DECOIT

D.A.CH Security 2014

SIEM-Ansätze zur Erhöhung der IT-Sicherheit auf Basis von IF-MAP

Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

Inhalt

- SIEM-Definition und Ansätze
- SIEM-Technologien (u.a. Event Correlation, Identity Mapping)
- SIEM-Architektur auf Basis von IF-MAP
- Mehrwerte von SIEM-Systemen für Unternehmen
- Herausforderungen bei der Einführung

DECOIT

SIEM-Definition und Ansätze

Consultancy & Internet Technologies

SIEM-Ansatz

- Das Unternehmen und seine Werte sollten nach Schutzbedarfsfeststellung geschützt sowie die Kosten dieser Schutzmaßnahmen abgeschätzt und in Relation zum Ergebnis (Reduktion der Eintrittswahrscheinlichkeit eines Schadenfalles) gestellt werden
- Dadurch kann eine Optimierung des Risikomanagements ermöglicht werden, ohne die Verfügbarkeit des Netzwerks und seiner Dienste zu reduzieren
- Zielsetzung ist es, die Verfügbarkeit und IT-Sicherheit von Netzwerk und Diensten zu erhöhen und messbar zu machen!

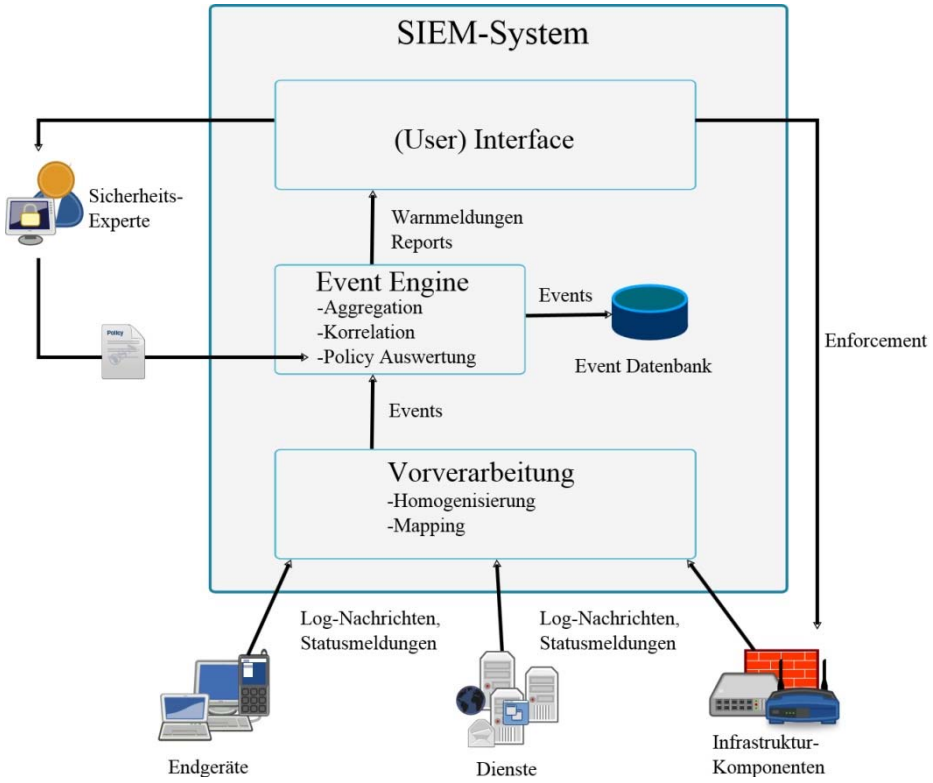
Definition eines SIEM-Systems

- 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
- Beide Bereiche können unterschiedlich kombiniert werden, um je nach Anforderungen und Leistungsfähigkeit ein SIEM-System zusammenzustellen

* Definition von Mark Nicolett und Amrit Williams von Gartner im Jahre 2005

Schwerpunkt eines SIEM-Systems

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

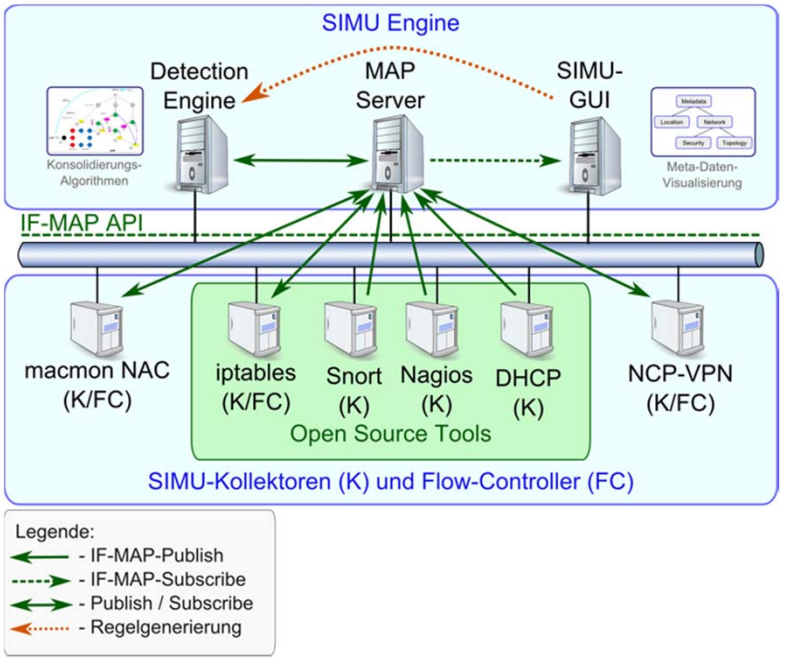


SIEM-Technologie

- Ein SIEM-System besteht aus diversen Modulen
  - 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

www.simu-project.de

- Das SIMU-Projekt vom BMBF startete im Oktober 2013 und wird im September 2015 enden
- Es soll eine leichte Integrierbarkeit in KMU-Infrastrukturen ermöglicht werden
- Die Nachvollziehbarkeit von relevanten Ereignissen und Vorgängen im Netz soll gegeben sein
- Geringer Aufwand für Konfiguration, Betrieb und Wartung
- Als Protokoll zur Log-Konsolidierung soll IF-MAP der TCG zum Einsatz kommen



DECOIT

SIEM-Konzept und -Architektur

Consultancy & Internet Technologies

DECOIT

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)

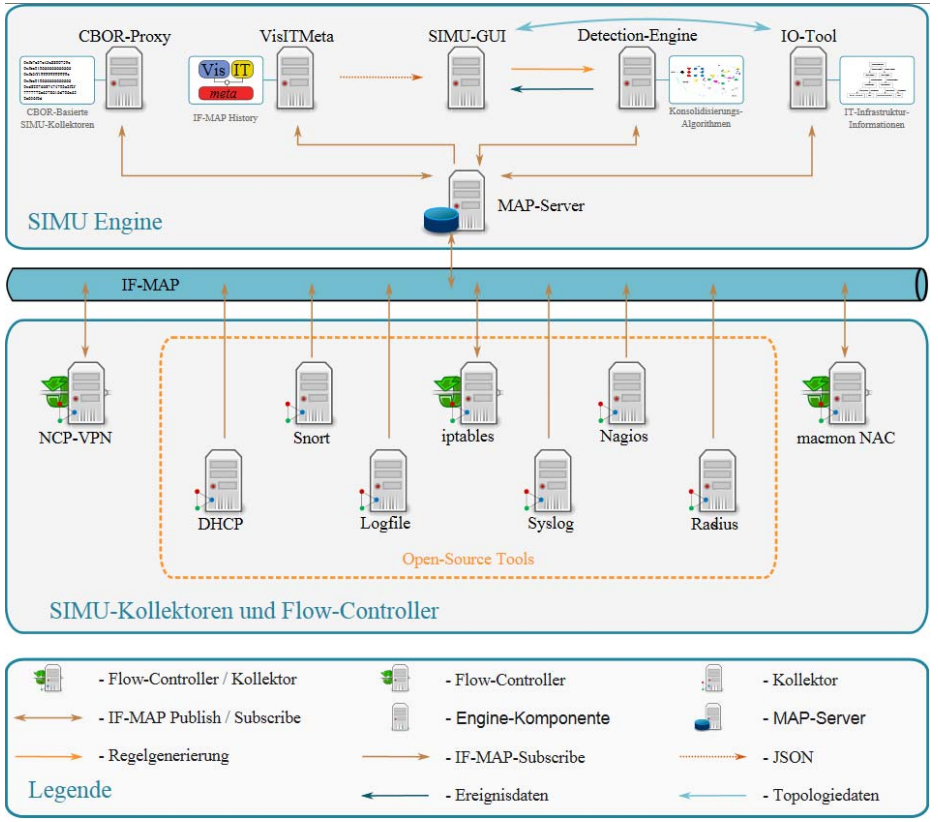
DECOIT

Gemeinsame Wissensbasis

- 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.

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
  - Protokollschnittstellen



IF-MAP-Definition

- Für den Austausch von Informationen zwischen der SIMU-Engine und den Kollektoren und Flow-Controllern wird das IF-MAP-Protokoll der Trusted Computing Group (TCG) eingesetzt
- IF-MAP ist ein offen spezifiziertes, herstellerunabhängiges Protokoll zum Austausch von Metadaten innerhalb eines Netzwerkes in Echtzeit
- IF-MAP definiert zwei Rollen:
  - Ein Server, der **Metadata Access Point (MAP)**, dient als zentrale Zugriffspunkt und Sammelstelle für beliebige Metadaten
  - **MAP-Clients (MAPCs)** können über das IF-MAP-Protokoll auf den MAP-Server zugreifen, um Metadaten zu veröffentlichen, sie zu durchsuchen oder Abonnements auf Metadaten registrieren

DECOIT

IF-MAP-Kommunikation

- Die Kommunikation zwischen einem MAPC und dem MAPS basiert auf einem Publish-Search-Subscribe-Modell, bei dem sowohl synchron als auch asynchron MAP-Daten ausgetauscht werden können:
  - Durch die **Publish-Operation** kann ein MAPC neue Metadaten veröffentlichen, vorhandene Metadaten ändern oder löschen
  - Ein MAPC kann per **Search-Operation** nach vorhandenen Metadaten suchen
  - Über die **Subscribe-Operation** kann sich ein MAPC über Änderungen der im MAPS gespeicherten Metadaten informieren lassen. Dabei wird seitens des MAPC spezifiziert, welche Art von Metadatenänderungen relevant ist. Nur solche Änderungen haben eine Benachrichtigung durch den MAPS zur Folge.

DECOIT

SIMU-Kollektoren u. Flow-Controller (1)

- Android-Kollektor: Einbeziehung von mobilen Smartphones zur Überprüfung von Firmware, Kernel etc.
- DHCP-Kollektor: Extrahiert Metadaten zu aktuellen IP-Leases des DHCP-Servers aus dem Lease-File von DHCP-Servern
- Radius-Kollektor: Liefert Metadaten zu Benutzeranmeldungen sowie Metadaten zu den Benutzern selbst (Gruppen, Berechtigungen)
- Syslog-Kollektor: Stellt voraggregierte Metadaten zum Zustand von Hosts und Diensten (CPU-Last, fehlgeschlagene Log-Ins) zur Verfügung
- Nagios-Kollektor: Veröffentlicht aus Nagios extrahierte Metadaten zum Zustand von Hosts und Diensten (u.a. Netzwerkverfügbarkeit)
- Snort-Kollektor: Übersetzt Snort-Alarme in IF-MAP-Metadaten
- Logfile-Kollektor: Generischer Kollektor zur Auswertung beliebiger Log-Dateien und Transformation in IF-MAP-Metadaten

SIMU-Kollektoren u. Flow-Controller (2)

- Die Integration weiterer Flow-Controller-Komponenten ist in Arbeit:
  - **Iptables-Flow-Controller:** Ermöglicht das automatische Anlegen von Firewall-Regeln für Hosts als Reaktion auf bestimmte Metadaten und veröffentlicht diese als Enforcement-Reports im MAP-Server
  - **macmon NAC:** Das NAC-System von macmon secure publiziert verschiedene Daten zu aktiven Endgeräten im Netzwerk. Hierzu gehören vor allem Autorisierungsinformationen zu bekannten Endgeräten, deren Standort im Netzwerk (physikalischer Port, WLAN-AP) und weitere Geräte-Charakteristika wie Betriebssystem-informationen und offene Ports
  - **NCP-VPN:** Die von NCP entwickelte VPN-Lösung kann eine Reihe relevanter Metadaten auf dem MAP-Server zur Verfügung stellen. Dies sind insbesondere Informationen über angemeldeter Benutzer sowie die IP-Adresse der Geräte, mit denen die Benutzer im VPN angemeldet sind, Datendurchsatz und Verbindungszeit der jeweiligen Benutzer. Es wird ein Enforcement auf VPN-Ebene ermöglich

SIMU-Engine

- MAP-Server: zentraler Austauschpunkt von Informationen. Alle Sensoren und Flow-Controller veröffentlichen gesammelte Informationen via IF-MAP im MAP-Server
- Detection Engine: sucht nach Abweichungen von definierten Zuständen durch Pattern Matching und Anomalie-Erkennung
- IO-Tool: der Datenbestand wird mit weiteren Asset-Informationen über die Netzwerkinfrastruktur angereichert, was eine Korrelation mit zusätzlichen Informationen ermöglicht
- VisITMeta: Langzeitarchivierung des IF-MAP-Graphen zur Visualisierung der Ergebnisse
- CBOR-Proxy: als Alternative zur SOAP-/XML-Kommunikation nach RFC-7049 zum schlankeren Datenaustausch

DECOIT

Fazit

DECOIT

Herausforderungen

- 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
- Zur IF-MAP-Nutzung müssen alle Sicherheitskomponenten eine IF-MAP-Schnittstelle anbieten

DECOIT

Mehrwerte

- Das im SIMU-Projekt entwickelte SIEM-System soll eine leichte Integrierbarkeit in eine bestehende Infrastrukturen und den wartungsarme Betrieb des Systems ermöglichen
- Durch den Einsatz von IF-MAP als Integrationsplattform ist es möglich herstellerübergreifend eine Vielzahl von Komponenten an das SIMU-System anzubinden
- Die zentrale Verfügbarkeit von Infrastrukturdaten und dynamischen Ereignisdaten ermöglicht eine bessere und umfassendere Gesamtsicht auf den Zustand des Netzwerks
- Gleichzeitig wird durch die Abbildung auf IF-MAP Metadaten eine erste Homogenisierungs-Stufe für Informationen aus unterschiedlichen Datenquellen und Formaten erreicht

DECOIT

Vielen Dank für ihre Aufmerksamkeit

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

Consultancy & Internet Technologies