CCIE HUB

LEARN | LAB | CERTIFY

CCNA CYBER SECURITY

PROTECTING YOUR DIGITAL WORLD

TALK TO US

+91 96502 72078

+91 70111 33431

info@cciehub.in

FOLLOW US

www.cciehub.in

1.0 Security Concepts - 20%

1.1 Describe the CIA triad

1.2 Compare security deployments

- 1.2.a Network, endpoint, and application security systems
- 1.2.b Agentless and agent-based protections
- 1.2.c Legacy antivirus and antimalware
- 1.2.d SIEM, SOAR, and log management
- 1.2.e Container and virtual environments
- 1.2.f Cloud security deployments

1.3 Describe security terms

- 1.3.a Threat intelligence (TI)
- 1.3.b Threat hunting
- 1.3.c Malware analysis
- 1.3.d Threat actor
- 1.3.e Run book automation (RBA)
- 1.3.f Reverse engineering
- 1.3.g Sliding window anomaly detection
- 1.3.h Threat modeling
- 1.3.i DevSecOps

1.4 Compare security concepts

- 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment)
- 1.4.b Threat
- 1.4.c Vulnerability
- 1.4.d Exploit

1.5 Describe the principles of the defense-in-depth strategy

1.6 Compare access control models

- 1.6.a Discretionary access control
- 1.6.b Mandatory access control
- 1.6.c Nondiscretionary access control
- 1.6.d Authentication, authorization, accounting
- 1.6.e Rule-based access control
- 1.6.f Time-based access control
- 1.6.g Role-based access control
- 1.6.h Attribute-based access control

1.7 Describe terms as defined in CVSS

- 1.7.a Attack vector
- 1.7.b Attack complexity
- 1.7.c Privileges required
- 1.7.d User interaction
- 1.7.e Scope
- 1.7.f Temporal metrics
- 1.7.g Environmental metrics

1.8 Identify the challenges of data visibility (network, host, and cloud) in detection

1.9 Identify potential data loss from traffic profiles

1.10 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

1.11 Compare rule-based detection vs. behavioral and statistical detection

2.0 Security Monitoring - 25%

2.1 Compare attack surface and vulnerability

2.2 Identify the types of data provided by these technologies

- 2.2.a TCP dump
- 2.2.b NetFlow
- 2.2.c Next-gen firewall
- 2.2.d Traditional stateful firewall
- 2.2.e Application visibility and control
- 2.2.f Web content filtering
- 2.2.g Email content filtering

2.3 Describe the impact of these technologies on data visibility

- 2.3.a Access control list
- 2.3.b NAT/PAT
- 2.3.c Tunneling
- 2.3.d TOR
- 2.3.e Encryption
- 2.3.f P2P
- 2.3.g Encapsulation
- 2.3.h Load balancing

2.4 Describe the uses of these data types in security monitoring

- 2.4.a Full packet capture
- 2.4.b Session data
- 2.4.c Transaction data
- 2.4.d Statistical data
- 2.4.e Metadata
- 2.4.f Alert data

2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting

2.7 Describe social engineering attacks (manual and generative AI)

2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

2.11 Identify the certificate components in a given scenario

- 2.11.a Cipher-suite
- 2.11.b X.509 certificates
- 2.11.c Key exchange
- 2.11.d Protocol version
- 2.11.e PKCS

3.0 Host-Based Analysis - 20%

3.1 Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures, and predictive AI

- 3.1.a Host-based intrusion detection
- 3.1.b Antimalware and antivirus
- 3.1.c Host-based firewall

3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

3.3 Describe the role of attribution in an investigation

- 3.3.a Assets
- 3.3.b Threat actor
- 3.3.c Indicators of compromise
- 3.3.d Indicators of attack
- 3.3.e Chain of custody

3.4 Identify type of evidence used based on provided logs

- 3.4.a Best evidence
- 3.4.b Corroborative evidence
- 3.4.c Indirect evidence

3.5 Interpret operating system, SIEM, SOAR platform, application, or command line logs to identify an event

3.6 Interpret the output report of malware analysis tools such as a detonation chamber or sandbox

- **3.7.a Hashes**
- **3.7.b URLs**
- **3.7.c Systems, events, and networking**

4.0 Network Intrusion Analysis -20%

4.1 Map the provided events to source technologies

- 4.1.a IDS/IPS
- 4.1.b Firewall
- 4.1.c Network application control
- 4.1.d Proxy logs
- 4.1.e Antivirus
- 4.1.f Transaction data (NetFlow)

4.2 Compare impact and no impact for these items

- 4.2.a False positive
- 4.2.b False negative
- 4.2.c True positive
- 4.2.d True negative
- 4.2.e Benign

4.3 Compare deep packet inspection with packet filtering and stateful firewall operation

4.4 Compare inline traffic interrogation and taps or traffic monitoring

4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic

4.6 Extract files from a TCP stream when given a PCAP file and Wireshark

4.7 Identify key elements in an intrusion from a given PCAP file

- 4.7.a Source address
- 4.7.b Destination address
- 4.7.c Source port
- 4.7.d Destination port
- 4.7.e Protocols
- 4.7.f Payloads

4.8 Interpret the fields in protocol headers as related to intrusion analysis

- 4.8.a Ethernet frame
- 4.8.b IPv4
- 4.8.c IPv6
- 4.8.d TCP
- 4.8.e UDP
- 4.8.f ICMP
- 4.8.g DNS
- 4.8.h SMTP/POP3/IMAP
- 4.8.i HTTP/HTTPS/HTTP2
- 4.8.j ARP

4.9 Interpret common artifact elements from an event to identify an alert

- 4.9.a IP address (source / destination)
- 4.9.b Client and server port identity
- 4.9.c Process (file or registry)
- 4.9.d System (API calls)
- 4.9.e Hashes
- 4.9.f URI / URL

4.10 Interpret basic regular expressions

5.0 Security Policies and Procedures - 15%

5.1 Describe management concepts

- 5.1.a Asset management
- 5.1.b Configuration management
- 5.1.c Mobile device management
- 5.1.d Patch management
- 5.1.e Vulnerability management

5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61

5.3 Apply the incident handling process such as NIST.SP800-61 to an event

5.4 Map elements to these steps of analysis based on the NIST.SP800-61

- 5.4.a Preparation
- 5.4.b Detection and analysis
- 5.4.c Containment, eradication, and recovery
- 5.4.d Post-incident analysis (lessons learned)

5.5 Map the organization stakeholders against the NIST IR categories (CMMC,NIST.SP800- 61)

- 5.5.a Preparation
- 5.5.b Detection and analysis
- 5.5.c Containment, eradication, and recovery
- 5.5.d Post-incident analysis (lessons learned)

5.6 Describe concepts as documented in NIST.SP800-86

- 5.6.a Evidence collection order
- 5.6.b Data integrity
- 5.6.c Data preservation
- 5.6.d Volatile data collection

5.7 Identify these elements used for network profiling

- 5.7.a Total throughput
- 5.7.b Session duration
- 5.7.c Ports used
- 5.7.d Critical asset address space

5.8 Identify these elements used for server profiling

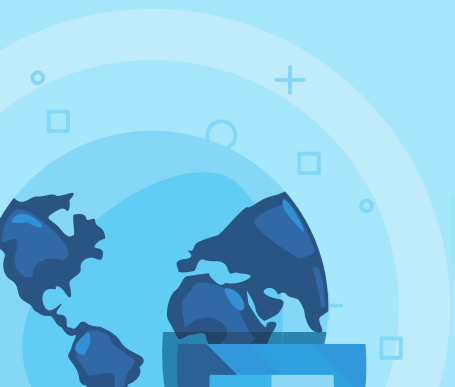
- 5.8.a Listening ports
- 5.8.b Logged in users/service accounts
- 5.8.c Running processes
- 5.8.d Running tasks
- 5.8.e Applications

5.9 Identify protected data in a network

- 5.9.a PII
- 5.9.b PSI
- 5.9.c PHI
- 5.9.d Intellectual property

5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)



CCIE HUB

CONTACT US

+91-9650272078, +91-8700479492

info@cciehub.in

www.cciehub.in

C 33 & 34, Sector 2, Noida, Gautam Buddha Nagar, Uttar Pradesh 201301