Implementing Cisco Cybersecurity Operations (210-255)

Exam Description: The Implementing Cisco Cybersecurity Operations exam (210-255 SECOPS) is a 90-minute, 60-70 question assessment. This exam is the second of the two required exams to achieve the Cisco Certified CyberOps Associate certification (formerly called CCNA Cyber Ops). This program aligns with the job role of an associate-level Security Operations Center (SOC) Security Analyst. The SECOPS exam tests a candidate's knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a SOC.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

15% 1.0 Endpoint Threat Analysis and Computer Forensics

1.1 Interpret the output report of a malware analysis tool such as AMP Threat Grid and Cuckoo Sandbox

1.2 Describe these terms as they are defined in the CVSS 3.0:
1.2.a Attack vector
1.2.b Attack complexity
1.2.c Privileges required
1.2.d User interaction
1.2.e Scope

1.3 Describe these terms as they are defined in the CVSS 3.0
1.3.a Confidentiality
1.3.b Integrity
1.3.c Availability

1.4 Define these items as they pertain to the Microsoft Windows file system
1.4.a FAT32
1.4.b NTFS
1.4.c Alternative data streams
1.4.d MACE
1.4.e EFI
1.4.f Free space
1.4.g Timestamps on a file system

1.5 Define these terms as they pertain to the Linux file system
1.5.a EXT4
1.5.b Journaling

- 1.5.c MBR
- 1.5.d Swap file system
- 1.5.e MAC

1.6 Compare and contrast three types of evidence

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

1.7 Compare and contrast two types of image

- 1.7.a Altered disk image
- 1.7.b Unaltered disk image

1.8 Describe the role of attribution in an investigation

- 1.8.a Assets
- 1.8.b Threat actor

22% 2.0 Network Intrusion Analysis

2.1 Interpret basic regular expressions

2.2 Describe the fields in these protocol headers as they relate to intrusion analysis:

- 2.2.a Ethernet frame
- 2.2.b IPv4
- 2.2.c IPv6
- 2.2.d TCP
- 2.2.e UDP
- 2.2.f ICMP
- 2.2.g HTTP

2.3 Identify the elements from a NetFlow v5 record from a security event

2.4 Identify these key elements in an intrusion from a given PCAP file

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

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

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

- 2.6.a IP address (source / destination)
- 2.6.b Client and Server Port Identity
- 2.6.c Process (file or registry)
- 2.6.d System (API calls)
- 2.6.e Hashes

2.6.f URI / URL

2.7 Map the provided events to these source technologies
2.7.a NetFlow
2.7.b IDS / IPS
2.7.c Firewall
2.7.d Network application control
2.7.e Proxy logs
2.7.f Antivirus

2.8 Compare and contrast impact and no impact for these items
2.8.a False Positive
2.8.b False Negative
2.8.c True Positive
2.8.d True Negative

2.9 Interpret a provided intrusion event and host profile to calculate the impact flag generated by Firepower Management Center (FMC)

18% 3.0 Incident Response

3.1 Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2

3.2 Map elements to these steps of analysis based on the NIST.SP800-61 r2
3.2.a Preparation
3.2.b Detection and analysis
3.2.c Containment, eradication, and recovery
3.2.d Post-incident analysis (lessons learned)

3.3 Map the organization stakeholders against the NIST IR categories (C2M2, NIST.SP800-61 r2)
3.3.a Preparation
3.3.b Detection and analysis
3.3.c Containment, eradication, and recovery
3.3.d Post-incident analysis (lessons learned)

3.4 Describe the goals of the given CSIRT
3.4.a Internal CSIRT
3.4.b National CSIRT
3.4.c Coordination centers
3.4.d Analysis centers
3.4.e Vendor teams
3.4.f Incident response providers (MSSP)

3.5 Identify these elements used for network profiling
3.5.a Total throughput
3.5.b Session duration

3.5.c Ports used
3.5.d Critical asset address space

3.6 Identify these elements used for server profiling
3.6.a Listening ports
3.6.b Logged in users/service accounts
3.6.c Running processes
3.6.d Running tasks
3.6.e Applications

3.7 Map data types to these compliance frameworks
3.7.a PCI
3.7.b HIPPA (Health Insurance Portability and Accountability Act)
3.7.c SOX

3.8 Identify data elements that must be protected with regards to a specific standard (PCI-DSS)

23% 4.0 Data and Event Analysis

4.1 Describe the process of data normalization
4.2 Interpret common data values into a universal format
4.3 Describe 5-tuple correlation
4.4 Describe the 5-tuple approach to isolate a compromised host in a grouped set of logs
4.5 Describe the retrospective analysis method to find a malicious file, provided file analysis report
4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains
4.7 Map DNS logs and HTTP logs together to find a threat actor
4.8 Map DNS, HTTP, and threat intelligence data together
4.9 Identify a correlation rule to distinguish the most significant alert from a given set of events from multiple data sources using the firepower management console
4.10 Compare and contrast deterministic and probabilistic analysis

22% 5.0 Incident Handling

5.1 Classify intrusion events into these categories as defined by the Cyber Kill Chain Model
5.1.a Reconnaissance
5.1.b Weaponization
5.1.c Delivery
5.1.d Exploitation
5.1.e Installation
5.1.f Command and control
5.1.g Action on objectives

5.2 Apply the NIST.SP800-61 r2 incident handling process to an event

5.3 Define these activities as they relate to incident handling
5.3.a Identification
5.3.b Scoping

5.3.c Containment
5.3.d Remediation
5.3.e Lesson-based hardening
5.3.f Reporting

5.4 Describe these concepts as they are documented in NIST SP800-86

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

5.5 Apply the VERIS schema categories to a given incident