

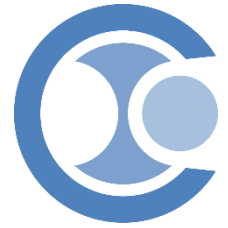
Erfüllung von Compliance- Anforderungen durch automatisierte Bearbeitung von Sicherheitsvorfällen

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

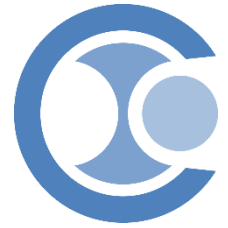


DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
<https://www.decoit.de>
info@decoit.de

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

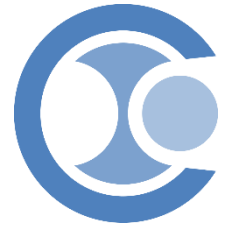


- 2-Jahres-Projekt ZIM (BMWi)
- Zeitdauer 01.05.2016 – 30.04.2018
- URL-Adresse: www.clearer-project.de
- Projektziel: Automatisierte IT-Compliance in Verbindung mit einem NAC-System
- Partner:
 - Industrie: DECOIT[®] GmbH, IT-Security@Work GmbH, macmon secure GmbH
 - Hochschulen: Hochschule Hannover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

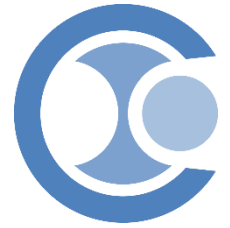


- Kontinuierliche Erhöhung der „Schnittstellen“ ins WWW
 - Internet of Things
 - Cloud Dienste
 - Industrie 4.0
 - Medical IT-Devices/Equipment
- Viele spezialisierte IT-Sicherheitskomponenten
- Die IT-Sicherheitskomponenten interagieren nicht oder nur rudimentär miteinander

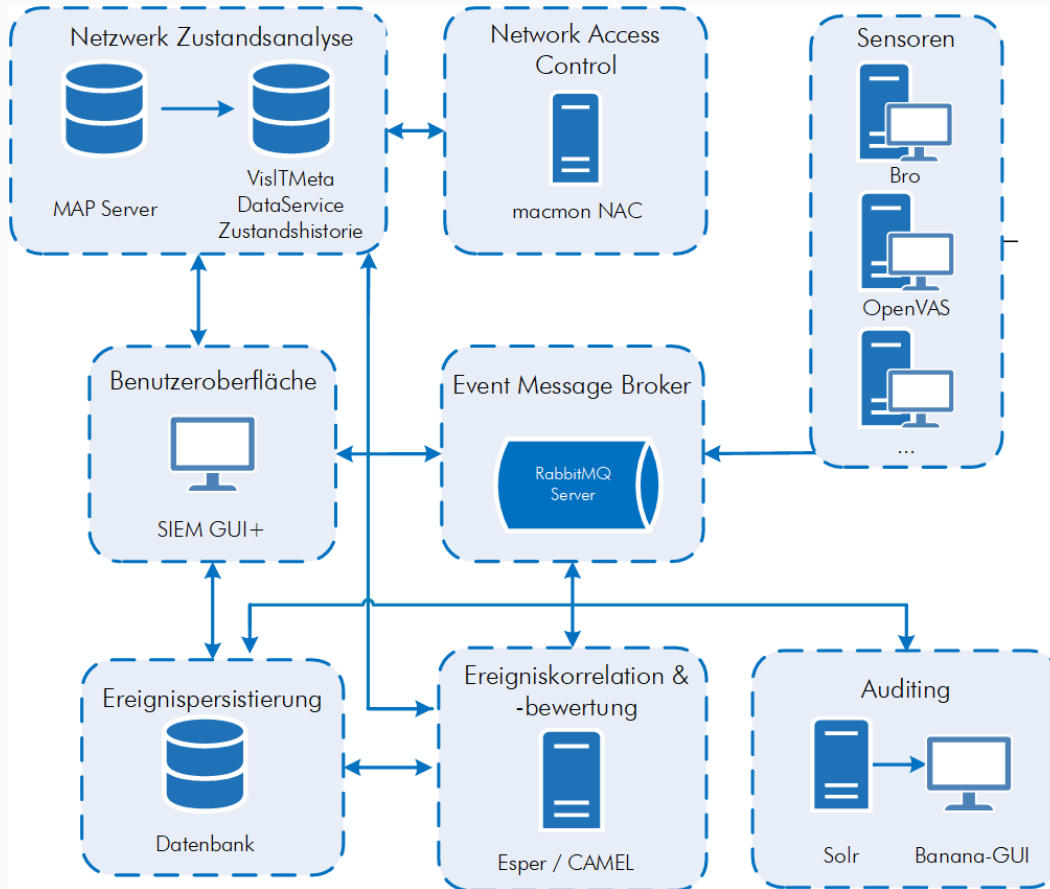
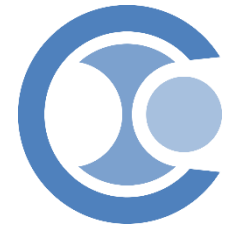
Eine stärkere Vernetzung aller IT-Sicherheitskomponenten muss erfolgen!



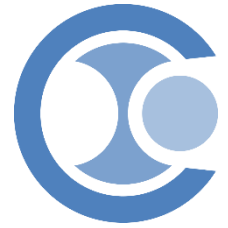
„Das Ziel des CLEARER-Projektes ist es, eine automatisierte Überwachung und Steuerung von Compliance-Aspekten in der IT auch für kleine Unternehmen zu ermöglichen.“



- 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



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



Übersicht

Vorfälle

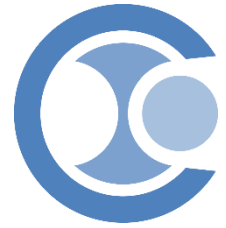
Status	Anzahl	Risikoklasse	Anzahl
Neu:	16	Hohes Risiko (7-10):	3
In Bearbeitung:	2	Mittleres Risiko (4-6):	4
Unbekannt:	0	Niedriges Risiko (0-3):	11

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



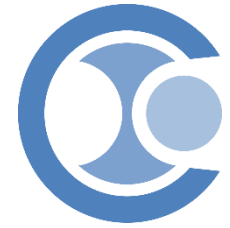


Vorfälle

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



Details für Vorfall

Allgemeine Informationen

Titel: Schwachstelle CVE-1999-0524 auf Endgerät b8:27:eb:a2:df:9f

Datum: 2018-07-20 09:58:51

Risiko: 0 (niedrig)

Fällig am: **2018-07-25 09:58:51**

Ticket

Bearbeiter: Thomas Rix

Status: In Bearbeitung [Abschließen](#)

Zeit gearbeitet: 0 Minuten

Zeit buchen: Minuten [Buchen](#)

Vorfallbeschreibung

Handlungsempfehlungen

- [Informationen über die gefundene Schwachstelle abrufen: CVE-1999-0524](#)
- Netzwerkzugriff für das Endgerät mit der MAC-Adresse **B8-27-EB-A2-DF-9F** sperren. ✔ Erfolgreich [Ausführen](#)

Verlauf [Kommentieren](#)

Erstellt 2018-07-20 09:58:52
von Administrator 09:58:52

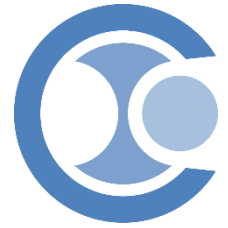
Das Ticket wurde erstellt

Übernommen 2018-07-20 10:10:10
von Thomas Rix 10:10:10

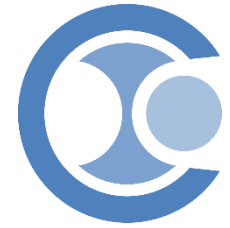
Die Bearbeitung wurde von **Thomas Rix** übernommen.

Status geändert 2018-07-20 10:26:05
von Thomas Rix 10:26:05

Der Status wurde von **NEW** auf **OPEN** geändert.



- 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



Vulnerability Events
🏠 📄 📧 📄 ⚙️

TIME WINDOW

03/10/2018 12:35:39 to 06/22/2018 14:35:05 ✓

Relative | Absolute | Since

TIMEPICKER

SEARCH

● *

Q+

HITS

78

FILTERING

time must

field : detect_time

from : 10.3.2018 12:35:39 GMT+0100

to : 22.6.2018 14:35:05 GMT+0200

EVENT COUNTS

View | Q Zoom Out | ● (78) count per 1d | (78 hits) | Time correction : browser

CVES

nocve (72) cve (6) 1999 (6) 0524 (6) Missing field (0) Other values (0)

HOSTS

10.241.0.101 (78) Missing field (0) Other values (0)

PORTS/PROTOCOLS

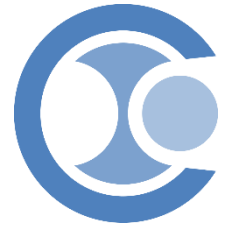
tcp (66) 80 (30) general (24) 22 (24) t (6) lcmp (6) cpe (6)

Fields

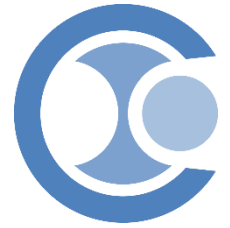
- _version_
- base_score
- bid
- cve
- description
- detect_time
- id
- name
- new_event_flag
- port
- publisher_id
- scanned_host
- scanner_id
- subnet

1 to 78 of 78 available for paging

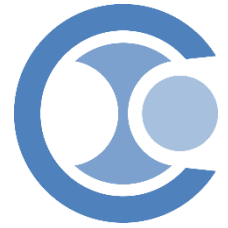
detect_time	port	subnet	description	cve	scanned_host	name
2018-04-17T13:01:52Z	general/tcp		Here is the route from 10.240.100.12 to 10...	NOCVE	10.241.0.101	Traceroute
2018-04-17T13:01:52Z	80/tcp		Generic web application scanning is disabl...	NOCVE	10.241.0.101	CGI Scanning Consolidation
2018-04-17T13:01:52Z	80/tcp		A web server is running on this port	NOCVE	10.241.0.101	Services
2018-04-17T13:01:52Z	80/tcp		Missing Headers	NOCVE	10.241.0.101	HTTP Security Headers Detection
2018-04-17T13:01:52Z	general/CPE-T		10.241.0.101/cpe/a/apache:http_server:2.2...	NOCVE	10.241.0.101	CPE Inventory
2018-04-17T13:01:52Z	22/tcp		The following options are supported by the...	NOCVE	10.241.0.101	SSH Protocol Algorithms Supported
2018-04-17T13:01:52Z	general/tcp		Best matching OS:	NOCVE	10.241.0.101	OS Detection Consolidation and Reporting
			OS: Debian GNU/...			



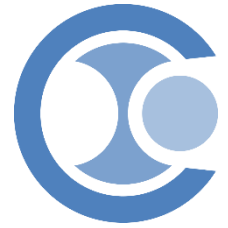
- Zweite Oberfläche Banana-GUI
- Dient der Verifikation und Nachvollziehbarkeit von Entscheidungen
- Aufbereitete Sicht auf Log-Informationen des Gesamtsystems
- Historische Sicht, da alle Informationen seit Systemstart dort abgelegt sind
- Audit-Oberfläche, um auch längere Zeiträume betrachten zu können



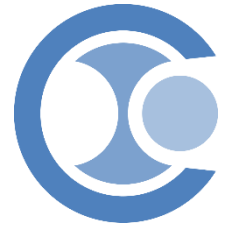
- Folgende Szenarien wurden bis zum Ende umgesetzt:
 - Aktualität Patch-Stand
 - Netzverkehr außerhalb der Arbeitszeit
- Weitere Szenarien sind geplant:
 - Sensitive Daten überwachen
 - Trennung von Produktions- und Office-Netzwerk
- Weitere Szenarien können nach Kundenanforderungen umgesetzt werden,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



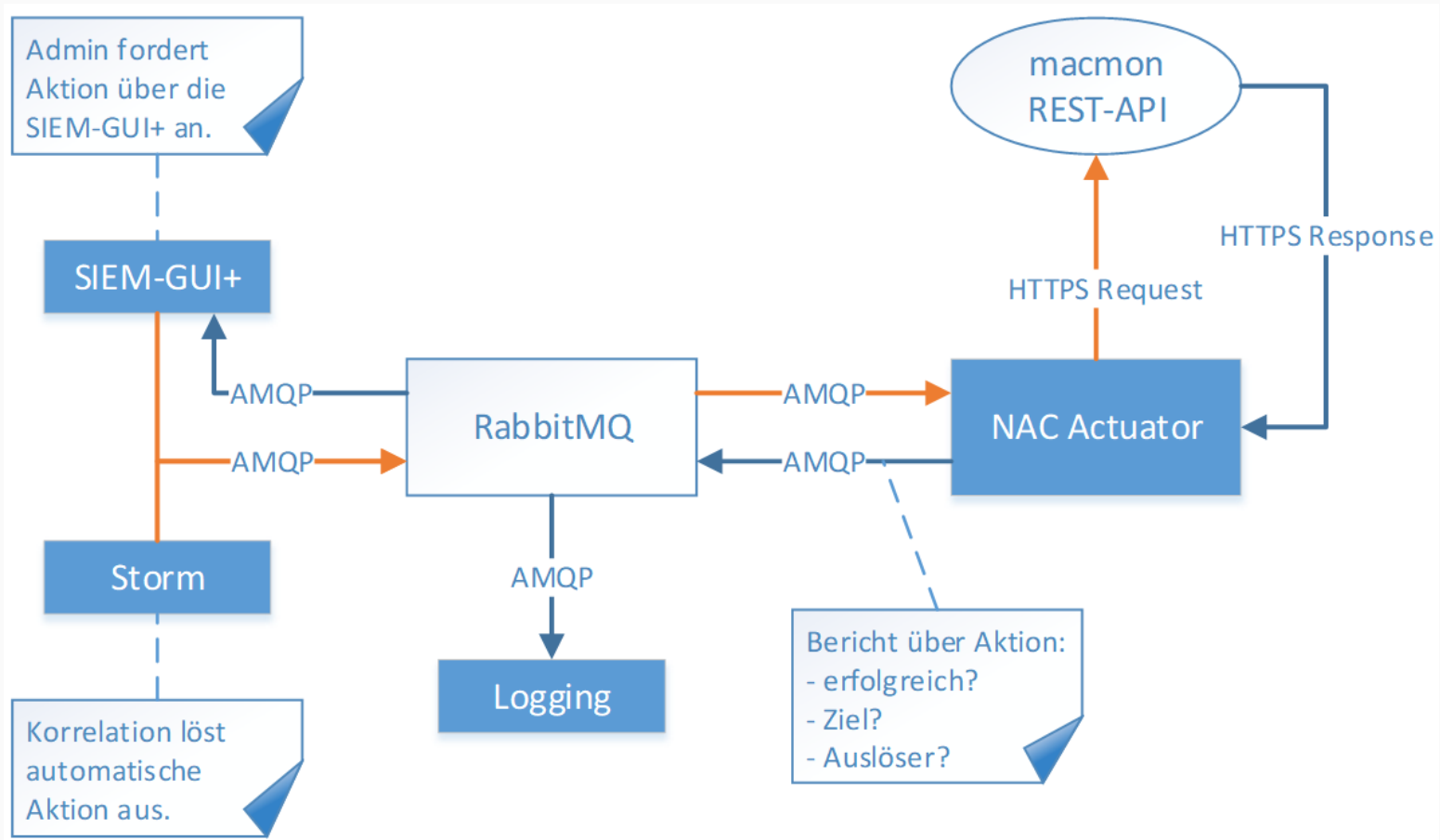
- Die Policy Engine (Esper, Camel) ist ein zentraler Punkt im CLEARER- System
- Diese führt die Compliance-Prüfung durch
 - Administrator definiert und konfiguriert Regeln sowie die Sensoren
 - Es werden alle Regeln ausgewertet, auf welche die Eingangsparmeter passen
 - Jede Regelprüfung wird protokolliert



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



- 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



- 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

Vielen Dank für Ihre Aufmerksamkeit!



DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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

