CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Wazuh Grundlagen

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

01 Was ist Wazuh?

02 Die Architektur

03 Installation und Basiskonfiguration

AGENDA

01 Was ist Wazhu?

Was ist Wazhu?

- Ursprung und Entwicklung:

  - Wazuh ist eine Open-Source-Sicherheitsplattform, die aus dem Projekt OSSEC entstanden ist.

  - Sie kombiniert unter anderem Funktionen von SIEM, HIDS, Log-Management

  - Erleichtert das Management komplexer Sicherheitsaufgaben

UEBERSCHRIFT

Was ist Wazhu?

- Open Source Sicherheitsplatform
- Überwachung, Erkennung und Reaktion auf Sicherheitsbedrohungen
- Funktionen von SIEM und IDS kombiniert
- Log Management
- File Integrity Monitoring und mehr

Hauptfunktionen

Funktion	Beschreibung
Log Management	Zentrale Sammlung und Analyse von System- und Applikations-Logs
Intrusion Detection (HIDS)	Überwachung von Host-Systemen auf verdächtige Aktivitäten
File Integrity Monitoring	Überwachung von Dateiänderungen auf kritischen Systemen
Vulnerability Detection	Schwachstellen-Scanning auf Hosts mittels Integration z. B. mit VulnDB

Hauptfunktionen

Funktion	Beschreibung
Configuration Assessmen	Vergleich der Systemkonfigurationen mit Sicherheitsrichtlinien
SIEM-Funktionalität	Ereigniskorrelation, Alarmierung und Dashboarding
Cloud-Sicherheit	Unterstützung von AWS, Azure und GCP durch spezielle Module
MITRE ATT&CK-Mapping	Erkennung von Techniken auf Basis des MITRE ATT&CK Frameworks

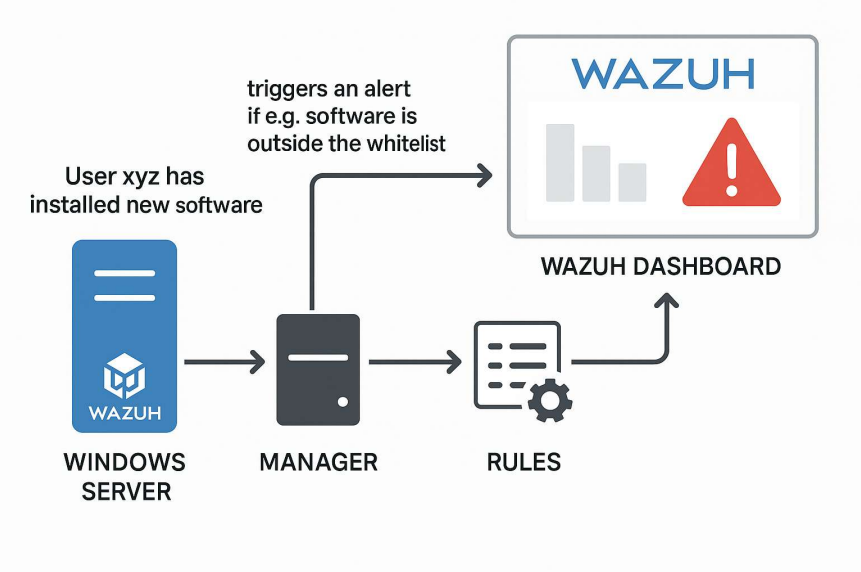
UEBERSCHRIFT

Einsatzmöglichkeiten

- Monitoring von Servern, Endgeräten und Cloud-Instanzen
- Erfüllung von Compliance-Vorgaben (z. B. PCI-DSS, ISO 27001, HIPAA)
- Frühzeitige Erkennung von Angriffen
  durch Regelwerke und Threat Intelligence
- SIEM-Alternative für kleine bis mittlere Unternehmen mit Open-Source-Fokus

Beispielanwendung

- Wazuh-Agent wird auf einem Windows-Server installiert.
- Der Manager empfängt Ereignisse wie „User xyz hat eine neue Software installiert“.
- Eine Regel triggert einen Alarm, wenn z. B. Software außerhalb der Whitelist auftaucht.
- Das Wazuh-Dashboard zeigt den Alarm visuell an.



UEBERSCHRIFT

Begriffserklärung: HIDS

- Ein HIDS (Host-basiertes Intrusion Detection System) überwacht Aktivitäten direkt auf den einzelnen Rechnern und Systemen.
- Im Gegensatz zum Netzwerk-IDS erkennt es Angriffe durch Monitoring von Log-Dateien, Prozessen und Dateisystemen direkt auf dem Host.
- Folge: Höhere Detailtiefe bei der Angriffserkennung.

02 Die Architektur

Architektur

Wazuh besteht aus mehreren Komponenten:

- Agent:
  Läuft auf jedem zu überwachenden System (Linux, Windows, macOS)

- Manager:
  Zentrale Analyseinstanz, korreliert Daten, erkennt Bedrohungen

- Indexierung (Elasticsearch/OpenSearch):
  Speichert und durchsucht Ereignisdaten

- Dashboard (Kibana oder Wazuh-eigen):
  Visualisierung, Alarmierung, Berichte

Architektur – Wazhu Agent

- Verantwortlich für lokale Datensammlung:
  Der Agent sammelt sicherheitsrelevante Daten auf dem Endgerät (z. B. Server oder Client).

- Plattformübergreifend:
  Unterstützt Windows, Linux, macOS, Solaris, AIX und andere Betriebssysteme.

- Kommunikation mit dem Wazuh-Manager:
  Der Agent sendet gesammelte Ereignisse (Logs, Prozesse, Dateiänderungen etc.) verschlüsselt an den Manager (meist über TCP/UDP oder persistente TCP-Verbindung).

Architektur – Wazhu Agent

- Typische Datenquellen:
  - Systemlogs (z. B. Syslog, Windows Eventlog
  - Datei-Integritätsprüfung (FIM – File Integrity Monitoring
  - Rootkit-Detection
  - Schwachstellen-Scans
    (z. B. über Wazuh-integrierten OpenSCAP oder Vulnerability Detector)

- Echtzeit-Überwachung:
  Erkennt verdächtige Aktivitäten nahezu in Echtzeit.

- Regelbasierte Analyse:
  Lokale Ereignisse werden mit Regeln abgeglichen, bevor sie (ggf. gefiltert) an den Manager weitergegeben werden.

Architektur – Wazhu Agent

- Selbstschutz:
  Optionaler Schutz vor Manipulation des Agenten
  (z. B. durch Deaktivierung).

- Zentrale Konfigurierbarkeit:
  Der Agent kann über den Manager remote verwaltet und aktualisiert werden.

- Einsatzgebiete:
  - Compliance (z. B. PCI-DSS, GDPR)
  - Incident Detection & Response
  - Schwachstellenmanagement
  - Dateiüberwachung

Architektur – Wazhu Manager

- Zentrale Analyse- und Entscheidungsinstanz:
  Empfängt, verarbeitet und analysiert die Daten der Wazuh-Agenten.

- Regelbasierte Verarbeitung:
  Nutzt ein leistungsfähiges Regelwerk, um eingehende Ereignisse zu korrelieren, zu bewerten und ggf. als Alarm zu klassifizieren.

- Alarmierung:
  Erkennt sicherheitsrelevante Vorfälle und erstellt entsprechende Alarme mit Schweregrad, Beschreibung und Zeitstempel.

- Integration externer Bedrohungsdaten:
  Kann mit Threat-Intelligence-Feeds (z. B. OTX, MISP) interagieren

Architektur – Wazhu Manager

- „Multi-Tenant“ fähig:
  Unterstützt mehrere Agenten in verschiedenen logischen Gruppen oder Organisationen.

- Verwaltung & Konfiguration der Agenten:
  Remote-Verteilung von Konfigurationen, Regeln und Skripten an Agenten.

- Kommunikation:
  Empfang der Agentendaten über verschlüsselte TCP/UDP-Verbindungen (i.d.R über Port 1514 oder 1515).

Architektur – Wazhu Manager

- Integration mit Elasticsearch & Kibana:
  Leitet analysierte Daten zur weiteren Aufbereitung, Visualisierung und Speicherung weiter.

- Skalierbarkeit:
  Kann in verteilten Setups mit Load Balancern, mehreren Manager-Instanzen oder Worker-Nodes betrieben werden.

- API-Schnittstelle:
  Bietet eine RESTful API für Automatisierung, Monitoring und externe Systemintegration.

Architektur – Indexierung

- Indexierung ist der Prozess, bei dem strukturierte oder unstrukturierte Daten in ein durchsuchbares Format überführt werden.
- In Wazuh wird jeder Logeintrag eines Agenten als Dokument gespeichert und durchsuchbar gemacht.
- Daten werden analysiert (z. B. durch Tokenisierung) und als sogenannte Dokumente in einem Index gespeichert.
- Ein Index entspricht einer Sammlung von Dokumenten mit ähnlicher Struktur.
- Die Indexierung erlaubt:
  schnelle Volltextsuche, Filterung, Aggregation und Analyse großer Datenmengen in Echtzeit.

Architektur – Dashboard

- Webbasierte Benutzeroberfläche:
  Ermöglicht die grafische Auswertung und Überwachung aller sicherheitsrelevanten Ereignisse.

- Visualisierung von Alarmen und Ereignissen:
  Zeigt erkannte Vorfälle, deren Schweregrad, betroffene Systeme und Zeitstempel an – oft in Form von Diagrammen, Tabellen oder Zeitachsen.

- Integration mit Kibana (bei Elasticsearch) bzw. OpenSearch Dashboards:
  Nutzt deren Funktionen für Visualisierung, Dashboards und Drilldowns.

- Suche & Filterung:
  Ereignisse lassen sich nach Datum, Schweregrad, Agent, Regel-ID, Benutzername, IP-Adresse u. v. m. durchsuchen und filtern.

Architektur – Dashboard

- Dashboards für unterschiedliche Zwecke:
  Vordefinierte Ansichten z. B. für:
  - Security Events
  - Compliance (PCI-DSS, GDPR etc.)
  - FIM (File Integrity Monitoring)
  - Vulnerability Detection
  - Agentenstatus

- Live-Überwachung & Statusanzeige:
  Zeigt den aktuellen Zustand der Agenten (aktiv, offline, mit Fehlern) in Echtzeit.

Architektur – Dashboard

- Reaktive Maßnahmen:
  Ermöglicht bei Bedarf die Weiterleitung von Alarmen an externe Tools (SIEM, E-Mail, Slack etc.) oder die manuelle Analyse tiefergehender Logs.

- Benutzer- und Rollenverwaltung:
  Zugriffsrechte lassen sich rollenbasiert einschränken (z. B. für Auditoren, Admins, Analysten).

03 Installation und Basis-konfiguration

Installation
(Prerequisits f. Manager)

- Hardware (für kleine bis mittlere Umgebungen):
  - CPU: ≥ 2 Cores
  - RAM: ≥ 4–8 GB
  - Speicherplatz: ≥ 20–50 GB (vom Logvolumen abhängig)

- Softwareabhängigkeiten:
  Python 3.xOpenSSLcurl, tar, wget, unzipsystemd oder initd je nach Distribution

- Netzwerk:
  Offen:
  - TCP-Port 1514/1515 (Kommunikation mit Agenten)
  - Optional: TCP-Port 55000 (Remote-Agentenmanagement per API)

Installation
(Prerequisits f. Agent)

Fast Keine Prerequisits ☺

- Geringe Ressourcenanforderungen
  - wenige MB RAM, kaum CPU-Last
- Unterstützt alle gängigen Betriebss<ysteme:
  - Windows, macOS, Linux, Solaris, AIX, BSD
- Kommunikationsfähigkeit mit dem Manager über die Ports TCP 1514 oder 1515 muss sicher gestellt werden.
- Java ist nicht notwendig

Installation

(Prerequisits f. Elasticsearch / OpenSearch)

- Hardware (für Produktivumgebungen):
  - CPU: ≥ 4 Cores
  - RAM: ≥ 8–16 GB (Elasticsearch JVM benötigt viel RAM)
  - Eine SSD wird empfohlen für schnellere Indexierung

- Software:
  - Java 11 (für Elasticsearch ≤7.10)
  - Elasticsearch/OpenSearch in kompatibler Version zum Wazuh-Manager

- Netzwerk:Offen:
  - TCP
    - Port 9200 (HTTP API),
    - Port 9300 (Cluster-Kommunikation)

Installation Wazhu Manager

- Von Wazhu gibt es ein Installationsscript, welche unter

  https://packages.wazuh.com/4.8/wazuh-install.sh

  herunter geladen werden kann.

- Link zur offiziellen Doku:

  https://documentation.wazuh.com/current/installation-guide/index.html

- Fehlermeldung auf Debian:
  ```
  ERROR: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9;
  CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04
  ```

  (Mit `sudo ./wazuh-install.sh -a -i --ignore-check` kann die Fehlermeldung umgangen werden. NUR FÜR TESTSYSTEME !)

Installation Wazhu Manager

- Beispielhafter Screenshot einer Installation auf einem Testsystem:

  Hinweis:
  Die Installation dauerte auf diesem Testsystem >5 Minuten.
  Geduld bewahren !

```
user1@debian:~$ sudo ./wazuh-install.sh -a -i --ignore-check
24/07/2025 18:46:30 INFO: Starting Wazuh installation assistant. Wazuh version: 4.8.2
24/07/2025 18:46:30 INFO: Verbose logging redirected to /var/log/wazuh-install.log
24/07/2025 18:46:31 WARNING: Hardware and system checks ignored.
24/07/2025 18:46:33 INFO: --- Dependencies ----
24/07/2025 18:46:33 INFO: Installing gawk.
24/07/2025 18:46:34 INFO: Wazuh web interface port will be 443.
24/07/2025 18:46:36 INFO: --- Dependencies ----
24/07/2025 18:46:36 INFO: Installing software-properties-common.
24/07/2025 18:46:44 INFO: Wazuh repository added.
24/07/2025 18:46:44 INFO: --- Configuration files ---
24/07/2025 18:46:44 INFO: Generating configuration files.
24/07/2025 18:46:44 INFO: Generating the root certificate.
24/07/2025 18:46:44 INFO: Generating Admin certificates.
24/07/2025 18:46:44 INFO: Generating Wazuh indexer certificates.
24/07/2025 18:46:45 INFO: Generating Filebeat certificates.
24/07/2025 18:46:45 INFO: Generating Wazuh dashboard certificates.
24/07/2025 18:46:45 INFO: Created wazuh-install-files.tar. It contains the Wazuh clus
asswords necessary for installation.
```

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- System vorbereiten:

```
sudo apt update && sudo apt upgrade -y

sudo apt install curl unzip gnupg apt-transport-https -y
```

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- Installer-Skript herunterladen:

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
chmod +x wazuh-install.sh
```

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- Installation ausführen:

  ```
  sudo ./wazuh-install.sh -a
  ```

- ‘-a‘ steht für All-in-One:

  Installiert
  - Wazuh-Manager
  - OpenSearch
  - Dashboard
  - und alle Abhängigkeiten

  auf einem Host.

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- Installation überprüfen:

```
sudo systemctl status wazuh-manager
sudo systemctl status opensearch
sudo systemctl status wazuh-dashboard
```

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- Zugriff auf das Dashboard:

  `https://<IP-des-Wazuh-Rechners>`

- Standard Zugangsdaten:

  Benutzer: admin
  Passwort: Wird am Ende der Installation angezeigt!

  Das Pw kann in der Regel auchaus folgender Datei herauskopiert werden:

  `~/wazuh-install-files/wazuh-passwords.txt`

Installation Wazhu Manager

Schritt für Schritt Anleitung:

- Falls aktiv muss die Firewall konfiguriert werden:
  (je nachdem welche Variante man installiert hat.

  Beispiel für die UFW:

  ```
  sudo ufw allow 443/tcp
  ```
- `sudo ufw allow 1514/tcp`
- `sudo ufw allow 1515/tcp`

DANKE!

Gibt es noch Fragen?

CloudCommand