Wazuh SIEM

6 Day Professional Training

IT FORTRESS

Powered by – IT Fortress

Master Wazuh SIEM: Your Path to Cybersecurity Excellence

About the Training

Elevate your cybersecurity skills with our **6-Day Professional Wazuh SIEM Training**. Designed for professionals seeking hands-on expertise in Security Information and Event Management (SIEM), this course equips you with the knowledge to manage, monitor, and secure IT infrastructures using Wazuh.

Key Training Details

- **Mode:** Online (Interactive Live Sessions)
- **Duration:** 6 Days (4 Hours/Day)
- **Language:** English
- **Software Version:** Wazuh (4.9.0 – 4.10.1)
- **Prerequisites:**
    - Ethical Hacking
    - Network Security
    - Networking Fundamentals
    - Basics of Cybersecurity
    - Basics of Linux command-line
- **Instructor:**
    - **Muhammad Moiz Ud Din Rafay**
    - Cybersecurity Expert | Wazuh SIEM Specialist

What You Will Learn

Our structured course ensures you transition from foundational understanding to advanced application.

Day 1

Module 1: Introduction to Wazuh SIEM

- Overview of SIEM and its Importance
- Introduction to Wazuh as a Security Platform
- Key Features and Architecture of Wazuh
- Understanding Wazuh Terminology
- Wazuh Vs Other SIEM Solutions

Module 2: Wazuh Installation

- 2.1 Installation Methods
- Setting up Wazuh on Virtual Machines
- Cloud Deployment (AWS, Azure, Google Cloud)
- Standalone Setup for Local Environments
- 2.2 Prerequisites and Best Practices
- System Requirements
- Network Configuration Guidelines
- Troubleshooting Installation Issues

Day 2

Module 3: Wazuh Configuration

- Setting up Agents and Managers
- Configuring Filebeat and Elasticsearch
- Creating and Managing User Roles
- Customizing Wazuh for Specific Use Cases

Module 4: Wazuh Log Analysis

- Collecting and Parsing Logs
- Understanding Log Categories and Types
- Techniques for Analyzing Security Events
- Troubleshooting Log Collection Issues

Day 3

Module 5: Wazuh Integrations

- 5.1 Firewall Integrations
- Integrating Wazuh with pfSense Firewall
- Fortinet Firewall Integration

- 5.2 Security Tool Integrations
  - Windows Sysmon and Defender Integration
  - Microsoft 365 Security Integration

- 5.3 IDS/IPS Integration
- Suricata and Snort with Wazuh

- 5.4 SOAR and Custom Integrations
- Automating Security with Wazuh and SOAR Tools
- Building Custom Integrations for Specific Requirements

Module 6: Wazuh Rules and Decoders

- Understanding the Rule Writing Syntax
- Creating and Managing Custom Rules
- Decoders: Parsing Custom Logs for Effective Analysis
- Testing and Debugging Rules and Decoders

Day 4

Module 7: Wazuh Active Response

- Setting up Active Response Modules
- Mitigating Brute Force Attacks Automatically
- Writing Custom Active Responses for Advanced Threats

Module 8: Compliance and Policy Management

- Using Wazuh for Regulatory Compliance (HIPAA, GDPR, PCI DSS, etc.)
- Automating Compliance Audits
- Leveraging CDB Lists for Security and Compliance

Day 5

Module 9: Threat Intelligence and Malware Analysis

- Leveraging Wazuh for Threat Intelligence
- Identifying Malware Behaviour with Wazuh Logs
- Integrating External Threat Feeds

Module 10: Wazuh Reporting and Dashboards

- Generating Comprehensive Reports
- Creating and Customizing Wazuh Dashboards
- Sharing Insights with Stakeholders

Day 6

Module 11: Advanced Use Cases

- Advanced Incident Detection and Response
- Building Multi-layer Security with Wazuh and Integrated Tools
- Custom Alerts and Advanced Notification Systems

Capstone Project

Apply your skills in a real-world scenario:

- Deploying Wazuh in a Simulated Enterprise
- Managing Security Events in Real-Time
- Responding to Cyber Threats Effectively

Why Choose Us?

- Comprehensive Curriculum
- Expert-Led Training by Industry Professionals
- Real-World Applications with Hands-On Labs
- Community Support and Resources Post-Training

Who Should Attend?

This course is ideal for:

- SOC Analysts and Engineers
- Cybersecurity Professionals
- Network Administrators
- IT Security Enthusiasts

Additional Benefits

- Access to Exclusive Wazuh Resources
- Certificate of Completion
- Guidance on Preparing for Wazuh Certifications

Register Today!

Don’t miss this opportunity to master one of the most versatile SIEM tools.

👉 **Visit:** www.itfortress.io

📧 **Contact Us:** training@itfortress.io

📞 **Call Us:** (+64)21145179

Unlock your cybersecurity potential with our expert-led Wazuh SIEM training. Reserve your spot now!