DECOIT

Meet & Greet

open it berlin
Berliner Netzwerk für freie IT

Pro-aktives Netzwerkmonitoring der nächsten Generation

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

Monitoring-Anforderungen

Consultancy & Internet Technologies

DECOIT

Anforderung an Monitoring-Systeme

- Im Betrieb der meisten Netzwerke wird aus historischen Gründen ein reaktives Netzwerkmanagement umgesetzt
- Dies bedeutet, dass der Anwender einen Fehler im Betrieb bemerkt und den Administrator über den Fehler informiert
- Dieser hat dann die Aufgabe aus der Fehler- und Logmeldungen die Ursache zu ermitteln und danach umgehend den Fehler zu beheben. Analoges gilt für Überlastverhalten.
- Für den IT-Administrator ergeben sich damit mehrere Notwendigkeiten:
  - Er muss über den Zustand der betriebsrelevanten Dienste auf dem Laufenden sein
  - Er muss fundierte Aussagen über die Nutzung der Systeme machen können
  - Er muss die Trends in der Nutzung dokumentieren

DECOIT

Pro-aktives Netzmonitoring (1)

- Ein pro-aktives Netzmonitoring meldet im optimalen Fall Systemausfälle, bevor ein Anwender diese 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 nachträgliche Fehler analysieren zu können
- Auch an Feiertagen und Wochenende werden alle aktiven Systeme überwacht
- Fast beliebige Systeme lassen sich in ein Monitoring einbetten
- Es existieren aber auch viele proprietäre Hersteller-Lösungen

Pro-aktives Netzmonitoring (2)

- Allerdings ergeben sich durch die Anzahl der Events folgende Problematiken:
  - Es ist Expertenwissen notwendig, um die Vielzahl an Logs effizient auswerten zu können
  - Die zu erfassenden Systeme müssen zeitnah in das Monitoring integriert und kontinuierlich gepflegt werden
  - Es werden viele „False Positives“ und „False Negatives“ angezeigt, die die Auswertung erschweren
  - Die Konfiguration solcher Systeme (das Anlernen) kostet Zeit und erfordert Know-how

DECOIT

SIEM-Arbeitsweise

Consultancy & Internet Technologies

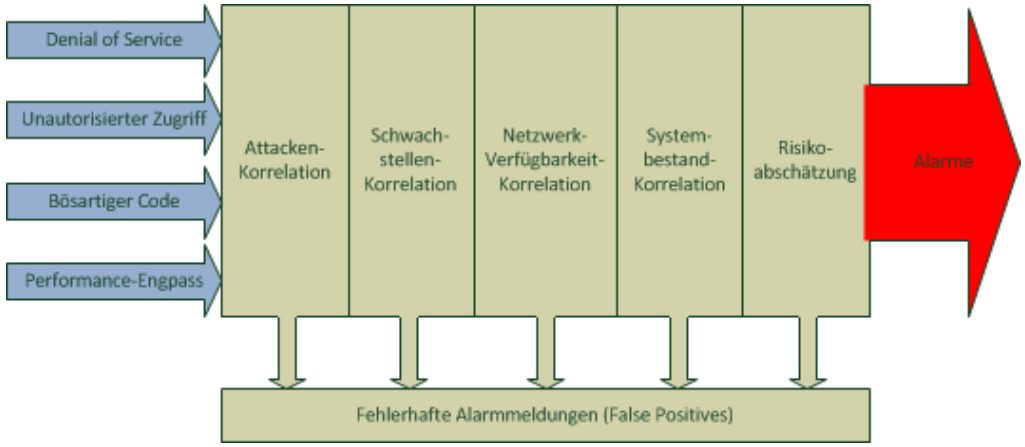
SIEM-Definition

- Als Monitoring-Lösung bietet sich der Einsatz eines SIEM-Systems an
- Ein SIEM-System besteht aus Security Event Management (SEM) und Security Information Management (SIM)*
- Das Security Event Management (SEM) beinhaltet:
  - Echtzeitüberwachung
  - Ergebniskorrelation
  - Event-Benachrichtigungen
- Das Security Information Management (SIM) 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



DECOIT

Sicherheitsrelevante Events

- Zusammenführung von sicherheitsrelevanten Events
  - **Extraktion:** Events sind in Rohform meist Einträge in Log-Dateien oder über das Netz versendete Systemmeldungen
  - **Homogenisierung/Mapping:** Events werden von unterschiedlichen Diensten erzeugt und aus unterschiedlichen Systemen extrahiert
  - **Aggregation:** Kollektoren aggregieren große Mengen gleichartiger Events über einen kurzen Zeitraum zu einem einzigen Event mit höherer Aussagekraft (z.B. Event-Typ, Inhalt und Menge der ursprünglichen Meldungen)
- Die Auswertung von Events wird anhand von Regelsätzen durchgeführt

SIEM-Technologien

- 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

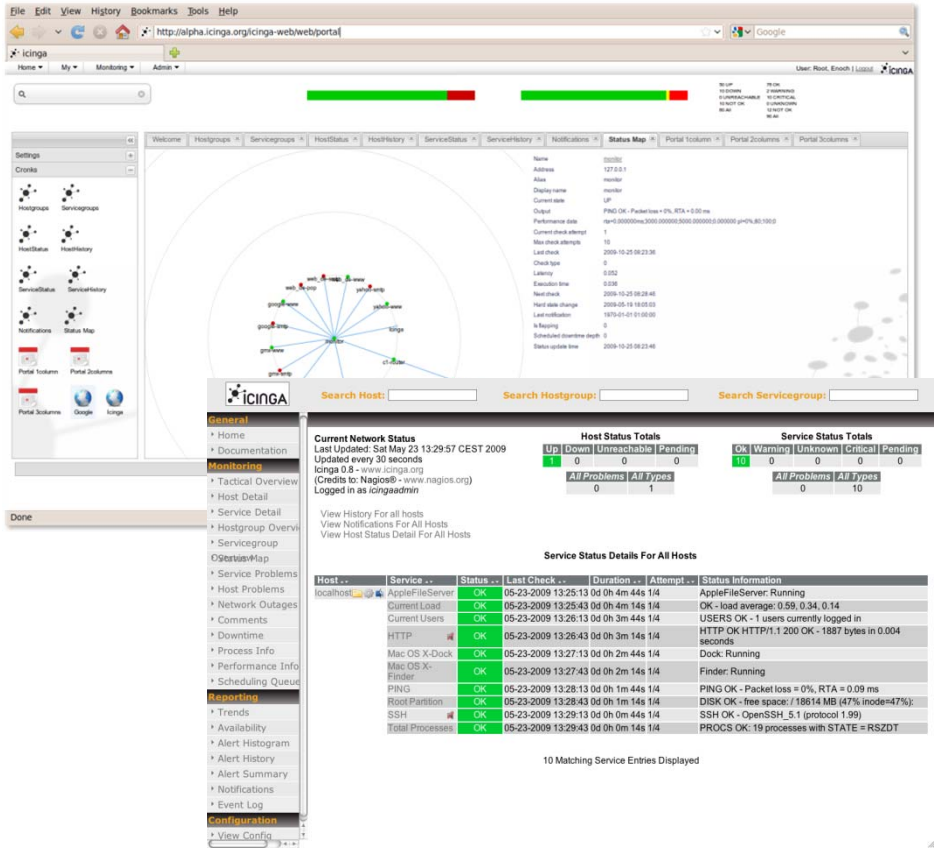
DECOIT

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



DECOIT

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

DECOIT

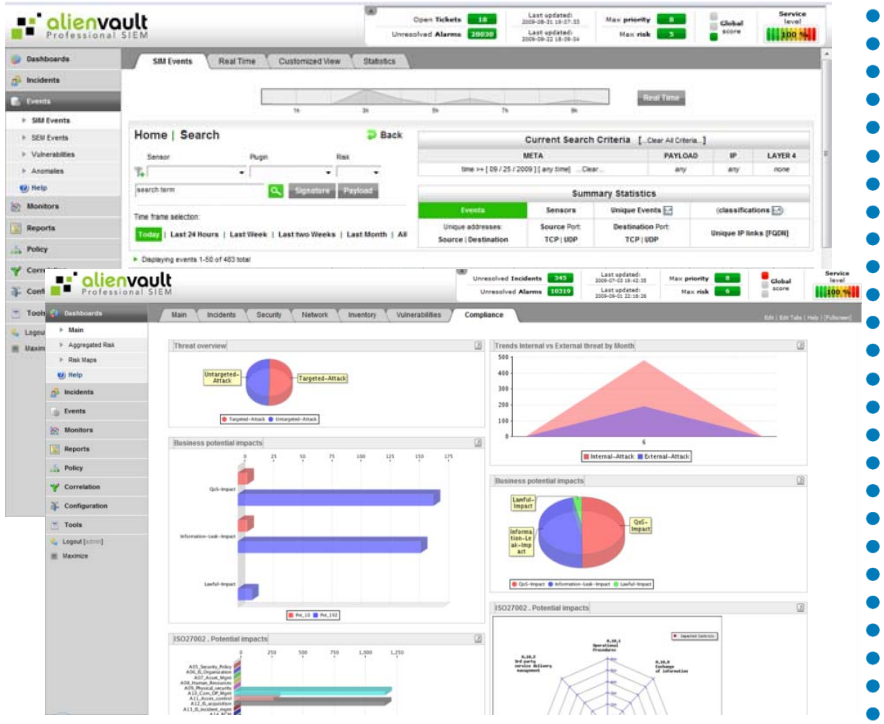
Open Source Security Information Management

- OSSIM ist mehr als ein reines Monitoring-System, sondern stellt bereits 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 ist
- Sämtliche Komponenten darf der Administrator einzeln konfigurieren oder durch eigene Komponenten ersetzen (z.B. den Schwachstellenscanner OpenVAS durch ein Nessus)
- Schwachstellen werden durch Tickets kommuniziert

Open Source Security Information Management

ALIEN VAULT OSSIM

- 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 es, 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)



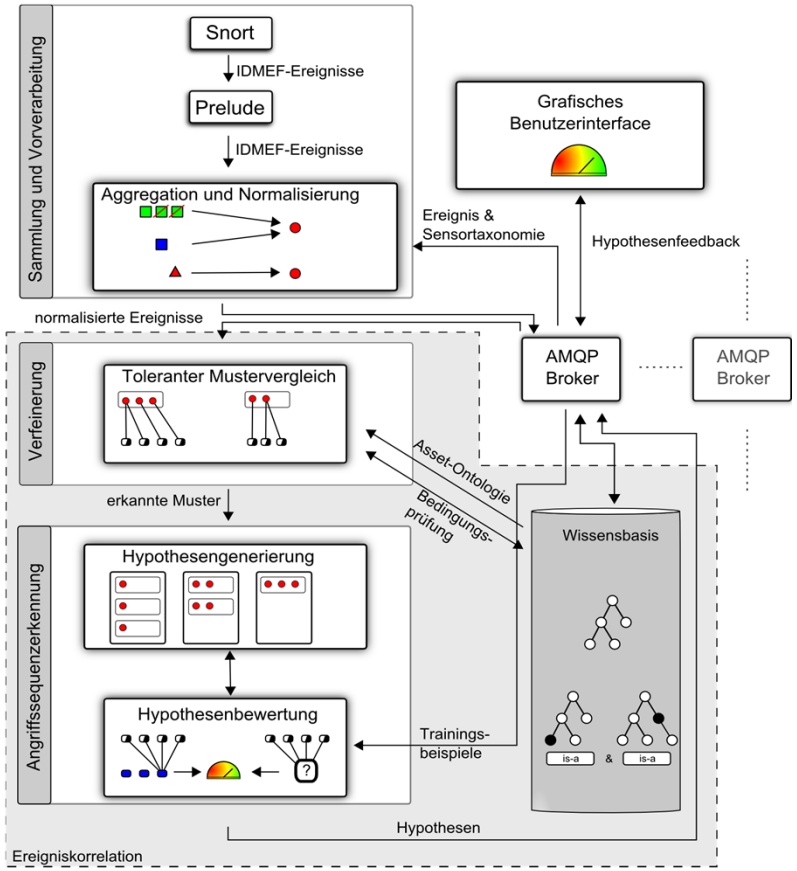
DECOIT

Forschungsprojekte

Consultancy & Internet Technologies

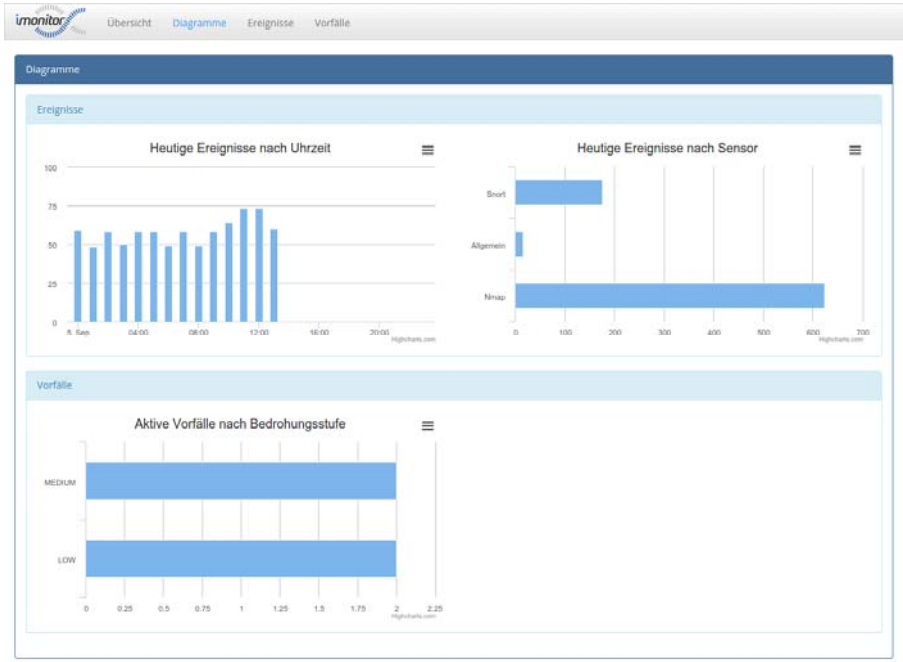
www.imonitor-project.de

- Das iMonitor-Projekt vom BMWi startete im Juli 2013 und wird im Juni 2015 enden
- Es soll eine neue Form der Ereigniskorrelation umgesetzt werden, die automatisiert neue Angriffsvarianten erkennt
- Korrelationsregeln sollen dabei nicht mehr nur manuell gepflegt werden müssen
- Eine Anomalie-Erkennung wird angestrebt – keine Mustererkennung



www.imonitor-project.de

- Hauptziele von iMonitor
  - Integration von unterschiedlichen Open-Source-Sensoren (Snort, Nmap und OpenVAS)
  - Entwicklung optimierter und skalierbarer KI-Verfahren
  - Automatisierte Definition von Handlungs-empfehlungen
  - Benachrichtigung und Dokumentation über ein Ticketsystem
  - Nutzung von Icinga als zentrales Monitoring-System

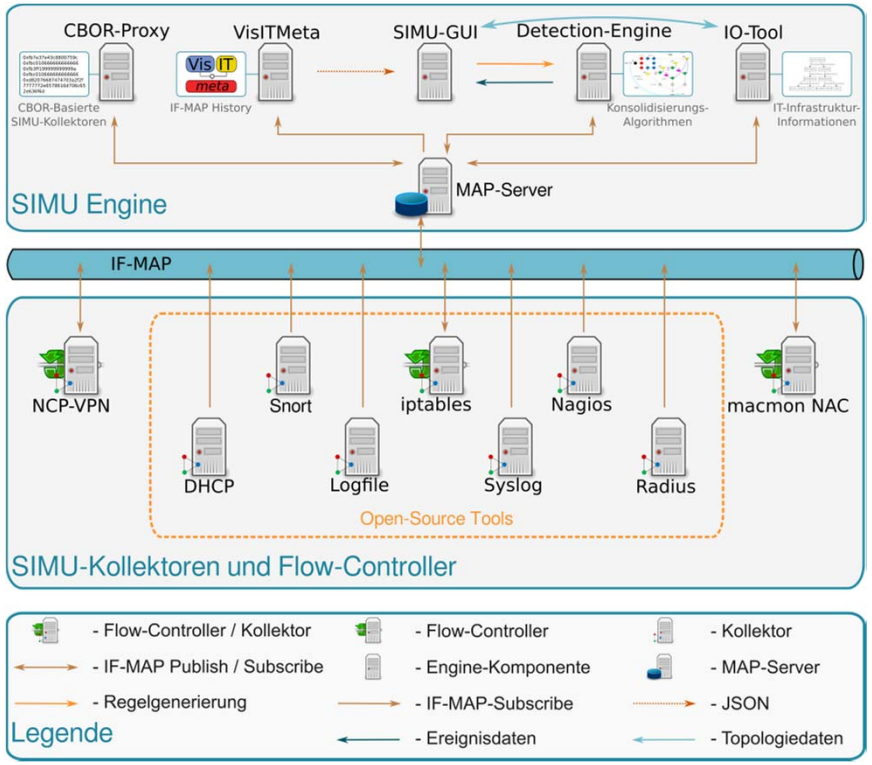


www.simu-project.de

- Das SIMU-Projekt vom BMBF startete im Oktober 2013 und wird im September 2015 enden
- Die Hauptziele des Projektes sind:
  - 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
- Die Datenkorrelation wird durch das IF-MAP-Protokoll der Trusted Computing Group (TCG) vorgenommen
- Dadurch ist der Austausch beliebiger Metadaten möglich
- Es werden Open-Source-Komponenten als Sensoren und Aktuatoren verwendet
- Eigenentwicklungen basieren ebenfalls auf dem Open-Source-Prinzip

www.simu-project.de

- SIMU-Kollektoren und Flow-Controller
  - IF-MAP-Clients
  - IF-MAP-Graph zur Analyse und intuitiven Regelerstellung (VisITMeta)
- SIMU-Engine
  - MAP-Server
  - Detection Engine
  - SIMU-GUI
  - CBOR-Proxy
  - IO-Tool



DECOIT

Fazit

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
- Aktuell werden verschiedene SIEM-Systeme von der DECOIT GmbH getestet (LogApp, ArcSight, LogRhythm, OSSIM)
- Ergebnis: Nicht alle SIEM-Systeme halten das, was sie versprechen!
- Durch die Nutzung von Open-Source-Systemen ergeben sich Vorteile bzgl. der Schnittstellen, Standards und Lizenzkosten
- Nur durch offene Schnittstellen kann das Zusammenspiel zwischen verschiedenen Sicherheitskomponenten gewährleistet werden
- Die Kosten und Beherrschbarkeit solcher Systeme stellen aber nach wie vor die Haupthindernisse für die Einführung dar

DECOIT

Vielen Dank für ihre Aufmerksamkeit

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

Consultancy & Internet Technologies