SCADAfence   CORTEX XSOAR BY PALO ALTO NETWORKS

Joint Solution Brief

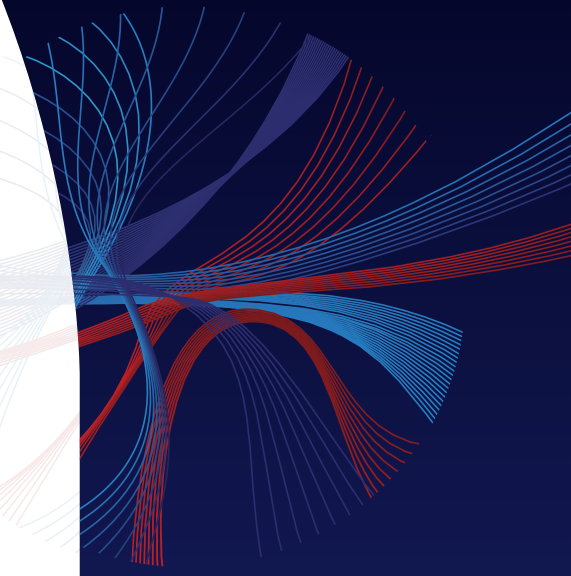
Automated Industrial Network Protection

With the rise of connected devices, organizations have recently been affected by numerous cybersecurity events involving industrial operations and critical infrastructures. As OT networks require increased connectivity to IT networks and the Internet as a whole, air-gapping is no longer a viable option. OT networks are now threatened by IT-origin attacks that can spread and affect operational activities. The implication of a compromised OT network can be substantial – including downtime and sabotage of goods – causing significant financial and reputational damage. To effectively manage security amidst today's convergence of IT and OT, Palo Alto Cortex's security orchestration and automation integrates OT security from SCADAfence Platform into daily IT security management.

The joint solution enables cross-platform visibility and security by coordinating OT protection with IT security processes.

Integration features

- Enrich Palo Alto Cortex's asset coverage with SCADAfence's asset inventory from the OT network including details such as vendor, model, OT protocols in use, and open alerts.
- Analyze exposure of the OT network to threats originating from IT such as connectivity with infected machines, malware behavior, and unauthorized access.
- Leverage hundreds of Palo Alto's product integrations to quickly respond to security threats while keeping OT protection in the loop.
- Manage (open and resolve) security alerts in SCADAfence Platform from Palo Alto Cortex or from any other tool via Palo Alto playbooks.
- Get detailed data (up to tens of thousands of assets from one monitoring sensor) of OT assets from SCADAfence Platform in Palo Alto Cortex including vendor, model, network connections, anomalous behavior, and more.
- Get SCADAfence Platform OT alerts in Palo Alto Cortex that cover malware and ransomware infections, external attacks, internal malicious actions, misconfigurations, and service/device level operational failures that can impact the critical production processes in OT environments.
- Run thousands of commands (including for the SCADAfence Platform) interactively via a ChatOps interface while collaborating with other analysts and Palo Alto's chatbot.



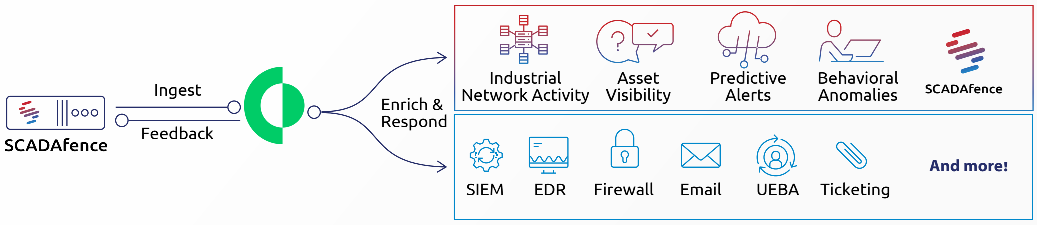
Key Benefits

- *Centralize intelligence across OT and IT networks to improve cross-environment visibility and coordinated, scalable response to attacks.*
- *Enforce industrial network protection policies as part of security orchestration processes in a consistent and rapid manner.*
- *Gain swift understanding into OT vulnerabilities that originate on IT networks or the Internet before executing enrichment and response.*
- *Shorten decision-making cycle by automating key tasks with human review.*

Compatibility

- *Products: Palo Alto Cortex, The SCADAfence Platform.*

SCADAfence



USE CASE #1

Automated Ot Security Enforcement and Response

1. Challenge: Management of OT and IT networks are usually isolated from each other, creating issues in enforcement and response to security threats. Internal processes and lack of critical knowledge sharing prevents unified incident handling processes. When an OT threat is detected, it often takes days until the correct measure is approved and implemented,resulting in highly exposed OT networks and vulnerable production processes.

2. Solution: SCADAfence Platform's OT alerts can be ingested into Palo Alto Cortex along with relevant data such as asset details, part alerts, and connectivity information. This enables security teams to perform enforcement actions either automatically or upon approval as part of Palo Alto playbooks that include both IT and OT information. Enforcement actions might include adding firewall and NAC rules, issuing malware scans, and so on.

3. Benefit: OT alert ingestion from SCADAfence into Palo Alto Cortex enables security teams to access all relevant information from a single management platform. Playbooks that coordinate across IT security products and OT environments standardize and accelerate incident handling to minimize operational downtime.

USE CASE #2

Study Ot Network Exposure To External Threats

1. Challenge: The evolving nature of OT networks has led to a relative lack of security measures such as authentication, encryption, and patching. This makes modern industrial operations susceptible to downtime, with minutes of outage leading to huge financial damages. Isolating OT and IT networks is no longer a viable solution due to the rise of industrial IoT and the digital transformation of OT. Thus, security teams need proactive visibility over OT networks and their exposure to threats originating from IT networks and the Internet.

2. Solution: Security teams can utilize Palo Alto Cortex's integration with the SCADAfence Platform to build a detailed OT exposure map whenever suspicious activity or infections occur on IT networks. It enables collection of asset data, connectivity data, anomalies, and past OT events into Palo Alto Cortex, helping security teams identify exposed and vulnerable assets in the OT network.

3. Benefit: Palo Alto playbooks coupled with the SCADAfence Platform ingestion and actions allow security teams to either proactively identify OT vulnerabilities and threats or – if the OT networks are already infected – to respond to attacks in an efficient, standardized, and cross-platform manner.

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, & 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, & building management industries to operate securely, reliably, and efficiently. To learn more, visit **www.scadafence.com**

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. For more information, visit **www.paloaltonetworks.com**

Our offices
Headquarters: Tel Aviv
Regional: New York, Munich, Tokyo

Contact us: info@scadafence.com
www.scadafence.com

SCADAfence