ARC VIEW

AUGUST 15, 2019

Users Need Enhanced OT Network Monitoring Capabilities to Support Future Requirements

By Sid Snitkin

Keywords

Continuous OT Network Monitoring, Industrial/OT Cybersecurity, IT/OT Cybersecurity Convergence, Nozomi Networks

Summary

Continuous operational technology (OT) network monitoring has become an essential part of every industrial/OT cybersecurity strategy. It provides the asset and connectivity information users need to build strong defenses. It also alerts users when defenses may be breached. These benefits are enough to justify investments in this technology, but product evaluations should also consider how products support future needs.

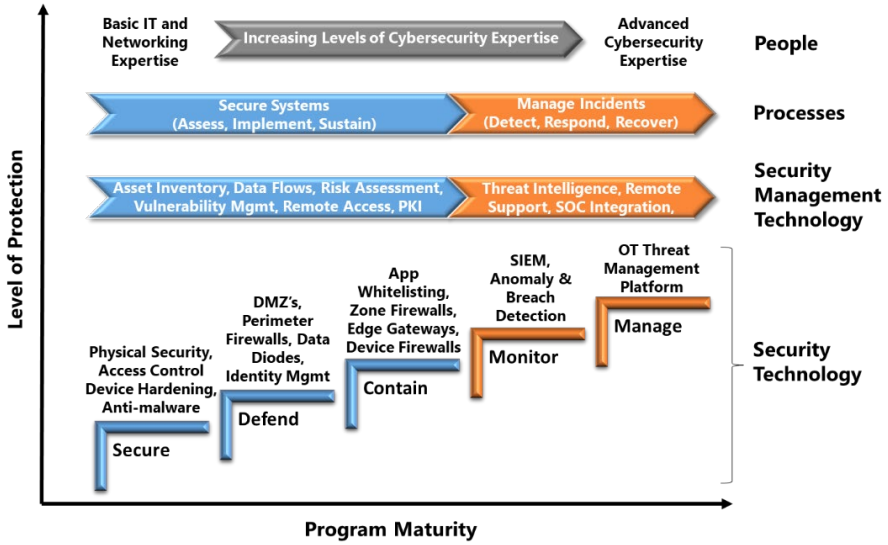
Better asset inventories and rapid threat detection should be enough justification for industrial companies to invest in continuous OT network monitoring. But product evaluations should also consider future developments like IT/OT cybersecurity convergence, external security support, and digital transformation.

Three major developments are changing OT cybersecurity requirements. Increased CISO involvement and IT/OT cybersecurity convergence demands more visibility of OT assets and vulnerabilities. Use of external service providers, like security operations centers (SOC) and third-party, managed security service providers (MSSP), requires more integration of OT and IT cybersecurity tools. Digital transformation initiatives expand the number and types of assets that need to be monitored.

ARC Advisory Group recently discussed these developments and their impact with Nozomi Networks executives. As we learned, the company's continuous OT network monitoring platform is protecting critical infrastructure around the world. Recent product enhancements reflect the company's efforts to support the new developments discussed in this report.

ARC Industrial/OT Cybersecurity Maturity Model

ARC's industrial/OT cybersecurity maturity model demonstrates the importance of continuous OT network monitoring. ARC developed the model 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 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 need these capabilities in place before the associated security technologies are implemented. Blue and orange colors in the model distinguish conventional, reactive defenses from the proactive strategies that enable rapid detection and response.

Continuous OT network monitoring is an enabler for every cybersecurity maturity step. It's asset discovery and inventory capabilities provide the starting point for 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

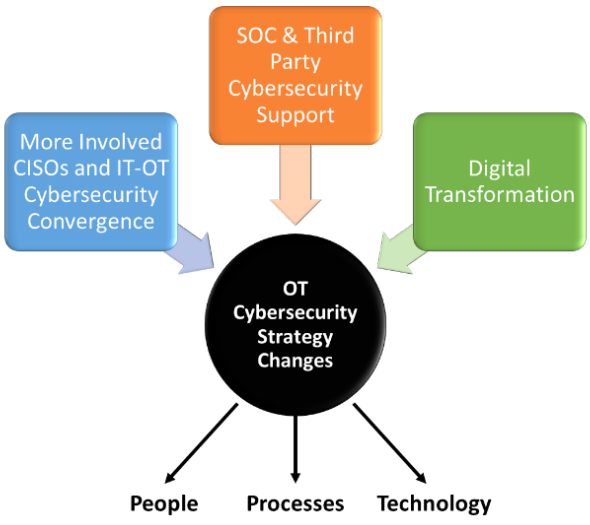
is also a foundational requirement for the forensic investigation and remediation activities performed in the Manage maturity level.

OT Network Monitoring Requirements Are Changing

While there are some differences, all the leading continuous OT network monitoring solutions can support the basic OT visibility and anomaly detection needs of plant cybersecurity teams. But industry developments are rapidly changing the requirements for an effective solution. Selecting a supplier that understands and is addressing these emerging needs is essential.

More Involved CISOs and IT/OT Cybersecurity Convergence

Reports of costly ransomware attacks and nation-state cyber activity have raised cybersecurity concerns among top managers of industrial companies. This is increasing CISO involvement in OT cybersecurity management and creates demand for more visibility into OT cyber risks and monitoring of corporate compliance policies. This also fuels efforts to converge IT and OT cybersecurity programs to ensure end-to-end governance of security across all business processes.



Rapid Industry Changes Require Enhanced Cybersecurity Strategies

While continuous OT network monitoring solutions already collect asset information through passive network monitoring, this is not enough to satisfy emerging visibility requirements. CISOs want the kind of information they get from active scanning, similar to the level of detail and coverage provided by IT network scanning tools. To meet these requirements, OT networking monitoring solutions will need controlled, active scanning that detects dormant devices and provides detailed asset information like active ports, software versions, etc. Ideally, the solution will provide CISOs and IT security teams with a detailed OT cyber risk assessment that includes details on OT vulnerabilities and policy violations.

SOC and Third-party Cybersecurity Support

Maintaining cybersecurity is an ongoing problem for industrial/OT cybersecurity programs. Overwhelmed staffs lack the time and expertise to deal with security updates and system alerts. Limited budgets and the general shortage of OT cybersecurity professionals drive plants to use corporate SOCs and MSSPs for cybersecurity support.

Future developments will require continuous OT network monitoring that includes active scanning, OT cyber risk visibility, integration with IT and SOC cybersecurity platforms, advanced alert filtering, scalable IoT device support, and flexible network monitoring options.

The effectiveness of external cybersecurity support teams is significantly enhanced when OT security management tools, like continuous network monitoring, are integrated with the service provider's preferred cybersecurity solutions. Active OT asset scanning and advanced alert filtering help defenders compensate for OT knowledge gaps. Integration helps ensure that OT threats are addressed promptly. Integration also allows defenders to correlate alerts with information from other sources, like threat intelligence. Active OT asset scanning ensures that defenders can get the detailed asset information they need without disrupting operations. Filtering cyber threats from other system events is essential to avoid security analyst overload and delays in recognizing attacks. Root cause support for alerts can help defenders understand the origin and propagation of malware.

Digital Transformation

Small operating margins and stiff competition require industrial companies to continuously improve performance. They see today's explosion in connectivity, cloud services, and analytics as an opportunity to gain the additional operational insight they need to lower costs and increase productivity. Digital transformation, the umbrella term for these efforts, fuels requests for more access to existing OT data stores and deployment of new, potentially insecure devices.

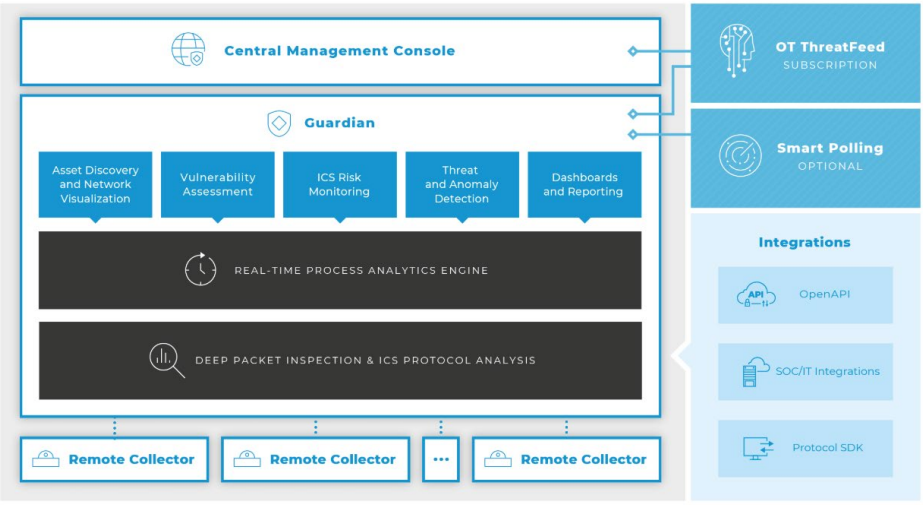
These developments create new requirements for continuous OT network monitoring solutions. Wide deployment of new devices significantly expands the number of assets and network connections that need to be monitored. These devices also use a variety of operating systems and communication protocols that need to be addressed with deep packet inspection (DPI). More complex architectures and new network appliances require more flexible monitoring options. This includes appliances for small

networks, active collectors for networks lacking mirroring capabilities, virtual collectors, and containerized solutions that can be embedded in smart switches and edge gateways.

Nozomi Networks Recognizes the Challenge

Nozomi Networks is a leading supplier of continuous OT network monitoring solutions. Organizations around the world use the company's security platform to protect critical infrastructure. The company's comprehensive set of products reflects its extensive experience in continuous OT network monitoring and understanding of emerging market needs. The Nozomi Networks platform consists of three key elements: Guardian, Remote Collectors, and the Central Management Console.

Guardian performs the bulk of the network monitoring activities. It includes functionality for message parsing, DPI, asset discovery, threat detection, and anomaly detection. This product also supports local users with network visualization, vulnerability assessment, risk monitoring, and security reporting. Guardian supports a wide range of industrial protocols and the company reports that it is already working on support for various IoT protocols. The product also supports use of threat information from the company's OT ThreatFeed subscription service to enhance detection of known threats.



Nozomi Networks Solution Architecture

Guardian acquires network traffic information through *Remote Collectors* that passively extract messages from control system networks. The company offers a range of remote collectors in a variety of physical and virtual forms.

The company also offers an active scanning option, Smart Polling, that enables Guardian to acquire additional asset information and support assets in networks lacking managed switches.

The *Central Management Console* aggregates data from multiple Guardian instances and enables centralized and remote cybersecurity management. According to the company, the Central Management Console can support thousands of sites and various deployment options. The product can also be used as a multi-tenancy 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 OT products, networking devices, SIEMs, popular IT security management tools, and access control products. The company also has an open API for sharing data with external applications.

Conclusion

Many industrial companies are already benefitting from the improved asset inventories and anomaly detection provided by continuous OT network monitoring. While product evaluations should verify that a solution provides these benefits, smart companies will also evaluate how the solution provider supports future developments like IT/OT cybersecurity convergence, third-party cybersecurity support, and digital transformation.

These new developments will impact every industrial company in some way. Adoption will be easier when OT networking monitoring capabilities include features like active scanning, compliance support, integration with SOC and IT applications, advanced alert filtering, and IoT device support. Our brief review of Nozomi Networks demonstrates that some suppliers are already addressing these needs. ARC encourages operators to consider this in selecting an OT network monitoring solution provider.

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.