Conducting Forensic Analysis and Incident Response Using Cisco Technologies for Cybersecurity v1.2 (300-215)

Exam Description: Conducting Forensic Analysis and Incident Response Using Cisco Technologies for Cybersecurity v1.2 (CBRFIR 300-215) is a 90-minute exam that is associated with the CCNP Cybersecurity Certification. This exam certifies 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 Cybersecurity 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, hex encoding, polymorphic and metamorphic coding
- 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
  - 1.6.d Memory forensics tools
- 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 SIEM, malware analysis, and other tools output(s) to identify IOC on a host
  - 2.3.a Process analysis
  - 2.3.b Log analysis including cloud-native application logs
  - 2.3.c Network traffic analysis for anomaly detection
- 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, Cisco Secure Endpoint, Cisco Secure Network Analytics, 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 SIEM, 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
	3.4	Recommend actions based on post-incident analysis
	3.5	Recommend mitigation techniques for evaluated alerts from firewalls, SIEM, SOAR platforms, intrusion prevention systems (IPS), data analysis tools such as Cisco Umbrella, Cisco Secure Network Analytics, and Cisco XDR), and other systems to respond to cyber incidents
	3.6	Recommend response to 0 day exploitations such as risk assessment and exploitation prediction, SIEM data collection and processing in AI-based predictive vulnerability management
	3.7	Recommend a response based on intelligence artifacts
	3.8	Recommend the Cisco security solution for detection and prevention
	3.9	Interpret threat intelligence feeds to determine IOCs and IOAs from 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, Firepower, Cisco Secure Endpoint, and Cisco Secure Network Analytics
15%	**4.0**	**Forensics Processes**
	4.1	Describe antiforensic techniques such as Geo location, obfuscation, evading detection, data destruction, and hindering forensics
	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
	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
	5.5	Analyze threat intelligence provided in different formats such as STIX and TAXII