

# Antivirus und Endpoint-Protection-Lösungen reichen nicht mehr aus?

System HACKED

## SIEM – Security Information and Event Management

Ein Sicherheitssystem, das alle netzwerkrelevanten Informationen und Meldungen überwacht, auswertet und über Angriffe informiert.

### Hauptaufgaben

- ✓ Archivierung der Eventdaten
- ✓ Bereitstellen von Echtzeitüberwachungsfunktionen
- ✓ Automatische Einleitung von Abwehrmaßnahmen
- ✓ Einhalten von Compliance-Vorschriften und Forensik-Grundlagen
- ✓ Durchführen von Analysen
- ✓ Korrelation von Ereignissen
- ✓ Erstellen von Business kritischen Berichten für Compliance und Kontrolle
- ✓ Managementkonsole: Überblick über den Sicherheitsstatus und versenden von Informationen

### Nutzen

- ✓ Sofortige Erkennung akuter Angriffe und Hilfe bei der Abwehr
- ✓ Visualisierung der Entwicklungen über lange Zeiträume (Bsp.: Nachvollziehen eines Hackerangriffs, Erkennung einer langsam antwortenden Datenbank)
- ✓ Bestmögliche Erfüllung von Compliance-Anforderungen
- ✓ Sicherheitsniveau im Unternehmen wird deutlich gesteigert

### S.I.E.M. Betriebsumgebungen

- ✓ m.a.x. cloud SIEM-as-a-Servie
- ✓ Hybrid Cloud
- ✓ On Premise

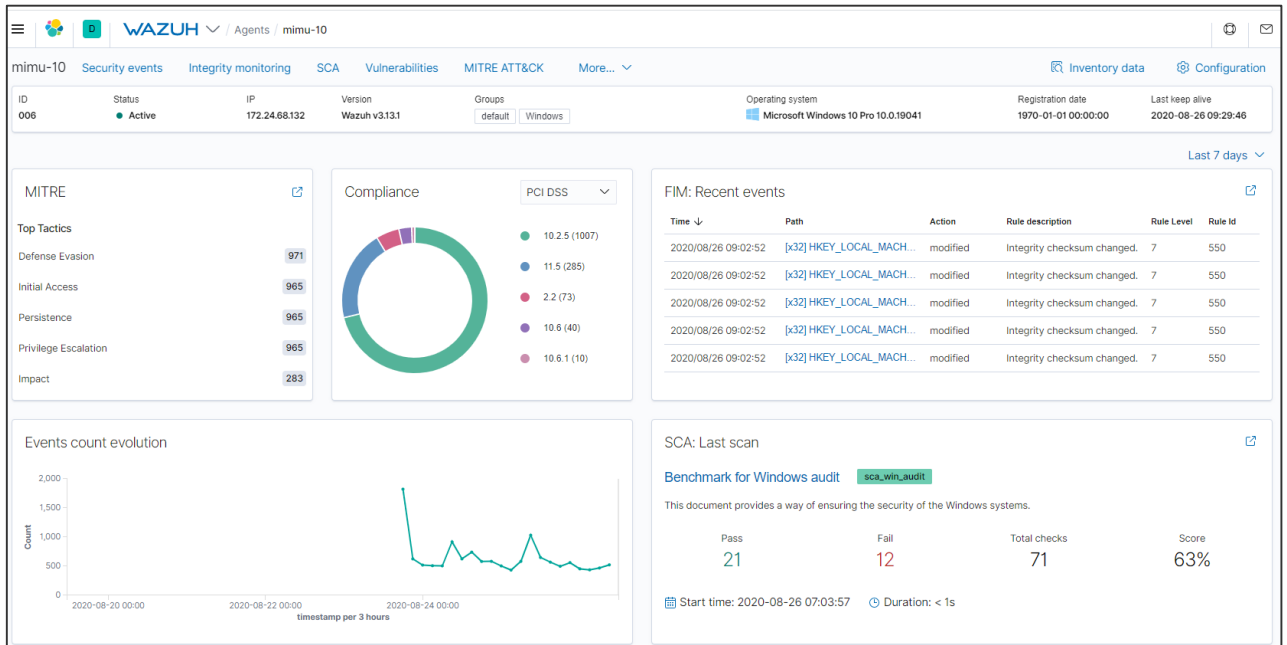
[www.max-it.de](http://www.max-it.de)

m.a.x. Informationstechnologie AG  
Landshuter Allee 12-14, 80637 München

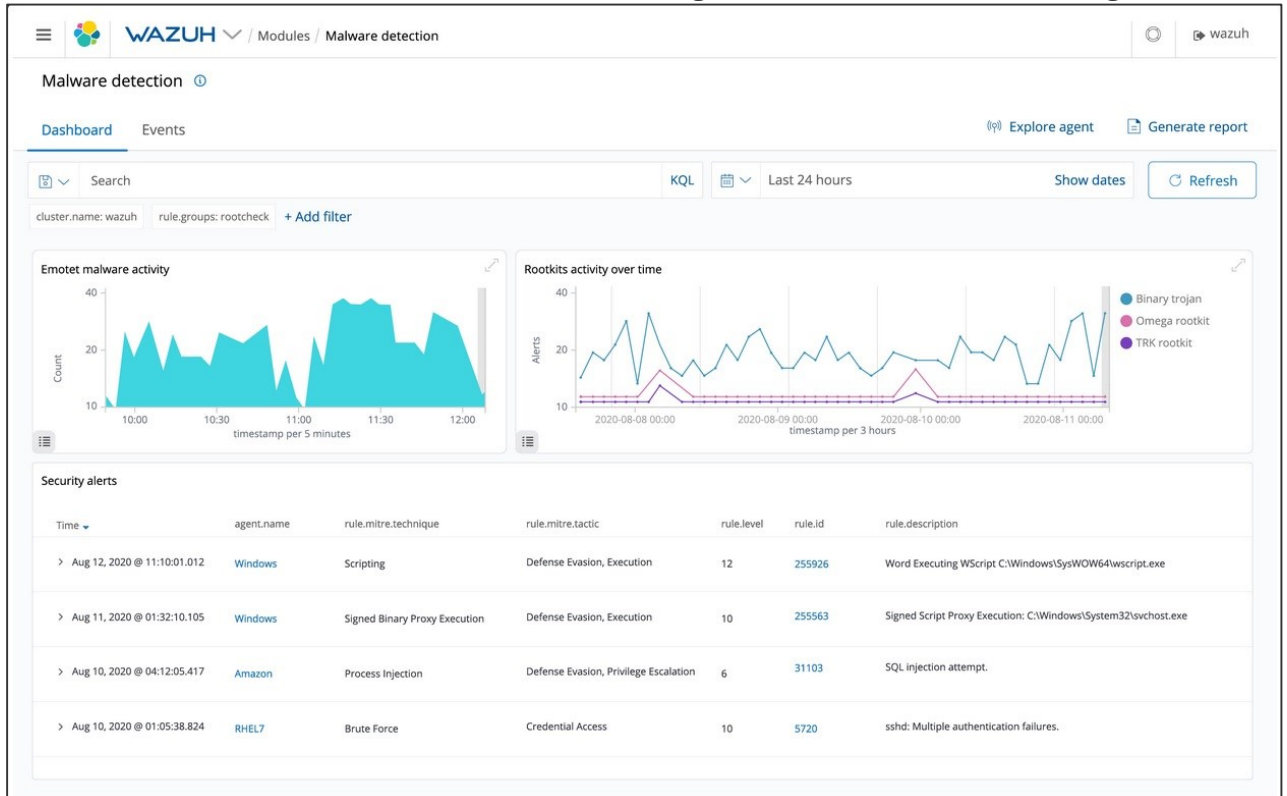
## Funktionsweise

- ✓ Mit Hilfe eines Syslog oder Agenten werden dem SIEM System die nötigen Log-Meldungen übermittelt. Zusätzlich zum zentralisierten Logging führt das SIEM System Protokollanalysen, Integritätsprüfungen, Windows-Registrierungsüberwachung, Rootkot-Erkennung, zeitbasierte Warnungen und optional aktive Antworten durch. Somit wird sofort anhand von Signaturen alarmgeschlagen, wenn ein Angriff stattfindet und kann so schnellstmöglich bekämpft und beseitigt werden.

## Managementkonsole: Detaillierter Einblick in Compliance-Themen wie z.B. Windowssicherheit



## Dashboard Malware Detection: Übersicht der erkannten und gebannten Mal- und Ransomware-Angriffe



Die m.a.x. it hilft Ihnen bei Konzeption, Design, Umsetzung und Implementierung.

Nehmen Sie Kontakt zu uns auf. Wir beraten Sie gerne.

Gilbert Flügl | Vertriebsmanager

Tel.: +49 (89) 54 26 26 - 133 | Mail: vertrieb@max-it.de