securitum

WAZUH Expert

Practical course on administering a SIEM tool

Language course: Polish

8 3-hour learning sessions

- Comprehensive knowledge: from installation to advanced configuration
- Experienced practice trainer
- Accessible online form
- Access to the recordings for 180 days from the date of training
- Meeting the requirements of the NIS 2 directive

FOR WHOM

- IT system administrators
- IT security specialists
- SOC employees
- IT security enthusiasts

WHY WAZUH?

- Open source, free security information and event management system
- Multiplatform, supports Windows, Linux and macOS among others
- Scalable, suitable for small and large infrastructures
- Integrates with major cloud solution providers: AWS, Azure or Google Cloud
- Offering advanced monitoring features
- Flexible, giving you the ability to customize to your organization's needs

BASIC MODULE

22 and 29 May 2025
5, 12 and 18 June 2025

899 PLN NET

ADVANCED MODULE

3, 10 and 17 July 2025

499 PLN NET

PRO TICKET

BASIC + ADVANCED MODULE

1299 PLN NET

wazuh.securitum.pl

TRAINER

Tomasz Turba. IT security consultant at Securitum. He is certified by Cisco, Red Hat, AWS, Microsoft, NSA 4011 and ABW. He has more than 15 years of experience in IT; he started as early as in high school, fulfilling orders as a neighborhood network administrator. He has worked with numerous institutions as a security consultant, pentester and RODO inspector. He has extensive experience as head of a CSIRT team. Since 2022 he has been a researcher and trainer at Securitum. Passionate about information security, with a drive for knowledge transfer. Conducts trainings on forensic analysis, network security, white intelligence OSINT, topics related to AI, as well as lectures on cyberawareness. Winner of several competitions for the best publication on IT security. Speaker at the MEGA Sekurak Hacking Party. Editor at sekurak.pl with books on IT security, published by Securitum.

AGENDA

SESSION Nº 1: Wazuh – introduction, installation and configuration:

1. Introduction to Wazuh:
   - What is Wazuh and what problems it solves.
   - Overview of Wazuh's architecture.
2. Preparation of the environment:
   - System requirements.
   - Preparing a virtual and physical machine with Linux.
3. Installing Wazuh:
   - Downloading and installing the Wazuh server.
   - Base configuration and installation of add-ons.
4. Basic configuration:
   - Configuring the Wazuh agent on Linux i Windows systems.
   - Post-testing, base tuning.
   - Agent configuration in agentless mode (Syslog and SSH).
5. Summary and Q&A session.

SESSION Nº 2: Wazuh – detailed configuration and troubleshooting:

1. Advanced configuration:
   - Configuration of rules and security policies.
   - Creation and modification of decoders.
2. Troubleshooting:
   - Troubleshooting common installation and configuration problems.
   - Log and error analysis.
3. Summary and Q&A session.

SESSION Nº 3: Wazuh – server management and system security:

1. User management:
   - Creating and managing user accounts in Wazuh.
   - Configuration of user roles and privileges.
   - Implementation of security policies for users.
   - Auditing and monitoring of user activities.
2. System security:
   - Securing communication between Wazuh components (SSL/TLS).
   - Configuration and management of firewalls.
   - Implementation of operating system security policies.
   - Monitoring and response to security breach attempts.
3. Backup and restoration of data:
   - Backup strategies for Wazuh.
   - Configuration of automatic backups.
   - Disaster recovery procedures.
4. Analysis and reporting:
   - Creating custom security reports.
   - Configuration of security breach notifications and alerts.
   - Analysis of logs to detect potential threats.
5. Summary and Q&A session.

SESSION Nº 4: Wazuh – incident response:

1. Introduction to basic concepts and threats.
2. Incident detection and response:
   - Creating and managing detection rules.
   - Analysis and response to alerts.
3. Simulation of an attack and analysis of its consequences using Wazuh.
4. Adjuncts of real incidents and response to them.
5. Summary and Q&A session.

SESSION Nº 5: Wazuh – cluster setup:

1. Introduction to cluster installation:
   - Benefits of using a cluster.
   - Overview of cluster architecture.
2. Cluster installation:
   - Configuration of cluster calls.
   - Load balancing and redundancy.
3. Scaling and optimization:
   - Performance monitoring.
   - Optimizing configuration for performance.
4. Summary and Q&A session.

SESSION Nº 6: Wazuh – advanced configurations:

1. Integration with external services:
   - Signature detection using YARA.
   - Message enrichment using LLM/AI.
   - Automation using Ansible.
   - Integration of other solutions using API.
2. Monitoring container events.
3. Monitoring of cloud infrastructure.
4. Updating agents through GPO policies.
5. Summary and Q&A session.

SESSION Nº 7: Wazuh – advanced optimizations:

1. Monitoring performance, metrics and processes.
2. Index and query optimization.
3. Best practices for cluster maintenance.
4. Cross-cluster search implementation.
5. Data retention optimization and log management.
6. Q&A session.

SESSION Nº 8: Wazuh – expert integrations:

1. Integration with Grafana.
2. Integration with MISP.
3. Integration with Suricata.
4. Integration with Zabbix.
5. Integration with Git.
6. Integration with Graylog.
7. Integration with nmap and ChatGPT.
8. Integration with CDB AlienVault.
9. Integration with Atlassian Jira.
10. Integration with Sysmon.
11. Integration with Microsoft API (Office365).
12. Q&A session.

Each session will be accompanied by a practical exercise – a laboratory for independent implementation.

REGISTRATION AND DETAILS

wazuh.securitum.pl

Additional questions: Aneta Jandziś
aneta.jandzis@securitum.pl
Phone +48 (12) 352 33 82
+48 516 824 029