CyberSec First Responder

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES

www.zetlantech.com

Course Modules

Identify

1. Identify assets (applications, workstations, servers, appliances, operating systems, and others).

- Asset identification tools
- Tools
- Operating system information
- Determine which tools to use for each part of the network
- Network topology and architecture information
- Data flow
- Vulnerable ports
- SPAN ports and TAP devices for live packet capture

2. Identify factors that affect the tasking, collection, processing, etc.,

- Identify relevant policies and procedures
- Collect artifacts and evidence based on volatility level
- Review service level agreements (SLAs)
- Network scanning
- Assets and underlying risks
- Data collection
- Data analytics and e-discovery
- Monitor threats and vulnerabilities
- Threat modeling
- Identify TTPs

3. Identify and evaluate vulnerabilities and threat actors.

- Vulnerability scanning tools
- Threat targets
- Mobile & IoT
- SCADA
- ICS & PLC
- Threat actors
- Threat motives/reasons
- Threat intent
- Attack phases & Attack vectors
- Technique criteria

CyberSec First Responder

4. **Identify applicable compliance, standards, frameworks, etc.,**
   - Privacy laws, standards, and regulations
   - Frameworks
   - Best practices

5. **Identify applicable compliance, standards, frameworks, etc.,**
   - Security laws, standards, and regulations
   - Frameworks

6. **Identify and conduct vulnerability assessment processes.**
   - Critical assets and data
   - Establish scope
   - Determine vulnerability assessment frequency
   - Identify common areas of vulnerability
   - Users
   - Internal acceptable use policies
   - Operating systems
   - Applications
   - Network operations and management
   - Firewall
   - Network security applications
   - Network devices
   - Network infrastructure

- DSL
- Wireless protocols
- IP addressing
- Configuration files
- IoT
- Regulatory requirements
- Changes to the system
- Determine scanning criteria
- IoC information
- Perform a vulnerability assessment
- Conduct post-assessment tasks
- Hardening
- Patches
- Exceptions documented

7. Establish relationships between internal teams & external groups

- Formal policies that drive these internal & external relationships
- SLAs
- Communication policies and procedures
- Points of contact and methods of contact
- Vendor agreements, NDAs, & vendor assessment questionnaires
- Privacy rules and laws
- Understanding of relevant law enforcement agencies

Protect

8. Analyze and report system security posture trends.

- Data analytics
- Prioritize the risk observations and formulate remediation steps
- Analyze security system logs, tools, and data
- Threats and vulnerabilities
- Intrusion prevention systems and tools
- Security vulnerability databases
- Discover vulnerabilities in information systems
- Create reports and document evidence

9. Apply security policies to meet the system's cybersecurity objectives and defend against cyber-attacks and intrusions.

- Cybersecurity policies and procedures
- Active Directory Group Policy Objects (GPOs)
- Best practices in hardening techniques
- Threats and vulnerabilities
- Security laws, standards, and regulations
- Risk management principles
- Attack methods and techniques
- DoS

CyberSec First Responder

10. Collaborate across internal and external organizational lines

- Organizational structure
- Internal teams
- Personnel roles and responsibilities
- Communication policies and procedures
- Knowledge sharing processes
- Conflict management
- SLAs
- Relationships with external stakeholders

11. Employ approved defence-in-depth principles and practices.

- Intrusion Prevention or Detection Systems (IDS/IPS)
- Firewalls
- Network Segmentation
- Endpoint Detection and Response (EDR)
- Account Management
- Patch management
- Mobile Device Management (MDM)

12. Develop & implement cybersecurity independent audit processes.

- Identify assets
- Cybersecurity policies and procedures
- Data security policies

- Cybersecurity auditing processes and procedures
- Audit objectives
- Network structure
- Compliance standards
- Document and communicate results

13. Plans of action are in place for vulnrablts identifd durng risk asmt

- Review assessments, audits, and inspections
- Analyze critical issues for action
- Develop plans of action
- Specify success criteria
- Remediation planning
- Resource implications
- Monitoring procedures

14. Protect organizational resources through security updates.

- Cybersecurity policies and procedures
- Software updates
- Firmware updates
- Software patches

15. Protect identity managmnt & access control within the organiztn

- Enterprise resources
- Access control
- Authentication systems
- Remote-access monitoring
- Cybersecurity policies and procedures
- Identity management
- Authorization
- Infrastructure/physical security
- Physical security controls
- User credentials

Detect

16. Analyze common indicators of potential compromise, anomalies..

- Analyze security system logs, security tools, and data
- IP networking/ IP resolving
- DoS attacks/ DDoS attacks
- Security Vulnerability Databases
- Intrusion Detection Systems
- Network encryption
- SSL decryption

CyberSec First Responder

- SIEM & Firewalls
- DLP & IPS
- IDS
- Evaluate and interpret metadata
- Malware
- Network topology
- Anomalies
- Unauthorized programs in the startup menu
- Malicious software
- Registry entries
- Unusual network traffic
- Off-hours usage
- New administrator/user accounts
- Guest account usage
- Unknown open ports
- Unknown use of protocols
- Service disruption
- Website defacement
- Unauthorized changes/modifications
- Recipient of suspicious emails
- Unauthorized sessions
- Failed logins
- Rogue hardware

17. Analysis of log files from various sources to idntfy possbl threats

- Log collection
- Log auditing
- Log enrichment
- Alerts, reports, and event correlation
- Log retention
- Log aggregator and analytics tools
- Linux tools
- Windows tools
- Scripting languages
- Cloud
- Threat feeds

18. Provide timely detection, identification, & alert of possibl attacks

- Asset discovery methods and tools
- Alerting systems
- Intrusion Prevention or Detection Systems (IDS/IPS)
- Firewalls
- Endpoint Detection and Response (EDR)
- Commn indcatrs of potential compromise, anomalies, & patterns
- Analysis tools
- Document and communicate results

19. Take appropriate action to document and escalate incidents

- Communication and documentation policies and processes
- Security incident reports
- Escalation processes and procedures
- Incident response teams
- Levels of Authority
- Personnel roles and responsibilities
- Document and communicate results

20. Determine the extent of threats & recommend courses of action

- Post exploitation tools and tactics
- Prioritization or severity ratings of incidents
- Communication policies and procedures
- Levels of Authority
- Communicate recommend courses of action & countermeasures

Respond

21. Execute the incident response process.

- Incident response plans and processes
- Communication with internal and external stakeholders
- Personnel roles and responsibilities
- Incident reporting & Containment Methods

- Containment Tools
- Windows tools to analyze incidents
- Linux-based tools to analyze incidents

22. Collct & seize docmntry or physcal evdence & create a forenscally

- Evidence collection, preservation, and security
- Chain of custody
- Forensic investigation
- Forensic collection and analysis tools
- Forensically sound duplicates
- Document and communicate results

23. Correlate incident data and create reports.

- Logs
- Data analysis
- Intrusion Prevention or Detection Systems (IDS/IPS)
- Forensics analysis
- Correlation analysis
- Event correlation tools and techniques
- Root cause analysis
- Alerting systems
- Incident reports
- Document and communicate results

24.Systm securty measurs in accordance with establshd procedures.

- Escalation procedures
- Organizational systems and processes

25. Determine tactics, techniques, & procedurs (TTPs) of intrusn sets.

- Threat actors
- Tactics
- Techniques
- Procedures

26.Interface with internal teams and external organizations

- Communication policies and procedures
- Internal communication methods
- External communication guidelines

Recover

27. Implement recovery planning processes and procedures

- Post-incident
- Analyze incident reports
- Execute recovery planning processes and procedures
- Document and communicate results

28.Implmt specific cyberscurty countermeasures for systems & apps.

- Security requirements of systems
- System interoperability and integration
- Prevention & mitigation
- Safeguards

29.Review forensic images & other data sources for recovery

- Memory forensics analysis/tools
- Data sources and disk images
- Analysis of digital evidence
- Hardware and software tools
- File copying techniques
- File modification, access, and creation times
- Forensic recordkeeping
- Forensic investigation
- Forensic collection and analysis tools

30. Provide advice and input for disaster recovery, contingency, etc.,

- Recovery planning processes
- Contingency planning
- Systems and assets
- Lessons learned
- Review of existing strategies
- Implement improvements
- Doc & communicate reprts, lessons learnd, & advice for recovery

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