secunet

Digitale Transformation und Cybersecurity Regulierung: gesetzliche Anforderungen, Lösungsansätze und Chancen

Joachim Cappel

Principal, Managementsysteme & Audits

secunet Security Networks AG

Agenda

01 Überblick: gesetzliche Vorgaben und Orientierungshilfe

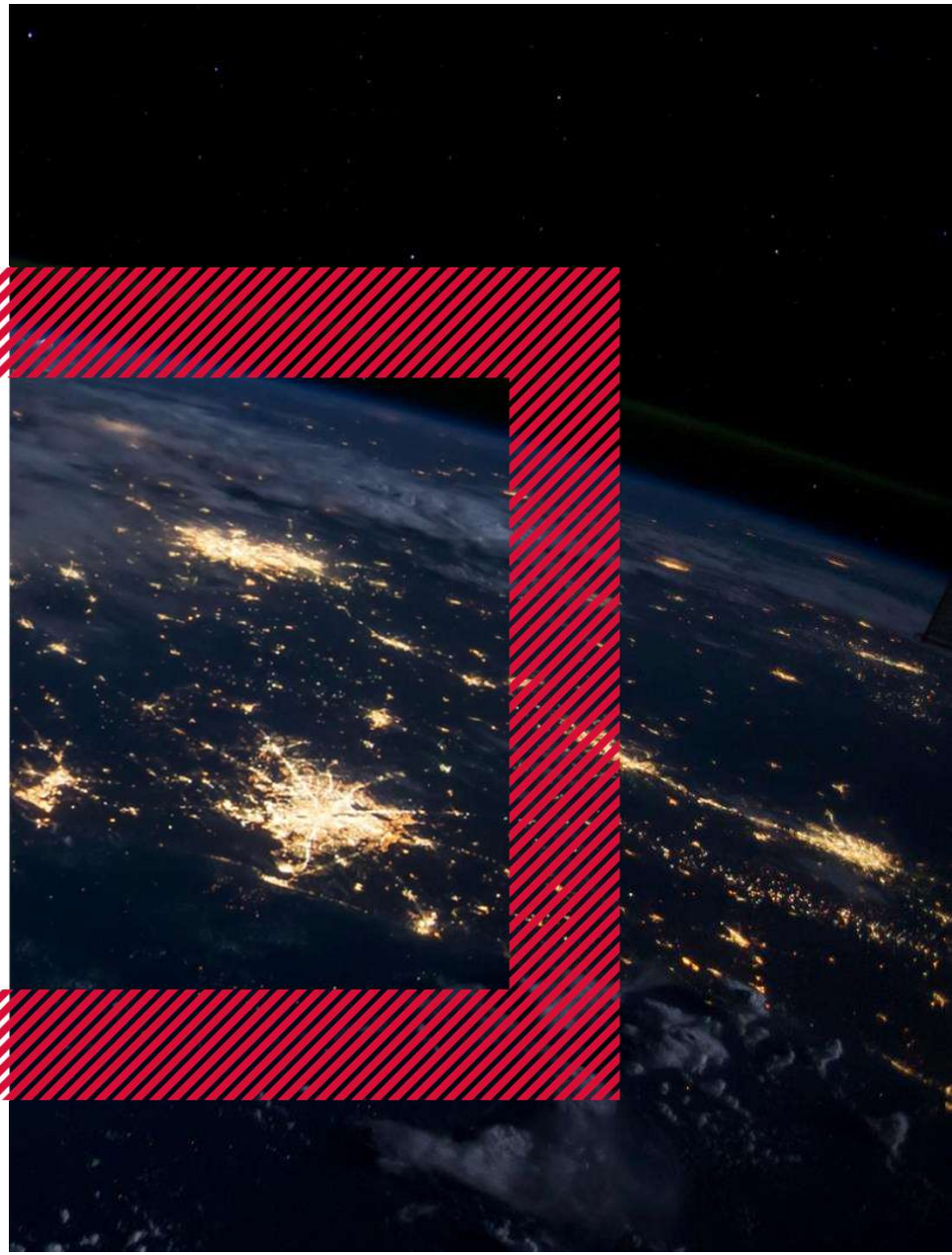
02 ISO/IEC 27002:2022 – Was hat sich geändert?

03 Wichtige Begriffe und deren Zusammenhang

04 Praktische Umsetzung

01

Überblick: gesetzliche Vorgaben und Orientierungshilfe



Massive Cyberangriffe auf deutsche Unternehmen

203 Mrd.
Euro Schaden
pro Jahr durch Angriffe auf deutsche Unternehmen

9 von 10
Unternehmen werden Opfer von Datendiebstahl, Spionage oder Sabotage

51 %
der betroffenen Unternehmen wurden in 2021 aus dem Bereich des organisierten Verbrechens und Banden attackiert

KRITIS-Meldungen

+ 14 %
Starker Anstieg von Angriffen aus Russland und China ggb. 2021

45 %
der Unternehmen meinen, dass Cyberattacken ihre geschäftliche Existenz bedrohen können

Quelle: BDI, Bitkom, Tenable

Gesetzliche Grundlage verändert sich

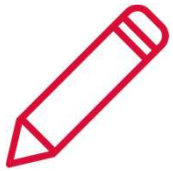
Das neue IT-Sicherheitsgesetz

Ab wann?

ab dem 1. Mai 2023

Was genau?

Anforderungen in der Orientierungshilfe



Wie erfolgt der Nachweis?

BSI veröffentlicht Formulare

Bußgelder werden erhöht!
4% vom Umsatz, bis zu 20 Mio. EUR

Orientierungshilfe des BSI

- Auditierbare Anforderungen im Sinne einer Prüf/Checkliste
  - **MUSS, SOLLTE, KANN** Anforderungen
- Referenziert auf **Grundschutzbausteine**
- Unterteilung der Anforderungen in:
  - Protokollierung
  - Detektion
  - Reaktion

Orientierungshilfe des BSI

Protokollierung

Umsetzung aller Basisanforderungen von **OPS.1.1.5 *Protokollierung***

- Filterung, Normalisierung, Aggregation, Korrelation
- Erneute Prüfung nach Umsetzung

Detektion

Umsetzung aller Basisanforderungen von **DER.1 *Detektion von sicherheitsrelevanten Ereignissen***

- **signaturbasierte Detektion**
- Kontinuierliche Datenüberwachung
- Einsatz von Network-Based Intrusion Detection Systemen
- Ereignismeldung und Vorfallverhinderung

Reaktion

Umsetzung aller Basisanforderungen von **DER.2.1 *Behandlung von Sicherheitsvorfällen***

- Effiziente Angriffsbehandlung
- Vorfallmeldung an Behörden
- Erhaltung der kritischen Dienstleistungen

Orientierungshilfe des BSI – Umsetzungsgradmodell

secunet monitor KRITIS

…erfüllt die Anforderungen

…ist kontinuierlich ausbaufähig für weitere Stufen des Umsetzungs-grad-Modells

0	keine Anforderungen umgesetzt keine Planungen zur Umsetzung von Anforderungen
1	Planungen zur Umsetzung von Anforderungen für mindestens einen Bereich noch keine konkreten Umsetzungen
2	Umsetzung der Anforderungen in allen Bereichen begonnen nicht alle MUSS-Anforderungen umgesetzt
3	Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft kontinuierlicher Verbesserungsprozess etabliert oder in Planung
4	Alle MUSS- Anforderungen wurden für alle Bereiche umgesetzt Alle SOLLTE-Anforderungen wurden umgesetzt kontinuierlicher Verbesserungsprozess
5	Alle MUSS- und SOLL- und KANN-Anforderungen wurden für alle Bereiche umgesetzt Zusätzliche Maßnahmen entsprechend der Risikoanalyse kontinuierlicher Verbesserungsprozess

Zulässig ab 1. Mai 2023

Zielumsetzungsgrad

02

ISO/IEC 27002:2022 – Was hat sich geändert?

Aufbau der neuen ISO27001:2022

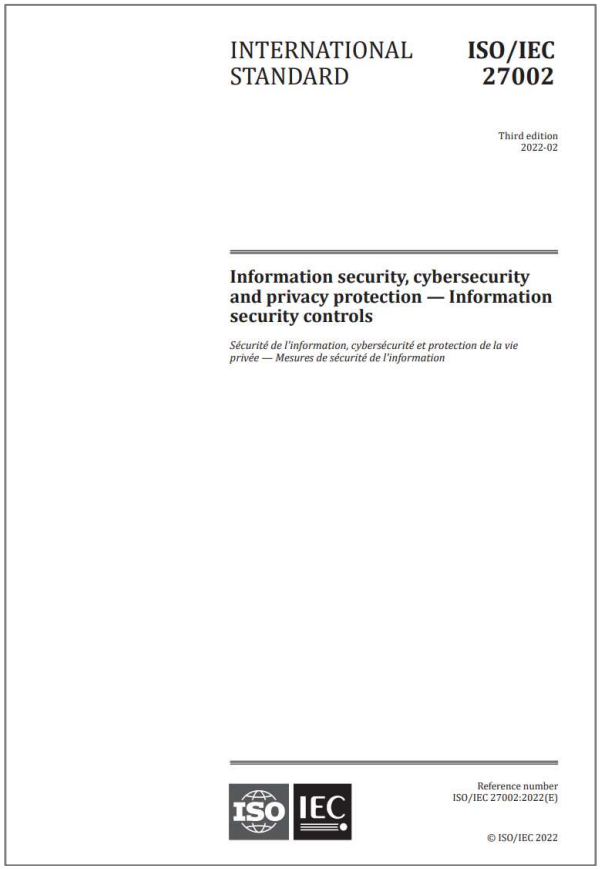
Kapitel 4 bis 10 ISO 27001

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung

Aufbau ISO27001: 2022

Annex A der ISO27001:2022 A.5 bis A.8

A.5 Organizational controls
A.5.1 – A.5.37
A.6 People controls
A.6.1 – A.6.8
A.7 Physical controls
A.7.1 – A.7.14
A.8 Technological controls
A.8.1 – A.8.34


INTERNATIONAL STANDARD
ISO/IEC 27002
Third edition 2022-02
Information security, cybersecurity and privacy protection — Information security controls
Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information
Reference number ISO/IEC 27002:2022(E)
© ISO/IEC 2022

- Neue Struktur der Annex A-Controls: Nur noch 4 Annex-Abschnitte
- Von 114 Anforderungen auf 93 reduziert (21 weniger)
- 56 Anforderungen wurden zu 24 Anforderungen zusammengefasst
- 11 neue Anforderungen sind dazugekommen
- 58 aktualisierte Anforderungen

03

Wichtige Begriffe und deren Zusammenhang

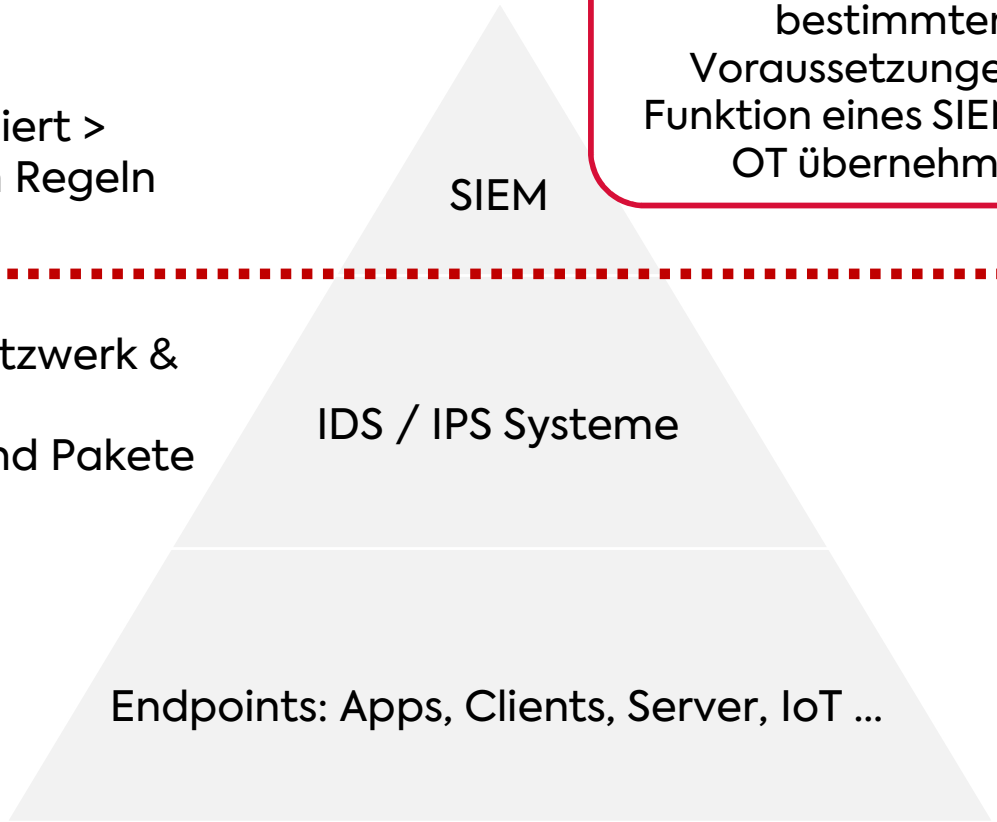
Technologien zur Angriffserkennung

Hinweis:
IDS Systeme können unter bestimmten Voraussetzungen die Funktion eines SIEM in der OT übernehmen.

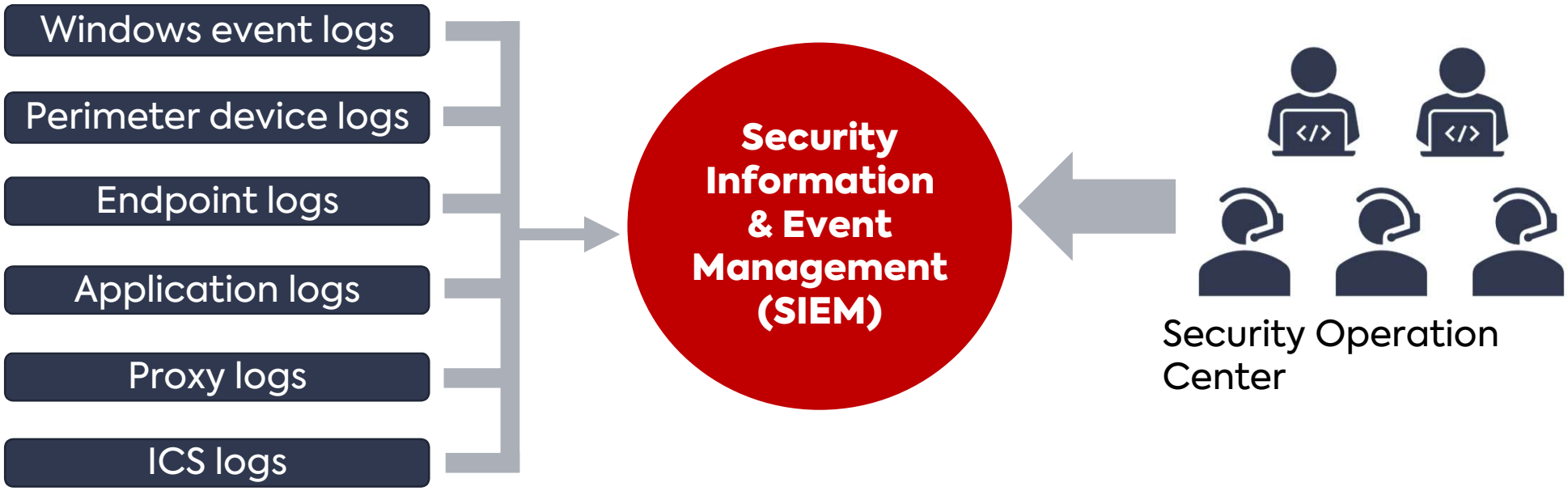
Daten werden aggregiert > normalisiert > gefiltert > korreliert nach definierten Regeln

Überwachung von Aktivitäten im Netzwerk & Netzwerkknoten
> IP Adressen, Netzwerkprotokolle und Pakete

Überwachung der Endgeräte durch Eventlogs und hostbasierte IDS Systeme



SIEM & SOC


Windows event logs
Perimeter device logs
Endpoint logs
Application logs
Proxy logs
ICS logs
Security Information & Event Management (SIEM)
Security Operation Center

04

Praktische Umsetzung

Ausbaustufen der IT / OT Security

Die Basis Sicherheit ist ein Standard, der in den meisten Unternehmen etabliert ist.

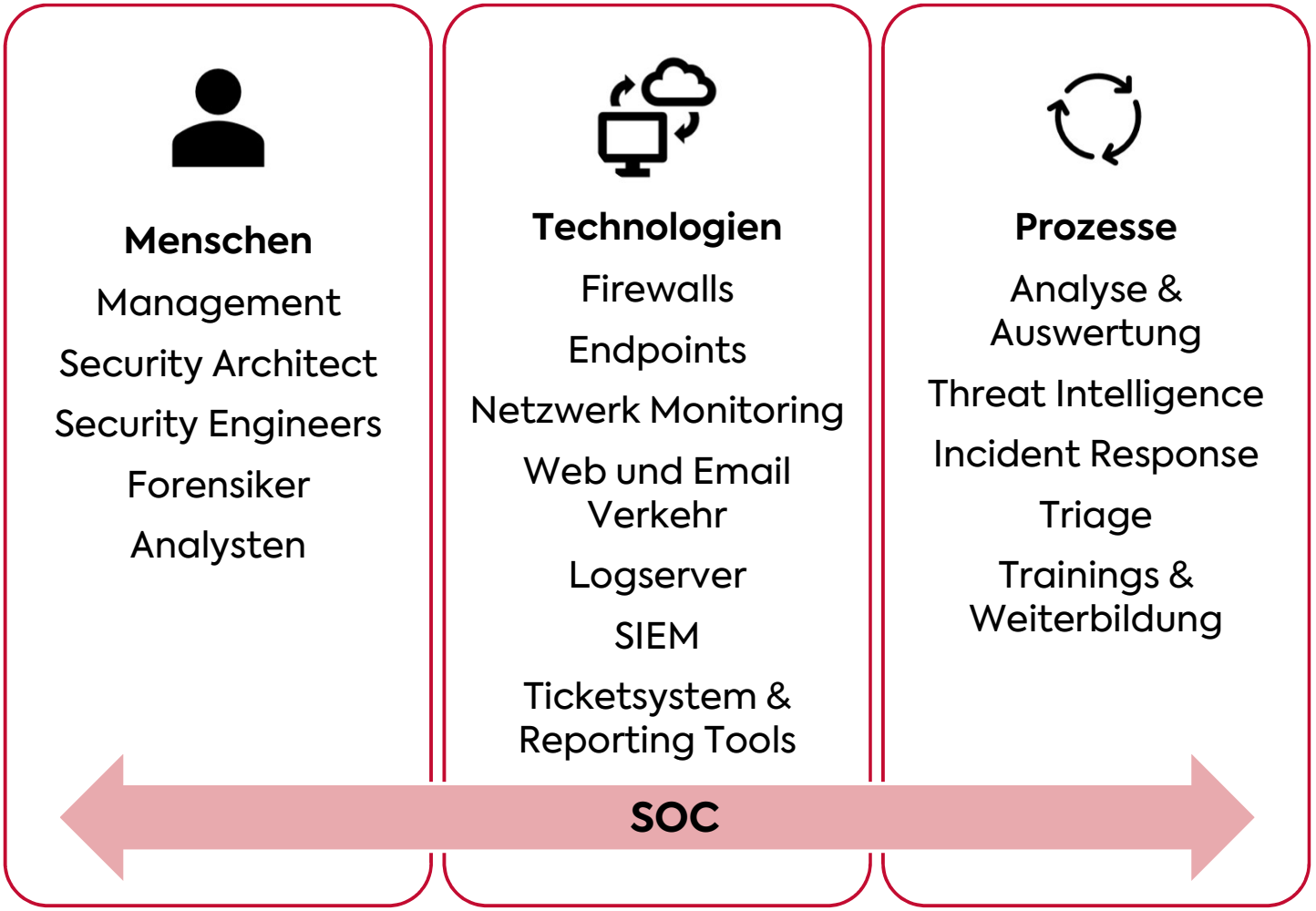
Basis Sicherheit
- Passwörter
- Active Directory
- Patch Management
- Backup Management
- Firewalls
- WAF / Proxy
- SPAM / WEB Filter
- ...

Prävention
- Endpoint Detection and Threat Response
- Extended Detection and Response
- Intrusion Detection Systeme
- Intrusion Prevention Systeme

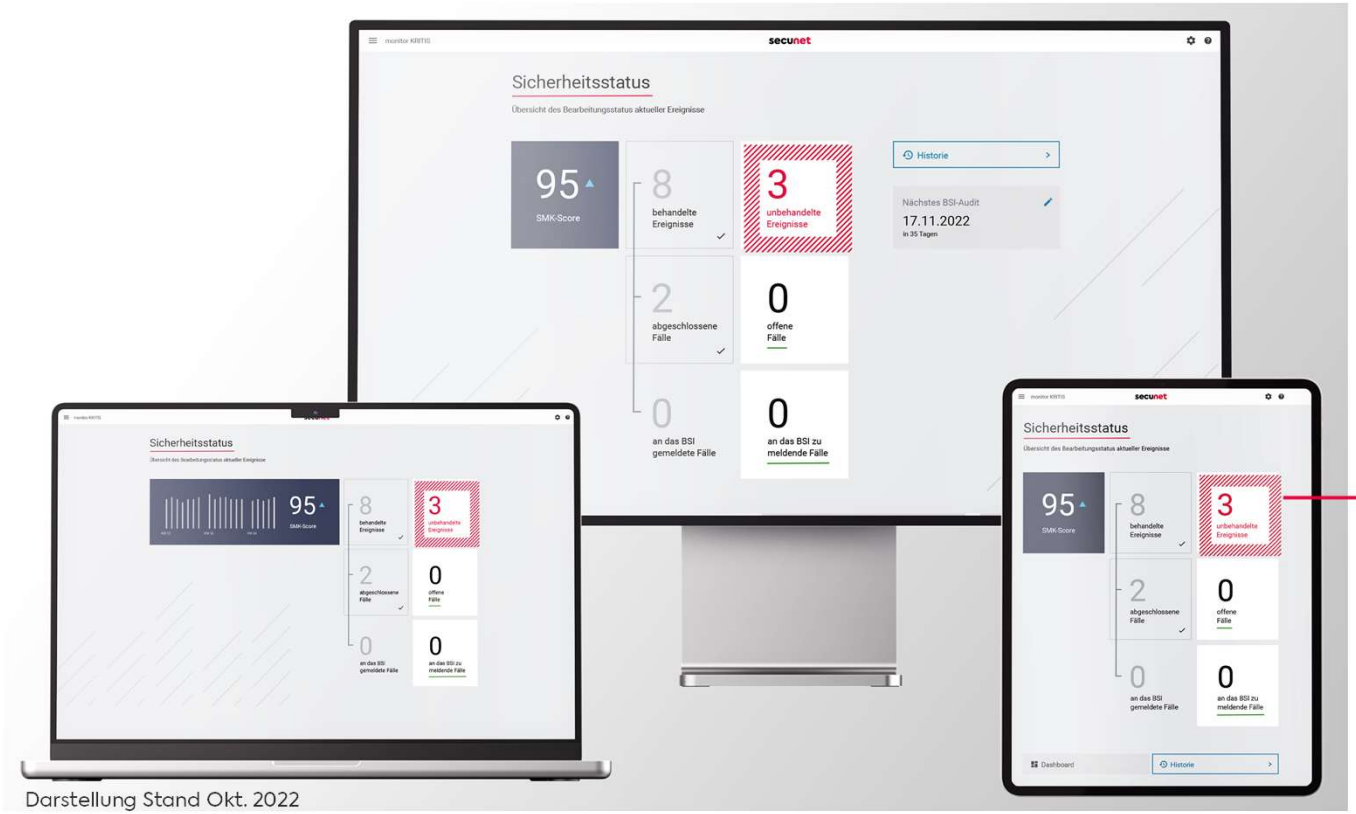
Security Operation Center (SOC)
- Aggregation, Korrelation von Logs
- Human / Threat Intelligence
- 24/7/365 Monitoring
- Incident Detection and Response
- Forensic

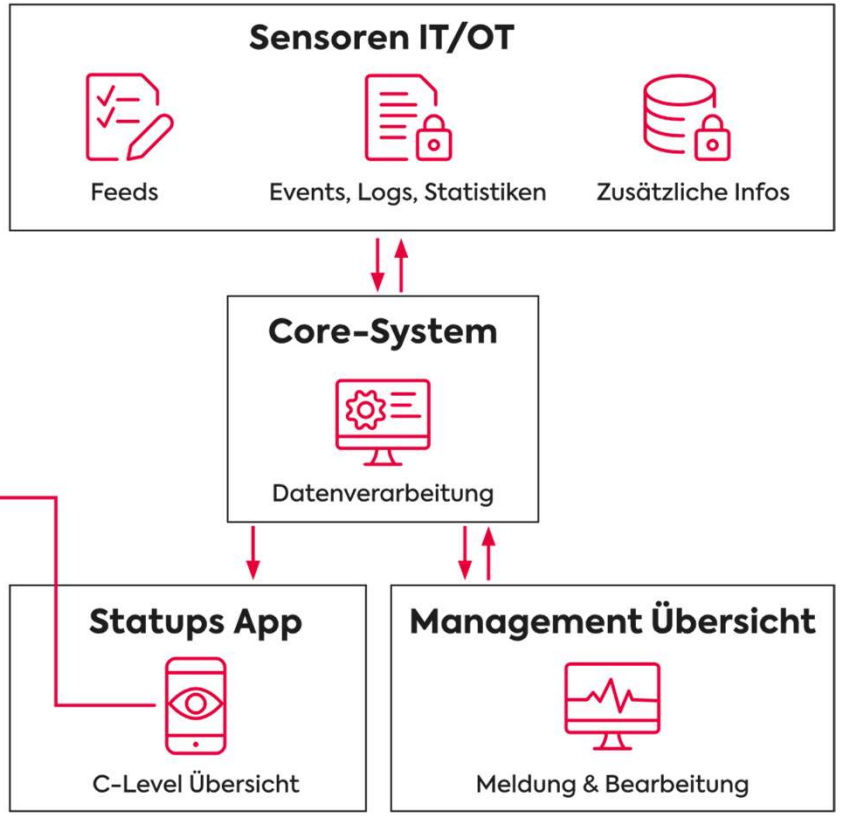
Den optimalen Schutz bietet ein Security Operation Center, welches rund um die Uhr für die Sicherheit der IT/OT verantwortlich ist.

Aufbau und Abhängigkeit eines SOC



secunet monitor KRITIS





Kontakt

Joachim Cappel

Principal Managementsysteme & Audits

secunet Security Networks AG

joachim.cappel@secunet.com

industry.vertrieb@secunet.com

it-sa 2022 in Nürnberg
Halle 7A Stand 526


secunet