# iSID
## Erkennen bösartiger Bedrohungen


- Automatisches Erlernen der Topologie und des Betriebs-verhaltens
- Zentraler Einsatz (mit von Radiflows Intelligenten iSAP-Sonden) oder örtlicher Einsatz an externen Standorten
- Netzwerkverkehr-Analyse nach SCADA-DPI-Protokollen
- 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 zum Erkennen aller Bedrohungen

iSID erlaubt das unterbrechungsfreie Überwachen 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 Topologie-änderungen (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, (Remote Terminal Units (RTU) und industrielle Protokolle.

### 3. REGELÜBERWACHUNG

Regeln für Netzwerkverbindungen defi¬nieren 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. WARTUNGS-MANAGEMENT

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 Para-metern, 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 Kon-figuration (z.B. Software-Updates, Ein- oder Ausschalten von Edge-Geräten, Aktivitäts-protokollierung).

*Fortsetzung ...*

## WARUM RADIFLOW?

Radiflow ist anerkannter Markt-führer in der industriellen Cyber-Sicherheit und bietet dedizierte Lösungen für die besonderen Anforderungen industrieller Infrastrukturen:

### ERFAHRUNG

Über 10 Jahre Erfahrung im Erkennen und Analysieren andauernder Bedrohungen und gezielter Attacken, einschließ-lich der auf kritische und industrielle Infrastrukturen.

### EINZIGARTIGE METHODIK

Radiflow bietet eine einzigartige Scan-Methode zum Erkennen bösartiger Angriffsvektoren, die zu Ausfällen führen können.

### EXPERTISE

Spezielles Expertenteam für industrielle Cybersicherheit, welches die unterschiedlichen Anforderungen von Automati¬sierung und Sicherheit versteht.

### PRODUKTPALETTE FÜR ANWENDER

Radiflow bietet eine ganzheitliche Dienstleistungs- und Technologie-Palette mit SCADA-Gateways, Routern und Firewalls, IDS für industrielle Netzwerke und vieles mehr.

## iSID - 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:**

SID 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 unautori¬sierte SCADA-Befehle und Anomalien im industriellen Betrieb.

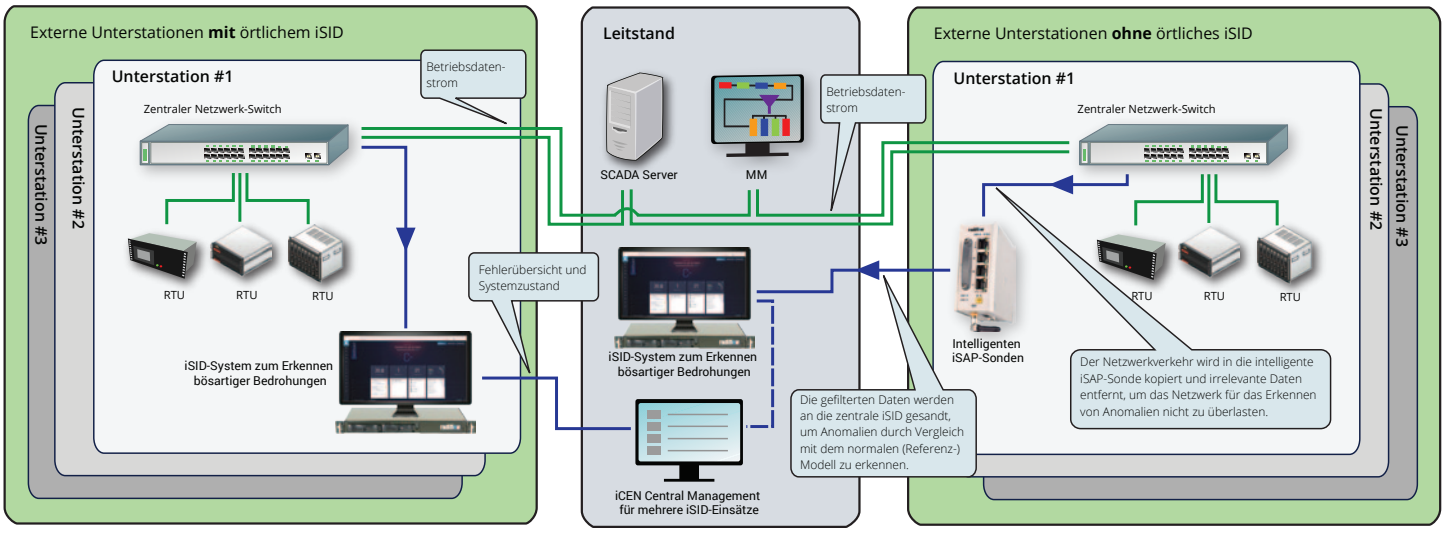
## Zentraler oder verteilter iSID-Einsatz

iSID kann an einem zentralen Standort oder örtlich an mehreren externen Standorten (oder einer Kombination aus beiden) 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. Die intelligente iSAP-Sonde von Radiflow löst dieses Problem: An den entfernten Standorten liest es den LAN-Verkehr vom lokalen Switch durch Port-Spiegelung mit und filtert die meisten 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 Über¬sichten zur Erkennung (z.B. Netzwerkrisiko, erkannte Ereignisse) und der Systemintegrität. Diese werden für ferngesteuerte Softwareaktualisierungen und -wartungen verwendet.




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

**US und Kanada:**
Tel.: +1 (302) 547-6839
sales_NA@radiflow.com

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

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

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