Unternehmensschutz:

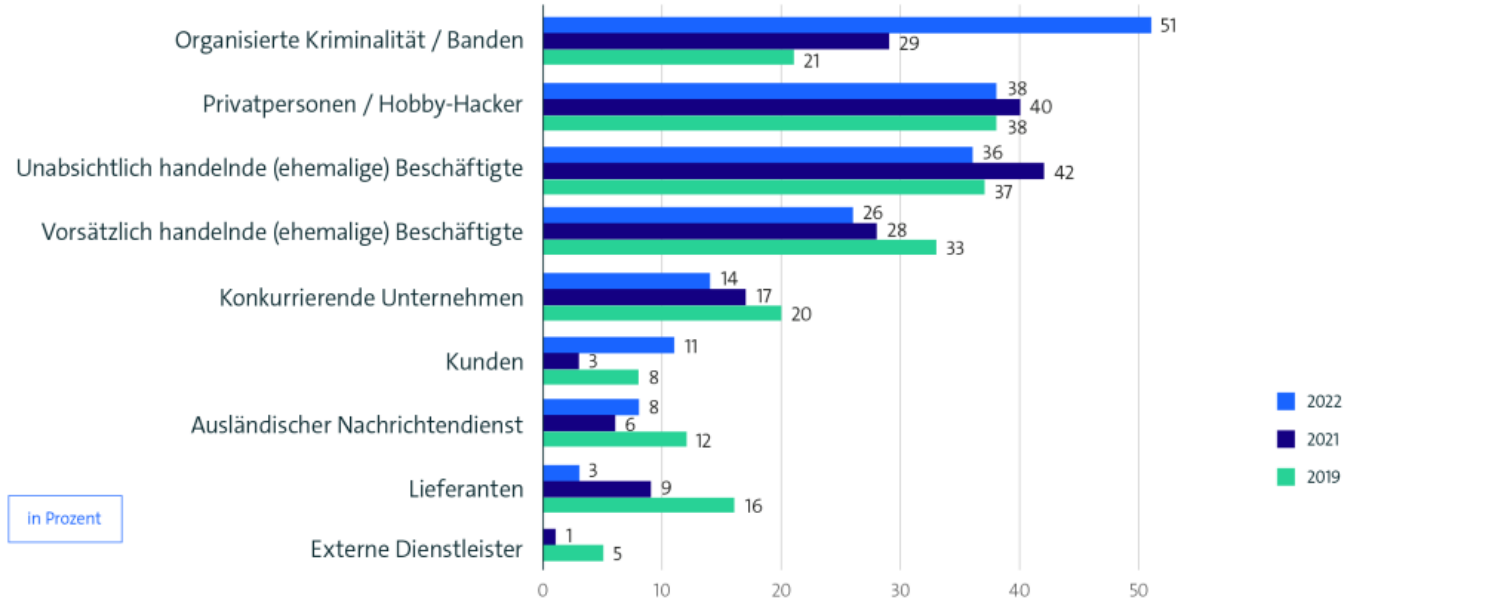
IT-Monitoring und Security Information and Event Management (SIEM) für den Mittelstand

DECOIT® GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
info@decoit.de

Statistiken zu Cyber-Attacken (1)

Attacken auf die Wirtschaft werden professioneller

Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?



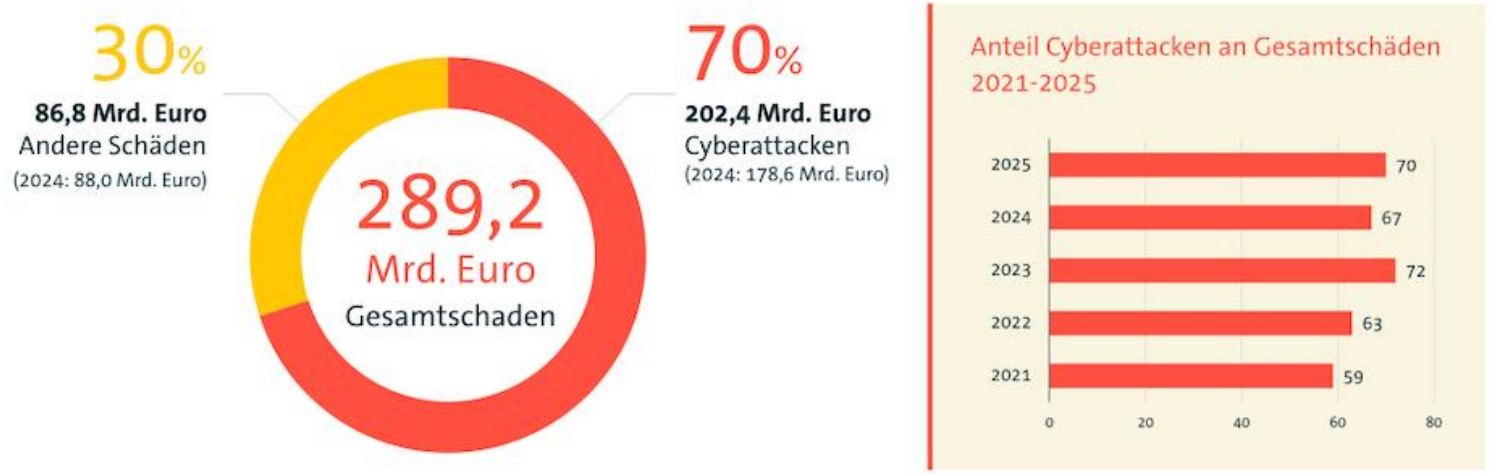
Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Statistiken zu Cyber-Attacken (2)

Großteil der Schäden entsteht durch Cyberattacken

Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Quelle: Bitkom Research 2025

bitkom

Erste Gegenmaßnahmen

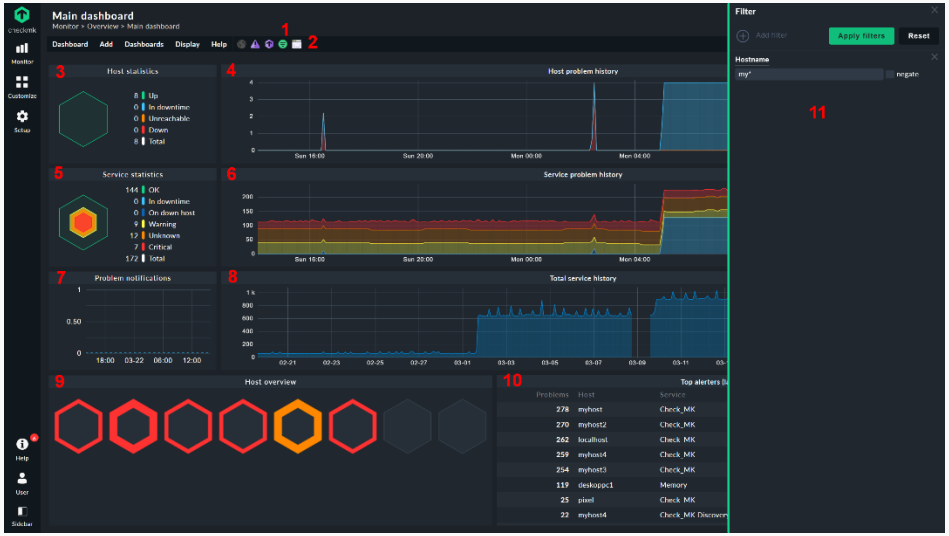
- Zur Absicherung wurden Access Control Lists (ACL) auf den Routern und Switches eingerichtet
- Statische Filter ließen sich allerdings nicht pflegen, weshalb diese später verbindungsabhängig (Stichwort: Stateful Inspection) in Firewalls umgesetzt wurden
- Application Ports wurden gesperrt, ohne den Datenverkehr zu analysieren
- Zur Anomalie-Erkennung wurden Intrusion Detection Systems (IDS) versucht einzuführen, ohne den administrativen Aufwand zu berücksichtigen
- Anti-Viren- und Anti-Spam-Systeme sind auf Basis von reiner Musterkennung im Einsatz

Einsatz von Überwachungssystemen

- Evolution der Überwachungs- und Regulierungssysteme:
  - **Netzmonitoring**: Überwachung der Verfügbarkeit und Netzdokumentation
  - **Network Access Control (NAC)**: Überwachung der Zugangskontrolle und Endgeräte-Dokumentation
  - **Security Information and Event Management (SIEM)**: Überwachung der IT-Sicherheit und Korrelation der Ereignisse (Vorfälle)
  - **Security Orchestration, Automation and Response (SOAR)**: Automatisiert und koordiniert die Reaktion auf Sicherheitsvorfälle

Netzmonitoring

- Ziel: Überwachung von Services und Serversystemen sowie Sammeln von Verfügbarkeitsstatistiken
- Aufgaben:
  - Einbindung von Netzwerk- und Serverkomponenten
  - Überwachung von Services (Diensten)
  - Eskalationsmanagement bei Alarmmeldungen (SMS, E-Mail)
  - Zusammenfassung von Alarmmeldungen
  - Unterscheidung unterschiedlicher Prioritäten

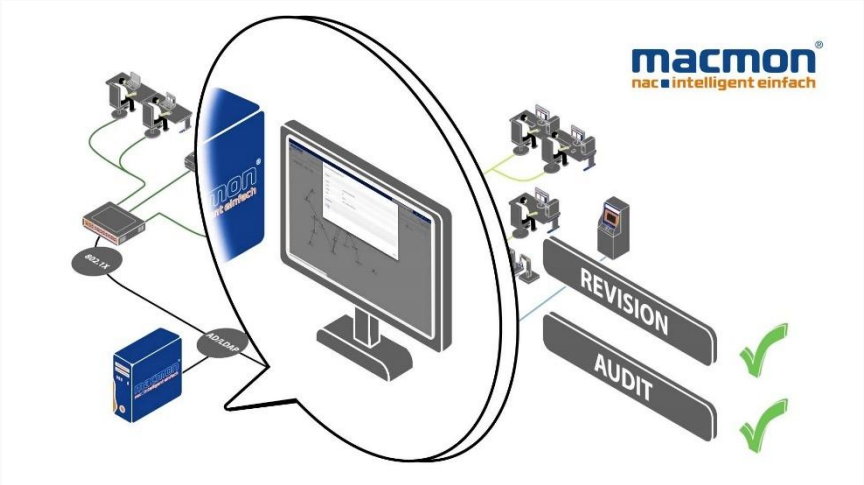


Netzmonitoring-Lösungen

- Nagios:
  - Quasistandard heutiger Monitoring-Lösungen
  - Bietet eine Sammlung von Modulen zur Überwachung des Netzwerks, der Hosts und bestimmter Dienste an
- Icinga:
  - Löste sich im Jahr 2009 als Fork von Nagios
  - Grund war die schleppende Entwicklung und fehlender Support
  - Die Weboberfläche wurde u.a. modernisiert
- Check_MK:
  - Ursprünglich seit 2009 reines Add-On für Nagios
  - Heute eigener leistungsfähiger Kern (komplette Monitoring-Lösung)
  - Wesentlich skalierbarer, performanter und einfacher zu konfigurieren

Network Access Control (NAC)

- Ziel: Zugangskontrolle von Systemen und Benutzern in Netzwerke
- Aufgaben:
  - Fremde Systeme erkennen
  - Auf Richtlinienkonformität überprüfen
    - Scan der installierten Programme
    - Scan der Sicherheitsupdates
  - Zugangsberechtigung erteilen oder verweigern
  - Verschieben von Systemen in bestimmte Netzwerke aufgrund der Richtlinien



NAC-Lösungen

- macmon secure:
  - BSI-zertifizierte NAC-Lösung
  - Herstellerunabhängig
  - Mischbetrieb mit und ohne 802.1X
  - Ermöglicht Compliance-Regeln einzusetzen
- PacketFence:
  - Open-Source-Lösung ohne Lizenzkosten
  - Ähnlich leistungsfähig wie Herstellerlösungen
  - Erkennen von Netzanomalien, proaktive Scans, Isolierung von problematischen Endgeräten

Security Information and Event Management (SIEM)

- Ziel: Gesamtübersicht über den Sicherheitsstatus des Netzwerkes bieten
- Aufgaben:
  - Sammeln sicherheitsrelevanter Informationen im Netzwerk
  - Bewerten dieser Informationen
  - Priorisierung der bewerteten Informationen
  - Meldungen über kritische Sicherheitslage geben
  - Handlungsempfehlungen bereitstellen

SIEM-Lösungen

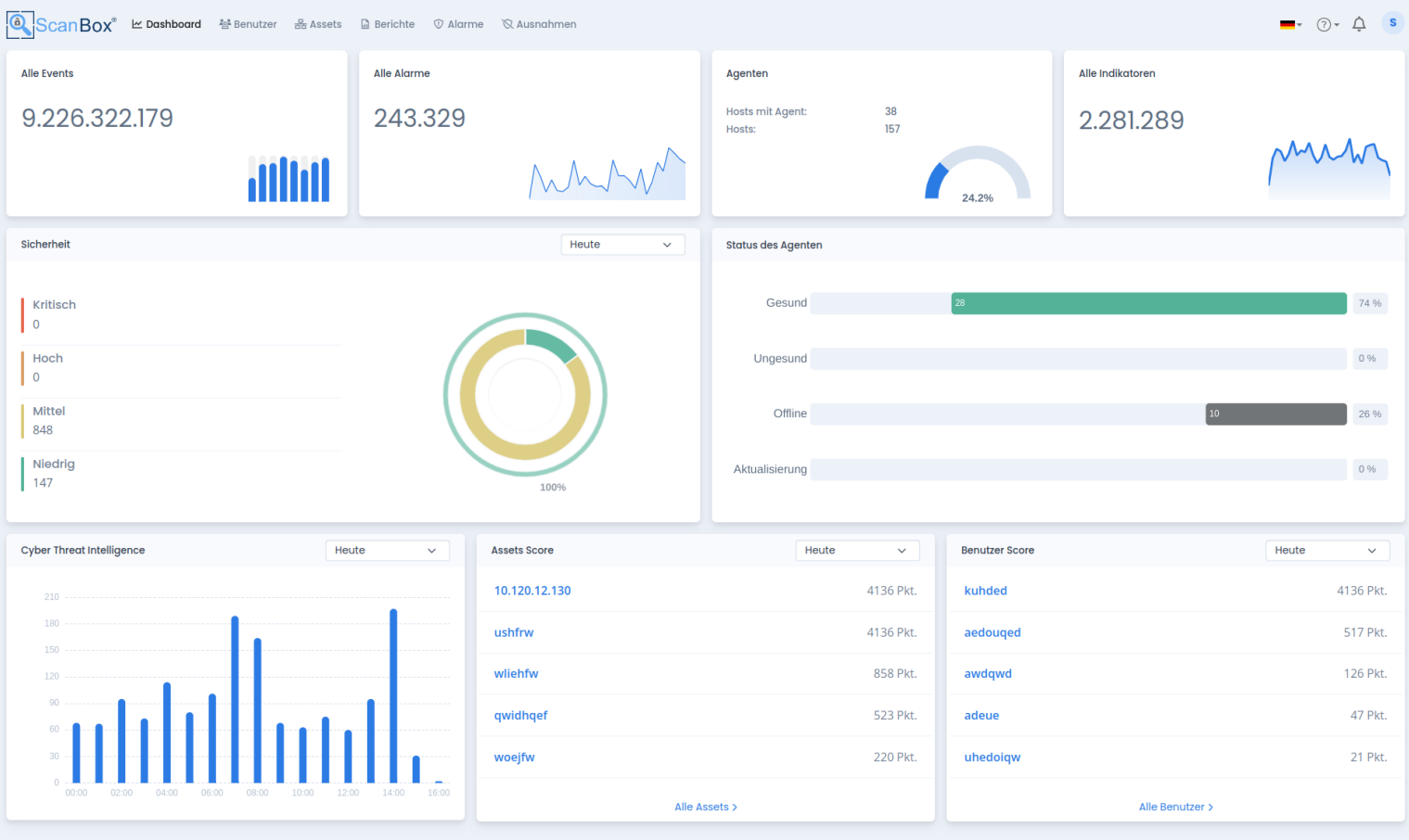
- LogRhythm:
  - Effizientes Pattern Matching
  - Dashboard ist anpassbar
  - Wahrscheinlichkeit für „False Positives“ ist angebbar
- OSSIM:
  - Ist als Open-Source-Lösung entwickelt worden
  - Wurde vom Hersteller AlienVault übernommen
  - Integriert andere Open-Source-Lösungen: OpenVAS, Snort, Nagios, Munin etc.

SIEM-Lösung ScanBox® (1)

- **Log- und Datensammlung:** erfasst und analysiert sämtliche Logs und Netzwerkdaten, um Anomalien zu erkennen und schnelle Reaktion auf Sicherheitsbedrohungen zu ermöglichen.
- **Cyber Threat Intelligence (CTI):** nutzt aktuelle Bedrohungsdaten, um verdächtige Muster zu identifizieren. Korreliert die Log- und Netzwerkdaten.
- **Sicherheitsanalyse von Assets, Benutzern und Alarmen:** bietet detaillierte Sicherheitsanalysen für einen umfassenden Überblick.
- **Regelmäßige Sicherheitsberichte:** erzeugt Sicherheitsberichte, die die aktuelle Bedrohungslage verständlich darstellen.

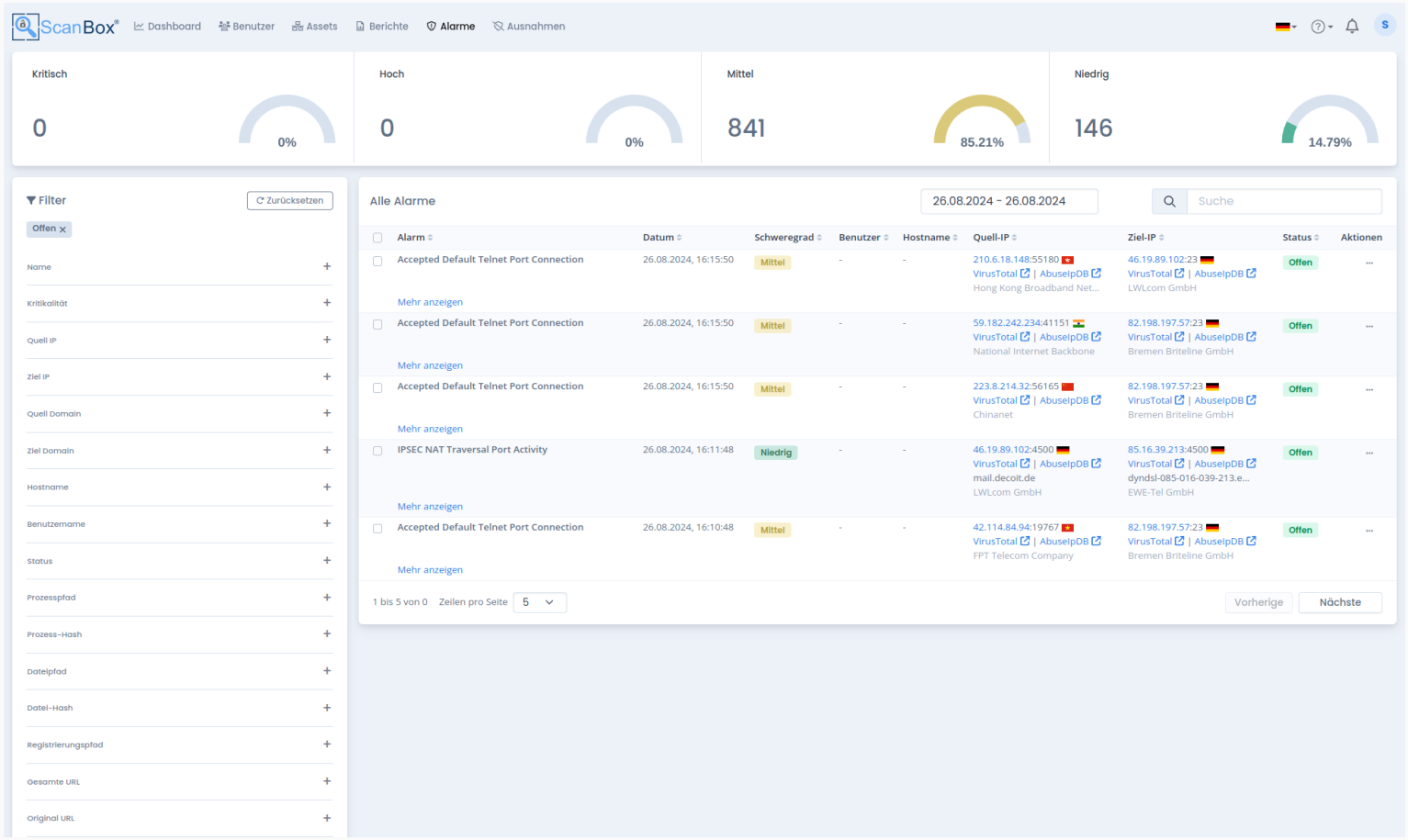
SIEM-Lösung ScanBox® (2)

- Dashboard-Übersicht:



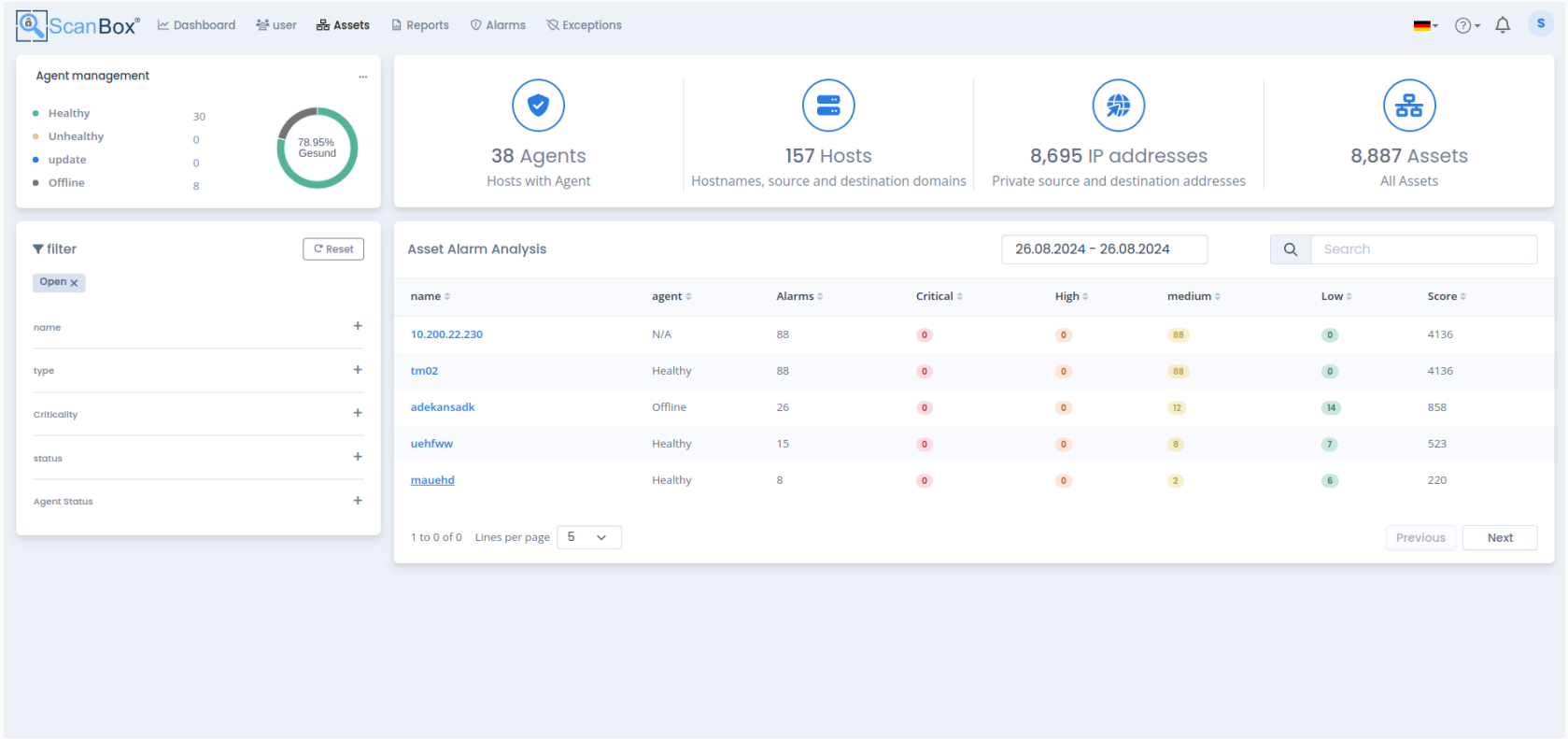
SIEM-Lösung ScanBox® (3)

- Übersicht über alle Alarme:



SIEM-Lösung ScanBox® (4)

- Übersicht über alle Assets:



IT-Sicherheit baut auf Open Source!

- Viele proprietäre Hersteller von IT-Sicherheitsprodukten nutzen heute Open-Source-Lösungen
- In manchen Bereichen haben sich dabei die Open-Source-Lösungen sogar durchgesetzt (Quasistandard)
  - VPN: OpenVPN
  - Firewall: pfSense / OPNsense
  - Anti-Viren-/Anti-Spam-Schutz: ClamAV / Rspamd
  - Proxy: Squid
  - Intrusion Detection Systeme: Snort / Suricata
  - Monitoring: Nagios / Icinga / Check_MK

Zusammenfassung

- Es gibt viele verschiedene Möglichkeiten, um pro-aktives Netzwerk- und Server-Monitoring zu betreiben
- SIEM-Systeme gehen einen Schritt weiter, indem sie die IT-Sicherheit mit einbeziehen und eine Risikoabschätzung ermöglichen
- Nicht alle SIEM-Systeme halten allerdings das, was sie versprechen!
- Man sollte sich von proprietären Systemen verabschieden und mehr auf offene Schnittstellen achten, um auch Drittsysteme einbinden zu können
- Open-Source-Lösungen besitzen daher einen entscheidenden Vorteil bei der Monitoring-/SIEM-Realisierung

Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de