Cybersecurity Foundations Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Cybersecurity Foundations is designed for professionals who want to build a broad understanding of modern cybersecurity threats, defensive controls, and organisational responsibilities.

The programme approaches secure system design from a complete security perspective rather than concentrating on a single technical discipline. Participants explore how different cybersecurity roles, controls, technologies, and processes work together to provide a cohesive security solution.

Throughout the course, learners examine current threat trends, network security, systems hardening, malware, social engineering, software vulnerabilities, identity management, data protection, PKI, monitoring, physical security, incident response, and legal considerations.

Instructor-led content is supported by labs and breakout discussion groups. Participants review real attack techniques and sample exploits while exploring the controls that can be used to reduce associated risks.

Within a controlled laboratory environment, learners also examine live malware examples, including botnets, worms, and Trojans. This provides practical insight into how malicious software behaves and how defensive technologies can be applied.

Prerequisites

Participants should have foundational knowledge of:

- TCP/IP networking
- Networking fundamentals
- IP addressing
- Basic network communication
- Common network devices and services

Knowledge equivalent to TCP/IP Networking or a similar networking fundamentals course will help participants gain more value from the programme.

Who Should Attend

The course is particularly suitable for:

- Network professionals who want to expand their cybersecurity knowledge
- Technical professionals considering cybersecurity as a career path
- Executives and managers who need to communicate more effectively with security teams
- Leaders responsible for implementing security at an organisational level
- Individuals who want a stronger understanding of cybersecurity fundamentals
- Professionals who need to understand threats, mitigating controls, and organisational security responsibilities

Cybersecurity Foundations Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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

- Improve their overall security awareness
- Interpret network mapping and footprinting tool output
- Reduce the attack surface of systems
- Apply networking knowledge to security controls
- Explain different data protection principles
- Understand the role of PKI and digital certificates
- Explain how trusted relationships are established between network devices
- Apply login security and identity management approaches
- Reduce the attack surface of network devices
- Evaluate current malware threats and anti-malware controls
- Identify social engineering techniques and common attack methods
- Understand software vulnerabilities and methods for reducing exploitation risk
- Explain monitoring and logging requirements
- Recognise privacy issues associated with monitoring activities
- Identify physical security controls
- Explain the relationship between physical security and IT security
- Describe incident response capabilities
- Identify important legal and regulatory cybersecurity considerations
- Understand basic investigative techniques
- Research and evaluate current cybersecurity trends

Training Outline

Module 1: Cybersecurity Awareness

This module introduces the core principles that form the foundation of cybersecurity.

Topics include:

- What is security?
- Confidentiality
- Integrity
- Availability
- Security baselining
- Human-related security concerns
- Types of threats
- Security controls
- What is hacking?
- Risk management
- Data in motion
- Data at rest
- Module review

Module 2: Network Discovery

This module examines the techniques used to identify and understand network environments.

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

Topics include:

- Networking review
- Discovery
- Footprinting
- Scanning
- Common Vulnerabilities and Exposures
- Security policies
- Vulnerabilities
- Module review

Participants consider how information exposed during network discovery can contribute to an attack surface.

Module 3: Systems Hardening

This section focuses on reducing system exposure and strengthening security configurations.

Topics include:

- What is hardening?
- Types of systems that can be hardened
- Security baselines
- Hardening methods
- Hardening systems by role
- Mobile devices
- Network hardening
- Analysis tools
- Authentication
- Authorization
- Accounting
- Physical security
- Module review

Module 4: Security Architecture

This module explores the main architectural elements used to build secure environments.

Topics include:

- Security architecture
- Network devices
- Network zones
- Network segmentation
- Network Address Translation
- Network Access Control
- Module review

Module 5: Data Security

Topics include:

- Cryptography

- Principles of permissions
- Access control
- Steganography
- Module review

Module 6: Public Key Infrastructure

This module examines how PKI is used to create and manage digital trust.

Topics include:

- Public Key Infrastructure
- Certification Authorities
- Enabling trust
- Certificates
- CA management
- Module review

Module 7: Identity Management

This module focuses on protecting and managing user and service identities.

Topics include:

- What is identity management?
- Personally Identifiable Information
- Authentication factors
- Directory services
- Kerberos
- Windows NT LAN Manager
- Password policies
- Password cracking
- Password assessment tools
- Password managers
- Group accounts
- Service accounts
- Federated identities
- Identity as a Service
- Module review

Module 8: Network Hardening

This module focuses on reducing risk across network devices and administrative access paths.

Topics include:

- Limiting remote administration access
- AAA for administrative access
- Simple Network Management Protocol
- Network segmentation
- Limiting physical access
- Establishing secure access
- Network devices

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Fundamental device protection
- Traffic filtering best practices
- Module review

Module 9: Malware

This section examines common malware techniques and defensive measures.

Topics include:

- What is malware?
- Infection methods
- Types of malware
- Botnets
- Worms
- Trojans
- Backdoors
- Countermeasures
- Protection tools
- Module review

Controlled laboratory activities are used to examine malware behaviour safely.

Module 10: Social Engineering

This module explores attacks that target people rather than technology alone.

Topics include:

- What is social engineering?
- Social engineering targets
- Social engineering attacks
- Statistical data
- Information harvesting
- Preventing social engineering
- Cyber awareness policies
- Procedures
- Social media
- Module review

Module 11: Software Security

This section examines security risks within software development and applications.

Topics include:

- Software engineering
- Security guidelines
- Software vulnerabilities
- Exploitation risk
- Security solutions
- Module review

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

Module 12: Environment Monitoring

This module focuses on security monitoring and logging.

Topics include:

- Monitoring
- Monitoring versus logging
- Monitoring benefits
- Logging benefits
- Logging
- Metrics
- Privacy considerations
- Module review

Module 13: Physical Security

This module examines the physical controls that support information security.

Topics include:

- What is physical security?
- Defense in depth
- Types of physical security controls
- Device security
- Human security
- Security policies
- Equipment tracking
- Module review

Module 14: Incident Response

This section explores how organisations prepare for and respond to security incidents.

Topics include:

- Disaster types
- Incident investigation
- Investigation techniques
- Business Continuity Planning
- Disaster Recovery Plans
- Forensic Incident Response
- Module review

Participants consider the main stages involved in identifying, investigating, containing, and recovering from incidents.

Module 15: Legal Considerations

This module introduces legal and regulatory issues associated with cybersecurity.

Topics include:

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Regulatory compliance
- Cybercrime
- Legal responsibilities
- Investigative considerations
- Module review

Module 16: Trends in Cybersecurity

This module examines the changing cybersecurity environment.

Topics include:

- Cybersecurity design constraints
- Cyber driving forces
- Levels of connectivity
- Dependence on connectivity
- Identity management trends
- Cybersecurity standards
- Cybersecurity training
- Emerging security considerations

Module 17: Course Look Around

The final module helps participants reflect on their learning and identify future development opportunities.

Topics include:

- Looking back
- Looking forward
- Planning your cybersecurity journey
- Identifying next steps for development