

**Course Description:** This three-day class covers the features and functionality of Sourcefire's 3D System including RNA, Intrusion Sensors, Defense Center and an overview of the Snort rules language. Users of Sourcefire products will learn to customize rules, troubleshoot, and write optimized rules with high performance while providing the highest levels of security.

**Who Should Attend:** Network administrators, security administrators, security consultants and others that are responsible for deploying and supporting Sourcefire's products are a must for this class.

**Prerequisites:** This course assumes that students have a technical understanding of TCP/IP networking and network architecture.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Customize rules
- Understand the Snort rules language
- Troubleshoot
- Write optimized rules with high performance

**Course Outline:**

Introduction

IDS/IPS &amp; RNA Technology Overview

Policy Management: Intrusion Sensor, RNA, and Compliance

Event Analysis &amp; Reporting

End-Point Intelligence

Flow Data Analysis

Nessus Scans

Rules and Rule Optimization

Rule Option Overview

Advanced Rule Options: Byte\_Test/Byte\_Jump &amp; PCRE

Rule Writing Best Practices and Troubleshooting

IDS/IPS &amp; RNA Technology Overview

3D Sensor Deployment and Network Architecture

Sourcefire 3D System Overview &amp; Product Installation

Basic Interface Navigation

Sensor Configuration and Management with the Defense Center

Configuring Interface Sets and Engine Instances

System Administration and Maintenance and Policy