

Teams: GLSD & SIBC

Workshop on:

Enterprise Security with Elastic XDR

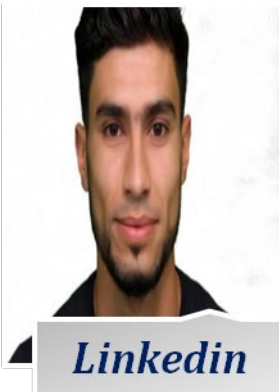
Enterprise Security has significantly changed in the era of cloud computing, Big data, machine learning, etc. New threats with higher levels of sophistication are born every day, which requires more evolving technologies and processes to counter them.

Elastic XDR builds on the power of Big data and the Elastic Stack to deliver a limitless and unified solution that provides detection, prevention, and response capabilities across the different levels of the organization's infrastructure.

In this workshop, you will learn about the Security mechanisms for Enterprise Security and how Elastic XDR actuate the big data to protect organizations from security threats.

Presented by Dr. Abdelwahhab Satta

Abdelwahhab has a PhD in cyber security and he is an Elastic specialist who works currently as a senior security solutions architect at Octodet. In his role, he helps businesses and industries building their Security Operation Centers (SOCs), Managed security services (MSSPs) and Managed Detection and Response services (MDRSs) on top of the Elastic XDR.



Learning Objectives

By participating in this workshop, you will:

- Learn about the fundamentals of Enterprise Security
- Learn about the role of big data in the core of enterprise security
- Learn about the design and implementation of Modern Security Operation Centers and Security as a Service
- Gain experience with Elastic Stack

Workshop Details

- **Technologies:** Elasticsearch, Kibana, Logstash, Beats, Elastic Agent.
- **Assessment Type:** Installation of the Elastic Stack and Ingest of some sample data, build of some visualizations using Kibana.
- **Hardware Requirements:**
 - Desktop or laptop computer capable of running the latest version of Chrome or Firefox.
 - Internet connection.
- **Operating System:** Preferably Linux or MacOS/ Windows with 4 GB RAM and 20 GB space or more to install the stack.
- **Downloads required:**
 - Elasticsearch : latest version (<https://www.elastic.co/downloads/elasticsearch>)
 - Kibana: latest version (<https://www.elastic.co/downloads/kibana>)
 - Logstash: latest version (<https://www.elastic.co/downloads/logstash>)
 - Filebeat: latest version (<https://www.elastic.co/downloads/beats/filebeat>)
 - Elastic Agent: latest version (<https://www.elastic.co/downloads/elastic-agent>)
- **Target audience:** Research professors, Doctoral researchers, Students, Social & business partners of the conference.
- **Languages:** English

Program

***December 12th 2022,
IT Room, NTIC Faculty, Constantine2-University***

Class 1 : <09:00 – 11> Enterprise Security Fundamentals

- **Session 1 — Overview of Enterprise Security**
 - Introduction to Enterprise security, current challenges and opportunities.
- **Session 2 — Big data in the core of Enterprise Security**
 - Security data sources, Log management, Security Events correlation, etc.

Class 2 : <11:15 – 13> Modern Security Operation Centers & Security-a-a-Service

- **Session 1 — Architecture, Implementation, Operation of a SOC**
 - Architecture design, State of the art of used technologies, SOC operations, Maturity levels, etc.
- **Session 2 — MITRE ATT&CK Framework, Proactive Security, and Threat Hunting**
 - Understanding the MITRE ATT&CK Framework, Exploration of the Enterprise Matrix, Introduction to Threat Hunting and Proactive Security.
- **Session 3 — Security as a Service: MSSPs vs MDRSs**
 - Understanding Security as a service and the different delivery models: MSSPs vs MDRSs.

Class 3: <13:30 – 16h> Hands on the Elastic Stack for security services

- **Episode 1 — Know what: Elasticsearch, Logstash, Kibana?**
 - Introduction to Big data management and exploration with the Elastic Stack.
- **Episode 1 — Deployment of the Elastic Stack & ingest of sample data**
 - Hands on Lab about the deployment of the Elastic Stack and ingestion of some sample data.
- **Episode 2 — Elastic XDR, Security Analytics, ML with Elastic Stack, etc.**
 - Exploration of Elastic Security features and capacities, and illustration with simple scenarios.