OPSWAT.

DATENBLATT

Neuralyzer™

OT-Cybersicherheit neu überdenken

Die Sichtbarkeit in OT-Umgebungen ist weiterhin eine große Herausforderung und ein Risikofaktor für Organisationen. OT-Umgebungen sind von Natur aus heterogen und bestehen nicht selten aus jahrzehntealten Geräten verschiedener Hersteller. Ein vollständiger Einblick in die Anlagen und die Vorgänge im Netzwerk ist ein wesentlicher Faktor bei allen effektiven OT-Cybersicherheitsprogrammen.

Unser Angebot

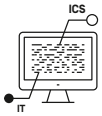
Neuralyzer befasst sich mit Gefahren für OT-Systeme, die sowohl von traditionellen IT- als auch von spezifischen ICS-Bedrohungen ausgehen. Es ist extrem einfach zu implementieren und dank der OT-nativen Benutzeroberflächen leicht zu bedienen. Das Arbeiten mit Neuralyzer erfordert kein besonderes Fachwissen oder Schulungen.

Neuralyzer bietet einen unerreichten Einblick in konvergierte IT/OT-Abläufe und liefert ein vertieftes Situationsbewusstsein für Bedrohungen im gesamten Netzwerk.

Es trägt zum Schutz Ihrer kritischen Ressourcen bei, indem es die Transparenz, Sicherheit und Kontrolle in Ihrem gesamten Betrieb maximiert und die Einhaltung regulatorischer Auflagen gewährleistet.

Neuralyzer setzt KI-Technologie wirksam ein, um Erkenntnisse über die einzigartigen Eigenschaften und Anforderungen von OT-Umgebungen zu gewinnen.

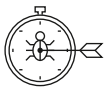
Vorteile



Deckt sowohl IT-Bedrohungen als auch spezifische ICS-Bedrohungen für OT-Systeme ab

Einfache Anwendung und für OT-Personal entwickelt

Bietet umfassende Transparenz und Managementinformationen zu ICS-Anlagen



Informiert Sie rechtzeitig und genau über alle Bedrohungen oder Anomalien im Netzwerk

Unterstützt regulatorische Auflagen mit umfassenden und objektiven Risikobewertungen

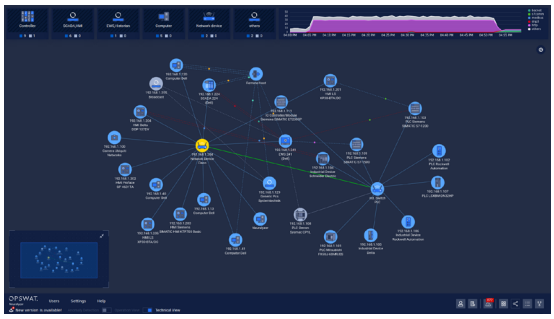
Bietet eine vereinheitlichte Sicht von Betrieb, Sicherheit und Compliance in einem einzigen Fenster

OPSWAT.

Neuralyzer

ANWENDUNGSFÄLLE

- Bestandsaufnahme der Anlagen und Schwachstellenanalyse
- Netzwerkvisualisierung und -überwachung
- Erkennung von und Reaktion auf Bedrohungen
- Gefährdungsbeurteilung und Alarmierungs-Workflow

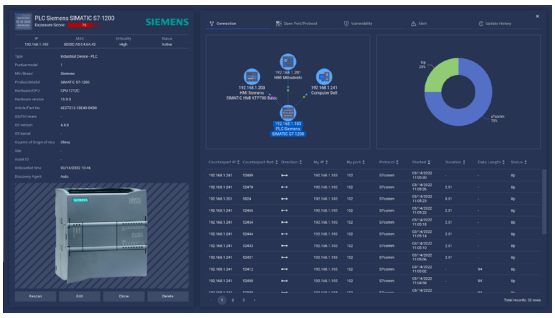


KI-BASIERTE ECHTZEIT-ANALYSE-ENGINE

- Erkennung von Verhaltensanomalien
- Erkennung von Änderungen bei Assets
- Erkennung von ungewöhnlicher Kommunikation
- Erkennung von Verstößen gegen Sicherheitsrichtlinien

VERTIEFTE NETZWERKANALYSE UND DEVICE-FINGERPRINTING

- Detaillierte Analyse des Netzwerkverkehrs
- Kenntnis von OT-Geräten und Protokollen
- Proprietäres ICS-Fingerprinting und Schwachstellen



TEILENUMMERN

Neuralyzer All-In-One Netzwerk-Gerät	NEU-AIO-STD

TECHNISCHE DATEN

Netzwerk	▪ 1 Onboard-Netzwerkadapter RJ-45, Gigabit Ethernet ▪ 1 WLAN-Karte Intel WLAN 6E (6GHz) AX211 2x2 Bluetooth 5.2 ▪ 2 zusätzliche Netzwerkadapter, USB 3.0 zu RJ-45, Gigabit Ethernet
Spannung	90–264 VAC, automatische Bereichswahl, 47 Hz–63 Hz
Stromverbrauch	220 W (maximal)
Gewicht	15.06 lbs. (maximal)
Abmessungen	344 mm (13,54 in.) x 540,2 mm (21,26 in.) x 52,5 mm (2,07 in.)

Funktionen

- Schnelles Erkennen von Geräten und Aufbau des Asset-Bestandes
- Sofortige Untersuchung der Konnektivität und Visualisierung des Netzwerks
- Fortlaufende Überwachung des Netzwerks zur Erkennung von Bedrohungen und Anomalien
- Konstante und objektive Beseitigung von OT-Schwachstellen und Risiken
- Strukturierter und optimierter Risikowarnungs-Workflow
- Globale, regionale und branchenbezogene Berichterstattung zur Einhaltung von Gesetzen und Richtlinien (Compliance)
- Umfassendes und individuell anpassbares Dashboard
- Einfache Bereitstellung, OT-gerecht und einfache Anwendung

OPSWAT.

Protecting the World's Critical Infrastructure