System Security Certified Practitioner

Zetlan Technologies

ZETLAN TECHNOLOGIES
www.zetlantech.com

Learn without Leaving Home..!

Online Course

Course Modules

Security Operations and Administration

1.Comply with codes of ethics

- ISC2 Code of Ethics
- Organizational code of ethics

2.Understand security concepts

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy
- Non-repudiation
- Least privilege
- Segregation of duties (SoD)

Zetlan Technologies

3.Identify and implement security controls

- Technical controls (e.j., session timeout, password aging)
- Physical controls (e.g., mantraps, cameras, locks)
- Administrative controls (e.g., security policies, standards)
- Assessing compliance
- Periodic audit and review

4.Document and maintain functional security controls

- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Compensating controls

5.Participate in asset mngmnt lifecycle (hardware, software)

- Process, planning, design and initiation
- Development/Acquisition
- Inventory and licensing
- Implementation/Assessment
- Operation/Maintenance
- Archiving and retention requirements
- Disposal and destruction

6.Participate in change management lifecycle

- Change management (e.g., roles, responsibilities, processes)
- Security impact analysis
- Configuration management (CM)

Zetlan Technologies

Participate in implementing security awareness and training
Collaborate with physical security operations

Access Controls

7.Implement and maintain authentication methods

- Single/Multi-factor authentication (MFA)
- Single sign-on (SSO) (e.g., Active Directory Federation Services
- Device authentication
- Federated access (e.g.Open Authorization 2 (OAuth2),(SAML))

8.Support internetwork trust architectures

- Trust relationships (e.g., 1-way, 2-way, transitive, zero)
- Internet, intranet and extranet
- Third-party connections

Zetlan Technologies

9.Participate in the identity management lifecycle

- Authorization
- Proofing
- Provisioning/De-provisioning
- Maintenance
- Entitlement
- Identity and access management (IAM) systems

10. Understand and apply access controls

- Mandatory
- Discretionary
- Role-based (e.g., attribute-, subject-, object-based)
- Rule-based

Risk Identification, Monitoring and Analysis

11. Understand the risk management process

- Risk visibility & reporting (e.g.risk register, sharg threat intelligt)
- Risk mngmt concepts (e.g., impact assessments, threat modelg)
- Risk management frameworks
- Risk tolerance (e.g., appetite)
- Risk treatment (e.g., accept, transfer, mitigate, avoid)

Zetlan Technologies

Legal and regulatory concerns (e.g., jurisdiction, limitations)

12. Participate in security assessment & vulnerability mngmt

- Security testing
- Risk review (e.g., internal, supplier, architecture)
- Vulnerability management lifecycle

13. Operate and monitor security platforms

- Source systems (e.g., apps, security appliances, network devices)
- Events of interest (e.g.anomalies, intrusions, unauthrized chngs)
- Log management
- Event aggregation and correlation

14. Analyze monitoring results

- Security baselines and anomalies
- Visualizations, metrics, & trends (e.g., notis, dashboards, timlns)
- Event data analysis
- Document and communicate findings (e.g., escalation)

Incident Response and Recovery

15. Support incident lifecycle e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO)

- Preparation
- Detection, analysis and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/implementation of new countermeasure

16. Understand and support forensic investigations

- Legal (e.g., civil, criminal, administrative) and ethical principles
- Evidence handling (e.g., first responder, triage, chain of custody)
- Reporting of analysis

17. Business continuity plan (BCP) & disastr recvry plan (DRP)

- Emergency response plans and procedures
- Interim or alternate processing strategies
- Restoration planning
- Backup and redundancy implementation
- Testing and drills

Cryptography

18. Understand cryptography

- Confidentiality
- Integrity and authenticity
- Data sensitivity (e.g., (PII),(IP), protected health informatn (PHI))
- Regulatory & industry best practice (e.g., (PCI-DSS), (ISO))

Zetlan Technologies

19. Apply cryptography concepts

- Hashing
- Salting
- Symmetric/Asymmtrc encryptn/Elliptic curve cryptography(ECC)
- Non-repudiation(e.g., digital signatures/certificates, (HMAC))
- Strength of encryption algorithms and keys (e.g., (AES), etc.)
- Cryptographic attacks, cryptanalysis, and countermeasures

20. Understand and implement secure protocols

- Services and protocols
- Common use cases
- Limitations and vulnerabilities

21. Understand public key infrastructure (PKI)

- Fundamental key management concepts (e.g., storage, rotation)
- Web of Trust (WOT)

Network and Communications Security

22. Understand & apply fundamental concepts of networking

- Open Systems Interconnection (OSI) and (TCP/IP) models
- Network topologies
- Network relationships (e.g., peer-to-peer (P2P), client server)
- Transmission media types (e.g., wired, wireless)
- Software-defined networking (SDN)
- Commonly used ports and protocols

Network attacks (e.g., (DDoS), (MITM), (DNS) poisoning)

23. Manage network access controls

- Network access controls, standards and protocols
- Remote access operation and configuration

Zetlan Technologies

24. Manage network security

- Logical and physical placement of network devices
- Segmentation (e.g., physical/logical,data/control plane(VLAN))
- Secure device management

25. Operate and configure network-based security devices

- Firewalls & proxies (e.g., filtering methods, (WAF), (IDS) & (IPS)
- Network intrusion detection/prevention systems
- Routers and switches
- Traffic-shaping devices (e.g., wide area network (WAN))

26. Secure wireless communications

- Technologies (e.g., cellular network, Wi-Fi, Bluetooth, (NFC))
- Authentication & encryption protocols (e.g.(WEP), (WPA), (EAP))
- Internet of Things (IoT)

Systems and Application Security

27. Identify and analyze malicious code and activity

- Malware (e.g.,rootkits, spyware, scareware, ransomware, trojans)
- Malware countermeasures (e.g., scanners, anti-malware)
- Malicious activity (e.g.insider threat, data theft)
- Malicious activity countermeasures (e.g., user awareness, systm)
- sandboxing, isolation, data loss prevention (DLP))

Zetlan Technologies

28. Implement and operate endpoint device security

- Host-based intrusion prevention system (HIPS)
- Host-based firewalls
- Application white listing
- Endpoint encryption (e.g., whole disk encryption)
- Trusted Platform Module (TPM)
- Secure browsing
- Endpoint Detection and Response (EDR)

29. Administer Mobile Device Management (MDM)

- Provisbg technques (e.g., (COPE), Bring Your Own Device(BYOD))
- Containerization
- Encryption
- Mobile application management (MAM)

30. Understand and configure cloud security

- Deployment models (e.g., public, private, hybrid, community)
- Servce models (e.g.,(IaaS), (PaaS) & Software as a Service (SaaS))
- Virtualization (e.g., hypervisor)
- Legal & regulatory concerns (e.g., privacy, surveillance)
- Data storage, processing, & transmission (e.g., archiving)
- Third-party/outsourcing requirements
- Shared responsibility model

For Enquiry: +91 8680961847

31. Operate and maintain secure virtual environments

- Hypervisor
- Virtual appliances
- Containers
- Continuity and resilience
- Attacks and countermeasures
- Shared storage

Zetlan Technologies

Zetlan Technologies

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