NIS2-Regelung der EU:

Herausforderungen der Cybersicherheit meistern

© DECOIT GmbH & Co. KG

NIS2-Regelung:

SIEM-Systeme zur Anomalie- und Angriffserkennung

Prof. Dr. Kai-Oliver Detken
DECOIT GmbH & Co. KG
Fahrenheitstraße 9, D-28359 Bremen
https://www.decoit.de
detken@decoit.de

© DECOIT GmbH & Co. KG

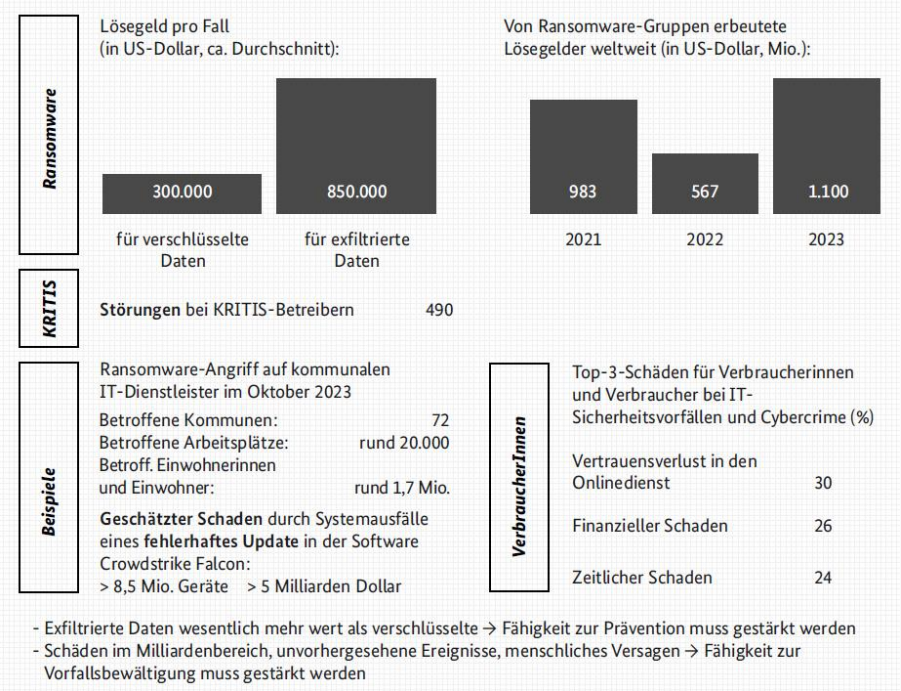
Bremer Systemintegrator und Softwarehaus

- **IT-Consulting**: ganzheitliche sowie herstellerneutrale Beratung
- **System Management**: Optimierung technischer Arbeitsabläufe, Integration von Hersteller- oder Open-Source-Lösungen in vorhandene Umgebungen
- **Software-Entwicklung**: Entwicklung von Individualsoftware, Anpassung bestehender Open-Source-Software an Kundenbedürfnisse
- **IT-Forschungsprojekte**: innovative IT-Lösungen
- **Produktentwicklung**: innovative Produkte auf Basis von F&E-Projekten

© DECOIT GmbH & Co. KG

BSI-Lagebericht 2024: Aktuelle Schadwirkung

- Die Zahl der Ransomware-Angriffe stieg deutlich an
- Angreifer nutzen Zero-Day-Schwachstellen
- Pro Tag werden 78 neue Schwachstellen in Software-Produkten bekannt
- Die Lage der IT-Sicherheit in Deutschland bleibt angespannt
- Opfer waren überwiegend KMU, IT-Dienstleister und Kommunen



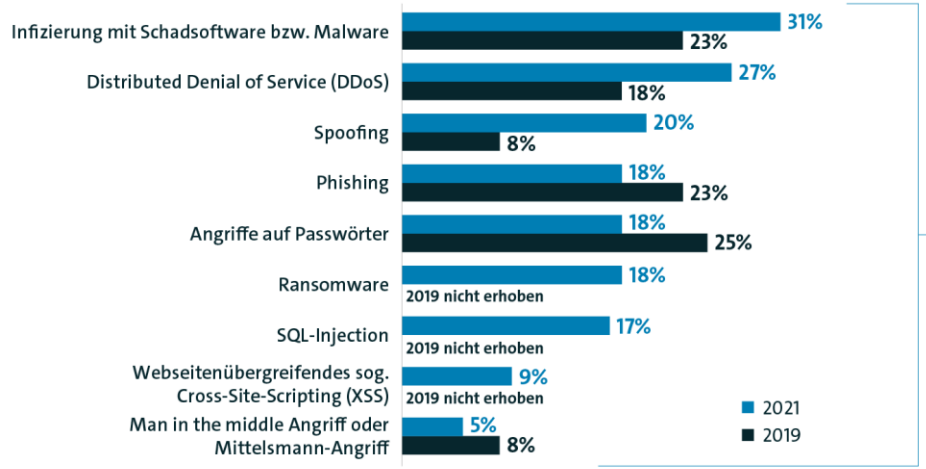
Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024-Doppelseite.pdf?__blob=publicationFile&v=3

© DECOIT GmbH & Co. KG

Status von Cyberangriffen

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

bitkom

© DECOIT GmbH & Co. KG

NIS2-Richtlinie

- Die NIS-2-Richtlinie setzt ab Oktober 2024 erhöhte Cybersicherheitsstandards für bestimmte Unternehmen in der EU
- Sie gilt für Firmen ab 50 Mitarbeitenden und 10 Mio. Euro Umsatz in 18 festgelegten Sektoren
- Zur Erfüllung der NIS-2-Richtlinie empfiehlt sich die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001
- Zur technischen Umsetzung ist ein System zur Angriffserkennung (SzA) zu empfehlen

© DECOIT GmbH & Co. KG

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)
  - **Endpoint Detection and Response (EDR)**: Überwachung von Endgeräten bzgl. IT-Sicherheit und Anomalien (AV-Weiterentwicklung)
  - **Security Orchestration, Automation and Response (SOAR)**: Automatisiert und koordiniert die Reaktion auf Sicherheitsvorfälle

© DECOIT GmbH & Co. KG

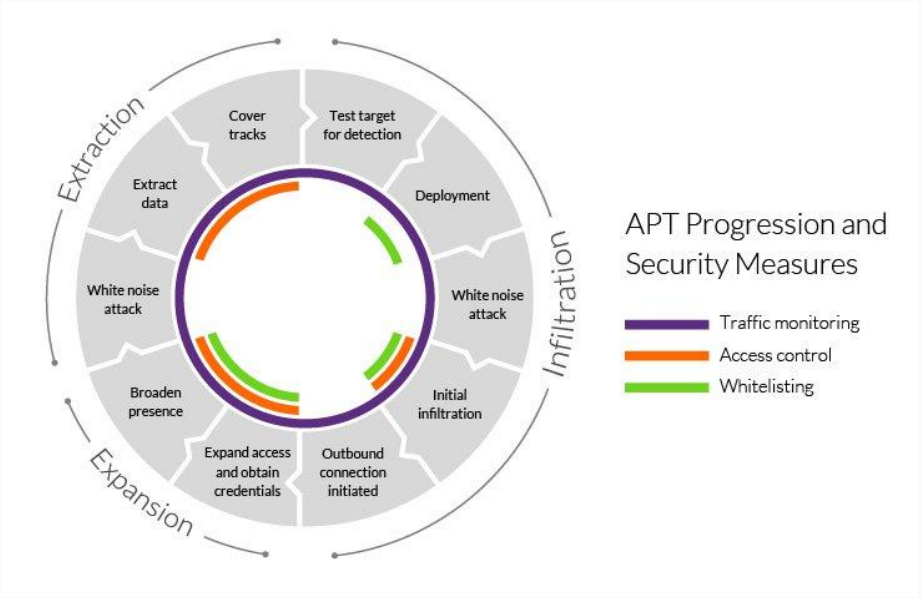
NIS2- und IT-SiG2.0-Anforderungen

- Um das IT-Sicherheitsgesetz (IT-SiG 2.0) und NIS2 erfüllen zu können lassen sich verschiedene Strategien nutzen:
  - 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

© DECOIT GmbH & Co. KG

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

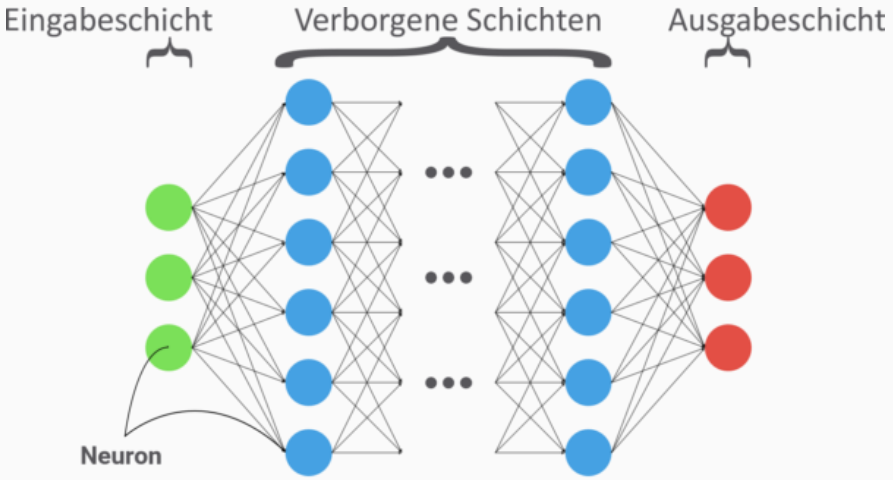


Quelle: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

© DECOIT GmbH & Co. KG

Was bedeutet KI überhaupt?

- Generell spricht man bei Machine Learning (ML) von Verfahren, die es erlauben anhand bestimmter Merkmale Dinge zu klassifizieren und zu erwartende Ergebnisse zu extra- bzw. interpolieren
- Dafür werden Neuronale Netze (NN) verwendet, die es erlauben aus dem Dateninput über synapsenartige Verschaltungen wahrscheinliche Ergebnisse vorherzusagen
- Dabei gilt: je kleiner der Datensatz ist, umso unwahrscheinlicher ist es, dass die NN-Ausgabe korrekt ist!
- Das NN besteht aus einem Algorithmus, dem ein Entscheidungsbaum antrainiert werden kann (z.B. TensorFlow)
- Sie bilden die Grundlage für das Deep Learning

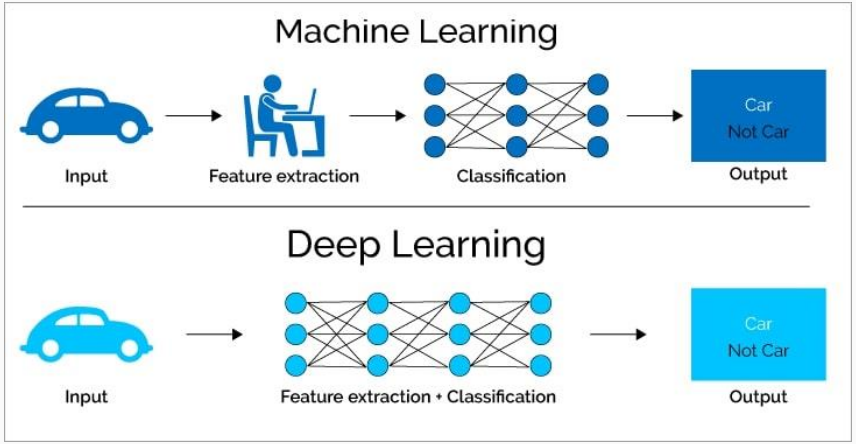


Quelle: https://nativdigital.com/neuronale-netze/

© DECOIT GmbH & Co. KG

Deep Learning

- Deep Learning ist eine spezielle Art des maschinellen Lernens, um Muster und Zusammenhänge in großen Datenmengen zu erkennen
- Deep Learning wird zunehmend in der Cybersicherheit eingesetzt, um fortschrittliche Angriffe wie APT-Angriffe zu erkennen, zu analysieren und abzuwehren:
  - Erkennen von Anomalien
  - Malware-Erkennung
  - Verhaltensanalyse
  - Vorausschauende Bedrohungsinformationen
  - Automatisierung von Sicherheitsmaßnahmen



Quelle: https://levity.ai/blog/difference-machine-learning-deep-learning

© DECOIT GmbH & Co. KG

Nutzung von KI-Algorithmen bei SIEM-Systemen

- 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.
- Grundsätzlich werden nicht verschiedene Algorithmen genutzt, sondern verschiedene Datensätze verwendet.

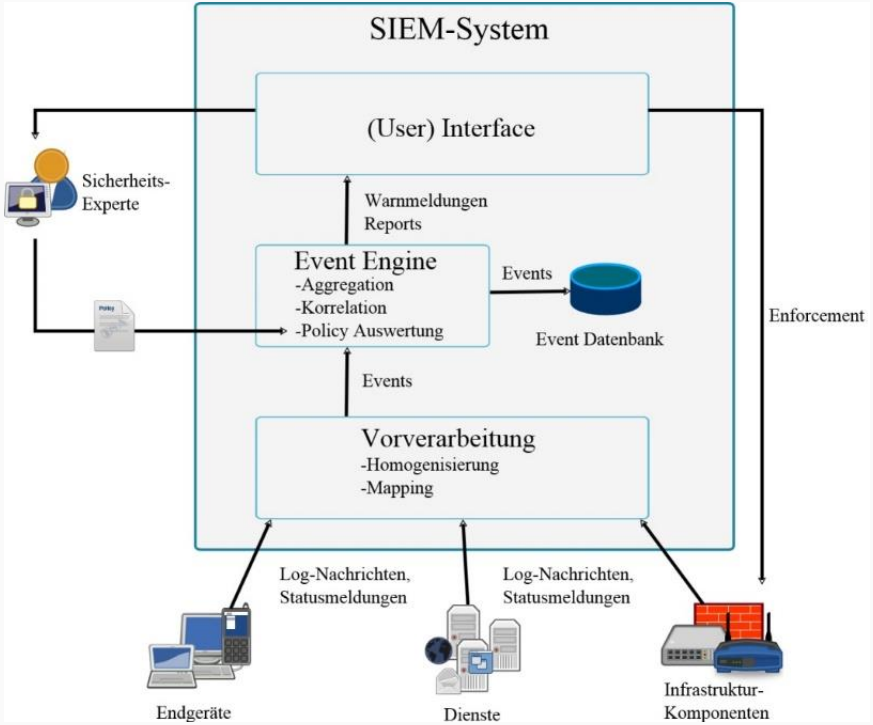
© DECOIT GmbH & Co. KG

KI-Alternative/-Ergänzung: 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

© DECOIT GmbH & Co. KG

Funktionsweise eines SIEM-Systems



- 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

© DECOIT GmbH & Co. KG

ScanBox-Version 1.x

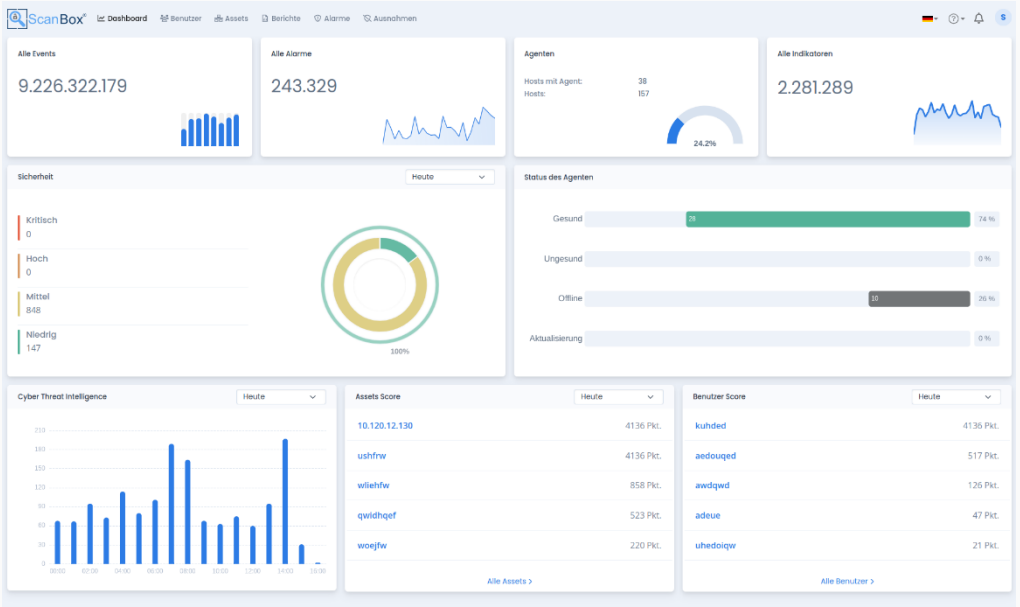
- Die Basis wurde in verschiedenen F&E-Projekten geschaffen
- In der Version 1.x kam noch eine Appliance zum Einsatz, die ausschließlich auf Netzwerkdaten ausgerichtet war
- Ursprüngliches Ziel war ein zeitbefristetes Sicherheitsmonitoring einzuführen, um eine automatische Analyse durchführen zu können
- 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/

© DECOIT GmbH & Co. KG

ScanBox 2.0 – Hauptfunktionalität

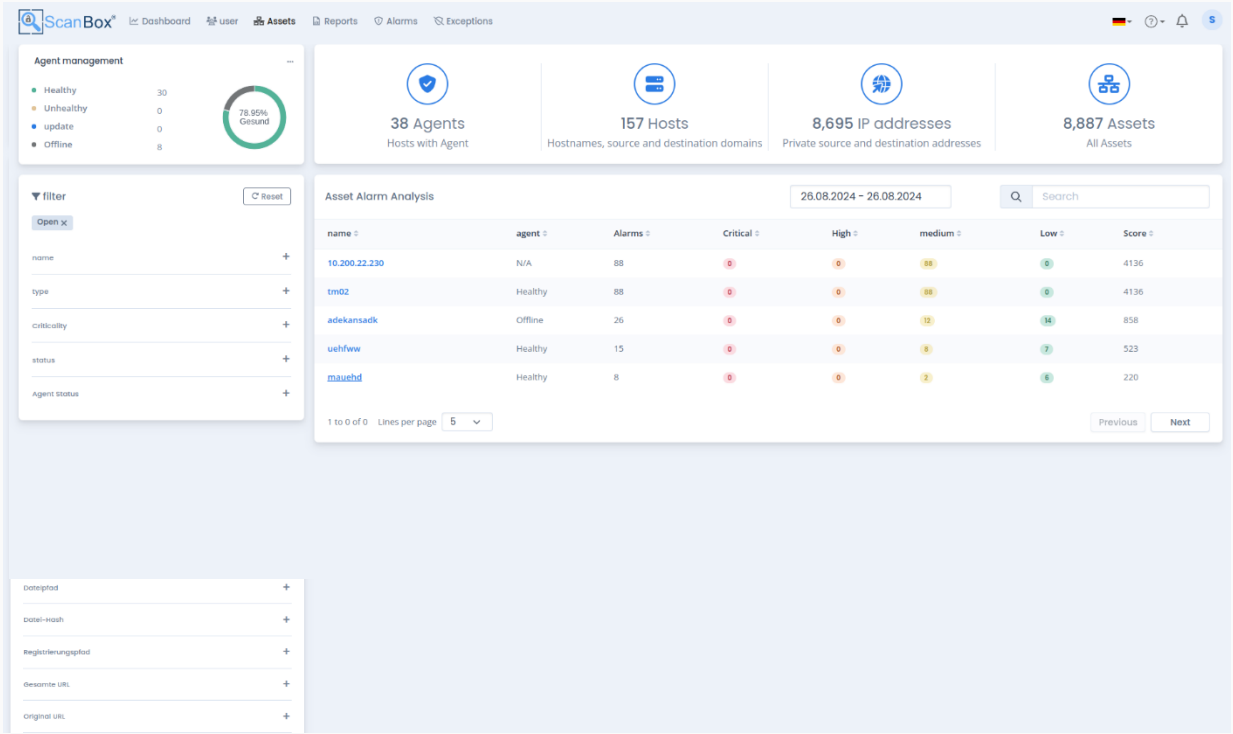
- Log- und Netzwerkdaten werden gesammelt
- Nutzt Cyber Threat Intelligence (CTI)
- Bietet Sicherheitsanalysen bezogen auf Assets, Benutzer und Alarme
- Regelmäßige Sicherheitsberichte
- Optional: es kann KI-Funktionalität zusätzlich lizensiert werden



SIEM-System der DECOIT®: https://www.scanbox-product.de

© DECOIT GmbH & Co. KG

ScanBox 2.0 – Alarme und Assets



- Einfaches Management der Agenten
- Einfaches Sicherheitsanalysetool für IT-Administratoren
- Erkennen auffälliger Benutzer und Assets

© DECOIT GmbH & Co. KG

ScanBox 2.0 – 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

© DECOIT GmbH & Co. KG

Ausblick

- Schreiben neuer Elastic-Agenten, falls noch nicht verfügbar (Beispiel: WithSecure-Einbindung)
- Anbindung von NAC-Systemen wie macmon secure und damit Weiterentwicklung zu einem SOAR-System
- Schwachstellenmanagement implementieren durch freie Datenbanken vom NIST
- KI-Intelligenz einbetten, als Copilot-Prozess (Support bei Alarmen, Regeln und Vorfällen)

© DECOIT GmbH & Co. KG

Vielen Dank für die Aufmerksamkeit!

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

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

© DECOIT GmbH & Co. KG