Performing CyberOps Using Cisco Security Technologies v1.1 (350-201)

Exam Description: Performing CyberOps Using Cisco Security Technologies v1.1 (CBRCOR 350-201) is a 120-minute exam that is associated with the Cisco CyberOps Professional Certification. This exam certifies a candidate's knowledge of core cybersecurity operations including cybersecurity fundamentals, techniques, processes, and automation. The course Performing CyberOps Using Cisco Security Technologies 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. Interpret the components within a playbook
2. Determine the tools needed based on a playbook scenario
3. Apply the playbook for a common scenario (for example, unauthorized elevation of privilege, DoS and DDoS, website defacement)
4. Infer the industry for various compliance standards (for example, PCI, FISMA, FedRAMP, SOC, SOX, PCI, GDPR, Data Privacy, and ISO 27101)
5. Describe the purpose of cyber risk insurance
6. Analyze elements of a risk analysis (combination asset, vulnerability, and threat)
7. Apply the incident response workflow
8. Describe characteristics and areas of improvement using common incident response metrics
9. Describe types of cloud environments
10. Compare security operations considerations of cloud platforms (for example, IaaS, PaaS)

30% 2.0 Techniques

1. Recommend data analytic techniques to meet specific needs or answer specific questions
2. Describe the use of hardening machine images for deployment
3. Describe the process of evaluating the security posture of an asset
4. Evaluate the security controls of an environment, diagnose gaps, and recommend improvement
5. Determine resources for industry standards and recommendations for hardening of systems
6. Determine patching recommendations, given a scenario
7. Recommend services to disable, given a scenario
8. Apply segmentation to a network
9. Utilize network controls for network hardening
10. Determine SecDevOps recommendations (implications)
11. Describe use and concepts related to using a Threat Intelligence Platform (TIP) to automate intelligence
12. Apply threat intelligence using tools

13. Apply the concepts of data loss, data leakage, data in motion, data in use, and data at rest based on common standards
14. Describe the different mechanisms to detect and enforce data loss prevention techniques
    - 14.a. endpoint-based
    - 14.b. network-based
    - 14.c. application-based
    - 14.d. cloud-based
15. Recommend tuning or adapting devices and software across rules, filters, and policies
16. Describe the concepts of security data management
17. Describe use and concepts of tools for security data analytics
18. Recommend workflow from the described issue through escalation and the automation needed for resolution
19. Apply dashboard data to communicate with technical, leadership, or executive stakeholders
20. Analyze anomalous user and entity behavior (UEBA)
21. Determine the next action based on user behavior alerts
22. Describe tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools)
23. Evaluate artifacts and streams in a packet capture file
24. Troubleshoot existing detection rules
25. Determine the tactics, techniques, and procedures (TTPs) from an attack

30% 3.0 Processes

1. Analyze components in a threat model
2. Determine the steps to investigate the common types of cases
3. Apply the concepts and sequence of steps in the malware analysis process:
    - a. Extract and identify samples for analysis (for example, from packet capture or packet analysis tools)
    - b. Perform reverse engineering
    - c. Perform dynamic malware analysis using a sandbox environment
    - d. Identify the need for additional static malware analysis
    - e. Perform static malware analysis
    - f. Summarize and share results
4. Interpret the sequence of events during an attack based on analysis of traffic patterns
5. Determine the steps to investigate potential endpoint intrusion across a variety of platform types (for example, desktop, laptop, IoT, mobile devices)
6. Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
7. Determine IOCs in a sandbox environment (includes generating complex indicators)
8. Determine the steps to investigate potential data loss from a variety of vectors of modality (for example, cloud, endpoint, server, databases, application)
9. Recommend the general mitigation steps to address vulnerability issues
10. Recommend the next steps for vulnerability triage and risk analysis using industry scoring systems (for example, CVSS) and other techniques

20%	**4.0**	**Automation**
	1.	Compare concepts, platforms, and mechanisms of orchestration and automation
	2.	Interpret basic scripts (for example, Python)
	3.	Modify a provided script to automate a security operations task
	4.	Recognize common data formats (for example, JSON, HTML, CSV, XML)
	5.	Determine opportunities for automation, orchestration, and machine learning
	6.	Determine the constraints when consuming APIs (for example, rate limited, timeouts, and payload)
	7.	Explain the common HTTP response codes associated with REST APIs
	8.	Evaluate the parts of an HTTP response (response code, headers, body)
	9.	Interpret API authentication mechanisms: basic, custom token, and API keys
	10.	Utilize Bash commands (file management, directory navigation, and environmental variables)
	11.	Describe components of a CI/CD pipeline
	12.	Apply the principles of DevOps practices
	13.	Describe the principles of Infrastructure as Code