MERCURY

Network & Information Security Systems Evaluation

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

MERCURY

Network & Information Security Systems Evaluation

Introduction

The Network & Information Security Systems Evaluation course provides a foundation for professionals responsible for protecting digital infrastructures. It focuses on evaluating and strengthening cybersecurity policies, procedures, and technical controls across modern enterprise environments. Participants will explore practical approaches to assessing network security posture, validating system integrity, and ensuring continuous protection of information assets. The course emphasizes structured methods for designing secure networks and deploying resilient servers and endpoint protection systems. It also develops the ability to monitor, coordinate, and maintain digital security frameworks aligned with current cyber risk landscapes. Learners will confidently support secure network operations and informed cybersecurity decision-making.

Targeted Groups

This Network & Information Security Systems Evaluation training targets professionals seeking knowledge and skills:

- IT security specialists seeking structured security evaluation skills.
- Network engineers responsible for secure infrastructure design.
- Systems administrators managing enterprise servers.
- Cybersecurity analysts are monitoring digital threats.
- IT auditors reviewing security policies and controls.
- Technical support professionals transitioning to cybersecurity roles.
- Risk and compliance officers are involved in information protection.
- Professionals preparing for advanced network security responsibilities.

Course Objectives

Participants will achieve the following objectives by completing the Network & Information Security Systems Evaluation course:

- Understand core principles of network and information security.
- Evaluate digital security policies and procedural effectiveness.
- Analyze common vulnerabilities in enterprise network environments.
- Test security controls using structured assessment approaches.
- Recommend improvements for cybersecurity frameworks and governance.
- Design secure network architectures for modern organizations.
- Verify system and application security configurations.
- Deploy servers with hardened security baselines.
- Implement endpoint protection and monitoring mechanisms.
- Coordinate security operations across IT environments.
- Monitor network activity using security analytics techniques.
- Maintain a continuous security posture through proactive controls.
- Support compliance with international cybersecurity standards.
- Strengthen incident readiness and response coordination.

Targeted Competencies

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

Participants will gain the following competencies during the Network & Information Security Systems Evaluation program:

- Network security assessment and risk identification skills.
- Digital security policy review and improvement capability.
- Secure network design and segmentation expertise.
- System and application verification proficiency.
- Server hardening and secure deployment practices.
- Endpoint security configuration and monitoring ability.
- Cybersecurity testing and validation techniques.
- Security operations coordination and reporting skills.
- Continuous monitoring using modern security tools.
- Practical understanding of enterprise cyber defense strategies.

Studying Scenarios

In this Network & Information Security Systems Evaluation training, participants develop skills through the following scenarios:

- Assessing the security posture of a corporate network environment.
- Reviewing and improving an organization's information security policies.
- Designing a secure network architecture for a growing enterprise.
- Validating server configurations against security baselines.
- Investigating endpoint security alerts and response actions.
- Coordinating monitoring activities within a security operations context.
- Recommending remediation actions after vulnerability testing.
- Maintaining continuous protection across hybrid IT environments.

Course Content

Unit 1: Foundations of Network & Information Security

- Overview of network and information security principles and concepts.
- Evolution of cybersecurity threats in modern digital ecosystems.
- Understanding the enterprise attack surface and threat landscape.
- Core components of information security frameworks.
- Importance of confidentiality, integrity, and availability in network protection.
- Introduction to cyber risk management in enterprise environments.
- Security governance and organizational responsibility models.
- Alignment of cybersecurity strategy with business continuity goals.

Unit 2: Evaluating Digital Security Policies and Procedures

- Structure of effective information security policies and standards.
- Methods for reviewing and auditing cybersecurity procedures.
- Mapping policies to regulatory and compliance requirements.
- Identifying gaps in existing digital security frameworks.
- Risk-based approach to security policy improvement.
- Coordinating policy implementation across departments.
- Monitoring policy effectiveness using security metrics.
- Maintaining documentation and version control for security procedures.

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

Unit 3: Network Security Design and Architecture

- Principles of secure network architecture design.
- Network segmentation and defense-in-depth strategies.
- Secure routing and switching configurations.
- Designing protected access for on-premises and cloud networks.
- Implementing firewalls and network security controls.
- Secure VPN deployment for remote connectivity.
- Network access control and identity-aware networking.
- High availability and resilience in secure network environments.

Unit 4: Systems, Servers, and Endpoint Security Deployment

- Secure server deployment and system hardening techniques.
- Verifying operating system and application security settings.
- Endpoint protection platforms and configuration practices.
- Patch management and vulnerability remediation workflows.
- Monitoring endpoints using advanced threat detection tools.
- Securing enterprise applications and service configurations.
- Logging, alerting, and security event correlation basics.
- Maintaining secure baselines across distributed IT assets.

Unit 5: Security Testing, Monitoring, and Continuous Improvement

- Structured approaches to cybersecurity testing and validation.
- Vulnerability assessment methodologies and tools overview.
- Continuous network monitoring and traffic analysis techniques.
- Security operations coordination and incident escalation.
- Measuring security performance using key risk indicators.
- Maintaining ongoing cyber resilience and threat readiness.
- Recommending improvements based on security findings.
- Building a culture of continuous security enhancement.

Final Insights & Key Takeaways

This program equips professionals with practical expertise to evaluate, design, and maintain resilient network and information security environments. Participants leave prepared to strengthen enterprise cyber defenses through structured assessment, secure deployment, and continuous monitoring.