Security Onion Certified Professional (SOCP)

version 430 Exam Blueprint

1. Design and Architecture – Approximately 24% of the questions (12)

This domain has been designed to assess the proficiency of administrators tasked with designing and installing a Security Onion 2.4 grid. It focuses on their ability to select the most appropriate Security Onion node(s) and deployment mode(s) based on different scenarios. The topics also include comprehending the purpose and functionality of different node types, recommended minimum hardware requirements, and the applications and services each node type employs. The following is a comprehensive breakdown of the subject areas assessed in this domain:

1.1. Explain the different deployment modes and node types and the role of each node
- 1.1.1. Import
- 1.1.2. Evaluation
- 1.1.3. Standalone
- 1.1.4. Distributed
- 1.1.5. Manager
- 1.1.6. Search
- 1.1.7. Forward

1.2. Identify the core components and their functionality within the following Security Onion nodes
- 1.2.1. Manager
- 1.2.2. Search
- 1.2.3. Forward
- 1.2.4. Receiver
- 1.2.5. Intrusion Detection Honeypot (IDH)

1.3. Describe the function of the following components
- 1.3.1. Elasticsearch
- 1.3.2. Elastic Agent
- 1.3.3. Logstash
- 1.3.4. Redis
- 1.3.5. Strelka
- 1.3.6. Stenographer
- 1.3.7. Suricata
- 1.3.8. Zeek

1.4. Determine the minimum hardware requirements of the following Security Onion nodes
- 1.4.1. Standalone
- 1.4.2. Manager
- 1.4.3. Search
- 1.4.4. Forward

2. Grid Management – Approximately 16% of the questions. (8)

This domain is designed to evaluate the proficiency of administrators in managing and maintaining a Security Onion 2.4 grid. The topics covered in this section include but are not limited to user management, firewall management, and key components of SaltStack, as well as configuring several core components of the Security Onion nodes. The following is a comprehensive breakdown of the subject areas that will be assessed in this domain:

2.1. Describe the following components of SaltStack and their functionality within a Security Onion 2.4 Grid
  2.1.1. Salt Masters
  2.1.2. Salt Minions
  2.1.3. Salt states
  2.1.4. Salt configuration files
2.2. Describe Role Base Access Control and explain how to assign, modify, and remove roles assigned to SOC user accounts
2.3. Explain how to add, disable, update, and remove SOC user accounts using the Users Administration interface
2.4. Explain how to add, disable, update, and remove SOC user accounts using the so-users command-line utility
2.5. Describe Multi-factor Authentication (MFA) and explain how to enable, modify, and disable MFA for SOC user accounts
2.6. Describe how to add and remove single IP address or subnets from the iptables firewall for the following roles using the Grid Configuration interface
  2.6.1. Analyst Web access to the SOC
  2.6.2. Elastic Agent Endpoints
  2.6.3. Security Onion Search Nodes
  2.6.4. Security Onion Forward/Sensor Nodes
2.7. Explain the process of adding and removing nodes from the Security Onion grid using the Grid Members interface in SOC

3. Grid Monitoring and Troubleshooting – Approximately 20% of the questions. (10)

This domain assesses the proficiency of the candidates in identifying potential issues in a Security Onion 2.4 grid. The assessment covers various topics such as navigating the Grid and InfluxDB interfaces, explaining the purpose and functionality of tools such as Telegraph and InfluxDB, building a custom dashboard, configuring notification endpoints and rules, and configuring check/alerts within InfluxDB. The assessment comprehensively evaluates the candidates' knowledge and skills in these subject areas. The following is a comprehensive breakdown of the subject areas that will be assessed in this domain:

3.1. Identify the different metrics available in the SOC Grid interface
3.2. Explain how to collect additional node metrics by pivoting from a node within the SOC Grid interface to InfluxDB
3.3. Describe how to upload PCAP and EVTX files for analysis using the SOC Grid interface
3.4. Explain the purpose of Telegraph in Security Onion 2.4
3.5. Explain the concept of buckets in InfluxDB
3.6. Describe how to perform the following tasks in InfluxDB
    3.6.1. Creating custom dashboards
    3.6.2. Adding custom cells to a dashboard
    3.6.3. Copying or moving cells between dashboards
    3.6.4. Enabling, disabling, and modifying pre-built checks
    3.6.5. Managing notation policies
    3.6.6. Manage notification rules
3.7. Determine the proper location on application logs on Security Onion nodes
3.8. Explain the tail and grep command-line tools and their use when analyzing log files

4. Grid Tuning – Approximately 20% of the questions. (10)

This domain is designed to evaluate the proficiency of the candidates in undertaking essential tasks necessary for the efficient functioning of the Security Onion 2.4 sensor grid. The topics covered in this section include, but are not limited to, Berkeley Packet Filters, addition of CPU cores or workers, allocation of applications to specific CPU cores, adjustment of Redis memory allotment, fine-tuning of Logstash pipeline batch size and workers, and refinement of Network Intrusion Detection System (NIDS) rules. The following is a comprehensive breakdown of the subject areas that will be assessed in this domain:

4.1. Explain the function of Berkeley Packet Filters (BPFs) and identify the correct BPF syntax
4.2. Describe how BPFs are implemented in Security Onion 2.4
4.3. Explain the following tuning consideration for Zeek
    4.3.1. Purpose of Zeek workers (lb_procs)
    4.3.2. How to determine the correct number of Zeek workers based on the volume of analyzed network traffic
    4.3.3. How to configure the number of workers on a specific node
    4.3.4. How to enable and disable Zeek scripts on a single node or globally on every node running Zeek
    4.3.5. How to configure CPU affinity for Zeek on a single node
4.4. Explain the following tuning consideration for Suricata
    4.4.1. Purpose of Suricata workers (threads)
    4.4.2. How to determine the correct number of Suricata workers based on the volume of analyzed network traffic
    4.4.3. How to configure the number of workers on a specific node
    4.4.4. How to configure CPU affinity for Suricata on a single node
4.5. Explain Logstash batch size and worker threads and the effects they have on the data pipeline
4.6. Describe how to modify the amount of system memory Redis uses to store events as they pass through the data pipeline
4.7. Describe Elasticsearch data streams and how events are written to (indexed) and collected (queried) from data streams
4.8. Describe how Elasticsearch Index Lifecycle Management (IML) are used to manage Elasticsearch data streams
4.9. Describe the process of adding custom queries to the Hunt and Dashboards interfaces in the SOC
    4.9.1. Describe how to modify the preset category values for the Cases interface
    4.9.2. Explain how to configure automatic observable extraction when an event is escalated to a case

5. Analyst Tools – Approximately 20% of the questions. (10)

This domain is centered around assessing the proficiency of candidates in the tools and techniques necessary to effectively investigate alerts and track down potential adversaries using Security Onion 2.4. The section encompasses a variety of topics, including but not limited to the effective use of the available applications and tools on Security Onion 2.4, as well as the appropriate process of acknowledging and escalating events in the Alerts interface. The following is a breakdown of the testable subject areas:

5.1. Describe the following Case management tasks
- 5.1.1. Attaching new events to a case
- 5.1.2. Adding Attachments and Observables
- 5.1.3. Setting values such as assignee, status, Traffic Light Protocol (TLP), and Permissible Action Protocol (PAP)

5.2. Describe the process of creating one or more data tables or visualizations in the Group Metrics section of the Hunt and Dashboards interface

5.3. Explain the following options in the SOC context menu
- 5.3.1. Include
- 5.3.2. Exclude
- 5.3.3. Only
- 5.3.4. Group by
- 5.3.5. New Group by
- 5.3.6. Correlate