skillsoft global knowledge™

CYBERSECURITY FOUNDATIONS

Course Code: 9701

Investigate cybersecurity threats and master techniques needed to protect your network.

In this cybersecurity course, you will gain a global perspective of the challenges of designing a secure system, touching on all the cyber roles needed to provide a cohesive security solution. Through lecture, labs, and breakout discussion groups, you will learn about current threat trends across the Internet and their impact on organizational security. You will review standard cybersecurity terminology and compliance requirements, examine sample exploits, and gain hands-on experience mitigating controls. In a contained lab environment, you will work with live viruses, including botnets, worms, and Trojans.

What You'll Learn

- Current cyber threats and cybersecurity site references
- Government-mandated directives and compliance requirements
- Cyber roles required to successfully design secure systems
- The attack cycle perpetrated by malicious hackers
- Enterprise policy requirements
- Best strategies for securing the enterprise with layered defenses
- How security zones and detailed logging augment information assurance
- Forensic challenges and incident response planning
- Risk management process
- Goals achievable with auditing, scanning, and testing systems
- Industry recommendations for maintaining secure access control
- Standards-based cryptographic solutions for securing communications

Who Needs to Attend

- Network professionals looking to advance their knowledge and explore cybersecurity as a career path.
- Executives and managers looking to increase their ability to communicate with security professionals and implement a robust security solution at the organizational level.
- Individuals wants to improve their understanding of cybersecurity fundamentals, including threats, mitigating controls, and organizational responsibilities.

Prerequisites

TCP/IP Networking or equivalent knowledge

CYBERSECURITY FOUNDATIONS

Course Code: 9701

CLASSROOM LIVE	$4,425 CAD	5 Day

Classroom Live Outline

1. Cybersecurity Awareness

- What is security?
- Confidentiality, integrity, and availability
- Security baselining
- Security concerns: Humans
- Types of threats
- Security controls
- What is hacking?
- Risk management
- Data in motion vs. data at rest
- Module review

2. Network Discovery

- Networking review
- Discovery, footprinting, and scanning
- Common vulnerabilities and exposures
- Security policies
- Vulnerabilities
- Module review

3. Systems Hardening

- What is hardening?
- Types of systems that can be hardened
- Security baselines
- How to harden systems
- Hardening systems by role
- Mobile devices
- Hardening on the network
- Analysis tools

- Authentication, authorization, and accounting
- Physical security
- Module review

4. Security Architecture

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

5. Data Security

- Cryptography
- Principles of permissions
- Steganography
- Module review

6. Public Key Infrastructure

- Public key infrastructure
- Certification authorities
- Enabling trust
- Certificates
- CA management
- Module review

7. Identity Management

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

8. Network Hardening

- Limiting remote admin access
- AAA: Administrative access
- Simple Network Management Protocol

- Network segmentation
- Limiting physical access
- Establishing secure access
- Network devices
- Fundamental device protection summary
- Traffic filtering best practices
- Module review

9. Malware

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

10. Social Engineering

- What is social engineering?
- Social engineering targets
- Social engineering attacks
- Statistical data
- Information harvesting
- Preventing social engineering
- Cyber awareness: Policies and procedures
- Social media
- Module review

11. Software Security

- Software engineering
- Security guidelines
- Software vulnerabilities
- Module review

12. Environment Monitoring

- Monitoring
- Monitoring vs. logging
- Monitoring/logging benefits
- Logging
- Metrics
- Module review

13. Physical Security

- What is physical security?
- Defense in depth
- Types of physical security controls
- Device security
- Human security

- Security policies
- Equipment tracking
- Module review

14. Incident Response

- Disaster types
- Incident investigation tips
- Business continuity planning
- Disaster recovery plan
- Forensic incident response
- Module review

15. Legal Considerations

- Regulatory compliance
- Cybercrime
- Module review

16. Trends in Cybersecurity

- Cybersecurity design constraints
- Cyber driving forces
- How connected are you?
- How reliant on connectivity are you?
- Identity management
- Cybersecurity standards
- Cybersecurity training

17. Course Look Around

- Looking back
- Looking forward
- Planning your journey

skillsoft global knowledge™

CYBERSECURITY FOUNDATIONS

Course Code: 9701

VIRTUAL CLASSROOM LIVE	$4,425 CAD	5 Day

Virtual Classroom Live Outline

1. Cybersecurity Awareness

- What is security?
- Confidentiality, integrity, and availability
- Security baselining
- Security concerns: Humans
- Types of threats
- Security controls
- What is hacking?
- Risk management
- Data in motion vs. data at rest
- Module review

2. Network Discovery

- Networking review
- Discovery, footprinting, and scanning
- Common vulnerabilities and exposures
- Security policies
- Vulnerabilities
- Module review

3. Systems Hardening

- What is hardening?
- Types of systems that can be hardened
- Security baselines
- How to harden systems
- Hardening systems by role
- Mobile devices
- Hardening on the network
- Analysis tools

- Authentication, authorization, and accounting
- Physical security
- Module review

4. Security Architecture

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

5. Data Security

- Cryptography
- Principles of permissions
- Steganography
- Module review

6. Public Key Infrastructure

- Public key infrastructure
- Certification authorities
- Enabling trust
- Certificates
- CA management
- Module review

7. Identity Management

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

8. Network Hardening

- Limiting remote admin access
- AAA: Administrative access
- Simple Network Management Protocol

- Network segmentation
- Limiting physical access
- Establishing secure access
- Network devices
- Fundamental device protection summary
- Traffic filtering best practices
- Module review

9. Malware

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

10. Social Engineering

- What is social engineering?
- Social engineering targets
- Social engineering attacks
- Statistical data
- Information harvesting
- Preventing social engineering
- Cyber awareness: Policies and procedures
- Social media
- Module review

11. Software Security

- Software engineering
- Security guidelines
- Software vulnerabilities
- Module review

12. Environment Monitoring

- Monitoring
- Monitoring vs. logging
- Monitoring/logging benefits
- Logging
- Metrics
- Module review

13. Physical Security

- What is physical security?
- Defense in depth
- Types of physical security controls
- Device security
- Human security

- Security policies
- Equipment tracking
- Module review

14. Incident Response

- Disaster types
- Incident investigation tips
- Business continuity planning
- Disaster recovery plan
- Forensic incident response
- Module review

15. Legal Considerations

- Regulatory compliance
- Cybercrime
- Module review

16. Trends in Cybersecurity

- Cybersecurity design constraints
- Cyber driving forces
- How connected are you?
- How reliant on connectivity are you?
- Identity management
- Cybersecurity standards
- Cybersecurity training

17. Course Look Around

- Looking back
- Looking forward
- Planning your journey

Jul 7 - 11, 2025 | 8:30 AM - 4:30 PM EDT

Jul 21 - 25, 2025 | 8:30 AM - 4:30 PM EDT

Sep 29 - Oct 3, 2025 | 8:30 AM - 4:30 PM EDT

Nov 10 - 14, 2025 | 8:30 AM - 4:30 PM EST

Jan 5 - 9, 2026 | 8:30 AM - 4:30 PM EST

CYBERSECURITY FOUNDATIONS

Course Code: 9701

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 7:16:49 AM