SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

KRITIS Defender.

Technisches Datenblatt

KRITIS Defender – Das Intrusion Detection System für Kritische Infrastrukturen

SPEZIFIKATIONEN	
Intrusion Detection Engine	Suricata
Kapazität	2 TB HDD für ca. 8 Wochen Netzwerklogs bei durchschnittlicher Auslastung
Monitoring NICs	**RJ45** 3 x 1000 MBit/s Erweiterbar auf 5 x 1000 MBit/s **SFP** auf Anfrage

DETEKTIONSMECHANISMEN	
Protokolle	• Detektion aller standardmäßigen Netzwerkprotokolle wie u.a. SMB, HTTP/S, DNS, FTP, ICMP, LDAP/S • Detektion von Automatisierungs- und Leittechnikprotokollen wie u.a. IEC-104, Modbus/TCP, Ethernet/IP
Mechanismen	• Erkennung von Anomalien in Netzwerkdaten • Erkennung bisher unbekannter Angriffe und Sicherheitsprobleme • Erkennung von bekannten Angriffen • Alarmierung bei Kommunikation mit Schad-Software-Servern
Indikatoren für Ereignisse	• ausecus Threat Intelligence: Proaktive Erkennung von Angriffen in Kritischen Infrastrukturen • Aus BSI-Meldungen, ICS-CERT Advisories, SCADA- und leitsystemspezifischen CVEs abgeleitete Indikatoren (IOCs) • Suricata, Emerging Threats

IT-SICHERHEIT	
Security Features	• Gehärtetes Linux • Sicheres User-Management • Sicherheitsgetestete Anwendung (Produkt-Pentests) • Code Reviews • Revisionssichere Dokumentation
Fernwartung	Hochsichere Reverse-SSH Verbindung nach Stand der Technik gemäß BSI TR-02102-4