FORTINET
NSE Training Institute

Advanced Analytics

In this three-day course, you will learn how to use FortiSIEM in a multi-tenant environment. You will learn to add various organizations to FortiSIEM and discover devices from each organization. You will learn to differentiate logs and events from each organization and apply appropriate rules. You will dive deep into rules and their architecture. You will also learn about incidents and how they are generated when a rule is triggered. You will learn about different clear conditions. You will also dive deep into baseline calculations performed on FortiSIEM. You will learn to create your own baseline profile and run queries based on the profile. Finally, you will learn the methods of remediation available on FortiSIEM.

In interactive labs, you will explore the role of FortiSIEM in a service provider environment. You will configure FortiSIEM in a cluster with a worker and NFS server for data storage. You will add organizations to FortiSIEM and manage the scope of each organization. You will register collectors from those organizations on FortiSIEM. You will also register Linux and Windows agents. You will analyze events from different organizations and understand how those events trigger some of the built-in rules. You will create your own rules and generate security events to trigger incidents for those rules.

Product Version

FortiSIEM 5.2.5

FortiGate 6.2.2

Formats

- Instructor-led classroom
- Instructor-led online
- Self-paced online

Agenda

1. Introduction to Multi-tenancy
2. Defining Collectors and Agents
3. Operating Collectors
4. FortiSIEM Windows and Linux Agents
5. Rules Breakdown
6. Single Subpattern Security Rule
7. Multiple Subpattern Rules
8. Introduction to Baseline
9. Baseline Rules
10. Clear Conditions
11. Remediation

Objectives

After completing this course, you should be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deployment
- Understand how FortiSIEM can be deployed in a hybrid environment with and without collectors
- Understand EPS restrictions on FortiSIEM
- Define organizations on FortiSIEM and assign collectors to organizations
- Deploy collectors in a multi-tenant solution
- Register collectors on the supervisor
- Understand the impact of excessive collectors on a FortiSIEM cluster
- Identify the impact of excessive collectors on a FortiSIEM cluster
- Manage EPS assignment on collectors
- Manage collector high availability
- Maintain and troubleshoot a collector installation
- Install Windows and Linux agents and identify the benefits of log collection through agents
- Understand agent architecture and associate templates with Windows and Linux agents
- Understand rule processes architecture and differentiate between a rule worker and a rule master
- Understand how the rule engine sliding time window works when it is evaluating rules
- Understand the out-of-the-box single pattern security rules and how to create rules by evaluating security events
- Define actions for a single pattern security rule
- Understand incident generation and identify the attributes that trigger an incident
- Identify multiple pattern security rules and define conditions and actions for them
- Understand how baseline data is useful in creating conditions in rules
- Differentiate between a standard report and a baseline report
- Understand the built-in baseline profile and learn to create your own baseline profiles
- Understand how statistical average and standard deviation calculations are performed on FortiSIEM
- Understand hourly buckets for weekdays and weekends
- Clone and edit some out-of-the-box baseline rules
- Understand clear conditions on FortiSIEM and walk through a rule with clear conditions
- Learn about remediation options on FortiSIEM and analyze some out-of-the-box remediation scripts

Who Should Attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiSIEM devices in an enterprise or service provider deployment used to monitor and secure the networks of customer organizations should attend this course.

Participants should have a thorough understanding of all the topics covered in the *NSE 5 FortiSIEM* course before attending the *NSE 7 Advanced Analytics* course.

Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts
- Basic understanding of SIEM products
- Basic understanding of Linux

It is *highly recommended* that you have an understanding of the topics covered in the *NSE 5 FortiSIEM* course.

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  - HTML5 support
  - An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser

You should use a wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Certification

This course is intended to help participants prepare for the *NSE 7 Advanced Analytics* certification exam.