Fortinet and Nozomi Networks Secure Industrial Control Systems Through Joint Partnership

Collaboration Brings Sophisticated Security Solutions to Critical Infrastructure Operators as Frequency of Cyber attacks Increases

"The cybercrime world is expanding with each passing day and has led to a growing threat for global critical infrastructure systems. The convergence of IT and critical infrastructure requires operators and government agencies to apply robust security solutions that can scale and accommodate the complex interactions between IT and physical processes within these environments. Together with Nozomi Networks, we are providing the most complete Security Fabric designed to support the full range of industrial installations bringing seamless protection to critical infrastructures worldwide," Patrice Perche, senior executive vice president, Worldwide Sales and Support, from Fortinet said.

Fortinet, the global leader in high-performance cyber security solutions, and Nozomi Networks, a leading provider of real-time visibility and advanced monitoring capabilities for industrial networks, are collaborating to provide a new and innovative security solution for Industrial Control Systems (ICS).
[if !supportLists]· [endif]Nozomi's SCADA guardian and Fortinet's Security Fabric deployed together provide ICS customers with comprehensive cybersecurity protection, from real time anomaly detection to swift corrective action.
[if !supportLists]· [endif]SCADA guardian non-intrusively detects anomalies and suspicious behavior in the ICS network and alerts Fortinet's FortiGate enterprise firewalls to block the suspicious traffic, optimizing industrial operational efficiency by preventing system downtime and data loss.
[if !supportLists]· [endif]Fortinet's Security Fabric is an intelligent and adaptive architecture designed to deliver distributed security for protections against threats from the Internet of Things (IoT) and remote devices, through the infrastructure core, and into the cloud. It also enables the implementation of end-to-end segmentation and other innovative security strategies for comprehensive threat protection to help industrial customers protect their critical assets across the

expanding attack surface.
[if !supportLists]· [endif]Fortinet's Advanced Threat Protection (ATP) framework enables dynamic generation of local threat intelligence and automated response coupled with FortiGuard services for global threat intelligence protections.

Andrea Carcano, founder and CEO of Nozomi Networks states that, "when you combine Nozomi Networks' non-intrusive anomaly detection with Fortinet's in-line enforcement and network segmentation capabilities, the integrated solution enhances visibility and security beyond what each product could do on its own. This collaboration provides our joint customers with a comprehensive and proactive SCADA security solution enabling them to deploy the most robust ICS security solution on the market today."

Unparalleled Combination of Detection and Security for Critical Infrastructure

Research indicates that critical infrastructure organizations are under a state of constant cyberattack. As these attacks get more sophisticated and increase in frequency, infrastructure operators from utility companies, transportation groups, natural resource producers, and more, must solve security gaps that will continue to grow wider over time.

In part, this is a consequence of the inevitable convergence of Operational Technology (OT) with Information Technology (IT), leaving industrial control systems (ICS) exposed to the same security breaches experienced by IT networks. However, while the impact of a security breach on most IT systems is limited to financial loss, attacks on ICS have the added potential to destroy equipment, threaten national security, and even endanger human life.

Much of the underpinning technology of ICS, while extremely robust and reliable, was never designed to be accessible from remote networks. Solving ICS security issues requires a holistic approach that unifies the best of current IT network security capabilities with an extensive understanding of ICS processes and protocols.

Industrial customers will benefit from the combination of Fortinet's

extensive cybersecurity infrastructure expertise and Nozomi Networks' deep understanding of ICS networks, protocols and device behaviour. Together, Nozomi Networks and Fortinet will help industrial customers to better protect their critical assets from both cybercriminals and employees that unintentionally leave ICS systems vulnerable.

[if !supportLists]· [endif]Fortinet's Security Fabric enables granular security policies that can be enforced based on criteria such as user identity, application, location, and device type.
[if !supportLists]· [endif]FortiGate's end-to-end segmentation capabilities implemented throughout the ICS network can provide greater visibility and scale to large ICS deployments making them even more secure.
[if !supportLists]· [endif]Fortinet's Advanced Persistent Threat Protection Framework detects and analyzes advanced attacks that might bypass more traditional signature-based defenses.
[if !supportLists]· [endif]FortiGate's rugged next-generation firewalls are built to withstand the extreme temperatures, harsh climates and hazardous locations that are common in remote ICS environments.
[if !supportLists]· [endif]Nozomi SCADA guardian is a network monitoring and protection solution developed specifically for ICS. An integrated discovery and learning capability for ICS, it facilitates the creation of tailored security profiles and automatically detects critical anomalies. Additionally, underlying industrial processes are constantly monitored at the deepest level through an innovative Industrial Virtual Image Technology.