MERCURY

# Vulnerability Assessment & Security Issue Analysis

31 May – 4 June 2027
Madrid (Spain)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

# Vulnerability Assessment & Security Issue Analysis

**Ref:** 121384_1030385 **Date:** 31 May – 4 June 2027 **Location:** Madrid (Spain) **Fees:** 6200 Euro

## Introduction

The Vulnerability Assessment & Security Issue Analysis course provides a structured framework for evaluating system weaknesses and identifying potential cyber risks within modern IT environments. This course strengthens participants' ability to interpret vulnerability scan results and configuration data with precision and confidence. It emphasizes systematic security assessment practices aligned with current cybersecurity standards and enterprise risk management needs. Participants will explore practical methods for detecting misconfigurations, prioritizing risks, and supporting secure system hardening. The course also focuses on improving analytical thinking when reviewing security findings across networks, applications, and operating systems. Professionals will support proactive vulnerability management to strengthen the organization's security posture.

## Targeted Groups

This Vulnerability Assessment & Security Issue Analysis training targets professionals seeking knowledge and skills:

- Cybersecurity analysts seeking structured vulnerability assessment skills.
- IT security specialists are responsible for system hardening.
- Network administrators manage secure infrastructure environments.
- Risk management professionals supporting cyber risk programs.
- The SOC team members are reviewing security scan outputs.
- Compliance officers monitor security configuration baselines.
- Information security officers are improving threat visibility.
- Technical auditors evaluate system security controls.

## Course Objectives

Participants will achieve the following objectives by completing the Vulnerability Assessment & Security Issue Analysis course:

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Understand core principles of vulnerability assessment and risk exposure.
- Identify common system security weaknesses and misconfigurations.
- Interpret vulnerability scan reports with analytical accuracy.
- Correlate configuration data with potential cyber threats.
- Prioritize remediation based on risk severity and business impact.
- Evaluate network, host, and application vulnerabilities systematically.
- Apply structured approaches to security issue analysis.
- Support continuous vulnerability management programs.
- Improve reporting clarity for technical and non-technical stakeholders.
- Strengthen proactive cyber risk reduction strategies.
- Align vulnerability assessment activities with security best practices.
- Enhance decision-making using evidence-based security data.

## Targeted Competencies

Participants will gain the following competencies during the Vulnerability Assessment & Security Issue Analysis program:

- Analytical review of vulnerability assessment results.
- Systematic identification of security configuration gaps.
- Risk-based vulnerability prioritization techniques.
- Technical interpretation of security scan data.
- Detection of network and host misconfigurations.
- Structured cyber risk evaluation skills.
- Security posture assessment across enterprise systems.
- Effective documentation of security findings.
- Coordination between security and IT operations teams.
- Continuous monitoring mindset for vulnerability management.

## Studying Scenarios

In this Vulnerability Assessment & Security Issue Analysis training, participants develop skills through the following scenarios:

- Analyzing vulnerability scan results in enterprise networks.
- Reviewing insecure system configurations in real cases.
- Prioritizing critical vulnerabilities in production environments.
- Investigating misconfigured servers and exposed services.
- Evaluating patch management gaps and risks.
- Correlating threat intelligence with vulnerability data.
- Assessing compliance deviations in security baselines.
- Reporting security findings to management stakeholders.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

# Course Content

## Unit 1: Foundations of Vulnerability Assessment

- Overview of the modern vulnerability management lifecycle.
- Definition of vulnerabilities, exposures, and attack surfaces.
- Role of vulnerability assessment in cybersecurity strategy.
- Types of security weaknesses in IT environments.
- Understanding threat actors and exploitation methods.
- Relationship between risk management and vulnerability scanning.
- Key terminology in security assessment processes.
- Common challenges in identifying system vulnerabilities.

## Unit 2: Vulnerability Scanning and Data Analysis

- Principles of automated vulnerability scanning tools.
- Interpreting vulnerability scan reports effectively.
- Understanding false positives and validation techniques.
- Mapping vulnerabilities to CVSS risk scoring models.
- Analyzing configuration data for hidden weaknesses.
- Correlating scan results with asset criticality.
- Reviewing network, host, and application scan outputs.
- Establishing scan schedules and coverage strategies.

## Unit 3: Identifying System Security Issues

- Detecting insecure system configurations.
- Recognizing common operating system vulnerabilities.
- Identifying network exposure and open port risks.
- Evaluating application security weaknesses.
- Reviewing access control misconfigurations.
- Assessing patch and update compliance gaps.
- Investigating privilege escalation risks.
- Linking vulnerabilities to potential attack paths.

## Unit 4: Risk Prioritization and Remediation Planning

- Risk-based vulnerability prioritization frameworks.
- Evaluating the business impact of security weaknesses.
- Developing remediation and mitigation strategies.
- Coordinating patch management processes.
- Tracking remediation progress and validation.
- Communicating risk levels to stakeholders.
- Integrating vulnerability data into risk registers.
- Supporting continuous security improvement programs.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

## Unit 5: Continuous Vulnerability Management & Reporting

- Building a sustainable vulnerability management program.
- Establishing security configuration baselines.
- Continuous monitoring of system security posture.
- Metrics and KPIs for vulnerability management.
- Preparing professional vulnerability assessment reports.
- Supporting compliance and audit requirements.
- Aligning vulnerability management with security operations.
- Enhancing organizational cyber resilience.

## Final Insights & Key Takeaways

Effective vulnerability assessment requires continuous analysis of configuration data and security findings. Organizations that adopt structured vulnerability management significantly reduce cyber risk exposure and strengthen overall system security.