ARC VIEW

FEBRUARY 1, 2018

Critical Industries Need Continuous ICS Security Monitoring

By Sid Snitkin

Keywords

Anomaly and Breach Detection, Continuous ICS Security Monitoring, Nozomi Networks

Summary

Most industrial managers recognize that a cyber incident could jeopardize the safety, continuity, and profitability of their operations. Many have invested in basic defensive technologies, like anti-malware software and firewalls, and best practices recommended by automation suppliers and security consultants. This should protect operations from common hackers and may be adequate for low-risk operations that can tolerate disruptions. But it is not enough for critical infrastructure facilities facing the threat of advanced, targeted attacks. These organizations need to continuously monitor systems and investigate any suspicious behavior.

Operators of critical infrastructure need the risk mitigation provided by continuous ICS security monitoring. The potential safety, environmental, compliance, and business continuity impacts of an incident make it critical to avoid all unnecessary risks. Critical infrastructure operations are also targets of sophisticated, well-resourced attack teams that can easily overcome basic cyber defenses.

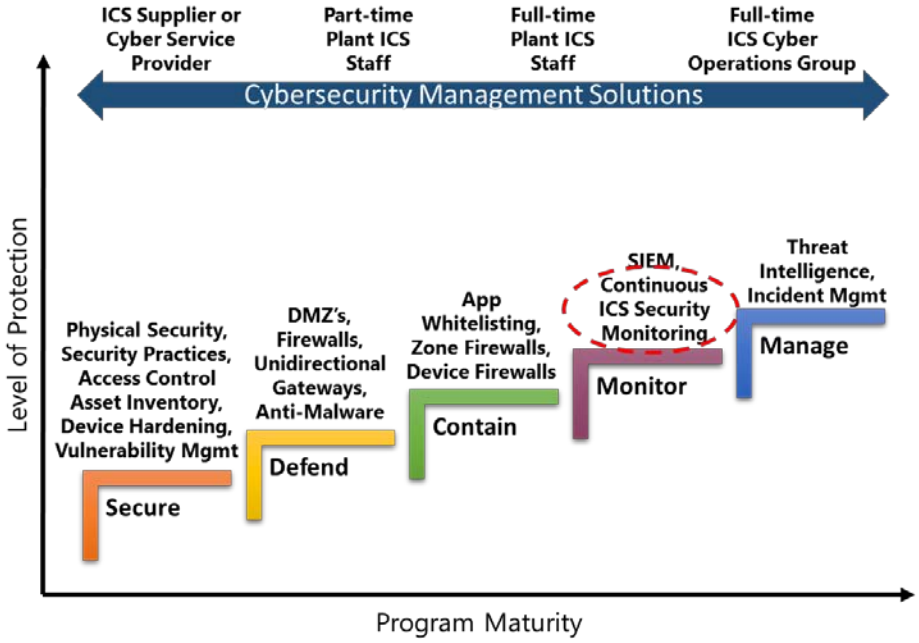
Continuous industrial control system (ICS) security monitoring technologies provide defenders with the visibility needed. While some companies may not be aware of these solutions, others are already integrating them into their cybersecurity management programs. Chief information officers (CIOs), chief information and security officers (CISOs), and active defenders in corporate security operations centers (SOCs) are also interested in the real-time plant security visibility these solutions provide. Suppliers support these needs and are working to extend integration with popular cyber-defense tools.

ARC discussed these issues with Nozomi Networks executives during a recent briefing. As we learned, critical infrastructure operators around the

world use the company's SCADAguardian platform to monitor their ICS cybersecurity in real time and detect threats.

Critical Infrastructure Needs Prudent Cybersecurity

ARC's Industrial Cybersecurity Maturity Model illustrates the importance of continuous ICS security monitoring. We developed this model to help industrial managers understand cybersecurity challenges without having to become cybersecurity experts. It also provides a way for managers to understand cybersecurity investments with respect to cyber risks and the cost-benefits of different technologies.



Continuous ICS Security Monitoring Helps Defend Against Sophisticated Targeted Cybersecurity Attacks

ARC's model breaks cybersecurity into a set of steps that reduce cyber risks incrementally. Each step addresses a specific, easily understandable, security issue. These include securing individual devices, defending plants from external attacks, containing malware that may still get into a control system, monitoring systems for suspicious activity, and actively managing sophisticated threats and cyber incidents. Each step has an associated set of actions, technologies, and resources that can be used to accomplish its goals. Continuous ICS security monitoring is the foundation for level four cyber risk mitigation.

Government and industry ICS cybersecurity guidelines and standards generally focus on getting companies to invest in at least a minimum level of protection against common cyber-attack scenarios. This roughly equates to the first three steps in ARC's model and may be adequate for companies in low-risk industries and regions or those that can tolerate some process disruptions.

Operators of critical infrastructure don't have this luxury. They need the additional risk mitigation provided by the higher steps in ARC's model. The potential safety, environmental, compliance, and business continuity impact of an incident in these operations demands that all unnecessary risks be avoided. Recent incidents, particularly in power networks, show that critical infrastructure operations are also targets of sophisticated, well-resourced attack teams that can easily overcome basic cyber defenses.

Requirements for Continuous ICS Security Monitoring

IT cybersecurity teams have many tools for monitoring the security of business systems. But continuous ICS security monitoring has unique challenges and constraints that typically demand a built-for-purpose solution. Following are ARC's requirements for an acceptable ICS solution:

- **Passive Monitoring** – no impact on the flow of time-sensitive industrial network messages or the operation of individual cyber assets
- **Message Parsing** – ability to parse messages at all seven OSI layers and understand all industrial protocols and commands in a company's ICS. This goes far beyond the deep packet inspection (DPI) in next-generation, IT firewalls
- **Asset Inventory** – support automatic building of a cyber asset inventory, including basic configuration data and message connectivity. Manual collection is impractical in ICS given the size and geographic distribution of cyber assets and the need to detect new devices and connections
- **Anomaly Detection** – automatic detection of suspicious system behavior with a low rate of false positives. This includes identifying ICS and process problems. An ideal solution automatically learns normal be-

havior, helps companies establish a secure baseline, and leverages signature detection to rapidly detect known threats

- **Alerts** – alerting with information about the nature of the suspicious activity and the cyber assets involved. An ideal solution provides incident correlation that combine alerts from a single attack into one incident to speed incident response and minimize operator "alert fatigue"

- **Dashboard** – a user-friendly dashboard that provides a clear overview of system status and enables easy, ad hoc access to all security information and message flows. An ideal solution does this through drillable network diagrams with inquiry capabilities

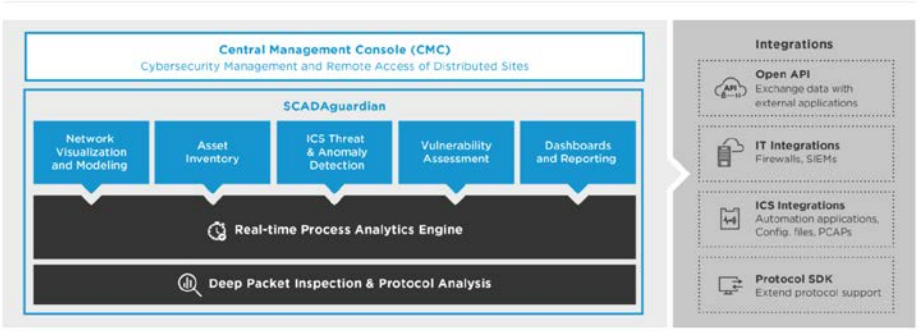
- **Integration** – bi-directional integration with security information and event management (SIEM) and other security applications to enable security teams to compare information from a variety of sources

- **Scalability** – supports all ICS cyber assets regardless of how they are spread across different networks and facilities. An ideal solution provides operational visibility and real-time analysis across multiple geographies or business units

- **Deployment** – supports a variety of deployment options and use by plants, corporate security teams, and third-party service providers

Nozomi Networks Meets ARC's Requirements

The Nozomi Networks solution fulfills all the above requirements for continuous ICS security monitoring. The solution includes two key components: SCADAguardian, which continuously gathers and analyzes real-time messages flowing in control system networks; and, a central management console that aggregates data from multiple sites to provide centralized and remote cybersecurity management.



Nozomi Networks Solution Architecture

The SCADAguardian product has built-in DPI support for a wide range of popular IT and industrial protocols and the company has a protocol SDK to address other parsing needs. SCADAguardian uses sophisticated machine learning analysis methods to help ensure rapid, reliable detection of suspicious activity. This includes artificial intelligence, rules, and signature-based detection of abnormal behavior patterns and process anomalies.

SCADAguardian supports auto discovery with highly visual mapping of industrial assets. This includes identifying devices and vulnerabilities. Results are presented in the system dashboard in a user friendly way that facilitates visibility and enables users to drill down on all asset and vulnerability information. The SCADAguardian dashboards, reports, and alerts are also customizable.

According to the company, the Nozomi Networks central management console scales to monitor thousands of sites and supports various deployment options and hierarchical aggregation of ICS data. The product can also be used as a multitenancy solution for shared or MSSP (Managed Security Service Provider) deployments and very large-scale enterprise deployments.

Integration has been a key focus of Nozomi Networks development efforts. The company has developed interfaces for a wide range of ICS products, networking devices, SIEMs, and popular security management products, like FireEye and Leidos ASM. The company also has an open API for sharing data with external applications. Integrations with industrial firewalls enable asset operators to automatically block attacks.

Conclusion

Operators of critical infrastructure need to do all they can to minimize the safety, environmental, compliance, and business continuity risks related to cyber-attacks. This includes rapidly detecting and remediating system anomalies to minimize the impact of a successful intrusion.

Continuous ICS security monitoring provides the visibility that defenders need to manage today's sophisticated attacks. Our review of Nozomi Networks illustrates that good solutions are available and ARC encourages operators to consider how this technology might improve their cybersecurity program and provide related operational benefits.

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.