Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity v1.1 (300-220)

Exam Description: The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity v1.0 (CBRTHD 300-220) exam is a 90-minute exam that is associated with the CCNP Cybersecurity Certification. This exam certifies a candidate's knowledge for conducting threat hunting and defending including threat modeling techniques, threat actor attribution techniques, threat hunting techniques, threat hunting processes, and threat hunting outcomes. The course, Conducting Threat Hunting and Defending 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 Threat Hunting Fundamentals

1.1 Apply the Threat Hunting Maturity Model to an organization's environment, as it relates to the Pyramid of Pain

1.2 Describe threats and how to model them with standards such as MITRE ATT&CK, MITRE CAPEC, TaHiTI, and PASTA

1.3 Describe the limiting factors of detection tools for malware behavior, propagation, and detection

1.4 Describe the advantages and disadvantages of automation such as artificial intelligence and machine learning in the operation of a SOC

1.5 Determine differences in tactics, techniques, and procedures of an advanced persistent threat and threat actor using logs

1.6 Interpret a threat intelligence report and draw conclusions about a threat actor (known advanced persistent threat/commodity human-driven/commodity machine-driven)

1.6.a tactics

1.6.b techniques

1.6.c procedures

10% 2.0 Threat Modeling Techniques

2.1 Select the threat modeling approach for a given scenario

2.2 Use MITRE ATT&CK to model threats (tactics, techniques, and procedures or changes in tactics, techniques, and procedures)

2.3 Describe the uses of structured and unstructured threat hunting

2.4 Determine the priority level of attacks based on the Cyber Kill Chain and MITRE ATT&CK

2.5 Determine the priority level of attacks based on the MITRE CAPEC model

2.6 Perform threat intelligence handling: gathering, cataloging, utilizing, and removing 2022 Cisco Systems, Inc. This document is Cisco Public. Page 2

Cisco Confidential

20% 3.0 Threat Actor Attribution Techniques

3.1 Determine attack tactics, techniques, and procedures using logs

3.2 Interpret tactics, techniques and procedures of a given threat actor

3.3 Select the delivery method, payload, tactic, or timeline that indicates an authorized assessment or an attack (threat actor or penetration tester)

3.4 Determine usable artifacts for detection of advanced persistent threat actors at all levels of the Pyramid of Pain

3.4.a tactics

3.4.b techniques

3.4.c procedures

20% 4.0 Threat Hunting Techniques

4.1 Use scripting languages such as Python and PowerShell to augment detection or analytics

4.2 Perform a cloud-native threat hunt

4.3 Determine undetected threats using SIEM data and endpoint artifacts

4.4 Determine the C2 communications to and from infected hosts using endpoint applications, processes, and logs

4.5 Select suspicious activity using session and protocol data

4.6 Determine the stage of infection within C2 communications using traffic data

4.7 Select weakness in code using code-level analysis tools such as PE Checker, BURP Suite, and SEM Grep

4.8 Describe the analysis process for applications and operating systems used by IoT devices

4.9 Describe memory-resident attacks and how to perform analysis using memory-specific tools such as volatility

4.10 Construct a signature for detection or analysis

4.11 Recognize the likelihood of attack by an attack vector within a given environment

20% 5.0 Threat Hunting Processes

5.1 Describe the process to identify memory-resident attacks

5.2 Determine compromises by reverse engineering

5.3 Determine known and unknown gaps in detection

5.3.a vulnerabilities

5.3.b configuration errors

5.3.c threats

5.4 Interpret data from memory-specific tools

5.5 Construct a runbook or playbook to address a detectable scenario

5.6 Recommend tools, configurations, detection, and deception techniques for a given scenario

5.7 Recommend attack remediation strategies based on the results of a threat assessment

5.8 Recommend changes to improve the effectiveness and efficiency of a threat hunt

5.9 Recommend security countermeasures and mitigations for identified risks

10% 6.0 Threat Hunting Outcomes

6.1 Describe how multiproduct integration enhances data visibility within a product and accelerates analysis

6.2 Diagnose analytical gaps using threat hunting methodologies

6.3 Recommend a mitigation strategy to block C2 traffic

6.4 Recommend changes in hunt capability to advance to the next Threat Hunting Maturity Model phase

6.5 Recommend changes to a detection methodology to augment analytical and process gaps

6.6 Use presentation resources to convey findings and direct environmental change