SOLUTION BRIEF

Integrated Cybersecurity Technology from Dragos and Swimlane

Faster Detection and Response with Centralized Case and Vulnerability Management Across IT and OT

HIGHLIGHTS

- Centralized view of IT/OT networks with dynamic notification, case management and reporting for faster and effective response.
- Comprehensive ICS/OT vulnerability management with corrected, automated enrichment, prioritized guidance that allows customers to manage the entire lifecycle of specific vulnerabilities.
- Context rich ICS/OT asset visibility that analyzes multiple data sources including protocols, network traffic, asset characterizations and anomalies.
- Support the sharing of native and historical indicator of compromise (IOC) within IT and OT environments, including Dragos's curated and exclusive OT IOCs, providing insights to triage threats and to enable recognition of persistent threats over time.
- Rapidly pinpoint malicious behavior on your ICS/OT network, provide in-depth context of notifications, and reduce false positives for intelligence-driven threat detection.

As Operational Technology (OT) networks integrate with Information Technology (IT) networks within industrial organizations, it's becoming essential that security operations teams have complete visibility and correlation across both domains for effective asset visibility, threat detection, and incident response. Technology integrations between Turbine and the Dragos Platform improve visibility and provide centralized case management, automated ticketing, and vulnerability management to enable a more robust Security Operations Center (SOC).

THE CHALLENGE

Cyber threats targeting industrial infrastructure sectors like electric utilities, oil & gas, manufacturing, and others are increasing. As these organizations continue their digital

transformation in OT, expanding network connectivity and process efficiencies, adversaries can now target both IT and OT networks. Despite the continued integration of these networks, defending them requires different skills and approaches.

Cybersecurity analysts at industrial organizations not only need to understand what IT and OT threats exist but also implement a program to detect and respond to them within their organization. It's imperative that security teams get the maximum value out of existing cybersecurity technology investments and integrating complementary platforms will also help provide more holistic visibility and case management to improve cybersecurity operations efficiencies.

Adversaries targeting OT often leverage connectivity from the enterprise networks to pivot into industrial networks. In these events, security teams responsible for the availability of both IT and OT networks need complete situational awareness to quickly correlate any suspicious activity and vulnerabilities across both domains to ensure adversaries are detected early and to make critical decisions as efficiently as possible.

THE SOLUTION

To address these challenges, the Dragos Platform integration with Swimlane Turbine provides improved visibility, allowing industrial organizations to monitor, detect and respond to threats across their IT and OT environments to reduce their mean time to recover (MTTR).

Together, Swimlane Turbine, an AI-enabled low-code security automation platform, and the Dragos OT Cybersecurity Platform allow users to utilize both IT and OT visibility and enrichment into a single system. This integration is designed to streamline vulnerability management and simplify collaboration with IT through automated asset enrichment, notifications triage, incident escalation/response, and vulnerability triage.

The Dragos Platform provides Turbine users comprehensive asset visibility, vulnerability management, and the industry's most effective threat detection in ICS and OT environments. By analyzing a broad range of data sources, including protocols, network traffic and logs, it rapidly pinpoints threats with reduced false positives. The platform offers in-depth contextual alerts, enriched risk scores, and prioritized guidance that allows customers to manage the full lifecycle of specific vulnerabilities in their environment, showing historical disposition – through continuous, automated collection and analysis. This approach ensures a high level of preparedness and protection against operational threats, safeguarding critical processes and infrastructure.

Swimlane Turbine sets a new standard for security automation, with its ability to ingest, enrich, and action on petabytes of data at machine-speed. Turbine helps security teams unify complex environments by connecting typically siloed technologies. It is approachable enough for those with no coding experience and sophisticated enough to satisfy OT and IT security operations. Turbine automates and enriches incident response, collecting alert and event data from the Dragos Platform and automatically centralizes and responds to alerts using automated workflows to reduce mean time to detect and respond.

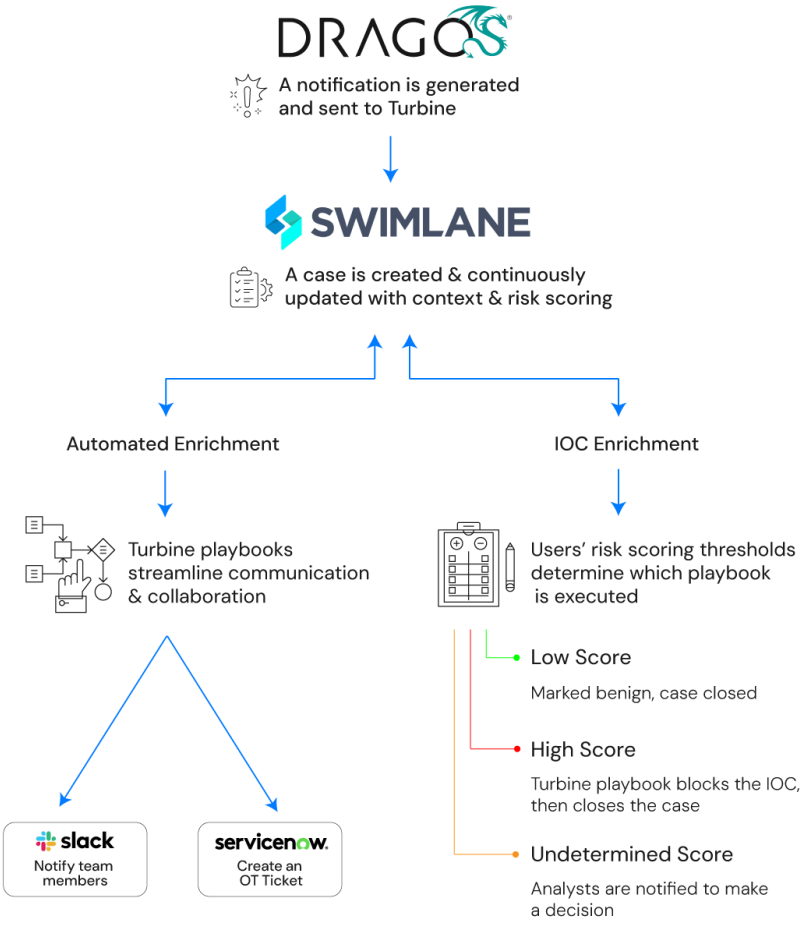

Diagram 1. Notification triage utilizing automated and IOC enrichment for faster, more accurate response.

Integrating the Dragos Platform and Swimlane Turbine provides security professionals with unparalleled coverage across IT and OT networks, resulting in greater situational awareness and decision making, improving the return on investment (ROI) of your SOC and reducing the time spent on manual or mundane tasks.

By harnessing the power of automation, data ingestion, and case management, security teams can build a bridge that strengthens the security posture across IT and OT environments.

HOW IT WORKS

The Turbine and the Dragos Platform integration is available in the Swimlane in-app marketplace.

Start by finding the Dragos integration within the in-platform Turbine marketplace. Once located, you will see a button that says "+ connect". Hitting this button will install the integration and save its capabilities within persistent storage. To access the installed connector, users can navigate to the orchestration section on the left side panel and scroll down to connectors. Once there, select the Dragos integration and setup your API key and secret as an asset. Saving these credentials will enable the user to begin using the Turbine and Dragos Platform API to transfer information between the two solutions. Once configured, the integration allows the Dragos Platform to automatically

synchronize assets and notifications within Turbine per the defined frequency interval providing users with an accurate inventory that can be used to serve many different functions.

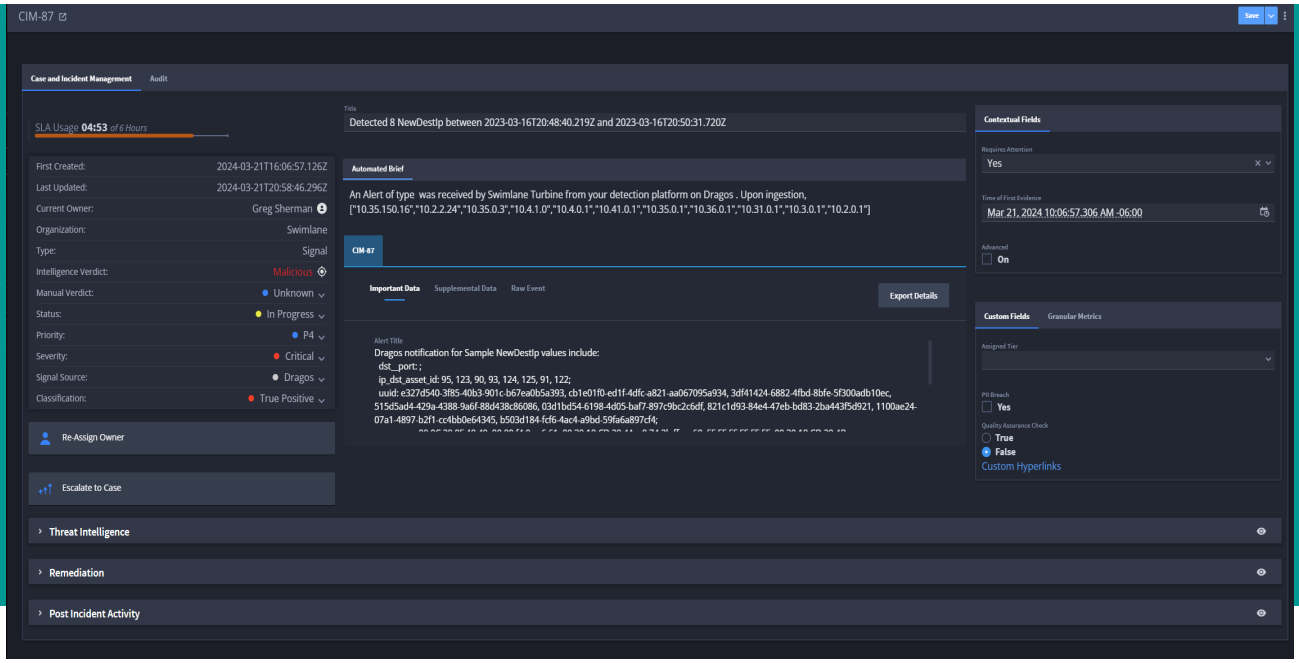

Figure 1. OT notification from the Dragos Platform in Swimlane Turbine case management view.

With Turbine's ability to automatically ingest data from any connected tool, users now have a centralized case management view of the Dragos Platform's context rich ICS/OT asset inventory, detections and vulnerabilities. Turbine also enables automated enrichment, prioritized guidance to triage threats, operational efficiency with dynamic notification ingestion and enhanced reporting. All these features add value across the organization's security posture and equate to faster, more accurate response within IT and OT operations.

ADVANTAGES OF THE INTEGRATED SWIMLANE TURBINE AND DRAGOS PLATFORM SOLUTION INCLUDE:

- More efficient security operations by integrating the technologies enables defenders with a more comprehensive workflow from initial threat detection through response, improving mean time to recovery (MTTR).
- Intelligence-driven threat detection improves detection confidence and reduces alert fatigue.
- Build internal team expertise and IT/OT collaboration to ensure knowledge transfer and expertise and develop robust internal defensive capabilities.
- Reduce risk while ensuring operations of critical infrastructure and business continuity.
- Leverage common controls framework to organize compliance efforts to meet CISA guidelines and easily determine the status of OT infrastructure and automate reporting for relevant regulatory programs and industry standards like NIST CSF, NERC CIP, ISA/IEC 62443, CFATS, ANSI/AWWA G430, GxP, IT-SIG 2.0, and many others.

For more information, please visit http://www.dragos.com/partner/swimlane/
or contact us at info@dragos.com