FortiAnalyser

Durée : 1 Jours

Résumé

In this one-day class, students will learn the fundamentals of using FortiAnalyzer 6.2 for centralized logging and reporting. Students will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, students will examine some helpful troubleshooting techniques.

In interactive labs, students will explore administration and management; register devices for log collection with FortiAnalyzer; use FortiAnalyzer to centrally collect logs; perform a forensic analysis of logs based on simulated network attacks; create reports; and explore solutions to common misconfiguration issues.

Public visé

Anyone who is responsible for the day-to-day management of FortiAnalyzer devices, and FortiGate security information.

Objectifs

After completing this course, you will be able to:

• Describe key features and concepts of FortiAnalyzer

• Deploy an appropriate architecture

• Use administrative access controls

• Monitor administrative events and tasks

• Manage ADOMs

• Configure RAID

• Register supported devices

- Troubleshoot communication issues

- Manage disk quota

- Manage registered devices

- Protect log information

- View and search logs

- Troubleshoot and manage logs

- Monitor events

- Generate and customize reports

- Customize charts and datasets

- Manage reports

- Troubleshoot reports

Contenu