



OPEN SOURCE SECURITY OPERATIONS

wazuh.

Security sichtbar machen. Risiken erkennen. Handlungsfähig bleiben.

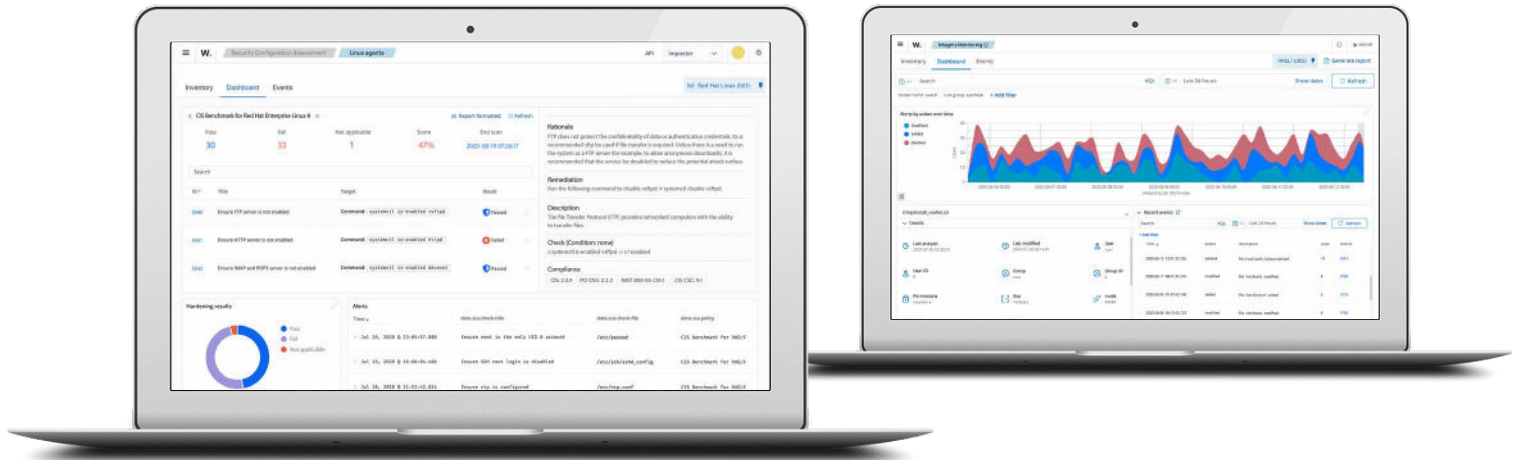
Cyberangriffe, neue regulatorische Anforderungen und wachsende IT-Komplexität stellen Unternehmen vor eine zentrale Frage:

Wie behalten Sie den Überblick über Ihre IT-Sicherheit – ohne immer mehr isolierte Tools einzuführen?

Wazuh schafft eine zentrale Sicht auf sicherheitsrelevante Ereignisse, Systeme, Schwachstellen und Konfigurationen: SIEM und XDR, Endpoint Monitoring, File Integrity Monitoring, Security Configuration Assessment, Vulnerability Detection und automatisierte Reaktionen – in einer Open-Source-Plattform.

Ob On-Premises, Cloud oder hybrid:

Wazuh integriert sich flexibel in bestehende IT-Landschaften und passt sich individuellen Security-Anforderungen an.



Warum wazuh?

Open Source – keine Lizenzkosten pro Agent oder Logvolumen, volle Kontrolle.

- ✓ **Zentrale Transparenz**
Events aus Endpoints, Servern, Netzwerk, Anwendungen und Cloud an einem Ort.
- ✓ **Bedrohungen erkennen**
regelbasierte Detection macht verdächtige Aktivitäten frühzeitig sichtbar.
- ✓ **Schwachstellen identifizieren**
Software- und Systemdaten werden automatisiert mit aktuellen CVEs abgeglichen.
- ✓ **Sicher konfigurieren**
Security Configuration Assessment prüft Systeme gegen CIS-Benchmarks.
- ✓ **Automatisiert reagieren**
Active Response löst definierte Gegenmaßnahmen aus – vom IP-Block bis zur individuellen Aktion.
- ✓ **Compliance unterstützen**
Mappings für PCI DSS, NIST, GDPR und weitere Frameworks; auch für ISO 27001 und NIS2 liefert Wazuh wertvolle technische Nachweise.

Eine Plattform. Viele Use Cases.

SIEM & XDR – Logs und Events aus Windows, Linux, Active Directory, Firewalls, Anwendungen und Cloud zentral korrelieren.

- ✓ **Endpoint Security**
Agent überwacht Systemaktivität, Inventar und Konfigurationsänderungen direkt am Endpunkt.
- ✓ **File Integrity Monitoring**
macht unerwartete Änderungen an kritischen Dateien und Verzeichnissen sichtbar.
- ✓ **Vulnerability Detection**
zeigt zentral, welche Systeme von bekannten CVEs betroffen sind.
- ✓ **Cloud & Container Monitoring**
bezieht AWS, Azure, Google Cloud, Microsoft 365, GitHub und Kubernetes-Workloads mit ein.



Von Daten zu echten Security Use Cases

Security Monitoring endet nicht beim Sammeln von Logs. Der Mehrwert entsteht, wenn daraus konkrete Detection- und Response-Prozesse werden – zum Beispiel bei einer ClickFix-Angriffskette:

1. Ereignis

Ein Nutzer führt nach einer gefälschten Verifizierungsaufforderung einen Befehl über die Windows-Ausführen-Funktion aus.

2. Korrelation

Wazuh verknüpft den ausgeführten Prozess mit dem Browser als Elternprozess und der Nutzeraktivität.

3. Detection

Eine Regel erkennt das ungewöhnliche Prozess-Verhältnis und die verdächtige Kommandozeile als typisches ClickFix-Muster.

4. Alert

Der Vorfall wird priorisiert und mit vollem Kontext dargestellt: Nutzer, Endpunkt, Kommandozeile.

5. Response

Eine automatisierte Gegenmaßnahme isoliert den Endpunkt oder beendet den Prozess.

Aus Logs werden Security Events. Aus Security Events werden Use Cases. Aus Use Cases wird handlungsfähige IT-Sicherheit.

wazuh + becon

Open Source bedeutet nicht: Do it yourself. Als Wazuh Gold Partner begleiten wir Sie von der ersten Evaluation bis zum produktiven Security-Betrieb.

✓ PoC & Assessment

Wazuh praxisnah in Ihrer eigenen Umgebung evaluieren.

✓ Architektur & Implementierung

vom kompakten Einstieg bis zur hochverfügbaren Plattform.

✓ Integration von Datenquellen

Windows, Linux, Active Directory, Firewalls, Cloud und weitere Systeme.

✓ Use Cases, Decoder & Rules

individuelle Detection statt unnötiger Alert-Flut.

✓ Security & Compliance

FIM, SCA und Vulnerability Detection als Bausteine für ISO 27001 und NIS2.

✓ Tuning & Betrieb

Performance, Retention und Detection Rules laufend optimiert – auch als Managed Platform.

✓ Training & Support

Know-how für Ihr Team, ergänzt durch direkten technischen Support.

Wazuh kennenlernen – ohne großes Projekt.

Sie möchten wissen, ob Wazuh zu Ihrer Infrastruktur passt? Starten Sie mit einem kompakten Proof of Concept: Wir bringen gemeinsam eine erste Wazuh-Umgebung zum Laufen, binden exemplarische Systeme an und zeigen anhand Ihrer Infrastruktur, welches Potenzial darin steckt.



Kontaktieren Sie uns! Wir beraten Sie gerne

Sie benötigen:

- ✓ Unterstützung bei der Einführung von Wazuh?
- ✓ Support für Ihre Wazuh-Umgebung?
- ✓ Beratung zum Thema Wazuh?

Oder stehen vor einer besonderen Herausforderung?
Unser engagiertes Team steht Ihnen für eine unverbindliche Beratung gerne zur Verfügung.

Jetzt Beratung vereinbaren



becon GmbH

Hauptstraße 8b

82008 Unterhaching



✉ info@becon.de

☎ +49 (0) 89608668-0

🌐 www.becon.de