SCADAfence cybereason

Joint Solution Brief

Stop Attacks Across OT and IT with Multi-Layered Defense

A Joint Solution from Cybereason and SCADAfence

Cybereason and SCADAfence combine the industry-leading endpoint protection platform with the most comprehensive continuous OT network visibility and threat detection available. The result is correlated operational network traffic and behavioral detection with host and user behaviors across multiple network areas, enabling your organization to detect and stop complex attacks earlier and more completely across IT and OT.

A single security breach of an industrial control system can quickly result in intellectual property theft like a drug formula leak, production line shutdowns, or physical damage, such as those from altered critical values in a desalination facility. Further, attacks on an OT environment are difficult and potentially dangerous to respond to. However, for the vast majority of OT attacks, the attacker's beachhead is an endpoint connected to the corporate environment. Attackers leverage this to move laterally across the network, collecting data and gaining privileges to access additional endpoints and machines that control industrial equipment like programmable controllers, sensors, valves, and more.

This connection between attacks on IT and OT systems, combined with many security products' siloed approach and inability to converge into a single, useful display for analysts, is being actively exploited by attackers targeting industrial control systems.

> *"The SCADAfence platform can run OT-specific DPI at wire speed. It does not miss any data on threats inside the OT network, reducing the number of false positives."*

Gartner

Source: Cool Vendors in Cyber-Physical Systems Security, April 2020

Key Benefits:

- *Stop attacks across the corporate environment before they reach OT environments.*
- *Understand the full scope of the attack across IT and OT environments in a single console.*
- *Gain real-time visibility across attacks in IT and OT environments as part of a single Malop.*
- *Ensure high fidelity alerts with correlation across OT network traffic and endpoint data.*
- *Implement risk mitigation for USB devices with endpoint controls.*
- *Enhanced visibility and correlation between endpoint processes and operational activities.*

SCADAfence

cybereason

Take a Multi-Layered Approach to IT and OT Defense

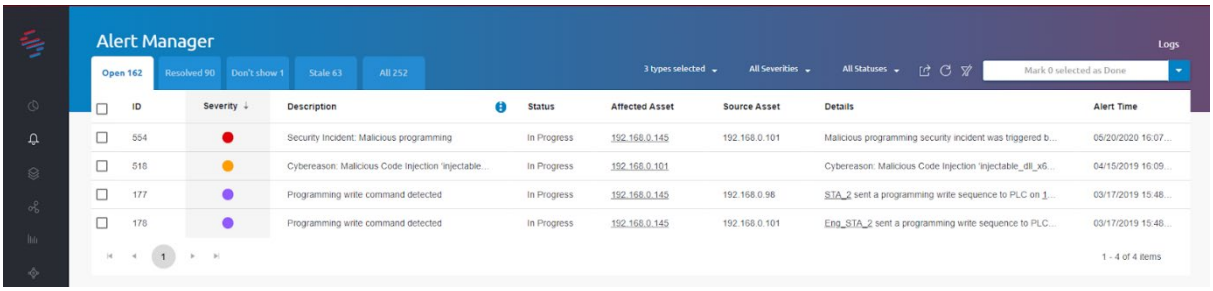
The Cybereason Defense Platform integrates seamlessly with the SCADAfence Platform to give endpoint controls alongside high-fidelity behavioral indicators of compromise across endpoints and operational network equipment. With this combination, security analysts have the visibility to respond across IT and OT environments, all within a single console. This integration enriches customers' SCADAfence risk model and gives analysts needed visibility into OT equipment. Eliminate blind spots between IT and OT by combining Cybereason and SCADAfence.

The Malop Difference, Now with Network Visibility

Leverage a fully contextualized view of each stage of an attack: every process, network connection, machine, and user involved in an attack. The Cybereason Malop enables analysts to triage attacks in minutes, identify the full scope of the attack and act immediately, reducing risk and cost. With the Cybereason and SCADAfence joint solution, the Malop now integrates the most comprehensive, continuous OT network monitoring to give industrial control systems a multi-layered defense. Ensure low false positives and high visibility of attacks across IT and OT environments in a single platform.

Efficient Detection of Incidents

With Cybereason and SCADAfence, analysts can correlate network traffic behavior with host and user behaviors across multiple network areas. Easily surface critical events and detect incidents across machines and networks that would previously go completely undetected. Quickly react and precisely prevent further attack propagation with automatic correlation of OT manipulation commands with compromised host indications.

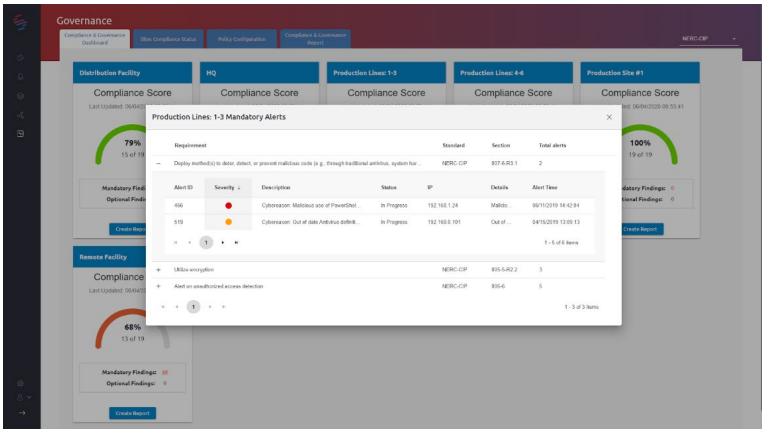


The SCADAfence Platform triggers incident alerts correlated with Cybereason alerts.

Compliance Management

Today, many common-industry standards and regulations such as: NERC-CIP, NIST CSF & IEC-62443 mandate security controls on endpoints. For example, IEC-62443 SR-3.2 requires the existence of protection mechanisms to prevent, detect, report and mitigate the effects of malicious code, and the capability to update the protection mechanisms.

Cybereason's detection engine enriches SCADAfence's compliance management portal to give analysts an across-organization compliance dashboard. This dashboard lets measure and track industry standards and organizational policies for compliance, which cuts down on manual audits and improves data accuracy. All data is based on real traffic, no questionnaires.



Integrated Compliance Management by SCADAfence and Cybereason.

Asset Data Enrichment

The SCADAfence Platform's deep packet inspection (DPI) engine identifies a wide range of host attributes that are part of the industrial protocols communication and are related to OT processes. By combining this information with detailed host data from Cybereason, analysts get a new level of visibility into network assets and their security status. The correlation of OT and IT data, user and application level actions with network activity, change control and up-to-date CVE statuses, is all correlated together for high-efficacy alerting and a single unified viewpoint.

Assisted Enforcement

When detecting network-wide and asset-specific incidents, the SCADAfence Platform updates the Cybereason Defense Platform so it can block access to host interfaces and block malicious services. This enables accurate and immediate response to security incidents.

About Cybereason

Cybereason, creators of the leading Cyber Defense Platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint prevention, detection and response, and active monitoring. The solution delivers multi-layered endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is a privately held, international company, headquartered in Boston with customers in more than 30 countries.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. 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 manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, go to www.scadafence.com.