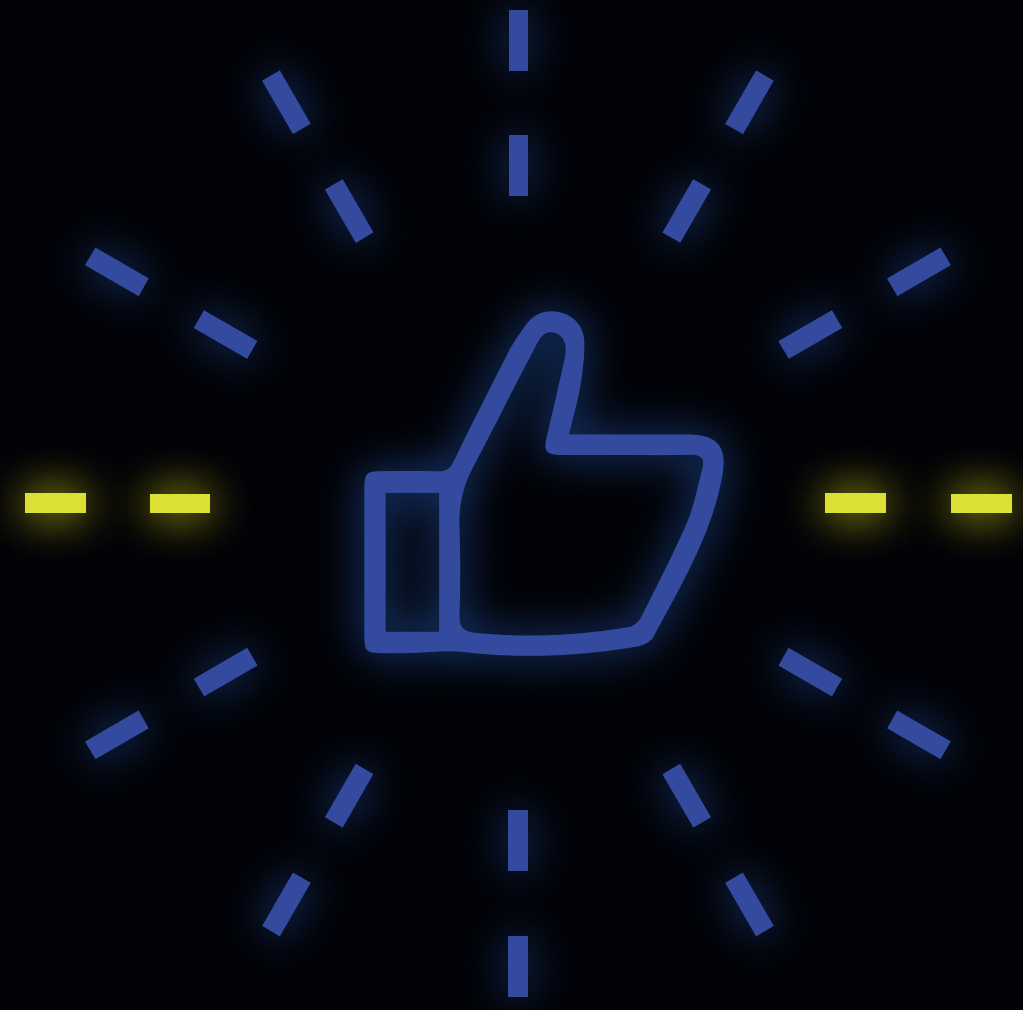
Radiflow

Security Brief: “The Five Best Practices that will Protect Your OT/ICS Network in 2021”

The Radiflow Cybersecurity Team

May 2021



In recent years, industrial organizations in practically all sectors have become prime targets for cyber attacks. And while the motivations, tactics, national affiliations and sophistication of the attackers vary, the conventional wisdom you should heed is that your network is either already under attack, or will be soon.

Here are five tips that will bring your OT-security operation up to par:

1. The Basics

While most of the news about recent OT-cyberattacks focus on new and sophisticated attacker techniques, in many cases network breaches resulted from poor password management, outdated user access authorizations, outdated device software and such.

In fact, according to Verizon's Business 2020 Data Breach Investigation Report, 81% of all data breaches (in all sectors) were caused by compromised weak passwords; still, 61% of surveyed companies never installed policies for password complexity. Password and user authentication fixes are easy and quick to implement, and must be reviewed periodically.

Another CISO pain point is by employee activity: inside jobs, human error and employees activating phishing attacks. To safeguard your OT network, make sure to set up gateway rules at production units that alert on or prevent technician activity outside of the set parameters for each maintenance session, as well as device and communication rules that detect and block abnormal types of network activity associated with technician error (e.g. setting device operational parameters outside of a preconfigured range).

2. Know your network risk

As McKinsey's "Risk-based approach to cybersecurity" report states: "The most sophisticated institutions are moving from a "maturity based" to a "risk based" approach for managing cyber risk. OT network risk – defined as the sum-total of the impact of all threats, multiplied by the quantitative probability of their occurrence – is OT cybersecurity's "new frontier".

The simple idea behind risk-based network protection is that your cyber-security efforts (read: dollars) should focus on:

- The attackers and attack techniques that actually threaten your network (based on threat intelligence)
- The business units that are the most critical

Knowing your risk posture enables prioritizing risk mitigation measures by overall effectiveness, and optimizing your cyber-security expenditure. Radiflow's Industrial Risk Assessment & Management Platform methodically combines the threat level to each and every device and business unit and the impact of an attack of each business unit. By simulating tens of thousands of breach scenarios using a unique analysis algorithm, it's able to accurately calculate network risk, and produce an easy-to-follow roadmap toward achieving the highest level of security per dollar spent, automatically optimized to meet the security needs of each business unit (based on criticality) and the user's tolerable risk level.

3. See your network

Even if you think you know the ins and outs of your operational network – all devices and device properties, inter- and intra-network connections, communication protocols, used and unused ports, and other network characteristics – you probably don't.

The ability to visualize your network, in a form that's useful to the CISO or any other network professional, is essential to protecting it. As an example, Radiflow's map-based visual topology model of the OT network presents all network assets, down-drillable to their properties, connections and vulnerabilities, in multiple modes (Perdue, Flow, Analyst & Custom). Our network map also features an Attack Vector Analyzer, which detects vulnerabilities to assets caused by connections to other at-risk business processes.

4. Make sure you're standard-compliant

With the rise in OT cyber-attacks, governments and research institutes have issued a slew of standards and regulations for protecting communication networks at critical infrastructures. These standards provide excellent guidelines for implementation, operation and auditing, and in some countries are mandatory, imposing a hefty cost for non-compliance.

Two of the most globally-adopted standards are:

- The International Society of Automation's (ISA) is IEC 62443, a multi-part series of standards and technical reports on the subject of Industrial Automation and Control System (IACS) security, covering system integration practices, development lifecycle security, security specifications, requirements and levels for IACS components. Radiflow has long championed the IEC 62443 standard, and its solutions are recognized as strong IEC 62443 enablers.
- The American National Institute of Standards & Technology (NIST) Cybersecurity Framework, which integrates industry standards and best practices to help organizations manage their cybersecurity risks and provides a common language that allows staff at all levels—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks. (Radiflow was included in an example solution for securing electric utilities networks, put together by NIST's NCCoE – National Cybersecurity Center of Excellence).

5. Consider using a cloud-based managed security services (OT-MSSP)

MSSPs are a viable alternative to in-house security monitoring, for organizations that are unable to set up a full-fledged OT security department, due to:

- Lack of funding for an adequate cybersecurity program
- The shortage of cybersecurity personnel trained in protecting Industrial Control Systems.

Cloud-based Managed Security Service Providers (MSSPs) have in recent years stepped in to meet the needs of smaller OT organizations. You get the enterprise-level SOC (Security Operations Center) and security solutions, monitored by skilled operators, with low upfront costs.

Prior to regular monitoring of your network traffic for signs of possible attacks, the MSSP will perform a network analysis to "learn" the topology, assets, protocols, ports and all other network properties, toward creating a baseline digital image used for data traffic analysis, toward monitoring the network for abnormalities, continuously monitoring the network's risk posture (following changes to the network and to the threat landscape), and automatically adjusting its recommended mitigations for optimized security.

Conclusion

While attacks on industrial organizations have been on the rise and are expected to increase in the coming years, the tools, standards, guidelines and best-practices needed to detect and prevent attacks are readily available; furthermore, organizations that lack the resources, know-how and/or manpower to set up an in-house ICS security operation can alternately use the services of OT-MSSPs which offer the utmost level of OT security with very little upfront expenditure. We urge you to take the needed steps to protect your ICS operations.

Radiflow's team is known for its cybersecurity expertise and reputation in the OT world. If you are concerned about the security of your OT systems – and you should be – but don't know what to do about it, **contact us today**. We can help.