



EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Co-funded by
the European Union

Acknowledgement

- *Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Network Protection for Energy Control Systems

Overview

- Topic-1: Introduction to Energy Control Network Protection
- Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks
- Topic-3: Essential Protection for Energy Control Networks
- Topic-4: Advanced Protection for Energy Control Networks

Agenda

01. Security Monitoring
02. SIEM Information Sources
03. SIEM Functionality
04. Example SIEM Solutions
05. Elasticsearch and Kibana

Objectives

At the end of this session, you should be able to ...



1. Describe the **different types** of security **information** and **events**
2. **Associate** the different **types** of security **information** and **events** with the **tools** that generate them (e.g. attack **detection alerts** originate from an **IDS**, etc.)
3. Explain the **challenges** of security **information** and **event management** and how **SIEM solutions** address these **challenges**, i.e. describe their **purpose**
4. **Describe** the **functionality SIEM solutions** typically provide
5. List the main **SIEM solutions** that are **available** on the **market (commercial and open-source)** and their features

Security Monitoring

- **Monitoring** is **necessary** to **determine** if a breach in security has **occurred** or if a **control** has been **circumvented**.
- Security **controls** can provide indicators of **potential threat** agent activity.
- The following can provide **these indicators**:
 - Anti-Virus Systems (AVS)
 - Syslog
 - Firewall Logs
 - Network Intrusion Systems (NIDS)
 - Host Intrusion Detection Systems (HIDS)
- **Continuous** security **monitoring** is essential to the protection of **critical** systems.





A Major Security Challenge: Data Overload

- We are drowning in security data:
 - System logs
 - Proxy logs
 - Application logs
 - Firewall logs
 - Antivirus logs
 - NIDS events
 - HIDS events
 - Packet captures
- No single **indicator** is useful by **itself** when **determining** whether an **asset** is **compromised**.



Managing Security Information and Events

- **Security Information and Event Management (SIEM) solutions** can help to **mitigate** data **overload**.
- A **SIEM solution** is an integrated suite of **security tools** used to **manage multiple** security **applications** and **devices**.
- SIEM **applications** present a holistic view into the relative **state** of security across a network or enterprise.
- SIEMs have the **capability** to **normalize** logging data.

SIEM Information Sources



Security Devices

- Network Intrusion Detection Systems (NIDS)
- Host Intrusion Detection Systems (HIDS)
- Intrusion Prevention Systems (IPS)
- Antivirus Software
- Honeypots
- Firewalls



Network Devices

- Routers
- Switches
- Wi-Fi Access Points
- VPN Gateways
- Network Taps



Server

- Web Servers
- Mail Servers
- Application Servers
- Databases
- Cloud Servers



Applications

- Intranet Applications
- Web Applications

Technologies and Data



Firewall

- Log data



HIDS, NIDS, IPS

- Alerts



Routers, Network Taps

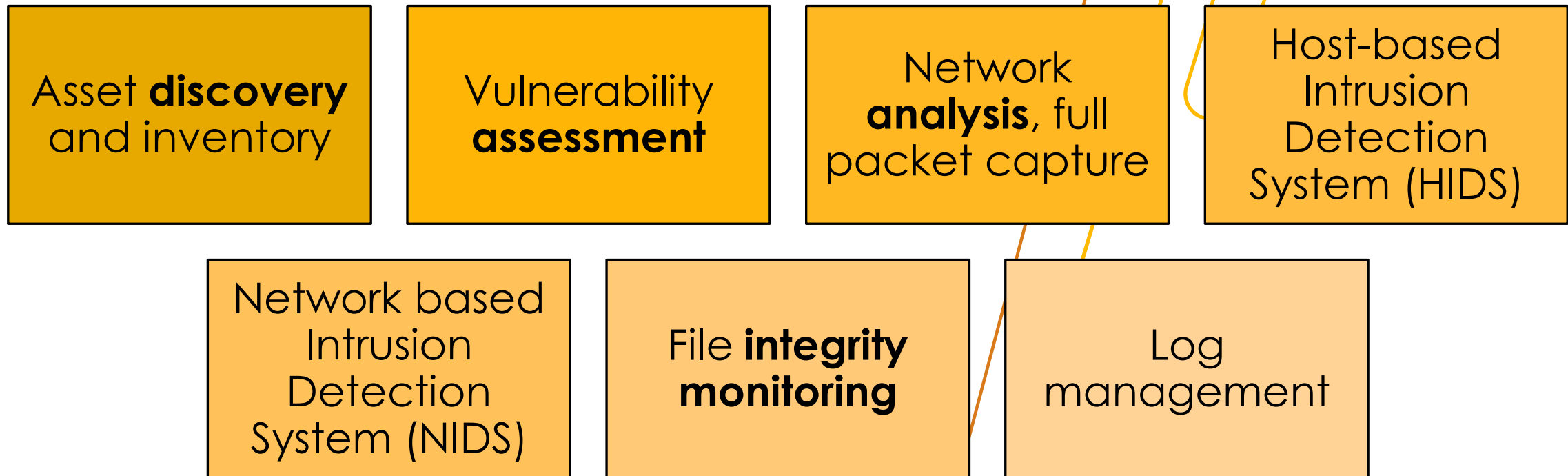
- Full packet captures
- Flow data



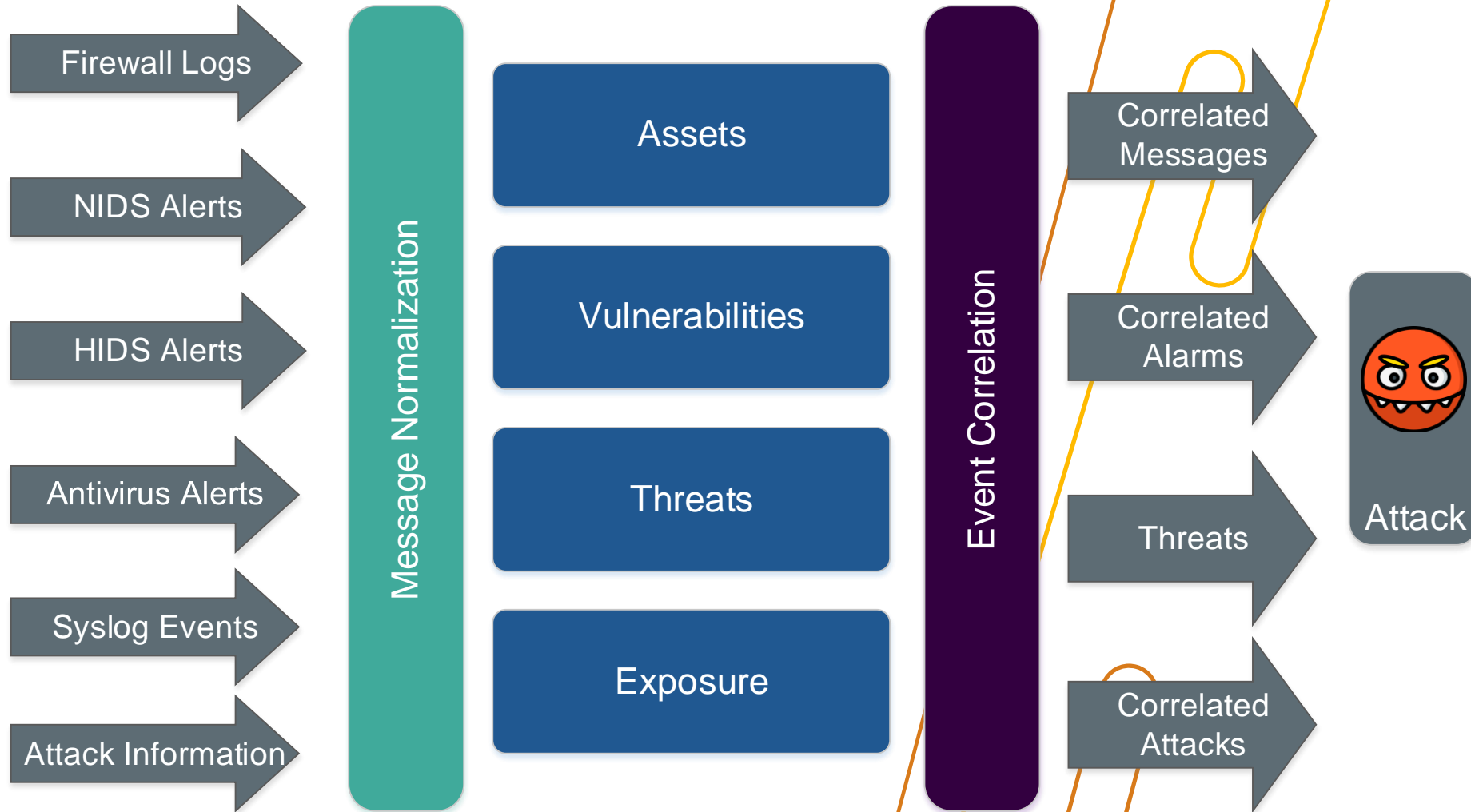
Servers, Workstations

- System logs
- Monitoring agents

SIEM Functionality



SIEM Process



Example SIEM Solutions

- **Commercial**

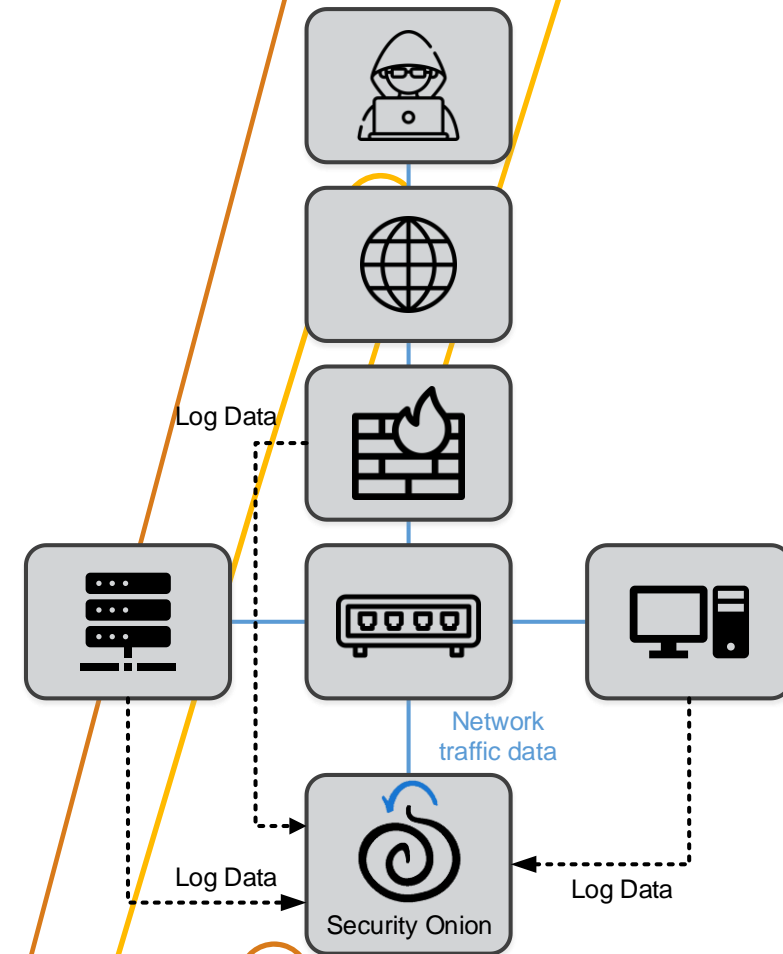
- Micro Focus ArcSight Enterprise Security Manager (ESM)
- AlienVault Unified Security Management USM
- Splunk
- SolarWinds Security Event Manager
- Elastic SIEM

- **Open Source**

- **Security Onion**
 - <https://securityonionsolutions.com>
- Open Source Security Information Management (OSSIM)
 - <https://www.alienvault.com/products/ossim>

Security Onion

- **Free** and **open platform** for **Network Security Monitoring (NSM)** and **Enterprise Security Monitoring (ESM)**
- The **NSM** is monitoring the network for security related events
 - **Proactive**: identify **expiring** SSL certificates
 - **Reactive**: **incident response** and network **forensics**
 - Provides context, **intelligence**, and situational **awareness** of your network
- The **ESM** adds endpoint **visibility** and **other telemetry**



Network Security Monitoring

Intrusion detection

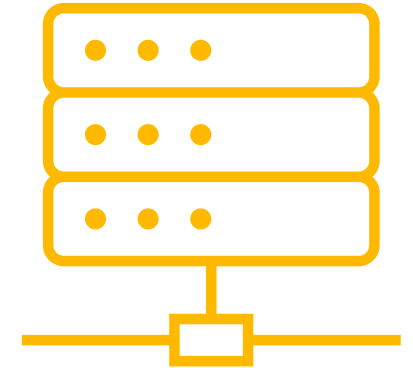
NIDS (Network Intrusion Detection System) monitors network **traffic** and uses attack **fingerprints** and **identifiers** to **detect suspicious activities**
Suricata can be used as a **NIDS**

Network metadata

Logs of **connections** and **standard protocols** like DNS, HTTP, FTP, SMTP, SSH, and SSL.
Visibility of the context of **data** and **events**

Full packet capture

Records all **data** on the network
Provides **information** about **when, where, and what**



Enterprise Security Monitoring

- Provides **endpoint** visibility and can **collect logs** from a wide **variety** of **devices** like **firewalls** and **routers**.
- For **endpoint** detection **Kibana** is providing an **Wazuh** plugin
 - **Wazuh** is a **free, open source HIDS (Host Intrusion Detection System)** for different **operating systems**.
 - The **Wazuh** agent **provides** visibility of network **endpoints**.
 - Supports **real-time alerting, file integrity checking, log file analysis, policy monitoring, rootkit detection, and active response**.
- The **correlation** of **host-** and **network-based events** can improve **incident detection capabilities significantly**.
- Collect **information** also from other **endpoint** agents like **osquery**.
- Use standard **Syslog** in **cases** where agents are not **available** or can not be **installed** for other reasons.



OSSIM

- **OSSIM** is the **Open Source Security Information Management**
- OSSIM provides **log analysis**, **asset** and **vulnerability management** and **detection systems** using other open-source software security components
- Browser-based user interface for graphical analysis
- **OSSIM** includes:
 - Asset discovery
 - Vulnerability assessment
 - Intrusion detection
 - Behavioral monitoring

Elasticsearch and Kibana



- **Elasticsearch** is a distributed **RESTful search and analytics engine** that enables fast **searching, indexing, and analyzing of data**.
- **Kibana** is an open-source **data visualization dashboard** for **Elasticsearch**, which provides **visualization** capabilities on top of the **content indexed** on an **Elasticsearch cluster**.
- Users can create **bar, line, and scatter** plots or **pie charts** and **maps** on top of **large volumes** of data.
- In the **SIEM** context, **Kibana** enables users to **investigate, analyze, filter, and visualize different** network aspects (**system states, events, traffic, etc.**).

Functions Overview

- The **Elastic platform** offers a variety of **search**, **filtering**, and **visualization** functions for **analyzing diverse system data sets**. The most important functions are
 - **Kibana**
 - **display** and **share** a **collection** of visualizations
 - interactively **explore data** by **querying** and **filtering** documents
 - create **visualizations** and **aggregate** data **stores** in **Elasticsearch** indices
 - **Observability**
 - **monitor** and **react** to events happening within the **entire environment**
 - **Security**
 - explore **security metrics** and **logs** for **events** and **alerts**
 - **Wazuh plugin**
 - security information management
 - threat detection and response
 - auditing and policy monitoring



What Is Kibana?

- Kibana **offers** comprehensive and **well-structured** overviews of Elastic Stack data by providing the following key **functions**:
 - An **analytics** and **visualization** platform for user-tailored **filtering** and **visualizations** of **Elasticsearch** data
 - A user **interface** for **Elastic Stack management** (security **settings**, user **roles**, **snapshots**, etc.)
 - A **centralized hub** for accessing Elastic's **solutions**, from document **discovery** to **SIEM** functions



Elastic Security

- **Elastic Security** offers **threat detection** features, endpoint prevention, and response **capabilities**, including:
 - A detection **engine** to **identify** attacks and system **misconfiguration**.
 - A workspace for **event triage** and **investigations**.
 - Interactive **visualizations** to **investigate** process **relationships**.
 - **Embedded** case **management** and **automated actions**.
 - Detection of **signatureless** attacks with prebuilt **machine-learning anomaly** jobs and detection rules.



Security Views 1/2

- Security **views** are **accessed** through the **sidebar** menu under the "**Security**" keyword. Central views of Security covered in this manual are the Detections, Hosts, Network, Timelines and Cases views.
- **Detections View**
 - The **Detections** feature **searches** for **threats** and creates **alerts** when they are **detected**.
 - **Alerts** are **created** based on **conditions** defined by **detection** rules.
- **Hosts View**
 - Key **metrics** regarding **host-related** security events.
- **Network View**
 - Overview of **key network** activity **metrics** in an **interactive** map and **event tables**

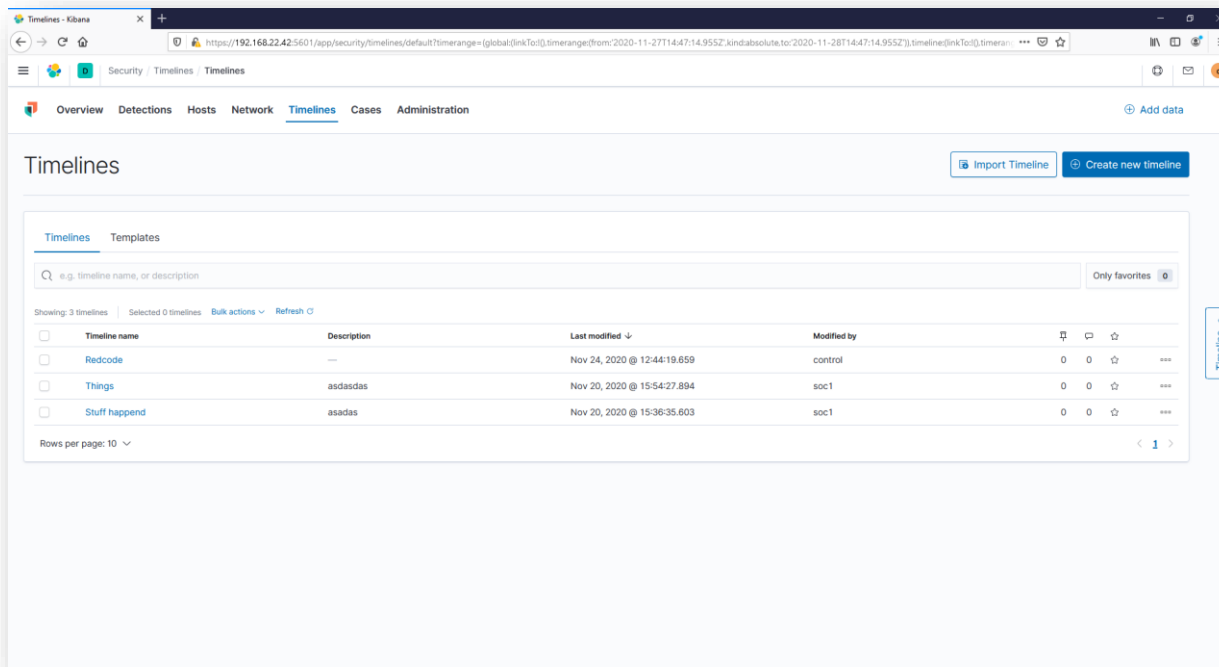
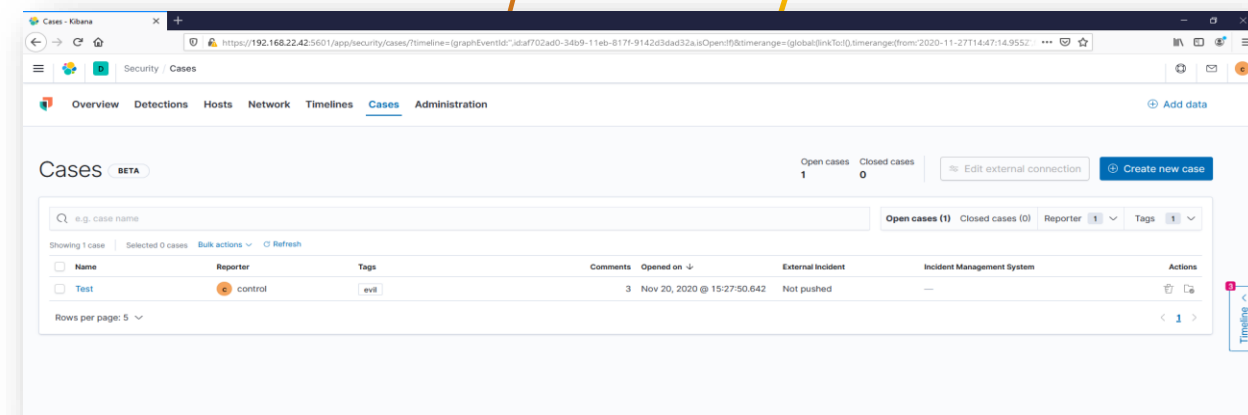
The screenshot shows the 'Detections' view in the Kibana interface. The top navigation bar includes 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. The main content area displays a 'Trend' bar chart showing 870 alerts over time, with a legend for 'Unusual Process Execution - Temp' and 'Persistence via Kernel Module Modification'. Below the chart is a table of alerts with columns for timestamp, rule, severity, risk score, event module, event action, event category, host name, user name, and source IP.

Timestamp	Rule	Severity	Risk Score	event.module	event.action	event.category	host.name	user.name	source.ip
Nov 28, 2020 @ 14:58:59.328	Unusual Process Execution...	medium	47	auditd	executed	process	backup-server	root	---
Nov 28, 2020 @ 14:58:59.328	Unusual Process Execution...	medium	47	auditd	executed	process	backup-server	root	---
Nov 28, 2020 @ 14:58:59.328	Unusual Process Execution...	medium	47	auditd	executed	process	backup-server	root	---
Nov 28, 2020 @ 14:58:59.328	Unusual Process Execution...	medium	47	auditd	executed	process	backup-server	root	---

The screenshot shows the 'Hosts' view in the Kibana interface. The top navigation bar includes 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. The main content area displays a 'kibana' host profile with fields for Host ID, IP addresses, MAC addresses, Platform, Operating system, Family, Version, Architecture, Cloud provider, Region, Instance ID, and Machine type. Below the profile are two charts: 'User authentications' showing 202 success and 0 fail, and 'Unique IPs' showing 40 source and 35 destination.

Security Views 2/2

- **Timeline View**
 - **Workspace** for **alert investigations** and **threat discovery** in the network.
 - Interesting **objects** can be **dragged** and **dropped** objects of interest (e.g., IP addresses) into the **Timeline Event Viewer**



- **Cases View**

- The **Cases view** is used to open and track security **issues**. Descriptions of **cases**, as well as **comments**

Wazuh Kibana Plugin

- **Wazuh** provides a **host-based security** visibility using **lightweight** agents
- It is an **open-source** project supporting **detection, visibility, and compliance**.
- The **Wazuh plugin** allows for visualization and analysis of Wazuh alerts **stored** in **Elasticsearch**. It provides the following **features**:
 - Search and filter alerts
 - View and edit the Wazuh manager configuration
 - Manage ruleset (rules, decoders, CDB lists)
 - Manage groups of agents
 - Check the status and logs of the Wazuh cluster
 - Manage agents, their configuration, and data inventory
 - Explore and interact with the Wazuh API through the Dev Tools



Fleet and OSQUERY

- Fleet is an **open-source** device management tool using **osquery**.
- **osquery** is an agent for **operating system monitoring**, and analytics framework.
- **osquery** can query **running processes**, load kernel **modules**, open network **connections**, browser **plugins**, **hardware** events, **file hashes**, etc.
- Run live **queries** against **all** or a **subset** of hosts.



Summary

- There is a **deluge** of **security information** and **events** that can be used to support security operations
- A major **challenge** is data overload because of the **vast quantities** of security information from a multitude of **sources**
- **Security Information and Event Management (SIEM) solutions** are intended to address this **challenge**
- **SIEM solutions** ingest data of various **sorts**, **normalize** it, and provide **visualization** and **analysis tools** to support **security operations**
- Several **commercial** and **open-source** solutions **exist**

Connect with CyberSecPro: How to register and other practical information

1. Website:
www.cybersecpro-project.eu
2. X (Twitter):
https://twitter.com/CyberSecPro_eu
3. LinkedIn:
<https://www.linkedin.com/company/cybersecpro-euproject/>



**Co-funded by
the European Union**

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany Visit Website	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria Visit Website	APIROPLUS SOLUTIONS LTD Cyprus Visit Website	SINTEF AS Norway Visit Website	Social Engineering Academy GmbH Germany Visit Website	Tallin University of Technology Estonia Visit Website
Logo missing	 COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Visit Website	COFAC Portugal Visit Website	Consiglio Nazionale delle Ricerche Italy Visit Website	Technical University of Braunschweig Germany Visit Website	Technical University of Crete Greece Visit Website	trustilio B.V. The Netherlands Visit Website
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 LNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FDICAL POINT Belgium Visit Website	Goethe University Frankfurt Germany Visit Website	Information Technology for Market Leadership Greece Visit Website	Uninova Portugal Visit Website	Universidad de Malaga Spain Visit Website	Universidade Nova De Lisboa Portugal Visit Website
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télécom France Visit Website	Laurea University of Applied Sciences Finland Visit Website	Maggioli S.p.A. Italy Visit Website	University of Cyprus Cyprus Visit Website	University of Novi Sad Faculty of Sciences Serbia Visit Website	University of Piraeus Research Center Greece Visit Website
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal Visit Website	Security Labs Consulting Ltd Ireland (Republic) Visit Website	Serious Games Interactive Denmark Visit Website	ZELUS P.C. Greece Visit Website		

Thank you

Please send all questions to:
Stefan Schauer

Stefan.Schauer@ait.ac.at

Abdelkader Shaaban,

abdelkader.Shaaban@ait.ac.at