Helpdesk Certification Training Course

Helpdesk Support Specialist (HSP)

Course Number: #MDTS-105
Course Length: 10 days
Number of Exams: 1
Certifications: Security Plus

The Helpdesk Specialist course is 100% hands-on training. This course prepares students with Helpdesk skillset that allows them to perform successfully on the job. The focus is to provide students with hands-on training.

These courses assume you are familiar with using personal computers, mouse and keyboard (basic typing skills are recommended). You should be comfortable in the Windows environment and be able to use Windows to manage information on your computer. Specifically, you should be able to launch and close programs, navigate to information stored on the computer and manage files and folders.

HELPDESK SUPPORT SPECIALIST

MD Tech Solutions Helpdesk Support Specialist course is 100% hands-on training. In this course, the student learns how to take calls, fix user's systems issues, install and configure printers and more. This course will provide you with the skillset to take on a career as a Helpdesk Support Specialist. to become a Helpdesk Specialist, you must first obtain a Security+ IAT Level II certification or higher. During this training, we will offer CompTIA Security+. The Security+ Certification is a Worldwide Trusted Certification to validate Fundamental Skills and Knowledge of Vendor-Neutral IT Security. The Cert Training is an additional Week Per Course.

Course Outline

Agenda

Course Overview

- Introductions
  - Instructor
  - Students
- Course Overview
  - Breaks
  - Rules
- Video
  - Phone Calls
  - Helpdesk Calls
- Lab (User Administration)
- Revert Computer back to New
- Resumes
- Interviewing

Capture a Snapshot of laptop

- Run Microsoft Update
- Uninstall Virus Protection

- Install McAfee
    - Schedule Scan
- Install Printers
    - Troubleshoot Printer Issues
- Rename Computer
- Add Computer to Domain
- Working as a Team (Project)
- Resumes
- Interviewing

TCP/IP and Cabling

- Networking
    - IP Address
    - DHCP
    - DNS
- Port Security
    - Initial
    - Clear Errdisable
- Active Directory
    - Create New Account
    - Reset Password and Account Lockout
    - Enable and Disable User Account
    - Move User to Disable Account Group
    - Group Policy
- Cabling
    - Types of Cables
    - Wiring (Crossover, Straight Through…)
- Resumes
- Interviewing

Review Helpdesk Reporting Tools

- Remedy
- Service Now
- Take Service Call
- Difficult Customer
- Resolve Computer Issue
- How to get 5-star customer satisfaction ratings
- Resumes
- Interviewing

Hands On

- Lab Hands on Support Desk Calls and Resolutions
- Resumes
- Interviewing

Security Plus

1.0 Network Security

1.1 Implement security configuration parameters on network devices and other technologies.

- Firewalls
- Routers
- Switches
- Load Balancers
- Proxies
- Web security gateways
  VPN concentrators
  NIDS and NIPS
  Protocol analyzers
  Spam filter
  UTM security appliances
  Web application firewall vs. network firewall Application aware devices

1.2 Given a scenario, use secure network administration principles.

- Rule-based management
- Firewall rules
- VLAN management
- Secure router configuration
- Access control lists
- Port Security
- 802.1x
- Flood guards
- Loop protection
- Implicit deny
- Network separation
- Log analysis
- Unified Threat Management

1.3 Explain network design elements and components.

- DMZ
- Subnetting
- VLAN
- NAT
- Remote Access
- Telephony
- NAC
- Virtualization
- Cloud Computing
- Layered security / Defense in depth

1.4 Given a scenario, implement common protocols and services.

- Protocols
- Ports

- OSI relevance

1.5 Given a scenario, troubleshoot security issues related to wireless networking.

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
  Disable SSID broadcast
  TKIP
  CCMP
  Antenna Placement
  Power level controls
  Captive portals
- Antenna types
- Site surveys
- VPN (over open wireless)

2.0 Compliance and Operational Security

2.1 Explain the importance of risk related concepts.

- Control types
- False positives
- False negatives
- Importance of policies in reducing risk
- Risk calculation
- Quantitative vs. qualitative
- Vulnerabilities
- Threat vectors
- Probability / threat likelihood
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated with Cloud Computing and Virtualization
- Recovery time objective and recovery point objective

2.2 Summarize the security implications of integrating systems and data with third parties.

- On-boarding/off-boarding business partners
- Social media networks and/or applications
- Interoperability agreements
- Privacy considerations
- Risk awareness
- Unauthorized data sharing
- Data ownership
- Data backups
- Follow security policy and procedures
- Review agreement requirements to verify compliance and performance standards

2.3 Given a scenario, implement appropriate risk mitigation strategies.

- Change management ☐ Incident management
- User rights and permissions reviews
- Perform routine audits
- Enforce policies and procedures to prevent data loss or theft
- Enforce technology controls

2.4 Given a scenario, implement basic forensic procedures.

  - Order of volatility
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
- Witnesses
- Track man hours and expense
- Chain of custody
- Big Data analysis

2.5 Summarize common incident response procedures.

- Preparation
- Incident identification
- Escalation and notification
- Mitigation steps
- Lessons learned
- Reporting
- Recovery/reconstitution procedures
- First responder
- Incident isolation
- Data breach
- Damage and loss control

2.6 Explain the importance of security related awareness and training.

- Security policy training and procedures
- Role-based training
- Personally identifiable information
- Information classification
- Data labeling, handling and disposal
- Compliance with laws, best practices and standards
- User habits
- New threats and new security trends/alerts
- Use of social networking and P2P
- Follow up and gather training metrics to validate compliance and security posture

2.7 Compare and contrast physical security and environmental controls.

- Environmental controls
- Physical security
- Control types

2.8 Summarize risk management best practices.

- Business continuity concepts
- Fault tolerance
- Disaster recovery concepts

2.9 Given a scenario, select the appropriate control to meet the goals of security.

Confidentiality
Integrity
Availability
Safety

3.0 Threats and Vulnerabilities

3.1 Explain types of malware.

- Adware
- Virus
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets
- Ransomware
- Polymorphic malware
- Armored virus

3.2 Summarize various types of attacks.

- Man-in-the-middle
- DDoS
- DoS
- Replay
- Smurf attack
- Spoofing
- Spam
- Phishing
- Spim
- Vishing
- Spear phishing
- Xmas attack
- Pharming
- Privilege escalation
- Malicious insider threat
- DNS poisoning and ARP poisoning
- Transitive access
- Client-side attacks
- Password attacks
- Typo squatting/URL hijacking
- Watering hole attack

3.3 Summarize social engineering attacks and the associated effectiveness with each attack.

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
  Hoaxes
  Whaling
  Vishing
  Principles (reasons for effectiveness)

3.4 Explain types of wireless attacks.

- Rogue access points
- Jamming/Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing
- Near field communication
- Replay attacks
- WEP/WPA attacks
- WPS attacks

3.5 Explain types of application attacks.

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Integer overflow
- Zero-day
- Cookies and attachments
- LSO (Locally Shared Objects)
- Flash Cookies
- Malicious add-ons
- Session hijacking
- Header manipulation
- Arbitrary code execution / remote code execution

3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.

- Monitoring system logs
- Hardening
- Network security
- Security posture
- Reporting
- Detection controls vs. prevention controls

3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.

- Interpret results of security assessment tools
  Tools
  Risk calculations
  Assessment types
  Assessment technique

3.8 Explain the proper use of penetration testing versus vulnerability scanning.

- Penetration testing
- Vulnerability scanning
- Black box
- White box
- Gray box

4.0 Application, Data and Host Security

4.1 Explain the importance of application security controls and techniques.

- Fuzzing
- Secure coding concepts
- Cross-site scripting prevention
- Cross-site Request Forgery (XSRF) prevention
- Application configuration baseline (proper settings)
- Application hardening
- Application patch management
- NoSQL databases vs. SQL databases
- Server-side vs. Client-side validation

4.2 Summarize mobile security concepts and technologies.

- Device security
- Application security
- BYOD concerns

4.3 Given a scenario, select the appropriate solution to establish host security.

- Operating system security and settings
- OS hardening
- Anti-malware
- Patch management
- White listing vs. black listing applications
- Trusted OS
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
- Host software baselining
- Virtualization

4.4 Implement the appropriate controls to ensure data security.

- Cloud storage

- SAN

Handling Big Data
Data encryption
Hardware based encryption devices
Data in-transit, Data at-rest, Data in-use

- Permissions/ACL
- Data policies

4.5 Compare and contrast alternative methods to mitigate security risks in static environments.

- Environments
- Methods

5.0 Access Control and Identity Management

5.1 Compare and contrast the function and purpose of authentication services.

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- Secure LDAP

5.2 Given a scenario, select the appropriate authentication, authorization or access control.

- Identification vs. authentication vs. authorization
- Authorization
- Authentication
- Authentication factors
- Identification
- Federation
- Transitive trust/authentication

5.3 Install and configure security controls when performing account management, based on best practices.

- Mitigate issues associated with users with multiple account/roles and/or shared accounts ☐ Account policy enforcement
- Group based privileges
- User assigned privileges
- User access reviews
- Continuous monitoring

6.0 Cryptography

6.1 Given a scenario, utilize general cryptography concepts.

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods

Transport encryption
Non-repudiation
Hashing
Key escrow

- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy

6.2 Given a scenario, use appropriate cryptographic methods.

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
- Cipher suites
- Key stretching

6.3 Given a scenario, use appropriate PKI, certificate management and associated components.

- Certificate authorities and digital certificates
- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models