Die KRITIS-Lösung zur Angriffserkennung –

gemäß IT-Sig 2.0

secunet monitor KRITIS ist die passive und rückwirkungsfreie Monitoring-Lösung zur signaturbasierten Angriffserkennung auf Netz- und Systemebene (NIDS- und SIEM-Funktionalität) nach aktuellen und zukünftigen Regularien.

secunet
monitor KRITIS

2 Ebenen der Angriffserkennung

Systemebene

- Nutzung der Log-Daten von unterschiedlichen IT- und OT-Systemen
- Aggregation und Analyse der Log-Daten in einem zentralen Speicher (SIEM)

Netzebene

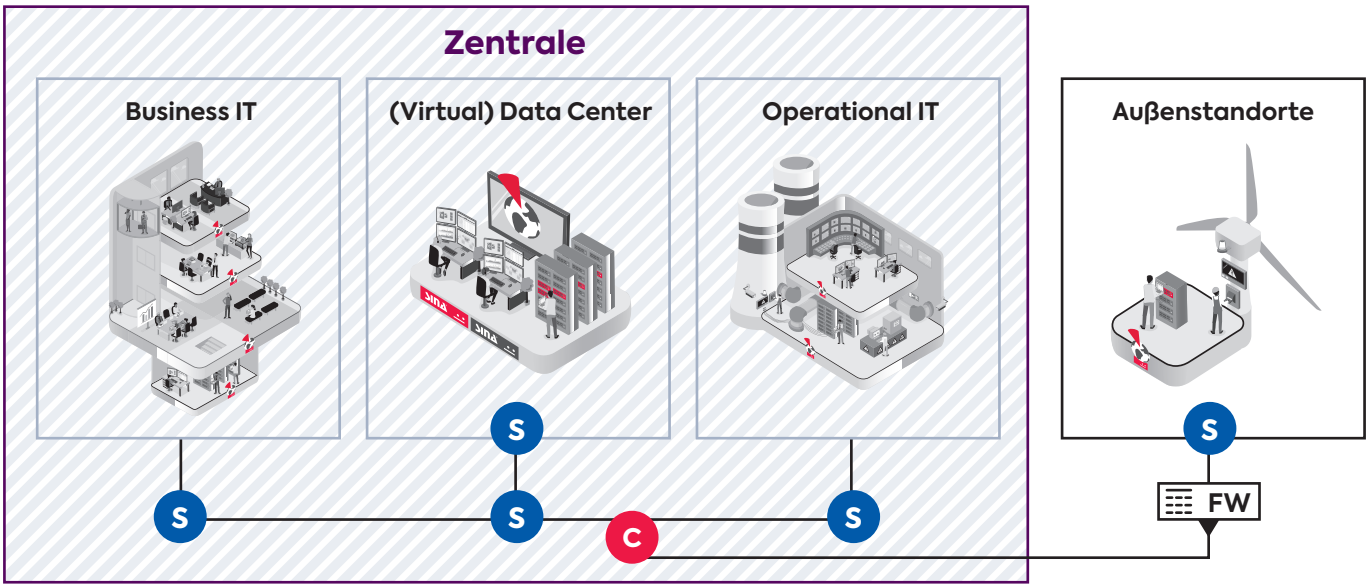
- Nutzung eines netzbasierten IDS (NIDS) zur Netzwerkanalyse
- Echtzeit-Bewertung der Flow-Daten und Übermittlung von Daten zu sicherheitsrelevanten Ereignissen (Events) an einen zentralen Speicher

- **Abgleich gegen existierende Muster**
- **Aufbereitung der Daten zur Alarmierung und weiteren Analyse**

Die einfache Lösung zur Angriffserkennung optimiert für KRITIS-Betreiber

- Umsetzung aller technischen MUSS-Anforderungen der Orientierungshilfe zur Erfüllung des IT-SiG 2.0
- Signaturbasierte Angriffserkennung auf Netzebene (NIDS)
- Aggregation und Analyse von Log-Daten auf System-Ebene
- Passives und rückwirkungsfreies System für IT & OT
- Modular, leicht nutzbar und kosteneffizient Installations- und betriebsfähig in Airgapped-Umgebungen
- Übersichtliches Changelog zur sicheren Dokumentation
- Unterstützt Meldungen von Sicherheitsvorfällen an das BSI
- Globales Whitelisting

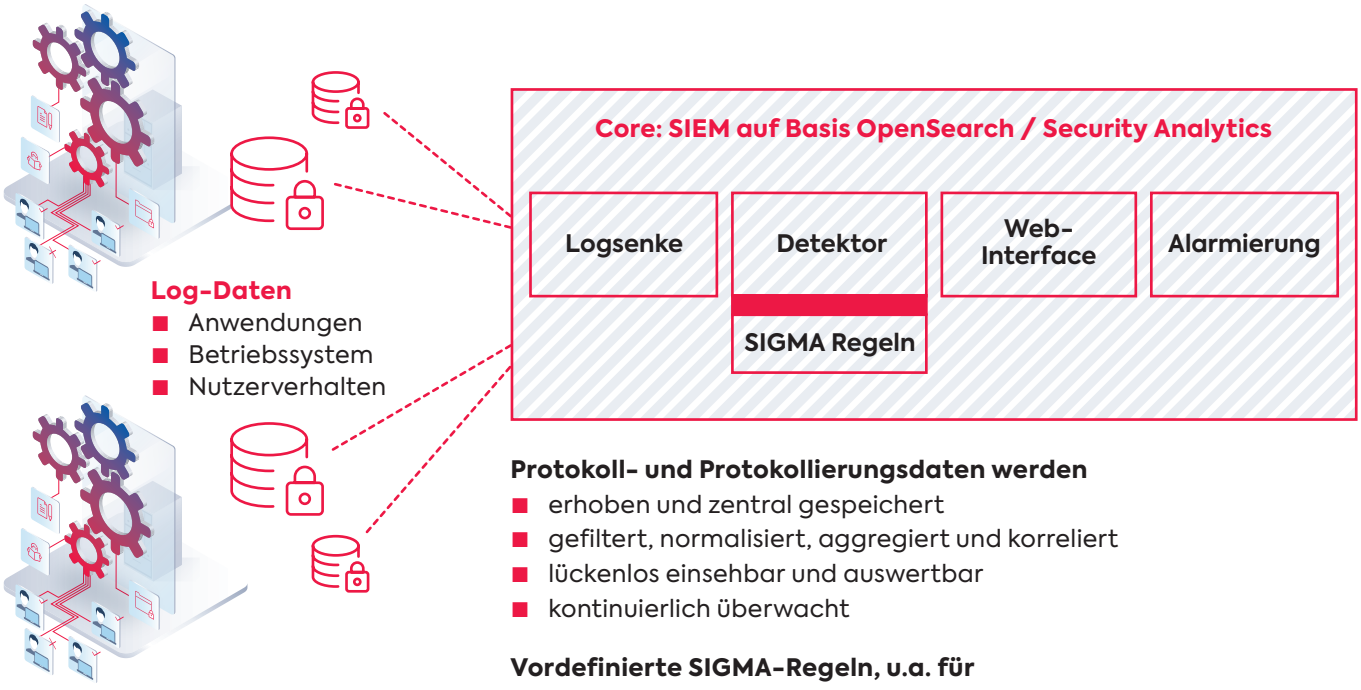
Netzwerkebene: Funktionsweise der Komponenten



S Sensor
- Analysiert den Netzwerkverkehr an wichtigen Knotenpunkten
- Erzeugt Events

C Core
- Aggregation der Events
- Stellt die Benutzeroberfläche bereit

Systemebene: Funktionsweise der Komponenten



Protokoll- und Protokollierungsdaten werden
- erhoben und zentral gespeichert
- gefiltert, normalisiert, aggregiert und korreliert
- lückenlos einsehbar und auswertbar
- kontinuierlich überwacht

Vordefinierte SIGMA-Regeln, u.a. für
- Applikationen (Active Directory, DNS, u.a.)
- Betriebssyteme (Linux, MS Windows, u.a.)

Hier Kontakt aufnehmen info@secunet.com

secunet