MAY 30, 2019

SCADAfence Helps Industrial Companies Secure Systems and Manage Cyber Incidents

By Sid Snitkin

Keywords

Industrial/OT Cybersecurity, Asset Inventory, Vulnerability Management, Detection and Response, SCADAfence

Summary

Continuous monitoring of control system networks is essential for developing and managing effective industrial cybersecurity programs. It enables companies to maintain accurate asset inventories and data flow maps. Visibility of system activities allows rapid detection of abnormal events, whether they are related to malware, equipment failures, or user errors.

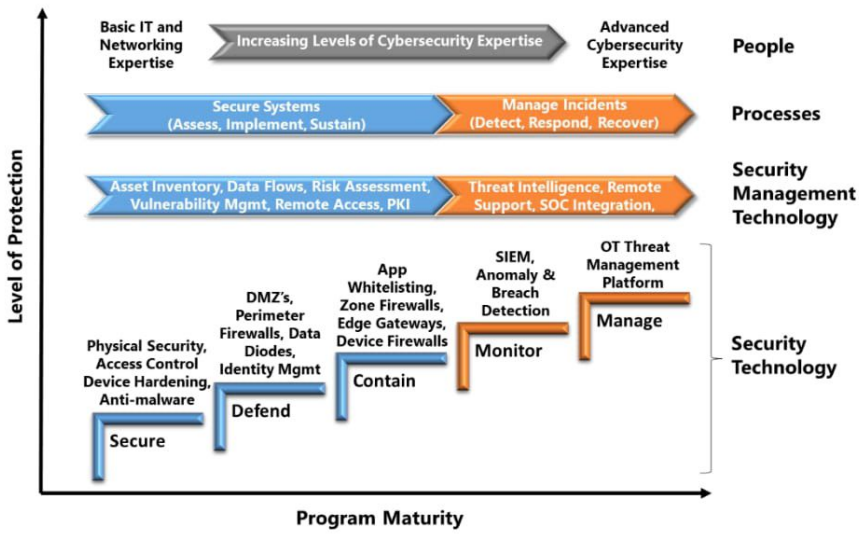
Continuous monitoring of control system networks is essential for developing and managing effective industrial cybersecurity programs. This report discusses the key features of an effective continuous network monitoring solution and how the SCADAfence Platform was designed to meet these needs.

Recent incidents, like the Ukrainian power outage and disruption of Norsk Hydro aluminum production, demonstrate the importance of sustaining cyber defenses. But they also show that conventional cyber defenses can be overcome by sophisticated cyber-attacks. Continuous system monitoring is critical to minimize the impact of such compromises.

ARC recently discussed these issues with executives from SCADAfence, a provider of continuous network monitoring for large, complex control systems in manufacturing, building management, and critical infrastructure industries. Applications utilizing the company's SCADAfence Platform include Mitsui Fudosan's large real estate portfolio and Europe's largest manufacturing facility.

ARC Industrial/OT Cybersecurity Maturity Model

ARC's industrial/OT cybersecurity maturity model provides a basis for understanding the importance of continuous network monitoring. This model was developed to help companies build and manage effective cybersecurity programs.



ARC Industrial/OT Cybersecurity Maturity Model

ARC's model breaks cybersecurity into a sequence of steps that an organization needs to pass through to establish a program that achieves its risk management goals. Each step addresses a specific, easily understandable, security issue like **securing** individual devices, **defending** plants from external attacks, **containing** malware that finds a way into the control system, **monitoring** systems for signs of cyber compromise, and **managing** active attacks and cyber incidents. Proceeding sequentially through these steps ensures that the program has a solid foundation and the maturity to maintain the integrity of each layer of defense.

Each step has an associated set of people, processes, and technologies that accomplish its goals. Security technologies represent the kinds of solutions that can be used to build the system's security layers. Security management technologies provide the capabilities needed to select, implement, and sustain the effectiveness of spanned security technologies. Companies should have these capabilities in place before the associated security technologies are implemented. Blue and orange colors are used to distinguish

conventional, reactive defenses from the proactive strategies that enable rapid detection and response.

The Role of Continuous Networking Monitoring

Continuous network monitoring is an enabler for every step in cybersecurity maturity. It's asset discovery and inventory capabilities provide the starting point for the actions taken at the Secure level. Advancements to Defend and Contain require its deep understanding of data flows within the system and across system perimeters. Its ability to compare messages with established baselines is the essence of anomaly detection, the additional protection provided by the Monitor maturity level. Continuous message information is also a foundational requirement for the forensic investigation and remediation activities performed in the Manage maturity level.

Continuous network monitoring is an enabler for every step in ARC's Industrial/OT Cybersecurity Maturity model. Implementation of this technology should be on the agenda of every company regardless of cybersecurity maturity level.

To support these diverse requirements, companies need a continuous network monitoring solution with the following capabilities:

- **Non-Disruptive and Comprehensive Monitoring** – Passive, no-impact interaction with control system networks. Monitoring and analysis of all messages regardless of system size and message frequencies.
- **Automatic Asset Discovery** – Automatic detection of control system assets across all networks and sub-networks with no limitation on number or type of assets. Discovery should include collection of detailed information about each device like device type, vendor, model, network address, hardware/software version, and configuration. The solution should also advise of cybersecurity risks associated with assets.
- **Friendly User Interface** – User interface with convenient access to all asset data, connectivity, cyber risks, and anomalous behavior alerts.
- **Industrial Deep Packet Inspection (DPI)** – Ability to parse all IT and industrial protocols and messages used within the control system.
- **Anomaly Detection** – Automatic development and maintenance of "normal behavior" baselines and reliable detection of deviations. Solution should not miss real anomalies nor overburden users with erroneous

alerts. Alerts should include contextual information that operators and defenders need to evaluate and take corrective measures.

- **Easy Integration** – Established integrations or appropriate APIs for other technology solutions, like SIEMs and threat management platforms.

SCADAfence Continuous Network Monitoring

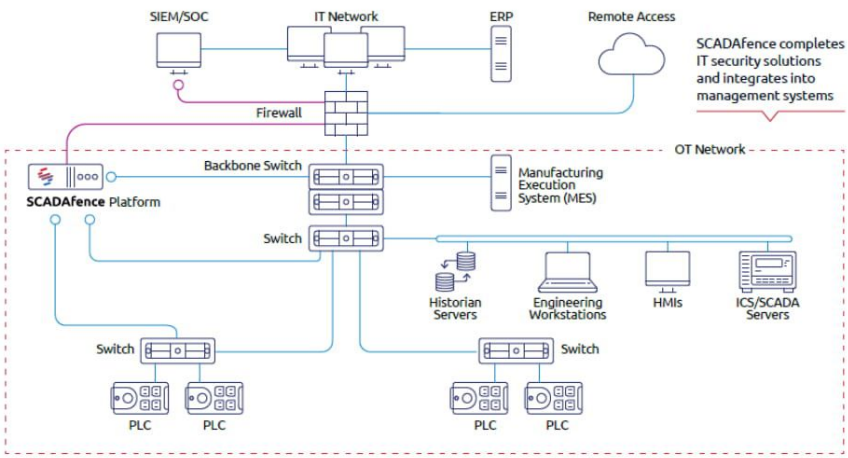
SCADAfence helps industrial companies reduce cyber and operational threats to their facilities. Companies in manufacturing, building management, and critical infrastructure rely upon their SCADAfence platform for security, visibility, and to enable digital transformation.

The SCADAfence Platform is specifically designed for continuous network monitoring in large-scale industrial/OT networks. Companies in manufacturing, building management, and critical infrastructure rely upon this solution for security, visibility and to enable digital transformation.

SCADAfence Platform is a non-intrusive, continuous network monitoring solution for operational technology (OT) networks. It provides automatic asset discovery and inventory management, threat detection, and risk management. According to the company, through a wide range of algorithms, including behavioral analysis and deterministic engines, it detects anomalies and security events that can compromise system availability and affect the safety and reliability of industrial/OT networks and assets. Key features of the product include:

- Automatic discovery and full visibility of industrial/OT asset inventory
- Network mapping and connectivity analysis
- Network dashboard for traffic and security health
- Detection of suspicious activities, exposures and malware attacks
- Operational alerts on asset/service availability and performance issues
- Proactive, actionable warnings of risks and vulnerabilities
- Deep analysis of industrial protocols and industrial equipment activities
- Logical assets grouping and alerts on suspicious traffic among groups
- Automated management level reports

The SCADAfence Platform was designed to integrate seamlessly into existing networks. The platform connects to switch mirror ports (with an option for active polling of configuration and data), and integrates with existing security products via standard industry interfaces.

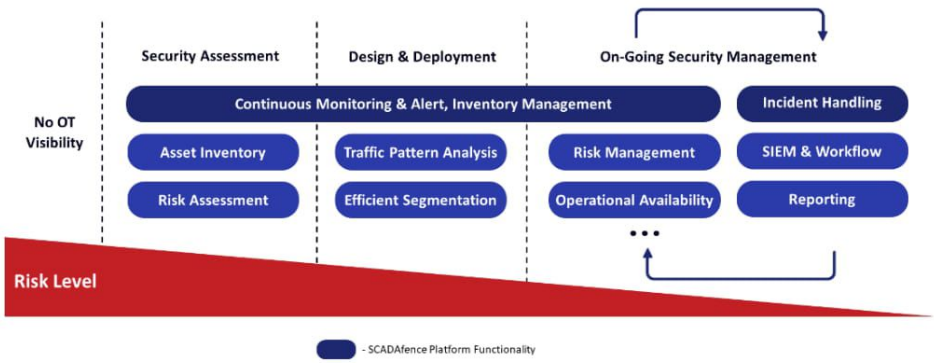


SCADAfence Platform Implementation Architecture

Scalability is a key feature. Industrial/OT systems vary significantly in size and complexity, from hundreds to tens of thousands of cyber assets. Digital transformation is increasing the complexity of every system. Recognizing this, SCADAfence built its platform with features that address the monitoring challenges of large-scale, complex systems:

- More powerful sensors that can support full coverage of large-scale network traffic (no sampling/filtering of communications) and minimize the users' hardware and software costs
- Tailored algorithms that understand large, complex environments, which reduces false positives with increased asset discovery and anomaly detection accuracy
- User interface that enables convenient access to information for tens of thousands of devices

SCADAfence supports users with technology and services throughout their cybersecurity maturity journey. This should help reduce the time and effort needed to develop a reliable asset inventory and data flows that are prerequisites for design and implementation of appropriate security technologies. During implementation, the solution helps security teams monitor progress and maintain updated asset inventories. Following implementation, the solution provides continuous monitoring of the system and alerts operators to unexpected behaviors.



SCADAfence Supports the Security Lifecycle

Conclusion

Operators in critical industries need to ensure that industrial/OT control systems are secure and reliable. Every company needs an Industrial/OT cybersecurity program with the people, processes, and technology maturity to support its cyber risk exposure.

Continuous network monitoring is a foundational technology that can help companies implement and sustain the necessary defenses to reduce cyber risks. It also represents low-hanging fruit, as deployments provide significant, immediate benefits.

This ARC View highlights the features that should be considered when selecting a continuous network monitoring solution. ARC recommends that companies follow the guidance in this report to ensure that the necessary capabilities are implemented. As the review of SCADAfence Platform illustrates, appropriate technology solutions are readily available.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.