BLACKBIRD FOR TRAINING

Advanced Cybersecurity Operations: Monitoring, Threat Management, and Secure Architecture

27 September – 1 October 2027
Düsseldorf (Germany)

UK Traininig
PARTNER



www.blackbird-training.com

Advanced Cybersecurity Operations: Monitoring, Threat Management, and Secure Architecture

Ref: 3255556_204677 **Date:** 27 September – 1 October 2027 **Location:** Düsseldorf (Germany) **Fees:** 5900 GBP

Introduction

In today's highly connected and constantly evolving digital landscape, cybersecurity can no longer rely on reactive defenses alone. Organizations must adopt proactive, intelligence-driven security operations to effectively protect their systems, data, and business continuity.

This intensive 1-week technical cybersecurity training course is designed to equip professionals with the practical knowledge and hands-on skills needed to monitor, detect, mitigate, and respond to cyber threats across modern IT environments. The program delivers comprehensive coverage of security monitoring and detection, vulnerability management, network security controls, incident response, secure architecture, and the evolving cyber threat landscape.

Through real-world case studies, practical exercises, and operational best practices, participants will learn how to design, implement, and manage effective cybersecurity defenses aligned with globally recognized standards and frameworks such as NIST CSF, NIST 800-53 and 800-61, ISO 27001, MITRE ATT&CK, and Zero Trust Architecture.

This course empowers attendees to enhance threat visibility, strengthen cyber resilience, and respond decisively to incidents while supporting secure and resilient business operations.

Course Objectives

By the end of this course, participants will be able to:

- Understand the modern cyber threat landscape and attacker tactics, techniques, and procedures TTPs
- Implement effective security monitoring and detection capabilities using logs, SIEM platforms, and threat intelligence
- Identify, assess, prioritize, and remediate vulnerabilities through structured vulnerability management processes
- Design and enforce network security controls to reduce attack surfaces and prevent lateral movement
- Develop and execute incident response plans aligned with industry best practices
- Apply secure architecture principles to build resilient on-premises, cloud, and hybrid environments
- Continuously improve organizational cybersecurity posture through monitoring, testing, and optimization



Course Outlines

Day 1: Cyber Threat Landscape & Security Monitoring Foundations

- Overview of the global cyber threat landscape and emerging attack trends
- Threat actor profiles: cybercriminals, nation-state actors, insiders, and hacktivists
- Understanding attack cycles and the MITRE ATT&CK framework
- Fundamentals of security monitoring and detection
- Log management, security telemetry, and visibility across endpoints, networks, and cloud environments
- Introduction to SIEM, SOAR, and threat intelligence sources

Day 2: Monitoring & Detection Operations

- Designing an effective security monitoring strategy
- Detection use cases: brute force attacks, malware activity, lateral movement, and data exfiltration
- Building correlation rules, alerting mechanisms, and tuning to reduce false positives
- Integrating and enriching threat intelligence
- Continuous monitoring metrics and key performance indicators KPIs
- Hands-on exercise: building and analyzing detection scenarios

Day 3: Vulnerability Management & Network Security Controls

- Vulnerability management lifecycle: discovery, assessment, prioritization, remediation, and validation
- Vulnerability scanning tools and techniques
- Risk-based prioritization using CVSS, exploitability, and asset criticality
- Network security fundamentals: firewalls, IDS/IPS, segmentation, and secure configurations
- Zero Trust and defense-in-depth design principles
- Reducing attack surfaces through strong network controls

Day 4: Incident Response & Cyber Crisis Management

- Incident response frameworks NIST 800-61, SANS
- Incident classification and severity assessment
- Roles and responsibilities within an incident response team
- Detection, containment, eradication, and recovery processes
- Digital forensics fundamentals and evidence handling
- Post-incident analysis, lessons learned, and reporting
- Tabletop exercise: responding to a simulated cyber incident



Day 5: Secure Architecture & Operational Resilience

- Secure architecture principles and secure-by-design approaches
- Security architecture for on-premises, cloud, and hybrid environments
- Identity and Access Management IAM fundamentals
- Secure application and infrastructure design concepts
- Integrating security into DevOps and cloud deployments
- Final workshop: designing a secure, monitored, and resilient cybersecurity architecture
- Knowledge assessment and roadmap for continuous improvement

Why Attend This Course: Wins & Losses!

- Understand Real-World Threats: Gain deep insight into today's cyber threat landscape and attacker behavior
- Improve Detection Capabilities: Build monitoring and detection strategies that significantly reduce threat dwell time
- Strengthen Vulnerability Management: Learn how to prioritize and remediate vulnerabilities based on real business risk
- Enhance Network Defense: Apply modern network security controls and Zero Trust principles
- Respond with Confidence: Develop practical incident response skills to manage cyber crises effectively
- Design Secure Systems: Apply secure architecture principles across IT and cloud environments
- Boost Cyber Resilience: Improve your organization's ability to prevent, detect, respond to, and recover from cyber attacks

Conclusion

This 1-week advanced cybersecurity training course is a strategic investment for cybersecurity professionals, SOC analysts, network engineers, security architects, and IT risk practitioners. It delivers the knowledge, tools, and practical experience required to defend modern digital environments against increasingly sophisticated cyber threats.

By the end of the program, participants will be fully equipped to monitor and detect threats proactively, manage vulnerabilities effectively, respond to incidents decisively, and design secure architectures that support long-term operational resilience.

Join this course to elevate your cybersecurity capabilities and become a key contributor to building secure, resilient, and future-ready organizations.

