Erfüllung von Compliance-Anforderungen durch automatisierte Bearbeitung von Sicherheitsvorfällen

K.-O. Detken, T. Rix, M. Jahnke (DECOIT GmbH)
M. Steiner (IT-Security@Work GmbH)

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

Agenda

- Einleitung
  - Kooperationsprojekt
  - Motivation
  - Ziele
- Umsetzung
  - Architektur
  - GUI
  - Anwendungsszenarien
  - Dynamische Compliance
  - NAC-Schnittstelle
- Fazit

Einleitung
Kooperationsprojekt

- 2-Jahres-Projekt ZIM (BMWi)
- Zeitdauer 01.05.2016 – 30.04.2018
- URL-Adresse: www.clearer-project.de
- Projektziel: Automatisierte IT-Compliance in Verbindung mit einem NAC-System
- Partner:
  - Industrie: DECOIT® GmbH, IT-Security@Work GmbH, macmon secure GmbH
  - Hochschulen: Hochschule Hannover
  - Assoziiert: AchtWerk GmbH, rt-solutions.de GmbH

DECOIT®

Einleitung
Motivation

- Kontinuierliche Erhöhung der „Schnittstellen“ ins WWW
  - Internet of Things
  - Cloud Dienste
  - Industrie 4.0
  - Medical IT-Devices/Equipment
- Viele spezialisierte IT-Sicherheitskomponenten
- Die IT-Sicherheitskomponenten interagieren nicht oder nur rudimentär miteinander

Eine stärkere Vernetzung aller IT-Sicherheitskomponenten muss erfolgen!

Einleitung

Ziele

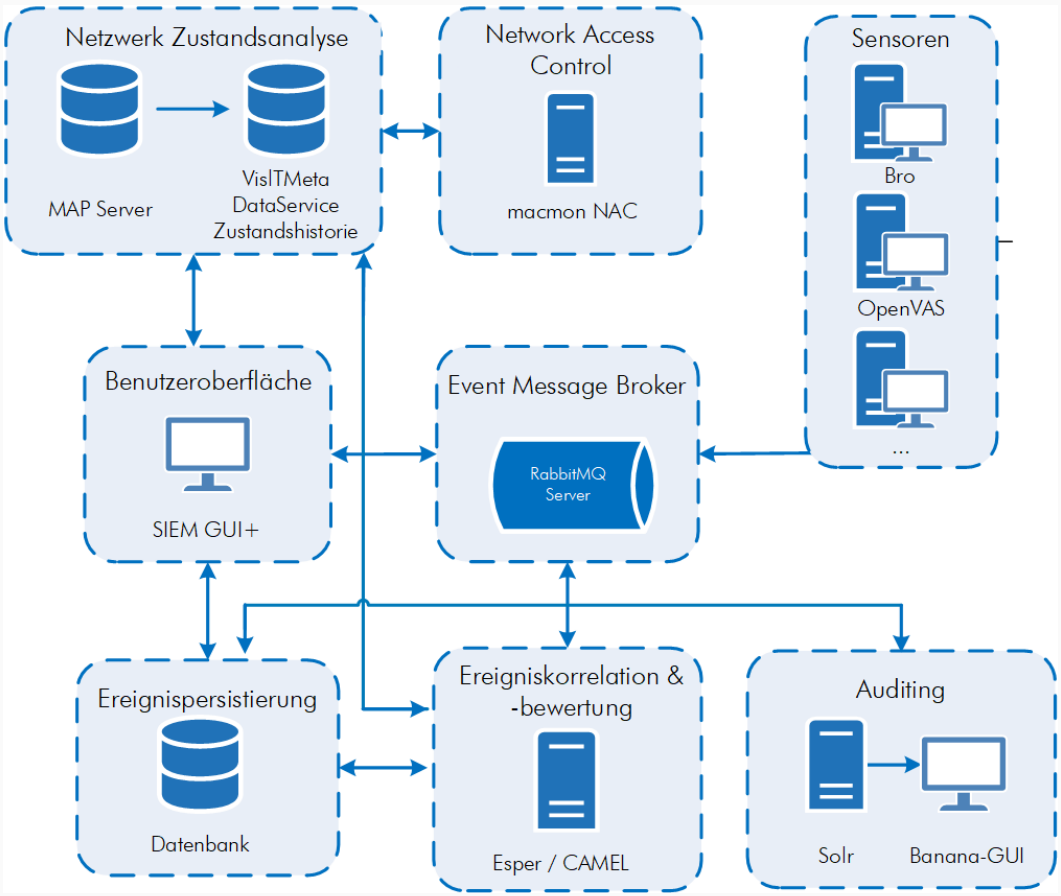
„Das Ziel des CLEARER-Projektes ist es, eine automatisierte Überwachung und Steuerung von Compliance-Aspekten in der IT auch für kleine Unternehmen zu ermöglichen.“

Einleitung

Ziele

- Vernetzung mit verschiedenen Diensten und Datenquellen:
  - Network Acces Control (NAC)
  - Intrusion Detection System (IDS)
  - Schwachstellen-Scanner
  - Logdaten
- KMUs unterstützen bei der Einhaltung von IT-Compliance
- Melden von Verstößen
- Unterstützung bei der Lösung von Verstößen

Umsetzung
Architektur



- MAP-Server / VisITMeta
- NAC-Modul
- SIEM-GUI+
- RabbitMQ
- OpenVAS und Bro
- MariaDB
- Apache Camel
- Esper
- Solr und Banana-GUI

Umsetzung
GUI-Oberfläche SIEM-GUI+

Übersicht Diagramme Vorfälle VisITMeta Management Administration **Logout** Thomas Rix (trix) ©2014-2018 DECOIT GmbH

Übersicht

Vorfälle

Status	Anzahl	Risikoklasse	Anzahl
Neu:	16	Hohes Risiko (7-10):	3
In Bearbeitung:	2	Mittleres Risiko (4-6):	4
Unbekannt:	0	Niedriges Risiko (0-3):	11

Meine Vorfälle

Status	Anzahl	Risikoklasse	Anzahl
Neu:	1	Hohes Risiko (7-10):	1
In Bearbeitung:	2	Mittleres Risiko (4-6):	0
Unbekannt:	0	Niedriges Risiko (0-3):	2

Bedrohungsstufe

Umsetzung

GUI-Oberfläche SIEM-GUI+

Übersicht | Diagramme | Vorfälle | VisITMeta | Management | Administration

Logout Thomas Rix (trix) ©2014-2018 DECOIT GmbH

Vorfälle

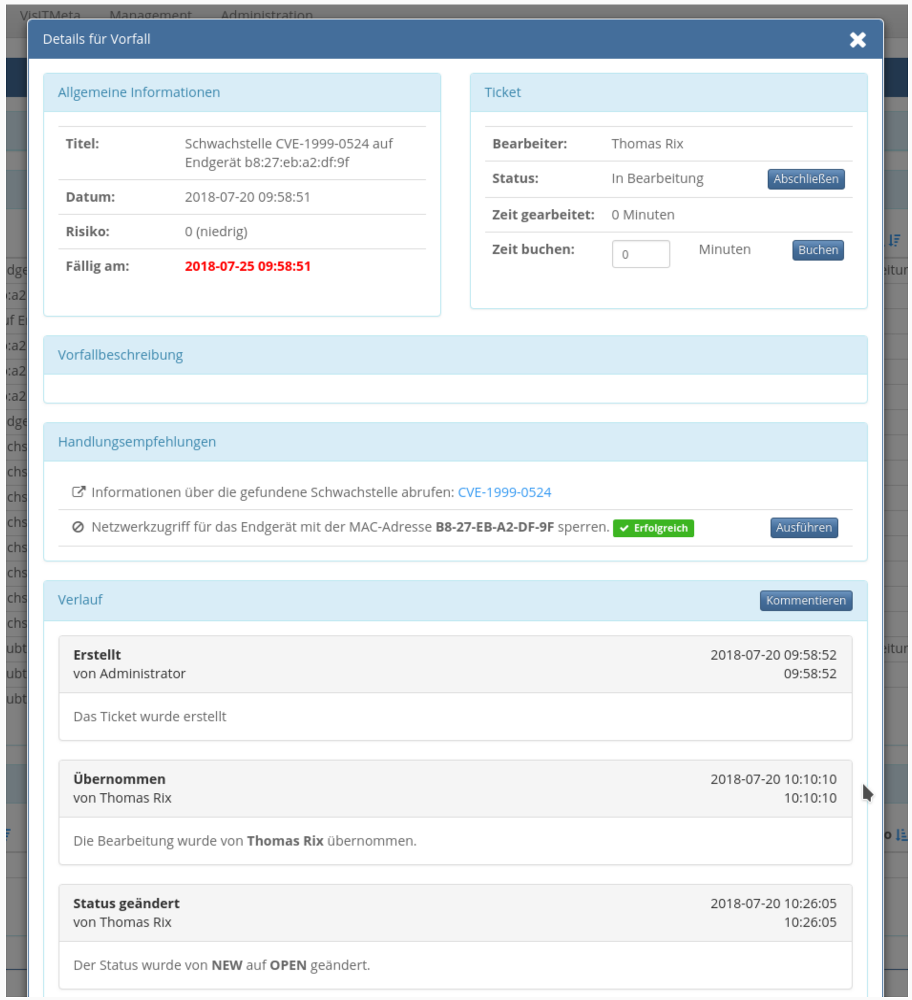
Filter

Aktive Vorfälle

Zeit	Titel	Risiko	Fällig am	Status	Bearbeiter	Aktionen
2018-07-20 09:58:51	Schwachstelle CVE-1999-0524 auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 09:58:51**	In Bearbeitung	Thomas Rix	Details
2018-07-20 09:58:51	Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 09:58:51**	Neu	---	Details Übernehmen
2018-07-20 09:58:51	Schwachstelle CVE-2004-2320 (+1) auf Endgerät b8:27:eb:a2:df:9f	6	**2018-07-22 09:58:51**	Neu	---	Details Übernehmen
2018-07-20 09:58:51	Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 09:58:51**	Neu	---	Details Übernehmen
2018-07-20 09:58:51	Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 09:58:51**	Neu	---	Details Übernehmen
2018-07-20 09:58:51	Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 09:58:51**	Neu	---	Details Übernehmen
2018-07-20 09:58:52	Schwachstelle CVE-2003-1418 auf Endgerät b8:27:eb:a2:df:9f	4	**2018-07-22 09:58:52**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	3	**2018-07-25 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle CVE-2003-1418 auf Endgerät b8:27:eb:a2:df:9f	4	**2018-07-22 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle CVE-2003-1567 (+1) auf Endgerät b8:27:eb:a2:df:9f	6	**2018-07-22 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 10:16:57**	Neu	---	Details Übernehmen
2018-07-20 10:16:57	Compliance-Verletzung durch Schwachstelle CVE-1999-0524 auf Endgerät b8:27:eb:a2:df:9f	0	**2018-07-25 10:16:57**	Neu	Thomas Rix	Details
2018-07-20 11:29:26	Netzwerkverkehr außerhalb der erlaubten Zeiten von 10.10.100.24 nach 10.241.0.10	10	**2018-07-21 11:29:26**	In Bearbeitung	Thomas Rix	Details
2018-08-06 11:51:23	Netzwerkverkehr außerhalb der erlaubten Zeiten von 10.10.100.11 nach 10.241.0.10	10	**2018-08-07 11:51:23**	Neu	---	Details Übernehmen
2018-08-06 11:51:23	Netzwerkverkehr außerhalb der erlaubten Zeiten von 10.10.100.11 nach 10.241.0.10	10	**2018-08-07 11:51:23**	Neu	---	Details Übernehmen

Umsetzung

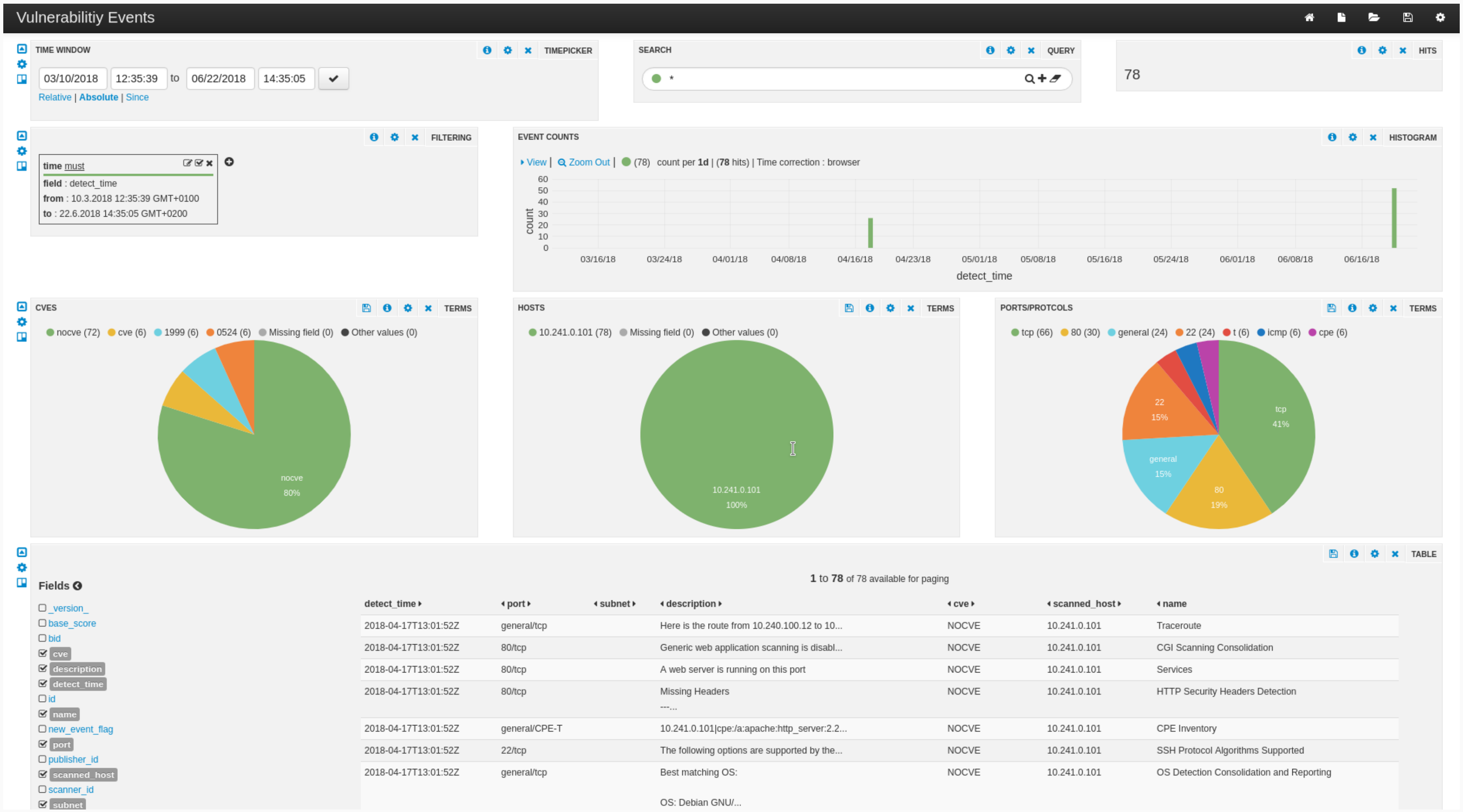
GUI-Oberfläche SIEM-GUI+



Umsetzung
GUI-Oberfläche

- SIEM-GUI+ dient als zentrale Oberfläche für die Benutzer
- Es werden Compliance- und Netzwerk-Zustände dargestellt
- Rechte- und Rollenmanagement mithilfe von LDAP
- Ticketsystem für Bearbeitung und Dokumentation von Vorfällen und deren Lösung
- Integration von VisITMeta zur Darstellung des IF-MAP Graphen

Umsetzung
Oberfläche Banana-GUI



Umsetzung
Oberfläche Banana-GUI

- Zweite Oberfläche Banana-GUI
- Dient der Verifikation und Nachvollziehbarkeit von Entscheidungen
- Aufbereitete Sicht auf Log-Informationen des Gesamtsystems
- Historische Sicht, da alle Informationen seit Systemstart dort abgelegt sind
- Audit-Oberfläche, um auch längere Zeiträume betrachten zu können

Umsetzung
Anwendungsszenarien

- Folgende Szenarien wurden bis zum Ende umgesetzt:
  - Aktualität Patch-Stand
  - Netzverkehr außerhalb der Arbeitszeit
- Weitere Szenarien sind geplant:
  - Sensitive Daten überwachen
  - Trennung von Produktions- und Office-Netzwerk
- Weitere Szenarien können nach Kundenanforderungen umgesetzt werden, zur Erhöhung der Funktionalität

Umsetzung
Dynamische Compliance

- Die Policy Engine (Esper, Camel) ist ein zentraler Punkt im CLEARER- System
- Diese führt die Compliance-Prüfung durch
  - Administrator definiert und konfiguriert Regeln sowie die Sensoren
  - Es werden alle Regeln ausgewertet, auf welche die Eingangsparameter passen
  - Jede Regelprüfung wird protokolliert

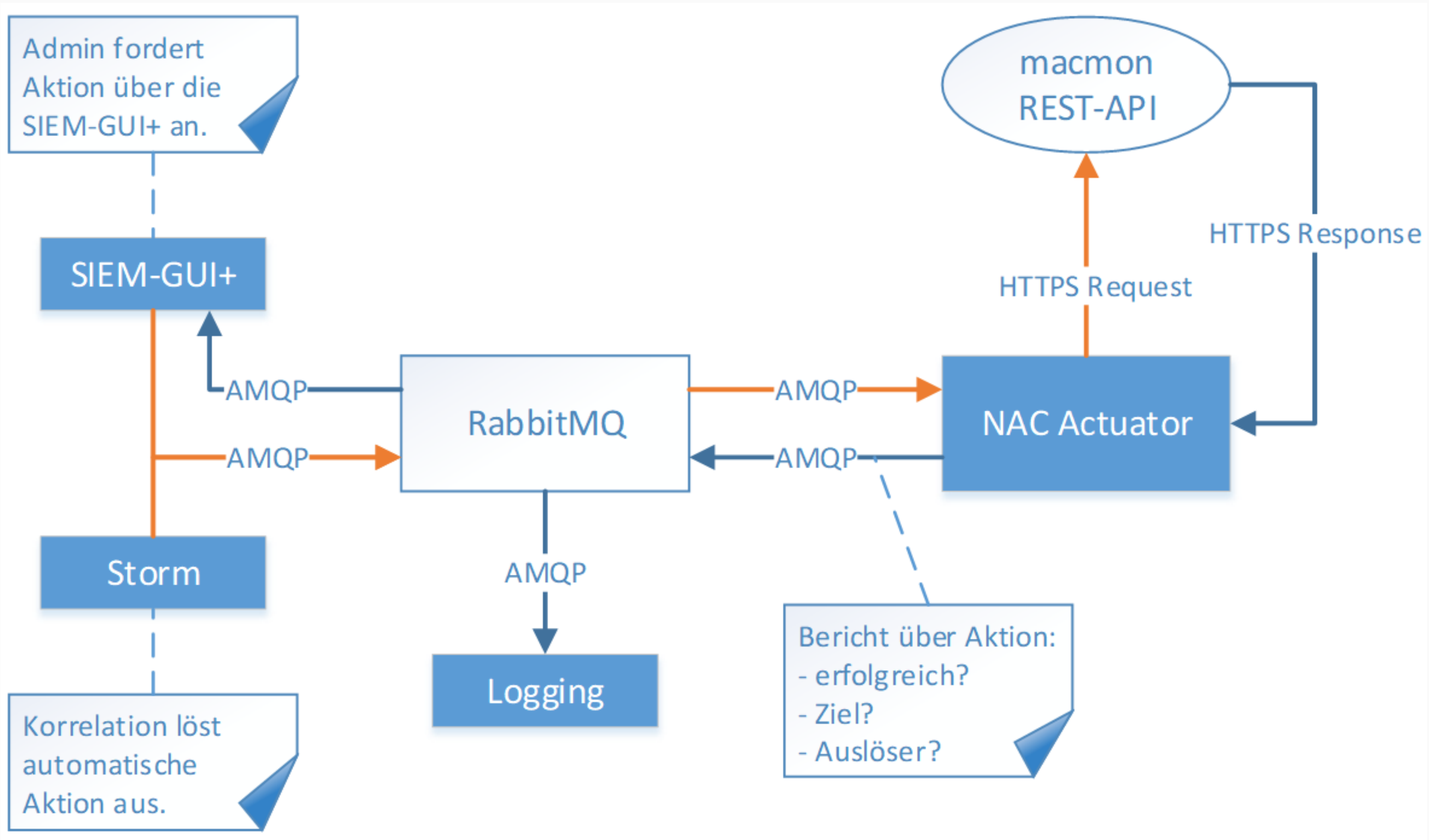
Umsetzung
Dynamische Compliance

- In CLEARER gibt es vier unterschiedliche Formen der dynamischen Compliance
  - Steuerung der Regelauswertung
  - Veränderbarkeit der Netzstruktur
  - Prioritätsschiebung
  - Automatische Regelsetzung

Umsetzung
NAC-Schnittstelle (1)

- Die Steuerung der Zugriffe der Endgeräte über das Compliance-Regelwerk erfolgt über die NAC-Schnittstelle
- Das NAC-System erhebt dabei die Infrastruktur und können von CLEARER zur Korrelation und Bewertung herangezogen werden
- Die Umsetzung erfolgte über eine Rest-API, unabhängig von einer bestimmten Herstellerlösung
- Aktionen können dadurch von CLEARER im NAC-System ausgelöst werden (z.B. Sperren/Entsperren von Endgeräten)
- NAC-Aktuator bereitet die Anfragen entsprechend auf

Umsetzung
NAC-Schnittstelle (2)



Fazit

- Ziel von CLEARER war die automatisierte Bearbeitung von relevanten Sicherheitsvorfällen für KMUs
  - Dafür mussten einige Anwendungsszenarien implementiert werden
  - Während des Projektes wurden nur zwei Szenarien umgesetzt
  - Das Ziel konnte bei noch geringer Funktionalität erreicht werden
  - Anbindung an das NAC-System macmon secure ist umgesetzt worden
- Architektur und Technologien sind leistungsfähig
- Weiterentwicklung zur Produktreife mit diversen Szenarien ist in Arbeit: Vorstellung auf der it-sa in Nürnberg im Oktober!
- Ein weiteres Szenario ist bereits umgesetzt worden
- Die SIEM-GUI+ wird ebenfalls kontinuierlich weiterentwickelt

.DECOIT®

Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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