



Cisco Certified Support Technician – Cybersecurity

Online Course

Learn
Remotely..

ZETLAN TECHNOLOGIES
www.zetlantech.com

Cisco Certified Support Technician – Cybersecurity



Course Modules

1. Define Essential Security Principles

- Vulnerabilities, threats, exploits, and risks; attack vectors
- Hardening
- Defense-in-depth
- Confidentiality, integrity, and availability (CIA)
- Types of attackers
- Reasons for attacks
- Code of ethics

2. Explain Common Threats and Vulnerabilities

- Malware
- Ransomware
- Denial of Service
- Botnets
- Social Engineering Attacks (Tailgating, Spear Phishing, etc.,)
- Physical Attacks
- Man in the middle
- IoT vulnerabilities
- Insider Threats
- Advanced Persistent Threat (APT)



Cisco Certified Support Technician – Cybersecurity



3. Explain Access Management Principles

- Authentication
- Authorization, and accounting (AAA)
- RADIUS
- Multifactor Authentication (MFA)
- Password Policies

4. Explain encryption methods and applications

- Types of encryptions, hashing, public key infrastructure (PKI)..
- Strong vs. weak encryption algorithms
- States of data and appropriate encryption
- Protocols that use Encryption

5. Describe TCP/IP protocol vulnerabilities

- TCP
- UDP
- HTTP
- ARP
- ICMP
- DHCP
- DNS

Zetlan Technologies



ZETLAN TECHNOLOGIES

Cisco Certified Support Technician – Cybersecurity

6. Explain how Network Addresses Impact Network Security

- IPv4 and IPv6 addresses
- MAC addresses
- Network segmentation
- CIDR notation
- NAT
- Public vs. Private Networks



7. Describe Network Infrastructure and Technologies

- Network security architecture
- DMZ
- Virtualization
- Cloud
- Honeypot
- Proxy server
- IDS
- IPS

Zetlan Technologies

8. Set up a Secure Wireless SoHo Network

- MAC address filtering
- Encryption standards and protocols
- SSID



ZETLAN TECHNOLOGIES

Cisco Certified Support Technician – Cybersecurity

9. Implement secure Access Technologies

- ACL
- Firewall
- VPN
- NAC



10. Describe Operating System Security

- Windows, macOS, and Linux
- CLI and PowerShell
- File and Directory Permissions
- Privilege Escalation

11. Familiarity with Appropriate Endpoint Tools

- Netstat
- Nslookup
- Tcp Dump

Zetlan Technologies

12. The endpoint systems meet security policies & standards

- Hardware inventory (asset management)
- Software Inventory
- Program Deployment
- Data Backups
- Regulatory compliance (PCI DSS, HIPAA, GDPR)
- BYOD (Device Management, Data Encryption, etc)



ZETLAN TECHNOLOGIES

Cisco Certified Support Technician – Cybersecurity

13. Implement Software and Hardware Updates

- Windows Update
- Application Updates
- Device Drivers
- Firmware
- Patching



14. Interpret System Logs

- Event Viewer
- Audit logs
- System and Application Logs
- Syslog
- Identification of Anomalies

15. Demonstrate Familiarity with Malware Removal

- Scanning systems
- Reviewing scan logs
- Malware Remediation

16. Explain vulnerability management

- Vulnerability Identification
- Management, and mitigation
- Active and Passive reconnaissance
- Testing (Port scanning, Automation)



Cisco Certified Support Technician – Cybersecurity

17. Use threat intelligence techniques to identify vulnerabilities

- Uses and limitations of vulnerability databases
- Industry-standard tools used to assess vulnerabilities
- Common Vulnerabilities and Exposures (CVEs), etc.,
- Ad Hoc and automated threat intelligence



18. Explain risk management

- Vulnerability vs. risk
- Ranking risks
- Approaches to risk management
- Risk mitigation strategies
- Levels of risk (low, medium, high, extremely high)
- Risks associated with specific types of data and data classifications
- Security assessments of IT systems
- Importance of disaster recovery & business continuity planning
- Features of disaster recovery plans & business continuity plans
- Backup & disaster recovery controls (detective, preventive, etc)

19. Security events and know when escalation is required

- Role of SIEM and SOAR
- Monitoring Network data to identify security incidents
- Identifying suspicious events as they occur



Cisco Certified Support Technician – Cybersecurity

For Enquiry: +91 8680961847

20. Digital forensics and attack attribution processes

- Cyber Kill Chain
- MITRE ATT&CK Matrix, and Diamond Model
- Tactics, Techniques, and Procedures (TTP)
- Sources of evidence (artifacts)
- Evidence Hndlg (preserving digital evidence, chain of custody)

21. Impact of compliance frameworks on incident handling

- Compliance frmwrks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA)

22. The elements of cybersecurity incident response

- Policy, plan, and procedure elements
- Incident Response Lifecycle Stages



Zetlan Technologies

Free Advice: +91 9600579474

www.zetlantech.com



**LEARN
REMOTELY!!**

**The efficiency of online learning
in terms of time management,
flexibility, and the ability
to access resources anytime,
anywhere can be compelling.**



ZETLAN TECHNOLOGIES
www.zetlantech.com

**For contact: +91 8680961847
+91 9600579474**

