Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (300-215)

Exam Description: Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (CBRFIR 300-215) is a 90-minute exam that is associated with the Cisco CyberOps Professional Certification. This exam tests a candidate's knowledge of forensic analysis and incident response fundamentals, techniques, and processes. The course Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps helps candidates to prepare for this exam.

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. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20% 1.0 Fundamentals

1.1 Analyze the components needed for a root cause analysis report

1.2 Describe the process of performing forensics analysis of infrastructure network devices

1.3 Describe antiforensic tactics, techniques, and procedures

1.4 Recognize encoding and obfuscation techniques (such as, base 64 and hex encoding)

1.5 Describe the use and characteristics of YARA rules (basics) for malware identification, classification, and documentation

1.6 Describe the role of:

1.6.a hex editors (HxD, Hiew, and Hexfiend) in DFIR investigations

1.6.b disassemblers and debuggers (such as, Ghidra, Radare, and Evans Debugger) to perform basic malware analysis

1.6.c deobfuscation tools (such as, XORBruteForces, xortool, and unpacker)

1.7 Describe the issues related to gathering evidence from virtualized environments (major cloud vendors)

20% 2.0 Forensics Techniques

2.1 Recognize the methods identified in the MITRE attack framework to perform fileless malware analysis

2.2 Determine the files needed and their location on the host

2.3 Evaluate output(s) to identify IOC on a host

2.3.a process analysis

2.3.b log analysis

2.4 Determine the type of code based on a provided snippet

2.5 Construct Python, PowerShell, and Bash scripts to parse and search logs or multiple data sources (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid)

2.6 Recognize purpose, use, and functionality of libraries and tools (such as, Volatility, Systernals, SIFT tools, and TCPdump)

30% 3.0 Incident Response Techniques

3.1 Interpret alert logs (such as, IDS/IPS and syslogs)

3.2 Determine data to correlate based on incident type (host-based and network-based activities)

3.3 Determine attack vectors or attack surface and recommend mitigation in a given scenario

3.4 Recommend actions based on post-incident analysis

3.5 Recommend mitigation techniques for evaluated alerts from firewalls, intrusion prevention systems (IPS), data analysis tools (such as, Cisco Umbrella Investigate, Cisco Stealthwatch, and Cisco SecureX), and other systems to responds to cyber incidents

3.6 Recommend a response to 0 day exploitations (vulnerability management)

3.7 Recommend a response based on intelligence artifacts

3.8 Recommend the Cisco security solution for detection and prevention, given a scenario

3.9 Interpret threat intelligence data to determine IOC and IOA (internal and external sources)

3.10 Evaluate artifacts from threat intelligence to determine the threat actor profile

3.11 Describe capabilities of Cisco security solutions related to threat intelligence (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, and AMP for Network)

15% 4.0 Forensics Processes

4.1 Describe antiforensic techniques (such as, debugging, Geo location, and obfuscation)

4.2 Analyze logs from modern web applications and servers (Apache and NGINX)

4.3 Analyze network traffic associated with malicious activities using network monitoring tools (such as, NetFlow and display filtering in Wireshark)

4.4 Recommend next step(s) in the process of evaluating files based on distinguished characteristics of files in a given scenario

4.5 Interpret binaries using objdump and other CLI tools (such as, Linux, Python, and Bash)

15% 5.0 Incident Response Processes

5.1 Describe the goals of incident response

5.2 Evaluate elements required in an incident response playbook

5.3 Evaluate the relevant components from the ThreatGrid report

5.4 Recommend next step(s) in the process of evaluating files from endpoints and performing ad-hoc scans in a given scenario

5.5 Analyze threat intelligence provided in different formats (such as, STIX and TAXII)