Performing Cybersecurity Using Cisco Security Technologies v1.2 (350-201)

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

30%	**2.0**	**Techniques**
	2.1	Recommend AI-powered data analytic techniques to meet specific needs or answer specific questions
	2.2	Describe the use of hardening machine images for deployment
	2.3	Describe the process of evaluating the security posture of an asset
	2.4	Evaluate the security controls of an environment, diagnose gaps, and recommend improvement
	2.5	Determine resources for industry standards and recommendations for hardening of systems
	2.6	Determine patching recommendations, given a scenario
	2.7	Recommend services to disable, given a scenario
	2.8	Apply segmentation to a network
	2.9	Utilize network controls for network hardening
	2.10	Determine DevSecOps recommendations (implications)
	2.11	Describe use and concepts related to using a Threat Intelligence Platform (TIP) to automate intelligence

2.12   Apply AI-driven threat intelligence using tools

2.13   Apply the concepts of data loss, data leakage, data in motion, data in use, and data at rest based on common standards

2.14   Describe the different mechanisms to detect and enforce data loss prevention techniques
       2.14.a   Host
       2.14.b   Network
       2.14.c   Application
       2.14.d   Cloud

2.15   Recommend tuning or adapting devices and software across rules, filters, and policies

2.16   Describe the concepts of security data management

2.17   Describe use and concepts of SIEM tools for security data analytics

2.18   Recommend procedural and SOAR workflows from the described issue through escalation and the automation needed for resolution

2.19   Apply dashboard data to communicate with technical, leadership, or executive stakeholders

2.20   Analyze anomalous user and entity behavior (UEBA) using SIEM data

2.21   Determine the next action based on user behavior alerts

2.22   Describe tools and their limitations for network analysis such as packet capture tools, traffic analysis tools, network log analysis tools

2.23   Evaluate artifacts and streams in a packet capture file

2.24   Troubleshoot existing detection rules

2.25   Determine the tactics, techniques, and procedures (TTPs) from an attack

30%   3.0   Processes

3.1   Analyze components in a threat model

3.2   Determine the steps to investigate the common types of cases

3.3   Apply the concepts and sequence of steps in the malware analysis process:
       3.3.a   Extract and identify samples for analysis such as packet capture or packet analysis tools
       3.3.b   Perform reverse engineering
       3.3.c   Perform dynamic malware analysis using a sandbox environment
       3.3.d   Identify the need for additional static malware analysis
       3.3.e   Perform static malware analysis
       3.3.f   Summarize and share results

3.4   Interpret the sequence of events during an attack based on predictive AI analysis of traffic patterns

3.5   Determine the steps to investigate potential endpoint intrusion across a variety of platform types such as desktop, laptop, IoT, mobile devices

3.6   Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)

3.7   Determine IOCs in a sandbox environment (includes generating complex indicators)

2024 Cisco Systems, Inc. This document is Cisco Public.   Page 2

Cisco Confidential

3.8   Determine the steps to investigate potential data loss from a variety of vectors of modality such as cloud, endpoint, server, databases, application

3.9   Recommend the general mitigation steps to address vulnerability issues

3.10   Recommend the next steps for vulnerability triage and risk analysis using industry scoring systems such as CVSS and other techniques

20%   4.0   Automation

4.1   Compare concepts, platforms, and mechanisms of SOAR

4.2   Interpret basic scripts such as Python

4.3   Modify a provided script to automate a security operations task

4.4   Recognize common data formats such as JSON, HTML, CSV, XML

4.5   Determine opportunities for automation, orchestration, and machine learning within a SOAR platform

4.6   Determine the constraints when consuming APIs such as rate limited, timeouts, and payload

4.7   Explain the common HTTP response codes associated with REST APIs

4.8   Evaluate the parts of an HTTP response (response code, headers, body)

4.9   Interpret API authentication mechanisms: basic, custom token, and API keys

4.10   Utilize Bash commands (file management, directory navigation, and environmental variables)

4.11   Describe components of a CI/CD pipeline

4.12   Apply the principles of DevOps practices

4.13   Describe the principles of Infrastructure as Code