Monitoring für Industrie 4.0:

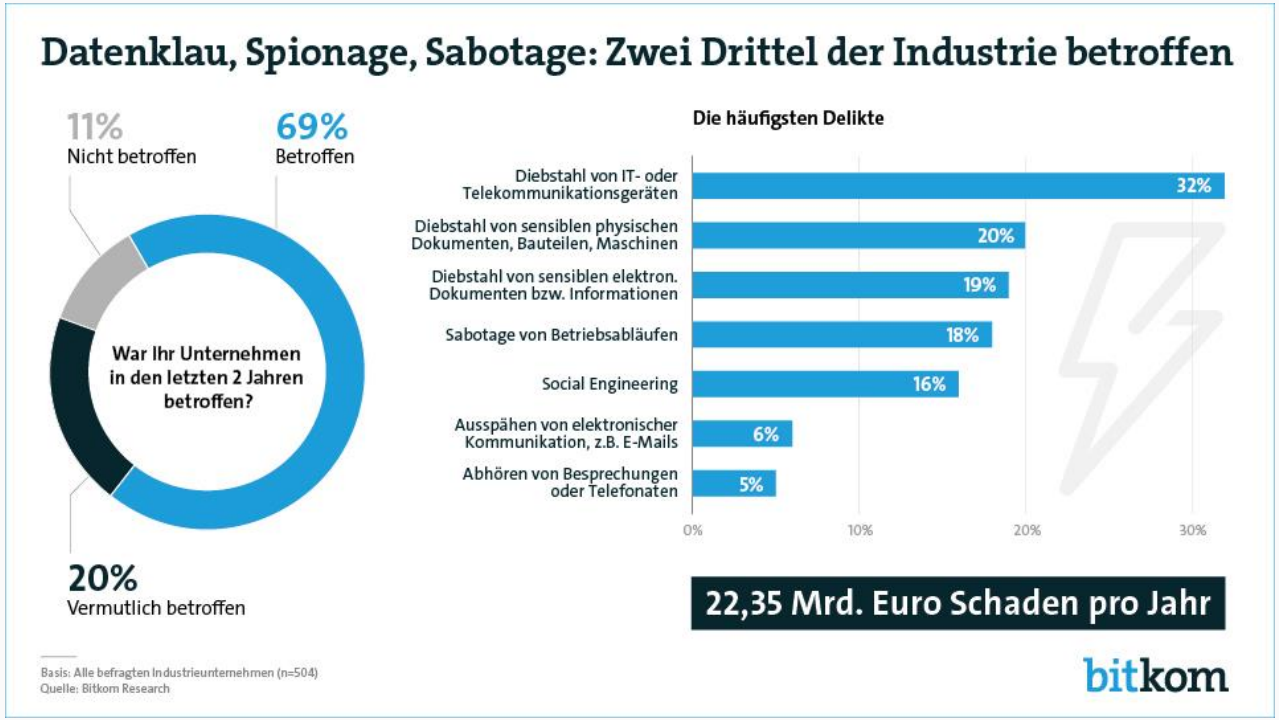
Aufspüren, Dokumentieren und Bereinigen von Schwachstellen in Verwaltungs- und Produktionsnetzwerken

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

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

Zunehmende Internet-Attacken



Erste Gegenmaßnahmen

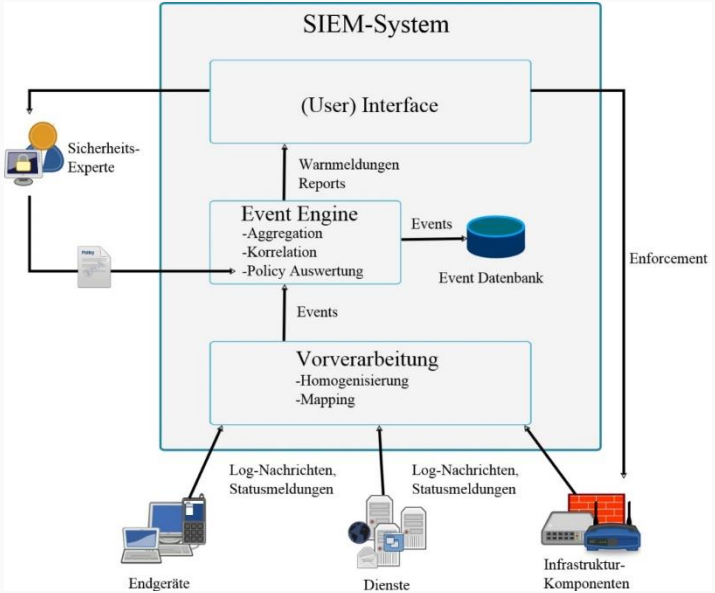
- Zur Absicherung wurden Access Control Lists (ACL) auf den Routern und Switches eingerichtet
- Statische Filter ließen sich allerdings nicht pflegen, weshalb diese später verbindungsabhängig (Stichwort: Stateful Inspection) in Firewalls umgesetzt wurden
- Application Ports wurden gesperrt, ohne den 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 Überwachungs-systemen

- 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)

SIEM-Schwerpunkte

- Überwachung und Verwaltung von
  - Benutzerdiensten und -privilegien
  - Verzeichnisdiensten
- Änderungen der Systemkonfiguration
- Bereitstellung zur Auditierung
- Überprüfung der Vorfälle



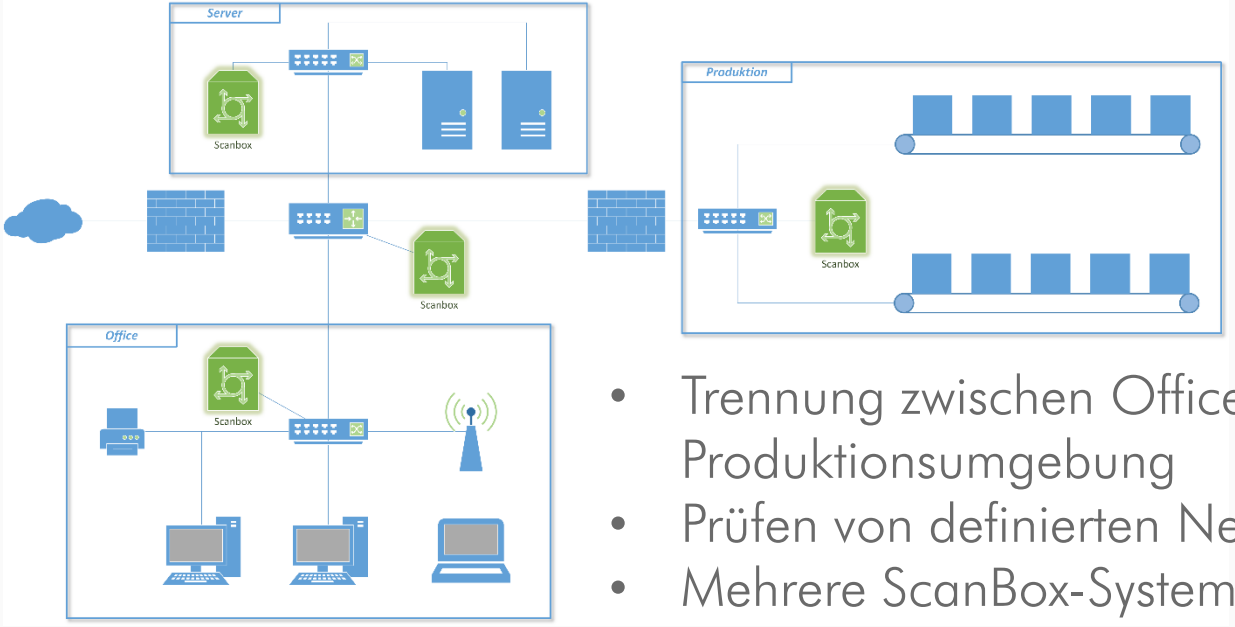
Ausgangssituation bei KMUs

- 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
- IT-Sicherheit im Produktionsumfeld hinkt der Büroumgebung um ca. 10 Jahre hinterher

ScanBox-Lösungsansatz

- Eine Security-Analyse über ein „Out-of-the-Box“-System vollautomatisch zu initialisieren, abzuwickeln und die Ergebnisse zu visualisieren
- Das System wurde als spezialisierte, genau für diesen Anwendungsfall adaptierbare Hardware-Box (Appliance), entwickelt
- Im Gegensatz zu reinen Analyse- und Monitoring-Tools werden Bezüge der identifizierten Risiken des Unternehmens hergestellt
- Nutzer erhalten ihrem Kompetenzlevel entsprechende konkrete Handlungsempfehlungen, deren Validität ebenfalls überprüft wird
- Die Erhöhung des Sicherheitsniveaus in KMUs und eine verbesserte Dokumentation wird angestrebt

Einsatzszenario



- Trennung zwischen Office- und Produktionsumgebung
- Prüfen von definierten Netzsegmenten
- Mehrere ScanBox-Systeme können im Einsatz sein

www.scanbox-project.de

Scan Box

Monitoring- & Security-Analysetool für Industrie 4.0

Ausgangssituation

Wesentliche Motivation zur Entwicklung der ScanBox ist die Erkenntnis, dass Klein- und Mittelständische Unternehmen (KMU) oft nicht die Unterstützung eines Vollzeit-Administrators haben, der sich bis ins kleinste Detail mit der Hardware und dem Netzwerk und demzufolge auch mit dem Bedrohungspotenzial auskennt. Vielmehr werden generelle IT-Kenntnisse in KMU angestrebt, um in allen IT-Bereichen rudimentär unterstützen zu können. Hierbei kommt das Thema IT-Sicherheit oftmals zu kurz, da dieses Umfeld keine direkten Auswirkungen auf das Tagesgeschäft hat. KMU sind verglichen mit großen Unternehmen bei prinzipiell gleicher Gefährdungslage deutlich höheren Risiken ausgesetzt.

Das Monitoring und die Bewertung von Netzwerk- und Informations-Sicherheit haben Auswirkungen auf das Rating und den Wert von Unternehmen. Gesetzgeberische und regulatorische Vorgaben erzwingen regelmäßige Kontrollen und Transparenz des vorhandenen Sicherheitsstandards. Abgesehen von den betriebswirtschaftlichen Schäden sind die Haftungsrisiken, mit denen für Geschäftsführer und IT-Verantwortliche in Unternehmen im Fall von nachweislichen Versäumnissen im Bereich der IT-Sicherheit konfrontierte werden, erheblich. Dennoch steigt die Zahl von Sicherheitsvorfällen jährlich.

ScanBox-Lösungsansatz

Der innovative Kern des Projektes beruht deshalb auf dem Ansatz, eine komplexe, nicht triviale,

Scan Box

- Projekt
- Partner
- News
- Veröffentlichungen
- Termine
- Download
- Datenschutz
- Impressum

gefördert durch
Bundesministerium für Wirtschaft und Energie
ZIM Zentrales

ScanBox-Projekt

- Das ScanBox-Projekt startete im Mai 2018 und endete im Juli 2020 mit folgenden Partnern:
  - DECOIT® GmbH (Projektmanagement und Entwicklung)
  - Telco Tech GmbH (Entwicklung und Anbieter)
  - Technische Hochschule Brandenburg (Entwicklung)
- Als assoziierte Partner waren beteiligt:
  - hanseWasser Bremen GmbH (Anwendungspartner)
  - HFC Human-Factors-Consult GmbH (Entwicklungspartner)
- Erste Performance- und Interoperabilitätstests konnten bereits erfolgreich bei der hanseWasser GmbH durchgeführt werden
- Dabei wurden innerhalb von 6 Wochen sowohl die IT- als auch die OT-Umgebung analysiert

ScanBox3000

- Vorprojekt: Bedarfsermittlung
  - IP-Netze
  - Geräte
  - Subnetzmasken etc.
  - Konfiguration der Szenarien
- Grundeinrichtung nach Installationsanleitung ist im ersten Schritt notwendig
  - CentOS-Betriebssystem
  - Software-Komponenten
  - SIEM-GUI+

ScanBox3000-Appliance

ScanBox4000-Appliance

Unterstützte Szenarien (1)

- Szenario 1: Definition von Kommunikationsregeln (Hosts, Netze, zeitliche Einschränkungen) zur Erkennung von Verstößen
- Szenario 2: Analyse von Logs (Windows Event Logs und syslog)
- Szenario 3: Integritätsüberwachung für Dateien (Zugriff per SSH oder Agents auf dem entsprechenden System)
- Szenario 4: Erkennung von fehlgeschlagenen SSH-Logins
- Szenario 5: Verwundbarkeitsscan
- Szenario 6: Malware Erkennung in der Netzkommunikation

Unterstützte Szenarien (2)

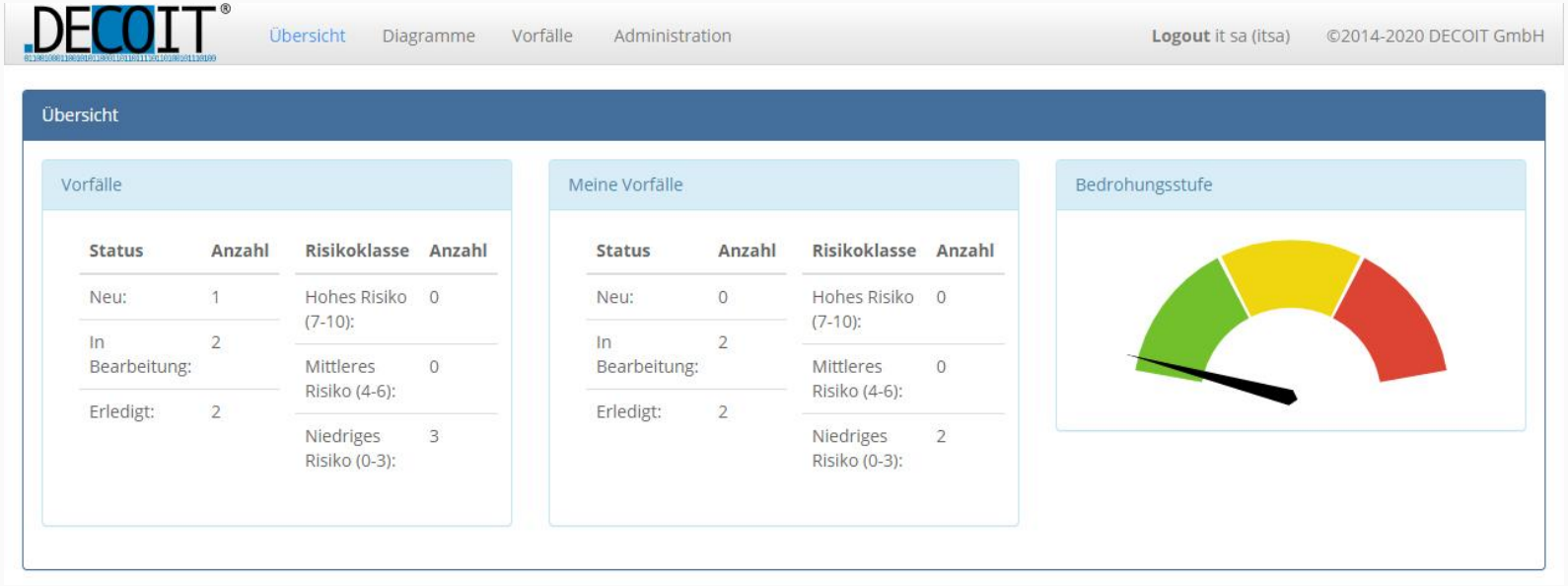
- Szenario 7: Login-Versuche auf Windows-Serversystemen
- Szenario 8: Erkennen neuer Netzverbindungen
- Szenario 9: Erkennen neuer Protokolle im Netz

Es lassen sich beliebig neue Szenarien nach Anforderungswunsch hinzufügen!

Funktionsumfang

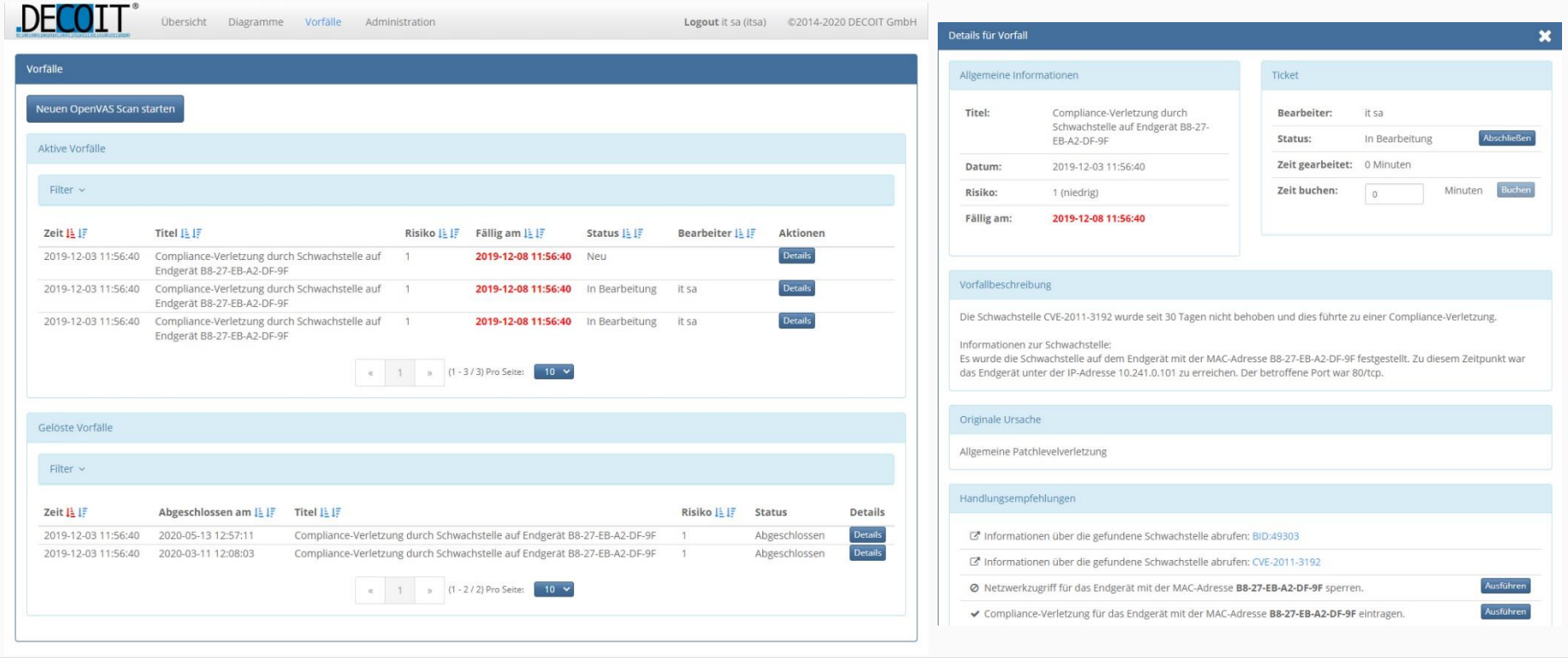
- Funktionalität:
  - Mit den Sensoren werden Netzwerk- und Serverdaten gesammelt
  - Die Daten werden ausgewertet und reale Vorfälle entdeckt
  - Anschließend erfolgt die Zuordnung zu bekannten CVE-Schwachstellen
  - Handlungsempfehlungen werden daraus abgeleitet
  - Eine kontinuierliche Risikobewertung findet statt
  - Integriertes Ticketsystem zur Vorfallbearbeitung
  - Produkt ist geeignet für IT- und OT-Umgebungen
- Voraussetzungen:
  - Switch-Mirror-Port für Netzüberwachung
  - Konfiguration der Netzregeln
  - Konfiguration der Szenarien

SIEM-GUI+

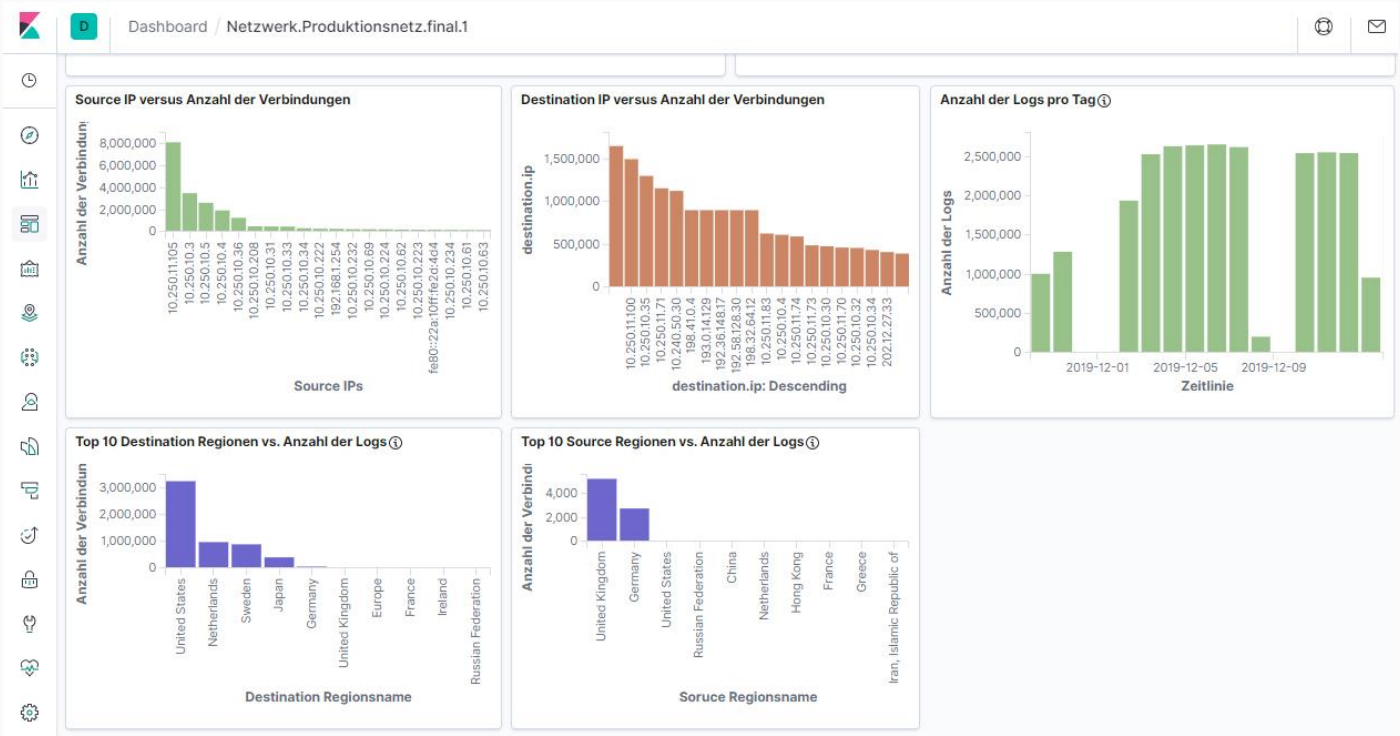


- Vernetzung von Schwachstellen-Scannern (aktiv/passiv) und Logdaten in einem SIEM-Modul zur Durchsetzung der IT-Unternehmensrichtlinien
- Nachvollziehbare und nachweisbare zentrale Sammlung aller sicherheitsrelevanten Informationen

Vorfallauflistung und -beschreibung



ScanBox-Reporting



Umsetzung

- Datenvolumengrenze muss angegeben werden aufgrund begrenztem Speicherplatz auf der Appliance
- Auf Wunsch kann auf externem Storage archiviert werden
- Vorprojektierung ist erforderlich, um alle Rahmenbedingungen abzuklären (z.B. welche Netze überwacht werden sollen)
- Anhand der gesammelten Anforderungen wird eine Basiskonfiguration erstellt und die ScanBox ausgeliefert
- Support kann per E-Mail oder/und Service-Vertrag beauftragt werden
- Die ScanBox 3000 kann kontinuierlich oder für einen bestimmten Zeitraum begrenzt eingesetzt werden

Kosten

	ScanBox3000		ScanBox4000
	bis 50 VM	bis 150 VM	bis 250 VM
Hardware-Appliance	2.800,00 €	2.915,00 €	6.081,20 €
HW-Maintenance p.a.	336,00 €	349,80 €	729,72 €
HW-Lieferzeit	ca. 3 Wochen nach Bestellung	ca. 3 Wochen nach Bestellung	ca. 12 Wochen nach Bestellung
Software CLEARER	1.200,00 €	1.800,00 €	2.700,00 €
Vorprojekt für Anforderungen	450,00 €	450,00 €	450,00 €
Vorbereitung ScanBox	450,00 €	450,00 €	450,00 €
SW-Maintenance p.a.	300,00 €	600,00 €	1.000,00 €
SW-Support per E-Mail p.a.	500,00 €	500,00 €	500,00 €
Service-Vertrag (2 Stunden pro Monat)	225,00 €	225,00 €	225,00 €
Gesamtpreis (ohne Support)	5.536,00 €	6.564,80 €	11.410,92 €

Maintenance ist verpflichtend, Support per E-Mail oder Service-Vertrag ist optional

Zusammenfassung

- Die ScanBox3000 ermöglichen es, dass das interne Netz kontinuierlich auf Schwachstellen analysiert werden kann
- Dabei wird zwischen IT- und OT-Netzen unterschieden (aktive/passive Scans)
- Die Funktionalität wächst dabei mit den unterstützten Szenarien
- Weiterentwicklungen werden durch Maintenance-Verträge kostenfrei zur Verfügung gestellt
- Es wird eine Echtzeitanalyse der Vorfälle durch die SIEM-GUI ermöglicht
- Eine Offline-Analyse kann durch das Reporting-Modul mittels Kibana erfolgen
- Die Namensgebung „ScanBox“ wird sich aus rechtlichen Gründen noch ändern

Vielen Dank für die Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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