BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Security Information and Event Management (SIEM) Solution

Course Introduction

This course is designed to develop SIEM Deployment Experts and Administrators by training them on the implementation, configuration, and administration of a market-leading SIEM product. Through hands-on lab exercises, participants will gain the essential skills needed for all aspects of SIEM deployment, ensuring comprehensive knowledge and practical experience. The course also covers critical operational functions, including event search capabilities, creation of monitoring rules, and customization of dashboards. By the end of the program, students will be proficient in both the technical and operational aspects of SIEM management, ready to effectively deploy and administer SIEM solutions in real-world environments.

Training Course Methodology

This course is designed to be interactive and participatory, and includes various learning tools to enable the participants to function effectively and efficiently. The course will use sessions, exercises, and case applications, and presentation about proven-by-practice methods, new insights and ideas about emotional intelligence and its effects in a corporate world.

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

- Understand the basics of networking, including TCP/IP protocols, IP addressing, subnetting, and firewall zoning concepts.
- Identify prominent network attacks and their impact, and learn how various network security tools like firewalls, IDS/IPS, and DLP operate at a high level.
- Gain foundational knowledge in logging, log management, and network security management using SIEM solutions.
- Develop the ability to gather information for SIEM solutions, plan and implement both standalone and distributed SIEM deployments, and integrate SIEM with event sources for effective event monitoring.
- Master SIEM administration tasks, including user management, customization of monitoring dashboards, and creation and customization of monitoring rules to enhance network security operations.

Course Outline

- **Day 01**

  Module 1:

  - Basics of Networking, Understanding TCP/IP protocol, Assigning IP Address & Subnets, Firewall Zoning concept
  - Prominent Attack and their impact
  - Network Security Tools and how they operate (Firewall, IDS/IPS, DLP etc. at very high level)
- **Day 02**

  Module 2:

  - Basics of logging & log management
  - Network Security Management using SIEM

    - What is SIEM and its need Understand the SIEM components (connector/ collector, logger/indexer, console etc.)
- **Day 03**

  Module 3:

    - SIEM Solution Information gathering forSIEM solution Developing SIEM solution and plan implementation (standalone, distributed deployments etc
    - Integration of SIEM with event sources & Configure SIEM for event monitoring
- **Day 04**

  Module 4:

    - SIEM Administration
    - User administration
    - Customization of monitoring dashboard
- **Day 05**

  Module 5:

    - Monitoring rule customization
    - Creation of custom monitoring rule

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 16, 2025	June 20, 2025	5 days	4950.00 $	Spain - Madrid
Sept. 8, 2025	Sept. 12, 2025	5 days	4250.00 $	UAE - Dubai
Dec. 29, 2025	Jan. 2, 2026	5 days	4250.00 $	UAE - Abu Dhabi