Produkt-Datenblatt

iSID

Erkennen bösartiger Bedrohungen

- Automatisches Erlernen der Topologie und des Betriebsverhaltens
- Zentraler Einsatz (mit Radiflows iSAP Smart Collectors) oder örtlicher Einsatz an externen Standorten
- Netzwerkverkehr-Analyse von SCADA-Protokollen mit DPI
- Überwachen von Änderungen der SPS-Konfiguration
- Modellgestützte Anomalie-Analysen
- Signaturgestütztes Erkennen bekannter Schwachstellen
- Ungestörter Netzwerkbetrieb
- Geringe Fehlalarmquote
- Zentrale Verwaltung mehrerer iSID-Instanzen mit iCEN

SECHS SICHERHEITSPAKETE FÜR EINE UMFASSENDE BEDROHUNGSERKENNUNG

iSID erlaubt die unterbrechungsfreie Überwachung der Änderungen und des Verhaltens verteilter SCADA-Netzwerke, unterstützt von sechs Sicherheitspaketen, die besondere Funktionen für bestimmte Netzwerkaktivitäten bieten:

1. NETZWERK-SICHTBARKEIT: iSID liest den gesamten OT-Netzverkehr mit, bildet ein visuelles Netzwerkmodell aller Geräte, Protokolle und Sitzungen ab und alarmiert bei erkannten Topologieänderungen (z.B. neue Geräte oder Sitzungen).

2. CYBER-ANGRIFFE: Das Cyber-Attack-Paket erkennt und isoliert die aus öffentlichen Datenquellen (Antivirus-Forscher) und Radiflow-Labs bekannten Bedrohungen des SCADA-Netzwerks, speziell für SPS, RTUs (Remote Terminal Unit) und industrielle Protokolle.

3. REGELÜBERWACHUNG: Regeln für Netzwerkverbindungen definieren und ändern, um bestimmte Befehle (z.B. " in den Controller schreiben") und Betriebsbereiche (z. B. "Turbine nicht über 800 U/min betreiben") zu prüfen.

4. WARTUNGSMANAGEMENT: Schränkt das Netzwerk für geplante Wartungen ein und erstellt Arbeitsaufträge für bestimmte Geräte in festgelegten Zeitfenstern. Nach Sitzungsende wird ein Protokoll über alle Wartungsaktivitäten erstellt.

5. ANOMALIE-ERKENNUNG: Das Paket Anomalie-Erkennung modelliert das Verhalten des Netzwerks mit mehreren Parametern, z.B. Gerätesequenz-Abtastdauer, Häufigkeit von Einstellwerten u.a.m., um Verhaltensanomalien zu erkennen.

6. BETRIEBSVERHALTEN: Überwacht und prüft die Geräte-Verwaltung (SPS, RTU & IED) an externen Standorten und warnt bei Änderungen der Firmware oder Konfiguration (z.B. Software-Updates, Ein- oder Ausschalten von Edge-Geräten, Aktivitätsprotokollierung).

ÜBER RADIFLOW

Radiflow entwickelt zuverlässige Lösungen für industrielle Cyber-Sicherheit für kritische Geschäftsabläufe. Unser Portfolio an bahnbrechenden Lösungen für ISC / SCADA-Netzwerke ermöglicht es Benutzern, die Transparenz und Kontrolle über ihre OT-Netzwerke aufrechtzuerhalten. Unsere intelligente Plattform zur Erkennung und Analyse von Bedrohungen für die industrielle Cybersicherheit minimiert potenzielle Geschäftsunterbrechungen und -verluste in Ihrer OT-Umgebung.

Das Radiflow-Team besteht aus Fachleuten mit unterschiedlichem Hintergrund, aus Cyber-Experten von Elite-Militäreinheiten und aus Automatisierungsexperten von globalen Anbietern von Cybersicherheit. Radiflows Lösungen wurden 2009 gegründet und werden von großen Industrieunternehmen und Versorgungsunternehmen erfolgreich eingesetzt, um mehr als 6.000 kritische Einrichtungen weltweit zu schützen.

Mehr unter www.radiflow.com.

Radiflow

TYPISCHE ANWENDUNGEN

TECHNIKER VOR ORT:

iSID überwacht automatisch die Wartungsaktivitäten im vordefinierten Zeitfenster. Arbeiten an anderen Geräten oder außerhalb der Zeit lösen Warnmeldungen aus.

UNAUTORISIERTE ÄNDERUNGEN DER SPS-KONFIGURATION:

iSID erkennt bekannte Protokollbefehle, welche die SPS-Konfiguration beeinflussen.

SCADA-SERVER-ANGRIFF:

iSID erkennt und alarmiert bei Änderungen am Industriemodell, einschließlich ungewöhnlicher Befehlsfolgen und Zeitraster.

SPYWARE:

iSID erkennt Versuche, das Netzwerk mit Spionage-Malware nach SCADA-Geräten wie SPS und RTUs zu durchsuchen.

MAN-IN-THE-MIDDLE

iSID erkennt Rogue-Geräte im Netzwerk anstelle eines gültigen Servers, einer Workstation oder eines SCADA-Controllers (MAC oder IP-Adressendiebstahl).

MALWARE BLACK ENERGY (BE):

iSID erkennt und alarmiert explizit beim Auftauchen von BE und entdeckt durch BE-SCADA-Plugins gesendete unautorisierte SCADA-Befehle und Anomalien im industriellen Betrieb.

ZENTRALER ODER VERTEILTER ISID-EINSATZ

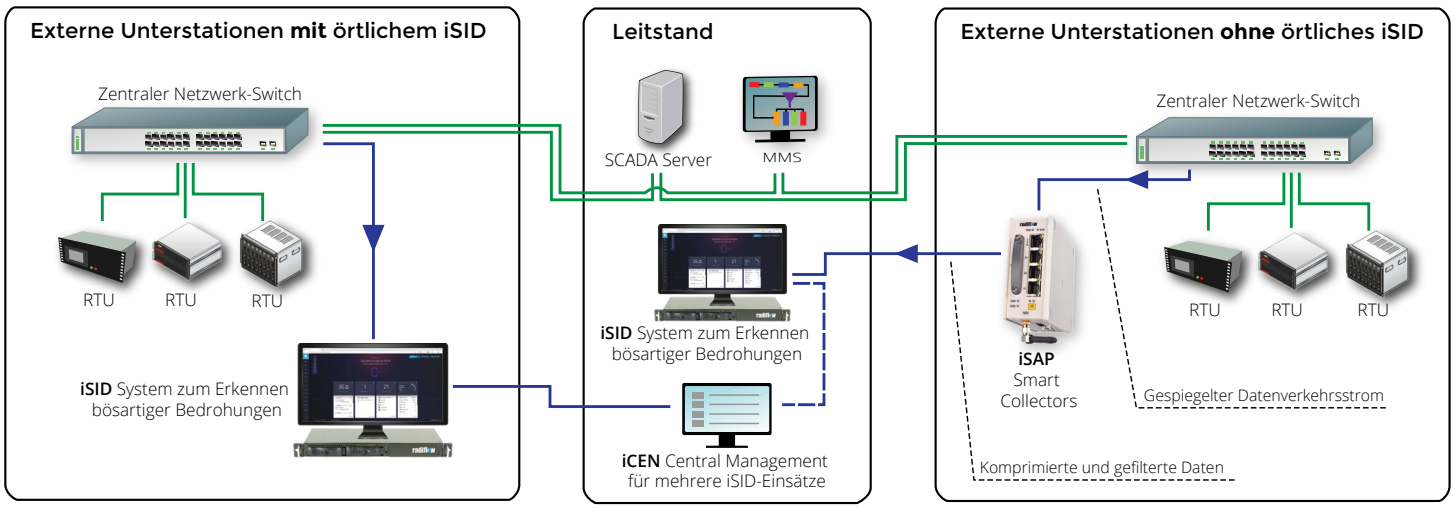
iSID kann an einem zentralen Standort oder örtlich an mehre-ren externen Standorten (oder einer Kombination aus beidem) eingesetzt werden, um Bedrohungen zu erkennen.

Zentralisierte IDS-Einsätze führen meist zu Netzwerküberlastungen wegen der großen Datenmengen, die von den örtlichen Standorten an das zentrale IDS gesendet werden müssen. Der iSAP Smart Collector von Radiflow löst dieses Problem: An den entfernten Standorten liest es den LAN-Verkehr vom lokalen Switch durch Port-Spiegelung mit und filtert einen großteil der irrelevanten Daten aus, ohne den SCADA-Verkehr (z.B. ModBus-Daten) zu stören.

Um das Netzwerk weiter zu entlasten, werden die gefilterten Daten komprimiert und über VPN-Tunnel an die zentrale iSID gesendet.

Mehrere iSID-Einsätze an externen Standorten (meist den größeren) werden mit Radiflows iCEN Central-Monitoring-System für iSID überwacht und verwaltet. iCEN bietet eine Sicht auf den Betriebsstatus aller iSIDs, laufende Übersichten zur Erkennung (z.B. Netzwerkrisiko, erkannte Ereignisse) und der Systemintegrität. Diese werden für ferngesteuerte Softwareaktualisierungen und -wartungen verwendet.

TYPISCHER AUFBAU



iSID-Einsatzmodell, das den zentralen Einsatz in der Leitstelle und den örtlichen Einsatz an externen Standorten kombiniert (mit iSAP Smart Collectors)

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

Radiflow
www.radiflow.com | info@radiflow.com