Erfüllung von Compliance-Anforderungen durch automatisierte Bearbeitung von Sicherheitsvorfällen

Kai-Oliver Detken[1] · Marcel Jahnke[1] · Thomas Rix[1] · Marion Steiner[2]

[1]DECOIT GmbH
{detken | jahnke | rix}@decoit.de

[2]IT-Security@Work GmbH
marion.steiner@isw-online.de

Zusammenfassung

Jedes Unternehmen, unabhängig von der Größe, besitzt heute eine IT-Infrastruktur, die zumindest mit Anti-Viren-Lösungen, Firewalls, Monitoring- und Backup-Systemen abgesichert ist. Oftmals kommen Remote-Zugänge mittels VPN-Gateway hinzu, die externen Mitarbeitern ermöglichen von außen sicher auf das Unternehmensnetz und seine Dienste zuzugreifen. Sind höhere Ansprüche vorhanden, so wird auf Zugangskontrolle mittels Network Access Control (NAC) oder Angriffserkennung über Intrusion Detection- (IDS) und Intrusion Prevention Systeme (IPS) gesetzt. Allerdings sind die verschiedenen Systeme oftmals als Insellösungen implementiert, insbesondere, wenn sie nicht vom gleichen Hersteller kommen. Um über seinen aktuellen Sicherheitsstatus Bescheid zu wissen und alle sicherheitsrelevanten Informationen auszuwerten, können Security Information and Event Management (SIEM) Systeme eingesetzt werden. Über solche Systeme lassen sich auch Richtlinien definieren, anhand derer Vorfälle zu Compliance-Anforderungen überwacht werden. Idealerweise beziehen solche SIEM-Lösungen auch andere Sicherheitssysteme über Schnittstellen mit ein und werten vorhandenen Logs mit aus. Es fehlen oftmals allerdings Möglichkeiten, eine automatisierte Bearbeitung von relevanten Sicherheitsvorfällen bzw. eine dynamische Anpassung der Compliance-Regeln abzubilden. Ebenso sind die Systeme meist nur von Systemexperten konfigurierbar, so dass dies nicht durch den Compliance- oder Informationssicherheitsbeauftragten erfolgen kann. Dies soll durch das Forschungsprojekt CLEARER nun ermöglicht werden.

1 Einleitung

Das Ziel des CLEARER-Projektes [CLEA18] ist es, eine automatisierte Überwachung und Steuerung von Compliance-Aspekten in der IT auch für kleine Unternehmen zu ermöglichen. Hierzu findet eine Vernetzung von Sicherheitssystemen wie Network Access Control (NAC), Intrusion Detection System (IDS) und Schwachstellen-Scanner statt, um Logdaten weiterer Systeme auszuwerten. Dadurch kann dann festgestellt werden, ob das Unternehmen definierte Richtlinien eingehalten oder verletzt hat. Über die SIEM-Funktionalität lassen sich Angriffe und Verstöße permanent erkennen, bewerten und entsprechend priorisieren. Anschließend können bei relevanten Events Reaktionen eingeleitet oder IT-Administrationen sowie Compliance-Beauftragte informiert bzw. bei Ausübung ihrer Arbeiten unterstützt werden. Der Aufbereitung

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 164-176.

aller gesammelten Daten fällt dabei eine wichtige Rolle zu, um bei erfolgten Angriffen eine einfachere Forensik zu ermöglichen.

Die zentrale Sammlung aller sicherheitsrelevanten Informationen muss dabei die Anforderungen der Nachvollziehbarkeit und Nachweisbarkeit erfüllen. Auditoren sollen durch das System in der Lage sein, eine Compliance-Statuskontrolle einfacher durchzuführen, während IT-Administratoren von verstehbaren Handlungsempfehlungen profitieren. Auf der einen Seite entsteht so eine große Datenmenge, um im Falle eines Audits die korrekte Funktion des Systems nachweisen zu können, und auf der anderen Seite sollten nur die relevanten Informationen den Nutzer erreichen, um ggf. eingreifen zu können oder informiert zu sein. Ebenso soll das System auf den aktuellen Zustand der IT-Umgebung eingehen können und anhand der vorliegenden Daten weiter lernen, Anomalien erkennen und diese melden. Dabei ist eine Zielsetzung, dass das IT-Compliance-Regelwerk dynamisch angepasst werden kann, um auf neue Bedrohungsszenarien schnell reagieren zu können. Als Basis für die Erkennung von Vorfällen wurden verschiedene Szenarien definiert, die zukünftig weiter ausgebaut werden sollen.

2 CLEARER-Architektur

Die letzte Version der CLEARER-Architektur besteht aus verschiedenen Komponenten (siehe Abbildung 1), von denen an dieser Stelle die Wichtigsten kurz beschrieben werden.

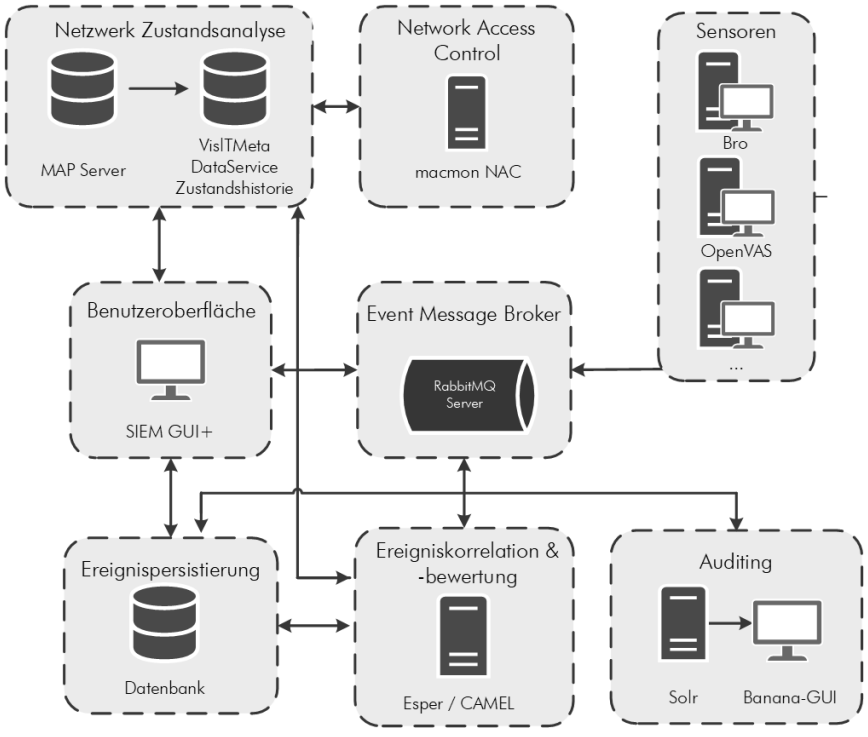

Abb. 1: CLEARER-Architektur in der Gesamtübersicht

Enthalten sind folgende Hauptkomponenten:

a. *MAP-Server / VisITMeta*: Netzwerk-Zustandsanalyse und Historie

b. *NAC-Modul*: Netzwerk-Zugangskontrolle sowie Bereitstellung von Infrastruktur- bzw. Zustandsdaten durch macmon NAC

c. *SIEM-GUI+*: Benutzeroberfläche und Event-Anzeige

d. *RabbitMQ*: Event Message Broker
e. *OpenVAS und Bro*: Sensoren zur Ereignis-Generierung
f. *MariaDB-Datenbank*: Ereignis-Persistierung
g. *Apache Camel*: regelbasierte Routing- und Konvertierungs-Engine
h. *Esper*: Ereigniskorrelation und -bewertung
i. *Solr und Banana-GUI*: Auditing und gezielte Suche

Bei der Verarbeitung wird eine Trennung von Ereignis- und Zustandsdaten vorgenommen. Das IF-MAP-Protokoll wird zur Kommunikation mit dem zentralen MAP-Server genutzt, der die Zustandsdaten der Infrastruktur verarbeitet. Der Event Message Broker wird hingegen als Message-Queue für die aufkommenden Ereignisse verwendet. Neben der Performance spielen hier auch Compliance-Anforderungen eine entscheidende Rolle. Protokolle und die verwendete Datenbank müssen eine schnelle Schreib-Performance aufweisen, um keine Ereignisse zu verlieren. Des Weiteren dürfen Ereignisse nicht verändert werden (Überprüfung der Compliance) und die Selbstüberwachung ist vorgesehen. Treten Verluste oder Inkonsistenzen auf, muss dies und der betroffene Zeitraum erkennbar sein.

2.1 Benutzer-Oberflächen

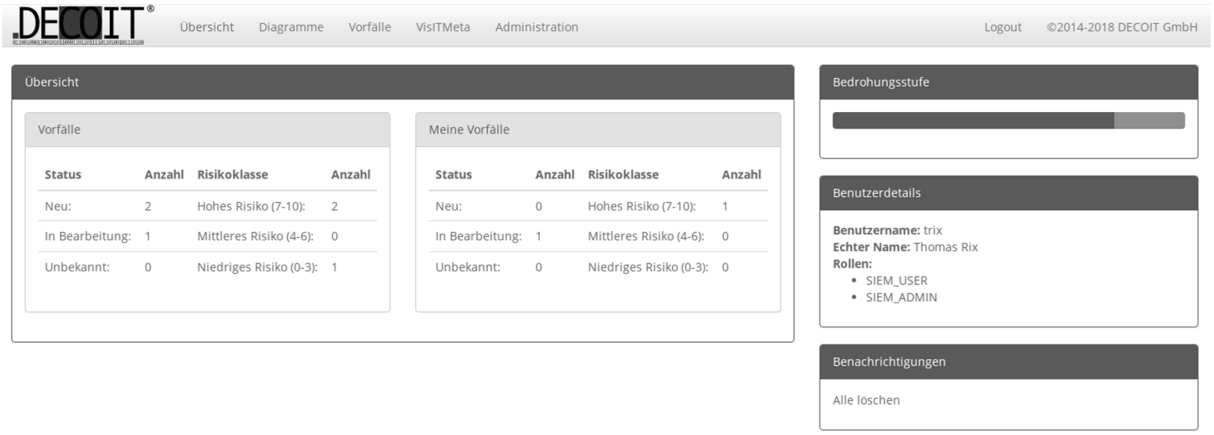

Abb. 2: Oberfläche der SIEM-GUI+

Die *SIEM-GUI+* fungiert als zentrale Oberfläche für den Benutzer des CLEARER-Systems (siehe Abbildung 2). Über sie wird daher die normale System-Funktionalität genutzt, d.h. es werden die Informationen über die Compliance- sowie Netzwerk-Zustände angezeigt und konfiguriert. Es wurde ein Rollen- und Rechtemanagement integriert, um Administratoren und Benutzer voneinander zu trennen. Im Hintergrund wird dabei auf einen LDAP-Server zurückgegriffen. Dies erleichtert die Integration des CLEARER-Systems in Infrastrukturen, die bereits einen Verzeichnisdienst verwenden, da so die Benutzer nur in einem System gepflegt werden müssen. Die GUI enthält auch ein integriertes Ticketsystem, auf das der Zugriff auf Tickets und Queues über Berechtigungen gesteuert wird. Die Ereignis-Ansicht der Oberfläche bietet zukünftig auch Filtermechanismen und Seitenumbrüche zur Aufbereitung der Anzeige, damit auch größere Ereignismengen angezeigt werden können.

Eine Vorfälle-Übersicht ermöglicht des Weiteren, mithilfe von Filterfunktionen nach Zeitraum oder Typ, die einfache Suche nach relevanten Compliance-Ereignissen. Weiterhin kann die

Oberfläche zum Verwalten des Regelwerks genutzt werden, indem Parameter der einzelnen Regeln dynamisch verändert werden können.

Eine weitere visuelle Anzeige in der SIEM-GUI+ verweist auf *VisITMeta* [VIME18], welches in der Lage ist IF-MAP-Graphen [TCG12] darzustellen. Dadurch kann der Netzwerkzustand übersichtlich angezeigt werden (siehe Abbildung 3). Die Zustandsinformationen sind dabei im MAP-Server als Datenbank enthalten. Auf sie wird via IF-MAP schreibend zugegriffen, um den Systemzustand zu aktualisieren. Für den lesenden Zugriff wird dem MAP-Server der Dataservice von VisITMeta nachgeschaltet. Dieser erlaubt den Zugriff auf die Historie des MAP-Graphen und ermöglicht so einen Blick auf vergangene Zustände.

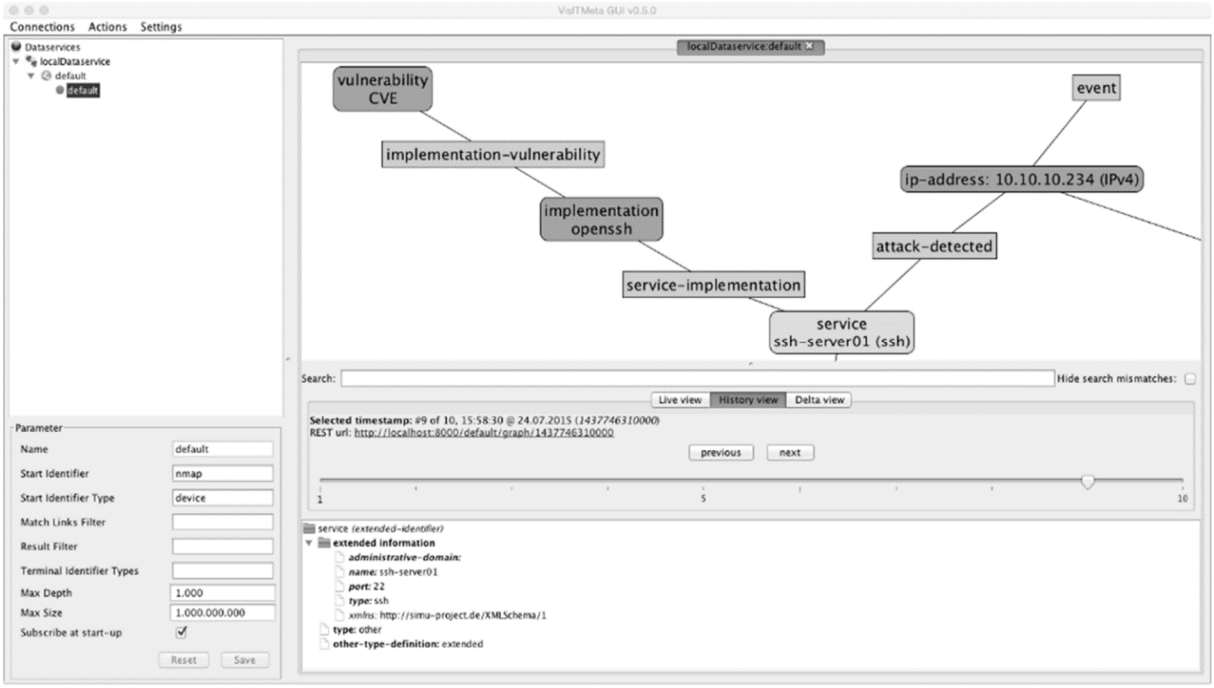

Abb. 3: IF-MAP-Graph von VisITMeta

Eine weitere Oberfläche in CLEARER ist die *Banana-GUI*. Sie dient dazu, die korrekte Funktion des Systems zu verifizieren und nachzuvollziehen sowie Verarbeitungsprobleme zu analysieren. Sie bietet dazu eine aufbereitete Sicht auf die Log-Informationen des Gesamtsystems und unterscheidet sich von der Statusanzeige der SIEM-GUI+ durch eine historische Sicht auf die Log-Informationen. Hiermit lassen sich z.B. die Entscheidungen des Regelwerks in CLEARER zu jedem beliebigen Zeitpunkt in der Historie nachvollziehen. Diese GUI erlaubt es insbesondere auch, die korrekte Funktionsweise des Systems zu analysieren, und somit die Korrektheit der Compliance-Meldungen durch CLEARER nachzuvollziehen. Im Gegensatz zur Statusanzeige der SIEM-GUI+ unterstützt die Banana-basierte Log-Ansicht eine freie Konfiguration der angezeigten Diagramme und Berichte. Diese freie Konfiguration unterstützt Audit-Prozesse maßgeblich, da sich das Berichtswesen auf die Anforderungen des Auditors anpassen lässt. Durch die Trennung der operationalen Statusanzeige der SIEM-GUI+ und der historischen Sicht der Log-GUI Banana sind die Anwendungsfälle strikt voneinander getrennt und eine einfachere Abschottung und eventuelle Pseudonymisierung von Daten in der Statusanzeige wird möglich. Hierdurch können betriebsrechtliche Vorschriften in jedem Fall erfüllt werden. [DKRS17]

2.2 Module

Die interne Kommunikation wird über den RabbitMQ-Message-Broker [RABB17] und das Protokoll *Advanced Message Queuing Protocol (AMQP)* [AMQP17] durchgeführt. Insbesondere Ereignisdaten, Korrelationsergebnisse etc. werden darüber übertragen. Dazu dienen je nach Anwendungsfall verschiedene AMQP-Exchanges und Message-Queues, wodurch eine Nachricht auf einfache Art und Weise an viele interessierte Empfänger geschickt werden kann. Sie müssen sich lediglich beim RabbitMQ die entsprechenden Message-Queues abonnieren. Um bei einer hohen Anzahl von Ereignissen zumindest die Größe der einzelnen Nachrichten selbst klein zu halten und so den Traffic zu reduzieren, wird der Inhalt der AMQP-Nachrichten im *CBOR* Datenformat [BOHO13] kodiert.

Um externe Sensoren, wie beispielsweise OpenVAS oder das IDS Bro, an den Message-Broker anzuschließen, werden entsprechende Komponenten benötigt, die die Daten in das CLEARER eigene Format konvertieren und die Kommunikation mit dem Broker übernehmen. Für viele Tools, die ihre Ereignisdaten über Logs zur Verfügung stellen, kann der DECOmap [SIMU2015] verwendet werden. Bei anderen Sensoren kommen speziell auf diesen Sensor zugeschnittene Entwicklungen zum Einsatz. Im Fall von OpenVAS wird ironvas [HSH18] verwendet, was es zusätzlich ermöglicht, OpenVAS-Scans über entsprechende AMQP-Nachrichten durch das CLEARER-System selbst zu starten. Somit kann automatisch geprüft werden, ob eine erkannte Schwachstelle nach einer gewissen Zeit behoben wurde.

Die Ereigniskorrelation ist einer der zentralen Bausteine des CLEARER-Systems. Diese arbeitet mit den Rohdaten der verschiedenen Sensoren, erkennt in diesen mit Hilfe eines Regelwerks bestimmte Muster und erzeugt daraus vordefinierte, abstrahierte Informationen. Diese werden in einem weiteren Schritt bewertet und von der Policy-Engine genutzt, um (sicherheitsrelevante) Vorfälle und im Speziellen Verletzungen von Compliance-Regeln zu erkennen. Für die Ereigniskorrelation wurde die CEP-Engine *Esper* [ECBR09] ausgewählt. Es wird außerdem für die Bewertungs-Engine verwendet. Die umfangreichen Korrelationsmöglichkeiten Espers erleichtern dabei die Bewertung. Durch die universelle Ausrichtung und Abfragesprache von Esper ist die Korrelation unterschiedlicher Ereignisse gegeben. Außerdem bietet Esper Zeitfenster und Operatoren zur Korrelation von Ereignissen aufgrund der zeitlichen Reihenfolge an. Weiterhin erlaubt Esper die Verwendung von Variablen in Statements. Das ermöglicht es, bestimmte Parameter von Szenarien zur Laufzeit über die SIEM-GUI+ den eigenen Anforderungen anzupassen, ohne die komplette Engine neu starten zu müssen.

Die technische Umsetzung der *Policy-Engine* erfolgt ebenfalls über die CEP-Engine Esper. Dabei gestalten sich die Anforderungen im Vergleich zu der Bewertungs-Engine nicht wesentlich anders. Die Policy-Engine nimmt die bewerteten Ereignisse der Bewertungs-Engine entgegen. Wie die Bewertungs-Engine benötigt auch die Policy-Engine den Zugriff auf IF-MAP-Zustandsdaten und auf aktuelle sowie ggf. vergangene Ereignisdaten. IF-MAP-Daten werden in der ersten Umsetzung nur gelesen. Der größte technische Unterschied zur Bewertungs-Engine liegt in der Reaktion auf Ereignisse, auf die eine Aktion erfolgen muss. Außerdem kann die Anzeige des Compliance-Status über eine direkte Anbindung oder den Umweg über die Datenbank realisiert werden. [DKRS17]

Der von Ereigniskorrelation und Policy-Engine benötigte Zugriff auf Zustandsdaten und vergangene Ereignisdaten wird nicht direkt über Esper selbst realisiert. Stattdessen werden die Esper-Statements als Teil einer Apache-Camel-Route ausgeführt. Dieses Vorgehen erlaubt es, eingehende Sensordaten mit Szenario-spezifischen Daten anzureichern. Beispielsweise kann

der aktuelle Zustand über VisITMeta angefragt werden, um zu einer vom Sensor gelieferte IP-Adresse die aktuell zugeordnete MAC-Adresse zu ermitteln oder die Rolle eines Benutzers auszulesen, um diese Information später in die Bewertung einfließen zu lassen. Der Zugriff auf vergangene Events ist über diesen Ansatz ebenfalls möglich, indem die gewünschten Daten aus der Ereignisdatenbank abgefragt werden. Dies erlaubt es unter anderem den Kontext eines verspätet eingetroffenen Ereignisses wiederherzustellen, um eine erneute Bewertung einer Situation durchführen zu können. Neben dem Anreichern von eingehenden Ereignissen werden diese Daten primär für spätere Audits abgelegt. Zusätzlich erhält auch die SIEM-GUI+ lesenden Zugriff auf die Daten, um beispielsweise auf den Vorfallmeldungen entsprechende Tickets zu generieren. Zusätzlich kümmert sich Camel darum, die eingehenden Sensordaten den jeweiligen Szenarien zuzuordnen.

Um die Szenarien zentral über die SIEM-GUI+ konfigurieren zu können, stellt die SIEM-GUI+ eine *zentrale Management Komponenten (ZMK)* bereit. Damit die ZMK nicht aktiv herausfinden muss, welche Komponenten aktuell verwendet werden und welche dieser Komponenten über die Änderungen bestimmter Parameter informiert werden müssen, melden sich stattdessen die Komponenten selbst bei der ZMK an. Dies erlaubt es den einzelnen Komponenten bei Bedarf die aktuelle Konfiguration von einer zentralen Anlaufstelle zu beziehen und sich für zukünftige Updates einzutragen. Der Austausch der Szenario-Konfigurationen erfolgt über den vorhandenen RabbitMQ. Dabei wird die initiale Anfrage nach der aktuellen Konfiguration direkt von der ZMK beantwortet. Für spätere Updates trägt sich der Client in den entsprechende Exchange mit dem Routing Key seines Szenarios ein.

Eine weitere Aufgabe der ZMK, ist die Verwaltung von Zertifikaten aller CLEARER-Komponenten. Um die Kommunikation der einzelnen Komponenten abzusichern, verwenden diese SSL/TLS. Entsprechend wird ein Mechanismus benötigt, um zum einem initiale Zertifikate zu generieren und zum anderen, um Zertifikate zu aktualisieren. Dabei agiert die ZMK wieder als Server und bildet die CLEARER interne Root-CA. Als Client ist auf jeder Komponente ein ZMK-Agent vorhanden, der das Schlüsselmaterial der jeweiligen Komponente verwaltet. Um ein neues Zertifikat durch die ZMK signieren zu lassen und so eine für alle Komponenten vertrauenswürdige Zertifikatskette aufzubauen, erstellt der Client zu seinem Zertifikat einen sogenannten *Certificate Signing Request (CSR)*. Damit die ZMK den initialen CSR zulässt, muss der Client ein über die SIEM-GUI+ generierten CSR-Token vorlegen. Ein CSR-Token kann nur ein einziges Mal genutzt werden und die Gültigkeit eines nicht genutzten Tokens verfällt nach einer kurzen Zeit. Über den Umweg der Tokens wird verhindert, dass unbemerkt Zertifikate durch die ZMK signiert werden. Solange ein so durch die ZMK signiertes Zertifikat gültig ist, erlaubt die ZMK weitere CSRs zu diesem bekannten Public Key. Das erlaubt es dem ZMK-Agent sein Zertifikat automatisch zu verlängern, weshalb relativ kurze Laufzeiten für die Zertifikate gewählt werden können (z.B. 90 Tage).

2.3 NAC-Schnittstelle

Das CLEAER-System verfügt über eine *Schnittstelle* zu NAC-Systemen, um diese um SIEM-Funktionalität zu ergänzen und damit eine Steuerung der Zugriffe durch Endgeräte über Compliance-Regelwerke zu ermöglichen. Dazu benötigt das CLEARER-System Zugriff auf die vom NAC erhobenen Infrastrukturdaten wie bekannte Systeme im Netzwerk, deren IP- und MAC-Adressen sowie authentifizierte Benutzerkonten. Diese Daten werden vom NAC-System im Zustandsspeicher abgelegt und von CLEARER bei der Korrelation und Bewertung von Ereignissen herangezogen. Bei der Anbindung von *macmon secure* [MACM18] wurde auf eine

REST-API-Schnittstelle zurückgegriffen (siehe Abbildung 4), die es seit der neusten Version des NAC-System gibt. Dadurch lassen sich alternativ auch andere NAC-Lösungen integrieren, wodurch man nicht auf einen bestimmten Hersteller angewiesen ist.

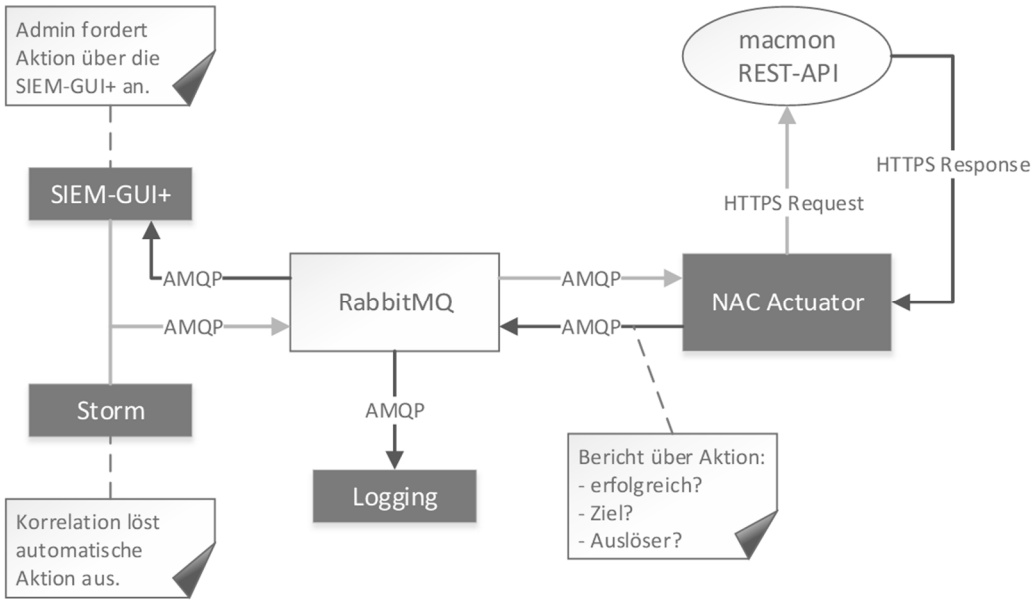

Abb. 4: NAC-Schnittstelle von CLEARER über REST-API

Über die CLEARER-API können nun Aktionen im NAC-System ausgelöst werden, wie beispielsweise das Sperren oder Entsperren von Geräten über die MAC-Adresse. Auch Infrastrukturdaten lassen sich austauschen. Zur Herstellerunabhängigkeit wurde ein *NAC-Aktuator* entwickelt, der eingehende Anfragen entsprechend aufbereitet. Eine Kommunikation ist über die REST-API in jedem Fall in beide Richtungen möglich.

3 Anwendungsszenarien

Um die Einhaltung von Compliance-Anforderungen im Unternehmensnetz überwachen zu können, wurden Anwendungsszenarien definiert und implementiert. Denn nur Anforderungen, die das System kennt, kann es auch überprüfen um Anomalien feststellen. Innerhalb des Projektes wurden daher zunächst vier Szenarien festgelegt, die nach Bedarf erweitert werden können:

a. **Aktualität Patch-Stand in einer Windows-Umgebung:** die Updates von Windows-Systemen werden überwacht und Alarmmeldungen ausgegeben, wenn nach einer definierten Zeit offene Sicherheitspatches nicht eingespielt wurden.

b. **Trennung von Produktions- und Office-Netzwerk:** Anhand von Netzwerkscans wird auf unterschiedliche Netze Rücksicht genommen und Analysen über den Sicherheitszustand durchgeführt.

c. **Netzverkehr außerhalb der Arbeitszeit:** Anomalien können sich auch durch Netzwerkverkehr äußern, der plötzlich zu ungewohnten Zeiten auftritt.

d. **Sensitive Daten überwachen:** Dateien auf Serversystemen, die mittels Integritätscheck gesichert wurden, werden auf Veränderungen überwacht.

Mit Hilfe dieser Szenarien kann beispielsweise eine Schwachstelle identifiziert und priorisiert werden. So können Scans automatisch in bestimmten Abständen oder manuell durchgeführt

werden. Die Ergebnisse werden dann anhand von Infrastrukturinformationen bewertet und in der SIEM-GUI+ entsprechend angezeigt. Es wird ein Ticket generiert und eine E-Mail mit einer Handlungsempfehlung an den IT-Administrator gesendet. Nach beispielsweise 30 Tagen wird ein neuer Scan ausgeführt und erkannt, dass die Schwachstelle immer noch existiert. Es wird daher zusätzlich zu dem vorhandenen Ticket eine Compliance-Verletzung gemeldet. Zusätzlich erfolgt eine Protokollierung für die Rückverfolgbarkeit der Compliance. Durch die aktuell verwendeten Tools können Schwachstellen unterschiedlicher Betriebssysteme ermittelt werden. Grundsätzlich wird darauf geachtet, dass die Umsetzung der Szenarien unabhängig vom Zielsystem ist. Dennoch können aber auch Spezialfälle für bestimmte Systeme unterstützt werden.

4 Dynamische Compliance

Die *Policy Engine* stellt einen zentralen Punkt der CLEARER-Architektur dar. Sie führt auf Basis der von den Sensoren gesammelten Informationen die Compliance-Überprüfung durch und stößt, wo nötig, geeignete Reaktionen an (siehe Abbildung 5). Dieser Vorgang lässt sich in folgende Stufen einteilen:

a. Vor und während dem Einsatz von CLEARER werden durch den Administrator Regeln konfiguriert. Hierzu kann die dafür vorgesehene SIEM-GUI+ sowie Esper verwendet werden. Sobald die einzusetzenden Sensoren konfiguriert sind und Daten liefern, bewertet die Policy Engine diese auf Basis der eingestellten Regeln.

b. Grundsätzlich werden alle Regeln ausgewertet, bei denen die eingehenden Informationen den Eingangsparameter entsprechen und dann wird eine definierte Aktion ausgelöst. Falls für die Auswertung einer Regel Informationen über aktuelle Zustände im Netzwerk (z.B. welche Nutzer gerade angemeldet sind) relevant sind, werden diese aus den Zustandsspeicher abgerufen und ebenfalls ausgewertet. Regelüberprüfungen können regelmäßig oder anlassbezogen, wie etwa nach Eingang einer bestimmten Informationsart, stattfinden.

c. Das Prüfen der Regel wird protokolliert. Hierbei werden sowohl die Tatsache, dass eine Regelprüfung erfolgte, als auch die dabei getroffene Entscheidung, die dazu führenden Gründe – also die Informationen, die als Eingabe für die Regel dienten – und eventuell ausgelöste Reaktionen aufgezeichnet. Diese automatisch auszuführenden Reaktionen sind vom Administrator dem durch das jeweilige Bedrohungsszenario entstehenden Risiko angemessen zu konfigurieren. Die Reaktionen können dabei von „nichts tun“ über eine einfache Benachrichtigung des für den jeweiligen Bereich Verantwortlichen bis hin zu konkreten Anweisungen, was ein Administrator zu tun hat oder zum automatisierten Eingriff durch das System (z.B. zur Abschottung ganzer (Teil-)Netze), reichen.

Die Funktionalität kann folgendes Szenario verdeutlichen: anhand einer eingehenden Logdatei eines VPN-Gateways wird erkannt, dass ein Nutzer via VPN eine Verbindung zum Unternehmensnetzwerk hergestellt hat. Die Information „angemeldet via VPN“ wird mit Verknüpfung zum betroffenen Nutzer im Zustandsspeicher abgelegt. Die Meldung der Anmeldung löst darüber hinaus eine Regelkontrolle aus. Die zugehörige Regel besagt, dass Dateien, die als „streng geheim“ klassifiziert sind, nur auf dem Unternehmensgelände eingesehen werden dürfen. Die Policy Engine prüft daher den Zustand des Nutzers, erkennt diesen als per VPN angemeldet und lässt als Reaktion die Zugriffsrechte des Nutzers auf alle ihm normalerweise zur Verfügung

stehenden streng geheimen Dateien sperren und protokolliert die Entscheidung und die darauffolgende Reaktion. Sobald der Nutzer die VPN-Verbindung beendet werden die Dateien auf demselben Weg wieder freigegeben.

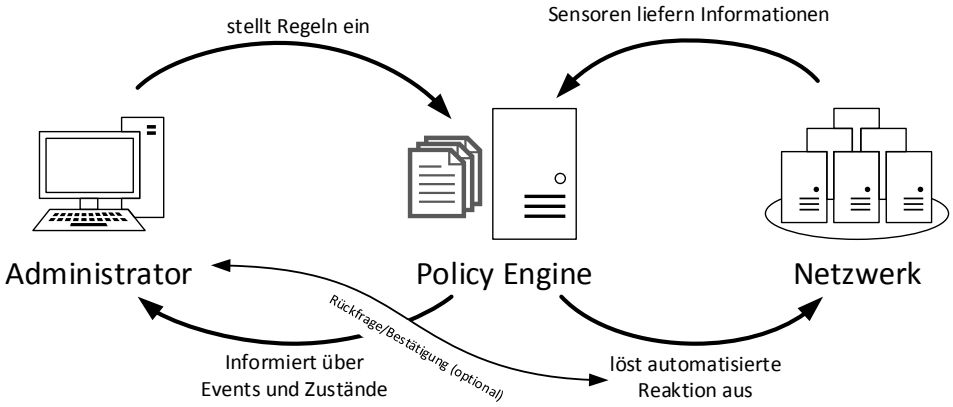

Abb. 5: Prozessablauf der Policy Engine zur Compliance-Überprüfung

In einem anderen Beispiel wird erkannt, dass ein Sicherheits-Update für eine im Unternehmen eingesetzte Software verfügbar ist. Dieses Event starten einen Timer, nach dessen Ablauf eine Regelüberprüfung stattfindet, bei der für jedes Gerät einer festgelegten Gruppe die aktuell installierte Version der Software geprüft wird. Ist das Update installiert, wird dies protokolliert und keine Reaktion ausgelöst. Falls nicht, wird eine Benachrichtigung an den Nutzer des Geräts und/oder den zuständigen Administrator gesendet.

4.1 Anwendungsbeispiele

Zur Umsetzung der *dynamischen Compliance-Überwachung* wird zwischen verschiedenen Varianten der Dynamik unterschieden:

a. *Steuerung der Regelauswertung*: für konkrete Events/Eventtypen durch Administratoren/Compliance-Officer, basierend auf einem konkreten Vorfall, kann die Reaktion bei Folgeaktionen angepasst werden.

b. *Veränderbarkeit der Netzwerkstruktur*: die Überwachung erfolgt nicht nur auf statischen Regeln, sondern bezieht auch Veränderungen im Netzwerk mit ein. Änderungen im Netzwerk können zu anderen Regelergebnissen führen, ebenso können Änderungen im Netzwerk die Auswertung von Regeln auslösen.

c. *Prioritätsverschiebungen*: Basierend auf Erfahrungswerten können Regeln nicht nur für einzelne Events angepasst, sondern die grundsätzlichen ausgelösten Reaktionen können im laufenden Betrieb verändert werden.

d. *Automatischer Regelsetzung*: Das System kann selber neue Regeln lernen, in dem es das Systemverhalten lernt sowie Anomalien erkennt und bewertet. Je nach Event kann das System dabei ggf. eine konkrete Reaktion vorschlagen oder aber für eine erkannte Anomalie nachfragen, ob der Benutzer hierfür eine Reaktion definieren möchte.

Detektiert CLEARER beispielsweise einen Verstoß gegen eine Compliance-Regelung im Unternehmensnetz, wird der Administrator über die SIEM-GUI+ in Kenntnis gesetzt und ggf. ein Vorschlag zur Lösung der gegebenen Situation angezeigt. Bei diesen Meldungen ist es möglich, diese bewusst abzulehnen und das damit möglicherweise entstehende Risiko zu akzeptieren. Es

ist aber auch möglich, zum Ablehnen die Zustimmung eines Compliance-Verantwortlichen oder die Angabe einer Begründung zu fordern. Das Ablehnen von Meldungen wird in jedem Fall dokumentiert und erfüllt so die Anforderungen aus dem Risikomanagement. Es ist darüber hinaus möglich, die Priorität einer Meldung in der SIEM-GUI+ festzulegen bzw. abzuändern. Auch solche Maßnahmen müssen protokolliert werden.

Ein Administrator bzw. Compliance-Officer ist außerdem in der Lage, das Regelwerk zur Laufzeit von CLEARER zu ändern, um so schnell auf geänderte Umstände in der Infrastruktur oder auf Schwächen der Regelkonfiguration reagieren zu können und Ausfallzeiten zu minimieren. Solche Änderungen im Regelwerk bergen ein nicht unerhebliches Sicherheitsrisiko, denn wenn sie missbräuchlich erfolgen, wird die Compliance-Prüfung quasi außer Kraft gesetzt. Entsprechend sind sie zu protokollieren und – zumindest in besonders sensiblen Umgebungen – dem Vieraugenprinzip zu unterstellen.

Das Netzwerk in einem Unternehmen ist stetigen Veränderungen unterworfen. CLEARER ist in der Lage sein, auf diese Änderungen einzugehen. Zum einen erkennt CLEARER dazu neue Netzgeräte und zum anderen wendet es Regeln dafür an. Bei Nutzung neuer Netzgeräte, für die noch keine Regel existiert, sehen die Einsatzszenarien sinnvolle Standardwerte vor, die bei Bedarf von dem verantwortlichen Administrator angepasst werden können.

Auch eine automatische Prioritätsverschiebung ist möglich, etwa bei gefundenen Schwachstellen und den zugehörigen Patches oder beim automatischen Erkennen eines signifikanten Wechsels des Netzwerkbereichs eines Geräts, zum Beispiel aus dem internen Netz in eine DMZ. Durch die erhöhte Priorität werden anschließend Regelverletzungen mit Bezug zu diesem System als kritischer eingestuft, was dann beispielsweise den empfohlenen Bearbeitungszeitraum verkürzt oder die jeweiligen Vorfälle umgehend eskaliert.

4.2 Regelsprache

Die *Policy Engine* kontrolliert eingehende Events auf Basis der durch einen Benutzer bestimmten Regeln. Damit dieser die Regeln nicht direkt in technischer Form in den Konfigurationsdateien der Eventverarbeitung eintragen muss, soll eine leicht verständliche, von Menschen lesbzw. schreibbare Sprache entwickelt werden, in der diese Regeln stellvertretend geschrieben werden können. Diese Regeln sollen dann mithilfe eines Parsers, der die Regeln einlesen und interpretieren kann, in die technische Konfiguration der Policy Engine übertragen werden. Die Regeln werden dabei aus vier Teilen zusammengesetzt: Szenario-Auswahl, Anwendungsbereich, Entscheidungsgrundlage und Reaktion.

Eine Regel könnte dabei wie folgt aussehen:

```
GRANT_ACCESS
PERSON name_der_person
TO gebaeude_2
ALLOW
```

Schlüsselwörter werden dabei **fett** und Platzhalter für Werte *kursiv* geschrieben. Schlüsselwörter steuern das Verhalten der Regel und können einen oder mehrere Parameter erhalten. Format und Inhalt dieser Parameter sind vom Schlüsselwort abhängig. Die Reihenfolge der Schlüsselworte innerhalb einer Regeldefinition ist für jedes Szenario fest vorgegeben. Die Parameter stellen die Informationen dar, die vorliegen müssen, damit die Regel ausgewertet wird.

Jede Regel beginnt mit einem Schlüsselwort, das das Szenario eindeutig identifiziert. Das Szenario legt fest, was im Folgenden kontrolliert werden soll. Die in einem zu kontrollierenden Event benötigten Felder sind also direkt von der Art des Szenarios abhängig. Je nach gewähltem Szenario ändern sich die benötigten Parameter einer Regel und der Umgang damit.

Die weiteren Parameter einer Regel unterscheiden sich zwar abhängig vom gewählten Szenario, besitzen aber eine identische Struktur. Zunächst wird der Anwendungsbereich bzw. die von der Regel kontrollierten Entitäten definiert. Hierbei kann es sich beispielsweise um Nutzer(-gruppen), Hosts oder Netzwerkbereiche handeln. Dann wird die Bedingung angegeben, unter der die anschließend definierte Reaktion ausgelöst wird. Diese kann mit für dieses Szenario definierten Schlüsselworten auf eine feste Anzahl an Vorgängen eingeschränkt sein, beispielsweise **ALLOW** bzw. **DENY**. Soll eine freier gestaltbare Reaktion gewünscht sein, kann die Definition der Regeln für das jeweilige Szenario auch das Ausführen eines Programms oder Skripts mittels des Schlüsselworts **EXECUTE** vorsehen.

Die Parameter, die einem Schlüsselwort übergeben werden, enden immer am Beginn des nächsten Schlüsselwortes. Die Definition einer Regel endet immer mit dem nächsten auftretenden Szenario-bezeichnenden Schlüsselwort.

Zusätzlich zu den reinen Definitionen von Regeln erlaubt die vorgesehene Regelsprache Aliase für feste Werte, vergleichbar mit Konstanten in der Programmierung. Aliase müssen immer am Beginn eines Regeldokuments definiert werden. Die beiden dazu benötigten Teile sind:

1. Name des Alias (Schlüsselwort **SET** *name*)
2. Repräsentierter Wert (Schlüsselwort **TO** *wert*)

Das Anlegen von Aliasen dient einer Verbesserung der Übersichtlichkeit und Wartbarkeit der Regeldefinitionen. Dabei wird es auch möglich sein, anstelle eines einzelnen Werts in einem Feld eine kommagetrennte Liste von Werten anzugeben. Dies kann dann wie folgt aussehen:

```
SET host_a TO 127.1.2.7, 127.1.2.8
```

oder

```
GRANT_ACCESS
PERSON name_der_person, name_einer_anderen_person
TO gebaeude_2, gebaeude_3
ALLOW
```

Eine Regel, die eine Liste beinhaltet, wird immer dann angewendet, wenn ein Element aus jeder Liste im geprüften Event vorliegt.

4.3 Abstrakte Regeldefinition

Damit CLEARER eigenständig Entscheidungen über den Compliance-Status treffen kann, müssen *Regeln* in Bezug auf die Anwendungsszenarien definiert werden:

a. *Szenario Dateizugriffe*: Sämtliche Regeln sollen beim Erscheinen eines neuen Logeintrags auf diesen angewandt werden. Verzeichnisse sind wie Dateien zu behandeln. Die Regeln sollen mit einem logischen **AND** verknüpfbar und vom Administrator vorübergehend für bestimmte Nutzer deaktivierbar sein. Bausteine hierfür sind der zugreifende Nutzer, die betroffene Datei und die verwendete Zugriffsart. Dazu kommen das Ergebnis des Zugriffs, die Berechtigungen und der Zeitpunkt des Ereignisses.

b. *Szenario Zugriffsrechte*: Die Regeln für Zugriffsrechte werden bei jeder Änderung an diesen kontrolliert. Dateien und Verzeichnisse sind identisch zu behandeln. Bausteine sind der verwaltete Benutzer, die Zugriffsrechte des Benutzers auf Dateien und die Attribute des Nutzers.

c. *Szenario Patch-Status*: Die Notwendigkeit einer Software-Aktualisierung wird in CLEARER mithilfe eines Schwachstellenscanners erkannt. Findet dieser an einem System eine Schwachstelle, wird ein Timer gestartet oder ein Termin gesetzt, zu dem ein Update installiert sein soll, dass die Schwachstelle behebt. Bei Ablauf des Timers wird das betroffene System erneut gescannt. Die Bausteine hier sind die Information über den Fund einer Schwachstelle aus den Berichten des Schwachstellenscanners und Timer/Termine zu denen Updates fällig sind.

d. *Szenario „Nutzung unerlaubter Web-/Cloud-Dienste"*: Ausgehender Datenverkehr wird überprüft. Zusätzlich wird eine Möglichkeit zum Abfangen von gesendeten Paketen benötigt. Bausteine sind die White- bzw. Blacklist für Internetdienste sowie IP-Adressen von ausgehendem Datenverkehr.

e. *Szenario „Tor geschlossen während der Nachtstunden"*: Während ein Gerät nicht online sein sollte, wird dessen Onlinestatus regelmäßig überprüft. Bausteine hierfür sind die Liste von Geräten/Nutzern und deren erlaubten Online-Zeiträumen (Urlaub und andere Abwesenheiten einstellbar), die aktuelle Uhrzeit und der aktuelle Onlinestatus der Geräte. Mögliche Informationsquellen sind regelmäßiges Anpingen des Geräts, die Auswertung von Router-Logs und das Auslesen von An- und Abmeldungen aus Verzeichnisdiensten.

Als Reaktion auf das Erkennen eines Compliance-Vorfalls mithilfe einer der oben genannten Regeln wird ein Ticket generiert. Dieses enthält Informationen über den Vorfall, wie damit umzugehen ist und bis wann die Bearbeitung abgeschlossen sein soll. Das Ticket wird dem zuständigen IT-Administrator zugewiesen und ist zusätzlich für den Compliance-Verantwortlichen und dem Leiter des Bereichs, in dem sich der Vorfall ereignete, einsehbar (Überschneidungen bei den Personen möglich). Eine automatisierte Prüfung des Fälligkeitsdatums der Tickets ist nicht vorgesehen. Diese ist allerdings manuell problemlos möglich.

Automatische Reaktionen auf gefundene Vorfälle sind auf Basis von Erfahrungen bei verschiedenen Kunden nicht erwünscht, da das Risiko einer Einschränkung des Betriebs aufgrund von „false positives" zu hoch ist und die Nachvollziehbarkeit von Änderungen am überwachten System erschwert würde.

5 Resümee

Das CLEARER-Projekt ist angetreten, um eine automatisierte Bearbeitung von relevanten Sicherheitsvorfällen zu ermöglichen. Dies soll durch eine dynamische Compliance-Anpassung unterstützt werden. Um dieses Ziel zu erreichen, sind einige Anwendungsszenarien zu implementieren, damit das System lernen und Anomalien ausreichend erkennen kann. Während das Projekt dies nur exemplarisch anhand eines Prototypens zeigen konnte, muss die zukünftige Entwicklung zu einem Produkt zeigen, inwieweit die ursprünglichen Anforderungen sich umsetzen lassen. Eine Evaluierung über die Effektivität von CLEARER kann daher erst erfolgen, wenn mehr Szenarien integriert wurden. Dies hängt aber wiederum auch stark von zukünftigen Kundenanforderungen ab, so dass man auf die weitere Entwicklung gespannt sein darf.

Danksagung
Das CLEARER-Projekt (www.clearer-project.de) ist ein gefördertes BMWi-Projekt mit einer Laufzeit von zwei Jahren, welches im Mai 2016 seine Arbeiten aufnahm und im April 2018 endete. An dem Projekt waren die Firmen DECOIT GmbH (Projektleitung), IT-Security@ Work (ISW) und macmon secure GmbH sowie die deutsche Forschungseinrichtung Hochschule Hannover beteiligt. Als assoziierte Partner nahmen der Hersteller Achtwerk GmbH und der SIEM-Anbieter rt-solutions.de GmbH an dem Projekt teil. Daher gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten die erfolgreiche Projektarbeit erst ermöglicht haben.

Literatur

[AMQP18] Webseite des AMQP-Protokolls: http://www.amqp.org

[BOHO13] C. Bormann, P. Hoffman: Concise Binary Object Representation (CBOR). Internet Engineering Task Force (IETF), RFC-7049, Standards Track, IETF 2013.

[CLEA18] Webseite des F&E-Projektes CLEARER: https://www.clearer-project.de. BMWi-Projekt des ZIM-Förderrahmens

[DKRS17] Detken, Kleiner, Rohde, Steiner: IT-Sicherheitsanalyse durch NAC-Systeme mit SIEM-Funktionalität. In P. Schartner, A. Baumann (Hrsg.): DACH Security 2017, syssec (2017) 431-443.

[ECBR09] M. Eckert, F. Bry: Complex Event Processing (CEP). GI, 5. Mai 2009.

[HSH18] Hochschule Hannover: http://trust.f4.hs-hannover.de/index.html

[MACM18] Hersteller-Webseite von macmon secure: https://www.macmon.eu

[SIMU2015] Webseite des F&E-Projektes SIMU: https://www.simu-project.de. BMBF-Projekt von KMU-Innovativ

[TCG12] TCG Trusted Network Communications: TNC IF-MAP Metadata for Network Security. Specification Version 1.1, Revision 9, 7th of May 2012.

[VIME18] VisITMeta-Webseite: http://trust.f4.hs-hannover.de/projects/visitmeta.html