REPORT REPRINT

Radiflow says it can empower managed service providers to deliver OT security services

OCTOBER 14 2019

By Aaron Sherrill

Threats to industrial systems are no longer hypothetical, but now represent a large and growing challenge to industrial operators of all types. Radiflow is aiming to empower MSSPs with the ability to monitor and protect large and distributed OT networks, and reduce the risks of business interruption in operational environments.

Introduction

Industrial and critical infrastructure networks – such as power generation and distribution, water, oil and gas, renewable energy, and process manufacturing – are both vital and vulnerable, often plagued with poor IT infrastructure design. Gradually, constructed over many years, these networks have evolved into large, complex distributed systems that are vulnerable to cyber-threats and nation-state attacks.

Successful cyber incidents in these sectors not only affect brand reputation, revenue and production, but can also be fatal, with devastating consequences to the health and safety of human lives. Unfortunately, most industrial enterprises lack the internal resources and expertise to effectively manage their cybersecurity efforts by themselves, and most managed security service providers (MSSPs) lack the tools and technologies to effectively secure and protect operational technology (OT) networks.

Radiflow, a provider of cybersecurity technologies for industrial networks, is aiming to empower MSSPs with the ability to monitor and protect large and distributed OT networks, and reduce the risks of business interruption in operational environments.

451 TAKE

Threats to industrial systems are no longer hypothetical, but now represent a large and growing challenge to industrial operators of all types. The increase in security incidents and breaches in recent years involving critical infrastructure systems indicates that the global industrial sector is increasingly becoming the target of cyberattacks. In response, industrial operators are making substantial investments in ICS security. Yet many industrial enterprises, especially smaller operators, lack the expertise and resources to deploy and manage cybersecurity technologies, identify vulnerabilities, and detect threats in their ICS and SCADA environments.

These industrial enterprises desire to partner with MSSPs to fill the gaps in their cybersecurity postures, but have discovered that most MSSPs lack the technologies and skills to secure and protect OT environments. Radiflow's OT-MSSP partner program should prove a win for MSSPs looking to expand their services and offer their customers more value, and for industrial operators that want to improve their cybersecurity postures and gain access to expertise and technologies aimed at protecting their OT networks.

Context

Headquartered in Mahwah, New Jersey, Radiflow was founded in 2009 by CEO Ilan Barda and Chairman Zohar Zisapel. With offices in the US, UK, Israel and Europe, the privately held company employs over 50 people, most with backgrounds in cybersecurity and industrial automation systems. Radiflow reports it has 76 customers worldwide, including Tier 1 critical infrastructure operators in the US and Europe, and is protecting nearly 3,000 sites with its technologies. Radiflow closed an $18m investment round last year led by ST Engineering Ventures, the corporate venture capital arm of technology, defense and engineering company Singapore Technologies Engineering. The company says it is experiencing strong demand for its industrial cybersecurity products.

Radiflow is primarily a technology company focused on providing cybersecurity products designed to protect industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems on industrial automation networks. The company's product portfolio includes industrial threat monitoring and visibility systems, industrial traffic probes and collectors, and secure remote access gateways.

Radiflow's threat detection and analysis platform, iSID, provides nonintrusive monitoring of distributed industrial networks, building a baseline of all the assets and patterns of the behaviors in the network, and alerting on any anomalies. Its secure remote access gateway, iSEG, is a physical device designed to secure both machine-to-machine and human-to-machine traffic through deep packet inspection. The device provides secure remote access, firewall and VPN capabilities.

According to Radiflow, many industrial enterprises lack the knowledge and competencies to understand where and how to leverage OT cybersecurity controls. As a result, Radiflow added security assessment services to its portfolio last year. The assessment service is designed to discover, classify and map all network assets to help industrial operators identify vulnerabilities and risks to their organization. The findings are used as the foundation of a cybersecurity plan for the organization.

However, Radiflow says that even when they are armed with a comprehensive cybersecurity plan and a variety of IT and OT cybersecurity products, most industrial enterprises and critical infrastructure operators lack the internal expertise to effectively secure the organization and continuously monitor the environment for indicators of compromise. In response, Radiflow recently launched a partner program with offerings designed to empower MSSPs to protect industrial networks and facilities with OT cybersecurity services.

OT cybersecurity for MSSPs

Radiflow's OT-MSSP partner program provides both cybersecurity technologies and a framework for MSSPs to offer security services aimed at securing and protecting ICS and SCADA networks. Renewable energy, municipal water utilities, manufacturing and building management are among the key industry segments that are looking for MSSPs to help with protecting their OT infrastructure. According to Radiflow, power generation and power transmission providers tend to be reluctant to share information, and are less likely to outsource to a managed service provider.

Radiflow's OT-MSSP offering begins with iSAP smart collectors installed at each production facility to passively collect and securely transport all data traffic to iSID, Radiflow's industrial threat detection system. Through a self-learning process, iSID creates a baseline network topology model of all devices, connections and ports. Once the baseline has been established, iSID begins identifying OT network vulnerabilities, and enables MSSPs to perform network monitoring and threat detection. The system can also be used to apply security upgrades to any newly detected devices.

MSSPs can leverage Radiflow's CIA-based Advanced Risk Assessment engine and Attack Vector Simulation modeling capabilities to provide recommendations for prioritizing and reducing vulnerabilities, testing the organization's security posture, and optimizing security expenditures. The partner program also enables MSSPs to generate security posture reports used in quarterly business reviews with customers. These reports take into account the changes in the network, the evolving threat landscape, new vulnerabilities that have been discovered, and attack vector trends.

Recognizing that delivering OT cybersecurity services requires more than just technology, the company has built a framework for MSSPs that includes the tools, procedure and support necessary for MSSPs to be successful. Radiflow says it works closely with each partner to implement the framework and processes required to deliver OT cybersecurity services.

Radiflow suggests that one area MSSPs find unique to OT cybersecurity is incident response. Unlike IT cybersecurity, where applications, devices or systems that are involved in an attack can often be (automatically) shut down, taken offline or quarantined, OT systems are rarely permitted to be shut down, even in the event of a cyber-attack. As a result, preparation and readiness are crucial to minimizing the impact of a security incident. Radiflow guides MSSP partners on incident preparation, including running and documenting what-if scenarios, creating response plans, and mitigating exposure.

Radiflow says that response to the OT-MSSP partner program has been strong since the program launched. The company reports it has MSSP partners actively engaged and delivering OT cybersecurity services in Austria, Germany, Switzerland, France, the UK and the US.

Competition

Radiflow faces a range of competitors targeting the ICS and SCADA security market. The industrial cybersecurity space is heating up because companies in this market have attracted significant investment over the last couple of years. Claroty locked down a $60m series B investment last year, bringing its total funding to $93m. Dragos raised $37m in new venture capital late last year, bringing its total funding to $48m. Nozomi Networks announced it had raised $54m in total investments, including a $30m series C round last year.

Several other industrial cybersecurity companies and Radiflow competitors have raised funding recently, including Indegy, Bayshore Networks, CyberX, SCADAfence and TraxpX Security. Rival Sentryo was recently acquired by Cisco, which plans to incorporate Sentryo's edge sensor and industrial networking hardware with its IOx application framework.

While many of these competitors have partner programs that target MSSPs and other service providers, most are positioned as sell-through partnerships, rather than empowering and supporting MSSPs to deliver OT cybersecurity services.

In addition to this crowd of industrial cybersecurity vendors, Radiflow faces competition from security providers and technology vendors that have IIoT (industrial internet of things) and other cybersecurity offerings targeted at the industrial operator market, including SecurityMatters, Cyberbit, Cybereason, DarkTrace, Xage Security and Armis. Again, many of these providers also target MSSPs for sell-through opportunities, but several aim to enable MSSPs to provide security services to the industrial market segment with their respective technologies.

SWOT Analysis

STRENGTHS

Radiflow's ease of deployment for MSSPs using its novel iSAP smart collectors, broad customer base, OT risk assessment methodology, and OT-MSSP framework provide a high level of assurance to MSSPs looking to partner with an industrial cybersecurity technology provider.

WEAKNESSES

As IT and OT cybersecurity converge, Radiflow will need to consider expanding the integration capabilities of its OT cybersecurity technologies with third-party OT and IT cybersecurity tools. Integrations will be paramount for MSSPs that are looking to drive scale through automation, orchestration and machine learning.

OPPORTUNITIES

Radiflow's emphasis on empowering MSSPs is a differentiator in a market where partner programs tend to focus on sell-through opportunities. The company's OT-MSSP Cybersecurity Program should be welcomed by MSSPs looking to expand their security services portfolio and market reach into the industrial cybersecurity segment.

THREATS

The cybersecurity market can be confusing to navigate, crowded with vendors that tout solutions that can cover both IT and OT cybersecurity needs. As Radiflow looks to expand its OT-MSSP partner program, it will need to spend time educating the MSSP market on the value of its OT-specific approach to industrial cybersecurity, and how its technologies and program differentiate in a market where providers sound increasingly similar.