DECOIT

33. BremSec-Forum

Security Information Event Management (SIEM) - Aktuelle Entwicklungen

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

Kurzvorstellung der DECOIT GmbH

- Gründung am 01.01.2001
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Fokus: Herstellerneutrale, ganzheitliche Beratung von IT-Lösungen
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
  - *Consulting:* ganzheitliche sowie herstellerneutrale Beratung
  - *Systemmanagement:* Umsetzung und Support von Hersteller- oder Open-Source-Lösungen
  - *Software-Entwicklung:* Entwickeln von Individuallösungen mit hohem Innovationscharakter
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen

DECOIT

Bestandsaufnahme IT-Sicherheit

Consultancy & Internet Technologies

Die Entwicklung der IT-Sicherheit (1)

- Am Anfang stand die Verfügbarkeit und Vernetzung von IT-Services im Vordergrund
- Zur Absicherung wurden Access Control Lists (ACL) auf den Routern und Switches eingerichtet
- Statische Filter ließen sich allerdings nicht pflegen, weshalb diese später verbindungsabhängig (Stichwort: Stateful Inspection) in Firewalls umgesetzt wurden
- Application Ports wurden gesperrt, ohne den Datenverkehr zu analysieren
- Zur Anomalie-Erkennung wurden Intrusion Detection Systems (IDS) versucht einzuführen, ohne den administrativen Aufwand zu berücksichtigen
- Intrusion Prevention Systems (IPS) sollten hingegen Anomalien in der Entstehung verhindern und die Log-Flut eindämmen

Die Entwicklung der IT-Sicherheit (2)

- IPS-Lösungen erhöhten allerdings den Aufwand pro Port und Paket, was bei 10-Gbit/s-Netzen zu Performance-Engpässen führen konnte
- Zudem schafften Protokolle (z.B. SOAP), die über diverse Ports, Schichten und Verschlüsselung kommunizieren zusätzliche Herausforderungen
- Heute sind viele unterschiedliche Insellösungen im Einsatz (AV-, IDS-, IPS-, FW-, VPN-, NAC-Systeme etc.), die keine einheitliche Aussage über Anomalien im Netzwerk zulassen
- Zudem sind die verschiedenen Herstellerlösungen meistens nicht kompatibel zueinander!
- Durch Monitoring-Systeme kann heute allerdings immerhin pro-aktiv der Netz- und Serverstatus erfasst werden

DECOIT

Pro-aktives Netzmonitoring

- Ein pro-aktives Netzmonitoring meldet Systemausfälle, bevor ein Anwender dieses bemerkt
- Der IT-Administrator hat bessere Pflegemöglichkeiten, da er den Zustand des Gesamtnetzes (Server, Clients, IP-Telefone, Netzwerk) kennt und darauf Einfluss nehmen kann
- Zusätzlich wird eine aktuelle Dokumentation ermöglicht, die interaktiv auf dem neusten Stand gehalten wird
- Langzeitstatistiken helfen auch, nachträglich Fehler zu analysieren
- Auch an Feiertagen und Wochenende können alle aktiven Systeme überwacht werden
- Fast beliebige Systeme lassen sich in ein Monitoring einbetten – allerdings ohne Einbeziehung der IT-Sicherheit!

DECOIT

Einführung in SIEM

Zielsetzung eines SIEM-Systems

- 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!

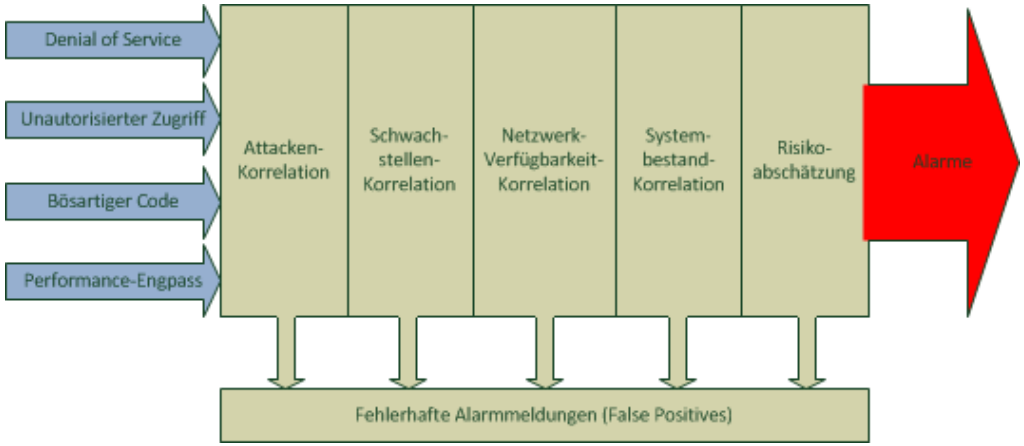
Definition eines SIEM-Systems

- 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

Event Correlation

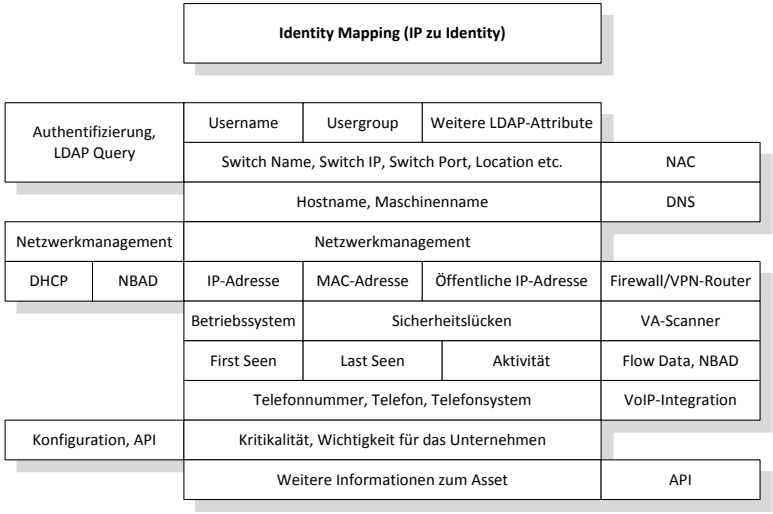
- Die Event-Korrelation ist die wichtigste Basisfunktionalität, da die vorhandenen Logfiles aufgenommen, archiviert, normalisiert und korreliert werden müssen, um eine Gefährdung überhaupt erkennen zu können
- Dabei werden die Daten über verschiedene Kanäle aufgenommen, wie z.B. Agenten, syslog, SNMP, Webservices oder OPSEC
- Alle Events laufen an zentraler Stelle auf, um dort unterschieden zu werden, ob es sich bei dem Event um eine Gruppe einer bestimmten Problemstellung oder um eine bereits identifizierte Gefahrenstellung handelt
- Events und False Positives werden reduziert. Daraus kann das SIEM-System wiederum eine Aktion (automatisiert oder nach Bestätigung) generieren, um das Problem selbst zu lösen
- Das SIEM-System bezieht zur Problemerkennung Netzwerkdaten und Events mit ein und kombiniert diese Daten zu einer Problemstellung (Handlungsempfehlung)

Network Behaviour Anomaly Detection (NBAD)

- Durch NBAD ist ein SIEM in der Lage Anomalien auf Netzwerkebene zu erkennen, Kommunikationsverhalten festzustellen und Abweichungen von der Normalität zu verfolgen bzw. bei Bedarf diese in die Korrelation der Problemstellung mit aufzunehmen
- SIEM-Systeme der neuen Generation sind zudem in der Lage ein Content Inspection durchzuführen und dadurch nicht nur die Netzwerkschickten 1-4 zu untersuchen, sondern auch Schicht-7-bezogene Analysen vornehmen zu können
- Dadurch lässt sich feststellen, wenn Systeme oder Benutzer freigeschaltete Protokolle (z.B. http, DNS) nutzen, um Sicherheitskomponenten zu umgehen
- Ein solches SIEM-System soll die Lücke von einem IPS/IDS-System zur Expertenanalyse schließen und neben bekannten Angriffen auch unbekannte Angriffsmuster erkennen
- Die meisten SIEM-Hersteller, die NBAD unterstützen, arbeiten derzeit mit fünf Erkennungsmethoden: Behaviour, Anomaly, Threshold, Policy und Custom

Identity Mapping

- Sicherheitssysteme, die Anomalien oder Angriffe auf das Unternehmensnetz melden, beschreiben den Angreifer und das Opfer stets mittels einer IP-Adresse
- Das ist in DHCP- und NAT-basierten Netzumgebungen problematisch
- Die Identität des Opfers oder des Angreifers muss aber zweifelsfrei geklärt werden
- SIEM-Systeme können diese Informationen aus verschiedenen, teilweise redundanten Quellen sammeln und stellen diese in Echtzeit zur Verfügung
- Dabei erlauben die dahinterliegenden Datenbanken auch das Suchen nach Asset-Informationen (Identity-Informationen) bezogen auf verschiedene Zeiträume



Key Performance Indication

- Dadurch, dass ein SIEM-System Netzwerkdaten, Logfiles, sicherheitsrelevante Informationen und Asset-Details zentral vereint, kann es in der Lage sein, die IT-Sicherheit messbar zu machen
- Diese Messbarkeit wird durch sog. Key-Performance-Indikatoren umgesetzt, die messen, wann organisatorisch definierte Maßnahmen greifen und wann dies nicht der Fall ist
- Zusätzlich können sie den Einfluss, den das Nichtgreifen einer Maßnahme auf die Verfügbarkeit, Sicherheit und die Integrität wichtiger Unternehmenswerte hat, darstellen
- Beispiel: ein Virus wurde erkannt. Das SIEM-System ist in der Lage den Erfolg der Gegenmaßnahmen zu erkennen und die Komponenten herausheben, die den Virus erkannt und gestoppt haben

Compliance Reporting

- Das Reporting eines SIEM-Systems muss nach bestimmten Compliance-Regeln durchgeführt werden, um auch definierte Aussagen zur IT-Sicherheit treffen zu können
- Zudem muss die IT-Compliance immer wieder hinterfragt und durch das SIEM-System untersucht werden
- Die SIEM-Ergebnisse müssen daher immer wieder einer Auswertung unterzogen werden
- Dies betrifft beispielsweise die Anzahl der korrekten Alarme, False Positives oder der Bedrohungen insgesamt
- Diese kann man halb- und ganzjährig gegenüberstellen und so feststellen, ob das SIEM-System eine Verbesserung erwirkt hat oder man weiter an der Effizienz arbeiten sollte
- Für ein Unternehmen lassen sich dabei verschiedene Compliance-Typen nennen: Integrität, passend zur Unternehmensstrategie, Risikomanagement und Effektivität

Application Programming Interface (API)

- Ein SIEM-System muss der Bandbreite großer Diversitäten durch zwei Ansätze gerecht werden:
  - Schneller Support von weiterführenden, noch nicht integrierten Produkten, basierend auf verschiedenen Kundenanforderungen
  - Bereitstellen von generischen Schnittstellen zur Integration nicht bekannter Geräte bzw. Systeme
- Inventardatenbanken enthalten evtl. für die Asset- und Identity-Mapping-Darstellung wertvolle Informationen, wie z.B. Inventarnummer und Kostenstelle und müssen erweitert werden können
- Auch die Einbindung von Help-Desk- oder Ticket-Systemen muss möglich sein
- Die Daten müssen miteinander korreliert werden können

Role Based Access Control

- Das SIEM-Ziel ist es, eine zentrale Schnittstelle mit Sicht auf alle sicherheitsrelevanten Ereignisse innerhalb eines Unternehmens zu erstellen
- Dabei ist es natürlich notwendig, dass innerhalb des SIEM-Systems die bisherigen Organisationsstrukturen und Rechte des Unternehmens und seiner Mitarbeiter exakt abgebildet werden
- Das heißt, dass Problemstellungen, die nur in einen bestimmten Verantwortungsbereich fallen, auch nur von dem zuständigen Administrator eingesehen, modifiziert und bearbeitet werden dürfen
- Gleichzeitig muss es möglich sein, dass Rechte zwischen den Gruppen geteilt werden können
- Daher muss es möglich sein Modifikationen, Änderungen, Schreib- und Leserechte, Ticket- und Troubleshooting-Einstellungen entsprechend den Anforderungen definieren zu können

SIEM-Systeme müssen zusammenfassend...

- Die Prozesse auch mit einem hohen Grad an Automatisierung abzubilden
- Offene Schnittstellen besitzen, um die gesamte Infrastrukturinformationen zu integrieren
- Eine eigene Unternehmenswissensdatenbank besitzen, in der die Ergebnisse und Erkenntnisse von vorherigen Vorfällen gepflegt werden können
- Eine eingebaute Datenbank mit „Best Practices“-Werkzeugen zur Verfügung stellen
- Die Möglichkeit bieten, forensische und Trend-Analysen auf Basis der gesammelten Events zu ermöglichen
- Eingebaute Korrelation und Aggregation für bekannte Vorfälle von Betriebssystemen und Anwendungen anbieten und diese modifizieren zu können
- Eine automatisierte Reaktionsmöglichkeit auf Vorfälle anbieten (Intrusion Prevention System)
- Granulare Einstufungsmöglichkeiten für Vorfälle, basierend auf Servergruppen und Art des Ereignisses anbieten
- Automatische Eskalationsstufen bei Vorfällen anhand von SLAs anbieten

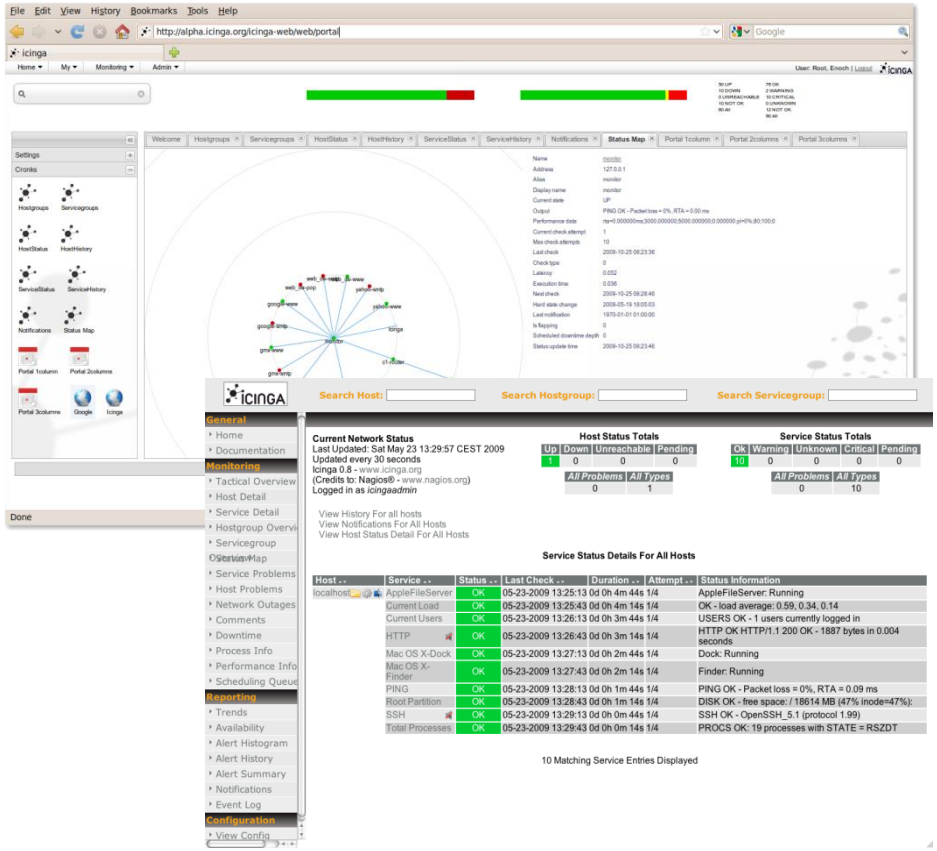
DECOIT

Monitoring- und SIEM-Beispiele

Consultancy & Internet Technologies

Icinga (Nagios)

- Icinga (Nagios) bietet hohe Flexibilität durch zahlreiche Plug-Ins, die Checks durchführen und die Möglichkeit bieten diese selbst zu programmieren
- Überprüfungs-, Benachrichtigungsintervalle und verzögerte Benachrichtigungen lassen sich frei definieren
- Benachrichtigungsgruppen können angelegt werden
- Berücksichtigung der Abhängigkeiten zwischen den einzelnen Hosts
- Icinga (Nagios) bietet ein Eskalationsmanagement



Eskalation und Benachrichtigungen

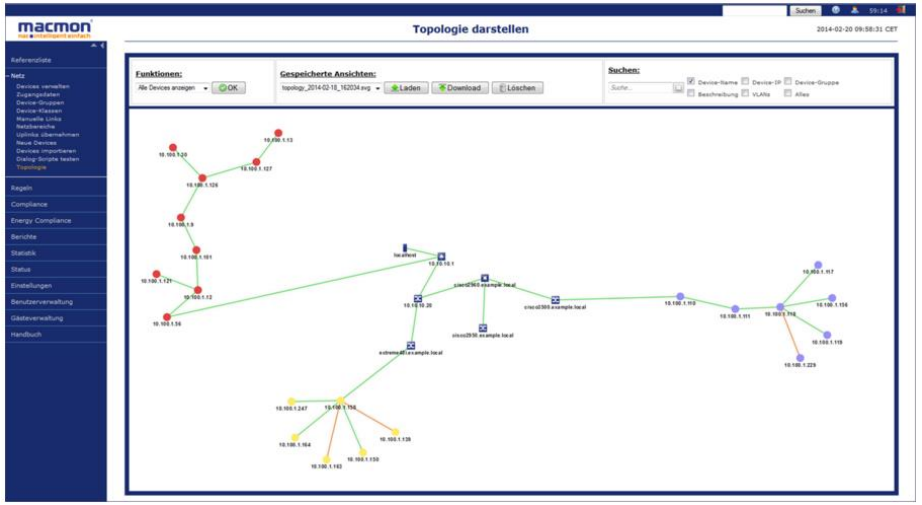
- Icinga besitzt ein ausgefeiltes Benachrichtigungssystem
- Es lässt sich einstellen wann, welche Personengruppen über welche Zustände und Ereignisse informiert werden
- Beim Ausfall oder bei der Über-/Unterschreitung von Grenzwerten, bietet Icinga verschiedene Formen von Benachrichtigungen an (E-Mail, SMS, VoIP-Anruf etc.)
- Nachrichten lassen sich zu beliebig festgelegten Zeiträumen versenden:
  - Kombinationen von Zeitraum-, Wochentag- und Uhrzeit-Angaben
  - Auch einzelne Kalendertage sind möglich
- Die DECOIT GmbH hat die vorhandenen Eskalationsstufen erweitert
  - Die Erweiterung ermöglicht es, Eskalationsstufen zusätzlich mit Bedingungen zu belegen
  - Nur wenn die Bedingungen zutreffen, wird eine Eskalationsstufe eskaliert
  - Somit ist es nun möglich, in Abhängigkeit des Zustands eines Dienstes, unterschiedliche Kontaktpersonen von Problemen zu unterrichten

NAC-Lösung als Basis

- Network Access Control (NAC) Lösung als zentrale Steuerinstanz
- Ziel:
  - Vollständige Sicht und Wissen, welche Personen und Geräte sich in dem eigenen Netzwerk befinden
  - Absicherung der Netzwerkzugänge
- Schnittstellen zu beliebigen Systemen und Kopplung mit anderen Sicherheitslösungen (z.B. Anti-Viren-Systeme, Notfallmanagement-Lösungen)
- Fokussiert das Netzwerk und seine Komponenten

Leistungsübersicht

- Sofortige Netzwerkübersicht
- Herstellerneutral durch SNMP-Anbindung
- Mehrstufige Zugriffskontrolle
- Mischbetrieb mit/ohne 802.1X
- Anbindung an führende Security-Produkte
- Intelligente Gäste-Verwaltung
- Steuerung des Netzwerkzugangs mobiler Geräte
- Analyse der IT Compliance



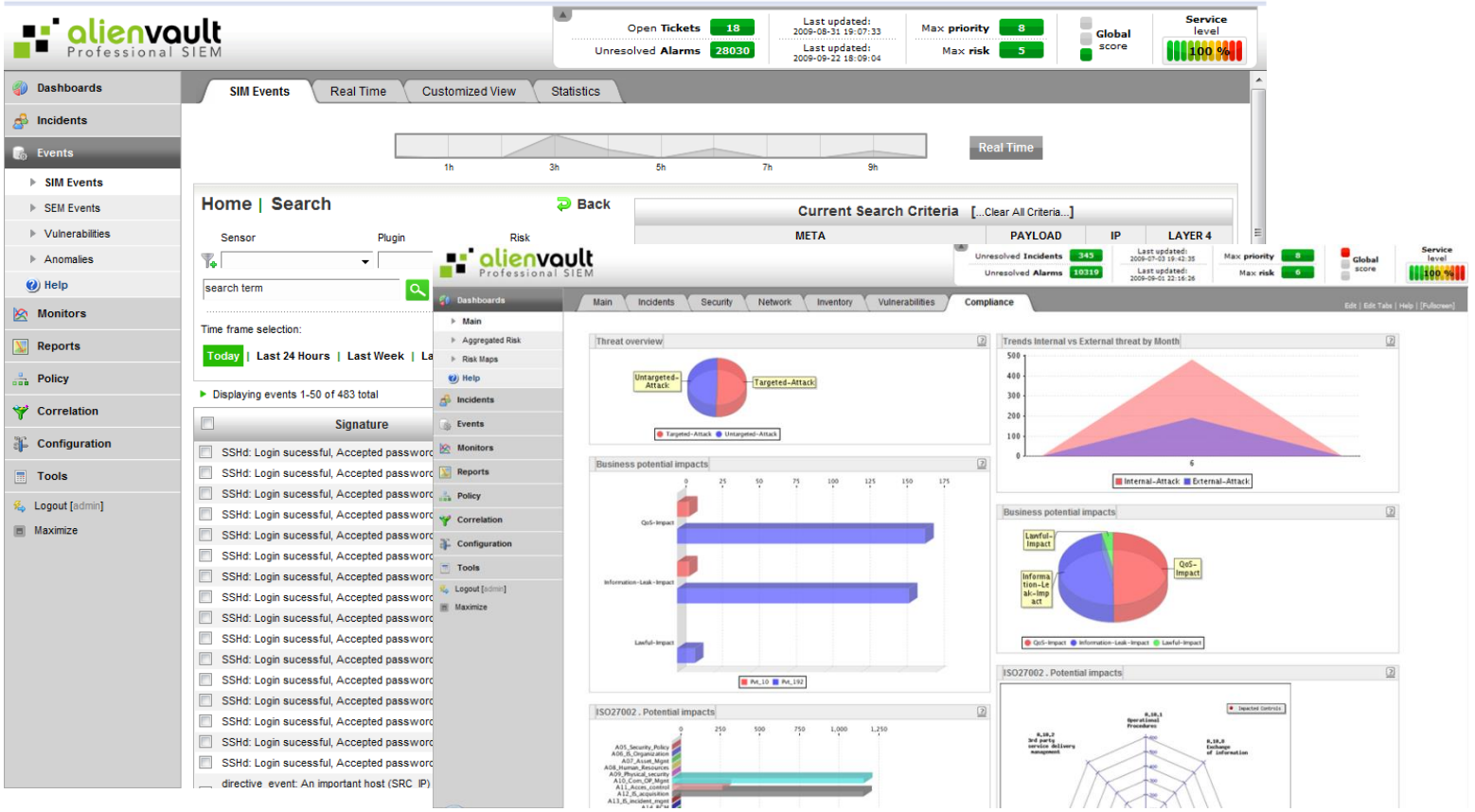
Open Source Security Information Management

- OSSIM ist mehr als ein reines Monitoring-System, sondern stellt ein echtes SIEM-System dar
- Der Hersteller Alien Vault hat dabei zwei Lösungen im Angebot:
  - eine kommerzielle Variante
  - eine Open-Source-Variante
- Über eine Web-Schnittstelle kann der Administrator alle notwendigen Konfigurationen (von der Netzwerkkonfiguration über die Benutzerverwaltung bis hin zu Backup/Restore) vornehmen
- Das GUI enthält ebenfalls eine komfortable Suche in den Logfiles, so dass der Zugriff per SSH nur in Notfällen erforderlich
- Sämtliche Komponenten darf der Administrator einzeln konfigurieren oder durch eigene Komponenten ersetzen (z.B. den Schwachstellenscanner Open VAS durch ein Nessus)
- Schwachstellen werden durch Tickets kommuniziert

DECOIT

Open Source Security Information Management

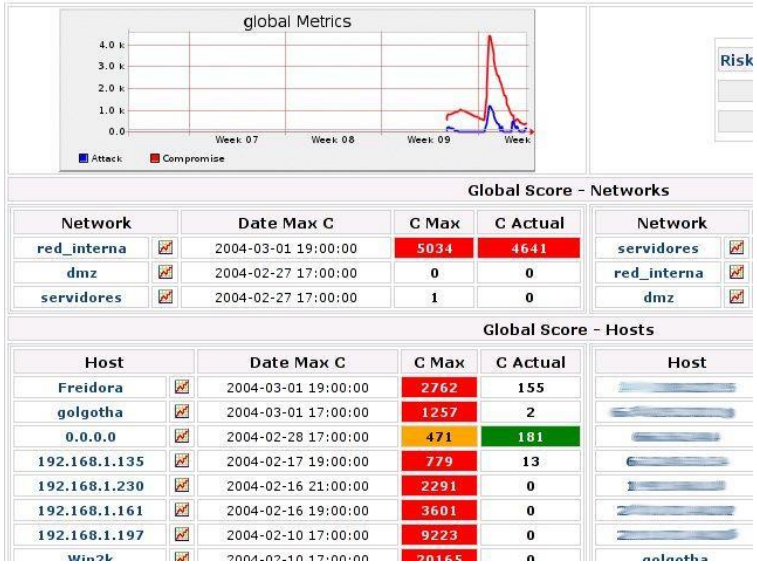
ALIEN VAULT OSSIM



Consultancy & Internet Technologies

Open Source Security Information Management

- Die wichtigste Funktionalität von OSSIM beinhaltet das Auswerten und Analysieren von Sicherheitsvorfällen (Security Incidents)
- Ähnliche Ereignisse werden dabei zu einer einzigen Meldung zusammengefasst
- Eine grafische Darstellung des Risikofaktors ermöglicht, dass die Meldungen nach Priorität geöffnet und bearbeitet werden können
- Die direkte Umwandlung in Tickets und Weiterleitung an den zuständigen Benutzer erleichtert dabei die Handhabung
- Als Quelle für die Meldungen fungieren
  - IDS-Sensoren (OSSEC)
  - Verwundbarkeitsscanner (Snort)



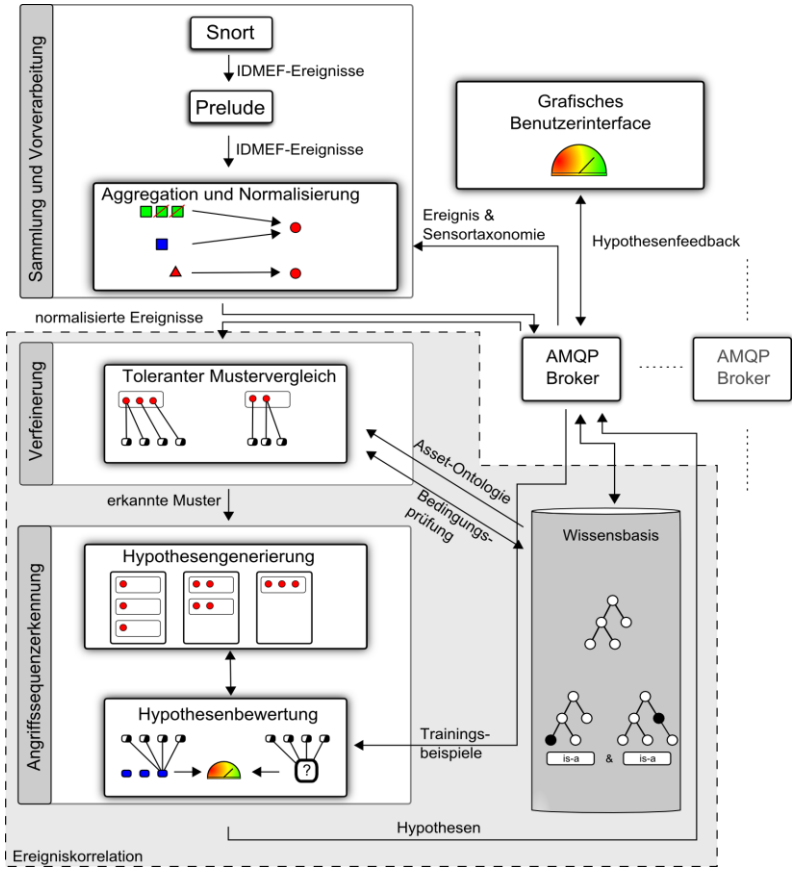
Forschungsprojekte

www.imonitor-project.de

- Das iMonitor-Projekt vom BMWi startete im Juli 2013 und wird im Juni 2015 enden
- Partner des „Bremer Projektes“ sind:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Universität Bremen, TZI (Entwicklung)
  - neusta GmbH (Entwicklung, Verwertung)
- Es soll eine neue Form der Ereigniskorrelation umgesetzt werden, die automatisiert neue Angriffsvarianten erkennt
- Korrelationsregeln sollen dabei nicht mehr nur manuell gepflegt werden müssen

www.imonitor-project.de

- Ziele von iMonitor
  - Integration von Sensorik
  - Entwicklung optimierter und skalierbarer KI-Verfahren
  - Datenschutzgerechten Austausch von Wissen über Sicherheitsvorfälle
  - Kombination mit anderen SIEM-Systemen
  - Verbesserung der Erläuterungen von Diagnosen von gemeldeten Vorfällen

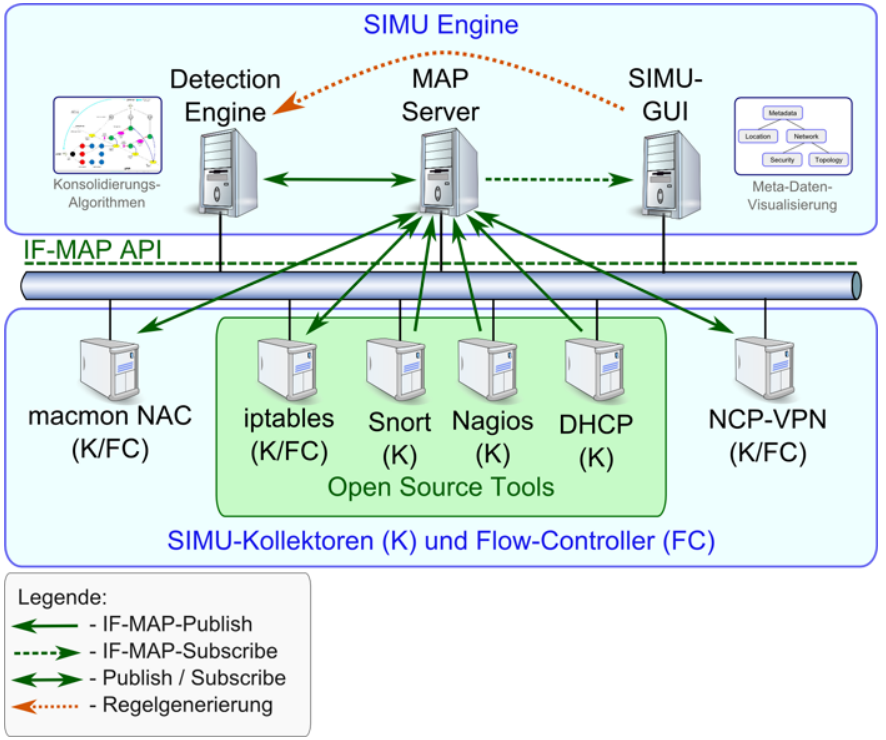


www.simu-project.de

- Das SIMU-Projekt vom BMBF startete im Oktober 2013 und wird im September 2015 enden
- Partner des Projektes sind:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Hochschule Hannover (Entwicklung, Veröffentlichung)
  - Fraunhofer SIT, Darmstadt (Entwicklung, Veröffentlichung)
  - macmon secure gmbh (Entwicklung, Verwertung)
  - NCP GmbH (Entwicklung, Verwertung)
- 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

www.simu-project.de

- SIMU-Kollektoren und –Flow-Controller
  - IF-MAP-Clients
  - IF-MAP-Graph zur Analyse und intuitiven Regelerstellung
- SIMU-Engine
  - MAP-Server
  - Detection Engine
  - SIMU-GUI



DECOIT

Fazit

DECOIT

Zusammenfassung

- Es gibt viele verschiedene Möglichkeiten, um pro-aktives Netzwerk- und Servermonitoring zu betreiben
- SIEM-Systeme gehen einen Schritt weiter, indem sie die IT-Sicherheit mit einbeziehen und eine Risikoabschätzung ermöglichen
- Nicht alle SIEM-Systeme halten allerdings das, was sie versprechen!
- Eine Übersicht wird von Mosaic Security Research angeboten: http://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management
- Man sollte sich von proprietären Systemen verabschieden und mehr auf offene Schnittstellen achten, um auch Drittsysteme einbinden zu können
- Auch kann nur so ein effektives Zusammenspiel zwischen verschiedenen Komponenten gewährleistet werden
- Open-Source-Lösungen besitzen daher einen entscheidenden Vorteil bei der Monitoring-/SIEM-Realisierung
- Die Kosten und Beherrschbarkeit solcher Systeme stellen nach wie vor die Haupthindernisse für die Einführung dar

Vielen Dank für ihre Aufmerksamkeit

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

Consultancy & Internet Technologies