Gigamon®

SCADAfence

Joint Solution Brief

Monitoring and Visibility for Smart Manufacturing

The Challenge

The increasing adoption of IT technologies, as part of the Industrial IoT/Industrie 4.0 revolution in industrial (ICS/SCADA) networks provides many benefits for manufacturing companies. The connectivity between the IT and OT (Operational Technologies) environments exposes the shop floor in smart manufacturing environments to emerging cyber threats such as operational downtime, product manipulation and theft of sensitive manufacturing information.

Integrated Solution

By integrating SCADAfence's Industrial Continuous Network Monitoring solution with Gigamon's GigaSECURE® Security Delivery Platform, security personnel can get holistic visibility and advanced detection capabilities that allow them to take control of their industrial environment. All this is done in real-time with a passive and low-risk solution.

Key Benefits

- Detect a variety of cyber attacks, from previously-known malware and disclosed vulnerabilities to new, sophisticated attack vectors
- Monitor and detect non-malicious operational threats such as misconfigurations and human errors
- Increased, industrial protocol context-aware, network visibility including automatic asset discovery, asset inventory and network topology
- Enhanced and faster response to events while determining root cause to minimize reoccurrence

Introduction

These days, industrial OT environments such as ICS/SCADA networks are no longer isolated from the outside world. With the adoption of Industrial IoT and other new technologies, today's day-to-day shop floor operations are more productive, easier to manage and most importantly, more cost-effective to operate. However, while providing many benefits, these technology changes have exposed mission critical systems to a new threat, cyber attacks.

Traditional IT technologies were not designed for OT environments and therefore do not fit the unique requirements they demand. This leaves smart manufacturing networks in industries such as pharmaceutical, chemical, food & beverage and automotive almost completely unprotected and unmonitored.

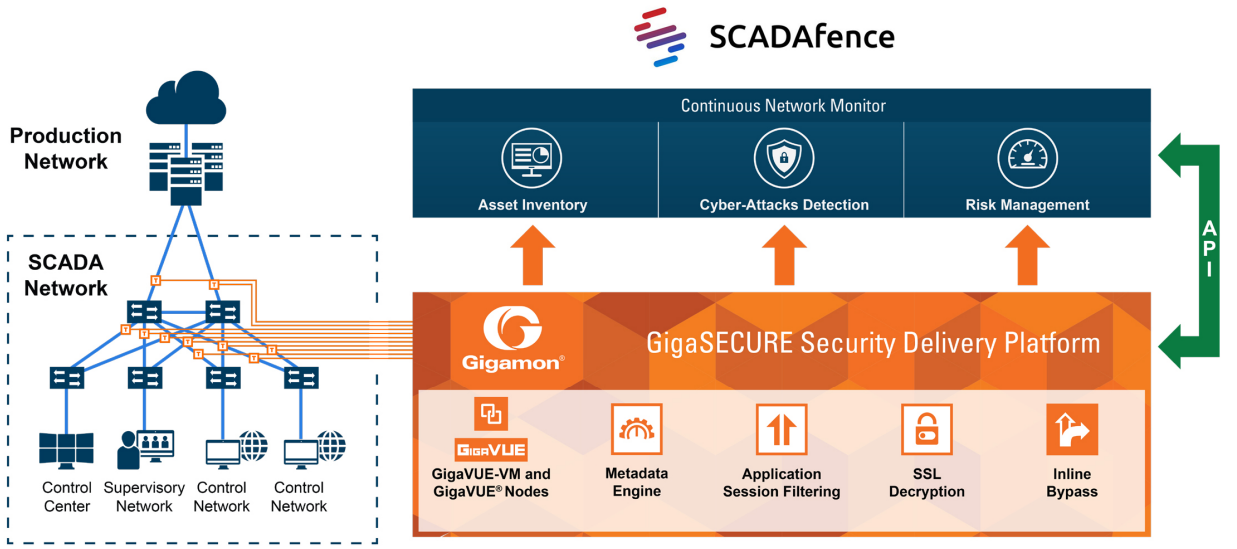
Events such as operational downtime, product manipulation and sensitive information theft can significantly impact companies in these industries. Today, pinpointing the root causes of these events is often difficult, making it hard to differentiate between malicious cyber attacks and operational non-malicious events; which means that repetitive incidents are almost inevitable.

The Gigamon and SCADAfence Joint Solution

SCADAfence and Gigamon have partnered to provide continuous passive monitoring for industrial networks in manufacturing industries. The joint solution provides IT and OT personnel with alerts on abnormal activities that jeopardize the operational continuity of the production network. In addition, the solution provides broad visibility into the day-to-day activity of the industrial environment allowing for various security and architecture flaws to be discovered using the SCADAfence dashboard and alert system.

Industrial networks are getting more complex and more dependent on standard Ethernet communication infrastructure. The joint solution leverages Gigamon's GigaSECURE capability to aggregate network traffic from across the ICS/SCADA environment. The Gigamon solution collects traffic from various sources in the network (using network taps or, if necessary, SPAN port data), ensuring traffic is monitored. If duplicate packets are captured due to the capture topology, traffic streams can be de-duplicated before analysis. The entire collection and aggregation process is done using passive and low-risk technologies and without posing risk to the industrial environment.

The network traffic gathered by the Gigamon solution are then passed to the SCADAfence continuous monitoring solution. This analyzes the internal communications and performs deep packet inspection (DPI) to understand the context of the industrial protocols that are in use. This analysis immediately starts



to provide the administrators with visibility into the day-to-day activity, including automated asset discovery and inventory, and network topology mapping. The solution will alert on a variety of events such as cyber attacks, from previously-known malware and disclosed vulnerabilities to new, sophisticated attack vectors, and non-malicious operational threats such as misconfigurations and human errors. By using the SCADAfence dashboard, administrators can quickly respond to alerts generated using forensics tools designed to improve accuracy and reduce the response time.

The joint solution gives operators visibility and understanding of their industrial SCADA networks in a non-intrusive manner, providing better insights into what is causing issues on the network and increasing operational efficiency.

Learn More

For more information on the SCADAfence and Gigamon solution, contact:

SCADAfence
www.scadafence.com

Gigamon®
www.gigamon.com

3195-01 06/16

Gigamon®
3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com