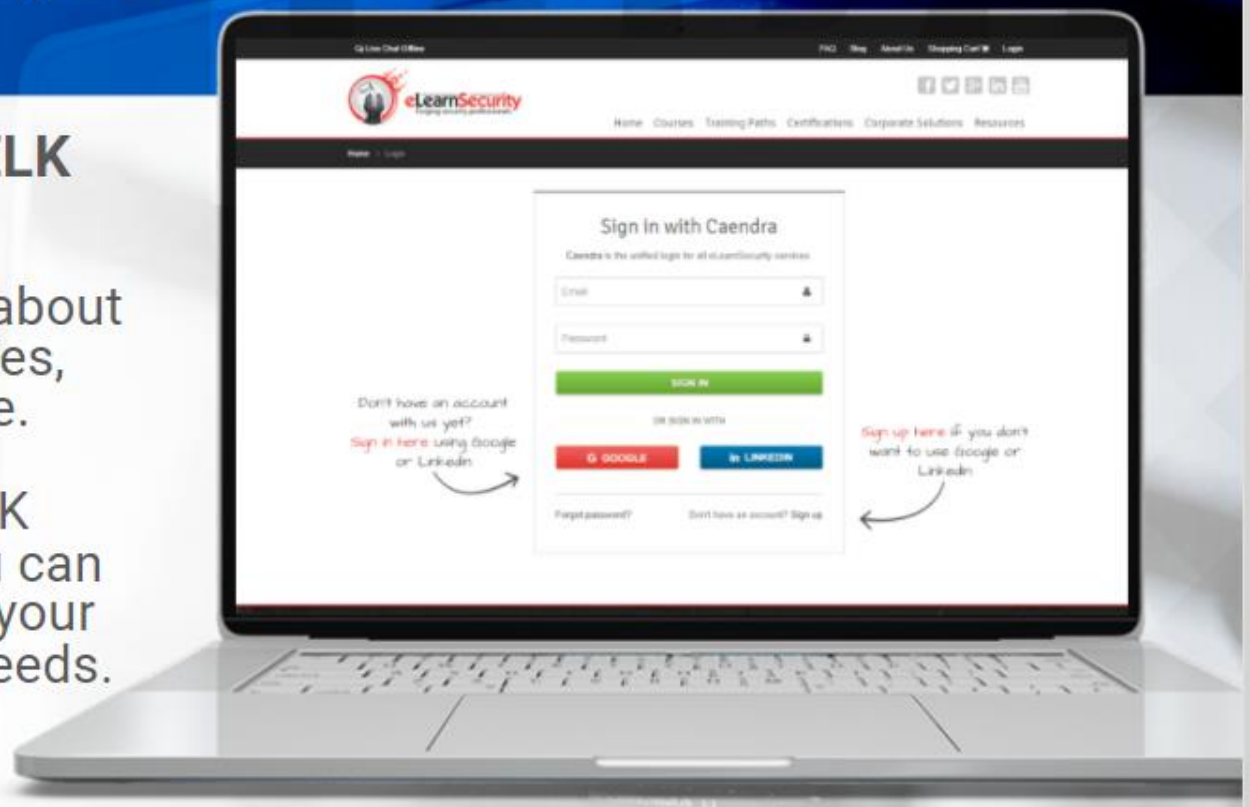


OUTLINE

# LAB: Effectively Using ELK Stack

## Effectively Using the ELK Stack

In this lab, you will learn about the ELK stack's capabilities, features, and architecture. Additionally, you will get familiar with effective ELK query writing, so that you can make the ELK stack suit your detection and analysis needs.




**To access, go to the course in your members area and click the lab drop-down in the appropriate module line to access a lab, or go to the virtual labs tab on the left navigation.*



OUTLINE

# References



OUTLINE

# References

## PCI DSS compliance

https://www.imperva.com/learn/data-security/pci-dss-certification

## ArcSight

https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview

## QRadar

https://www.ibm.com/security/security-intelligence/qradar

## Splunk Enterprise Security

https://www.splunk.com/en_us/software/enterprise-security.html

# References

## ELK stack

https://www.elastic.co/elk-stack

## HELK

https://github.com/Cyb3rWard0g/HELK

## Spark

https://spark.apache.org/docs/latest/

## GraphFrames

https://github.com/graphframes

# References

## Jupyter

https://jupyter.org/

# Labs

## Effectively Using Splunk (2 Scenarios)

In this lab, you will learn about Splunk's capabilities, features, and architecture. Additionally, you will get familiar with effective Splunk search writing, so that you can make Splunk suit your detection and analysis needs.

## Effectively Using the ELK Stack

In this lab, you will learn about the ELK stack's capabilities, features, and architecture. Additionally, you will get familiar with effective ELK query writing, so that you can make the ELK stack suit your detection and analysis needs.

***To access, go to the course in your members area and click the lab drop-down in the appropriate module line to access a lab, or go to the virtual labs tab on the left navigation.***