CBROPS – Cisco Certified CyberOps Associate

Zetlan Technologies

Follow us on

ZETLAN TECHNOLOGIES

www.zetlantech.com

Course Modules

1.Security Concepts

- Describe the CIA triad
- Compare security deployments
- Network, endpoint, and application security systems
- Agentless and agent-based protections
- Legacy antivirus and antimalware
- SIEM, SOAR, and log management e. Container & virtual envmt
- Cloud security deployments
- Describe security terms
- Threat intelligence (TI)
- Threat hunting
- Malware analysis
- Threat actor
- Run book automation (RBA)
- Reverse engineering
- Sliding window anomaly detection
- Principle of least privilege
- Zero trust
- Threat intelligence platform (TIP)
- Threat modelling

CBROPS – Cisco Certified CyberOps Associate

- Compare security concepts
- Risk (risk scoring/risk weighting, risk reduction, risk assessment)
- Threa •Vulnerability
- Exploit

- Describe the principles of the defence-in-depth strategy
- Compare access control models
- Discretionary access control
- Mandatory access control
- Nondiscretionary access control
- Authentication, authorization, accounting
- Rule-based access control
- Time-based access control
- Role-based access control
- Attribute-based access control
- Describe terms as defined in CVSS
- Attack vector
- Attack complexity
- Privileges required
- User interaction
- Scope
- Temporal metrics
- Environmental metrics

3.Host-Based Analysis

- Functionality of these endpoint tchnlgs in regard to scrty mnitr
- Host-based intrusion detection
- Antimalware and antivirus
- Host-based firewall
- Application-level allow listing/block listing
- Systems-based sandboxing (such as Chrome, Java, etc)
- Identify components of an operating system
- Describe the role of attribution in an investigation
- Assets
- Threat actor
- Indicators of compromise
- Indicators of attack
- Chain of custody
- Identify type of evidence used based on provided logs
- Best evidence
- Corroborative evidence

- Compare tampered and untampered disk image
- Interpret operating system, app, or command line logs
- Interpret the output report of a malware analysis tool
- Hashes
- URLs
- Systems, events, and networking

4.Network Intrusion Analysis

- Map the provided events to source technologies
- IDS/IPS
- Firewall
- Network application control
- Proxy logs
- Antivirus
- Transaction data (NetFlow)
- Compare impact and no impact for these items
- False positive
- False negative
- True positive
- True negative
- Benign
- Compare deep packet inspection with packet filtrg & stateful
- Compare inline traffic interrogation and taps or traffic monitorg
- Compare the characteristics of data obtained from taps
- Extract files frm a TCP stream whn gvn a PCAP file & Wireshark
- Identify key elements in an intrusion from a given PCAP file
- Source address
- Destination address
- Source port
- Destination port

CBROPS – Cisco Certified CyberOps Associate

- Protocols
- Payloads
- Interpret the fields in protocol headers as related
- Ethernet frame
- IPv4
- IPv6
- TCP
- UDP
- ICMP
- DNS
- SMTP/POP3/IMAP
- HTTP/HTTPS/HTTP2
- ARP
- Interpret common artifact elements from an event
- IP address (source / destination)
- Client and server port identity
- Process (file or registry)
- System (API calls)
- Hashes
- URI / URL
- Interpret basic regular expressions

CBROPS – Cisco Certified CyberOps Associate

- Elements in an incident rspns plan as stated in NIST.SP800-61
- Apply the incident handling process such as NIST.SP800-61
- Map elements steps of analysis based on the NIST.SP800-61
- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident analysis (lessons learned)
- Map the organization stakeholders against the NIST IR categres
- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident analysis (lessons learned)
- Describe concepts as documented in NIST.SP800-86
- Evidence collection order
- Data integrity
- Data preservation
- Volatile data collection
- Identify these elements used for network profiling
- Total throughput
- Session duration
- Ports used
- Critical asset address space

- Identify these elements used for server profiling
- Listening ports
- Logged in users/service accounts
- Running processes
- Running tasks
- Applications
- Identify protected data in a network
- PII
- PSI
- PHI
- Intellectual property
- Classify intrusion events into categories as defined
- Describe the relationship of SOC metrics to scope analysis

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