secunet

**Beginn: 15:00 Uhr**

# KRITIS: Rechtskonforme Umsetzung der notwendigen Angriffserkennung

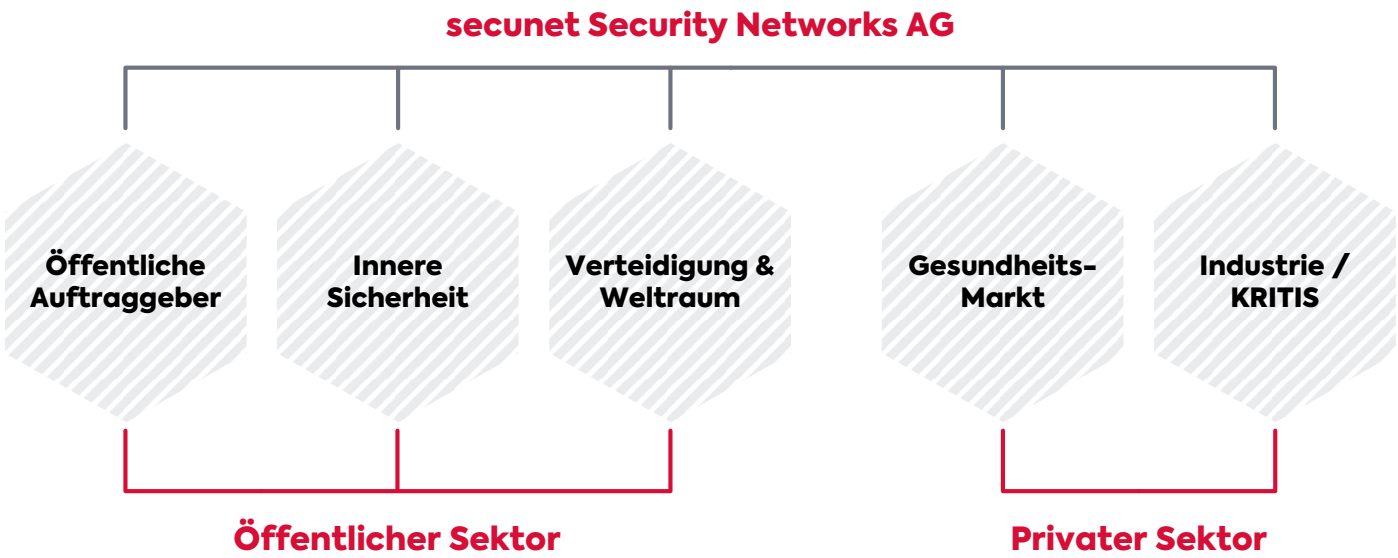
Yasmin Salloum

Benjamin Körner

Webinar, 21. September 2023

secunet Security Networks AG

# secunet auf einen Blick –
# 25 Jahre Kompetenz in IT-Security




- **> 1.000 Mitarbeiter**
- **12 Standorte**
- **347 Mio. Euro Konzernumsatz in 2022**
- **> 500 Kunden, u.a. Bundesministerien, EU und > 20 DAX-Konzerne**
- **Hauptaktionär: Giesecke + Devrient (75%)**

Sicherheitspartner der Bundesrepublik Deutschland

## Joint Venture

**SecuStack**

Cloud-Betriebssystem

## Tochtergesellschaften

**stashcat**

Sicherer Business-Messenger

**SysEleven**

Cloud & Managed Kubernetes

# Systeme zur Angriffserkennung – Projekt astora

**Die Kunden-Herausforderung:**

kurze Umsetzungszeit (September 2022 – Mai 2023)

**Das Projekt-Ziel:**

Umsetzung der Einzelanforderungen gemäß der BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

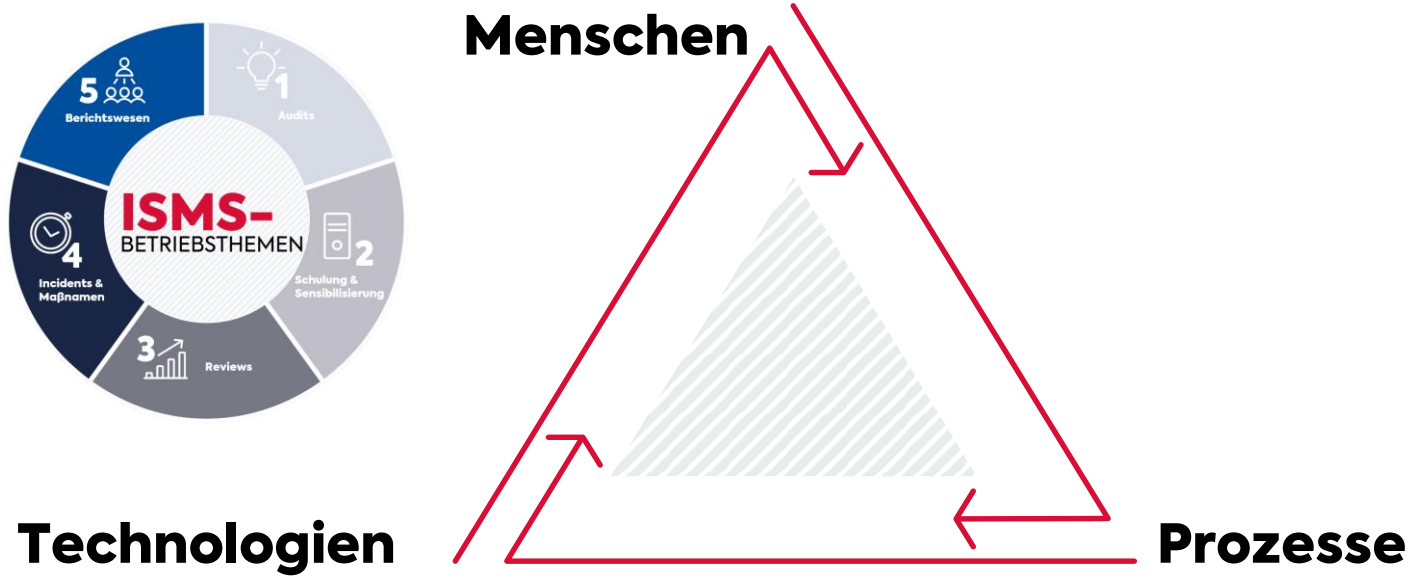
**Die Vorgehensweise:**

- Ermittlung der Anforderungen mit Handlungsbedarf (technisch und organisatorisch)
- Erstellung Projektplan
- Unterstützung bei der benötigten Dokumentation

# Was sind Systeme zur Angriffserkennung?

„Systeme zur Angriffserkennung (...) sind durch **technische Werkzeuge** und **organisatorische Einbindung** unterstützte **Prozesse** zur Erkennung von Angriffen auf informationstechnische Systeme.“ (IT-SiG 2.0 § 9b)

„Die eingesetzten Systeme zur Angriffserkennung müssen geeignete **Parameter** und **Merkmale** aus dem laufenden Betrieb **kontinuierlich** und **automatisch** erfassen und **auswerten**. Sie sollten dazu in der Lage sein, fortwährend **Bedrohungen** zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete **Beseitigungsmaßnahmen** vorzusehen.“ (§8a Absatz 1a BSIG)



# Wann müssen Unternehmen nachweisen?

## Bis zu welchem Zeitpunkt müssen Betreiber, die nach dem EnWG reguliert sind, den Einsatz von Systemen zur Angriffserkennung nachweisen?

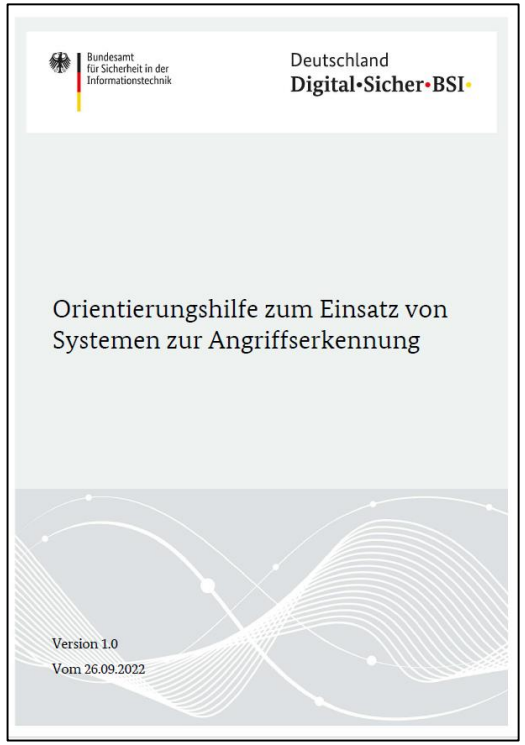
Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur gelten, haben gemäß § 11 Absatz 1f EnWG dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach § 11 Absatz 1e EnWG nachzuweisen.

## Wann müssen Betreiber, die nach BSIG reguliert sind, den Einsatz von Systemen zur Angriffserkennung nachweisen?

Nach dem BSIG regulierte Betreiber müssen dem BSI alle zwei Jahre ihre Nachweise gemäß § 8a Absatz 3 BSIG einreichen. Nachweise, die dem BSI ab dem 1. Mai 2023 vorgelegt werden, müssen auch Aussagen zur Umsetzung des Absatzes 1a, also zum Einsatz von Angriffserkennungssystemen, enthalten.

# Was ist die Orientierungshilfe?

- MUSS-, KANN- und SOLL-Anforderungen
  - Protokollierung
  - Detektion
  - Reaktion




» Die Orientierungshilfe kann als Hilfestellung zur Umsetzung der Anforderungen bezüglich der Angriffserkennung verstanden werden und ist für Auditoren die maßgebliche Grundlage in ihrer Beurteilung während eines Audits.

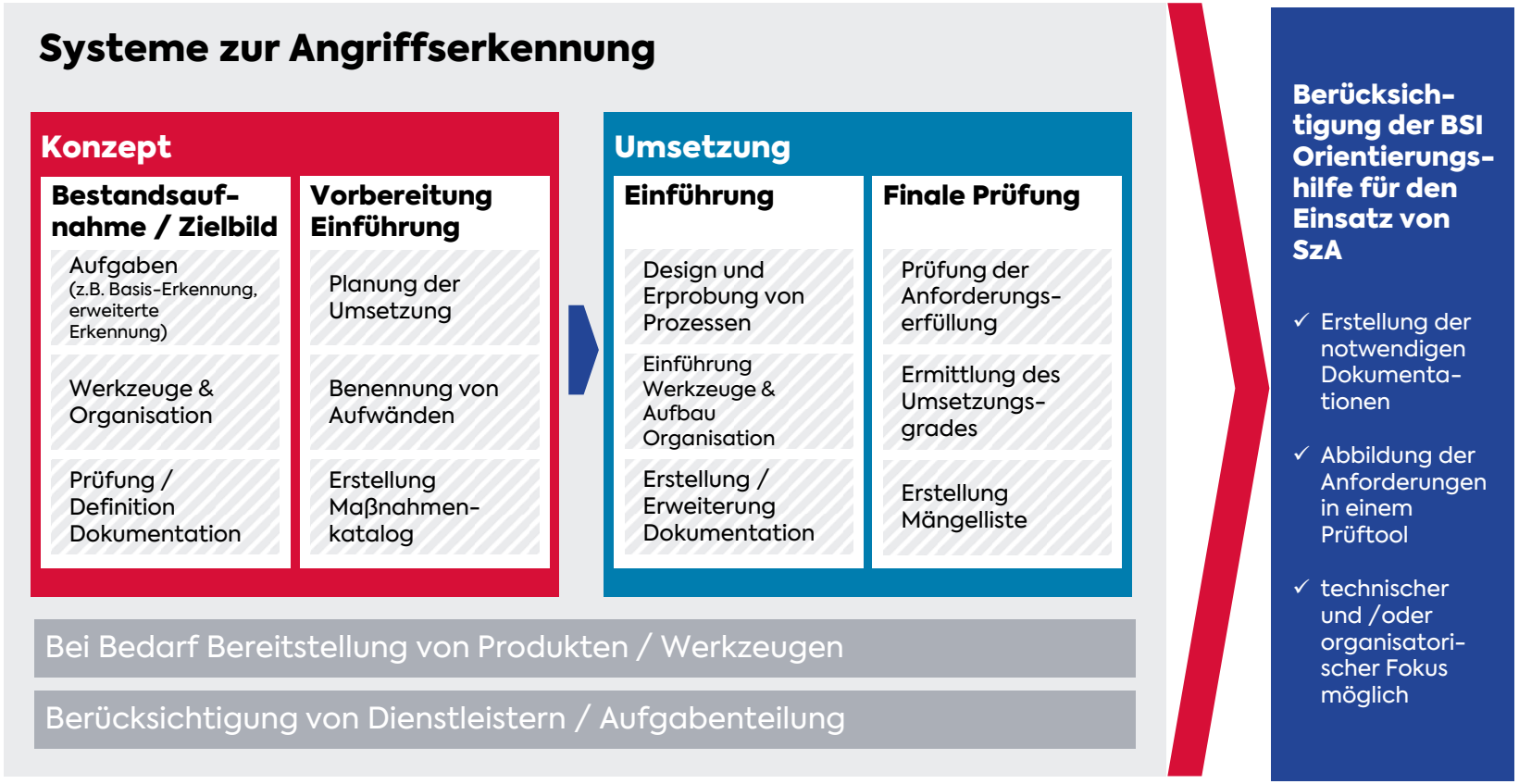
# Auszug Anforderungen OhSzA

- Der Betreiber MUSS alle zur **wirksamen Angriffserkennung** auf **System- bzw. Netzebene** notwendigen Protokoll- und Protokollierungsdaten [...] **erheben, speichern** und für die **Auswertung** bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.
- Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe **dokumentiert** werden, welche Ereignisse dieses bzw. diese **protokolliert**.
- Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich **zentralen Stellen gespeichert** werden.
- Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN **gefiltert, normalisiert, aggregiert und korreliert** werden.
- Alle Protokoll- und Protokollierungsdaten MÜSSEN **kontinuierlich überwacht und ausgewertet** werden.
- Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach **fachlicher Bewertung** und innerhalb einer der **Risikoanalyse entsprechend geringen Zeitspanne** eine qualifizierte und dem Bedarf entsprechende **Reaktion** eingeleitet wird.

# Das Umsetzungsgradmodell

| | |
|---|---|
| 0 | Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen. |
| 1 | Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen. |
| 2 | In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen erfüllt worden. |
| 3 Initiale Phase | Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung. |
| 4 Ausbau-Phase | Alle MUSS- Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert. |
| 5 | Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert. |

# Unser Vorgehensmodell



# Angriffserkennung durch Muster/Signaturen

**… im Netzwerk**

**… in Log- und Protokollierungsdaten**

# Wie erfolgt die Mustererkennung im Netzwerk?

# … und warum genau dort?

# Wissen Sie, was gerade in Ihrem Netzwerk passiert?

## Angriffe frühzeitig erkennen

Hier bemerken Sie den Angriff **ohne SzA**

**Unsichere Systeme finden und übernehmen**


**Durch Benutzer-interaktion:**
Phishing E-Mail
USB Stick
Social Engineering

Hier bemerken Sie den Angriff **mit SzA**

**Alles, was Sie erpressbar macht:**
Kundendaten
Geschäftsemails
Personaldaten
Produktionsgeheimnisse

**Mit Drohung Druck aufbauen:**
Sensible Daten veröffentlichen
Produktion dauerhaft stilllegen

# Wie erfolgt die Mustererkennung im Netzwerk?

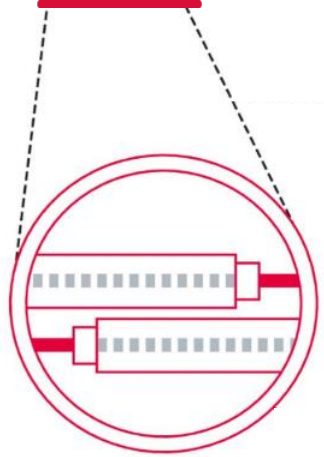
Kennt alle Signaturlisten von bekannten Angriffen (Feeds)

Muster erkannt:

Ereignis wird erzeugt !

Signaturbasierte Netzwerk-Events

Angreifendes System



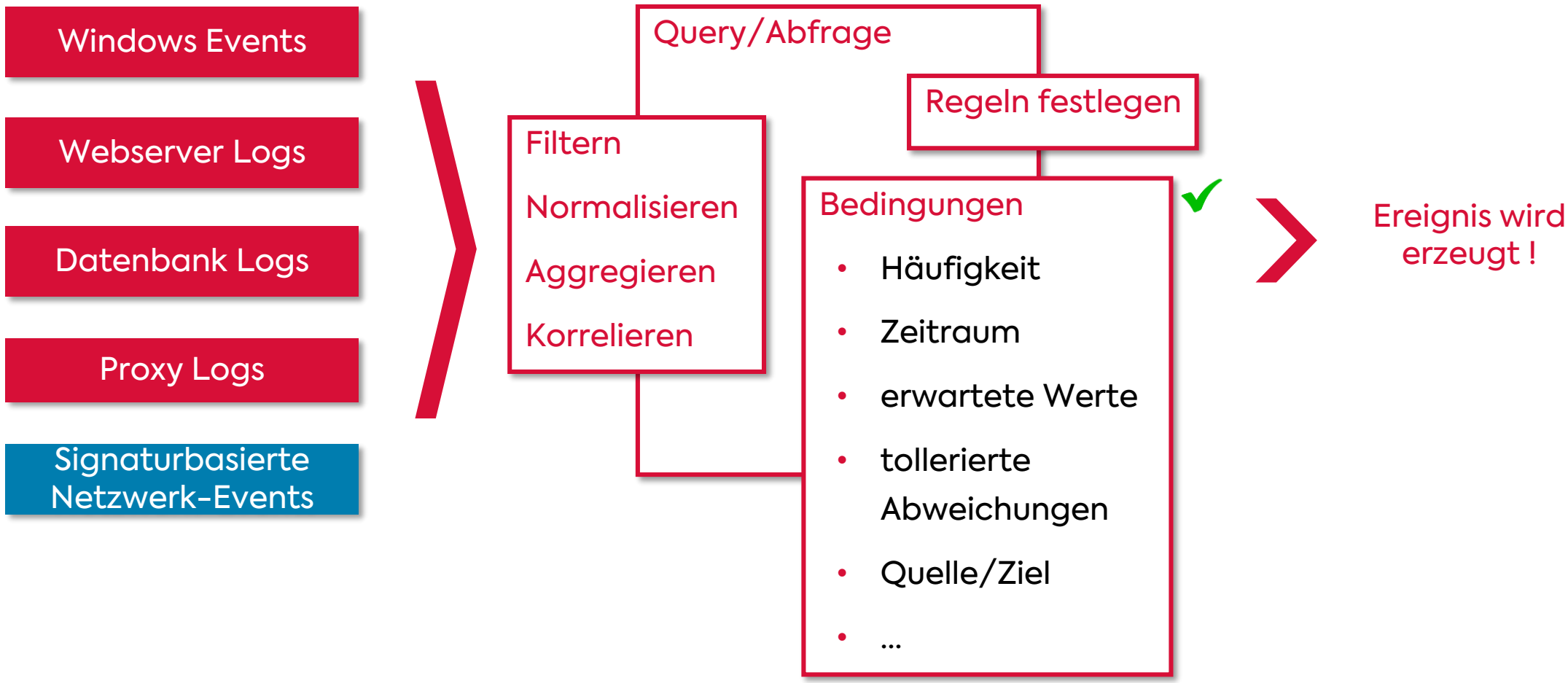
Abgleich des Netzwerktraffics auf diese bekannten Muster

Sämtliche Netzwerkgeräte

# Wie erfolgt die Angriffserkennung auf Basis der

# Log- oder Protokollierungsdaten ?

# Mustererkennung in Log- oder Protokollierungsdaten



# Bewertung von Ereignissen

- Was beinhaltet ein Ereignis für Informationen?

IP Adressen | Ports | Protokolle

MAC-Adressen | Systemzustände

Regelverstöße | Webzugriffe | ...

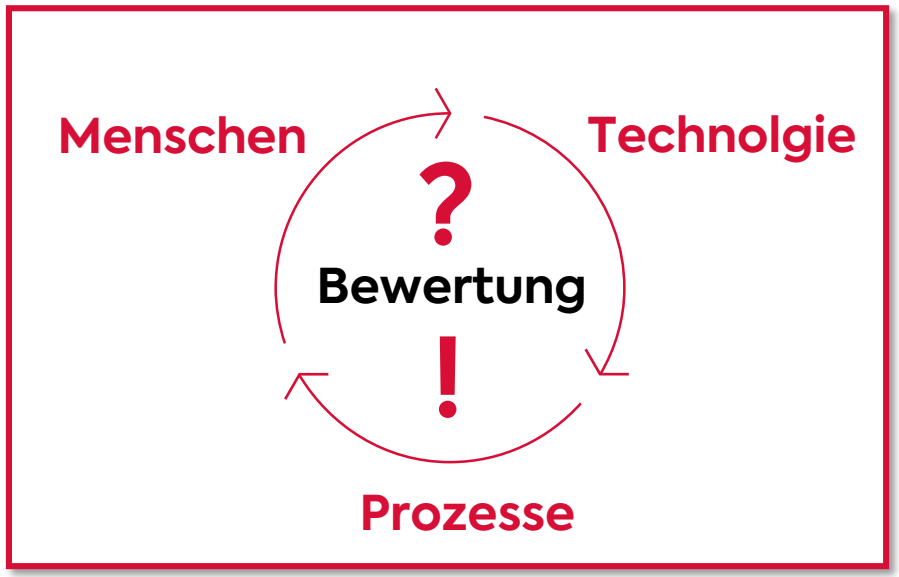
- Was ist ein Sicherheitsvorfall (QSE)?
  - Unerwünschtes Ereignis
- Folgen:
  - Ausspähen
  - Manipulation
  - Zerstörung
- **Ausfall und Beeinträchtigung von Kritischen Infrastrukturen**

- Was ist ein sicherheitsrelevantes Ereignis (SRE) ?
  - Wirkt sich auf die Informationssicherheit aus.
  - Beeinträchtigt die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit eines Systems.

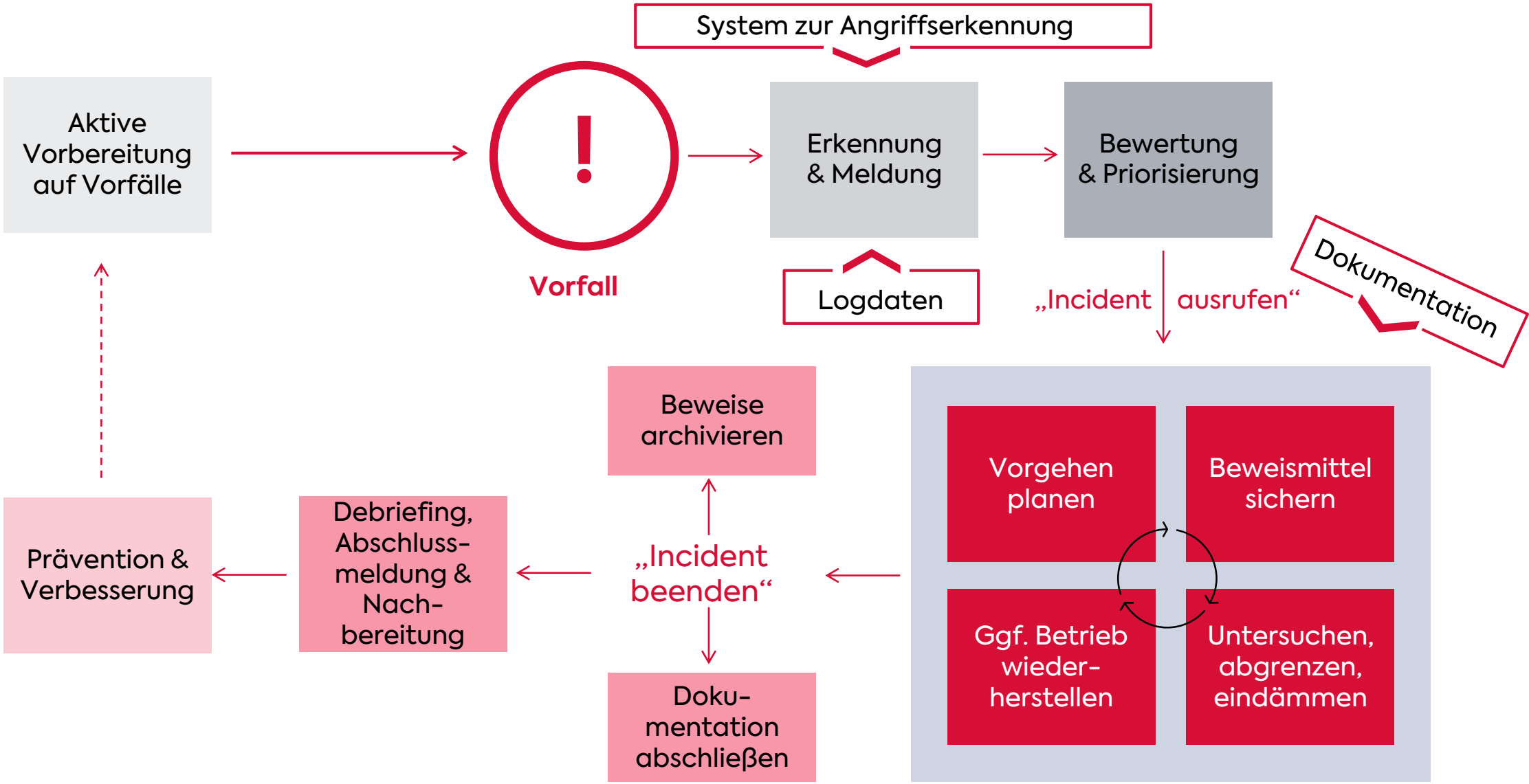
**Fehlgeschlagene Anmeldevorgänge**

**Detektion einer Schadsoftware**

**Missachtung einer Sicherheitsregel**



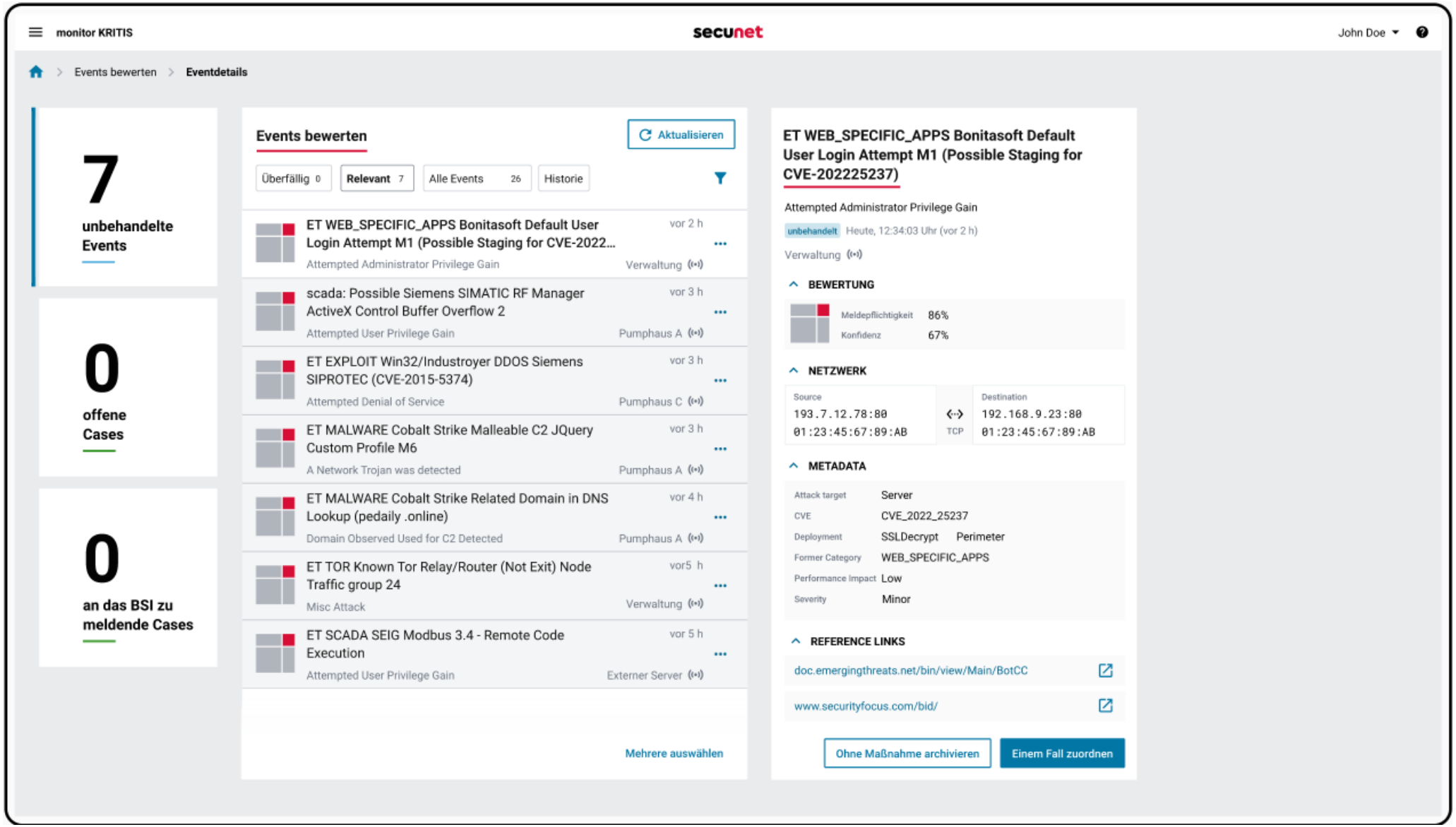
# Generischer Ablauf einer Vorfallbehandlung



secunet
monitor KRITIS

# Die einfache Lösung zur Angriffserkennung optimiert für KRITIS-Betreiber

- ✓ Umsetzung aller technischen MUSS-Anforderungen der Orientierungshilfe zur Erfüllung des IT-SiG 2.0
- ✓ Signaturbasierte Netzwerkangriffserkennung
- ✓ Logdatensenke für Protokollierungsdaten
- ✓ Optimiert für MSS/SOCs sowie für die Selbstverwaltung
- ✓ Unterstützt Meldungen von Sicherheitsvorfällen an das BSI
- ✓ Passives und rückwirkungsfreies System für IT & OT
- ✓ Übersichtliches Changelog zur sicheren Dokumentation
- ✓ Installationsfähig in Airgapped-Umgebungen
- ✓ Flexibel, unkompliziert und kosteneffizient


monitor KRITIS
secunet
John Doe
Events bewerten > Eventdetails
7
unbehandelte Events
0
offene Cases
0
an das BSI zu meldende Cases
Events bewerten
Aktualisieren
Überfällig 0
Relevant 7
Alle Events 26
Historie
ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022... vor 2 h
Attempted Administrator Privilege Gain Verwaltung
scada: Possible Siemens SIMATIC RF Manager ActiveX Control Buffer Overflow 2 vor 3 h
Attempted User Privilege Gain Pumphaus A
ET EXPLOIT Win32/Industroyer DDOS Siemens SIPROTEC (CVE-2015-5374) vor 3 h
Attempted Denial of Service Pumphaus C
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M6 vor 3 h
A Network Trojan was detected Pumphaus A
ET MALWARE Cobalt Strike Related Domain in DNS Lookup (pedaily .online) vor 4 h
Domain Observed Used for C2 Detected Pumphaus A
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 24 vor5 h
Misc Attack Verwaltung
ET SCADA SEIG Modbus 3.4 - Remote Code Execution vor 5 h
Attempted User Privilege Gain Externer Server
Mehrere auswählen
ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-202225237)
Attempted Administrator Privilege Gain
unbehandelt Heute, 12:34:03 Uhr (vor 2 h)
Verwaltung
BEWERTUNG
Meldepflichtigkeit 86%
Konfidenz 67%
NETZWERK
Source 193.7.12.78:80 01:23:45:67:89:AB
TCP
Destination 192.168.9.23:80 01:23:45:67:89:AB
METADATA
Attack target Server
CVE CVE_2022_25237
Deployment SSLDecrypt Perimeter
Former Category WEB_SPECIFIC_APPS
Performance Impact Low
Severity Minor
REFERENCE LINKS
doc.emergingthreats.net/bin/view/Main/BotCC
www.securityfocus.com/bid/
Ohne Maßnahme archivieren
Einem Fall zuordnen

# Save The Date – unsere Industrial Security Events

- **it-sa 2023**

  10.-12. Oktober, Messe Nürnberg, Halle 7A, Stand 611
- **Webinar: Sichere Kollaborations-Tools für die Industrie**

  16. Oktober, 15:00 – 16:00 Uhr
- **Webinar / Live Demo: secunet monitor KRITIS**

  19. Oktober, 15:00 – 15:30 Uhr
- **Webinar: Sichere Vernetzung von Maschinen und Anlagen**

  24. Oktober, 9:30 – 10:30 Uhr
- **Webinar: NIS-2 Richtlinie – Maßnahmen und Strategien für Industrieunternehmen**

  7. November, 11:00 – 12:00 Uhr

**Informationen und Anmeldung unter:**
**www.secunet.com/industrie**

# Kontakt Referenten

**Yasmin Salloum**

Beraterin

Management Systeme und Audit

secunet Security Networks AG

yasmin.salloum@secunet.com

**Benjamin Körner**

Senior Solution Engineer

Customer Project Management

secunet Security Networks AG

benjamin.koerner@secunet.com

**Ivanka Stefanova-Achter**

Business Enablement Manager (Vertrieb)

secunet Security Networks AG

Telefon: 0201 – 5454 2767

ivanka.stefanova-achter@secunet.com


secunet