SOLUTION BRIEF

Fortinet and SCADAfence OT Security Solution

Broad, Integrated and Automated Solution with Extended Visibility, Threat Detection and Policy Enforcement from IT to OT

Executive Overview

IT and operational technology (OT) are converging as the Industrial IoT revolution makes inroads into the manufacturing, critical infrastructure and building management industries. As part of the IT/OT convergence, air gapping is no longer a relevant strategy, since connectivity between OT networks and external environments has become a necessity – that significantly increases the exposure of critical operational systems and devices to cyber-attacks. To address the growing cyber threats, organizations are shifting their focus from air gaps and isolation to securing interconnected OT networks. These organizations are focused on integrating dedicated OT security solutions with their existing IT security architecture and processes.

SCADAfence and Fortinet have established a technology partnership to help organizations address OT security challenges. SCADAfence provides threat protection, risk management and visibility solutions for OT networks. Combining SCADAfence's dedicated OT security solutions with Fortinet's Security Fabric allows organizations to effectively enforce security policies, improve incident response and extend their visibility from IT to OT.

Security Fabric Components:

- FortiGate Enterprise Firewall
- FortiSIEM

Joint Solution Benefits:

- Integrate IT-OT security frameworks and processes
- Accurate asset discovery and inventory management across IT and OT
- Insights from SCADAfence platform for policy enforcement with the Fortinet Security Fabric
- Automation in OT for increased incident response efficiency and reduced response time

The Joint Solution

The joint solution of the Fortinet Security Fabric and SCADAfence empower OT security teams with enhanced control and improved resilience over their OT networks. With its deep understanding of the unique characteristics of industrial equipment and communications, SCADAfence provides administrators with visibility into their OT networks and allows them to better manage their cyber risks.

SCADAfence's platform monitors OT networks non-intrusively by passively analyzing industrial protocols and polling data from industrial control systems. The platform automatically discovers the assets in the OT network and digitizes the asset inventory. Then, it applies a combination of algorithms and behavioral analytics to detect cyber-attacks, policy violations, and other anomalous behaviors. Early risk detection allows OT security teams to be proactive and take action – thus preventing future incidents.

Once an incident is detected by SCADAfence, detailed information on assets such as device type, vendor, model, network address, hardware/software version, vulnerabilities and configuration, and alerts regarding malicious activities in the OT networks are sent to Fortinet, speeding an incident response aimed at containing threats and reducing risks. The integration also allows the optional ability to automate or semi-automate rule configuration and therefore reduce incident response time by improving the efficiency of processes. In addition, the SCADAfence platform enriches the information about OT devices in Fortinet's solutions, increasing OT asset inventory accuracy and extending visibility from IT to OT. Such integration allows security teams to leverage a deeper understanding of their OT network's security status into existing systems and procedures.

Use case 2 - FortiGate Enterprise Firewall

Prevention of internal threats using perimeter security controls of FortiGate Enterprise Firewall. By leveraging early detection of threats based on anomalies in the internal OT network, the combined solution can identify the infected systems and block their communications with external networks before any attempts to connect with C&C servers.

Use case 1 - FortiSIEM

Accelerating incident response and management by combining alerts and asset details from the internal OT networks with enterprise-wide security controls and information using FortiSIEM. Centralized information and management allows the security analysts to rapidly detect IOCs, identify the rootcause of issues, remediate threats and enforce security policies.

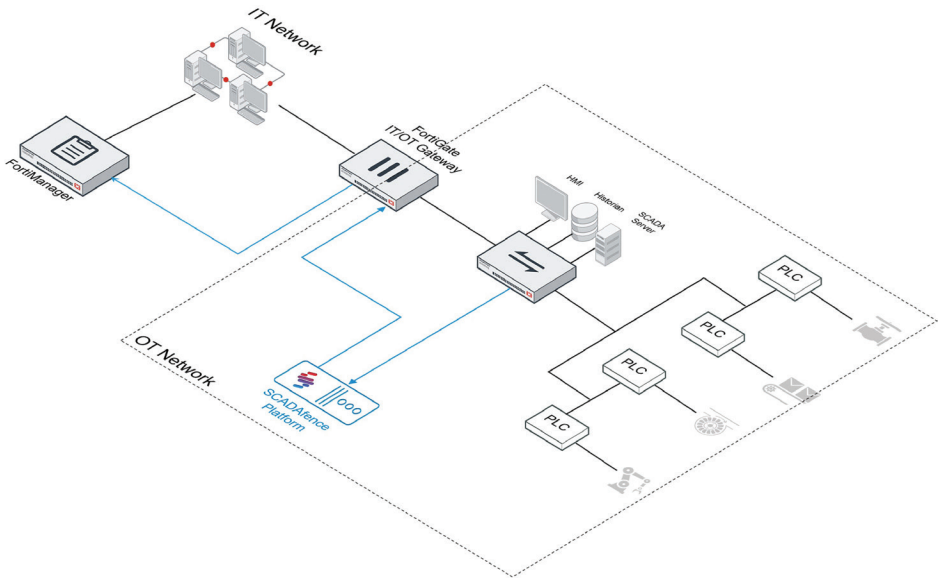

Figure 1: SCADAfence and Fortinet - unified IT/OT security.

Solutions Component

Fortinet Security Fabric

The Fortinet Security Fabric delivers a unified approach that is broad, integrated, and automated. FortiOS 6.2, the latest version of Fortinet's security operating system, powers the entire Security Fabric, helping customers reduce and manage the attack surface, prevent advanced threats, and reduce complexity. In addition to integrating Fortinet products and solutions, the Security Fabric includes prebuilt application programming interface (API) connections that ensure deep integration across all of the Security Fabric elements.

SCADAfence Platform

The SCADAfence platform continuously monitors OT networks and provides cybersecurity and visibility for ICS/SCADA networks. SCADAfence provides automatic asset discovery and inventory management, threat detection and risk management. Employing a wide range of algorithms, machine learning, and AI, it detects anomalies and security events that can compromise the availability and reliability of the OT network and its assets. SCADAfence is the only solution in the market that is able to support the unique requirements of large-scale industrial networks from a size, complexity and coverage perspective while maintaining an affordable TCO.

About SCADAfence

SCADAfence helps companies with large-scale operational technology (OT) networks embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. Our non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience. SCADAfence seamlessly integrates OT security within existing security operations, bridging the IT/OT convergence gap. We deliver security and visibility for some of the world's most complex OT networks, including Europe's largest manufacturing facility. Thanks to SCADAfence, companies in manufacturing, building management and critical infrastructure industries can operate securely, reliably and efficiently as they go through the digital transformation journey. Learn more at www.scadafence.com

FORTINET

www.fortinet.com

August 14, 2019 12:03 PM

465005-0-0-EN

D:\Fortinet\Work\2019\August\081419\sb-scadafence