BREWSTER TECHNOLOGY
COMPUTER TRAINING & SERVICE
www.brewstertech.com
16 Mount Ebo Road South, Suite 18 • Brewster, New York • 10509
Phone – (845) 279-9400 • Fax – (845) 279-9413

WHAT'S IN 98-367 SECURITY FUNDAMENTALS:

MTA validates building-block technology concepts and helps students explore, discover and pursue successful careers in Information Technology (IT) in an exciting and rewarding way! As the first step in the Microsoft Technology Certification Series, this new, entry-level certification provides students with confidence, credibility, and differentiation.

TARGET AUDIENCE:

Individuals looking to get started in Security fundamentals.

PREREQUISITES:

Hands-on experience with Windows Server, Windows-based networking, Active Directory, anti-malware products, firewalls, network topologies and devices, and network ports.

DURATION:

12 hours

BREWSTER TECHNOLOGY
COMPUTER TRAINING & SERVICE
www.brewstertech.com
16 Mount Ebo Road South, Suite 18 • Brewster, New York • 10509
Phone – (845) 279-9400 • Fax – (845) 279-9413

TOPICS COVERED IN 98-367 SECURITY FUNDAMENTALS:

Understanding Security Layers

Introducing Security

- Understanding Confidentiality
- Understanding Integrity
- Understanding Availability
- Defining Threats and Risk Management
- Understanding the Principle of Least Privilege
- Understanding Attack Surface
- Understanding Social Engineering
- Linking Cost with Security

Looking at Physical Security as the First Line of Defense

- Understanding Site Security
- Understanding Computer Security

Starting Security with Authentication

Starting Security with Authentication

- Authenticating with What You Know
- Authenticating with What You Own or Possess
- Authenticating with What You Are
- Introducing RADIUS and TACAS+
- Using Run As

Introducing Directory Services with Active Directory

- Looking ad Domain Controllers
- Introducing NTLM
- Introducing Kerberos
- Using Organizational Units
- Looking at Objects
- Using Groups
- Looking at Web Server Authentication

Comparing Rights and Permissions

Looking at NTFS

- Using NTFS Permissions
- Looking at Effective NTFS Permissions
- Copying and Moving Files
- Using Folder and File Owners

Sharing Drives and Folders

- Looking at Special and Administrative Shares

Introducing the Registry

Using Encryption to Protect Data

- Examining Types of Encryption
- Introducing Public Key Infrastructure
- Encrypting Email
- Encrypting Files with EFS
- Encrypting Disks in Windows

Introducing IPSec

- Encrypting with VPN Technology

Using Auditing to Complete the Security Picture

Understanding Security Policies

Using Password Policies to Enhance Security

- Using Password Complexity to Make a Stronger Password
- Using Account Lockout to Prevent Hacking
- Looking at Password Length
- Using Password History to Enforce Security
- Setting the Time between Password Changes
- Using Password Group Policies to Enforce Security
- Understanding Common Attack Methods

Understanding Network Security

Using Dedicated Firewalls to Protect a Network

- Examining Hardware Firewalls and Their Characteristics
- Using Hardware Firewalls versus Software Firewalls
- Using Stateful versus Stateless Inspection

Controlling Access with Network Access Protection (NAP)

- Understanding the Purpose of NAP
- Looking at How NAP Works
- Examining the requirements for NAP

16 Mount Ebo Road South, Suite 18 • Brewster, New York • 10509
Phone – (845) 279-9400 • Fax – (845) 279-9413

Using Isolation to Protect the Network

- Understanding Virtual LANs
- Understanding Routing
- Looking at Intrusion Detection and Intrusion Prevention Systems
- Looking at Honeypots
- Looking at DMZs
- Understanding Network Address Translation (NAT)
- Understanding Virtual Private Networks (VPNs)
- Understanding Internet Protocol Security (IPsec)
- Using Other VPN Protocols
- Looking at Server and Domain Isolation

Protecting Data with Protocol Security

- Understanding Tunneling
- Using DNS Security Extensions (DNSSEC)
- Utilizing Network Sniffing
- Understanding Common NETWORK Attack Methods

Securing Wireless Network

- Using Service Set Identifier (SSID)

Understanding Keys

- Utilizing MAC Filters
- Considering Pros and Cons of Specific Security Types

Protecting the Server and Client

Protecting the Client Computer

- Protecting Your Computer from Malware
- Utilizing Windows Updates
- Utilizing User Account Control
- Using Windows Firewall
- Using Offline Files
- Locking Down a Client Computer

Protecting Your Email

- Dealing with Spam
- Relaying Email

Securing Internet Explorer

- Looking at Cookies and Privacy Settings
- Examining Content Zones
- Phishing and Pharming

Protecting Your Server

- Placing the Server
- Hardening the Server
- Using Secure Dynamic DNS