IFIT Roundtable-Vortrag:

Die Ergebnisse des SEC-I4.0-Projekts

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

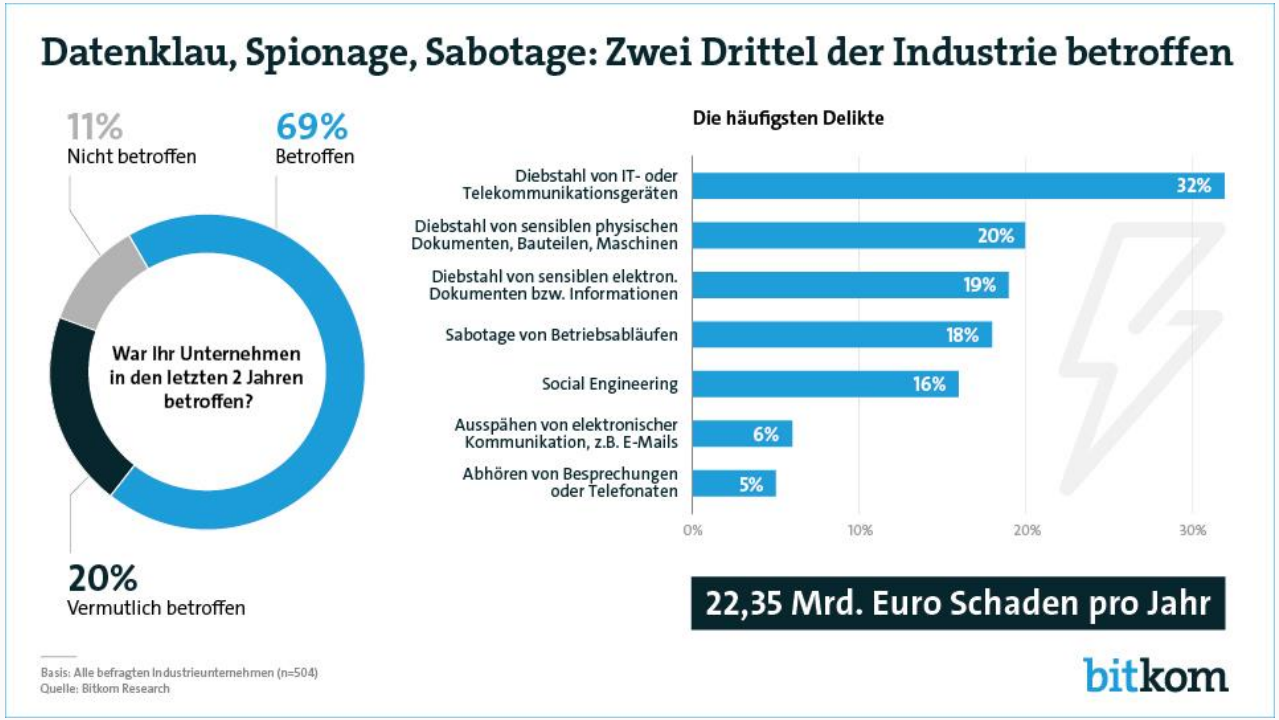
© DECOIT GmbH

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

Status Internet-Attacken



© DECOIT GmbH

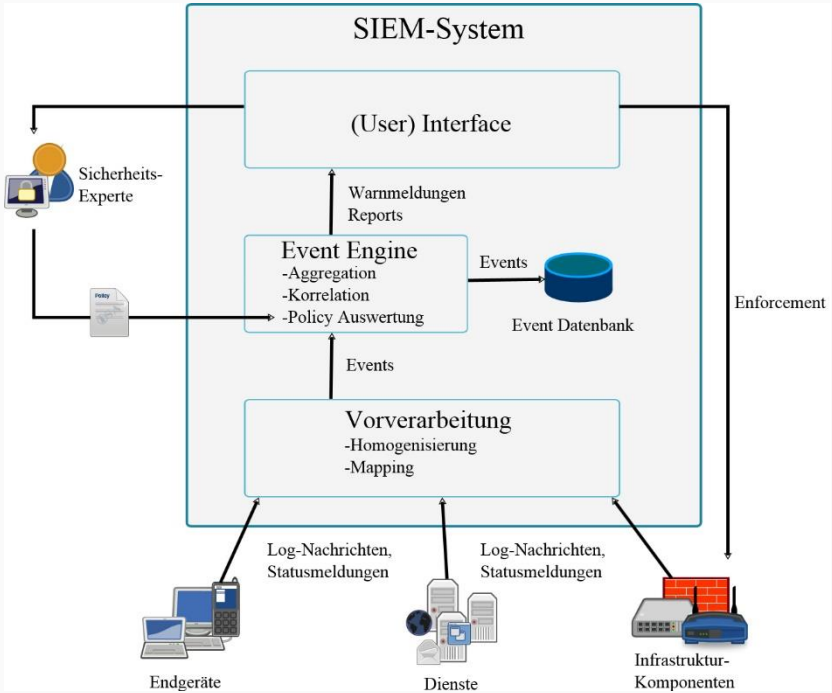
IT-Sicherheit baut auf Open Source!

- 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
  - SIEM: OSSIM

© DECOIT GmbH

SIEM-Definition

- Überwachung der IT-Sicherheit und Korrelation der Ereignisse (Vorfälle)
- Echtzeitüberwachung, Ergebniskorrelation, Logdaten-Langzeitanalyse sind die Hauptfunktionen
- Netzwerkverkehr und Serversysteme werden auf Anomalien untersucht
- Effektivität wird durch die verwendeten ML-Algorithmen bestimmt
- SIEM-Systeme sind im OT-Umfeld bisher kaum zu finden



© DECOIT GmbH

SEC I4.0
Start
Projekt
Partner
News
Veröffentlichungen
Termine
Förderung
Kontakt
SECurity Assessment für "Industrie 4.0"-Infrastrukturen durch Virtualisierung und Simulation
Projekt
Systeme der Fertigungs- und Prozessautomatisierung sind zunehmend gekennzeichnet durch vernetzte Rechner-, Mess-, Steuer- und Regelsysteme, vernetzte Agenten und Sensoren wie den Einsatz von SelfX-Technologien. Unterschiedliche Systeme und Informationsnetze erzeugen eine Vielfalt an komplexen, dynamisch-heterogenen IT-Landschaften. IT-Standardkomponenten ersetzen zudem immer mehr frühere proprietäre Systeme. Standardisierung und Vernetzung vermehren aber auch die Risiken, in Produktionsprozesse zu gelangen (einzudringen) und per Fernzugriff Geräte und Anlagen zu steuern. Durch Virtualisierung und Simulation lassen sich jedoch existierende Firmenwerte flexibel erfassen und analysieren, ohne dass Produktionsabläufe gestört oder gar unterbrochen werden. Sicherheitsanalysen und Penetrationstests

© DECOIT GmbH

Randdaten SEC-I4.0-Projekt

- BMBF-Projekt aus dem Bereich Zentrale Innovationsprogramm Mittelstand (ZIM)
- Laufzeit:
  - Start: 01.09.2019
  - Ende: 30.11.2021
- Partner:
  - DECOIT® GmbH: Konsortialführung und Entwicklung
  - Achtwerk GmbH & Co. KG: Entwicklung
  - Hochschule Bremen: Forschung und Simulation

© DECOIT GmbH

Ziele des SEC-I4.0-Projekts

- Ziel war es eine „intelligente“ Anomalie-Erkennung in Industrienetzen zu ermöglichen und diese vorab in einer Virtualisierungsumgebung zu simulieren
- SIEM-Ansätze sollten auf Industrie-Umgebungen adaptiert und Erkennungsalgorithmen auf Basis von „Machine Learning“ implementiert werden
- Durch das erweiterte Monitoring auf die IT-Sicherheit sollte ein „Security Assessment“ von Industrie4.0-Infrastrukturen ermöglicht werden, ohne dass in die reale Umgebung eingegriffen wird
- Erkennungs- und Analyseverfahren für industrielle Kommunikationsprotokolle in Industrie-4.0-Umgebungen sollten zum Einsatz kommen

© DECOIT GmbH

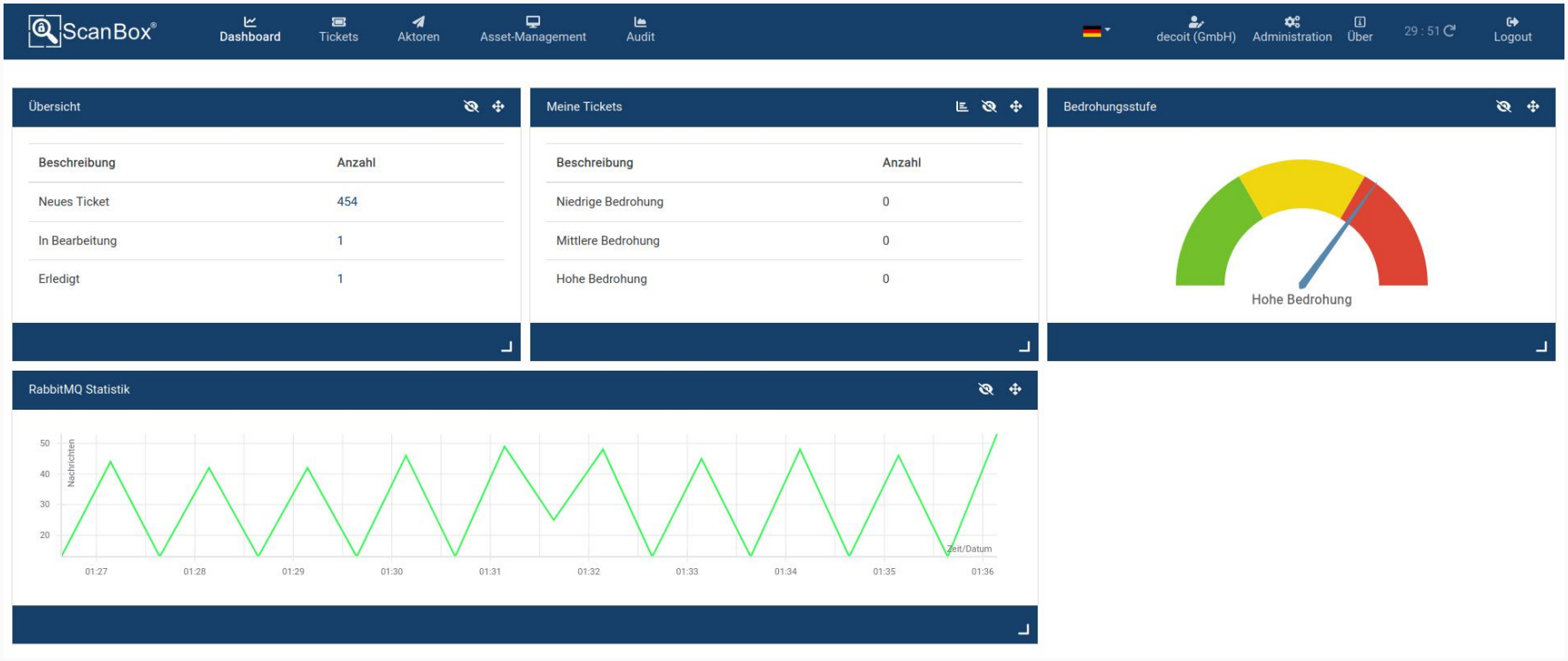
ScanBox als SIEM-Basis

- Die ScanBox der DECOIT® GmbH wurde als SIEM-Basis weiterentwickelt
- Die Monitoring- und Security-Analyse-Appliance ScanBox ist in der Lage aktive sowie passive Scans gleichermaßen durchzuführen
- Dadurch lässt sie sich sowohl in IT- als auch in OT-Umgebungen einsetzen
- Es wird nach Schwachstellen gesucht und diese im Dashboard angezeigt
- IT-Nutzer erhalten dafür konkrete Handlungsempfehlungen
- Jeder Vorfall wird in einem integrierten Ticketsystem aufgenommen und darüber bearbeitet
- Die Vorfälle lassen sich als Reports archivieren

www.scanbox-product.de

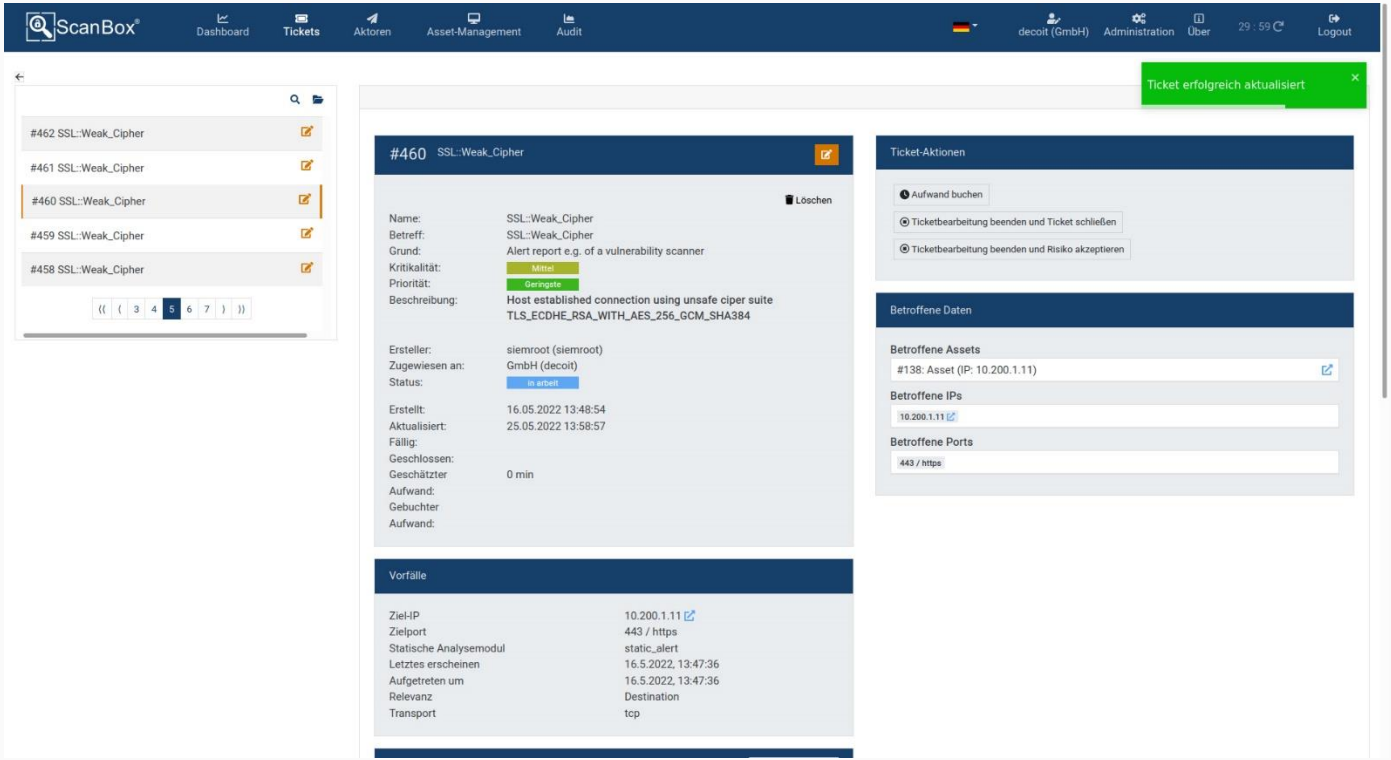
© DECOIT GmbH

Dashboard (1)



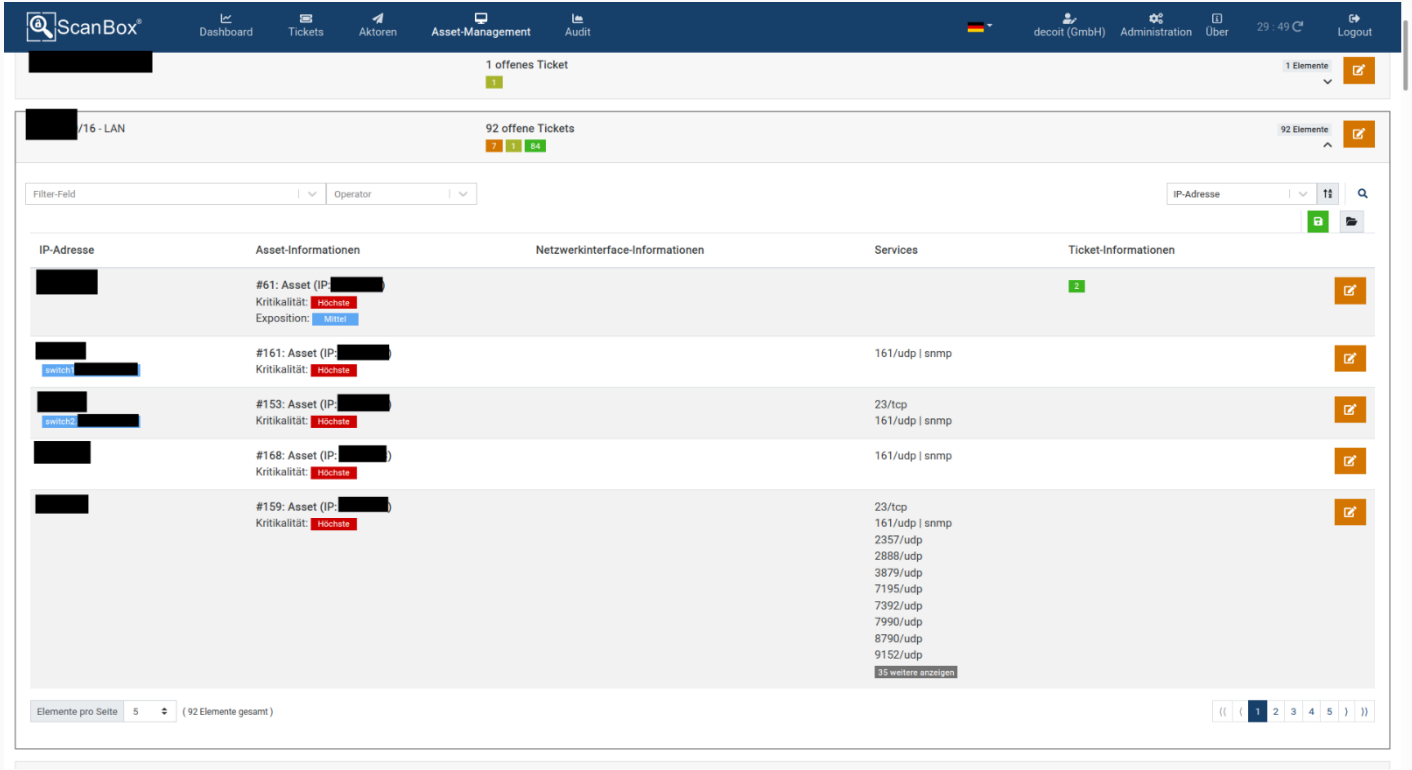
© DECOIT GmbH

Dashboard (2)



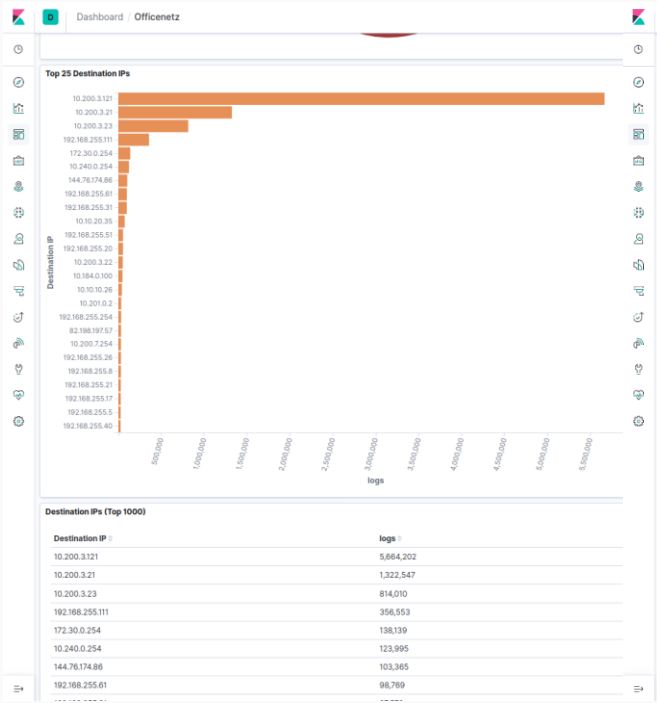
© DECOIT GmbH

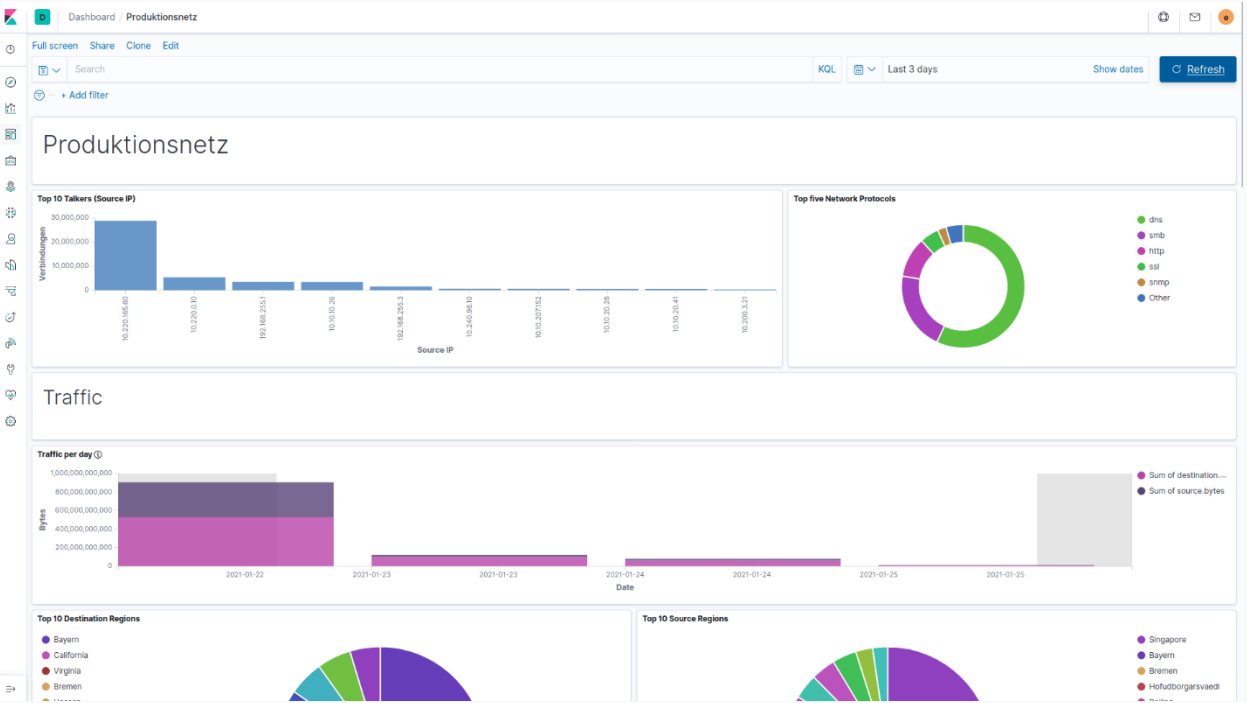
Dashboard (3)



© DECOIT GmbH

Audit-Dashboard





© DECOIT GmbH

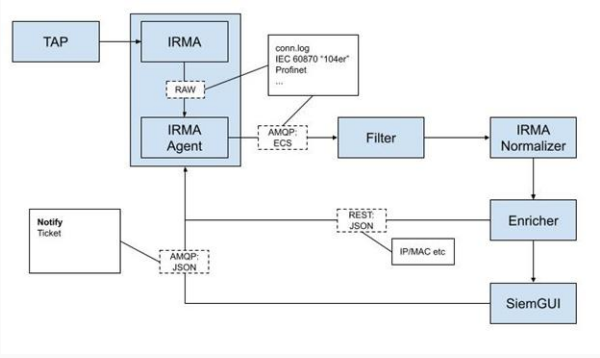
Einsatzszenarien

- IT-Büronetz
  - Es können aktive und passive Scans durch das Analysesystem in der ScanBox durchgeführt werden
  - Daten werden durch Switch-Mirror-Ports gesammelt und in Echtzeit im Dashboard oder nachträglich über das Reporting ausgewertet werden
  - Regelbasierte Schwachstellenanalyse für das Office-Netz
- OT-Produktionsnetz
  - Die IRMA-Appliance kommt als Sensor zum Einsatz
  - Anhand der Datenpakete eines Switch-Mirror-Ports erkennt IRMA die verwendeten Industrie-Protokolle
  - Die Datenlogs werden IRMA über eine REST-Schnittstelle dem Analysesystem in der ScanBox nachträglich zur Verfügung gestellt

© DECOIT GmbH

IRMA-ScanBox-Schnittstelle

- Die ScanBox und die IRMA wurden im Rahmen des Projekts um eine REST-API-Schnittstelle ergänzt
- Diese Schnittstelle ermöglicht das Abrufen von Alarmen, Assets und Verbindungen
- Es können Alarme an das zentrale Analysesystem der ScanBox übertragen, dort weiter analysiert und miteinander sowie mit anderen Datenquellen korreliert werden
- Zudem kann ScanBox auch gezielt Informationen zu Assets aus der IRMA abfragen
- Dies ermöglicht insbesondere das Anreichern mit Daten, die vom Nutzer bereits eingepflegt wurden



© DECOIT GmbH

Fazit

- Die Projektziele konnten fast alle erreicht werden, was durch die umfangreichen Vorarbeiten möglich war
- Ziel ist es, dass alle notwendigen Daten ausgewertet werden und nicht nur Inseldaten von IT-Sicherheitssystemen
- Dabei geht die Entwicklung immer mehr in Richtung KI-Funktionalität (weg von der reinen Mustererkennung)
- SEC-I4.0 lässt sich sowohl in OT-, als auch in IT-Umgebung einsetzen (Kombination von ScanBox und IRMA)
- Die Projektergebnisse konnten im Projekt leider nur innerhalb der Simulationsumgebung der Hochschule Bremen getestet werden

© DECOIT GmbH

Offene Problemstellungen

- SIEM-Hersteller haben sich in der Vergangenheit hauptsächlich auf IT-Netze (Office) bezogen
- OT-Netze wurden erst später berücksichtigt und teilweise immer noch nicht ausreichend (siehe Industrieprotokolle)
- KI-Algorithmen erzeugen immer noch zu viele „False Positives“
- SIEM-Anbieter stützen sich daher teilweise auf Rule-based Analysen
- OT-Netze werden meistens komplett abgeschirmt von anderen Netzen, wodurch es schwierig wird die Schwachstellen-Datenbank kontinuierlich auf dem neusten Stand zu halten

© DECOIT GmbH

Vielen Dank für die Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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

© DECOIT GmbH