Intelligente Erkennung von Sicherheitsvorfällen durch SIEM-Systeme

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

Agenda

- Einführung in die SIEM-Thematik
- Korrelation von Events
- Hersteller- und Forschungsansätze
- F&E-Projektbeispiele
- Zusammenfassung

Kurzvorstellung der DECOIT GmbH

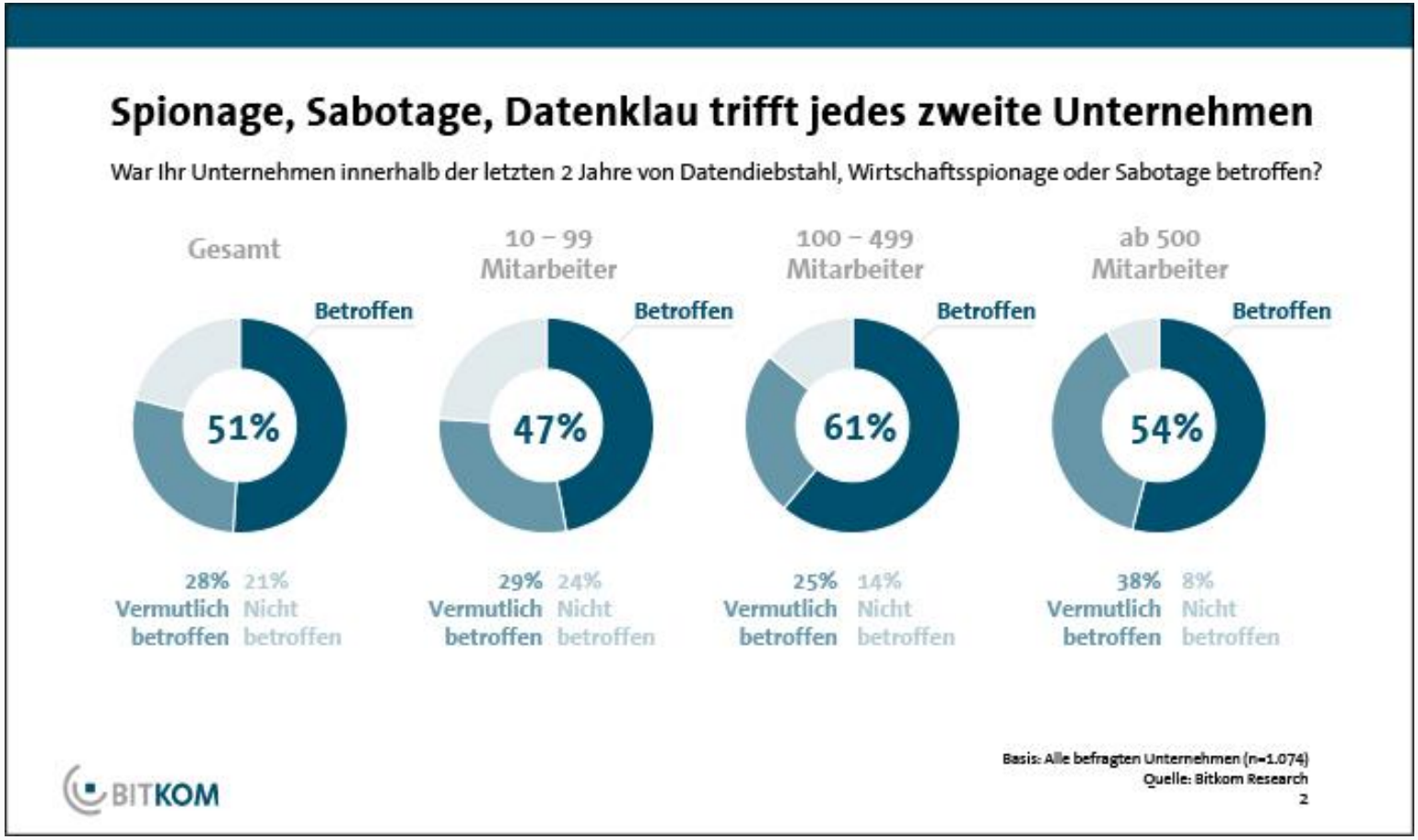
Bremer Systemintegrator u. Softwarehaus

- **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

DECOIT®

Einführung in SIEM-Thematik

BITKOM-Umfrage von 2015

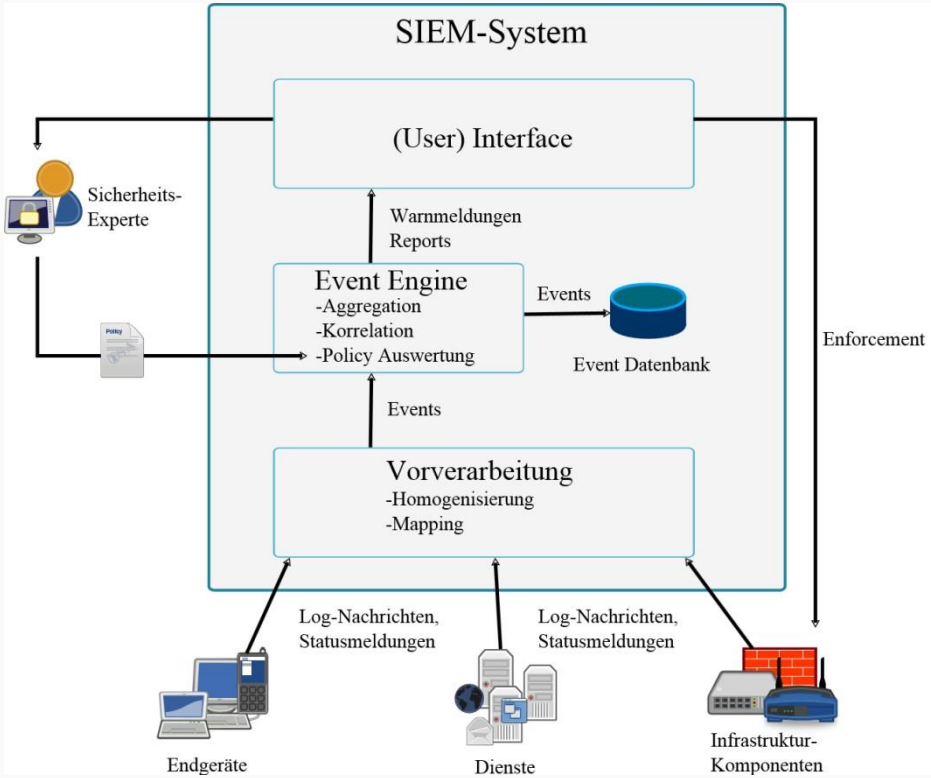


SIEM-Definition

- Der Begriff SIEM unterteilt sich in
  - Security Event Management (SEM)
  - Security Information Management (SIM)
- Das SEM-Sicherheitsmanagement beinhaltet:
  - Echtzeitüberwachung
  - Ergebniskorrelation
  - Event-Benachrichtigungen
- Das SIM-Sicherheitsmanagement beinhaltet:
  - Langzeiterfassung
  - Analyse von Logdaten
  - Reporting von Logdaten
- Grundsätzlich ermöglichen SIEM-Systeme durch das Sammeln von Sensorinformationen und Ereignissen, Bedrohungen zu erkennen und zu verhindern

SIEM-Schwerpunkte

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



SIEM-Technologien

- Ein SIEM-System kann aus diversen Modulen bestehen:
  - Event Correlation
  - Network Behaviour Anomaly Detection (NBAD)
  - Identity Mapping
  - Key Performance Indication
  - Compliance Reporting
  - Application Programming Interface (API)
  - Role Based Access Control
- Diese Module machen die Intelligenz eines SIEM aus, wodurch eine *Risikoanalyse* in Korrelation mit allen bekannten Events erfolgen kann

SIEM-Anforderungen

- Die Anforderungen orientieren sich an dem Haupt-Informationsfluss, d.h. das Sammeln der Informationen über das Verarbeiten bis zur Reaktion oder Alarmmeldung
  - *Sammeln* von Daten der zentralen Dienste und Netzkomponenten
  - *Aggregation* dieser Daten zu aussagekräftigen Ereignissen anhand einer flexibel definierbaren Policy
  - *Darstellungen* der sicherheitsrelevanten Ereignisse in verschiedenen Detailstufen
  - *Auslösen* von Alarmmeldungen oder ggf. aktiver Eingriff (Alerting/Enforcement)

DECOIT®

Korrelation von Events

Gemeinsame Wissensbasis (1)

- Um angemessene Entscheidungen zu treffen, ist es wichtig, eine aktuelle und korrekte *Wissensbasis* über die Geräte, Benutzer und Eigenschaften des Netzwerkes zu besitzen:
  - *Daten über Geräte*, die sich im Netz befinden, wie IP-Adresse, MAC-Adresse, DNS-Name, Betriebssystem etc.
  - *Informationen über Benutzer*, die an Systemen angemeldet sind, wie Name, Benutzergruppen, Berechtigungen etc.
  - *Detail-Informationen* über den Zustand der zentralen Dienste im Netzwerk, beispielsweise Informationen über aktuell angemeldete Benutzer, Fehlermeldungen etc.

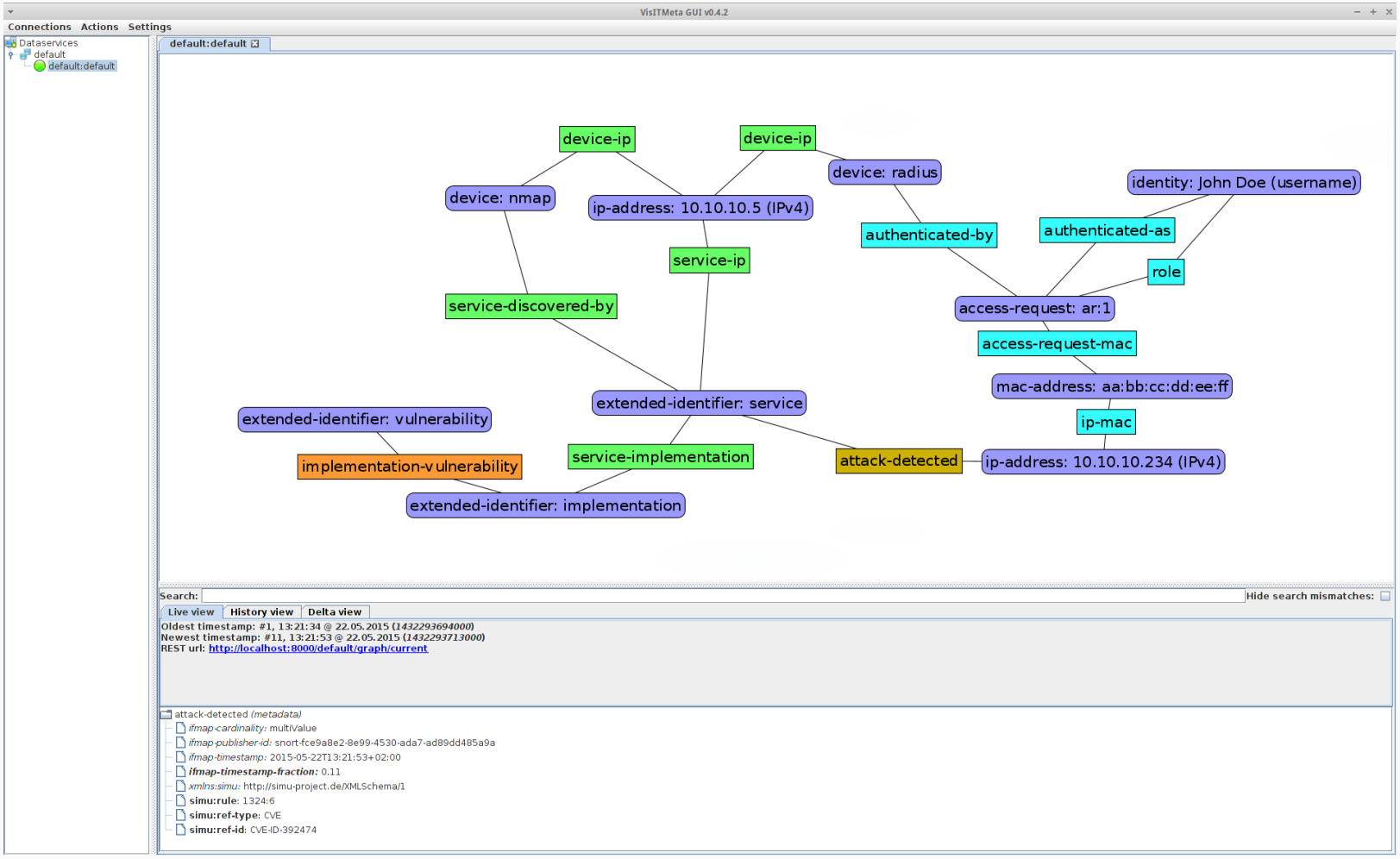
Gemeinsame Wissensbasis (2)

- Heutige Sicherheitskomponenten der Hersteller sind für Insellösungen entwickelt worden
- Offene Schnittstellen und einheitliche Datenformate fehlen oftmals
- SIEM-Lösungen sind komplexe Systeme und bestehen aus unterschiedlichen Modulen, Sicherheitskomponenten und Schnittstellen
- Die Abdeckung der Auswertemöglichkeiten hängt oftmals von dem Fokus des Herstellers ab
- Eine SIEM-Einführung beinhaltet häufig höhere Kosten (Lizenzen, Implementierung, Inbetriebnahme, Pflege)

Schaffung eines gemeinsamen Nenners durch IF-MAP

- *IF-MAP* ist ein offen spezifiziertes, herstellerunabhängiges Protokoll zum Austausch von Metadaten innerhalb eines Netzwerkes in Echtzeit
- Es wurde von der Trusted Computing Group (TCG) spezifiziert und liegt aktuell in der Version 2.2 vor
- IF-MAP definiert zwei Rollen:
  - Der *Meta-data Access Point Server (MAPS)* dient als zentraler Zugriffspunkt und Sammelstelle für beliebige Metadaten
  - *IF-MAP Clients (MAPC)* können über das IF-MAP-Protokoll auf den MAP-Server zugreifen, um Metadaten zu veröffentlichen, sie zu durchsuchen oder Abonnements auf Metadaten registrieren

Metadaten-Graph-Visualisierung



DECOIT®

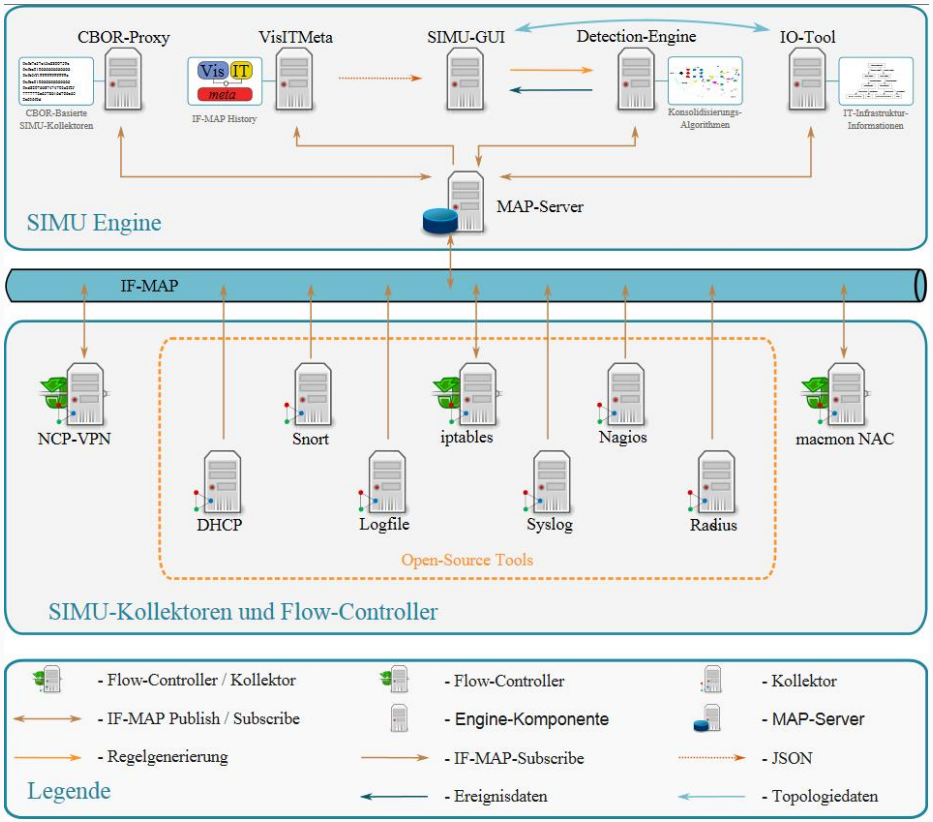
Forschungsansätze

Das F&E-Projekt SIMU

- Das SIMU-Projekt (www.simu-project.de) vom BMBF startete im Oktober 2013 und endete erfolgreich im September 2015
- Partner des nationalen Projektes waren:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Fraunhofer SIT (Konzeption)
  - Hochschule Hannover (Entwicklung)
  - Dritthersteller NCP und macmon secure
- Es sollte eine leichte Integrierbarkeit in KMU-Infrastrukturen ermöglicht werden
- Die Nachvollziehbarkeit von relevanten Ereignissen und Vorgängen im Netz sollte dabei gegeben sein
- Geringer Aufwand für Konfiguration, Betrieb und Wartung war das Ziel
- Als Protokoll zur Log-Konsolidierung sollte IF-MAP der TCG zum Einsatz kommen

Architektur im SIMU-Projekt

- SIMU-Kollektoren- und Flow-Controller:
  - Datensammlung
  - Enforcement
- SIMU-Engine:
  - Zentraler Wissens- und Datenspeicher
  - Komponenten zur Korrelation, Aggregation und Darstellung von Daten
  - Protokoll-Schnittstellen



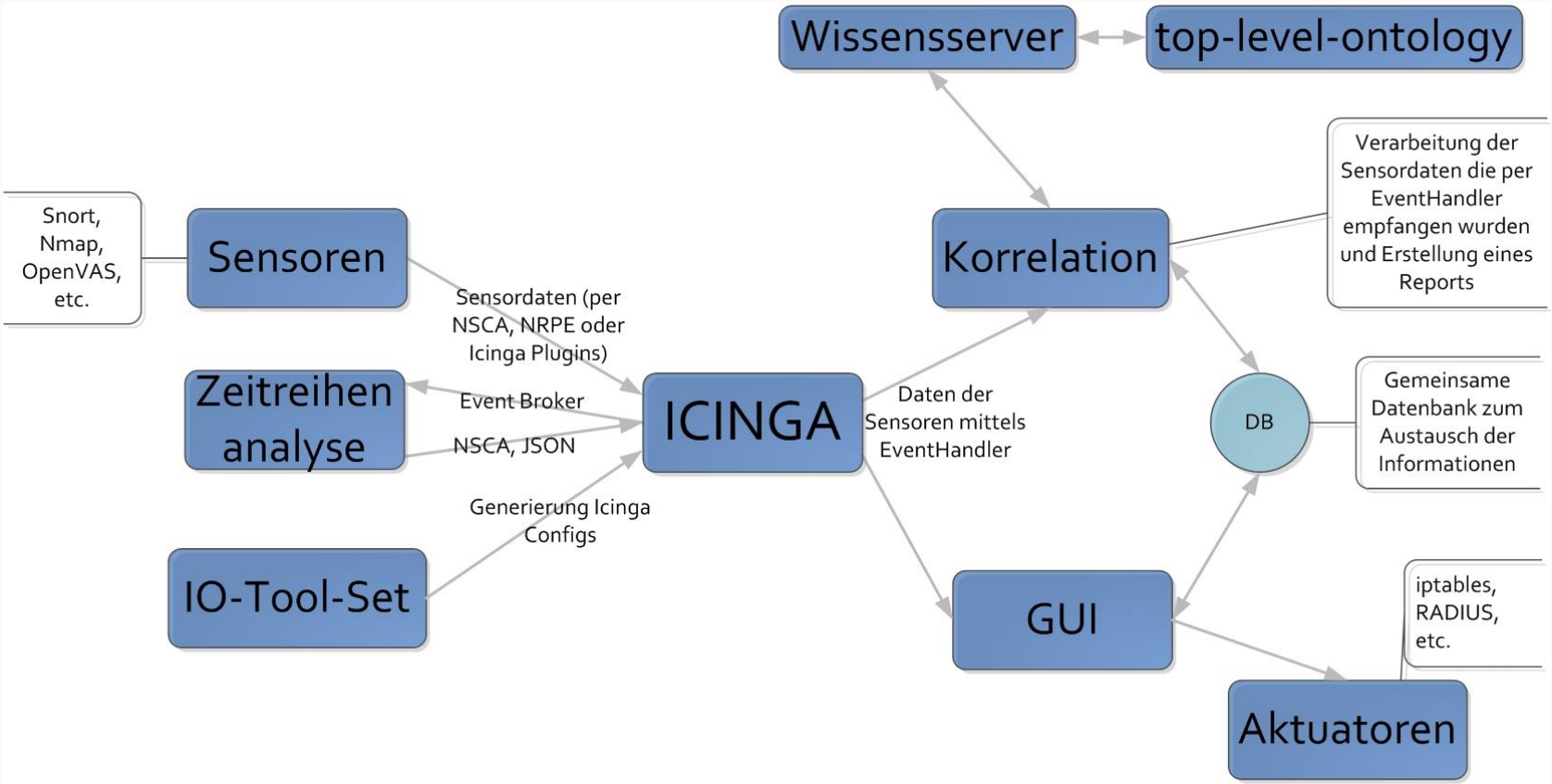
SIMU-Funktionalität

- Datenintegration auf Basis von IF-MAP
  - Standard der TCG
  - Graphbasiertes Modell
- Oberfläche (SIMU-GUI)
  - Visualisierung der Daten und Ereignisse
  - Nachverfolgung der Ereignisse
- Detection Engine
  - Regelbasierte Erkennung von Vorfällen
  - Definiert Muster im IF-MAP-Graphen, die sicherheitsrelevante Vorfälle beschreiben
  - Aktionen: Vorfall melden, ggf. Enforcement (z.B. Benutzer ausschließen)
  - Visualisierung der erkannten Vorfälle und Bearbeitung mit der SIMU-GUI

Das F&E-Projekt imonitor

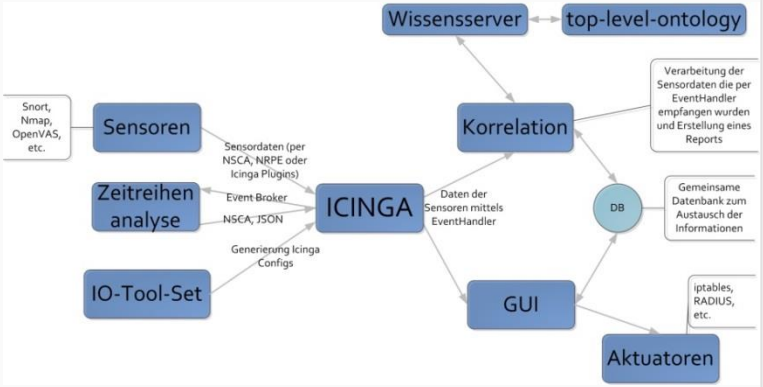
- Das iMonitor-Projekt (www.imonitor-project.de) vom BMWi startete im Juli 2013 und endete erfolgreich im Juni 2015
- Partner des „Bremer Projektes“ waren:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Universität Bremen, TZI (Entwicklung)
  - neusta GmbH (Entwicklung, Verwertung)
- Es wurde eine neue Form der Ereigniskorrelation umgesetzt, die automatisiert neue Angriffsvarianten erkennt (KI-Komponente)
- Korrelationsregeln müssen nicht mehr nur manuell gepflegt werden
- Events werden übersichtlich in einer SIEM-GUI angezeigt

iMonitor-Architektur (1)

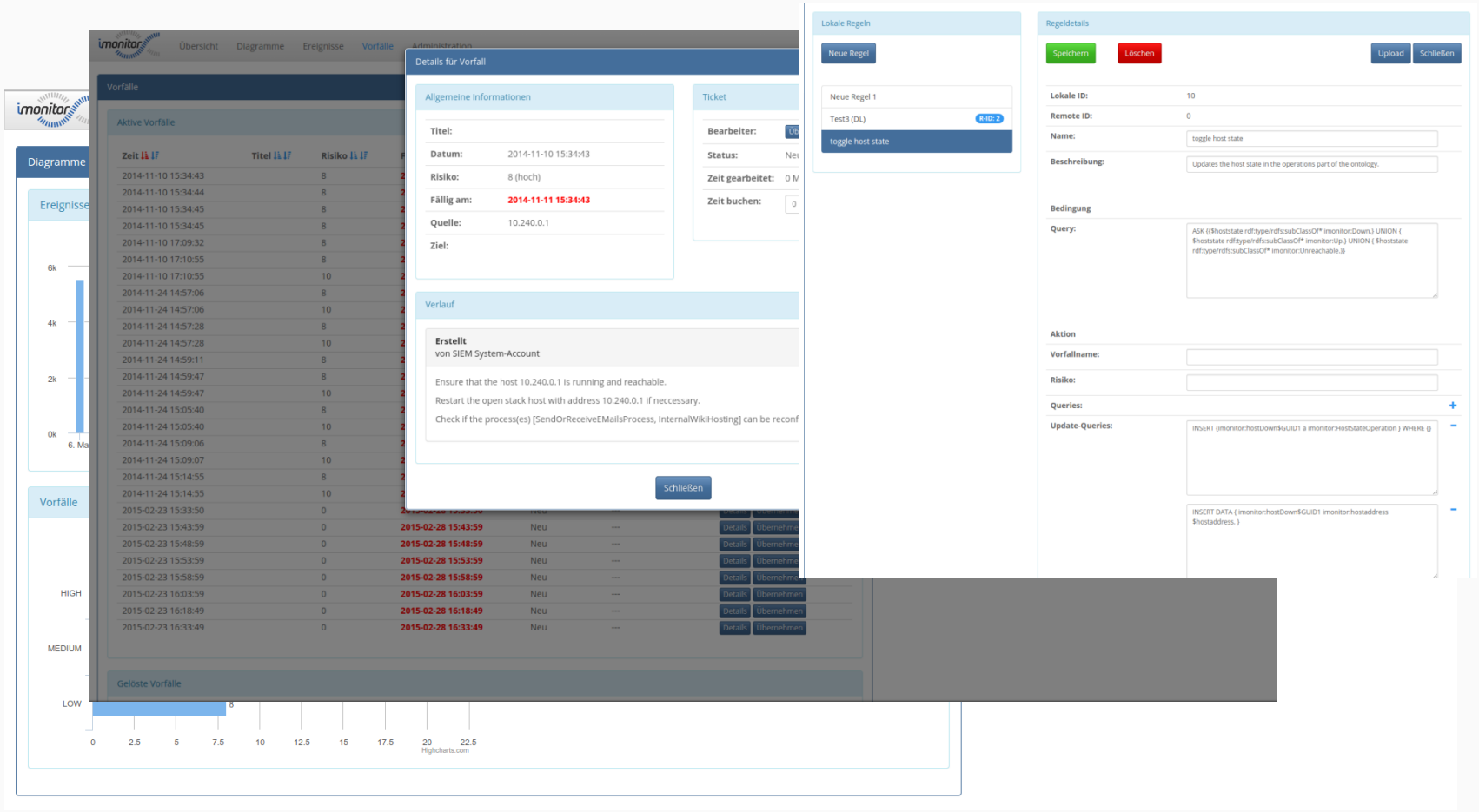


iMonitor-Architektur (2)

- **Sensoren:** Analysetools wie Snort, Nmap und OpenVAS sammeln Daten der Unternehmensumgebung, um das Normalverhalten zu erkennen
- **Zeitreihenanalyse:** Analysiert das Normalverhalten und versucht Anomalien ausfindig zu machen, ohne sich allein auf Mustererkennung zu stützen
- **IO-Toolset:** Erhebt die IT-Infrastruktur und ermöglicht logische Schlüsse auf der bestehende Datenstruktur und der Icinga-Konfiguration
- **GUI:** Grafische Oberfläche des SIEM-Moduls, um Vorgänge, Ereignisse und Tickets sowie eine Risikoabschätzung zentral sowie übersichtlich darzustellen
- **Korrelation:** Verarbeitung der Sensorereignisdaten und Erstellung eines Berichts sowie Vorschlag von Handlungsempfehlungen
- **Aktuatoren:** Komponenten wie iptables oder RADIUS, die in Echtzeit die Veränderung des Regelwerks vornehmen, stellen in einem Ticketsystem Handlungsempfehlungen dar



SIEM-GUI



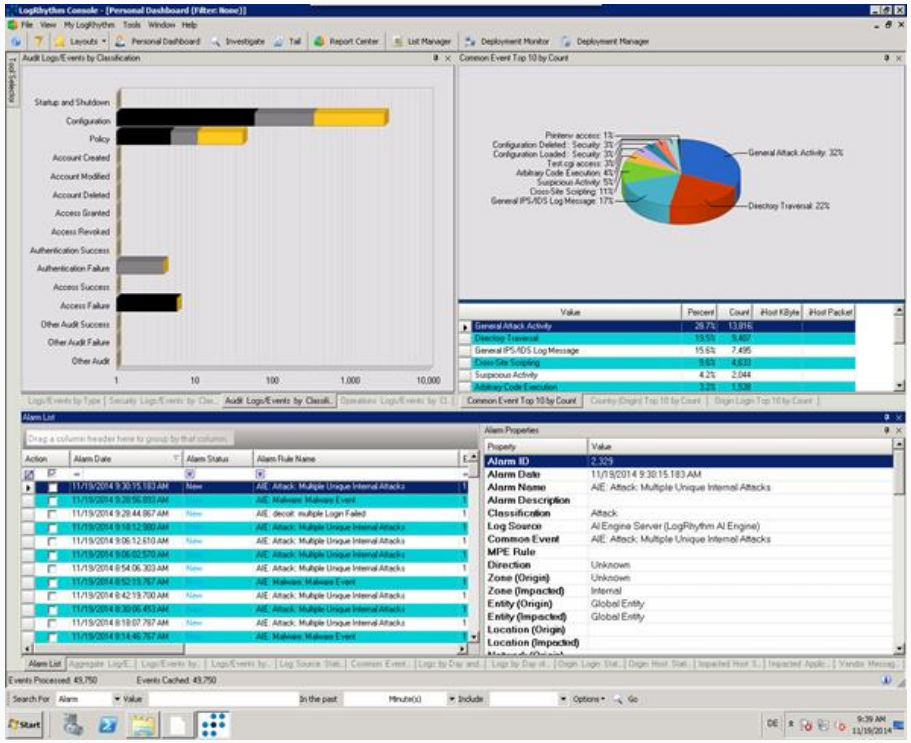
DECOIT®

Herstellerlösungen

Hersteller-Evaluierung

- Es wurden verschiedene SIEM-Hersteller durch die DECOIT GmbH evaluiert:
  - OSSIM von AlienVault
  - LogRhythm
  - LogApp von iQSol
  - ArcSight von Hewlett Packard
  - RadarServices
- Nicht alle Hersteller haben das gehalten, was sie in ihren Datenblättern versprochen haben
- Zudem bestand teilweise die SIEM-Lösung aus unterschiedlichen Inselsystemen (z.B. ArcSight, LogApp)
- In der Anomalie-Erkennung waren die Hersteller allerdings den Forschungsprojekten teilweise überlegen

- Wahrscheinlichkeit für ein „False Positive“ kann angeben werden
- Ein zentral installierter Agent kann sich von mehreren Systemen die Logs holen
- Neue Regeln können einfach erstellt werden
- Leider kommt auch hier keine KI zum Einsatz, sondern nur ein Pattern Matching
- Das Dashboard kann individuell angepasst werden und ist sehr übersichtlich gehalten



RadarServices

- Durch Machine-Learning-Technologien lernt die Software bei RadarServices sowohl saisonale Änderungen, als auch „normale“ Abweichungen von sicherheitsrelevanten Auffälligkeiten ohne vordefinierte Regelwerke zu unterscheiden
- Auf diese Weise können auch bislang unbekannte Angriffsmuster und Schadsoftware erkannt werden
- Zusätzlich kombiniert der IT-Dienstleister diese automatisierte Erkennung von Sicherheitsproblemen mit der Analyse und Bewertung durch Experten
- Tritt eine Notfallsituation ein, leitet RadarServices augenblicklich in Zusammenarbeit mit dem Kunden Gegenmaßnahmen ein
- Das SIEM-System wird als Managed Service angeboten

Auswertung

- Vor allem bei der Korrelation von Ereignissen und bei der Fähigkeit einfache und für jeden verständliche Handlungsempfehlungen zu generieren besteht viel Verbesserungsbedarf
- Alle getesteten Programme benötigen Experten, damit sie richtig konfiguriert und verwendet werden können
- Handlungsempfehlungen werden nicht angegeben und Alarme können oftmals nur verstanden werden, wenn das notwendige Fachwissen vorhanden ist
- Die Konfiguration ist vor allem bei komplexeren und kompetenteren Systemen wie OSSIM sehr aufwändig und weit von einer „One-Click-Solution“ entfernt

DECOIT®

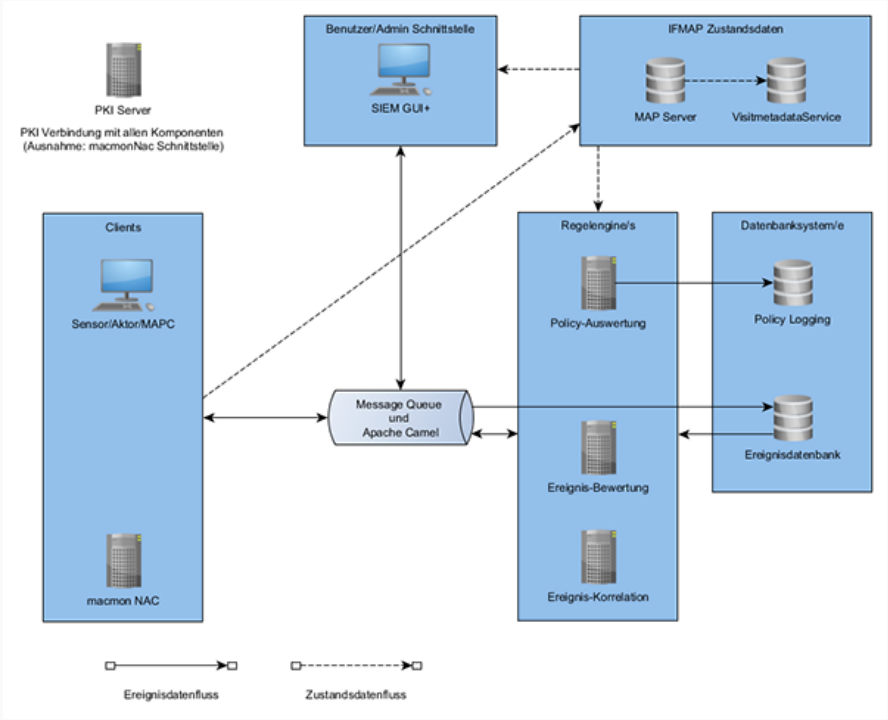
Zusammenfassung

Fazit

- SIEM-Systeme ermöglichen eine ganzheitliche Sicht auf die IT-Sicherheit eines Unternehmens
- Intelligente Anomalie-Erkennung ist bei den Anbietern bislang kaum vertreten (Schwerpunkt liegt auf Mustererkennung)
- Offene Schnittstellen sind notwendig, um auch andere Systeme mit einbinden zu können
- SIEM-Systeme müssen in Zukunft
  - intelligentere Selbstlernautomatismen bereitstellen,
  - einfacher zu handhaben sein,
  - kostengünstiger angeboten werden.
- Wenn diese Punkte nicht gelöst werden, droht eine ähnlich niedrige Verbreitung wie bei IDS-Lösungen

Ausblick

- Die Forschungsergebnisse von SIMU und iMonitor werden in einem neuen F&E-Projekt weiter vorangetrieben
- In dem BMWi-Projekt CLEARER (www.clearer-project.de) sollen die guten Ansätze in die Praxis überführt werden
- Ziel ist die Anbindung an ein bestehendes NAC-System, um dieses mit SIEM-Funktionen zu ergänzen
- Das Projekt geht gerade von der Konzeptions- in die Entwicklungsphase über



Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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