

StoneGate Training Program

Course Outline

StoneGate IPS v.4.3

StoneGate IPS

In the *StoneGate IPS* course the student will learn the basics of network attacks, intrusion detection and prevention, including where and why network sensors and analyzers are used. StoneGate IPS course will provide a two-day introduction to the world of intrusion detection and it will give the students an overview of all the major features of StoneGate IPS.

Course Goals

Upon completing the StoneGate IPS course, the student should be able to install a StoneGate IPS and be able to explain different deployment options for IDS/IPS installations. The student should be able to correlate network events between IDS/IPS and firewall logs. The student should also be able to manage incident situations and customize the IPS policies. Finally, the student should be able to monitor the information generated by the StoneGate components and use the incident management and IPS to react to non-wanted traffic in the network.

Course Objectives

Upon completing StoneGate IPS course, the student is able to:

- Explain basics of IDS/IPS technologies
- Realize what types of network security threats exist
- Understand the role of an IDS/IPS in the overall security framework
- Install and configure a StoneGate IPS system
- Explain the functioning of the IPS system
- Create custom situations
- Create new access and inspection rules
- Update the system using dynamic updates
- Use StoneGate IPS efficiently for daily network supervision purposes

Course Program for Two-Day Training

Day 1

- Introduction to IDS/IPS
- IPS concepts and Deployment Scenarios
 - LAB 1:** StoneGate Management Center installation
 - LAB 2:** IDS and Inline IPS Definition and Installation
- StoneGate IPS Policies
 - LAB 3:** System Policy Installation
- Fine-tuning IPS policies
 - LAB 4:** Fine-Tuning IPS policies

Day 2

- Sensor Inspection Methods
 - LAB 5:** Creating Custom Situations
- Analyzer Correlation Methods
 - LAB 6:** Using Correlation Situations
- Incident Management
 - LAB 7:** Using Incident Management Tools
 - LAB 8:** Hold the fort

Certification Exam: ***StoneGate IPS Architect (SGIPSA)***

Disclaimer

This document and the contents herein are provided as a convenience to you. The contents of the Course Outline document are provided on "as is" and "as available" basis without any warranties. Stonesoft Corporation does not warrant that this document will be without inaccuracies or contextual or typographical errors. Stonesoft Corporation reserves the right to revise this document or withdraw access to it at any time without prior notification.

Stonesoft Corporation

Itälahdenkatu 22 A
FIN 00210 Helsinki, Finland
tel. +358 9 476 711
fax +358 9 4767 1234
www.stonesoft.com

Stonesoft Inc.

1050 Crown Pointe Parkway,
Suite 900, Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax +1 770 668 1131
info.americas@stonesoft.com