CYBERSECURITY FOR MANUFACTURING FACILITIES

radiflow

COMPANY DESCRIPTION

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ICS/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and industrial system integrators from global cyber-security vendors.

Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 4,000 critical facilities worldwide. More at www.radiflow.com.

CHALLENGES

The Changing Landscape of Industrial Operations

Cyber threats to Operational Technology networks have in recent years been on the rise. Using widely-available tools, criminals, and increasingly nation-state actors, have set their sights on critical infrastructures, manufactures and other industrial operations that utilize ICS systems due to these systems' inherent vulnerabilities and the high financial losses to manufacturing enterprises due to down-time of production lines.

Today's manufacturing organizations face unique challenges and needs:

- Identifying, managing and mitigating risk: Industrial networks typically host an array of devices by multiple vendors. Understanding the risk introduced by each and the interplay between different business processes is key to adequate protection.
- The human factor: The widespread reliance on IoT-based automation, as well as the subsequent need to grant network access to in-house as well as 3rd-party (vendors, system integrators) personnel, have greatly increased manufacturers' exposures to cyber-threats, either through malicious or erroneous human activity.
- Incident investigation & auditing: The transition to remote cloud-based industrial operations requires organizational changes as well as new tools for analyzing incidents, logging and reporting.

SOLUTIONS

iSID Industrial Threat Detection & Monitoring

- Network visibility based on self-learning of the OT network through passive monitoring, with real-time alerting on parameter change attempts
- Signature-based identification and detection of IT- and OT-related threats
- Anomaly detection based on deep inspection of industrial protocols (e.g. Modbus, OPC UA, CIP)
- Event notifications via multiple reporting methods (GUI, Syslog, SMTP & Modbus)
- Smart collector for low-bandwidth transfer of data to central instance of iSID
- Central management of multiple iSID instances at in-house or MSSP SOC

The iSID Dashboard provides an at-a-glance view of overall network risk, device inventory and alerts

iSEG Secure DPI-Firewall Gateways

- Authentication Proxy Access (APA) for user authentication & pre-configured task-based access
- User activity log within each remote access session for compliance & auditing; validation of user behavior using a per-port Deep Packet Inspection (DPI) firewall
- IPsec VPN for secure inter-site connectivity between manufacturing facilities
- Ruggedized appliances with Ethernet & Serial interfaces

The iSEG RF-3180 Ruggedized Secure Gateway

CIARA Industrial Risk Analysis

- Assess the actual business-related impact of cyber-risk in OT networks with unique calculation of likelihood of attack
- Plain-language, prioritized mitigation recommendations
- Auto-generated risk analytics and risk impact reports, based on up-to-date OT TI
- IEC 62443 reporting support

The iRISK Dashboard

Technology Partners

Radiflow's solutions are further enhanced by a host of 3rd-party integrated systems:

SIEM

Data Analytics

Network Security

OT Security & Asset Management

Identity & Access Management

SECURING INDUSTRY 4.0

Overcoming the complexity of Smart Manufacturing

Industrial cyber security is one of the core features of transitioning to Industry 4.0.

The interconnectivity between the enterprise and its business partners and customers, the introduction of Industrial IoT devices and the dramatic increase in communication protocols (in the physical and application layers, smart logistics and production management, vertical integration between IT systems and OT networks and many other areas) all increase the complexity of the enterprise digital environment and its exposure to external and internal threats.

While many production facilities rely on a mix of DCS systems and supporting SCADA with PLCs for secondary systems, adequate protection requires a multi-prong approach to OT security: OT network visibility, identification of threats, real-time monitoring, OT-aware firewalls for zone segregation and risk management.

In addition, manufacturers need to prove compliance with various governing standards and regulations (e.g. IEC-62443).

Radiflow provides manufacturers with the tools to protect, visualize and safely maintain their systems:

- A complete visual model of the OT network: assets, connections, protocols and vulnerabilities
- CIA (Confidentiality, Integrity & Availability, as well as Safety) per-business process risk evaluation, using the CIARA Risk Analysis & Management platform
- MSSP/SOC ready with alert prioritization triage and multi-iSID system management solution
- Attack vector and attacker capability analysis for alert prioritization and optimizing risk mitigation investment
- Compliance enabler for IEC 62443 and other common standards and regulations
- Strong vendor support and strategic partnerships with leading solution providers

CASE STUDY

Securing a Global Chemicals Manufacturer

Securing a distributed manufacturing operation spanning multiple production facilities is always a challenge. The challenge is compounded when it comes to securing chemical manufacturing operations, due to the devastating environmental damages and threat to human life resulting from of a potential cyber-attack.

Objectives and Challenges:

While the customer's existing cyber-security system covered well its IT networks, it left open key functional gaps when applied to the OT network, such as the system's inability to handle OT-specific network protocols.

The objectives of the project, as specified in the manufacturer's tender, were:

- Continuous monitoring of all OT assets at all production lines across multiple sites
- Detecting and alerting on OT cyber threats and anomalies
- Tracing logic & firmware changes on all industrial controllers
- Reporting OT cyber-alerts to the facility SIEM (Security information and event management system)

Solution & Process

- Single instance of iSID installed locally at each production plant
- iSAP Smart Collector installed at each subnet (with multiple subnets at each plant) for sending a bandwidth-efficient mirrored stream of all TCP/IP data traffic to the local iSID
- Integration of the Radiflow system with the SIEMs (by different vendors) at each plant to provide the customer with a unified alerting system

As the customer operates dozens of facilities with different types of systems and topologies, the project required close cooperation between the customer and Radiflow to optimize the solution capabilities which may evolve over the project life-cycle. Radiflow research team utilized a machine-learning infrastructure to quickly parse additional protocols and provide full visibility for all assets at each site.

Why Radiflow?

The customer has stated the following reasons for selecting Radiflow:

- Technical solution that fully met all stated requirements; specifically mentioned was the use of iSAP Smart Collectors to send data traffic to each site's iSID without overloading the LAN
- Team expertise and long-term commitment to support the customer throughout the global deployment.
- Long-term price considerations

See all Radiflow case studies at radiflow.com/case-studies

radiflow

Scalable, flexible architecture for all types and sizes of industrial organizations

Comprehensive portfolio of detection and prevention tools as well as assessment and monitoring services

Planning value-add: tools for business-driven risk scoring and mitigation planning

Solution designed by industry experts and validated by external labs, protecting over 4,000 sites worldwide

US and Canada:
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

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

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