

# IT-SiG 2.0 – Angriffserkennung in KRITIS wird Pflicht

genua.



## Mit genua gesetzliche Vorgaben zur Cybersicherheit erfüllen

Mit dem IT-SiG 2.0 sind zahlreiche Änderungen im BSI-Gesetz in Kraft getreten und damit die Anforderungen an die Cybersicherheit verschärft worden: Gemäß § 8a Absatz 1a BSIG sind KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse verpflichtet, **ab dem 1. Mai 2023 ein System zur Angriffserkennung umzusetzen**. Mit cognitix Threat Defender bietet genua eine Lösung, mit der betroffene Organisationen dieser Verpflichtung nachkommen.

### Anforderungen an Systeme zur Angriffserkennung

Laut **BSI-Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung** basiert deren technische Funktionalität im Wesentlichen auf Abläufen, die sich drei Bereichen zuordnen lassen:

- Zum einen müssen die Systeme durch fortlaufende Auswertung der gesammelten Informationen (**Protokollierung**) sicherheitsrelevante Ereignisse erkennen (**Detektion**). Dies kann beispielsweise durch Missbrauchserkennung oder Anomalie-Erkennung erfolgen.
- Zum anderen sollten Systeme zur Angriffserkennung Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (**Reaktion**). Dies kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.



**cognitix Threat Defender:**  
Vollständige Kontrolle des Netzwerks,  
schnelle Anomalie-Erkennung und  
umfassende Risikobewertung

### cognitix Threat Defender erfüllt gesetzliche Vorgaben

genua bietet mit cognitix Threat Defender KRITIS-Betreibern ein intelligentes System zur Angriffserkennung nach aktuellem Stand der Technik. Die Lösung überwacht die Komponenten und Abläufe in Netzen, **detektiert** mit einer leistungsfähigen Echtzeit-Traffic-Erkennung abweichende Aktivitäten und **protokolliert** diese, **reagiert** automatisiert auf Störungen im Netzwerk und leitet die Behandlung von Sicherheitsvorfällen ein.

Damit erfüllt cognitix Threat Defender alle wesentlichen gesetzlichen Anforderungen an ein technisches System zur Angriffserkennung und erhöht gezielt die Netzwerksicherheit in kritischen Infrastrukturen.

Security  
made  
in  
Germany



## Jetzt cognitix Threat Defender zu Sonderkonditionen sichern!

Wir unterstützen Organisationen bei der Umsetzung der Anforderungen des § 8a Absatz 1a BSIG mit Sonderkonditionen für

### cognitix Threat Defender

System zur Angriffserkennungen gemäß BSI-Empfehlung: [www.genua.de/threat-defender](http://www.genua.de/threat-defender)

- Die Sonderkonditionen beinhalten **35 % Nachlass** auf sämtliche cognitix Threat Defender Listenpreis-Softwarepakete\*
- In Kombination mit bestehenden vertraglichen Ermäßigungen gewähren wir zusätzlich **20 % Nachlass** auf sämtliche cognitix Threat Defender Listenpreis-Softwarepakete\*
- Die Sonderkonditionen sind gültig für sämtliche Bestellungen **bis einschließlich 31. Mai 2023**

Gerne beraten wir Sie bei der Umsetzung der gesetzlichen organisatorischen Anforderungen mit unserem

### IT Security Assessment

Consulting-Angebot zur Einführung eines ISMS gemäß BSI-Empfehlung: [www.genua.de/consulting](http://www.genua.de/consulting)

**Sie möchten mehr erfahren?  
Nehmen Sie jetzt Kontakt zu uns auf!**

\* Angebot gilt nicht für VS-NfD-Systemlösungen mit genugate/genuscreen

## Technische und organisatorische Anforderungen, die Sie mit genua erfüllen

- Sie sind in der Lage, relevante Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch zu erfassen und auszuwerten
- Sie erhöhen die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit Ihrer informationstechnischen Systeme, Komponenten und Prozesse
- Sie stellen die frühzeitige Erkennung von Cyberangriffen sicher und unterstützen insbesondere die Schadensreduktion bzw. -vermeidung
- Sie erhalten Hinweise auf geeignete Beseitigungsmaßnahmen für eingetretene Störungen
- Das System zur Angriffserkennung bezieht alle maßgeblichen Systeme, Komponenten oder Prozesse ein wie z. B. IT, OT, Rechenzentren und Embedded Systems
- Die Qualität des eingesetzten Systems lässt sich anhand eines Umsetzungsgradmodells bewerten und damit der Fortschritt der organisatorischen und technischen Maßnahmen in der geprüften kritischen Infrastruktur beurteilen
- Sie können den Schutz Ihrer Informationssysteme gegenüber dem BSI nachweisen

## Reasons Why

- Experte für die IT-Sicherheit von Unternehmen und öffentlichen Organisationen
- Angebot eines umfangreichen, modularen IT-Security-Portfolios
- Kompromisslose Qualität bei allen Produkten, Dienstleistungen und Prozessen

## genua – Excellence in Digital Security

genua entwickelt innovative, zuverlässige sowie marktprägende Produkte und Lösungen. Ob im öffentlichen Sektor, bei Betreibern kritischer Infrastrukturen (KRITIS), in der Industrie oder im Geheimschutz: Wir liefern Antworten auf die IT-Security-Herausforderungen der Gegenwart und Zukunft.

### Interessiert?

**Hier erhalten Sie Beratung und ein Angebot:**  
T +49 89 991950-902 oder E [vertrieb@genua.de](mailto:vertrieb@genua.de)

### genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München  
T +49 89 991950-0 | E [info@genua.de](mailto:info@genua.de) | [www.genua.de](http://www.genua.de)

