FORTINET
Premier Authorized Training Center

NSE 6 CERTIFIED
SECURITY OPERATIONS
FORTINET

fast lane

FortiSIEM Analyst

Course Description

In this course, you will learn how to use FortiSIEM to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization. You will learn how to perform real-time and historical searches and build advanced queries. You will also learn how to perform analysis and remediation of security incidents using traditional and machine learning (ML)assisted methods.

Product Version:

- FortiSIEM 7.4

Course Duration:

3 Days

Prerequisites:

You must have an understanding of the topics covered in the following courses, or have equivalent experience.

- FortiGate Operator
- FortiSIEM Administrator

Outlines:

1. Introduction to FortiSIEM
2. Analytics
3. Nested Queries and Lookup Tables
4. Rules and Subpatterns
5. Incidents
6. Clear Conditions and Remediation
7. Threat Hunting
8. Performance Metrics and Baselines
9. Machine Learning
10. User and Entity Behavior Analytics
11. FortiSIEM ZTNA
12. Reports and Dashboards

Objectives:

After completing this course, you will be able to:

- Describe how FortiSIEM solves common cybersecurity challenges
- Describe the main components and the unique database architecture on FortiSIEM
- Perform real-time and historical searches
- Define structured search operators and search conditions
- Reference the CMDB data in structured searches

- Configure display fields and columns
- Build queries from search results and events
- Build nested queries and lookup tables
- Build rule sub patterns and conditions
- Manage and tune incidents
- Resolve an incident
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Create rules using baselines
- Analyze anomalies against baselines
- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Describe FortiSIEM ML modes and algorithms
- Describe how to train an ML model perform an analysis using a ML model
- Describe the benefits of deploying FortiSIEM UEBA
- Configure tags, rules, and incidents using UEBA data
- Describe how ZTNA tags affect the FortiSIEM incident and remediation process
- Configure a ZTNA tag using FortiSIEM to remediate incidents
- Generate and export a report
- Create a custom dashboard

Who should attend

Security professionals responsible for the detection, analysis, and remediation of security incidents using FortiSIEM should attend this course.