BLACKBIRD FOR TRAINING

# Network Security Monitoring and SIEM Implementation

4 – 8 January 2027
Düsseldorf (Germany)



# Network Security Monitoring and SIEM Implementation

**Ref:** 3255294_201940 **Date:** 4 – 8 January 2027 **Location:** Düsseldorf (Germany) **Fees:** 5900 GBP

## Introduction

In today's digital era, cyber threats have become more sophisticated, persistent, and damaging. Protecting organizational infrastructure now requires not just reactive defense mechanisms but proactive visibility and intelligent monitoring.

The Network Security Monitoring and SIEM Implementation course equips participants with the knowledge and skills to design, deploy, and manage effective network monitoring systems combined with Security Information and Event Management SIEM solutions.

This course bridges theoretical understanding and practical application. Participants will learn how to analyze network data, detect anomalies, and build a centralized monitoring environment capable of identifying, classifying, and responding to potential security incidents in real time.

## Course Objectives

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

- Understand the principles and components of network security monitoring.
- Implement SIEM solutions for event correlation and incident detection.
- Collect and analyze logs from multiple network sources.
- Identify suspicious network activities and potential cyber threats.
- Build and operate a Security Operations Center SOC environment.
- Develop incident response procedures and threat mitigation strategies.
- Integrate monitoring solutions with existing security frameworks.
- Enhance overall resilience against evolving cyberattacks.

## Course Outlines

### Day 1: Fundamentals of Network Security Monitoring

- Overview of network monitoring and its importance in cybersecurity.
- Types of cyber threats targeting network infrastructures.
- Core components and tools of network monitoring systems.
- Data collection and traffic analysis methods.
- Understanding patterns of normal versus abnormal network behavior.
- Practical exercise: basic traffic capture and anomaly detection.



## Day 2: Introduction to SIEM Systems and Log Management

- Understanding the concept and architecture of SIEM systems.
- How to aggregate and normalize data from diverse network sources.
- Log collection, parsing, and correlation techniques.
- Identifying key indicators of compromise IoCs.
- Configuring alerts and automated incident detection rules.
- Lab: real-time monitoring using a sample SIEM dashboard.

## Day 3: Building an Effective Security Monitoring Environment

- Designing and implementing a centralized monitoring system.
- Mapping data flows and identifying critical monitoring points.
- Choosing and configuring appropriate monitoring tools.
- Developing visualization dashboards for threat visibility.
- Generating analytical reports for management and audit purposes.
- Workshop: designing a security monitoring architecture for an enterprise.

## Day 4: Incident Response and Advanced Threat Analysis

- Understanding the incident response lifecycle.
- Conducting detailed forensic analysis using SIEM data.
- Tracing attack sources and reconstructing event timelines.
- Applying behavioral analytics for user and system activity tracking.
- Developing and executing rapid response plans.
- Exercise: simulating a cyberattack and responding through SIEM tools.

## Day 5: Integration, Evaluation, and Continuous Improvement

- Integrating SIEM with other security technologies firewalls, IDS, endpoint tools.
- Developing performance metrics to measure monitoring effectiveness.
- Reviewing system logs and identifying configuration gaps.
- Automating incident response and reporting workflows.
- Best practices for maintaining SIEM efficiency and scalability.
- Final project: building a complete security monitoring and response plan.



## Why Attend this Course: Wins & Losses!

- Gain a comprehensive understanding of modern network monitoring principles.
- Develop the ability to implement and manage SIEM platforms effectively.
- Learn to detect, analyze, and respond to cyber threats in real time.
- Improve organizational readiness for complex and evolving attacks.
- Strengthen data protection, compliance, and reporting capabilities.
- Build a robust foundation for establishing or enhancing a SOC.
- Integrate monitoring tools seamlessly within enterprise infrastructures.
- Acquire actionable insights applicable to real-world cybersecurity challenges.

## Conclusion

Network Security Monitoring and SIEM Implementation is a critical area of expertise for any organization aiming to maintain strong cybersecurity posture.

It goes beyond basic defense — focusing on proactive detection, rapid response, and intelligent analysis of network activity.

**Through this course, participants will gain practical experience in building and operating advanced monitoring systems that enhance threat visibility, reduce incident response time, and ensure the continuous protection of digital assets.**

