KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | July 2019

Radiflow SCADA Security Suite

Radiflow SCADA Security Suite is a comprehensive set of hardware products, software solutions, and managed services offering risk-based insights into ICS/SCADA networks, intelligent detection of IT and OT-related cyberthreats, as well as proactive protection against any deviations from established security policies.

by **Alexei Balaganski**
ab@kuppingercole.com
July 2019

Content

Related Research

Advisory Note: Industrial Control Systems: Getting a Grip on OT Cyber Security – 71110

Advisory Note: Plant Automation Security – 71560

Leadership Brief: Join the Dots: Operational Technology and Informational Technology – 72012

Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network – 72163

1 Introduction

Radiflow is an industrial cybersecurity vendor headquartered in Tel Aviv, Israel. Established in 2009, the company is a part of the RAD Group – a collective of multiple independent companies designing and manufacturing solutions for various areas of network and telecommunications industries. Following the philosophy of independent operations under joint strategic guidance by multiple company founders, the RAD Group has been Israel's most successful IT startup incubator, helping establish over a hundred of high-tech companies since the 1980s. With a yearly revenue of over $1.3 billion, the group currently comprises 10 companies including Radiflow, one of their youngest members.

Radiflow was founded by a group of seasoned veterans of telco and security industries with an initial focus on producing secure networking hardware for industrial environments. However, the company has quickly expanded their solution portfolio to provide a full range of hardware and software products, as well as managed services for securing ICS/SCADA infrastructures for industrial and other critical infrastructure customers. Currently, Radiflow's solutions are deployed in over 3,000 sites, protecting major industrial facilities around the world.

It has become somewhat commonplace in recent years to talk about the poor state of industrial cybersecurity and to put the blame on OT engineers for not giving enough attention to the modern cyberthreats. Of course, ensuring the security and safety of industrial control systems has always been the most important job for OT experts. However, after decades of dealing with unique technologies and regulations and with a traditionally strong focus on human and process safety, securing IT assets was by far not their top priority.

Just like other IT infrastructures, industrial networks are becoming increasingly complex, geographically dispersed and interconnected with open corporate networks. Today, potential impacts of purely IT-related risks for ICS systems are no longer limited to productivity or financial losses; they can cause massive disruptions of manufacturing processes, equipment problems or even large-scale catastrophes. And just like in "traditional IT", the biggest challenge for OT security specialists is no longer just to detect every potential threat in their networks, but not to get buried under a huge number of them – raising the need for a threat model that provides risk evaluation and prioritization to ensure that the most critical threats are being dealt with first.

Traditional passive intrusion detection systems favored by OT specialists for decades are no longer enough to meet these challenges. From machine learning-based anomaly detection to simple actionable insights and recommendations to fully automated mitigation controls – the functional scope of next-generation ICS/SCADA security solutions will be defined by intelligent risk management.

Radiflow's answer to these market demands is a complete portfolio of security solutions and services that do not just provide full visibility into OT network activities and intelligent detection of various threats. Indeed, the company aims to give their customers the means to model the most common cybersecurity risks, proactively assess their impact on the key ICS assets and in the end to offer actionable insights for prioritizing their mitigation. With these tools, OT security experts can not just anticipate the most probable attack vectors to be used by various malicious actors, but proactively neutralize them by focusing their efforts on protecting the riskiest assets first.

2 Product Description

Unlike many other vendors, especially start-ups, operating in the Operational Technology security market, Radiflow goes beyond a single product and offers a complete portfolio of hardware- and software-based products and services, which can be deployed and operated independently or as an integrated ICS/SCADA security suite.

The company's flagship product is the **iSID Industrial Threat Detection** platform, which provides non-intrusive monitoring of large and distributed industrial networks, discovery of network topology and normal behavior patterns, as well as detecting known malicious and previously unknown suspicious activities as deviations of those normal profiles.

Since most industrial networks only allow fully passive deployments of security solutions, this is how iSID is usually set up as well. Delivered as a pre-configured hardware appliance, it requires no changes to the existing infrastructure, only the access to a mirror port on a central network switch to capture the traffic flowing through the network for analysis. Similar to traditional IT-focused security intelligence solutions, the platform then uses this captured data to automatically enumerate all connected devices, discover the network topology and visually map all traffic flows between devices.

However, by utilizing deep packet inspection together with a massive knowledge base of industrial hardware and protocols, iSID is able to collect much more precise, protocol-specific data from each network session and thus provide much deeper visibility into every activity and to alert on any suspicious change.

However, perhaps the most interesting feature the company is currently heavily investing in is prioritization of detected threats according to business process risks – the technology Radiflow refers to simply as "Insights". As opposed to numerous alerts generated by typical SCADA monitoring solutions, iSID aims to reduce the strain on security analysts by performing automatic risk evaluation of each detected threat according to the company's own SCADA risk assessment model, which is tailored to specific attack vectors and process risks for each customer.

To achieve this, the company's methodology combines several approaches towards measuring the probability and impact of various SCADA risks:

- Exploitability analysis for each detected threat based on device properties, network connectivity and other factors (currently, the model covers over 60 different attack types).
- Business process modeling, which analyzes the basic topology to partition the network according to known SCADA processes, identify the most critical devices and prioritize certain risks associated with them (for example, a chemical plant and a power grid not only have different connectivity patterns but are subject to fundamentally different risks).
- Modeling the capabilities and preferred attack scenarios for different types of attackers, including various known device vulnerabilities and protocol exploits (based on a large database of known past incidents)

Of course, a substantial part of this methodology is already a part of many SCADA security analysts' daily jobs. However, it is currently still a largely manual and tedious process, which can only produce static point-in-time snapshots into SCADA network activities. With its AI-powered risk analytics module, Radiflow promises to make this process fully automated and continuous. Each detected threat is not just ranked according to potential risk impact specific to the customer's network architecture and business processes, the Insights provide specific, actionable recommendations for reducing these risks proactively.

On top of this common foundation, the platform offers several other functional packages that implement various operational and security capabilities. Radiflow customers are free to choose which modules to deploy depending on their current or future requirements.

The **Cyber Attack** module is scanning for cyberthreats targeting known vulnerabilities in OT networks. This covers both SCADA-specific threats targeting programmable logic controllers (PLC) and other industrial devices as well as more general IT threats that can harm Windows machines running HMI devices. This module relies on threat intelligence collected by Radiflow's own lab and on public data from the worldwide research community.

The **Policy Monitoring** module lets users define custom policies for every traffic flow to ensure that only valid commands and data ranges are allowed to reach an industrial controller. This rule-based policy framework (like "coolant pump motor should not drop below X rpm") provides the basic level of detection for potentially malicious OT activities and will generate an alert as soon as a rule is violated.

More advanced detection is provided by the **Anomaly Detection** module, which maintains an advanced behavior-based network model, taking multiple operational and security-related variables into account. This module is able to identify anomalies without predefined rules, just by detecting statistical outliers and other kinds of unknown but suspicious activities.

The **Operational Behavior** module is responsible for auditing the management of industrial devices, maintaining a full audit trail of all firmware updates, configuration changes, and other administrative activities. It can also generate alerts for selected remote sites.

Finally, the **Maintenance Management** module is used for tracking scheduled device maintenance and ensuring that these actions are performed only during specific time windows. An unplanned operation will immediately trigger an alert as well.

Quite often, large-scale deployments, either in complex and large networks or infrastructures with multiple remote sites, pose different scalability problems. On one hand, sending all network traffic to a single central location can overload the network with large amounts of data; on the other hand, collecting this data from sites with limited connectivity creates a multitude of challenges with latency, security, and access controls. The company implements a quite unique two-way scaling approach to address both issues.

Radiflow's **iSAP Smart Collectors** are compact and robust hardware appliances that can be deployed in every segment of an industrial network. These collectors utilize the same passive monitoring technology with deep packet inspection to identify and isolate only SCADA-relevant traffic and discard the rest. The relevant captured data is further compressed by the company's proprietary technology and then sent to a central iSID unit over an encrypted tunnel. These probes are engineered to ensure that their data transmissions are fully unidirectional, meaning that they cannot be exploited for unauthorized access to a remote network.

On the other hand, monitoring and centralized maintenance of multiple iSID deployments can be performed using another company's solution: the **iCEN Central Monitoring System**. iCEN provides unified visibility into each installation's operational status, a consolidated view into security posture and a single place to manage detection rules and threat updates.

Beside real-time alerting, the platform offers basic forensic workflow capabilities: each event can be reviewed, added to a baseline or escalated to a ticket. Integrations with SIEM solutions and more advanced forensic analysis tools are supported as well. Additionally, iSID can integrate directly with HMI hosts to display security-related information as a part of an existing OT process visualization.

For more open-minded customers, integrations with third-party network security products are available, which enable active mitigation capabilities (for example, to isolate a misbehaving device from the network on a firewall level).

However, Radiflow's **iSEG Secure Gateway** could be a more popular option for such scenarios. Designed specifically to securely manage identity and access for remote sites within critical infrastructures, iSEG is a standalone product that combines the company's SCADA monitoring and analytics capabilities with secure remote access functionality.

Deployed on the edge of a remote industrial network, iSEG not only provides an encrypted communications channel over fiber or cellular interfaces but performs continuous deep packet inspection of all SCADA traffic. When any malicious anomaly is detected, the gateway can generate alerts, block the activity automatically or completely isolate any affected subnet.

In addition, it enforces identity and access policies via Authentication Proxy Access (APA) to ensure that each access to devices within the network, either external or by an on-site maintenance worker, is validated, secured and audited for compliance. Companies that already use a company-wide Privileged Access Management (PAM) solution from CyberArk, the leading vendor in this market, can incorporate iSEG gateways into its centralized management.

In addition to product development, Radiflow offers several managed services both directly to their customers or to their managed security service provider partners.

The most notable is arguably the company's **iSOC** multitenant platform targeted towards MSSPs. The architecture optimized for scalable and secure data collection over low-bandwidth links combined with an administration console to provision and operate multiple isolated iSID deployments and direct integration with several threat intelligence feeds make for an efficient and easy-to-operate industrial security platform for multiple tenants, which can be deployed in a cloud environment. Even though the majority of Radiflow's customers are still large enterprises operating their own deployments, the company has already partnered with several prominent MSSPs.

Another service worth mentioning is the **iSEC ICS Security Assessment**, which provides an expert review of the customer's industrial network architecture and individual components, as well as a detailed analysis of all network activities over a period of 2-4 weeks to enumerate all assets, identify device vulnerabilities, network weaknesses, access control issues and review compliance with relevant regulations. As a result, customers are provided both with an executive summary for the management and a comprehensive technical report with all findings and an actionable mitigation plan.

3 Strengths and Challenges

What differentiates Radiflow from a large number of other vendors offering similar passive SCADA monitoring solutions is that the company goes beyond a single product. Thanks to their decade-long experience in industrial hardware design, Radiflow can offer a comprehensive solution portfolio that covers multiple aspects of ICS/SCADA security – from network discovery and monitoring to behavior analytics for both operational and security purposes to proactive hardening of OT networks and even active threat mitigation (even though the latter option is yet to gain substantial popularity among OT experts).

With a platform designed from the ground up to be scalable and multi-tenant, Radiflow can address the requirements of the largest industrial customers, as well as offer their MSSP partners a convenient solution for reselling OT security services.

However, perhaps the biggest development that differentiates iSID from more traditional intrusion detection systems is the recent addition of "Insights", the intelligent prioritization of detected threats according to their impact on specific customer's business processes. Thanks to the company's large database of modeled types of attacks and attackers combined with intelligent network segmentation based on business processes, the platform isn't just able to identify the most critical assets and most probable attack vectors but offer actionable recommendations for their proactive mitigation.

Strengths	Challenges
• A comprehensive suite of hardware, software and managed services for visibility, monitoring, threat detection and proactive protection of ICS/SCADA networks • Two-way platform scalability for large complex deployments; multi-tenant cloud platform for MSSPs • Automated risk analytics tuned to specific customer's business processes and assets • Actionable insights for proactive mitigation of the most critical risks	• Primarily targets large industrial customers, MSSP network is still being established • Risk analytics capabilities are not yet fully configurable; further developments expected in future releases

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com