Open Source-Sicherheitsüberwachung mit Wazuh

Agenda

Organisatorisches

- Geplante Dauer: 1 Stunde
- Nach etwa der Hälfte der Zeit kommen wir zum praktischen Teil
- Wir zeigen Euch ein Testbed von einem Projekt

Organisatorisches

- Geplante Dauer: 1 Stunde
- Nach etwa der Hälfte der Zeit kommen wir zum praktischen Teil
- Wir zeigen Euch ein Testbed von einem Projekt

Ziel: Herausarbeiten der Vorteile des Betriebens von Wazuh in kleinen Umgegebungen (aka KMUs)

Zu meiner Person

Kurze Vorstellung

- Thomas Heil
- Freiberuflicher Consultant
- Arbeitet für die OLANIS GmbH
- Arbeitet für ein paar Firmen, deren Name nicht genannt werden darf
- DevOps und klassische Administrator Tätigkeiten

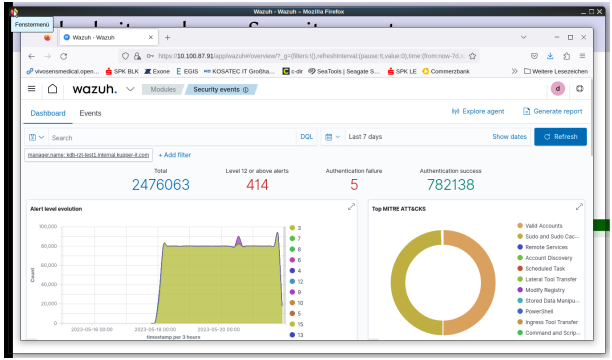
Zum heutigen Thema

SIEM + XDR + ... == Wazuh

- SIEM **Security Information and Event Management**
- XDR **Extended detection and response**
- Endpoint Security
- OpenSource
- breiter Funktionsumfang
- SOC ?
- IDS / IPS ?

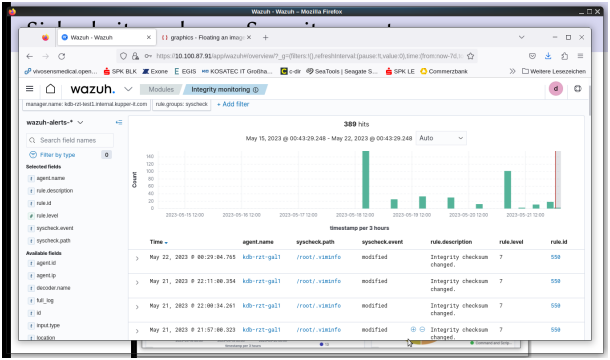
Sicherheitsanalysen; Security events

1. sammeln, aggregieren, indizieren und analysieren von Sicherheitsdaten



Veränderungen an Dateien / Integrity monitoring

1. Dateiänderungen, wie Rechte, Inhalt, Zugehörigkeit und Attribute



Office 365, AWS, Google Cloud Plattform, Github

1. Office365 Activity Monitoring via API
   `via API`

Office 365, AWS, Google Cloud Plattform, Github

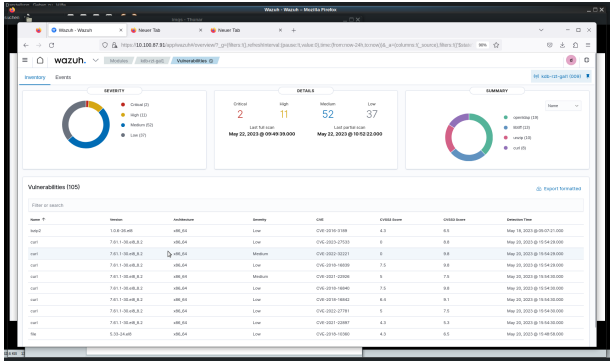
1. Office365 Activity Monitoring via API `via API`
2. Amazon AWS oder GCP

Office 365, AWS, Google Cloud Plattform, Github

1. Office365 Activity Monitoring via API `via API`
2. Amazon AWS oder GCP
3. Github

Vulnerabilities

1. Welche Anwendungen sind als CVE bzw. als Schwachstelle gelistet



Osquery, VirusTotal, Docker Listener

1. Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

Osquery, VirusTotal, Docker Listener

1. Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

2. virus total

Osquery, VirusTotal, Docker Listener

1. Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

2. virus total
3. docker listener

Osquery, VirusTotal, Docker Listener

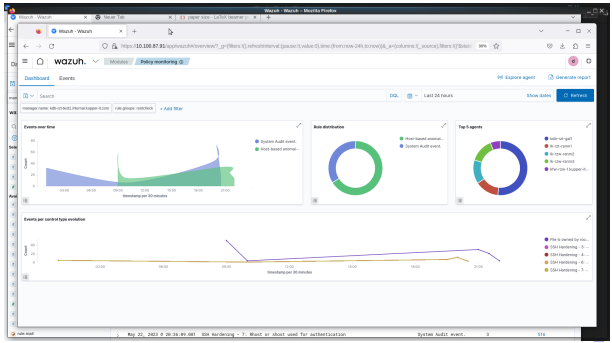
1. Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

2. virus total
3. docker listener
4. mitre attack

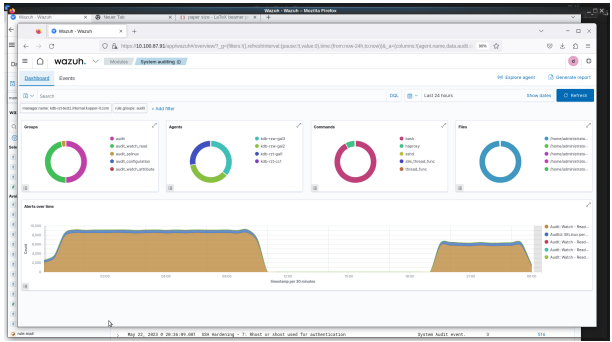
Policy monitoring

1. vergleiche das System gegen Veschiedene BaseLines
   siehe `/var/log/audit/audit.log`



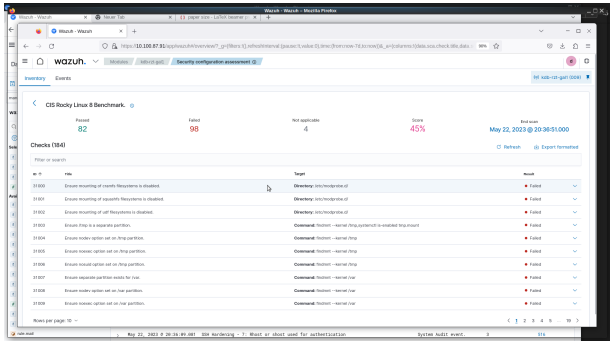
System auditing

1. Monitoring wichtiger Files und das Verhalten der Benutzer



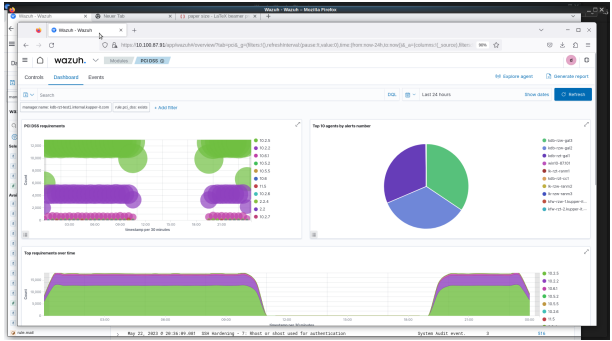
Security configuration assessment

1. Benchmarks wie CIS, die vorgeben, wie

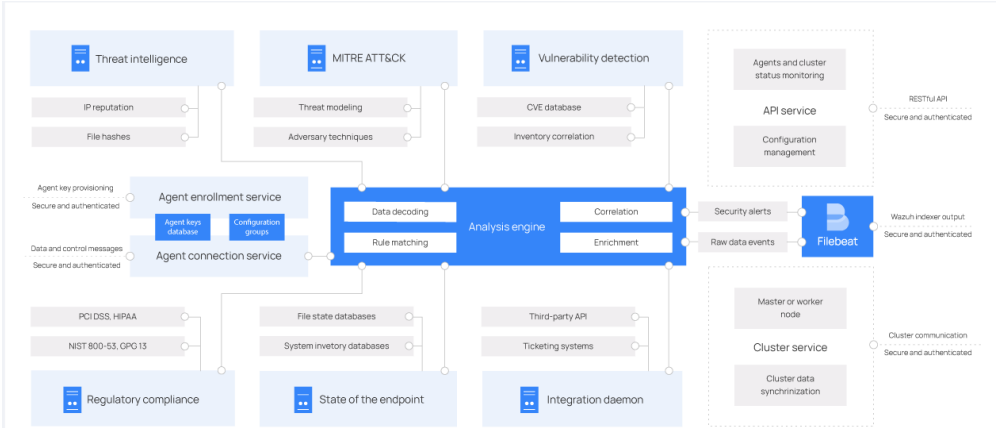


PCI-DSS

1. Anzeigen von COMPLIANCE Controls



Zusammenfassung / Wazuh Komponenten im Überblick



Wazuh Installation

```
curl -sO https://pack....com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

1. Warten !

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Wazuh Installation

```
curl -sO https://pack....com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

1. Warten !

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

2. Notieren des admin Passworts

Wazuh Installation

```
curl -sO https://pack....com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

1. Warten !

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

2. Notieren des admin Passworts
3. Neue Benutzer anlegen!

alternative Installationsvarianten

1. ansible

alternative Installationsvarianten

1. ansible
2. puppet

alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)

alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)
4. Amazon Machine Images (AMI)

alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)
4. Amazon Machine Images (AMI)
5. Deployment on Docker

alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)
4. Amazon Machine Images (AMI)
5. Deployment on Docker
6. Deployment on Kubernetes

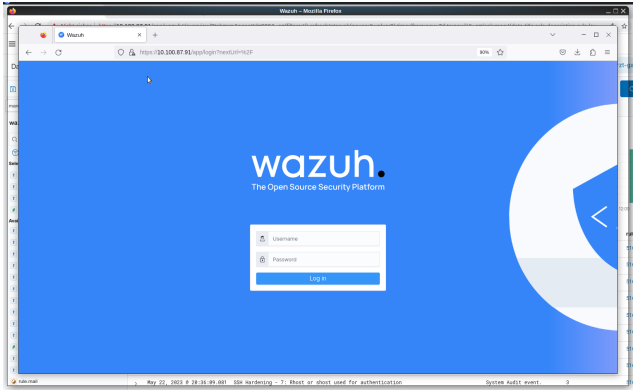
alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)
4. Amazon Machine Images (AMI)
5. Deployment on Docker
6. Deployment on Kubernetes
7. Offline Installation

alternative Installationsvarianten

1. ansible
2. puppet
3. Virtual Machine (OVA)
4. Amazon Machine Images (AMI)
5. Deployment on Docker
6. Deployment on Kubernetes
7. Offline Installation
8. From sources

Praktischer Teil / Wazuh Test-Installation



Schlussfolgerungen

- Ich habe `Active Response` unterschlagen
- Wazuh bringt viele Sachen mit, die aber auch aufwendig zu konfigurieren sind
- Wazuh kann im SOC (Security Operation Centre) eine Rolle spielen
- bei der Beschränkung auf das notwendige kann Wazuh für Kmus eine Möglichkeit sein, Ihr Sicherheitsbedürfnis zufrieden stellen zu können