Analyzing Logs with FortiAnalyzer 7.4 Course

Course Duration: 8 Hrs. **Course Code: FAZ-LOG-7.4**

Course Overview

The **Analyzing Logs with FortiAnalyzer 7.4** course is designed for security and network professionals who want to gain practical skills in collecting, analyzing, and interpreting logs using FortiAnalyzer. This course focuses on leveraging FortiAnalyzer 7.4 to gain visibility into network traffic, security events, and threat activity across Fortinet environments. Participants will learn how to investigate incidents, create dashboards and reports, and enhance security operations through effective log analysis.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiAnalyzer logging architecture and workflows
- Collect and manage logs from FortiGate and other Fortinet devices
- Analyze traffic, security, and event logs effectively
- Create and customize dashboards and reports
- Investigate security incidents using log data
- Correlate events and identify threats
- Optimize log analysis for SOC operations

Target Audience

This course is ideal for:

- SOC Analysts and Security Analysts
- Network and Security Administrators

- Incident Response Professionals
- Fortinet Solution Engineers
- IT Operations and Monitoring Teams

Pre-Requisites

Participants should have:

- Basic understanding of networking and security concepts
- Familiarity with FortiGate and Fortinet products
- Experience with log analysis is helpful but not required

Course Content

Module 1: Introduction to Log Analysis with FortiAnalyzer

- Role of logs in security operations
- FortiAnalyzer 7.4 overview
- Logging sources and data flow

Module 2: Log Collection and Management

- Configuring log forwarding
- Log storage and retention
- Managing log sources

Module 3: Log Analysis and Investigation

- Traffic and security log analysis
- Filtering, searching, and correlating events
- Identifying suspicious activity

Module 4: Dashboards and Visualization

- Predefined dashboards and widgets
- Creating custom dashboards
- Visualizing trends and threats

Module 5: Reporting and SOC Use Cases

- Report templates and customization
- Scheduled and on-demand reports
- Compliance and audit reporting

Module 6: Advanced Analysis and Best Practices

- Event correlation and threat hunting
- Performance optimization
- Log analysis best practices and course wrap-up