DECOIT

Workshop an der Hochschule Bremen

Sicherheitsrelevantes Monitoring zur Absicherung von Unternehmensdaten

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

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 Fehlermeldung des Anwenders die Fehlerursache 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

Pro-aktives Netzmonitoring

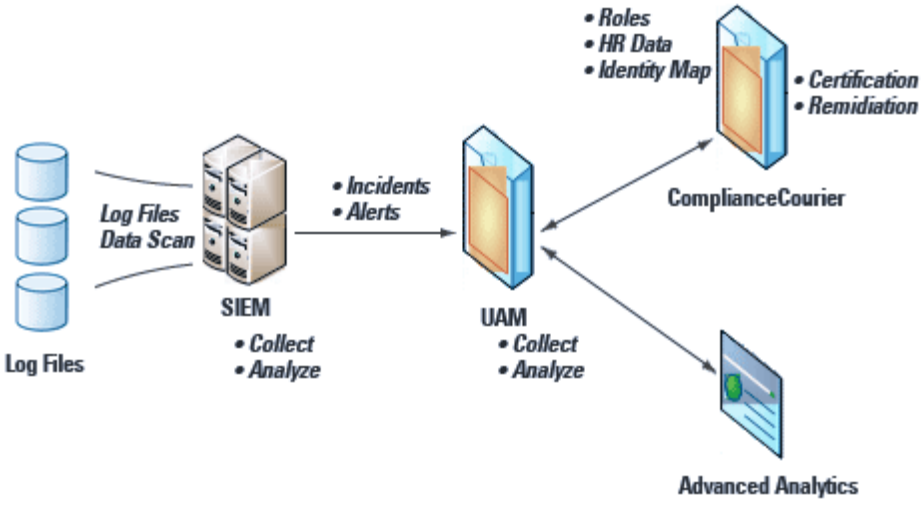
- Ein pro-aktives Netzmonitoring meldet Systemausfälle, bevor ein Anwender dieses bemerkt
- Der IT-Administrator hat bessere Pflegemöglichkeiten, da er den Zustand des Gesamtnetzes (Server, Clients, IP-Telefone, Netzwerk) kennt und darauf Einfluss nehmen kann
- Zusätzlich wird eine aktuelle Dokumentation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

Sicherheitsmanagement mit SIEM

- 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

Schwerpunkt eines SIEM-Systems

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



DECOIT

Sicherheitsrelevante Events

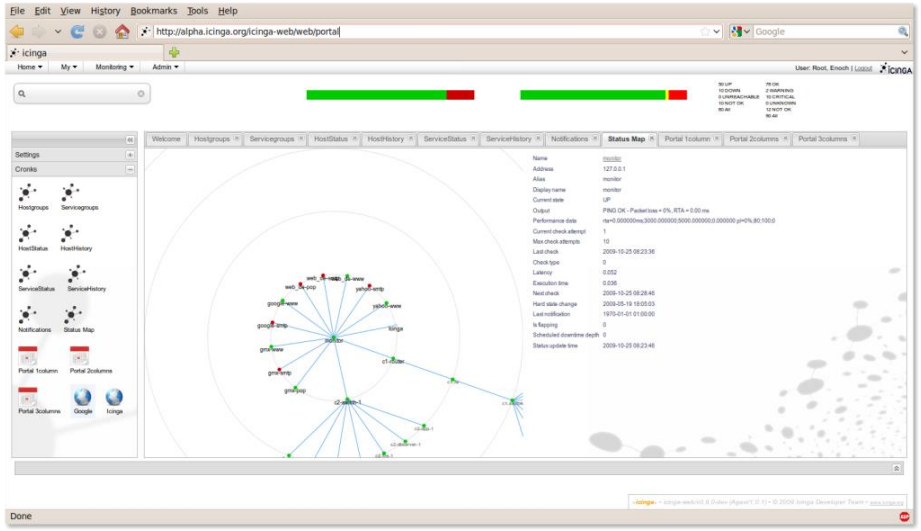
- Zusammenführung von sicherheitsrelevanten Events
  - **Extraktion:** Events sind in Rohform meist Einträge in Log-Dateien oder über das Netz versendete Systemmeldungen
  - **Homogenisierung/Mapping:** Events werden von unterschiedlichen Diensten erzeugt und aus unterschiedlichen Systemen extrahiert
  - **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

Auswahl von Monitoring-Systemen

- Unterschiedliche Monitoring-Protokolle lassen sich einsetzen:
  - Syslog
  - SNMPv1, SNMPv2, SNMPv3
  - Netflow
  - MIB-I, MIB-II
  - RMON1, RMON2, SMON
  - IF-MAP
- Unterschiedliche Monitoring-Systeme auf Basis von Open Source lassen sich unterscheiden:
  - Nagios (Icinga)
  - RRDtool (MRTG, Munin, Cacti)
  - OSSIM

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



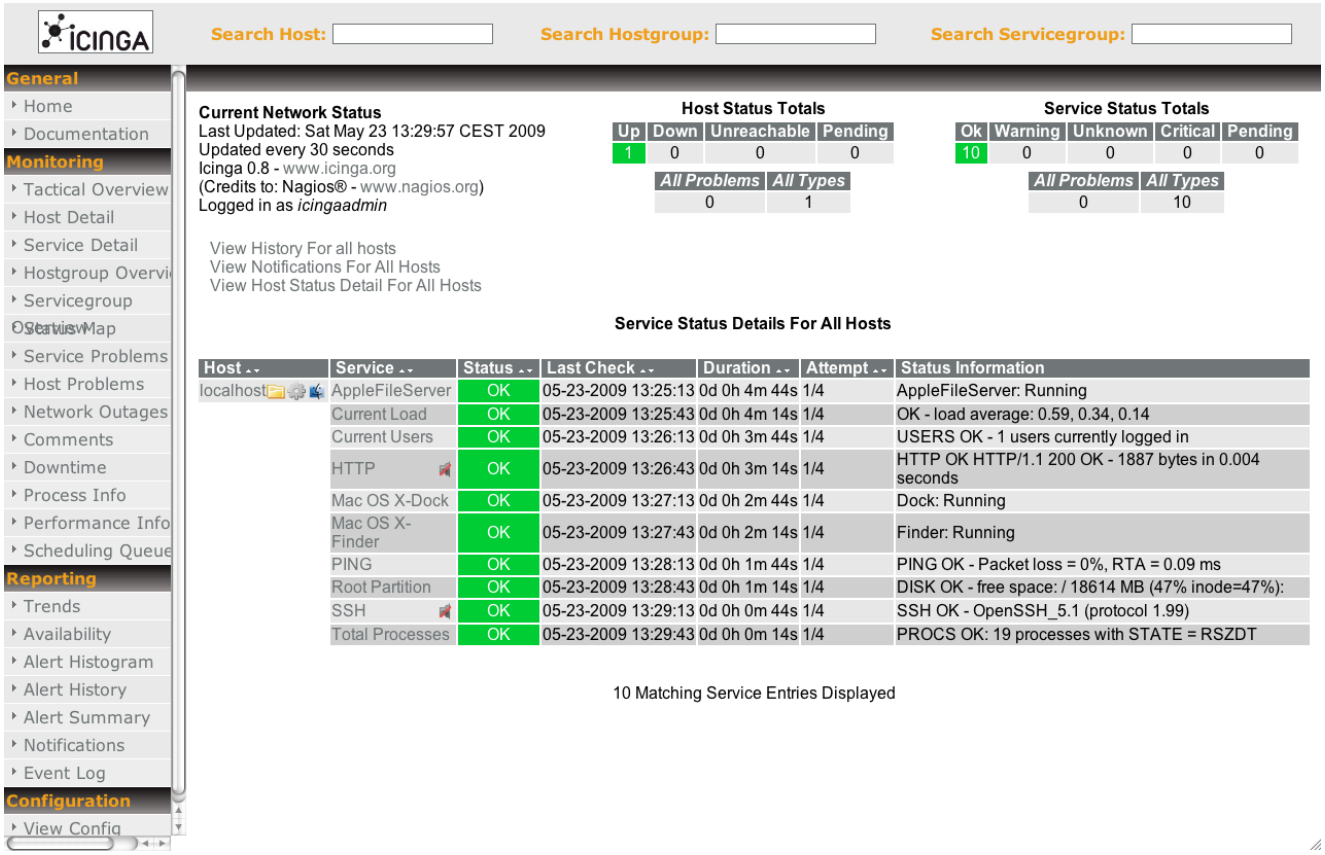
Icinga (Nagios)

- Konsolidierte Bewertung von einzelnen Alarmen mittels Plug-Ins ist möglich
- Nagios erlaubt die Überwachung von Log-Dateien nach regulären Ausdrücken
- Möglichkeit ein verteiltes Monitoring durchzuführen
- Hochverfügbarkeit kann realisiert werden
- Add-Ons für weitreichende Visualisierung von Zuständen und Verarbeitung von Performancedaten
- Nagios ist Open Source (GPL)

Überwachung

- Icinga (Nagios) führt die Überwachung mittels Plug-Ins durch und unterscheidet dabei zwischen Host- und Service-Checks:
  - Host-Check
    - Testet einen Rechner auf Erreichbarkeit (ping)
  - Service-Check
    - Prüft gezielt einzelne Netzwerkdienste ab: z.B. HTTP, SMTP, DNS usw., aber auch laufende Prozesse, CPU-Last oder Logfiles
- Zustände im Icinga (Nagios) sind farbcodiert:
  - Services-Zustände:
    - OK (grün), WARNING (gelb), CRITICAL (rot), UNKNOWN (orange).
  - Hosts-Zustände:
    - UP (grün), DOWN (rot), UNREACHABLE (rot).

Web-Interface – Service Detail



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 Nagios verschiedene Formen von Benachrichtigungen an (E-Mail, SMS, 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 bei Icinga 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

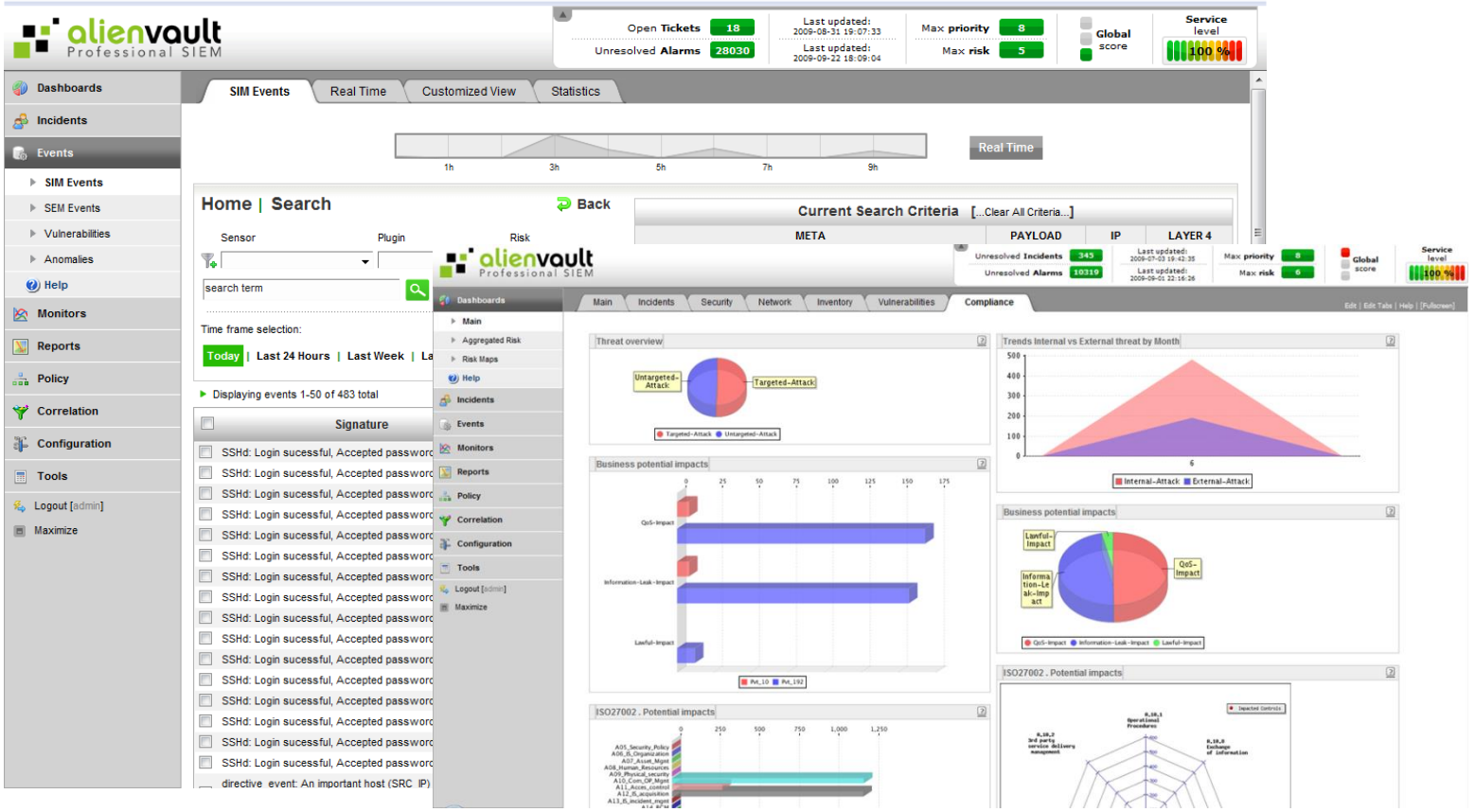
Open Source Security Information Management

- 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

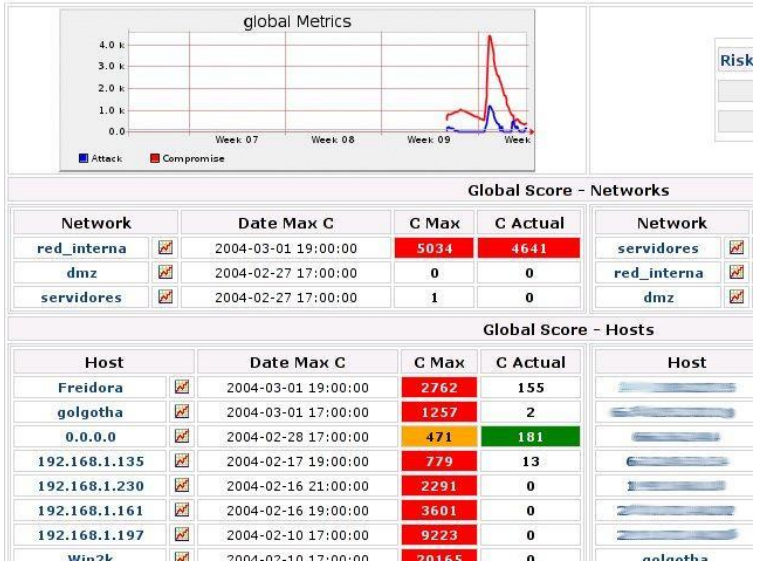
ALIEN VAULT OSSIM



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)

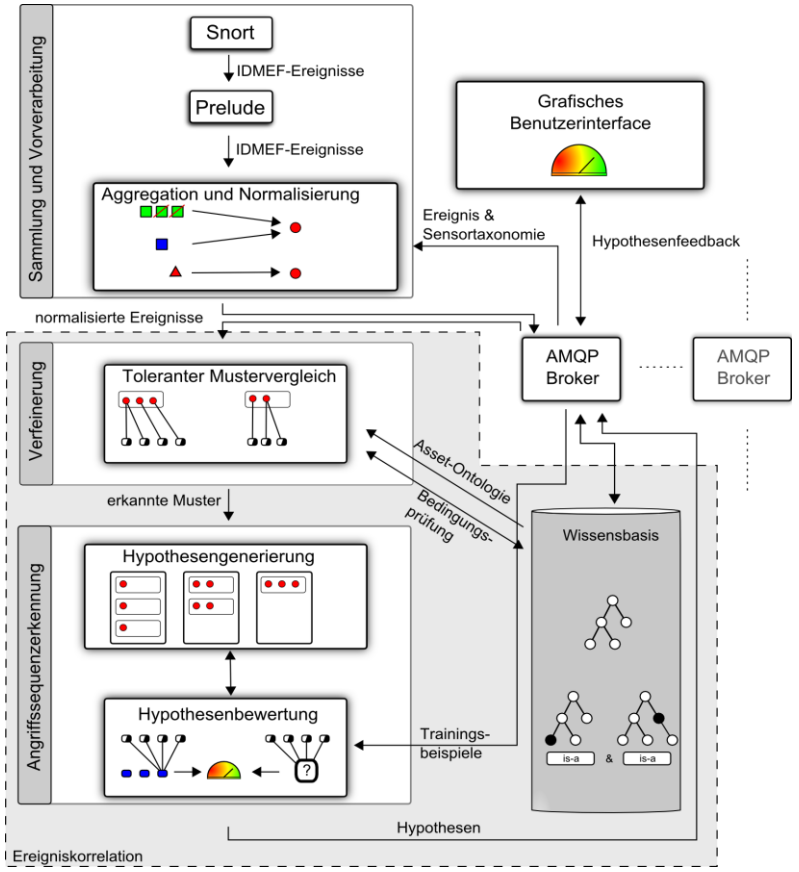


www.imonitor-project.de

- 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
- Das Projekt befindet sich noch in der Anfangs- bzw. Evaluierungsphase



Zusammenfassung

- Es gibt viele verschiedene Möglichkeiten, um aktives Netzwerk- und Servermonitoring zu betreiben
- Die DECOIT GmbH setzt dabei auf die Kombination verschiedener Systemlösungen, um das Beste aus verschiedenen Welten nutzen zu können
- Die Visualisierung des Netzes, seiner Server und Daten bekommt einer immer höheren Bedeutung, da auf der einen Seite die Verfügbarkeit ansteigt und auf der anderen Seite Virtualisierungstechniken das Netz immer unübersichtlicher werden lassen
- Neben der Verfügbarkeit profitiert auch die IT-Sicherheit und die Netzdokumentation vom Monitoring
- Es wird immer wichtiger Datendiebstahl vorzubeugen und ungewöhnliche Prozesse im Unternehmen wahrnehmen zu können

Vielen Dank für ihre Aufmerksamkeit

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

Consultancy & Internet Technologies