genua.

IT-SiG 2.0: Direkter Schutz für KRITIS-Organisationen

cognitix Threat Defender entdeckt in Echtzeit meldepflichtige Cyberattacken

Interne Netzwerksicherheit
Schnelle Anomalieerkennung
und umfassende Risikobewertung

Secur|Ty
made
in
Germany

Verteidigen Sie Ihre IT-/OT-Netze mit AI, Data Analytics und Threat Intelligence

Das IT-Sicherheitsgesetz (IT-SiG) verpflichtet Betreiber kritischer Infrastrukturen (KRITIS), außergewöhnliche IT-Störungen an das Bundesamt für Sicherheit in der Informationstechnik zu melden, die zu einem Versorgungsausfall geführt haben – oder zu einem solchen Szenario führen könnten.

cognitix Threat Defender

Fortschrittliche Schutzmaßnahmen zur Abwehr von Cyberattacken

Voraussichtlich dieses Frühjahr soll das IT-SiG 2.0 verabschiedet werden, das die Anomalieerkennung für KRITIS-Unternehmen und Organisationen gesetzlich verankert. Diese müssen innerhalb eines Jahres Vorkehrungen zur Abwehr von Cyberattacken treffen, indem sie Systeme zur Angriffserkennung einsetzen, die

- geeignete Parameter aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten;
- Bedrohungen identifizieren, vermeiden und geeignete Maßnahmen für eingetretene Störungen vorsehen.

Außergewöhnliche IT-Störungen erfordern ebensolche Schutzmaßnahmen – die Leistungen von Standard-Virenscannern oder Firewalls greifen hier zu kurz. cognitix Threat Defender von genua führt moderne Technologien mit Funktionen wie Netzwerkanalyse, Asset Tracking, Deep Packet Inspection sowie einer dynamischen Policy Engine in einem System zusammen.

Alle Vorteile auf einen Blick

Erkennt LAN-Anomalien und Angriffsmuster

Moderner Netzwerkschutz mit AI

Komplette Kontrolle über Netzwerkverkehr

Basis für Security Defined Networking

Vielseitig anwendbar in IT und OT

Monitoring mit Drilldown-Reporting

Hier erhalten Sie mehr Informationen und Beratung:

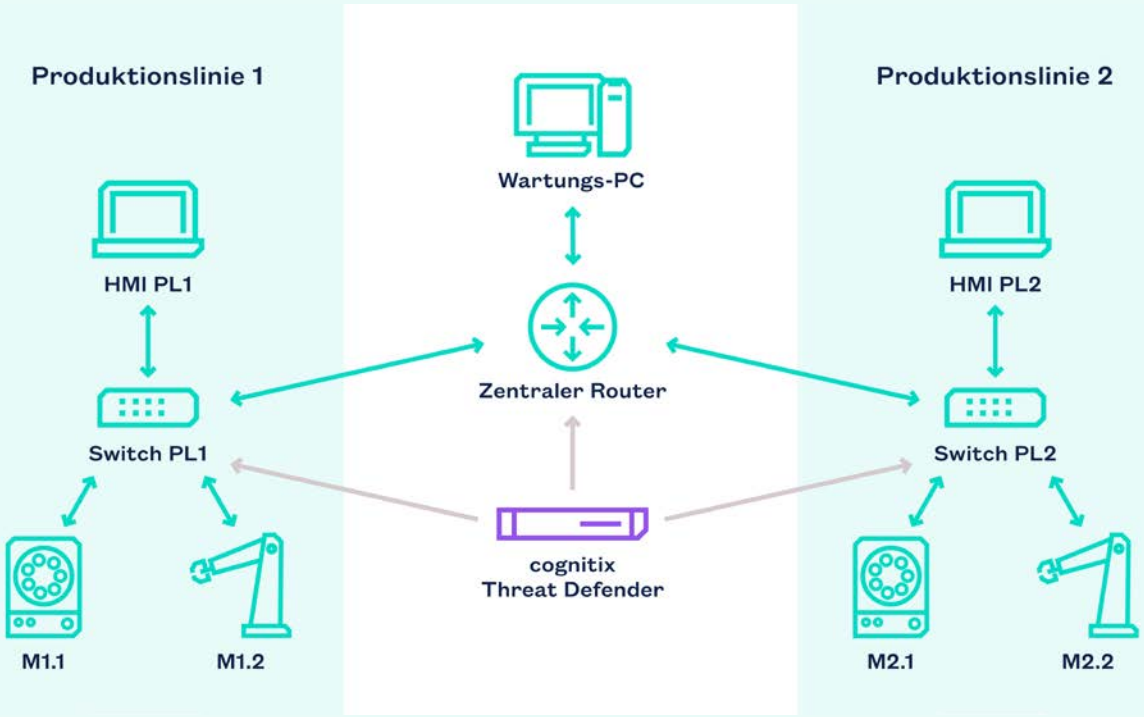
www.genua.de/threat-defender

Komplette Kontrolle des Netzverkehrs

cognitix Threat Defender analysiert den Netzwerkverkehr nach IP- und MAC-Adressen, Ports, Protokollen und Anwendungen der OSI-Schichten 2 bis 7. Dabei überprüft er den Traffic auf problematische Adressen, Domains oder Dateisignaturen. Zusätzlich werden auf Basis der Asset-Datenbank die Kommunikationsbeziehungen der Geräte untersucht. Den Geräten werden Verhaltensregeln zugeordnet und diese überwacht.

Anomalieerkennung in Echtzeit

Mit der automatischen Detektion des Netzwerkverkehrs erkennen Sie ungewöhnliche und vom üblichen Standardverhalten abweichende Muster (Anomalien) im Datenstrom und können somit Angriffe auf Ihre Netze frühzeitig abwehren.



Einfache, flexible Integration in Produktionsnetzwerke

» Da steckt sehr viel Intelligenz im System. Wir haben ohne zusätzlichen manuellen Aufwand eine permanente 24/7-Überwachung des Netzwerk-Traffics. Unser Netzbetrieb ist gegenüber immer komplexeren Angriffen nochmals ein gutes Stück sicherer geworden.

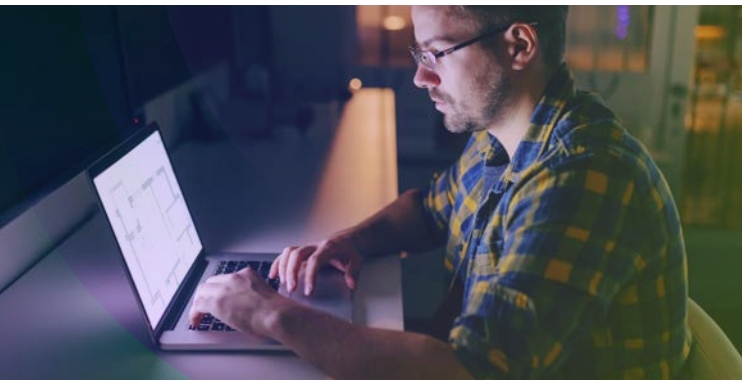
Carsten Viell,
IT-Leiter, Stadtwerke Bad Reichenhall

Monitoring mit Drilldown Reporting

Identifizieren Sie Bedrohungen über ein klares Monitoring mit aussagekräftigen Diagrammen und intuitiven Dashboards. Das interaktive Echtzeit-Reporting reicht vom Gesamtbild des Netzwerkverkehrs bis hin zu individuellen Benutzer- und Anwendungsdetails. Ein Echtzeitreporting mit einem Ampelsystem meldet mögliche Gefahren und Angriffe.

Zusätzliche Verteidigungslinie

Mit AI-, Data-Analytics- und Threat-Intelligence-Funktionen baut cognitix Threat Defender eine zweite Verteidigungslinie hinter der Perimeter Firewall im Netzwerk auf. So ergänzen Sie Ihre Firewall-Lösungen, die den Datenverkehr an den Schnittstellen kontrollieren und sichern, mit zukunftsweisender Technologie.



Anomalien in Echtzeit erkennen und Angriffe abwehren

Asset Tracking: Management von Geräten

cognitix Threat Defender erkennt und verwaltet alle in Ihrem Netzwerk vorhandenen Geräte mittels IP- und MAC-Adresse. Die dazu ermittelten Informationen werden um spezifische Metadaten ergänzt. So erstellen Sie einfach und schnell Sicherheitsrichtlinien für einzelne Geräte und deren Einsatzzweck.

Dynamische Netzwerksegmentierung mit AI und Data Analytics

Mit Hilfe von Artificial Intelligence und Data Analytics gruppiert cognitix Threat Defender Netzwerkteilnehmer verhaltensabhängig in dynamischen Netzwerkobjekten. Er reagiert automatisch auf verändertes oder unerwünschtes Verhalten und kann auffälligen Netzwerkteilnehmern bei Anomalieerkennung den Zugang zu bestimmten Ressourcen entziehen – ohne manuelles Eingreifen.

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? Kontaktieren Sie uns:
vertrieb@genua.de oder +49 89 991950-902

Mehr Produktinfos

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München,
T +49 89 991950-0, info@genua.de, www.genua.de