Security Onion

CERTIFIED PROFESSIONAL

(SOCP)

**Exam Blueprint**

Security Onion Certified Professional (SOCP)

Version 3.2

| | |
|---|---|
| **Certification** | Security Onion Certified Professional |
| **Exam Version** | 3.2 |
| **Target Platform** | Security Onion 3 |
| **Time** | 120 Minutes |
| **Total Questions** | 50 |

## About This Exam

The Security Onion Certified Professional (SOCP) exam validates an administrator's ability to design, deploy, manage, monitor, and tune a Security Onion 3 grid, as well as to use the analyst tools required to investigate alerts and hunt for adversaries. This blueprint outlines the domains, weightings, and objectives that define the scope of the exam.

## Domain Weighting

| # | Domain | Weight | Questions |
|---|---|---|---|
| 1 | Design and Architecture | 32% | ~16 |
| 2 | Grid Management | 20% | ~10 |
| 3 | Grid Monitoring and Troubleshooting | 10% | ~5 |
| 4 | Grid Tuning | 16% | ~8 |
| 5 | Analyst Tools | 14% | ~7 |
| 6 | Security Onion Pro | 8% | ~4 |

*Weightings are approximate and indicate the relative emphasis of each domain on the exam.*

## DOMAIN 1

## Design and Architecture

Weighting: 32% • Approx. 16 questions

> *Focuses on the knowledge required to design and install a Security Onion 3 grid. Candidates must choose the correct deployment mode and appropriate node(s) for a given scenario, and understand the purpose, hardware requirements, and services of each node type and core component.*

### 1.1. Explain the deployment modes and node types and the role of each

- Import
- Evaluation
- Standalone
- Distributed
- Manager
- Search
- Sensor

### 1.2. Identify the core components and their functionality within each node

- Manager
- Search
- Sensor
- Receiver
- Intrusion Detection Honeypot (IDH)

### 1.3. Describe the function of the following components

- Elasticsearch
- Elastic Agent
- Logstash
- Redis
- Strelka
- Suricata
- Zeek

### 1.4. Determine the minimum hardware requirements of the following nodes

- Standalone
- Manager
- Search
- Sensor

## DOMAIN 2
## Grid Management
Weighting: 20% • Approx. 10 questions

> *Focuses on administering and maintaining a Security Onion 3 grid, including user management, firewall management, the key components of SaltStack, and configuration of core components across the various node types.*

**2.1. Describe the components of SaltStack and their functionality in the grid**

- Salt Masters
- Salt Minions

**2.2. Describe Role-Based Access Control (RBAC) and how to assign, modify, and remove roles for 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-user command-line utility**

**2.5. Describe Multi-Factor Authentication (MFA) and how to enable, modify, and disable MFA for SOC user accounts**

**2.6. Describe how to add and remove single IP addresses or subnets from the host firewall for the following roles using the Grid Configuration interface**

- Analyst web access to the SOC
- Elastic Agent endpoints
- Security Onion search nodes
- Security Onion sensor nodes

**2.7. Explain the process of adding and removing nodes from the grid using the Grid Members interface in SOC**

## DOMAIN 3

## Grid Monitoring and Troubleshooting

Weighting: 10% • Approx. 5 questions

> *Focuses on identifying potential issues in a Security Onion 3 grid, including navigating the Grid and InfluxDB interfaces, understanding monitoring tools such as Telegraf and InfluxDB, building custom dashboards, configuring notification endpoints and rules, and configuring checks and alerts.*

**3.1. Identify the different metrics available in the SOC Grid interface**

**3.2. Determine the proper location of application logs on Security Onion nodes**

**3.3. Explain the tail and grep command-line tools and their use when analyzing log files**

## DOMAIN 4
## Grid Tuning
Weighting: 16% • Approx. 8 questions

> *Focuses on the tasks required to keep a grid running efficiently, including Berkeley Packet Filters, adding CPU cores or workers, pinning applications to specific cores, adjusting Redis memory, tuning the Logstash pipeline, and tuning NIDS rules.*

**4.1. Explain the function of Berkeley Packet Filters (BPFs) and identify correct BPF syntax**

**4.2. Describe how BPFs are implemented in Security Onion 3**

**4.3. Explain the following tuning considerations for Zeek**

- Purpose of Zeek workers (lb_procs)
- Determining the correct number of workers based on traffic volume
- Configuring the number of workers on a specific node
- Enabling and disabling Zeek scripts on a single node or globally
- Configuring CPU affinity for Zeek on a single node

**4.4. Explain the following tuning considerations for Suricata**

- Purpose of Suricata workers (threads)
- Determining the correct number of workers based on traffic volume
- Configuring the number of workers on a specific node
- Configuring CPU affinity for Suricata on a single node

**4.5. Explain Logstash batch size and worker threads and their effects on the data pipeline**

**4.6. Describe how to modify the amount of system memory Redis uses to store events in the data pipeline**

**4.7. Describe Elasticsearch data streams and how events are indexed and queried**

**4.8. Describe how Index Lifecycle Management (ILM) and Data Stream Lifecycles manage Elasticsearch data streams and indices**

**4.9. Describe SOC customization tasks**

- Adding custom queries to the Hunt and Dashboards interfaces
- Modifying the preset category values for the Cases interface

- Configuring automatic observable extraction when an event is escalated to a case

## DOMAIN 5
## Analyst Tools
Weighting: 14% • Approx. 7 questions

> *Focuses on the tools and techniques analysts use to investigate alerts and hunt for adversaries in Security Onion, including case management and acknowledging and escalating events in the Alerts interface.*

**5.1. Describe the following case management tasks**

- Attaching new events to a case
- Adding attachments and observables
- Setting values such as assignee, status, Traffic Light Protocol (TLP), and Permissible Actions 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 interfaces**

**5.3. Explain the following options in the SOC context menu**

- Include
- Exclude
- Only
- Group By
- New Group By
- Correlate

## DOMAIN 6

## Security Onion Pro

Weighting: 8% • Approx. 4 questions

> *Focuses on the feature set available with Security Onion Pro, including single sign-on (SSO) via OpenID Connect (OIDC), enterprise compliance features, guaranteed message delivery via Kafka, and the use cases for the Security Onion API.*

### 6.1. Identify the supported Single Sign-On (SSO) authentication providers

### 6.2. Explain the following compliance features

- Linux Unified Key Setup (LUKS)
- Security Technical Implementation Guides (STIG)
- Federal Information Processing Standards (FIPS)

### 6.3. Explain how to implement outbound notifications in Security Onion

### 6.4. Explain how Kafka provides guaranteed message delivery in the data pipeline

- Identify which applications on which nodes are replaced when Kafka is implemented
- Explain the responsibilities of Kafka controllers and brokers

### 6.5. Describe the functionality and components of the Security Onion API

### 6.6. Explain the following concepts when implementing Manager of Managers (MoM)

- Requirements
- Data isolation
- Subgrid outages