REPORT REPRINT

Nozomi Networks bulks up SCADAguardian's capabilities

PATRICK DALY

11 JAN 2019

The company rolled out several new features in its latest product release, including an active device querying capability, a threat intelligence subscription, a container-based deployment method and a new UI.

THIS REPORT, LICENSED TO NOZOMI NETWORKS, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR REPOSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

©2019 451 Research, LLC | WWW.451RESEARCH.COM

In November, Nozomi Networks released version 18.5 of its industrial control system (ICS) security offering SCADAguardian. The latest version of the product includes an ICS threat intel subscription, a new user interface, a container deployment option and active querying capabilities to supplement its passive detection. While the active queries were first previewed in August as part of SCADAguardian Advanced (SGA), it was not made generally available until this release cycle.

THE 451 TAKE

The latest version of Nozomi's flagship SCADAguardian product comes at a pivotal time in the development of the ICS security market and reflects several of the trends we are seeing across ICS security and the broader information security landscape. The introduction of active query functionality and an ICS-focused threat intelligence subscription are part of Nozomi's response to rising market demand for more robust capabilities to improve organizations' understanding of their security posture and aid in incident response and remediation. The company's new container-based delivery model is also interesting because it demonstrates a shift to a more agile method of delivering ICS security. Since it can be embedded directly into network switches and firewalls, we may begin to see options rolled out with broader policy enforcement capabilities based on the results of active queries or discovery of known vulnerabilities or threats in the environment.

CONTEXT

After being a relatively slow and sleepy space for several decades, the ICS security market has quickened its pace over the last five years. Increased convergence between IT and OT systems due to the deployment of ICS and supervisory control and data acquisition (SCADA) equipment with stronger computing and communications capabilities has forced ICS network operators and IT ops teams to consider the risks associated with this connectivity.

Recognizing the risks facing critical infrastructure, a market of vendors emerged, with products that could provide visibility into the security posture of an organization's ICS environments. As more vendors have entered the market, the visibility and anomaly detection features that serve as the foundation for many ICS security offerings have become increasingly commodified, forcing vendors to seek differentiation in the form of value-added functions like curated threat intelligence and simplified incident response tools.

PRODUCTS

The SCADAguardian 18.5 release updates the offering's user interface and adds three new components to the company's product portfolio: SGA, an OT threat intel feed and a container-based SCADAguardian deployment option.

SGA adds active query capabilities to Nozomi's arsenal, which the company is calling Smart Polling. The new product is currently being sold separately from the company's standard SCADAguardian product so that customers who are still wary of deploying anything active in their ICS environments can stick with the passive-only approach. The product's Smart Polling functionality provides deeper insight into individual assets' information than the passive-only approach can provide on its own. This includes discovery of asset firmware versions, patch levels and specific vulnerabilities present on a given device. Leveraging the asset-specific information gathered by SGA, customers can improve threat detection, cross-reference vulnerabilities with active threats for a more complete view of their security posture and manage asset configurations. In addition to querying specific devices, Smart Polling can actively scan specific areas of the network to provide security and IT ops teams with information needed for maintenance or incident response.

Nozomi's new OT ThreatFeed subscription provides customers with threat and vulnerability intelligence sourced from a combination of Nozomi's own security researchers and research conducted by the broader ICS security community and the US National Vulnerability Database. In addition to threat signatures, indicators of compromise and zero-day threats relevant for the customer environment, Nozomi includes remediation recommendations in OT ThreatFeed reports. These reports can help to inform security and IT ops teams on the vulnerabilities and threats that may affect their environments, assess the business impact of specific threats and improve their effectiveness in remediating vulnerabilities to reduce the likelihood of a breach or mitigate the damage done by active threats.

Nozomi also added a new container-based deployment model in the 18.5 release, allowing customers to embed SCADAguardian directly into network switches and routers on the ICS network. The new delivery model is partly intended to simplify customer deployment, but also improves scalability. Network operators no longer need to install new appliances (virtual or physical) on the network and new SCADAguardian instances can quickly be spun up if the network architecture changes or a customer builds a new site. The company also claims that the container-based model reduces SCADAguardian's total cost of ownership.

STRATEGY

Nozomi has built a large partner ecosystem over the last several years, primarily opting to partner with vendors on the IT side rather than those on the operational technology side, an implicit bet on continued IT/OT integration. Within the IT space, Nozomi partners with SIEM vendors like Hewlett Packard Enterprise ArcSight, IBM QRadar, LogRhythm and Splunk, MSSPs Atos, FireEye, IBM Security, Leidos and Leonardo, Firewall and NAC vendors Cisco, Check Point, Fortinet and Palo Alto, and several other IT and analytics vendors. These include Atos Codex, an LDAP/AD offering for IoT, BlackRidge Technology, which is used to import SCADA and DCS configurations, analytics vendor Gravwell for improved IT/OT situational awareness and ServiceNow's ticketing system.

COMPETITION

The companies that Nozomi most directly competes with includes Claroty, Dragos, Indegy and CyberX. However, this could be changing soon. ForeScout's recent acquisition of SecurityMatters brings the IT security company firmly into the ICS security market. Depending on the resources that ForeScout allocates to SecurityMatters and how effectively it can integrate the OT and IT sides of its new portfolio, the company may have a compelling value proposition. What's more, ForeScout may serve as a proof of concept for other IT security vendors thinking about acquiring their way into the ICS security market – if the acquisition generates positive value for the company, other IT security vendors may follow suit. Nozomi's broad range of IT partnerships and integrations and its long-standing focus on IT/OT integration would be very helpful in competing against IT security vendors with newly acquired ICS security assets.

Among Nozomi's current competition, the battleground is in building up value-adding security functions on top of the base visibility and anomaly detection that many ICS security vendors start with. Nozomi has done this by adding new deployment options, building out active search functionality with SGA and incorporating a threat intel subscription into SCADAguardian 18.5. This is on top of product enhancements from its last releases, including hybrid threat detection using YARA rules. However, Nozomi is not alone in building such functionality into its product. Many of its competitors have added improved functionality for threat intelligence, vulnerability management and incident response, and many have either begun to or already offered active queries in their products. Whichever of these vendors does the best job of integrating functions that simplify and improve the efficiency of OT security operations will likely emerge as the leader in this market.

SWOT ANALYSIS

STRENGTHS

SGA's Smart Polling capabilities offer customers far more advanced forensic device information than was previously capable with the passive-only approach and the container-based delivery model improves the company's agility in deploying and scaling SCADAguardian within customer environments.

WEAKNESSES

While having many IT-centric partnerships will be helpful as IT/OT convergence in ICS continues, Nozomi could benefit from adding more partnerships around OT analytics and industrial automation.

OPPORTUNITIES

Nozomi can begin exploring the ways that its offering can more tightly integrate with firewalls and network switches, such as for policy enforcement or network segmentation, now that its product can be embedded directly into the equipment as a container.

THREATS

Large IT security vendors like ForeScout coming into the market with a value proposition for combined IT and OT network security from a single provider may be a headwind for Nozomi's growth opportunities.