CYBERUNIVERSITY
by DataScientest

Intrusion Detection & SOC Program

Intrusion Detection & SOC

This training will allow you to identify and understand analysis and detection techniques. This course covers the most advanced attack techniques.
You will acquire the knowledge needed to deploy various intrusion detection tools and implement prevention solutions.
You will also learn the concepts and environment of a Security Operations Center (SOC).

TARGET AUDIENCE

- Systems and network engineers/administrators
- Security managers, SOC/Forensic analysts, and anyone meeting the prerequisites

PREREQUISITES

- Strong knowledge of networks and systems (Windows & Linux)
- Strong knowledge of cybersecurity

Duration: 4 days

TRAINING PROGRAM

1 - LOGGING SYSTEM:

- Prerequisites for setting up a logging system
- Architecture and design of a logging system
- Introduction to security incident detection

2 - INTRUSION DETECTION/PREVENTION SYSTEM:

- Definition and terminology
- The objectives of an IDS/IPS
- How an IDS/IPS works
- NIDS/NIPS in a network architecture
- Different IDS/IPS solutions
- NIDS/NIPS rules

3 - SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM):

- Definition and terminology
- The objectives of a SIEM
- How a SIEM works
- SIEM rules (Alert, Sigma, etc.)
- SIEM in a network architecture
- Different SIEM solutions
- Case study of a SIEM solution

4 - ENDPOINT DETECTION AND RESPONSE (EDR):

- Definition and terminology
- The objectives of an EDR
- How an EDR works
- EDR rules (Alert, Yara, etc.)
- Different EDR solutions
- Case study of an EDR solution

5 - HONEYPOT:

- Definition and terminology
- The objectives of a Honeypot
- How a Honeypot works
- Different Honeypot solutions
- Case study of a Honeypot solution

6 - NETWORK ANALYSIS: WIRESHARK:

- Objectives of Wireshark
- How Wireshark works
- Customizing menus
- Analysis of malicious traffic

7 - SECURITY OPERATIONS CENTER (SOC):

- Introduction to SOC
- Objectives of a SOC
- Services and functions of a SOC
- Structure of a SOC

8 - IMPLEMENTING A SOC:

- Defining your SOC project
- SOC architecture
- SOC tools
- Selecting and collecting the right data
- SLAs, indicators, and reporting
- BUILD phase
- RUN phase

9 - INCIDENT RESPONSE:

- What is incident management?
- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

10 - INTRODUCTION TO CYBER THREAT INTELLIGENCE (CTI):

- Definition and terminology
- Objectives of CTI
- The importance of CTI in a SOC
-

LEARNING OBJECTIVES

By the end of the training, participants will be able to:

- **Identify and understand analysis and detection techniques**
- **Acquire knowledge to deploy various intrusion detection tools**
- **Implement intrusion detection and prevention solutions**
- **Understand the concepts and environment of a Security Operations Center (SOC)**
- **Know how to use analysis tools**