

CROSSBEAM VIRTUAL TRAINING COURSE DESCRIPTION: IPS SOLUTION WITH SOURCEFIRE WORKSHOP (CBS-WEB-TRNG-SF)

This Virtual' format on-line course is designed to provide the participant a comprehensive technical review of the installation, basic configuration and operation of Sourcefire as a Crossbeam XOS Application. The lecture portion of the course is delivered on-line by invitation of Crossbeam Systems for qualified recipients. The 'Virtual' lectures are supported by detailed real-time lab exercises designed to be performed on the Crossbeam Remote Training Labs (RTL)

COURSE LENGTH:

This course is equivalent to a 1 day instructor led course. The On-line lecture requires approximately 3 hours to complete. The Labs will also take approximately 3 hours to complete. The Course is reinforced by an on-line test which is limited to 1 hour. One attempt is permitted. In the event of a failure, a second attempt at no charge maybe scheduled upon request. Access to the On-line program is granted upon confirmation of enrollment. Access to the RTL is available for a Monday to Friday week based on a published schedule.

AFTER COMPLETION OF THIS COURSE, YOU SHOULD BE ABLE TO:

- Install the Sourcefire 3D System application
- Configure a passive interface (IDS) solution with the Sourcefire 3D System on the Crossbeam X-series
- Configure an in-line interface (IPS) solution with the Sourcefire 3D System on the Crossbeam X-series
- Implement Sourcefire on Crossbeam in either a single system or dual box installation
- Monitor and troubleshoot traffic through the X-series chassis

PREREQUISITES

XOS Specialist Certification at XOS release 8.x
Sourcefire Applications

AUDIENCE:

Security Engineers, Operation Support Engineers who are responsible for the installation, configuration and deployment of network and Application software applications running on the X-Series Platform

COURSE OVERVIEW:

Lesson 1: XOS and Sourcefire Fundamentals

Introduction
XOS review
Sourcefire 3D System
Sourcefire requirements
Basic installation
Defense Center
Intrusion Sensor
Interface Sets
Detection Engine (DE)
IPS
RNA
Policy

Lesson 2: Solutions and Configuration

IPS configuration considerations
IDS configuration considerations
DBHA Layer 2 configuration considerations
Spanning tree

Lesson 3: Monitoring and Troubleshooting

Tools
Linux
XOS
Log files
Traffic monitoring
Statistics and error checking
Using TCPdump
Application troubleshooting

Lesson 4: Lab introduction

Review and introduction to the Remote Training Lab environment and access explained.

On-line Certification Exam