Orange
Cyberdefense

Cyber Defense Training

Experience Cyberdefense from a new perspective.

Defense against attacks under real conditions is the best way to acquire the qualifications and expert knowledge that really help in an emergency. In the Cyber Simulation Range, our hyperrealistic training environment, budding security experts have the opportunity to test their defense capabilities using a variety of attacks against IT and OT infrastructures and gain priceless practical experience without endangering the security of a real company.

More than just intensive product training: immerse yourself completely

Cyber simulation training is more than just intensive product training. A cyber defender has to make quick and correct decisions under pressure together with other specialists. Attack parameters must be identified, analyzed, interpreted and documented using a range of tools.

This requires a training environment that comes as close as possible to reality. This is what makes our training offer:

- Fully equipped CyberSOC for training with all tools
- Realistic simulated company infrastructure: servers, clients, applications, databases, etc.
- Simulated OT components: segmented production networks, control components, etc.
- Crash courses in modern security tools: SIEM, proxies, sandboxes, NextGen firewalls, intrusion detection, ticketing
- Experienced analysts as trainers
- Realistic attack scenarios, based on real incidents from the daily practice of our CyberSOCs
- Immersive training environment: simulation of power failures, security alarms, etc.

Fit for emergencies

The course participants train with components from leading providers of security solutions:

- Security Orchestration & Automation (SOA)
- NextGen SIEM & Log Management
- AI-based flow analytics and intrusion detection
- AI-supported user behavior analytics
- Malware Detection & Analytics Platforms
- External threat intelligence
- Deceive & Deception technology
- Incident Response Systems

The Cyber Simulation Range is part of the Information Security Hub (ISH) under the leadership of Munich Airport.

More at https://www.ish-muc.com/

ISH
Information Security Hub

Find out more on our professional trainings:
orangecyberdefense.com/no/training/

"Theoretical knowledge is not enough! Anyone who defends critical company data in CyberSOC must recognize attacks under real conditions, correctly assess them and be able to react correctly. You can only learn that in practice - or in the Cyber Simulation Range."

Andreas Günther // Manager CyberSOC Germany, Orange Cyberdefense

CSR101 - Security Incident Action for SOC Analysts - Level 1

In this course, the interaction of the components of a state of the art CyberSOC is explained and experienced in practice. The basics of the most important tools are also explained and practically trained.

What you get:

- Understand how a State of the Art CyberSOC works and how it works.
- Use the integrated tools of a complete CyberSOC Technology Stack.
- Learn to recognize, analyze and correctly classify incidents.
- Get advanced information using external threat intelligence.
- Take on different roles in the CyberSOC team under realistic conditions.

Fit for the CyberSOC: Graduates of the training are prepared for practical work in the security center and can recognize, analyze and ward off attacks.

CSR102 - Security Incident Action for SOC Analysts - Level 2

In addition to the detection and defense against tricky attacks, the focus here is particularly on operational technology (OT). Because production networks in particular are increasingly becoming the focus of attackers.

What you get:

- Face the new challenges in IT & OT security.
- Use the professional tools in CyberSOC to filter the relevant events from the data stream.
- Detect, analyze and evaluate complex, multi-stage and targeted attacks efficiently.
- React correctly to critical incidents even under pressure.
- Work effectively in a team with security analysts, IT forensic experts and defense specialists.

Prepared for IT & OT: Those who have completed this course can also defend control systems and production OT from cyber attacks from the CyberSOC.

For more information check
https://orangecyberdefense.no

Orange Cyberdefense
Lysaker Torg 25, N-1366 Lysaker

info@no.orangecyberdefense.com
+47 67 57 37 37