€TRAINING

Continuous Monitoring And Security Operations

2 - 6 December 2024
Kuala Lumpur (Malaysia)

Continuous Monitoring And Security Operations

REF: B1760 DATE: 2 - 6 December 2024 Venue: Kuala Lumpur (Malaysia) - Fee: 5850 Euro

Introduction:

This training program provides participants with essential knowledge and skills for continuous monitoring and security operations. It empowers them to implement effective monitoring strategies and security practices to safeguard IT environments and ensure ongoing protection against threats.

Program Objectives:

At the end of this program, participants will be able to:

- Understand the principles and practices of continuous monitoring and security operations.
- Implement and manage security monitoring tools and techniques.
- Analyze and respond to security incidents and threats.
- Develop and maintain security operations procedures.
- Evaluate and enhance security posture through continuous improvement.

Targeted Audience:

- Security Analysts.
- IT Security Managers.
- Network Security Engineers.
- Incident Response Teams.
- IT Operations Professionals.

Program Outline:

Unit 1:

Introduction to Continuous Monitoring:

- Overview of continuous monitoring concepts and importance.
- Key components and tools for continuous monitoring.
- Setting up monitoring systems and infrastructure.

- Defining monitoring objectives and scope.
- Integrating monitoring with other security operations.

Unit 2:

Security Operations Fundamentals:

- Core principles of security operations and incident management.
- Overview of security operations center SOC functions.
- Implementing and managing security operations processes.
- Security event and incident lifecycle management.
- Key performance indicators KPIs for security operations.

Unit 3:

Security Monitoring Tools and Techniques:

- Overview of common security monitoring tools SIEM, IDS/IPS.
- Configuring and tuning security monitoring systems.
- Collecting and analyzing security data and logs.
- Correlating and prioritizing security events.
- Using threat intelligence for proactive monitoring.

Unit 4:

Incident Response and Management:

- Incident detection and response strategies.
- Managing and escalating security incidents.
- Conducting forensic analysis and investigations.
- Developing and implementing incident response plans.
- Post-incident review and lessons learned.

Unit 5:

Enhancing Security Operations:

- Continuous improvement strategies for security operations.
- Evaluating and updating security policies and procedures.
- Implementing automation and orchestration in security operations.
- Measuring and reporting on security operations effectiveness.
- Future trends and technologies in continuous monitoring and security operations.