Course Description

SIEM-SOC course for admins, analysts, and advanced users.

this 5 day course will walk you through the SIEM-SOC world with the advanced theory of SOC generations, strategies, build your own SOC, and open discussions to enrich knowledge and share new ideas between the students. altogether with many LABs to practice event lifecycle via data mining, normalizing, handling and visualizing to better understand SIEM behind the scene.

How to get data, how to sanitize, normalize, aggregate, parse and so forth.
We will use cutting-edge SIEM and data technologies, environments and best practices to get you deep inside the process.

Target Audience

SIEM/SOC operators and managers , SIEM analysts

Prerequisites

- Knowledge in Regex
- Working with a SIEM solution
- Knowledge with ELK solution