DEMISTO | #SCADAfence

Automated Industrial Network Protection

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: Demisto Enterprise, SCADAfence Continuous Network Monitor (CNM)

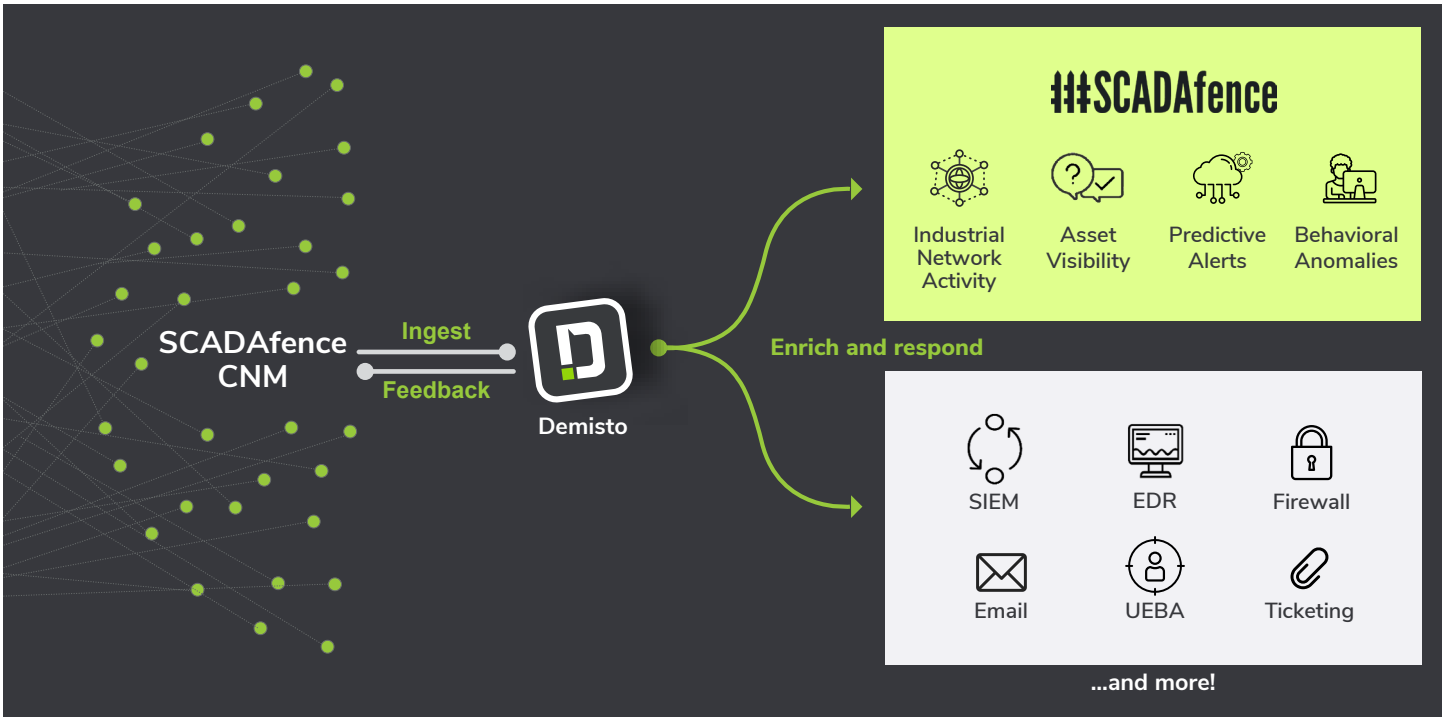
With the rise of connected devices, organizations have recently been affected by numerous cybersecurity events involving industrial operations and critical infrastructures. As OT networks require increased connectivity to IT networks and the Internet as a whole, air-gapping is no longer a viable option. 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, Demisto's security orchestration and automation integrates OT security from SCADAfence CNM 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 Demisto'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 Demisto product integrations to quickly respond to security threats while keeping OT protection in the loop.
- Manage (open and resolve) security alerts in SCADAfence CNM from Demisto Enterprise or from any other tool via Demisto playbooks.
- Get detailed data (up to tens of thousands of assets from one monitoring sensor) of OT assets from SCADAfence in Demisto Enterprise including vendor, model, network connections, anomalous behavior, and more.

- Get SCADAfence CNM OT alerts in Demisto Enterprise 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 SCADAfence CNM) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED OT SECURITY ENFORCEMENT AND RESPONSE

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.

Solution: SCADAfence CNM's OT alerts can be ingested into Demisto Enterprise 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 Demisto playbooks that include both IT and OT information. Enforcement actions might include adding firewall and NAC rules, issuing malware scans, and so on.

Benefit: OT alert ingestion from SCADAfence into Demisto 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

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.

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

Benefit: Demisto playbooks coupled with SCADAfence CNM 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 provides a cybersecurity and visibility platform for industrial ICS/OT networks as they increase levels of automation, connectivity and network complexity. SCADAfence's non-intrusive solutions reduce risks of operational downtime, production manipulation, data theft and ransomware attacks – without affecting production continuity. They enhance operational visibility, threat detection and risk management – and scale to meet the needs of large, complex industrial networks.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. For more information, visit **www.demisto.com** or email **info@demisto.com**.