iSID
Détection des menaces industrielles

- Apprentissage automatique de la topologie et du comportement opérationnel
- Déploiement sur un site central (à l'aide de sondes intelligentes iSAP de Radiflow ou localement sur les différents sites distants
- Analyse du trafic réseau par inspection approfondie des paquets des protocoles SCADA
- Surveillance des modifications de configuration des automates programmables
- Analyse de la détection des anomalies à partir d'un modèle, détection des vulnérabilités connues sur la base des signatures
- Fonctionnement non intrusif; Faible taude fausses alertes
- Gestion centralisée de multiples instances iSID à l'aide d'iCEN

Six modules de sécurité pour une détection des menaces complète

Constitué de six modules de sécurité, destinés chacun à un type spécifique d'activité réseau, iSID permet de surveiller les réseaux SCADA distribués de manière non intrusive à la recherche de modifications de topologie et de comportement.

1. VISIBILITÉ DU RÉSEAU

En analysant tout le trafic du réseau OT de manière passive, iSID crée un modèle de réseau visuel de tous les périphériques, protocoles et sessions, et émet des alertes en cas de détection de modification de la topologie (nouveaux périphériques ou nouvelles sessions, par exemple).

2. CYBERATTAQUE

Ce module gère les menaces connues destinées à exploiter les vulnérabilités du réseau SCADA, notamment celles contre les automates programmables, les terminaux distants et les protocoles industriels, en s'appuyant sur les sources de données publiques (laboratoires de recherche) et sur le laboratoire de recherche de Radiflow.

3. MONITORING DE LA STRATÉGIE DE SÉCURITÉ

Ce module permet de définir et de gérer les règles de sécurité de chaque liaison du réseau, et de valider des commandes spécifiques (« écrire sur le contrôleur », p. ex.) et des plages de valeurs opérationnelles (« ne pas régler la turbine à plus de 800 tours/minute », p. ex.).

4. GESTION DE LA MAINTENANCE

Ce module permet de limiter l'exposition du réseau lors des opérations de maintenance planifiées en créant des ordres de travail pour des périphériques spécifiques pendant des fenêtres temporelles définies. À la fin de la session, un rapport détaillant toutes les activités de maintenance est généré.

5. DÉTECTION DES ANOMALIES

Ce module permet de créer un modèle de réseau comportemental à l'aide d'une multitude de paramètres, comme le temps d'échantillonnage de la séquence des périphériques, la fréquence des valeurs opérationnelles etc., pour détecter les anomalies.

6. COMPORTEMENT OPÉRATIONNEL

Ce module permet de surveiller et d'auditer l'administration des appareils (API, terminaux distants et dispositifs électroniques) des sites distants en enregistrant l'activité et en émettant des alertes en cas de modification du microprogramme ou de la configuration (mises à jour logicielles, ou activation/désactivation d'équipements, p. ex.)

A continué....

POURQUOI RADIFLOW ?

Radiflow est un leader reconnu de la cybersécurité industrielle avec ses solutions dédiées aux besoins uniques des infrastructures industrielles.

EXPÉRIENCE

Plus de 10 ans d'expérience en matière de détection et d'analyse des menaces persistantes avancées et des attaques ciblées, notamment contre les infrastructures critiques et industrielles.

MÉTHODOLOGIE UNIQUE

Méthodologie d'analyse unique pour la détection des vecteurs d'attaques industrielles capables de paralyser les installations

EXPERTISE

Une équipe spécialisée d'experts en cybersécurité industrielle à la croisée des mondes de l'automatisation et de la sécurité

PORTEFEUILLE COMPLET

Portefeuille complet de services et de technologies comprenant passerelles SCADA, routeurs et pare-feux, IDS pour réseaux industriels, etc.

radiflow
Secure Your Assets

iSID - Cas d'usage types

TECHNICIEN SUR SITE

iSID surveille automatiquement les opérations de maintenance pendant la fenêtre temporelle prédéfinie. Les opérations dépassant le cadre de la maintenance génèrent des alertes.

MODIFICATIONS NON AUTORISÉES DE LA CONFIGURATION DES API

iSID détecte les commandes de protocole connues liées à la configuration des automates programmables (API).

ATTAQUE DU SERVEUR SCADA

iSID détecte les modifications apportées au modèle industriel, notamment les anomalies dans l'enchaînement et la séquence des commandes, et génère des alertes.

LOGICIELS ESPIONS

iSID détecte les tentatives d'analyse du réseau par les logiciels espions à la recherche d'équipements comme les automates programmables et les terminaux distants.

MAN-IN-THE-MIDDLE

iSID détecte les appareils réseau qui tentent de se faire passer pour un serveur, un poste de travail ou un contrôleur valide en volant leur adresse IP ou Mac, et génère des alertes.

PROGRAMME MALVEILLANT BLACK ENERGY (BE)

iSID identifie explicitement et génère des alertes. Il détecte aussi toutes les commandes SCADA non autorisées émises par les plugins SCADA de BE, ainsi que les anomalies du processus industriel.

Déploiement central ou distribué

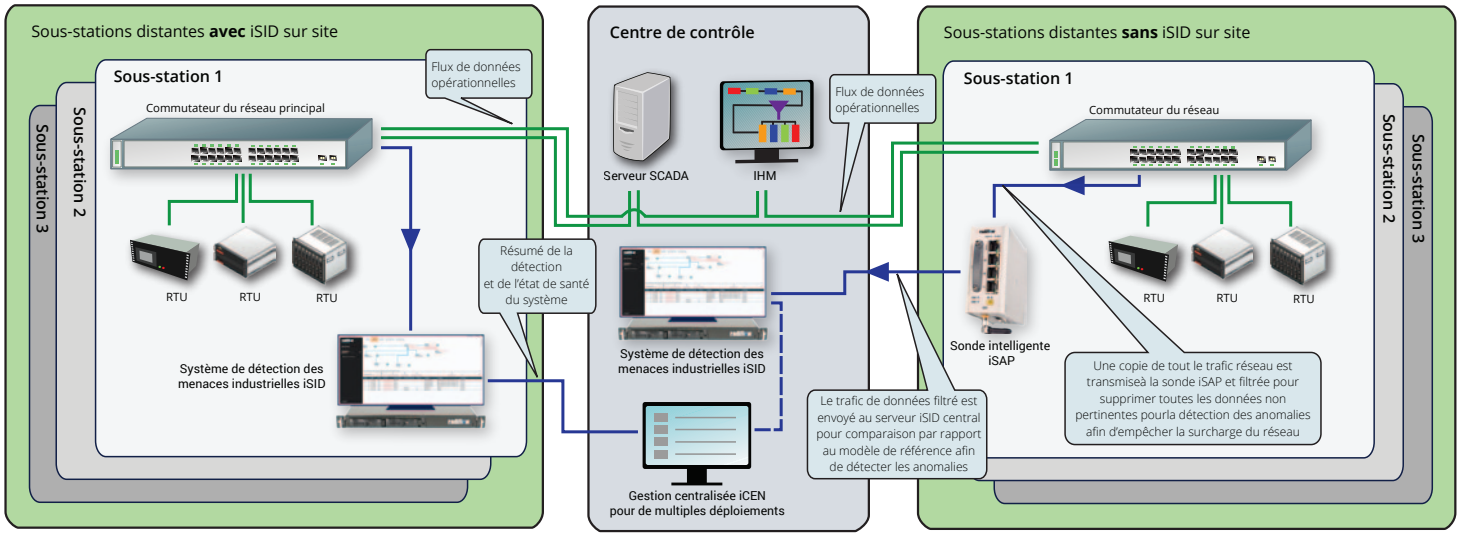
iSID peut être déployé au niveau d'un site central pour détecter les menaces de plusieurs sites distants, ou localement sur chaque site distant (en combinant ces deux modes).

Le déploiement centralisé surcharge généralement le réseau du fait des importantes volumétries de données remontées par chaque site distant vers le système IDS centralisé.

La sonde intelligence iSAP est conçue pour résoudre ce problème. Elle reçoit tout le trafic réseau provenant du commutateur local par la mise en miroir des ports et filtre les données tout en laissant passer le trafic SCADA (données ModBus, par exemple).

Pour éviter toute autre surcharge du réseau, les données filtrées sont compressées avant d'être envoyées vers le système iSID central via des tunnels VPN.

iCEN, le système de surveillance centralisée pour iSID de Radiflow, permet de superviser et de gérer de multiples déploiements d'iSID sur des sites distants (généralement des sites distants de grande taille) en indiquant l'état opérationnel de chaque système iSID, les données récapitulatives de la détection en cours (état des risques du réseau, événements détectés, etc.) et l'état de santé du système. Il sert aussi à la maintenance et à la mise à jour du logiciel à distance.



iSID deployment model, combining central deployment at control center and on-site deployment at remote sites (using iSAP Smart Probes)

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

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

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

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