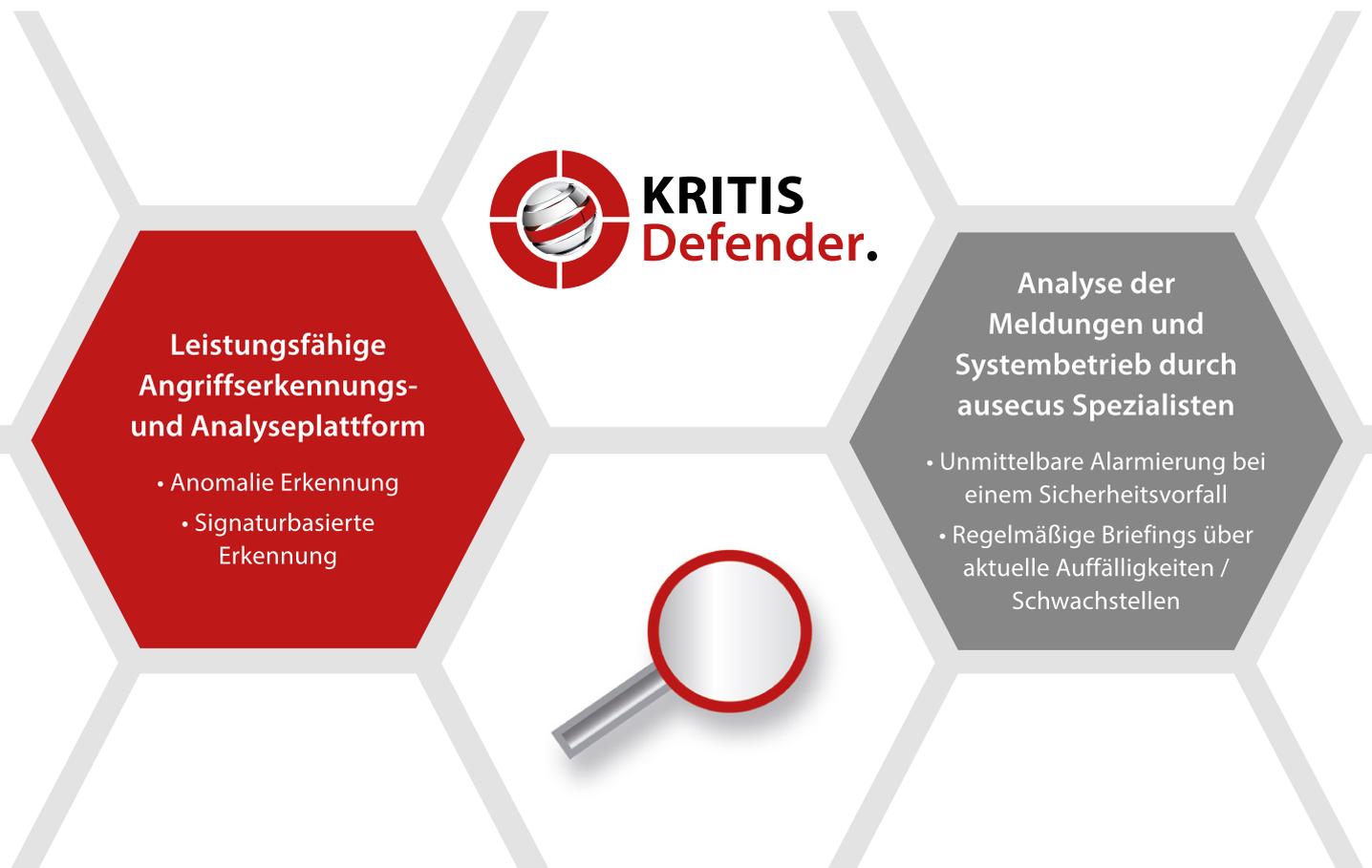


Angriffserkennungsservice KRITIS Defender

Angriffserkennung für Leit- und Fernwirktechnik von Kritischen Infrastrukturen als Dienstleistung.



- ✓ **Keine Investitionskosten**
Sie bezahlen die in Anspruch genommene Dienstleistung.
- ✓ **Kein zusätzliches Personal oder Know-How**
ausecus Spezialisten arbeiten für Sie.
- ✓ **Zugeschnitten auf die Leit- und Fernwirktechnik**
Kritischer Infrastrukturen der Sektoren Energie und Wasser



Kontakt

ausecus GmbH
Werner-von-Siemens-Str. 6
86159 Augsburg
Tel +49 821 207097-0
info@ausecus.com

KRITIS Defender Plattform

KRITIS Defender nutzt eine Hardware/ Softwareplattform, die von ausecus weiterentwickelt und bei Ihnen vor Ort betrieben wird.

Im Fokus: Schutz Ihrer Nutzdaten im Netzwerk

Die Erfassung der zu analysierenden Daten erfolgt rückwirkungsfrei. Dabei bleiben Ihre Daten immer in Ihrer Infrastruktur. Der Fernzugriff erfolgt mit sicheren Standardprotokollen (gem. BSI TR-02102-4) und ist an Ihre etablierten Verfahren anpassbar.

Erkennungsverfahren

Durch eine Vielzahl von aktuellen Detektionsverfahren für Office-IT und Leittechnik erreichen wir hohe Erkennungsraten bekannter und unbekannter Angriffe (Anomalien). Wir passen die Erkennungsverfahren ständig Ihren Gegebenheiten an, reduzieren Falsch-Positiv Meldungen und sorgen damit für einen effizienten Betrieb.



Die Erkennungsverfahren basieren u.a. auf:

- ▶ Anlagenspezifischen Betriebsverfahren und Protokolle (z. B. IEC 104)
- ▶ Umfangreiche, internationale Suricata Angriffssignaturdatenbank
- ▶ BSI KRITIS Cyber-Security Warnungen, Lageberichten & Vorfallmeldungen
- ▶ Cyber-Allianz-Zentrum Bayern (CAZ) des Bayerischen LfV
- ▶ Schwachstellen der Leittechnik & Leittechnikprotokolle

Open Source Software

Weltweit etablierte Open Source Softwaresysteme bieten kontinuierliche Innovation, hohes Sicherheitsniveau und Kosteneffizienz.



Betriebssystem



Intrusion Detection
Engine



Daten-Analyse



ANSIBLE

Automatisierung

Standard Industrie-Hardware

- ✓ Individuelle Hardwareplattformen je nach Leistungsbedarf
- ✓ Wir übernehmen die komplette Entstörung bis hin zum Hardwareaustausch

