



## Sourcefire 3D™ System Certification Study Guide

Candidates that successfully complete the requirements of the Sourcefire 3D System certification have distinguished themselves as having in-depth and thorough knowledge of Sourcefire products and their underlying technical concepts.

This exam consists of 100 random questions with a 3 hour time limit. Each student is guaranteed 2 attempts within the 60 day subscription period to pass the exam. After successfully passing the exam, certificates are available within 48 hours of achieving a score of 70% or better. An email with detailed instructions will be sent to the student for receiving a passing grade.

The proficiencies assessed in this certification program are as follows:

### IDS/IPS & RNA Technology:

- ▶ Understand what is meant by the term “Correlation”
- ▶ Know basic security principals and attack techniques
- ▶ Understand the various IDS/IPS evasion techniques
- ▶ Be familiar with the basics of TCP/IP network protocols
- ▶ Understand Impact and what data is required to calculate it
- ▶ Be familiar with the Sourcefire Intrusion Sensor, Sourcefire RNA and Sourcefire Defense Center architectural components

### System Settings, Policy & Health Monitoring:

- ▶ Understand the functionality of the Access List configuration
- ▶ Know the effect certain settings may have on the performance of the Defense Center
- ▶ In general, be familiar with the various Defense Center/Intrusion Sensor/RNA system policy settings
- ▶ Know the various options for managing time synchronization between Sourcefire 3D System devices
- ▶ Be able to define what is meant by a System Policy
- ▶ Understand the various options for database management for the various Sourcefire 3D System components
- ▶ Know the types of policies available on the Sourcefire 3D System and what each one does
- ▶ Be familiar with how the various health policy color codes help administrators determine the health state of the installation at-a-glance

**Sensor Management:**

- ▶ Know the communications architecture between the Defense Center and sensors and their associated settings
- ▶ Understand how licenses are applied to the various components of the Sourcefire 3D System
- ▶ Be familiar with the process of mounting sensors to the Defense Center
- ▶ Understand the various detection modes and how they relate to sensor deployments
- ▶ Understand the implications of remotely resetting components and which processes can be remotely reset through the Sourcefire 3D System interface
- ▶ Understand the concept of detection resources and how it relates to interface sets and sensor deployment options
- ▶ Be familiar with the in-line vs. passive Intrusion Sensor deployments
- ▶ Know the configuration options specific to in-line Intrusion Sensor deployments

**Administration & Maintenance:**

- ▶ Know how the backup & restore features work and the various options you can exercise relative to this functionality
- ▶ Be familiar with the various options for setting user preferences
- ▶ Understand the concept of Workflows
- ▶ Understand how user preference settings relate to user accounts
- ▶ Understand how rules are updated and system upgrades/patches are applied
- ▶ Know the features and functionality of the Audit and Syslog systems
- ▶ Be familiar with the system statistics information and which statistics are monitored
- ▶ Understand the capabilities of the Task Scheduling feature and the sequences in which certain tasks must be performed
- ▶ Know how to access and use the Task Queue feature
- ▶ Be familiar with the help system and how to obtain information from it
- ▶ Understand the elements of a user account that can be managed
- ▶ Be familiar with the various levels of user access and what elements of the system each access level can control
- ▶ Understand the basic process for setting up LDAP-based user account access
- ▶ Know the protocols involved in managing and administering the Sourcefire 3D System

**Event Analysis:**

- ▶ Understand how to use the various navigational elements of the Sourcefire 3D System user interface
- ▶ Know how to leverage the functionality of the Bookmark feature
- ▶ Know the various ways you can navigate from one type of alert table to another
- ▶ Be familiar with the various options for setting user preferences
- ▶ Know the implications of removing and excluding hosts from RNA
- ▶ Know the elements of RNA events, host profiles, network maps, client application maps, service maps and vulnerability maps
- ▶ Understand the concept of RNA flow data
- ▶ Be familiar with the summary pages for both RNA and Intrusion Sensor events
- ▶ Understand how to leverage the user interface for exploring events
- ▶ Know how to use the reporting feature and time range information is obtained by default
- ▶ Understand the concepts behind the Impact Flag and how the icons show in the interface to let an administrator know the implications of a given event
- ▶ Know the output options for the reporting engine
- ▶ Know the various ways reports can be generated
- ▶ Be familiar with the functionality of the clipboard and its various uses in the Sourcefire 3D System

**Intrusion Policy:**

- ▶ Know the elements of an intrusion policy and how you go about creating and managing existing policies
- ▶ Be familiar with the general architecture of the Intrusion Sensor's detection engine and how data flows through it
- ▶ Be familiar with the different kinds of preprocessors and what they do
- ▶ Understand the concept of normalization
- ▶ Know the configuration settings and options for preprocessors
- ▶ Understand how values are applied to policy variables
- ▶ Be familiar with the options for applying thresholds and alert suppression
- ▶ Know the various alert output options

**Rules:**

- ▶ Be familiar with rule options
- ▶ Know how to search for content in network traffic through the content option and its modifiers
- ▶ Have a basic understanding general rule options
- ▶ Be prepared to work though content option examples

**Active Scanning:**

- ▶ Understand the principals of vulnerability scans
- ▶ Understand the principals of port scanning and OS detection with Nmap
- ▶ Know the configuration and setup of Nessus
- ▶ Be familiar with the architectural implementation of Nessus and Nmap in the Sourcefire 3D System
- ▶ Know how to execute both Nmap and Nessus scans

**Enterprise Awareness:**

- ▶ Be familiar with the operation and options related to flow summary graphs
- ▶ Understand the workings of the profiling feature and its configuration options
- ▶ Be familiar with RUA architecture and its configuration
- ▶ Understand how to access and view the various types of RNA events
- ▶ Know the available alert types for compliance policy events
- ▶ Be familiar with the elements of a compliance policy
- ▶ Understand the concept of "Remediation"
- ▶ Understand the process of constructing compliance policy rules
- ▶ Know how to access compliance policy events
- ▶ Understand the White List capability and how to configure it
- ▶ Know how to view White List violations
- ▶ Familiarize yourself with the concept of host attributes and how they relate to White Lists

**Sourcefire 3D General:**

- ▶ Understand the fundamentals of tuning strategies
- ▶ Know how proper variable configuration plays a role with respect to sensor performance
- ▶ Be familiar with the general process of using the troubleshoot.pl script
- ▶ Know the general structure of the feedback produced by the troubleshoot.pl script
- ▶ Know how to configure Estreamer output
- ▶ Understand the structure of remediation modules

**Sample Questions:**

1. Given a packet that contains the string "silkworm" detected in a telnet data stream and the following two rules:

```
alert tcp any any -> any 23 (msg:"Silk1"; content:"silk";)
```

```
alert tcp any any -> any any (msg:"Silk2"; content:"silkworm";)
```

Which rule contains the most specific content item and would be selected first if the detection engine had to decide which one to alert on?

- a. Silk1
  - b. Silk2
  - c. They would alert concurrently
  - d. There is no match
2. Of the HTTP\_Inspect options listed below, which is NOT a global option?
    - a. ports
    - b. proxy\_alert
    - c. detect\_anomalous\_servers
    - d. None of the above
  3. A buffer overflow attack can result in which of the following outcomes?
    - a. Elevated privileges on the target host
    - b. Denial of service on the target host
    - c. Both A & B
    - d. Neither A or B
  4. Which of the following represents the management port number?
    - a. 443
    - b. 23
    - c. 8301
    - d. 8305

5. The mechanism in TCP/IP used to track which fragments belong to a given stream is ...

- a. Fragment offset
- b. Fragment flag bits
- c. Fragment identification
- d. Fragment options

Answer Key:

1. A | 2. A | 3. C | 4. D | 5. C