

# Die KRITIS-Lösung zur Angriffserkennung – gemäß IT-Sicherheitsgesetz

## § 8a Absatz 1a Satz 1 BSIG:

„Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung.“



### Ab wann?

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



### Was genau?

BSI veröffentlicht konkrete Anforderungen zur Angriffserkennung in der Orientierungshilfe.



### Wie erfolgt der Nachweis?

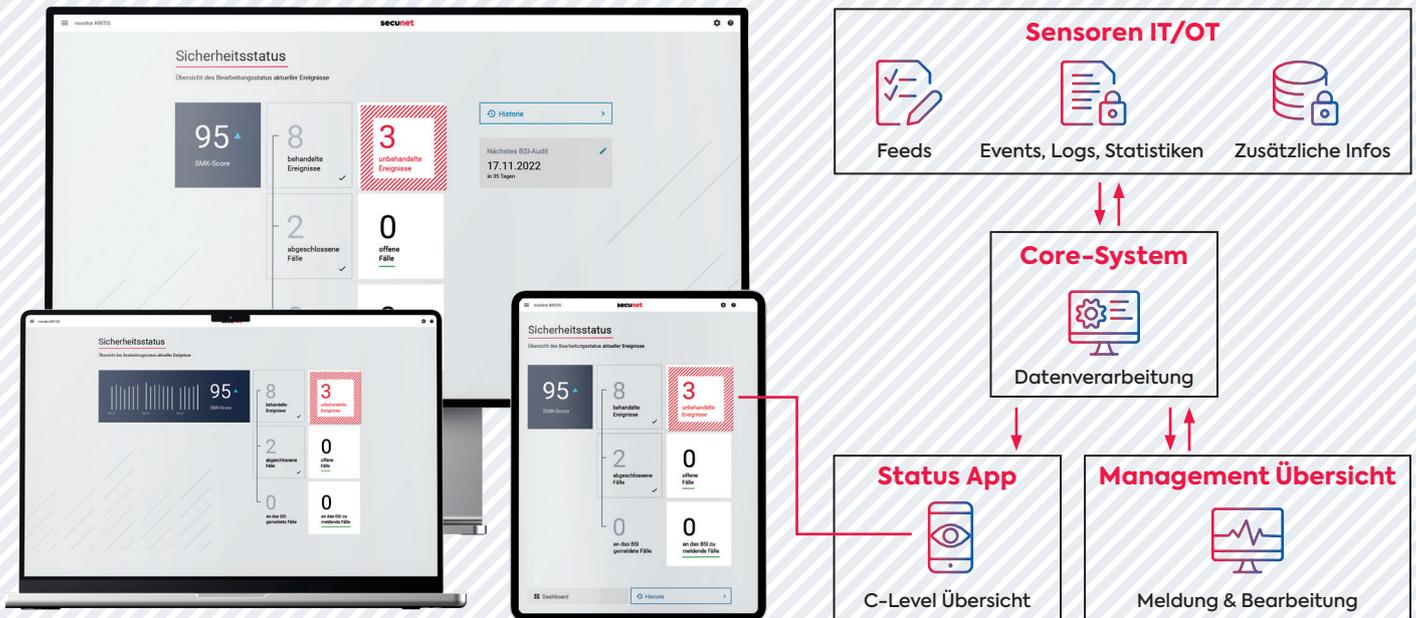
Für die Nachweiserbringung wird das BSI, analog zur etablierten Nachweiserbringung im Kontext des § 8a Absatz 3 und 1 BSIG, entsprechende Formulare veröffentlichen.

**secunet bietet die einfache, für KRITIS-Betreiber optimierte, Lösung zur Angriffserkennung**

**secunet**  
monitor KRITIS

**Unser Netzwerk-Monitoring-System auf Basis signaturbasierter Angriffserkennung:**

- MUSS-Anforderung laut BSI-Orientierungshilfe zum IT-Sicherheitsgesetz 2.0
- passives und rückwirkungsfreies System in IT & OT
- Anbindung des BSI IoC-Feeds für neue Signaturen und Vorbewertung der Events
- optimiert für BSI-Meldungen & BSI-Audits
- Updates für den Ausbau des Umsetzungsgrads (MUSS + KANN + SOLL)
- optimiert für Managed Security Services & SOCs



Darstellung Stand Okt. 2022

# secunet monitor KRITIS auf einen Blick

## Professionelle Beratung

Wir unterstützen KRITIS-Betreiber individuell & lösungsorientiert bei der Herstellung der Gesetzeskonformität; Beratung für „BSI-Audits“ (§8a BSIG)

## Flexible Integration

Schnelle Anpassungsfähigkeit; Optionale Anbindung an ein SIEM oder Übernahme der Logfunktionen durch die Lösung selbst; IT- & OT-Abdeckung

## Ressourcen- & Kosteneffizient

Reine Fokussierung auf die geforderten Elemente sowohl jetzt als auch in Zukunft

\*Orientierungshilfe – Systeme zur Angriffserkennung

## Zielgerichtetes Featureset:

Erfüllung der technischen Anforderungen (IT-SiG 2.0 & OH-SZA\*)

## Benutzerfreundlichkeit

Getrennte Status- & Management-Oberfläche mit intuitiver und komplexitätsreduzierter Handhabung; Ressourcensparende Bedienung und Verwaltung auch durch SI oder KMU

## Aktuelle Signaturen

Unter anderem Einbindung des BSI-IoC-Feeds zur Berücksichtigung aktueller Gefahren

## On Premises

Vollständige Integration und Betrieb der Sensoren und des Core-Systems auf Seite des Kunden (bei Fertigstellung der Lösung)

Hier Kontakt aufnehmen [info@secunet.com](mailto:info@secunet.com)

**secunet**