SCADAfence RAPID7

Joint Solution Brief

Advanced Non-Intrusive Monitoring

Continuous Monitoring of OT Networks

Table of Contents

How the SCADAfence Platform Protects OT Networks……2

The Most Advanced Non-Intrusive Monitoring in the Industry……3

The Highest Detection Rate With 100% Packet Analysis……..3

The Most Flexible and Cost-Effective Deployment Options……3

Minimum False Positives with SCADAfence's Micro-Granular Baseline……..4

Detailed Asset Inventory……5

The Asset Manager's Analysis Tools……..6

Asset Inventory Customization……..6

The Advantage of Device Profiling……6

Value Level Tracking & Profiling……7

Asset Vulnerability Management……..7

Asset Exposure Management……7

The Integration with Rapid7……..8

Asset Inventory Integration……...8

SCADAfence

RAPID7

How The SCADAfence Platform Protects OT Networks

The SCADAfence Platform provides an ongoing monitoring solution that first automatically discovers the assets and their roles in the network, and then provides visibility into their behaviors. The SCADAfence Platform provides real-time protection from malicious and non-malicious activities and network and service failures.

The SCADAfence Platform employs a wide range of algorithms and mechanisms, to detect anomalies and negative events that can compromise security, safety and reliability of the OT network and processes. It focuses on the following main aspects of OT network's security and resiliency:

Ongoing Asset Inventory Management

The SCADAfence Platform automatically discovers the assets in the network. It enables system administrators to monitor the assets behavior, traffic patterns and detect any anomalous behavior. The SCADAfence Platform identifies changes in the network architecture and alerts on any addition or removal of devices. This helps identify issues with the OT system's security and availability.

Ongoing Protection from Malware, Malicious or Accidental Actions

The SCADAfence Platform can detect from the basic until the most advanced attack scenarios. It has a comprehensive understanding of malicious activity profiles and ways of action, combined with deep packet inspection of network and industrial protocols. The SCADAfence Platform can also identify attack and misuse attempts, as well as accidental actions in the network, which can prevent one of the most dangerous and costly types of security incidents.

The SCADAfence Platform can detect device behavior that is typical to malware and ransomware, and alert on suspicious communications. This can help prevent spread and activation of these malicious pieces of code and prevent critical situation of ransom demands and halts in production.

The SCADAfence Platform can detect services that stopped to respond to traffic requests, devices that disappeared from the network, industrial protocols 'shut down' commands and many more. This can significantly reduce downtime and maintain continuity of production processes.

The Most Advanced Non-Intrusive Monitoring in the Industry

The SCADAfence Platform has been designed with a non-intrusive nature in mind. This means that the platform was built to optimize the information obtained from passive network monitoring, without the need of active polling. This includes very detailed asset information and traffic patterns. The SCADAfence Platform uses an advanced Deep Packet Inspection engine that also understands native OT protocols.

The Highest Detection Rate With 100% Packet Analysis

The SCADAfence Platform doesn't sample or filter traffic. It performs deep packet inspection to all packets, with the highest performance in the industry. This translates to the most accurate detection of network assets and events, even if they originate in a small number of packets.

The Most Flexible and Cost-Effective Deployment Options

The SCADAfence Platform provides continuous monitoring of the OT network. It is a transparent device and has no fingerprint in the environment, therefore it does not have any impact of the day-by-day production processes.

The SCADAfence Platform also has the widest range of deployment options supported: SPAN, RSPAN, VSPAN, TAPs, remote sensors and also unique NetFlow based monitoring which provides very cost-effective deployment options.

Smart Sensors: When sensors are required to monitor distributed parts of the network, the SCADAfence Platform supports "Smart" sensors, that perform local analysis of the information, (unlike other solutions that forward mass amounts of traffic to the central server, overloading the network). This is optimized for remote low bandwidth or slow connections, that otherwise would be impossible to monitor.

NetFlow Analyzer (sensor-less deployment): The SCADAfence Platform introduced the NetFlow Analyzer feature (starting in version 6.0). This feature allows organizations to skip the deployment of expensive sensors in each and every segment, and thus be able to monitor remote segments in an "agentless" cost effective manner. This is done by configuring supporting network infrastructure to send NetFlow data into a SCADAfence sensor.

The NetFlow data enrichment occurs inside the SCADAfence Platform in a way that is transparent to the user, adding assets, connections and statistics. This also integrates with all of SCADAfence's anomaly detection and vulnerability detection engines.

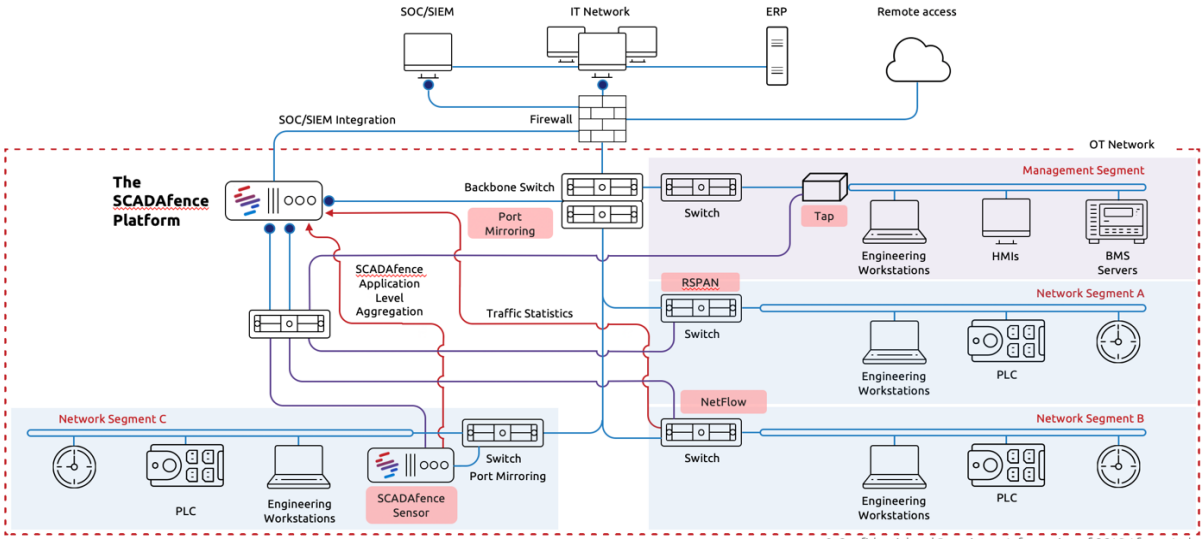

Diagram 1: The SCADAfence Platform's flexible deployment options

Minimum False Positives with SCADAfence's Micro-Granular Baseline

At the heart of the SCADAfence's Platform anomaly detection engine, one can find its award winning unique Micro-Granular baseline. The SCADAfence Platform creates a baseline of the network behavior, and employs AI algorithms to detect deviations from this baseline. It is unique by addressing each network asset independently. It is self-tuning and automatically adapts to changes in the network, thereby reducing the number of false positive alerts. It does not require extensive configuration, restarts or re-learning.

Another important advantage is that the industry leading anomaly detection algorithms provide value in a matter of days (even 24 hours), and not in weeks or months. The network administrator can see alerts immediately after the deployment. This makes the SCADAfence Platform usable in networks with a wide range devices, high loads and diverse traffic.

SCADAfence's Micro-Granular Baseline has the following advantages:

Minimum False Alerts – The granular and adaptive baseline minimizes the number of false alerts, making the SCADAfence Platform usable and trustable. The larger the network, the number of events grows exponentially, and thus makes this issue a critical one.

No User Configuration Required – The SCADAfence Platform can be deployed in the network quickly and with minimal effort. There is no need for a lengthy analysis and expert tuning.

Immediate Detection – Due to its design characteristics, the Micro-Granular baseline can detect anomalies in a matter of one to two days, and not weeks or months as with other solutions.

Continuous Coverage, No Stops/Restarts – As the baseline is adaptive and not arbitrarily set, there is no need to stop the baseline and re-learn. There is no longer a need for effort and time-consuming stop/restarts which make the SCADAfence Platform unusable for large periods of time and increases network exposure and risks.

More details on the baseline can be found here: https://www.scadafence.com/platform-technology/

Detailed Asset Inventory

The SCADAfence Platform automatically generates a detailed asset inventory of all devices connected to the network, including PLCs, HMIs, servers, and workstations. This is done without prior knowledge or user configuration and provides insight on important changes such as new device connections, device failures and changes done to the devices.

The SCADAfence Platform employs advanced AI to automatically determine the types of the devices and is able to provide an accurate inventory, as well as advanced security analysis of the network traffic patterns.

Internal Asset Structure

The SCADAfence Platform analyzes the OT industrial protocols and provides accurate information on the assets' internal structure. For example, PLC's with multiple rack slots.

Assets Behind Assets

Some OT network topologies include assets that are located behind certain gateways. Their traffic is often encapsulated in the gateway communication. The SCADAfence Platform is able to detect such communications, extract the encapsulated information and provide the users with full information on the network topology.

Deep Layer 2 Traffic Analysis

Often, OT networks include Layer 2 traffic on top of Layer 3, and send valuable information over it. The SCADAfence Platform is able to analyze Layer 2 communication and extract detailed information on Layer 2 assets such as switches and other equipment. The Layer 2 industrial protocols are presented on dedicated views in the UI.

The Asset Manager's Analysis Tools

The SCADAfence Platform's Asset Manager module provides tools to efficiently analyze the assets and detect changes in the inventory.

Assets Pivot Table – The unique dynamic table view enables the network administrator to analyze the asset inventory, based on configurable parameters such as vendor, type or OS.

Alerts on Changes on Misconfigurations of The Asset Inventory – The SCADAfence Platform alerts the administrator on new assets, missing assets, and assets with unsecure or misconfigured properties (such as multi-homed servers, duplicate IPs, and many more).

Alerts on Strange Behaviors – The SCADAfence Platform also alerts on assets strange behaviors that can indicate on security risks or network misconfigurations (such as communication attempts to unidentified ports or IPs, scans, and more).

Asset Inventory Customization

The Asset Manager enables users to add their own data to the asset inventory. Details such as physical asset location, owner or criticality can be easily added – manually or by automated process.

This data is integrated in the SCADAfence Platform's security engines. The security engines take this information into consideration when further analyzing the network.

Integrations - All asset inventory is exportable (and importable) by CSV or via REST API to external systems. This allows even further correlation and analysis with external systems.

The Advantage of Device Profiling

On top of the above automatic device type detection, the SCADAfence Platform further enhances the asset discovery ability by building device profiles. This enables it to classify devices that are relatively silent or do not provide identification information.

The SCADAfence Platform's AI algorithms cluster devices that have the same behavioral characteristics. It then crosses this information with a wide range of other points of data obtained from the network, to accurately determine the type of the devices. This advanced feature provides an accurate and comprehensive asset inventory, without the need for Active polling.

SCADAfence

RAPID7

Value Level Tracking & Profiling

When working to secure OT networks, the need for process value monitoring and alerting often rises. However, as the OT process can have hundreds or thousands of variables, it is often not feasible for the single user to define and manage alerts for all of them. Therefore, the SCADAfence Platform offers a unique feature: Variable Profiles and Similar Variables Association.

Variable Profiles - The profiles enable the user to manage large number of variables with a small number of policy items. Each profile represents a type of variable. For example, boiler temperature, engine speed, or valve pressure.

Similar Variables Association - The SCADAfence Platform automatically analyzes variables behavior over time, and suggests the user similar variables to be grouped into the above profiles. This unique capability, helps the user do the right grouping, avoid errors, and also helps discover and associate previously "unnoticed" variables.

Asset Vulnerability Management

The SCADAfence Platform matches industrial assets properties such as vendor, model and firmware version to industry CVEs and lists the relevant CVEs per each asset. The SCADAfence Platform also provides workflow tools to manage these CVEs.

Asset Exposure Management

The SCADAfence Platform monitors the asset behavior and provides the user with valuable information on protocols and traffic that the asset is doing, and alerts the user if exposures are found. The SCADAfence Platform also shows the user the list of protocols, detailed traffic information, down to the industrial protocol command, list of open ports, etc., and alerts on usage of insecure protocols, authentication methods, and many more.

The Integration with Rapid7

The SCADAfence Platform has an advanced integration implemented with Rapid7's offerings. The integration works both ways and adds great security and manageability value. The main scenarios and benefits are depicted in the diagram below:

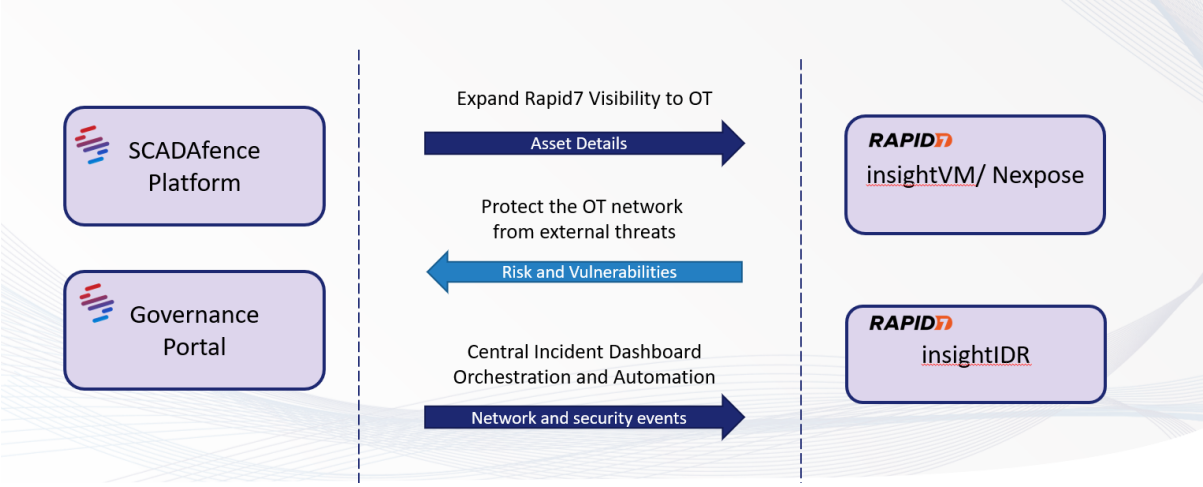

Diagram 2: SCADAfence – Rapid7 Integration

Asset Inventory Integration

SCADAfence's Enrichment of Rapid7's Asset Inventory

The SCADAfence Platform allows Rapid7 InsightVM to extend its visibility into the OT networks.

It enriches InsightVM's database with detailed asset information:

- Detailed asset information gathered from industrial protocols DPI
- Automatic Device Type (Role) identification
- Associated exposures (unsecure protocols, default passwords, list of open ports, etc.)
- Past asset activity (system events)

Rapid7's Enrichment of SCADAfence's Asset Inventory

Increase OT Security by enrichment of asset vulnerability data.

The SCADAfence Platform imports risk and vulnerability information on IT assets from Rapid7. It then correlates this with the OT communication map and can identify OT devices that communicate with exposed or even compromised IT devices. When such a case is detected, the SCADAfence Platform generates alerts, that can be sent to insightIDR and eradication actions can be performed.

This prevents security incidents by immediate response to threats on OT assets.

To learn more about the joint solution or to request a demo, please visit https://l.scadafence.com/rapid7-scadafence-joint-partnership.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 9,100 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organization. For more information, visit our website, check out our blog, or follow us on LinkedIn.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, visit our website, check out our blog, or follow us on LinkedIn.