Basic Security Workshop

4 Days / Instructor-Led / Format: On-Site or Virtual

Contact Us for Pricing

About this Course:

More and more emphasis is put on security these days. As systems become more complex and Cloud enters the picture, the attack surface for data and services becomes greater. But where do we begin? Where is the starting point in our knowledge of how to tackle issues or proactively protect our environments?

In this 3-day course, we will cover the starting points of where to begin. This will be an overview of technologies, techniques, best practices, and frameworks that are available to help an individual feel comfortable with concepts related to Security in an on-premises, cloud, and hybrid environment.

Key Learning Areas:

- Why be Concerned about Security?
- Corporate and Enterprise Environment Configurations
- Threat Awareness
- Security Threats
- Threat Mitigation
- Proactive Security

Who Should Attend:

Cloud Admins, Security Admins, Networking Admins

Prerequisites:

Intermediate knowledge of computers and networks. Foundational knowledge of cloud-based infrastructures, such as Microsoft Azure.

Course Outline:

Why Be Concerned about Security?

It can be easy to say, "Let's get focused on security", but there are several domains that must be considered. In this module we'll cover the top areas of security concern:

- Users

- Systems
- Networks
- Data

Corporate and Enterprise Environment Configurations

From traditional environments to new cloud-only environments to those getting the best of both worlds in a hybrid configuration, each one has its own set of benefits and challenges. And all of them require working with operating systems. In this module, we'll consider:

- Operating Systems
  - Windows
  - Linux
  - macOS
- On Premises
  - Users
  - Network Infrastructure Components – Software
  - Network Infrastructure Components – Hardware
  - Data Stores
  - Physical and Virtual Machines
- Cloud
  - Identity
  - Virtual Networking
  - Storage Accounts
  - Database systems
  - Virtual Machines
  - Container infrastructures
- Hybrid
  - Identity and Access control
  - Hybrid networks
  - Hybrid data storage
  - Hybrid machine environments

Threat Awareness

Now that we are aware of the need for security and the different types of environments that most of our organizations support, what do we have to help us understand the risks and exploits? That will be the central theme in this module when we cover:

- Mitre ATT&CK
- OWASP Top Ten
- Zero-Trust model
- Azure Security Baselines
- Other Security frameworks

Security Threats

Since we have an idea of the categories of threats and baselines that can help us see where to begin, what is actually out there to cause us our environments harm? While we cannot cover every scenario, we will cover commonly seen threats. Let's discover these in this module by taking a close look at:

- Operating Systems
  - Windows
  - Linux
  - macOS
- On Premises
  - Network and software threats
  - Database threats
  - Hardware based (physical) machine threats
  - Software based (virtual) machine threats
- Cloud
  - Virtual Network threats
  - Database and server threats
  - Virtual machine threats
  - Application threats
  - Container threats
- Hybrid
  - Inter-site security configuration threats
  - Container exploits
- People
  - Social Engineering
  - Phishing/Smishing/Vishing
  - Other people control techniques

Threat Mitigation

Ok, the threats are there, we see what we are up against. What do we have to help us thwart or respond to attacks or threats? We will review a number of tools here, in each environment, as well as the importance of education in a security plan for an organization:

- On Premises
  - Active Directory Group Policy Objects
  - Security Templates and Policies
  - Server and Service Best Practices
  - ITSM/SEIM/SOAR
  - System Center
    - ✓ Operations Manager
    - ✓ Configuration Manager / Endpoint Manager
    - ✓ Data Protection Manager
    - ✓ Service Manager and Orchestrator
- In Cloud
  - Identity
    - ✓ Identity and Access Control (IAM)
    - ✓ Role Based Access Control (RBAC)
    - ✓ Privileged Identity Management (PIM)
    - ✓ Conditional Access
  - Networking
    - ✓ Network Security Groups / Application Security Groups
    - ✓ NAT
    - ✓ Azure Firewall
  - Azure Policy
  - Azure Monitor
    - ✓ Log Analytics
  - Intune / Endpoint Manager
  - Microsoft Defender for Cloud
  - Microsoft Sentinel
- Hybrid
  - Azure Backup
  - Azure BluePrints
  - Azure Monitor
- Cultural Awareness

- Training
- Simulations

Module 6 – Proactive Security

So many spend much of their day just putting out fires. Do you feel like that? What can be done to be proactive in our security? In this final module, we'll discuss:

- On Premises
  - System Center
    - Configuration Manager
    - Operations Manager
  - Scripting
  - Centralized logging
  - ITSM/SEIM/SOAR
  - "Secure by Default" implementations
- In Cloud / Hybrid
  - Azure Monitor
    - Log Analytics
    - Dashboards
    - Queries
  - Alerting – Action Groups
    - Event Hub
    - Logic Apps
    - Automation Accounts
  - Azure Policy
  - Azure BluePrints
  - Third-Pary solutions available in Azure