The Challenge with Industrial Control Systems (ICS)

Industrial Control Systems (ICS) including Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), Programmable Automation Controller (PAC) and Distributed Control Systems (DCS) have increasingly come under attack. Industroyer-CrashOverride, WannaCry, BlackEnergy and STUXNET are examples of malware that have negatively impacted ICS systems with significant consequences. The questions that should be asked are why this is happening and should we be worried? Quite simply, these attacks indicate the vulnerability of ICS networks and the potential damage to the critical infrastructure that relies on them.

ICS systems were initially designed at a time when Operational Technology (OT) networks were analog, proprietary systems with little to no connectivity to the outside world. They were secured via relative isolation, often referred to as “air gapped” and “security by obscurity.” However, the advantages of leveraging common Internet protocols, combined with the ease and cost saving of using Windows-based terminals such as HMIs and SCADA Masters brought OT networks on a collision course with traditional IT systems and associated security risks. Two key issues with this transformation prevail. First, ICS networks involved with critical infrastructure can’t afford any unexpected outages—a.k.a. unplanned downtime—even for unscheduled maintenance or basic update patching, leaving the Windows-based terminals vulnerable. The second issue is that those serial protocols of ICS systems which were merely encapsulated in TCP/IP have no security features built into them, like basic authentication or encryption, again a fundamental vulnerability.

Once interconnected with a corporate network, ICS systems are exposed to the same potential cyber threats and damage that we see with regular IT security breaches (financial loss, data theft, etc...) but with an additional layer of operational disruption risk that has national security implications and/or the potential for safety risks, even loss of life. For example, according to the Federal Office for Information Security in Germany, a targeted attack in 2014 on a steel mill using spear phishing e-mails coupled with social engineering first enabled access to the steel mill’s IT network which then led the hackers to the OT network. The impact was an uncontrolled shutdown of a blast furnace, causing massive damage and downtime, along with significant safety risks. Unplanned outages minimally involve damages in the hundreds of thousands in equipment repair and typically escalate to hundreds of millions in lost revenue.

Solving these issues requires a solution that unifies the best of IT network security policy enforcement, risk management and capabilities with a core understanding of ICS priorities, processes and protocols.

MARKET DRIVERS

- As the backbone of critical infrastructure, ICS is ubiquitous in all industries including Energy, Electric, Water, etc...
- ICS networks are vulnerable and exposed to IT security threats
- ICS security incidents have increased in frequency with disastrous results including loss of life, major outages, billions in lost revenue, and large scale infrastructure damage

SOLUTIONS HIGHLIGHTS

- The Fortinet – Nozomi Networks solution combines sophisticated detection of ICS security issues with proactive threat remediation and containment
- Fortinet offers products for environmentally controlled and non-environmentally controlled facilities; which include the FortiSwitch, FortiGate, FortiManager, FortiAnalyzer and FortiSIEM
- Nozomi SCADAguardian protects the entire OT inside system and this tool works in tandem with Fortinet in quarantining and blocking malware
THE FORTINET-NOZOMI NETWORKS JOINT SOLUTION TAKES ON THE ICS SECURITY CHALLENGE

Fortinet and Nozomi Networks are collaborating to provide ICS environments with a holistic and comprehensive security platform. The solution combines Nozomi Networks’ SCADAguardian and its deep understanding of ICS networks, protocols, and device behavior with Fortinet’s extensive security product for OT/ICS/SCADA Systems. SCADAguardian’s non-intrusive ICS protocol monitoring capabilities profile the behavior of industrial devices with embedded artificial intelligence (A.I.) to detect anomalies in the ICS network in real-time. It works closely with Fortinet’s FortiGate and FortiSIEM as part of the Fortinet’s Security Fabric to respond and provide a secure gateway between the OT and IT networks.

Designed to minimize system downtime and limit data loss, the Fortinet-Nozomi Networks solution optimizes productivity and business continuity in industries reliant on ICS networks. How do we do this? By placing a Nozomi Networks SCADAguardian appliance in the OT network, it will passively monitor the network traffic creating an internal representation of the entire network, its nodes, and the behavior of each device in the network. If an anomaly or suspicious behavior is detected, an alarm is generated and sent to security operators and network administrators. At the same time, SCADAguardian is capable of automatically modifying the right policy in FortiGate to block the suspicious traffic. However, to scale the solution deeper into an ICS network, a tiered architectural approach is needed.

FORTINET AND NOZOMI NETWORKS TAKE ICS SECURITY TO THE NEXT LEVEL

With the adoption of standard IP networking, the typical ICS network followed normal networking conventions which meant that it was relatively flat and open. This lack of segmentation meant that once a threat can get into the system, it could move at will, increasing the amount of damage it could cause. IT networks address this issue by using Firewalls to segment their internal networks so that malware can be contained to only a portion of the network. This same protection can be applied to ICS networks by deploying FortiGate/SCADAguardian pairs deeper into the ICS network, as shown in Figure 2, scaling the solution across the whole of the ICS network and providing a greater granularity of protection.

Fortinet’s Security Fabric enables SCADAguardian integration with Fortinet’s extensive security offering, bridging the gap between IT and OT networks. For facilities like manufacturing plants that have numerous end devices and require real-time information, a FortiHypervisor could be incorporated with the FortiSIEM and SCADAguardian to meet this real-time information requirement.

In short, the active integration between SCADAguardian and Fortinet Security Fabric products provide ICS networks with the most comprehensive security solution available and enables optimum efficiency within, and beyond, the Industrial network.
SOLUTION BRIEF: FORTINET & NOZOMI NETWORKS ICS CYBERSECURITY SOLUTIONS

FIGURE 2

Centralized Management of Distributed SCADAguardian Appliances

Network Visualization and Modeling
Asset Inventory
ICS Anomaly, Intrusion and Risk Detection
Vulnerability Assessment
Dashboards and Reporting

Real-time Process Analytics Engine

Deep Packet Inspection & Protocol Analysis

FIGURE 3: SCADAGUARDIAN SOLUTION DIAGRAM
FORTINET SECURITY FABRIC COVERS YOUR ENTIRE NETWORK

BROAD COMPLEMENTARY SOLUTION PORTFOLIO

GLOBEAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.9897.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding. Fortinet reserves the right to change, modify, transfer or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.