Intelligentes Monitoring der IT-Sicherheit durch den Einsatz von SIEM

Kai-Oliver Detken · Carsten Elfers · Malte Humann
Marcel Jahnke · Stefan Edelkamp

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

Agenda

- Kurzeinführung in SIEM-Systeme
- Architektur des F&E-Projektes iMonitor
- Zeitreihenbasierte Anomalie-Erkennung
- Ereignis-Korrelation
- Erkennung von Vorfallvariationen
- Wissensaustausch
- Anwendungsfall
- Zusammenfassung

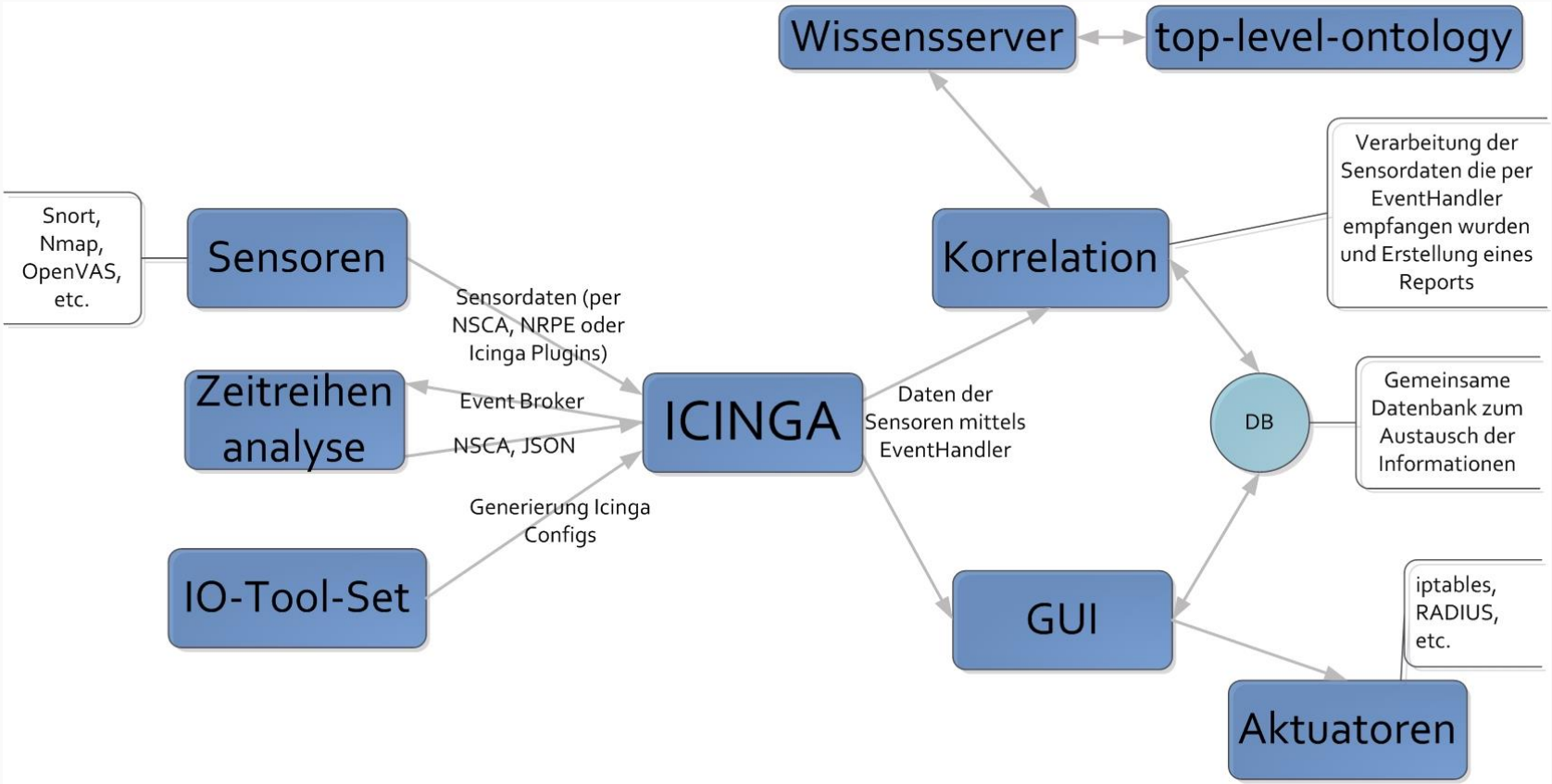
SIEM-Definition

- 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.

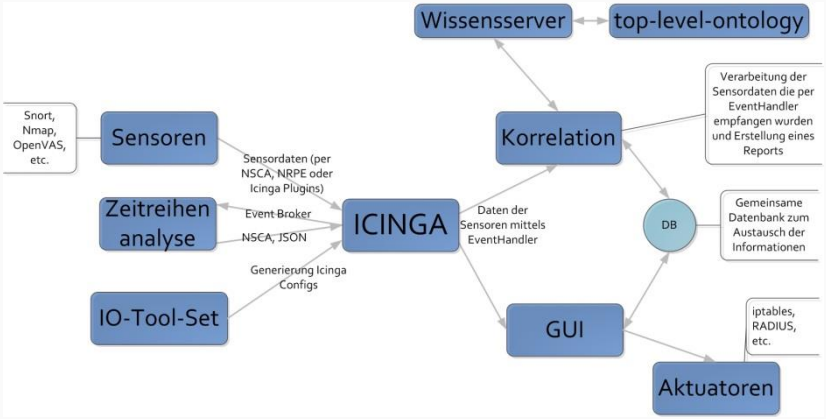
Das F&E-Projekt imonitor

- 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)



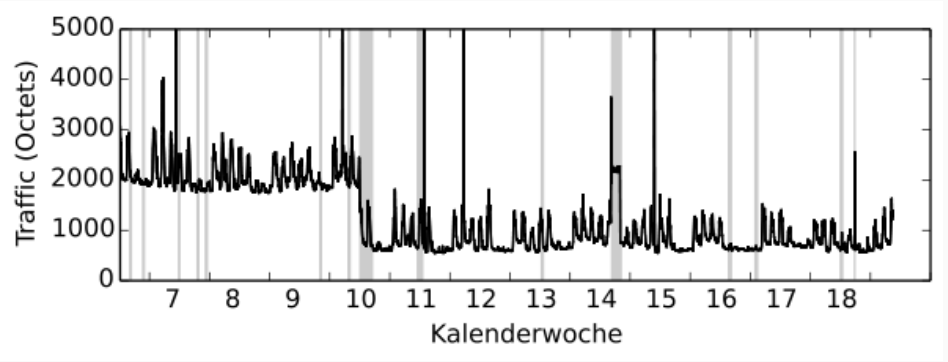
- **Sensoren:** Analysetools wie *Snort*, *Nmap* und *OpenVAS* sammeln Daten der Unternehmensumgebung, um das Normalverhalten zu erkennen
- **Zeitreihenanalyse:** Analysiert das Normalverhalten und versucht Anomalien ausfindig zu machen, ohne sich allein auf Mustererkennung zu stützen
- **IO-Toolset:** 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

Zeitreihenbasierte Anomalie-Erkennung (1)

- Die Zeitreihenanalyse erweitert *Icinga* um eine Komponente, die es ermöglicht, alle eingehenden *Performance-Daten* auf Anomalien zu überprüfen
- Da Icinga nicht auf Anomalie-Erkennung spezialisiert ist, können sie bisher nicht sicher erkannt werden
- Auch das Fehlen von Werten kann eine Anomalie darstellen, die nicht durch Schwellenwerte erkannt werden kann
- Daher müssen passende Schwellwerte vorab konfiguriert werden, um diese Überprüfung nutzen zu können
- Die zeitreihenbasierte Anomalie-Erkennung ermittelt die zur Auswertung nötigen Informationen selbst, auf Basis der eingehenden Performance-Daten
- Die Grundlage bildet dabei das Erkennen von sich wiederholenden Mustern in den Daten
- Ein längeres Trainingsintervall sollte eingeplant werden

Zeitreihenbasierte Anomalie-Erkennung (2)

- Da die Performance-Daten selbst nur Zahlenwerte sind, lassen sie sich zusammen mit dem jeweiligen Zeitpunkt der Meldung als eine Zeitreihe auffassen
- Um ein wiederkehrendes Muster zu erkennen, wird die Information eines Periodogrammes mit denen der zyklischen Autokorrelation kombiniert
- Aus den verbleibenden Musterlängen wird die mit größtem Autokorrelationswert ausgewählt
- Sobald die Länge des Musters bekannt ist bzw. geschätzt werden kann, lässt sich für die komplette Zeitreihe ein „durchschnittliches“ Muster berechnen
- Wird ein neuer Messwert von *Icinga* empfangen, kann er mit dem entsprechenden Eintrag im Muster verglichen werden



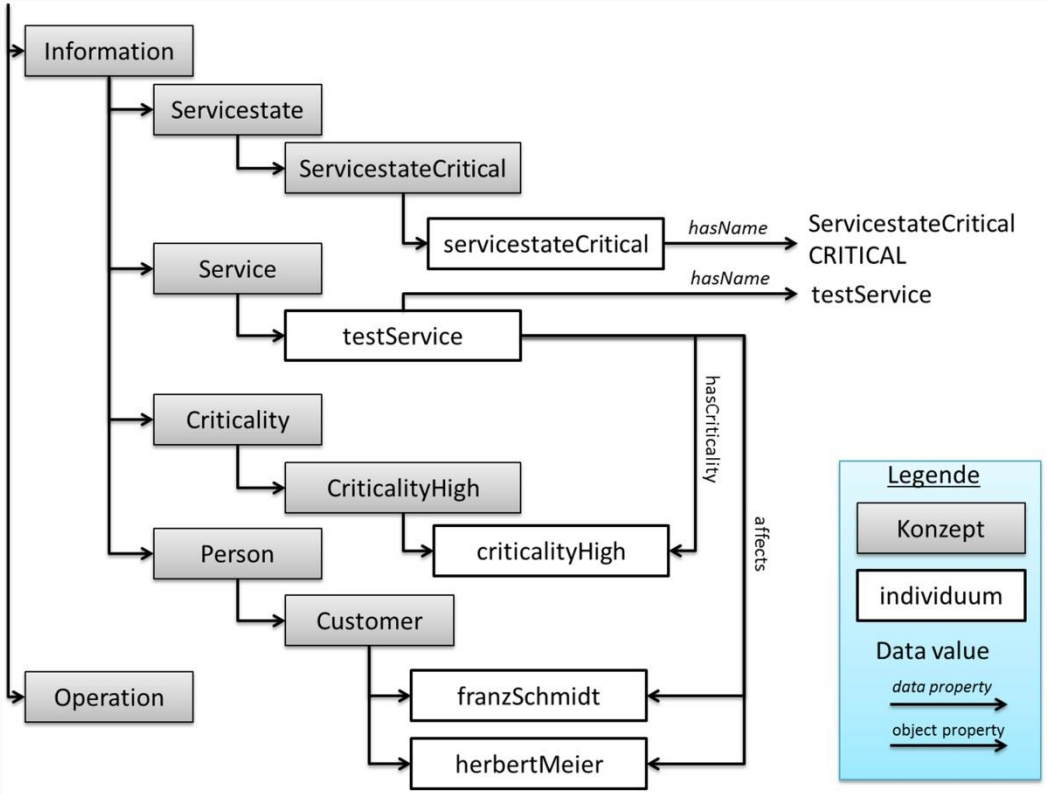
Von der Zeitreihenanalyse an Icinga gemeldete Anomalien (grau) in durch Icinga via SNMP gesammelten Trafficdaten (schwarz)

Ereignis-Korrelation (1)

- Um einen möglichst umfangreichen Nutzen aus Icinga-Sensorereignissen ziehen zu können, wurde Icinga um eine *Ereigniskorrelation* ergänzt
- Diese ermöglicht, Ereignisse sowohl mit Hintergrundwissen als auch Ereignisse untereinander in Beziehung zu setzen bzw. zu korrelieren
- Unter *Hintergrundwissen* versteht man z.B. Informationen über IT-Assets, Prozessschritte mit deren Abhängigkeiten oder eingesetzte Software und Softwareversionen mit deren Verwundbarkeiten
- Dadurch kann geprüft werden, ob bei einem Ausfall eines Hosts wichtige betriebliche Prozesse gefährdet sind oder ob eine erkannte Anomalie im Zusammenhang mit einer Verwundbarkeit steht
- In *iMonitor* wurde Icinga um eine solche Ereigniskorrelation, basierend auf einer sogenannten *Ontologie* bereichert
- Eine *Ontologie* ermöglicht die Repräsentation von SIEM relevanten Informationen in einer strukturierten Form

Ereignis-Korrelation (2)

- Die Abbildung zeigt einen Ausschnitt der Ontologie, die alle statischen Informationen in *Konzepte* strukturiert
- Beispiel: der kritische Servicezustand (ServicestateCritical) ist ein besonderer Servicezustand (Servicestate)
- So können *Korrelationsregeln* unabhängig von der konkreten Einsatzumgebung definiert werden
- In der Klasse *Information* werden alle statischen Infos gesammelt, während die Klasse *Operation* für die Korrelation zur Laufzeit verwendet wird
- Die Korrelationsregeln besitzen einen *Bedingungsteil* und einen *Aktionsteil*
- Im Aktionsteil kann eine *Handlungsempfehlung* zur Erklärung des Vorfalls generiert werden
- Dazu werden Hintergrundinfos gesammelt, die für eine Handlungsempfehlung oder Vorfallerklärung benötigt werden

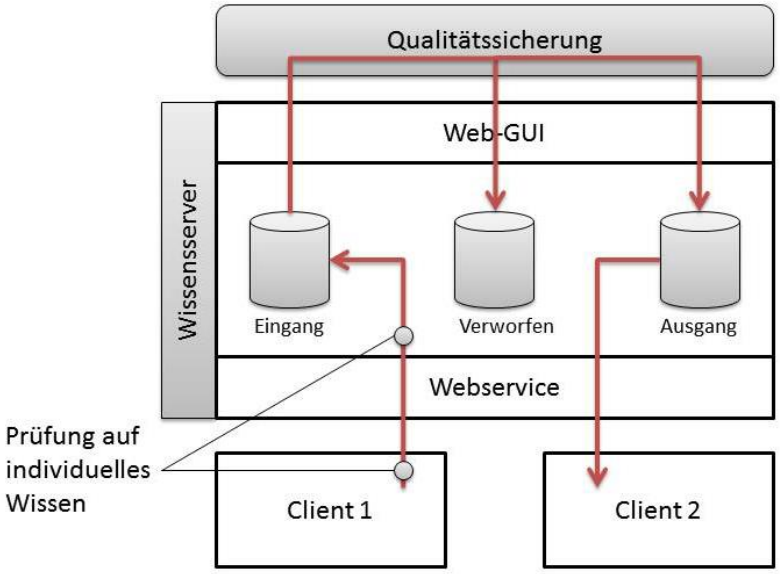


Erkennen von Vorfallvariationen

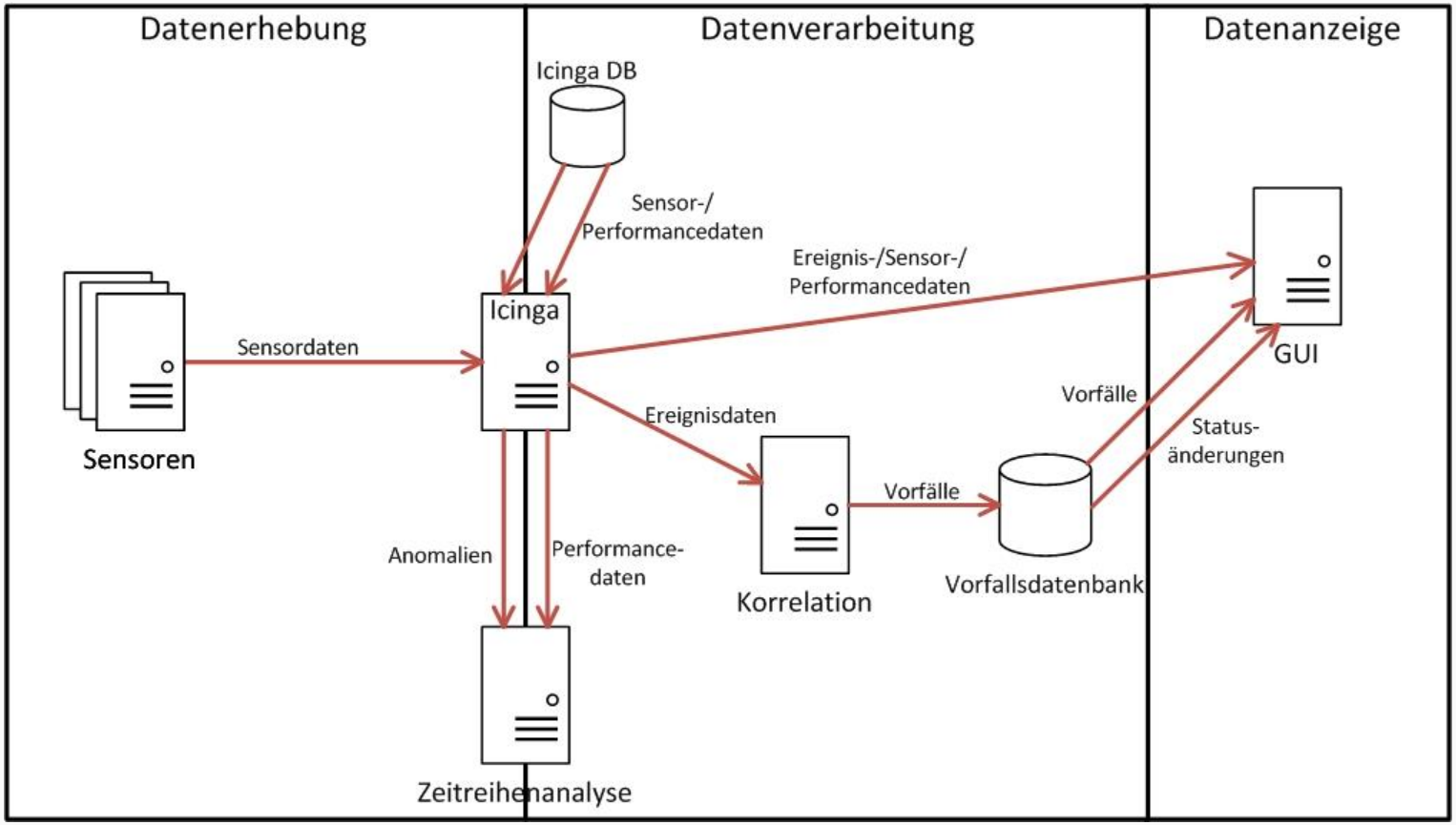
- *SPARQL* wurde als Anfragesprache für die Ereignis-Korrelation in iMonitor eingeführt
- Um auch Variationen von Vorfällen erkennen zu können, wurde die SPARQL-Anfragesprache zudem durch *Abstraktionsfunktionen* erweitert
- Mit einer Abstraktionsfunktion können Teile einer SPARQL-Bedingungen gekennzeichnet werden
- Diese Kennzeichnung führt dazu, dass für den Fall, dass keine Regel auf ein Ereignis greift, diese Bedingung automatisch von der Korrelation abstrahiert werden darf
- Der *Bedingungsteil* kann in iMonitor direkt in einer SPARQL-Abfrage individuell festgelegt werden
- Die *Abstraktion* wird solange wiederholt, bis mindestens eine Regel das Ereignis behandelt oder das an der Abstraktionsfunktion anzugebende Abstraktionsmaximum erreicht ist

Wissensaustausch

- Um den *Modellierungsaufwand* möglichst gering zu halten, wurde eine Methode entwickelt, die es ermöglicht die Korrelationsregeln auch anderen Systemen zur Verfügung zu stellen
- Zusätzlich können vorgefertigte Korrelationsregeln ohne Integrationsaufwand heruntergeladen und verwendet werden
- Bevor eine Regel zur Verfügung gestellt wird, wird vom Client geprüft, ob kein individuelles Wissen verwendet wurde
- Problematisch ist dabei jedoch die automatische Überprüfung der Semantik, die durch eine manuelle Qualitätssicherung umgesetzt werden sollte
- Das heißt, es wird jede neue Regel manuell überprüft, bevor sie freigeschaltet wird

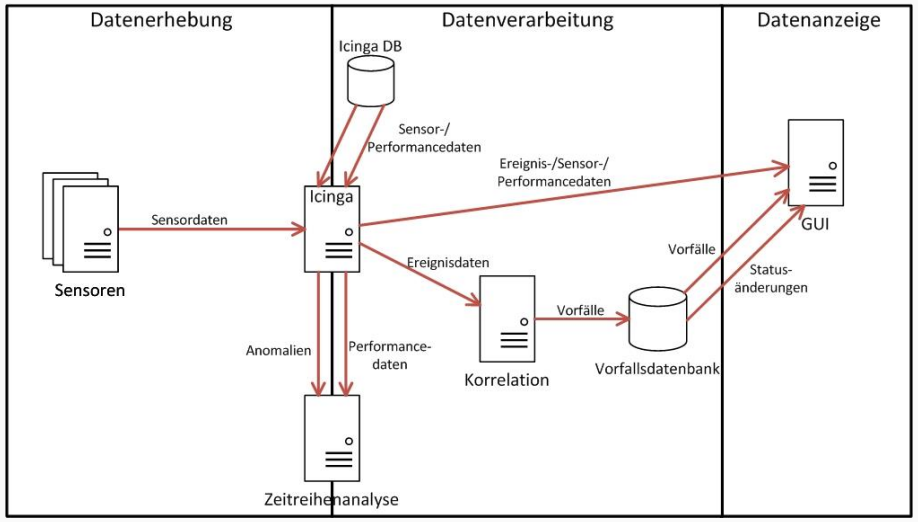


Anwendungsfall (1)

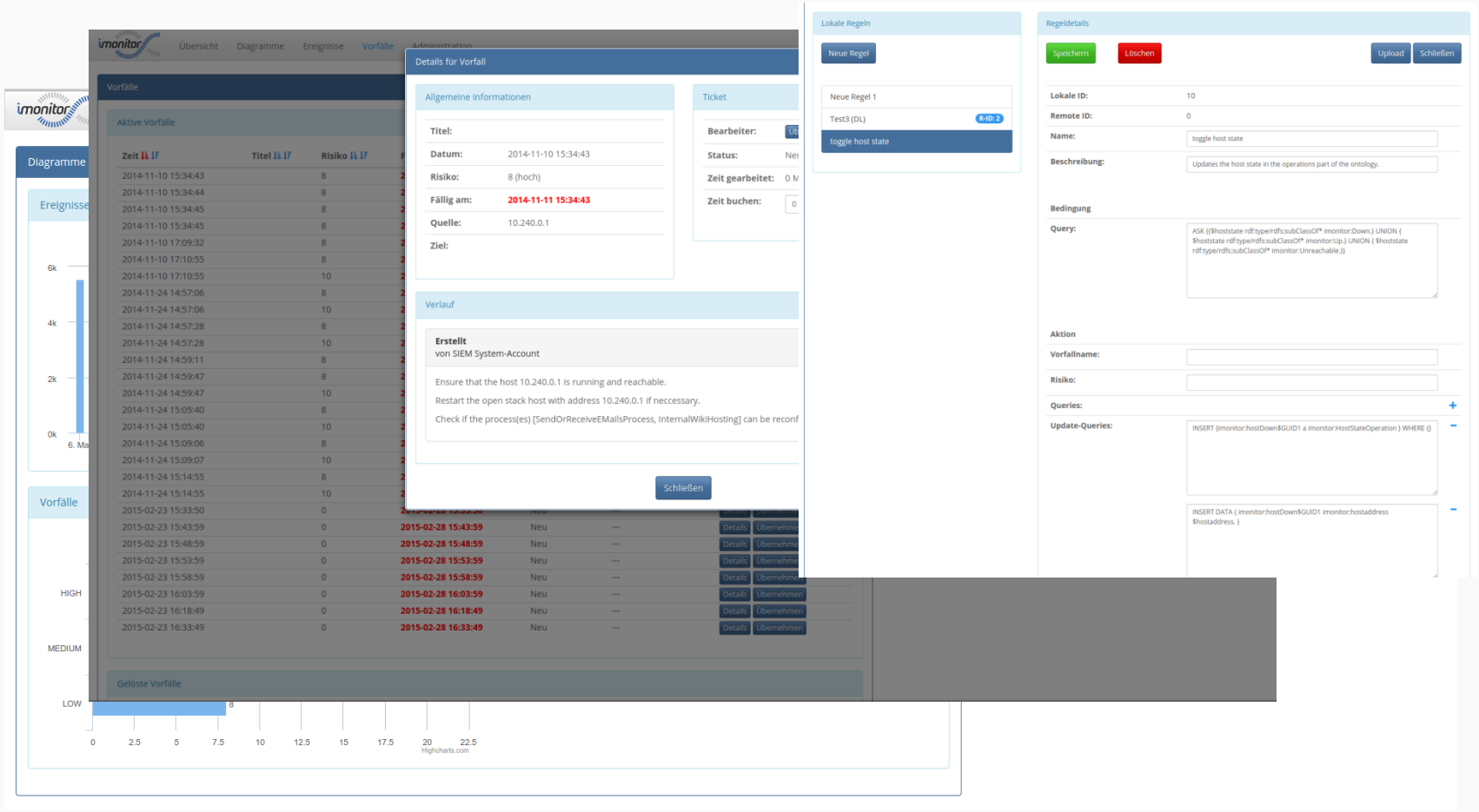


Anwendungsfall (2)

- Die *Datenerhebung* beinhaltet die Sensordaten der verschiedenen Kollektoren und die Erstellung der Hintergrundinfos
- *Die Datenverarbeitung* beinhaltet die Zeitreihenanalyse, die nach Anomalien die Datenbank durchforstet
- Zusätzlich ist hier auch die Korrelation enthalten, die die gespeicherten Daten aus Icinga verarbeitet und die einzelnen Ereignisdaten anhand der Regeln auswertet
- Die Vorfallsdatenbank enthält Erläuterungen des Vorfalls und etwaige Handlungsempfehlungen
- Die Korrelation stuft die Vorfälle in entsprechende Risikowerte ein
- Die *Datenanzeige* beinhaltet die SIEM-GUI, welche die Events anzeigt
- Wird ein neuer Vorfall in der Datenbank erkannt so legt die SIEM-GUI auch ein entsprechendes Ticket in dem angeschlossenem *Ticketsystem* an



SIEM-GUI



Zusammenfassung

- SIEM-Systeme ermöglichen eine ganzheitliche Sicht auf die IT-Sicherheit eines Unternehmens
- Intelligente Anomalie-Erkennung ist bei den Anbietern bislang kaum vertreten (Schwerpunkt ist Mustererkennung)
- Offene Schnittstellen sind notwendig, um auch andere Systeme mit einbinden zu können
- Skalierbarkeit und Performance von SIEM-Systemen ist durchaus ein Problem, welches auch bei iMonitor aufgetreten ist (Stichwort: Big Data)
- Teile der iMonitor-Arbeiten werden in die vorhandenen Monitoring-Systeme der Industriepartner einfließen
- Ausführliche Use-Case-Demonstration unter *Download* auf der Webseite: www.imonitor-project.de oder auf YouTube

Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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