ScanBox® für NIS-2

Sicherheitsmonitoring-Lösungen für Klein- und Mittelständische Unternehmen

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

Open Minds. Clear Strategies. Best Solutions.

Ausgangssituation bei KMUs

- KMU besitzen kein ausreichendes Fachpersonal, welches sich hinreichend mit Bedrohungspotenzialen auskennt
- Generelle IT-Kenntnisse werden bei KMU den Spezialkenntnissen vorgezogen
- IT-Sicherheit wird daher normalerweise vernachlässigt und nicht als integraler Geschäftsprozess gesehen
- Monitoring und Bewertung von Netzwerk- und Informations-Sicherheit haben aber heute Auswirkungen auf das Rating und den Wert von Unternehmen
- Gesetzgeberische und regulatorische Vorgaben erzwingen regelmäßige Kontrollen und Transparenz des vorhandenen Sicherheitsstandards
- Durch die NIS-2-Richtlinie sind nicht mehr nur KRITIS-Umgebungen betroffen

IT-Sicherheitsgesetz 2.0

- Mit dem IT-Sicherheitsgesetz (IT-SiG 2.0) sind zahlreiche Änderungen im BSI-Gesetz in Kraft getreten und damit die Anforderungen an die Cybersicherheit verschärft worden
- Gemäß § 8a Absatz 1a BSIG sind KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse verpflichtet, ab dem 1. Mai 2023 ein System zur Angriffserkennung umzusetzen
- Wie dieses System im Detail aussehen soll (IDS, IPS, SIEM, XDR, SOAR) wird offen gelassen
- Es gibt aber einen Maßnahmenkatalog, der beschreibt was ein solches Angriffserkennungssystem erfüllen sollte
- Die Anomalie-Erkennung wird als Methode genannt, aber nicht weiter spezifiziert

NIS-2-Richtlinie

- Die NIS-2-Richtlinie (EU 2022/2555) ist ein europäisches Gesetz zur Stärkung der Cybersicherheit, das am 16. Januar 2023 in Kraft trat und in Deutschland am 6. Dezember 2025 durch das NIS2UmsuCG verbindlich wurde
- Sie verpflichtet Unternehmen in „besonders wichtigen“ und „wichtigen“ Sektoren zu strengen Sicherheitsmaßnahmen, Risikomanagement und Meldepflichten, wobei Bußgelder bis zu 10 Mio. € oder 2% des Umsatzes drohen
- Einrichtungen mit mindestens 50 Mitarbeitern oder über 10 Mio. € Jahresumsatz in Sektoren wie Energie, Transport, Banken, Gesundheit, Wasser, digitale Infrastruktur und öffentliche Verwaltung sind betroffen
- Damit sind ca. 30.000 Unternehmen zusätzlich in Deutschland von dem Einsatz eines Angriffserkennungssystems betroffen!

NIS-2-Umsetzung

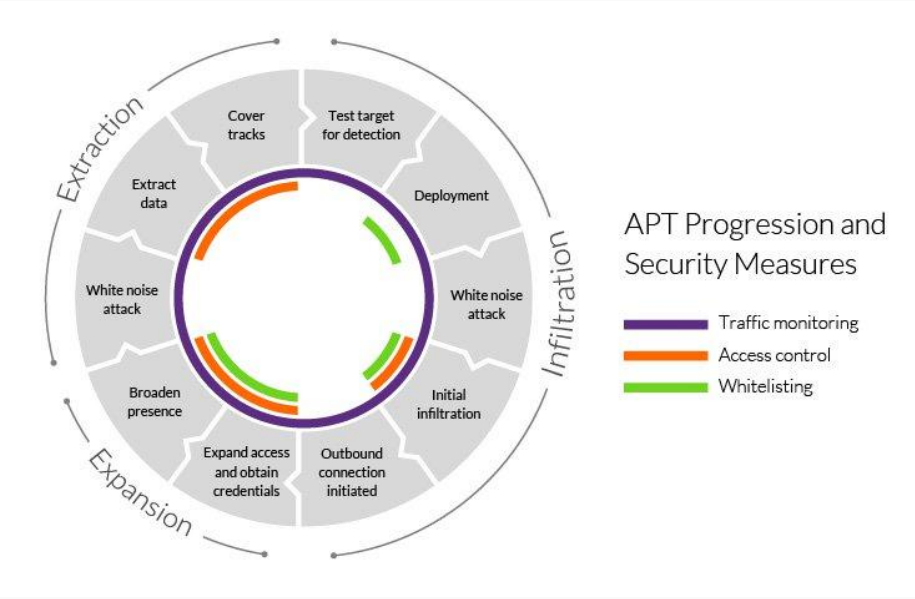
- **Maßnahmen:** Pflicht zur Umsetzung von Risikomanagementmaßnahmen wie Sicherheitskonzepten, Vorfallbewältigung, Lieferkettensicherheit, Verschlüsselung und Krisenmanagement
- **Meldepflichten:** Erhebliche Sicherheitsvorfälle müssen unverzüglich (innerhalb von 24h eine Frühwarnung) an das BSI gemeldet werden → das geht nur durch ein SIEM-System!
- **Registrierung:** Betroffene Unternehmen müssen sich im BSI-Portal mit einem ELSTER-Organisationszertifikat registrieren
- **Verantwortlichkeit:** Die Geschäftsführung ist direkt für die Einhaltung der Cybersicherheitsmaßnahmen verantwortlich und haftbar

NIS2- und IT-SiG2.0-Umsetzungen

- Um das IT-Sicherheitsgesetz (IT-SiG 2.0) zu erfüllen lassen sich verschiedene Strategien beschreiben
  - Einsatz eines SIEM/SOAR-Systems mit eigenem Fachpersonal
  - Einsatz eines SIEM/SOAR-Systems mit Unterstützung eines Security Operation Centers (SOC) des Anbieters
  - Einsatz eines SIEM/SOAR-Systems mit KI-basierter Angriffserkennung und automatisierten Gegenmaßnahmen
- Die letztgenannte Möglichkeit ist in OT-Netzen nicht umsetzbar bzw. erwünscht
- Trotzdem bieten Hersteller (z.B. CrowdStrike) solche Möglichkeiten an

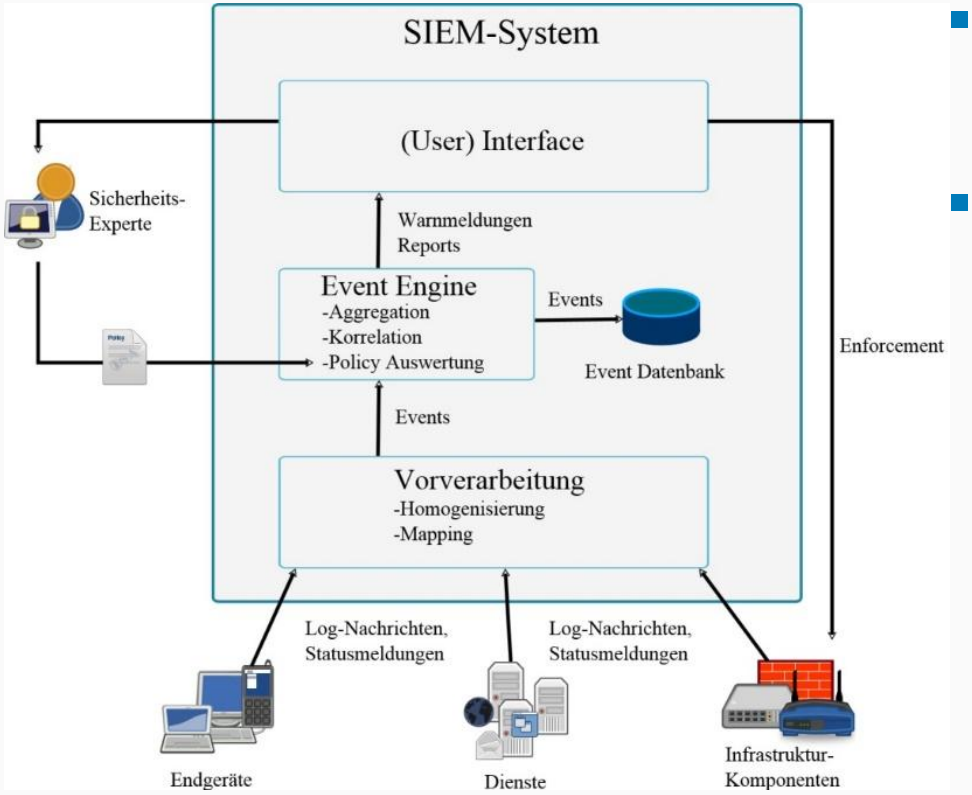
Advanced Persistent Threat (APT)

- APT ist ein komplexer, zielgerichteter Cyber-Angriff
- Der Angriff ist darauf ausgelegt über einen längeren Zeitraum hinweg unbemerkt im Zielsystem zu bleiben
- Schwachstellen des Zielsystems sollen auskundschaftet werden
- APTs sind schwer zu erkennen, da sie keinen unmittelbaren Alarm in Sicherheitssystemen auslösen
- Sie lassen sie sich durch die Nutzung von KI einfacher enttarnen, als durch den Sicherheitsexperten



Quelle: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

SIEM-Schwerpunkte



- Ziel: Gesamtübersicht über den Sicherheitsstatus des Netzwerkes bieten
- Aufgaben:
  - Sammeln sicherheitsrelevante Informationen im Netzwerk
  - Bewerten der Vorfälle anhand eines Sicherheitsexperten und mittels KI
  - Priorisierung der bewerteten Informationen
  - Meldungen über kritische Sicherheitslage geben
  - Handlungsempfehlungen bereitstellen

Nutzung von KI-Algorithmen

- SIEM-Systeme nutzen KI-Algorithmen auf verschiedene Weise, um Angriffe zu erkennen:
  - **Verhaltensanalyse:** SIEM-Systeme können KI-Algorithmen verwenden, um das normale Verhalten von Benutzern, Geräten und Anwendungen in einem Netzwerk zu modellieren
  - **Bedrohungsintelligenz:** KI-Algorithmen können dabei helfen, große Mengen von Bedrohungsdaten zu analysieren, um relevante Informationen zu identifizieren
  - **Automatisierung von Reaktionen:** Moderne SIEM-Systeme integrieren oft automatisierte Reaktionen auf Bedrohungen
  - **Erkennung von unbekannten Bedrohungen:** KI-Algorithmen sind auch in der Lage, Anomalien zu erkennen, die auf bislang unbekannte Bedrohungen hinweisen könnten

Cyber Threat Intelligence (CTI)

- Durch die CTI-Nutzung können potenzielle Gefahren erkannt und abgewendet werden
  - CTI beinhaltet die kontinuierliche Sammlung von Informationen über potenzielle Cyberbedrohungen aus verschiedenen Quellen
  - Die gesammelten Daten werden analysiert und bewertet
  - Schwachstellen und Angriffsmuster sollen besser erkannt werden
  - CTI-Plattformen erstellen Bedrohungsmeldungen, die von SIEM-Systemen eingelesen werden können (sog. Threat-Feeds)
- Die CTI-Datenbank dient dazu, bereits bekannte Bedrohungsindikatoren von außerhalb zu erhalten, um neue interne Angriffe besser identifizieren zu können
- Die gewonnenen Erkenntnisse werden in verständlicher Form zusammengefasst → Handlungsempfehlungen

ScanBox® -Version 1.x

- Die Basis wurde in verschiedenen F&E-Projekten geschaffen
- In der Version 1.x kam noch eine Appliance zum Einsatz, die ausschließlich auf Netzwerkdaten ausgerichtet war
- Ursprüngliches Ziel war ein zeitbefristetes Sicherheitsmonitoring einzuführen, um eine automatische Analyse durchführen zu können
- Ab der Version 2.0 wurden dann Logs von Client/Servern hinzugefügt, wodurch der Speicherbedarf nochmals stieg

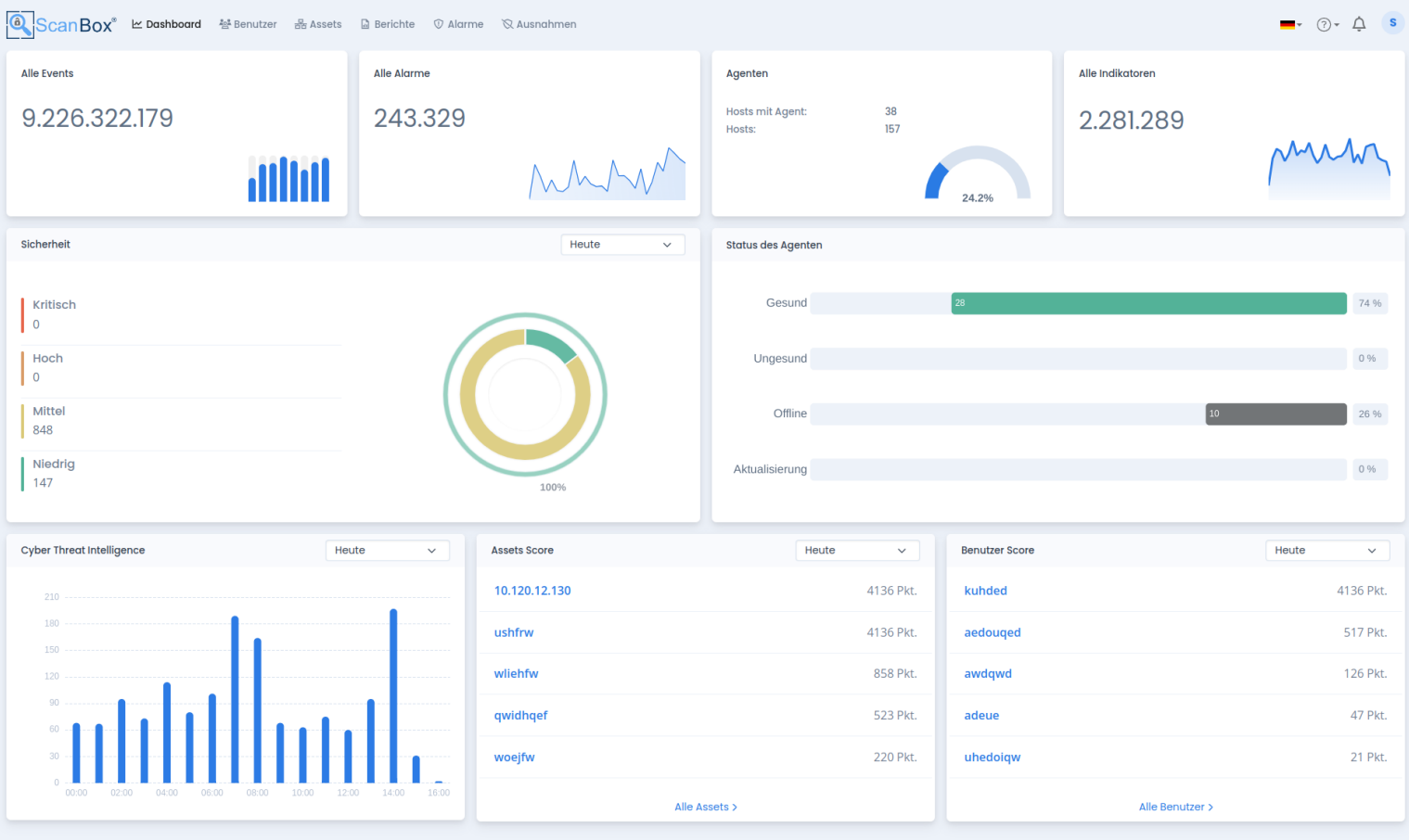
Quelle: https://www.telco-tech.de/produkte/scanbox/

SIEM-Lösung ScanBox® 2.0 (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.

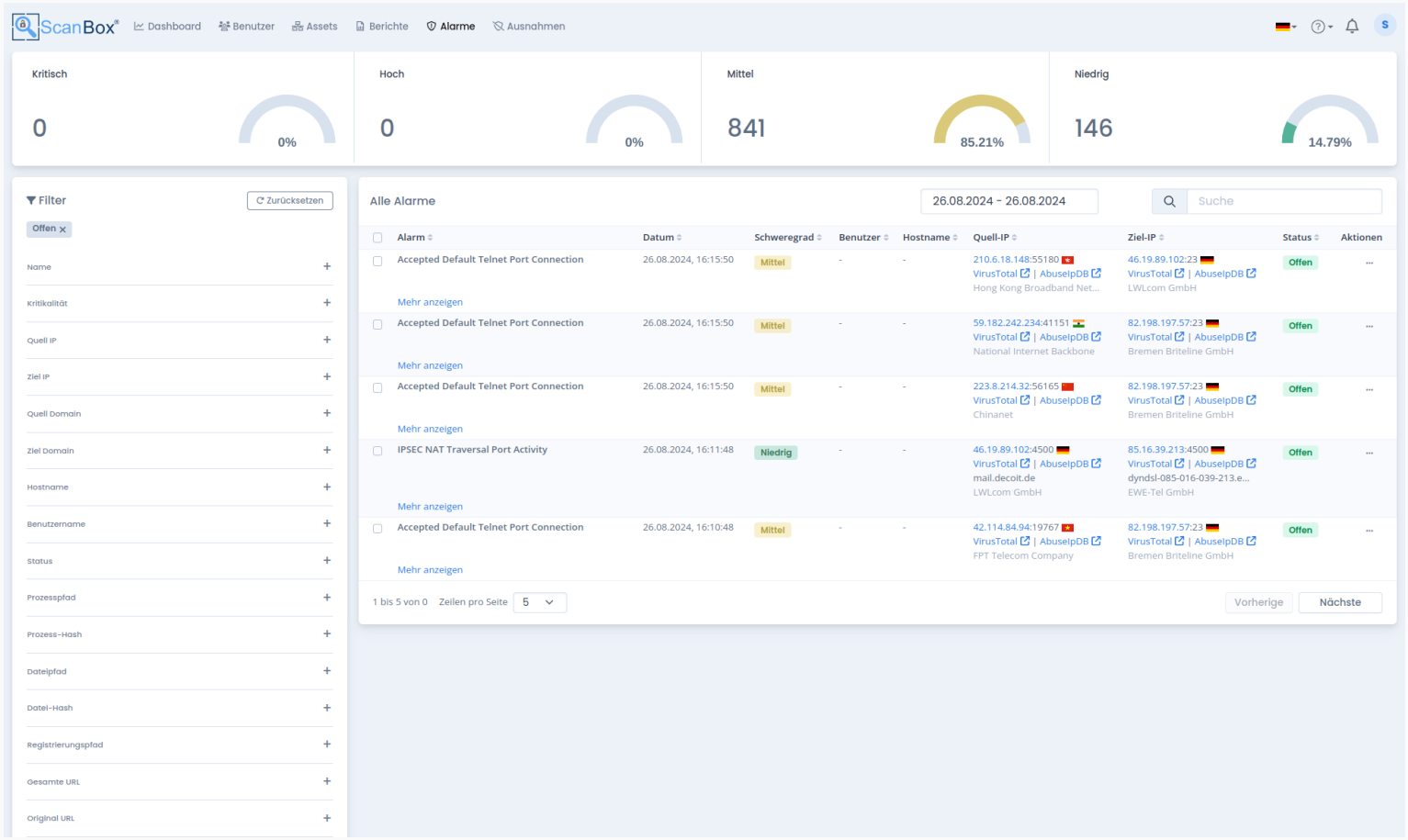
SIEM-Lösung ScanBox® 2.0 (2)

- Dashboard-Übersicht:



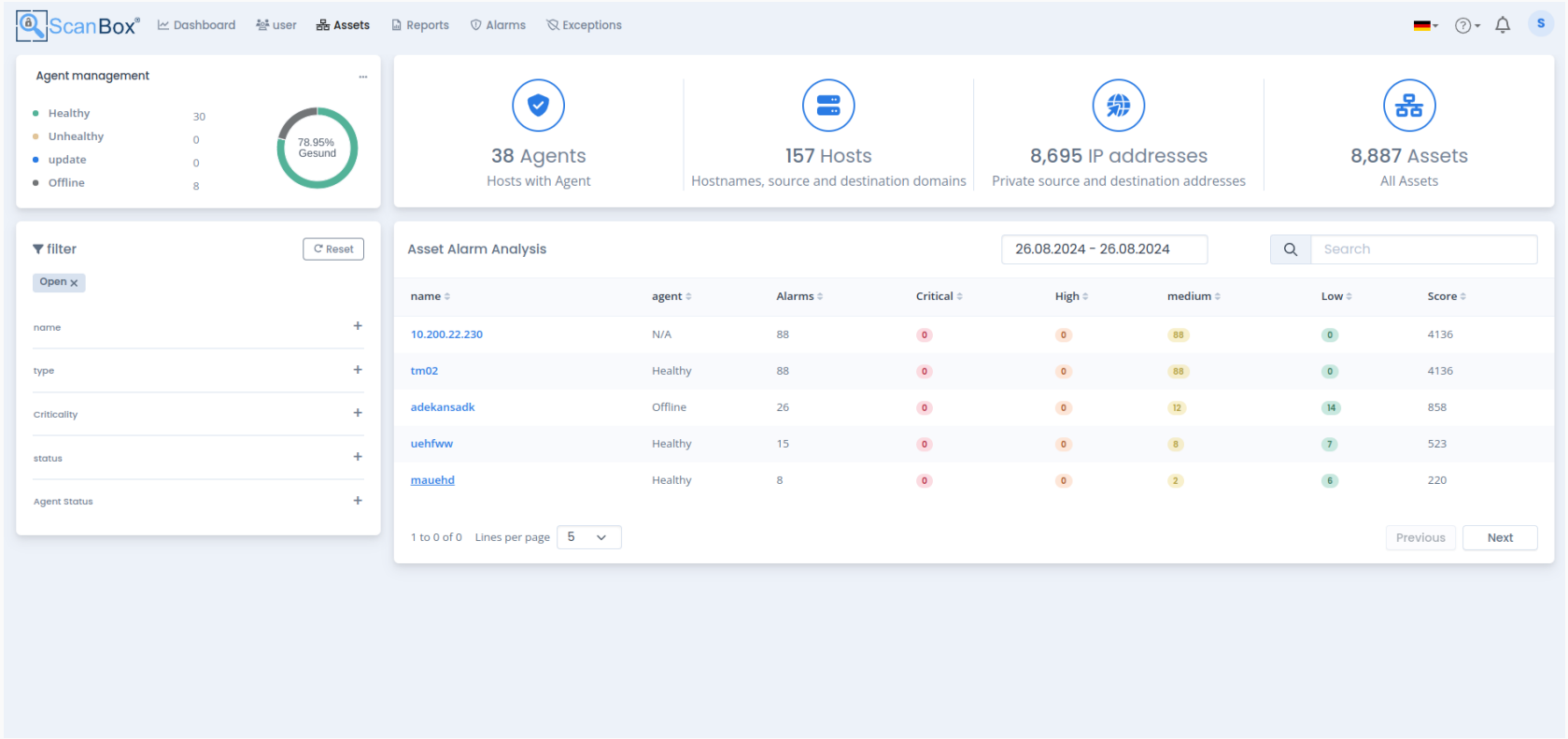
SIEM-Lösung ScanBox® 2.0 (3)

- Übersicht über alle Alarme:



SIEM-Lösung ScanBox® 2.0 (4)

- Übersicht über alle Assets:



ScanBox®-Kosten

- Kosten (einmalig)
  - Hardware
    - Virtuelle Maschinen (vom Kunden)
  - Installation
    - Netflow/Firewall-Logs
    - bis zu 5 Agenten
- Kosten (kontinuierlich)
  - Konfiguration
  - Alarm-Analyse
  - Updates
  - Rollout neuer Agenten

Zusammenfassung

- Die ScanBox® ermöglichen es, dass das interne Netz kontinuierlich auf Schwachstellen analysiert werden kann
- Die enthaltene regelbasierte Anomalie-Erkennung kann durch KI-Analyse nach Bedarf erweitert werden (über Lizenzen)
- Weiterentwicklungen (neue Leistungsmerkmale) werden durch Maintenance-Verträge kostenfrei zur Verfügung gestellt
- Ein kontinuierlicher Support während der Geschäftszeit der DECOIT® ist dabei mit enthalten (Lightweight SOC)
- Mit der NIS-2-Richtlinie werden auch mittlere Unternehmen gezwungen sich mit dieser Thematik auseinanderzusetzen
- Mit der ScanBox® kann ein Teilbereich von NIS-2 erfüllt werden

Vielen Dank für Ihre Aufmerksamkeit!

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

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