IBM Security Network Protection Administration and Configuration

Information

| | |
|---|---|
| **Length:** | 3.0 Days |
| **__Ref:** | IS671G |
| **Delivery method:** | ClassroomInstructor Led<br>Online |
| **Price:** | EUR |

Overview

IBM Security Network Prevention is a next-generation intrusion prevention system. This course provides the processes, procedures, and practice necessary to configure the Network Protection (XGS) appliance to protect your network. Students learn through hands-on labs how to configure the appliance, configure management and protection policies, and block a variety of common attacks.

Public

This course is designed for network and security professionals who evaluate, implement, manage, or monitor the IBM Security Network Protection appliance.

Prerequisits

Before taking this course, make sure that you have the following skills:
* Basic knowledge of information security concepts
* Familiarity with networking concepts, such as switching, routing, and firewalls, and tools, such as network sniffers and FTP clients
* Solid knowledge of the TCP/IP protocol and IPv4 networking
* Use the IBM Security SiteProtector™ console to manage agents. Students should attend IS604G, IBM Security SiteProtector System: Basic Implementation and Administration or an equivalent course before attending this class.

Objective

* Describe the characteristics and architecture of the IBM Security Network Protection appliance
* Connect the appliance to your network
* Configure initial settings on the appliance and register it with SiteProtector
* Use network objects and network access rules to configure the Network Access Policy
* Use IPS objects to configure the Intrusion Prevention Policy

* Describe different alert types and configure SNMP alerts generated by response objects and system alerts
* Use objects and policies to tune your security policy
* Capture network packets
* Configure local, remote, and passive user authentication
* Inspect outbound and inbound SSL traffic
* Use the SNORT syntax to incorporate rules in the appliance
* Use advanced threat protection and quarantine rules to block events
* Integrate the appliance with IBM Security QRadar SIEM
* Monitor events on the appliance

Topics

Unit 1: Introduction to IBM Security Network Protection
Unit 2: Setting up the appliance
Unit 3: Managing the appliance
Unit 4: Configuring the Network Access Policy
Unit 5: Configuring the Intrusion Prevention Policy
Unit 6: Using alerts and events
Unit 7: Tuning Network Access Policy rules and Intrusion Prevention behavior
Unit 8: Capturing network traffic
Unit 9: Controlling user access
Unit 10: Inspecting SSL-encrypted traffic
Unit 11: Implementing SNORT rules
Unit 12: Configuring advanced threat protection
Unit 13: Integrating with QRadar SIEM
Unit 14: Monitoring event data