Security Fundamentals

Duration: 3 Days Course Code: M40367

Overview:

In this course, you will be introduced to security concepts for today's business and technology professionals. You will cover layered security philosophy, physical security, Internet security, and wireless security principles. You will focus on operating system security, network security, and security software. The course is designed to help you prepare for Microsoft Technology Associate (MTA) Exam: 98-367 - Security Fundamentals, which can be taken outside of the course.

Target Audience:

IT management, project managers, compliance personnel, business analysts, or anyone who requires a basic understanding of core security concepts and their application in a private or public sector setting.

Objectives:

- Offensive and defensive security strategies and approaches
- Implement security in layers ranging from physical security, network security, and operating system security
- Secure authentication, access-control on file systems, and password policies for users
- Use Network Access Protection (NAP), firewalls, and protocol security for data in-flight
- Use security software as counter-measures, including anti-virus software, anti-spam software, and encryption

Prerequisites:

- General understanding and familiarity of IT business environments is beneficial

Follow-on-Courses:

- There are no follow-ons for this course.

Content:

Security Layers

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Security Policies

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles

- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Authentication, Authorization, and Accounting

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of

- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Network Security

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of

- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Protecting the Server and Client

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security

Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

- Security Fundamentals
- Physical Security as the First Line of Defense
- Core Security Principles
- Physical Security
- Authentication
- Rights and Permissions
- Auditing
- Encryption
- User Authentication
- Audit Policies
- Using Password Policies to Enhance Security
- Using Dedicated Firewalls to Protect a Network
- Controlling Access with Network Access Protection (NAP)
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Securing a Wireless Network
- Network Isolation
- Protocol Security
- Wireless Security
- Protecting a Computer from Malware
- Protecting the Client Computer
- Protecting E-Mail
- Protecting a Server
- Securing Internet Explorer

Further Information:

For More information, or to book your course, please Email us on:

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

UAE - training.emea@clclearningafrica.com