DECOIT®

secIT by Heise
HANNOVER 2018 6.+7. März

Das CLEARER-Projekt:

Open-Source-Lösungen im Umfeld von SIEM und NAC

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

Inhalte

- Motivation und Entwicklung der IT-Sicherheit
- Netzmonitoring
- Network Access Control (NAC)
- Security Information and Event Management (SIEM)
- Das CLEARER-Projekt
- Architektur und Szenarien
- Ergebnisse
- Ausblick

Firmenportfolio

- Gründung am 01.01.2001 als Bremer System- und Softwarehaus
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Fokus: Herstellerneutrale, ganzheitliche Beratung von IT-Lösungen
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
  - Consulting: ganzheitliche/herstellerneutrale Beratung
  - Systemmanagement: Planung, Umsetzung und Support von Hersteller- und Open-Source-Lösungen
  - Software-Entwicklung: Entwickeln von Individuallösungen und Produkten mit hohem Innovationscharakter
  - Forschungsprojekte: entwickeln innovativer IT-Lösungen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen

Motivation (1)

- BSI Studie (2011): IT-Sicherheit in kleinen und mittleren Unternehmen (KMU):
  - Ziel der Studie war es, den Ist-Zustand des IT-Sicherheits- und Krisenmanagements sowie der Sicherheit kritischer IT-Infrastrukturen im Bereich der kleinen und mittleren Unternehmen (KMU) zu ermitteln
  - Die Ergebnisse der Studie zeigten einen Nachholbedarf insbesondere im geordneten Management des IT-Sicherheitsprozesses und hinsichtlich präventiver IT-Sicherheitsmaßnahmen

Motivation (2)

- Informatik Aktuell (Nov. 2016): Angriffswelle rollt auf deutschen Mittelstand zu :
  - Beim CEO-Fraud sammeln Täter Informationen über das anzugreifende Unternehmen und geben sich anschließend als z.B. Geschäftsführer (CEO) gegenüber den Angestellten aus, um den Transfer eines größeren Geldbetrages ins Ausland zu veranlassen (Social Engineering)
  - Ransomware verschlüsseln Festplatten und geben den Zugang erst nach Zahlung eines Lösegelds wieder frei
  - Es ist zu befürchten, dass DDoS-Attacken aus dem Internet-der-Dinge auf uns zukommen werden (Beispiel: Ausfälle bei Amazon)

Motivation (3)

- Computerwoche (Dez. 2016): IT-Sicherheit/Prognosen für 2017:
  - Immer noch sind Spezialisten für IT-Sicherheit rar und begehrt
  - Diejenigen, die es gibt, haben in der Regel eine hohe Arbeitsbelastung
  - Deswegen werden Unternehmen zunehmend auf Automatisierungstools setzen
  - Dank dieser Tools sollten weniger Alarme mit höherer Relevanz auflaufen

Entwicklung der IT-Sicherheit (1)

- Am Anfang stand die Verfügbarkeit und Vernetzung von IT-Services im Vordergrund
- 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

Entwicklung der IT-Sicherheit (2)

- Intrusion Prevention Systems (IPS) sollten hingegen Anomalien in der Entstehung verhindern und die Log-Flut eindämmen
- IPS-Lösungen erhöhten allerdings den Aufwand pro Port und Paket, was bei 10-Gbit/s-Netzen zu Performance-Engpässen führen konnte
- Protokolle (z.B. SOAP), die über diverse Ports, Schichten und Verschlüsselung kommunizieren zusätzliche Herausforderungen
- Heute sind viele unterschiedliche Insellösungen im Einsatz (AV-, IDS-, IPS-, FW-, VPN-, NAC-Systeme etc.), die keine einheitliche Aussage über Anomalien im Netzwerk zulassen
- Verschiedenen Herstellerlösungen sind oft nicht kompatibel zueinander!

Einsatz von Überwachungssystemen

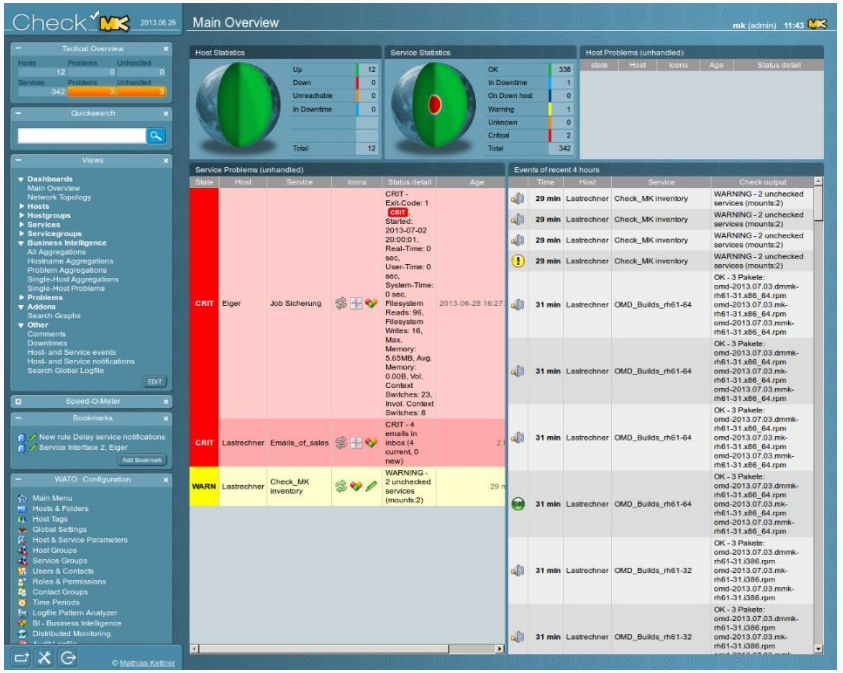
- Unterschiedliche Überwachungs- und Regulierungssysteme besitzen verschiedene Ausrichtungen:
  - **Netzmonitoring**: Überwachung der Verfügbarkeit
  - **Network Access Control (NAC)**: Überwachung der Zugangskontrolle
  - **Security Information and Event Management (SIEM)**: Überwachung der IT-Sicherheit

Pro-aktives Netzmonitoring

- Ein pro-aktives Netzwerk-Monitoring meldet Systemausfälle, bevor ein Anwender diese bemerkt
- Der IT-Administrator hat bessere Pflegemöglichkeiten, da er den Zustand des Gesamtnetzes (Server, Clients, IP-Telefone, Netzwerk) kennt und darauf Einfluss nehmen kann
- Zusätzlich wird eine aktuelle Dokumentation ermöglicht, die interaktiv auf dem neusten Stand gehalten wird
- Langzeitstatistiken helfen auch, nachträglich Fehler zu analysieren
- Auch an Feiertagen und Wochenende können alle aktiven Systeme überwacht werden
- Fast beliebige Systeme lassen sich in ein Monitoring einbetten – allerdings ohne Einbeziehung der IT-Sicherheit!

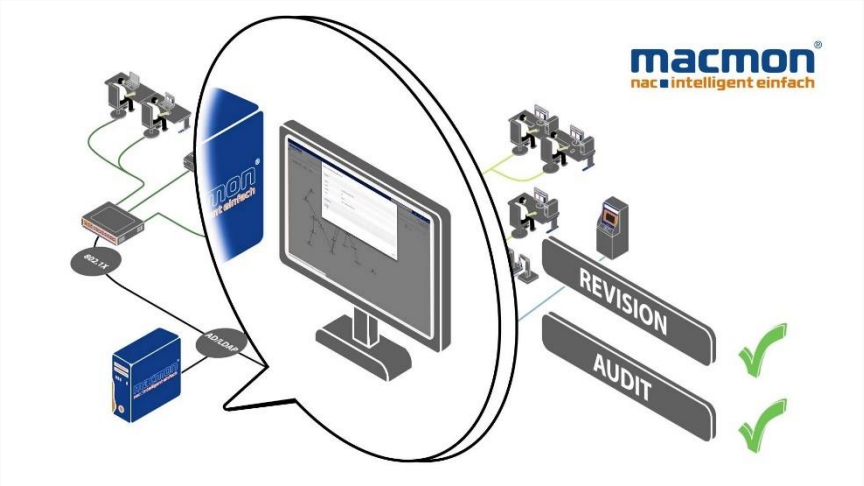
Netzmonitoring

- 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



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



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

Das Projekt CLEARER

- CLEARER steht für: Erfüllung von Compliance-Anforderungen durch automatisierte Bearbeitung von IT-Sicherheitsvorfällen
- Partner:
  - DECOIT GmbH (Konsortialführer, Entwicklung)
  - Hochschule Hannover (Entwicklung)
  - IT-Security@Work GmbH (IT-Compliance-Spezialist)
  - macmon secure gmbh (NAC-Hersteller)
- BMWi-(AiF)Projekt (01.05.16 – 30.04.2018)
- URL: www.clearer-project.de

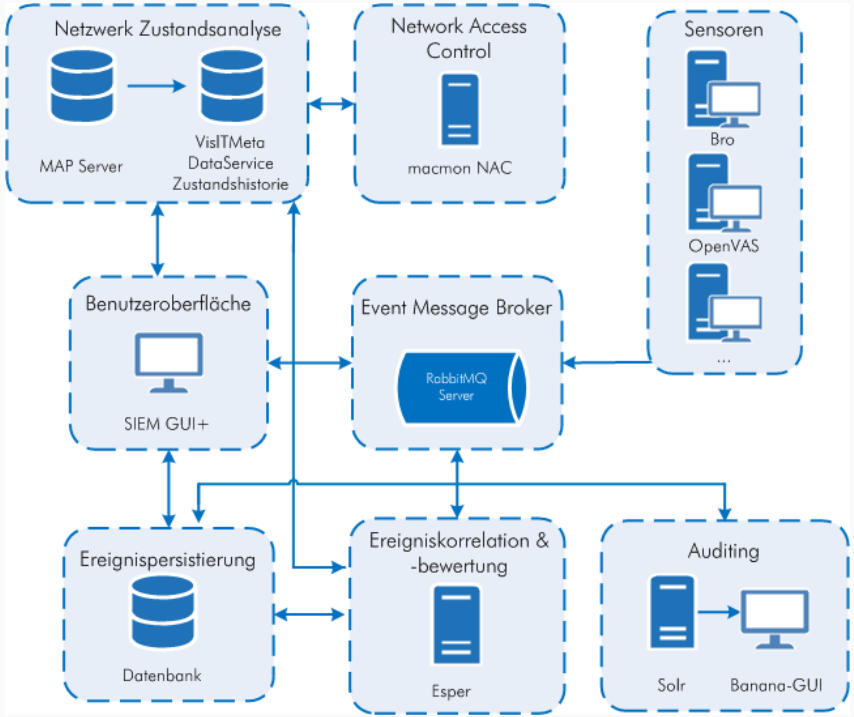
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Ziele des Projekts

- Vernetzung von NAC, Intrusion Detection System (IDS), Schwachstellen-Scanner und Logdaten durch Standards in einem SIEM zur Durchsetzung der IT-Unternehmensrichtlinien
  - Angriffe und Verstöße performant erkennen, bewerten und priorisieren
  - Reaktion einleiten oder Administration informieren und unterstützen
- Aufbereitung aller gesammelten Daten für einfachere Forensik bei erfolgten Angriffen
- Nachvollziehbare und nachweisbare zentrale Sammlung aller sicherheitsrelevanten Informationen
  - Einfachere Compliance-Statuskontrolle für Auditoren
  - Verstehbare Handlungsempfehlungen für den Administrator

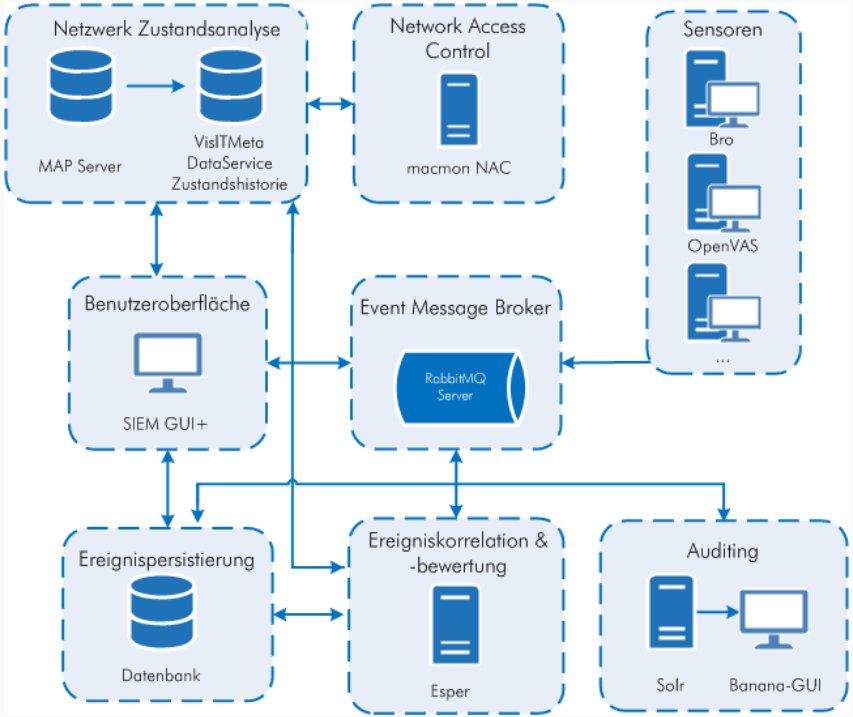
Architektur (1)

- Zentrale Message-Queue für Ereignisse, Hin- und Rückweg (Performance, Compliance, Kostenreduktion)
- Interface for Metadata Access Points (IF-MAP), Anbindung für Zustandsdaten (Standardisierung und Kostenreduktion)
- Trennung von Ereignis und Zustandsdaten durch IF-MAP (Standardisierung und Performance)
- Fokus auf schnelle Schreib-Performance der Datenbank (Performance und Compliance)
- Ereignisse dürfen nicht verändert werden (Compliance)
- Selbstüberwachung des CLEARER-Systems (Compliance)



Architektur (2)

- **MAP-Server**: Netzwerk-Zustandsanalyse und Historie
- **NAC-Modul**: Network-Access-Control mit macmon NAC
- **SIEM-GUI+**: Benutzeroberfläche und Event-Anzeige
- **RabbitMQ**: Event Message Broker
- **OpenVAS und Bro**: Sensoren zur Datengenerierung
- **Apache Camel Datenbank**: Ereignis-Persistierung
- **Esper**: Ereigniskorrelation und -bewertung
- **Solr und Banana-GUI**: Auditing und gezielte Suche



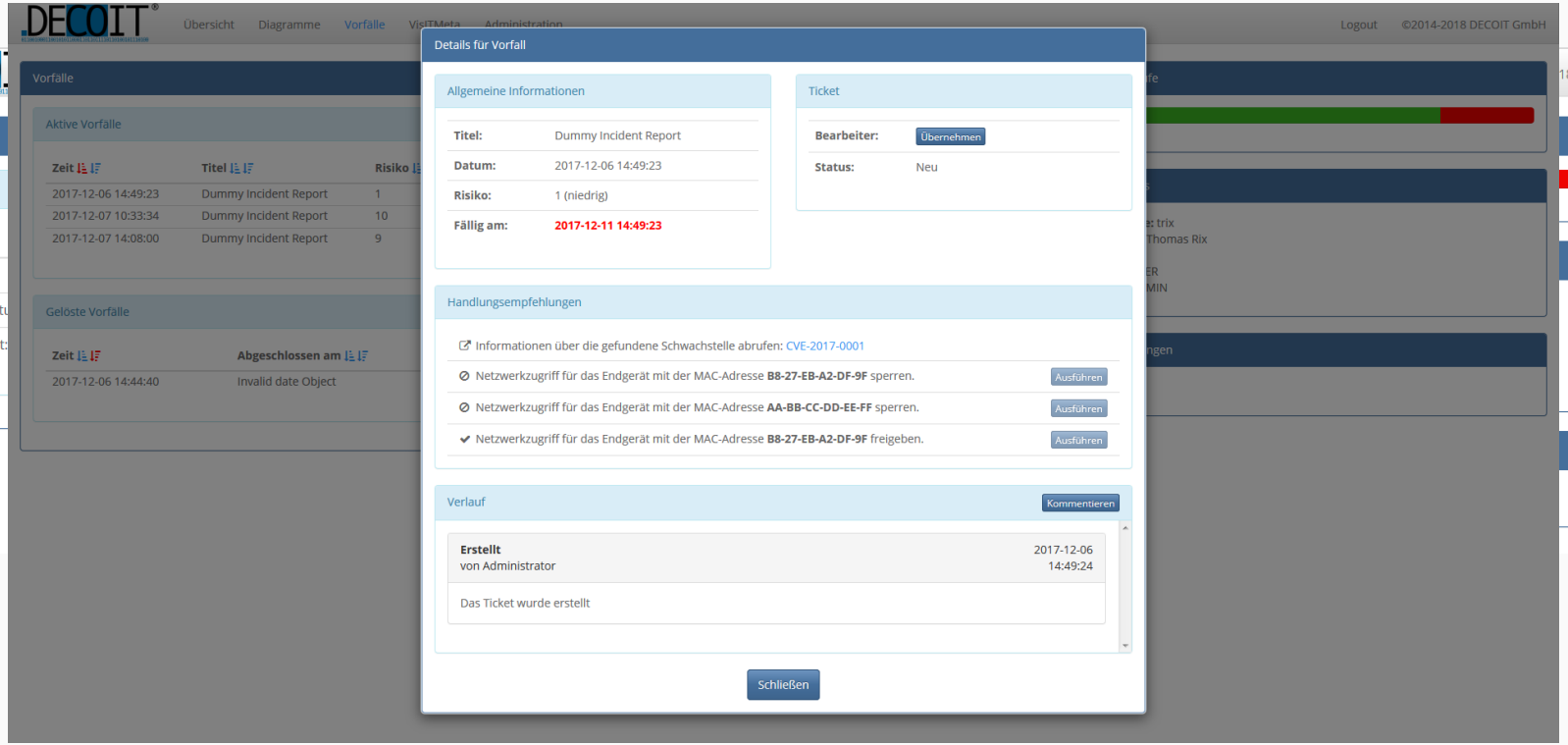
Szenarien in CLEARER

- **Updatestand in einer Windowsumgebung:** die Updates von Windows-Systemen werden überwacht und Alarmmeldungen ausgegeben, wenn nach einer definierten Zeit keine Aktualisierungen vorgenommen wurden
- **Trennung von Produktions- und Office-Netzwerk:** Anhand von Netzwerkscans wird auf unterschiedliche Netze Rücksicht genommen und Analysen über den Sicherheitszustand durchgeführt
- **Netzverkehr außerhalb der Arbeitszeit:** Anomalien können sich auch durch Netzwerkverkehr äußern, der plötzlich zu ungewohnten Zeiten auftritt
- **Sensitive Daten überwachen:** Dateien auf Serversystemen, die mittels Integritätscheck gesichert wurden, werden auf Veränderungen überwacht

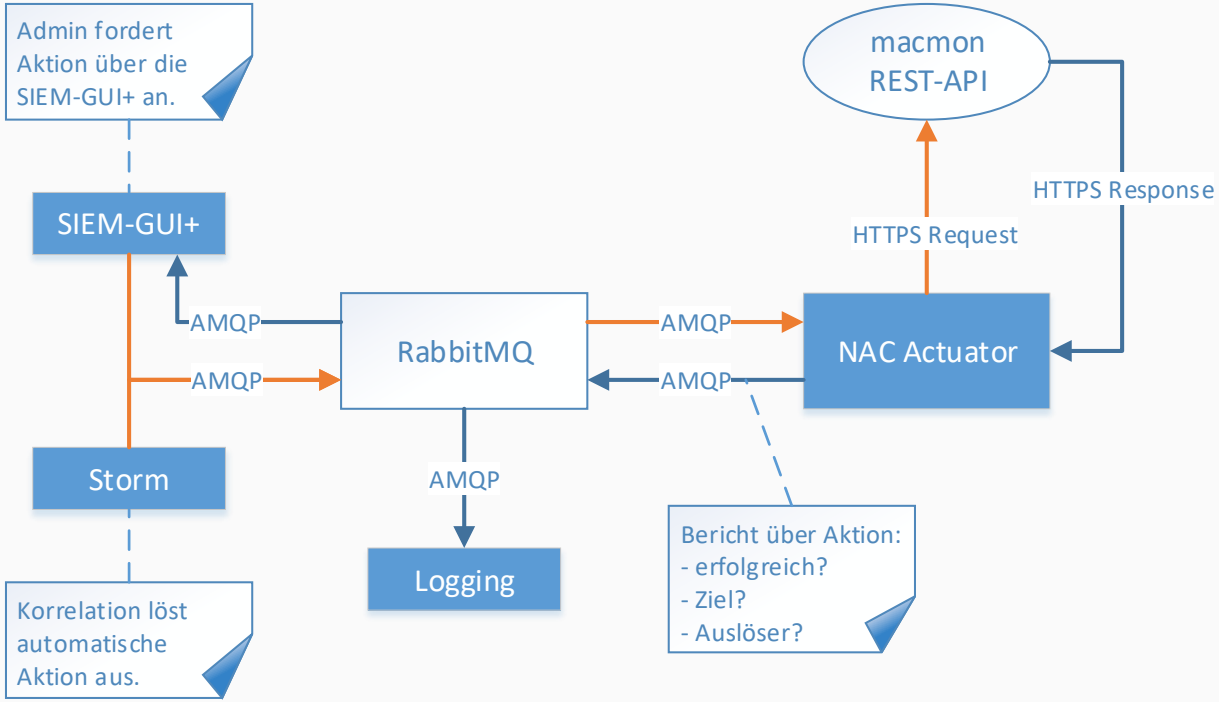
Beispielanwendung

- IT-Sicherheits-Schwachstellen identifizieren und priorisieren:
  - Schwachstellen-Scan kontinuierlich durchführen
  - Schwachstellenereignisse anhand von Infrastrukturinformationen bewerten
  - In der Oberfläche SIEM-GUI+ anzeigen
  - Nach 30 Tagen erneuten Scan ausführen
  - Schwachstelle existiert noch, Priorität erhöhen, Behebungszeit anpassen und E-Mail mit Aufforderung an den Admin senden
  - Protokollierung für Compliance-Rückverfolgbarkeit

SIEM-GUI+



Anbindung an macmon secure



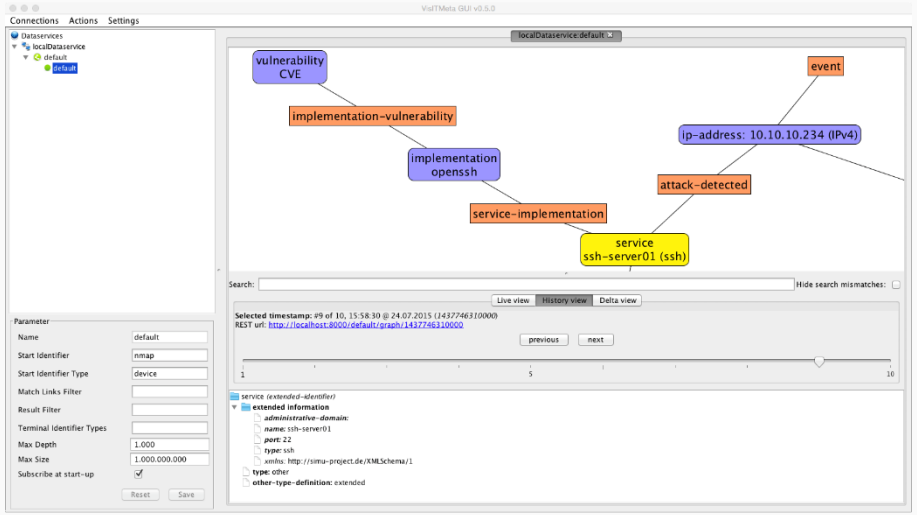
Anbindung an macmon secure

- Das CLEARER-System benötigt eine Schnittstelle zu NAC-Systemen, um diese mit SIEM-Funktionen ergänzen zu können
- Dies ist bei macmon secure neuerdings über eine REST-API möglich, die die alte macutil-Schnittstelle ersetzt
- Diese kann über HTTPS direkt angesprochen werden
- Eine Kommunikation ist in beide Richtungen möglich: z.B. lassen sich Infrastrukturdaten holen und ein Enforcement-Befehl zurücksenden
- Um unabhängig vom Hersteller zu sein, wurde ein NAC-Aktuator entwickelt, der eingehende Anfragen entsprechend aufbereitet

Leistungsmerkmale (1)

- Anzeige der wesentlichen Events und Ereignisse in der SIEM-GUI+
- Rollen- und -Rechtemanagement
- Sicht auf historische Daten für Audits über Banana-GUI
- Integriertes Ticketsystem mit einfachen Handlungsempfehlungen
- IF-MAP-Einsatz zur Speicherung und Visualisierung (z.B. über VisITMeta) des Netzwerkzustands
- Zentrale Datenbasis zeigte alle Ereignisse und kann große Datenmengen beinhalten

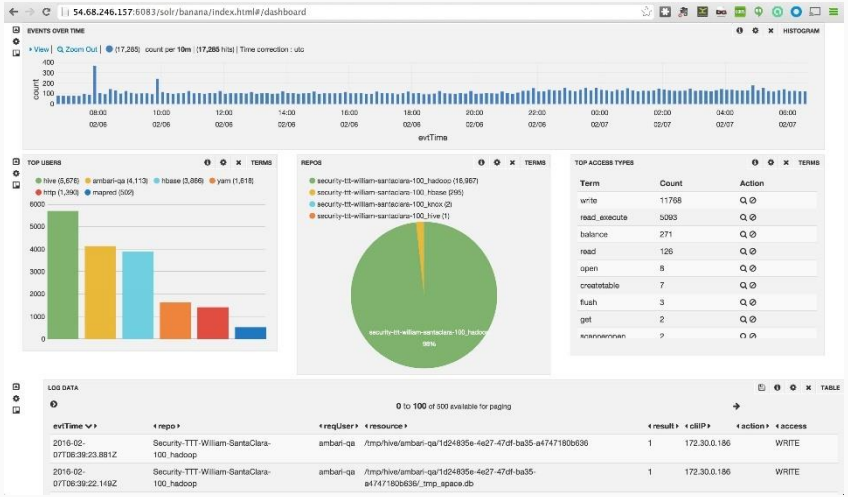
IF-MAP-Graph von VisITMeta



Leistungsmerkmale (2)

- Ereigniskorrelation und -bewertung mittels Esper zur Erkennung von Compliance-Verletzungen
- Dynamische Compliance-Anpassung durch Anpassung der Konfiguration zur Laufzeit
- Sammeln von Netzwerkzustand und -ereignissen durch entsprechende Sensoren (u.a. DECOmap)
- API-Schnittstellen-Support (z.B. REST) zur Anbindung von NAC-Systemen (z.B. macmon secure)

Banana-Auditoberfläche



Ergebnisse

- Schließen von Lücken der Nachweisbarkeit des Sicherheitsstatus
- Einfache Einbindung von NAC und diverser anderer IT-Sicherheitskomponenten in das SIEM-System von CLEARER
- Ganzheitlicher Ansatz zur Überwachung des Netzwerkes
- Kostenreduktion durch Open-Source-Komponenten
- Beliebig anpassbar und erweiterbar durch Open-Source-Komponenten

Ausblick

- CLEARER soll als Erweiterungsmodul von NAC-Systemen auf Basis der REST-API weiterentwickelt werden
- Dadurch erhält ein NAC-System zusätzlich SIEM-Funktionalität
- IT-Compliance wird dadurch ebenfalls integraler Bestandteil
- Der ursprünglich große Ansatz der Datenbank Cassandra (Cluster, hohe Skalierbarkeit) ist auf die Datenbank Camel heruntergebrochen worden
- CLEARER mit Zeitreihenanalyse zur Anomalie-Erkennung erweitern
- Weitere Einsatzszenarien realisieren, je nach Anforderungen

Vielen Dank für die Aufmerksamkeit!

www.clearer-project.de

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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