SSFRULES (SECURING CISCO NETWORKS WITH SNORT RULE WRITING BEST PRACTICES (SSFRULES) V2.1) 2.1

Objetivo

After taking this course, you should be able to: â□¢ Describe the Snort rule development process â□¢ Describe the Snort basic rule syntax and usage â□¢ Describe how traffic is processed by Snort â□¢ Describe several advanced rule options used by Snort â□¢ Describe OpenAppID features and functionality â□¢ Describe how to monitor the performance of Snort and how to tune rules

PÃºblico Alvo

This course is for technical professionals to gain skills in writing rules for Snort-based Intrusion Detection Systems (IDS) and intrusion prevention systems (IPS). The primary audience includes: â□¢ Security administrators â□¢ Security consultants â□¢ Network administrators â□¢ System engineers â□¢ Technical support personnel using open source IDS and IPS â□¢ Channel partners and resellers

PrÃ©-Requisitos

To fully benefit from this course, you should have: â□¢ Basic understanding of networking and network protocols â□¢ Basic knowledge of Linux command-line utilities â□¢ Basic knowledge of text editing utilities commonly found in Linux â□¢ Basic knowledge of network security concepts â□¢ Basic knowledge of a Snort-based IDS/IPS system

Carga HorÃ¡ria

24 horas (3 dias).

ConteÃºdo ProgramÃ¡tico

Outline

- Introduction to Snort Rule Development
- Snort Rule Syntax and Usage
- Traffic Flow Through Snort Rules
- Advanced Rule Options
- OpenAppID Detection
- Tuning Snort

Lab outline

- Connecting to the Lab Environment
- Introducing Snort Rule Development

- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID
- Tuning Snort