Cybersecurity Foundations

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