CYBER SECURITY PRINCIPLES, DOMAINS, AND MANAGEMENT

Version 2.1

1 Course Overview

During this course, attendees will gain a solid understanding of Cyber Security principles, domains, and management. Attendees will learn about user and device security, network and cloud security, application and data security, and the important area of detection and response. They will also learn about cyber threats and vulnerabilities, cryptography basics, security testing, security operations, data protection, securing critical infrastructure, and the impact of artificial intelligence on cyber security.

This course can be delivered in various levels of detail and therefore is applicable to a broad audience. We can deliver a 1-day, a 2-day and even a 3-day version depending on the desired level of detail and the target audience.

Please note that this course is delivered by senior consulting engineers who have many years of experience in networking, IT and Cyber Security.

2 Who Should Attend

This course is intended for professionals like:

- Account Managers
- Pre/Post Sales Engineers
- Solution Designers
- Staff of End User IT / Security Departments

3 Prerequisites

Attendees would benefit from having a good general understanding of networking and IT systems.

4 Why Attend a Blue River Experts Course

Our courses are not delivered by instructors but by consulting system engineers who have vast experience regarding real life design, deployment, and troubleshooting of actual customer installations. Besides delivering courses, our engineers usually design and deploy large enterprise solutions or perform real world POVs (proof of value) and POCs (proof of concept) for large customers. We are often requested and contracted by product vendors to help customers make buying decisions based on their particular use case. This allows us to discuss real world use cases, designs, and operational situations with our students.

If you would like to get educated by experts who will explain to you the whole life cycle from day 0 to day 2 as they have comprehensive knowledge from having written numerous business requirements documents, customer requirements documents, high level design and detailed design documents and having deployed and troubleshooted many customer installations then you should choose to attend one of our courses.

5 Course Objectives

After completing this course, attendees will be able to understand and explain:

- Security principles, concepts, and domains
- Threats and vulnerabilities
- Security testing
- Identity and access management, data protection, and privacy
- Cyber Security operations, incident handling, and response
- Critical infrastructure and the impact of artificial intelligence on Cyber Security

In short, have a comprehensive and well-informed conversation about Cyber Risk, Cyber Security Architectures and Cyber Security Operations.

6 Course Details

6.1 Principles of Information Security

6.1.1 Introduction to Information Security

6.1.2 Key Concepts

6.1.3 Risk Management in Information Security

6.1.4 Security Policies, Standard and Frameworks

6.1.5 Cyber Security Governance and Compliance

6.2 Cyber Threats and Vulnerabilities

6.2.1 Types of Cyber Threats

6.2.2 Common Vulnerabilities

6.2.3 Threat Actors and Motivations

6.2.4 The Impact of Cyber Security Incidents

6.2.5 Identifying and Assessing Vulnerabilities

6.2.6 Mitigating Threats and Vulnerabilities

6.2.7 Emerging Trends

6.3 Cryptography Basics

6.3.1 Introduction, Basic Terms

6.3.2 Principles of Cryptography

6.3.3 Types of Cryptographic Algorithms

6.3.4 Cryptography Protocols

6.3.5 Cryptography Standards

6.3.6 Practical Applications of Cryptography

6.3.7 Cryptographic Attacks

6.3.8 Challenges and Limitations

6.3.9 Emerging Techniques

6.4 Security Domains

6.4.1 User and Device Security

- Types of Endpoints, Endpoint Vulnerabilities
- Endpoint Protection Technologies
- Endpoint Security Management
- Mobile Device Security
- Data Protection and Encryption
- Securing IoT Devices
- Advanced Measures

6.4.2 Network Security

- Threats to Network Security
- Perimeter Based Security vs Zero Trust
- Network Security Technologies
- Next Generation Firewalls
- Securing Wireless Networks
- Zero Trust Architecture and Deployment
- Secure Access Service Edge (SASE)
- Network Monitoring and Management

6.4.3 Cloud Security

- The Shared Responsibility Model
- Cloud Security Architectures
- Zero Trust and Identity Access Management
- Virtual Firewalls, Web Application Firewalls
- Secure Access Service Edge (SASE)
- Security Operations in Cloud Environments

6.4.4 Application and Web Security

- Introduction to Application Security
- Fundamental Principles
- Understanding Web Application Architectures
- Common Vulnerabilities
- Securing Web Applications
- Mobile Application Security
- Application Security Testing
- Secure Development Life Cycle (SDLC)
- Application Security Frameworks

6.5 Security (PEN) Testing

6.5.1 Penetration Testing Programs

6.5.2 Penetration Testing Methods

6.5.3 Penetration Testing Steps

6.5.4 Vulnerability Assessment

6.5.5 Types of Penetration Testing

- Network Penetration Testing
- Web Application Penetration Testing
- Wireless Security Audits
- IOT / ICS Penetration Testing
- Cloud Penetration Testing
- Mobile Application Penetration Testing

6.5.6 Social Engineering Audits

6.5.7 Active Directory Security Audits

6.5.8 Bug Bounty Programs

6.6 Cyber Security Management and Practices

6.6.1 Identity and Access Management

- Fundamentals of Identity Management
- Least Privileged Access
- Access Management
- Implementing IAM Solutions
- IAM Policies and Governance

6.6.2 Active Directory Security

- Introduction to Active Directory
- Core Components of Active Directory
- Securing Active Directory
- Advanced Active Directory Security Measures
- Future Directions in Active Directory Security

6.6.3 Data Protection and Privacy

- Introduction to Data Protection and Privacy
- Difference Between Data Protection and Data Privacy
- Principles of Data Protection and Privacy
- Legal and Regulatory Frameworks
- Technological Measures for Data Protection
- Managing Data Privacy

6.7 Cyber Security Operations

6.7.1 Attack Surface Management

6.7.2 The Security Operations Center

- Roles and Responsibilities
- SOC Infrastructure and Tools
- SOC Models
- SOC as a Service
- Key Performance Indicators (KPIs) and Metrics

6.7.3 Threat Intelligence

- Understanding Threat Intelligence
- Threat Intelligence Platforms

6.7.4 Incident Handling and Response

- The MITRE ATT&CK Framework
- Incident Response Lifecycle
- Developing an Incident Response Plan
- Incident Handling and Analysis
- Threat Hunting

6.7.5 Security Monitoring and Event Management

- Security Information and Event Management (SIEM)
- Log Management and Analysis

6.7.6 Network Security Operations

- Network Monitoring and Defense
- Endpoint Security Operations

6.7.7 Cloud Security Operations

- Securing Cloud Environments
- Cloud Security Posture Management (CSPM)

6.7.8 Cybersecurity Automation and Orchestration

- Automated Threat Detection and Response
- Security Orchestration, Automation, and Response (SOAR)

6.8 Trends and Future Challenges

6.8.1 Securing Critical Infrastructure

- Introduction to Critical Infrastructure
- Identifying and Assessing Vulnerabilities
- Legal and Regulatory Framework
- Cyber Security Strategies for Critical Infrastructure
- Security Testing in ICS Environments

6.8.2 Artificial Intelligence and Cyber Security

- Introduction to Artificial Intelligence
- Intersection of AI and Cyber Security
- AI in Cyber Defense
- AI in Cyber Attacks
- Conclusions and Recommendations