JOINT SOLUTION BRIEF

Comprehensive Vulnerability Management and Response for Operational Technology

Swimlane & Nozomi Networks - Leveraging Automation to Drive IT/OT Convergence

The Challenge

Critical Infrastructure organizations across the globe are facing numerous challenges to keeping their cyber assets safe from potential attackers. The sheer number of cyber assets Operational Technology (OT) teams manage has exploded over the last decade and maintaining security across so many separate devices continues to get more difficult. As these assets grow in number, so too does the number of vulnerabilities across all these devices and the complexity in prioritizing the ones that are truly adding risk. Any connected asset that has not been fully updated introduces greater risk to the organization, potentially leaving them vulnerable to bad actors looking to gain access or hamper production. This also creates trouble when bringing on new assets, as many systems will need to recognize them as approved company assets before letting them communicate with other systems.

Customer Benefits

- Improved operational efficiency and greater accuracy
- Enhanced security posture across OT and IT
- Greater visibility into key metrics for management reporting
- Accelerate OT security advancement

Within OT environments today, there are also many obstacles to fostering collaboration between OT and IT teams. These groups have traditionally been siloed and OT teams really did not have many connected devices that required collaboration with IT before the Internet of Things came onto the scene. As users connect more and more items to the internet, they also introduce many new attack vectors across an organization. These shared attack vectors and connected devices are leading to more interactions between IT and OT, but it can be difficult to cut through legacy barriers or share information across disconnected tools. These issues in collaboration can really make it difficult to work together across teams and often lead to unexpected downtime, fragmented auditing and visibility, and duplicative work across items the other teams might have already worked on.

In addition to these challenges, Operational Technology teams face many of the same obstacles their colleagues in the SOC have been facing; issues such as difficulty hiring enough analysts, lengthy and manual investigations, disconnected technology, tool proliferation, and human error. What OT and IT teams really need is an easy collaborative solution, to multiply the work they can achieve and remove as many obstacles from everyday tasks as possible.

The Solution

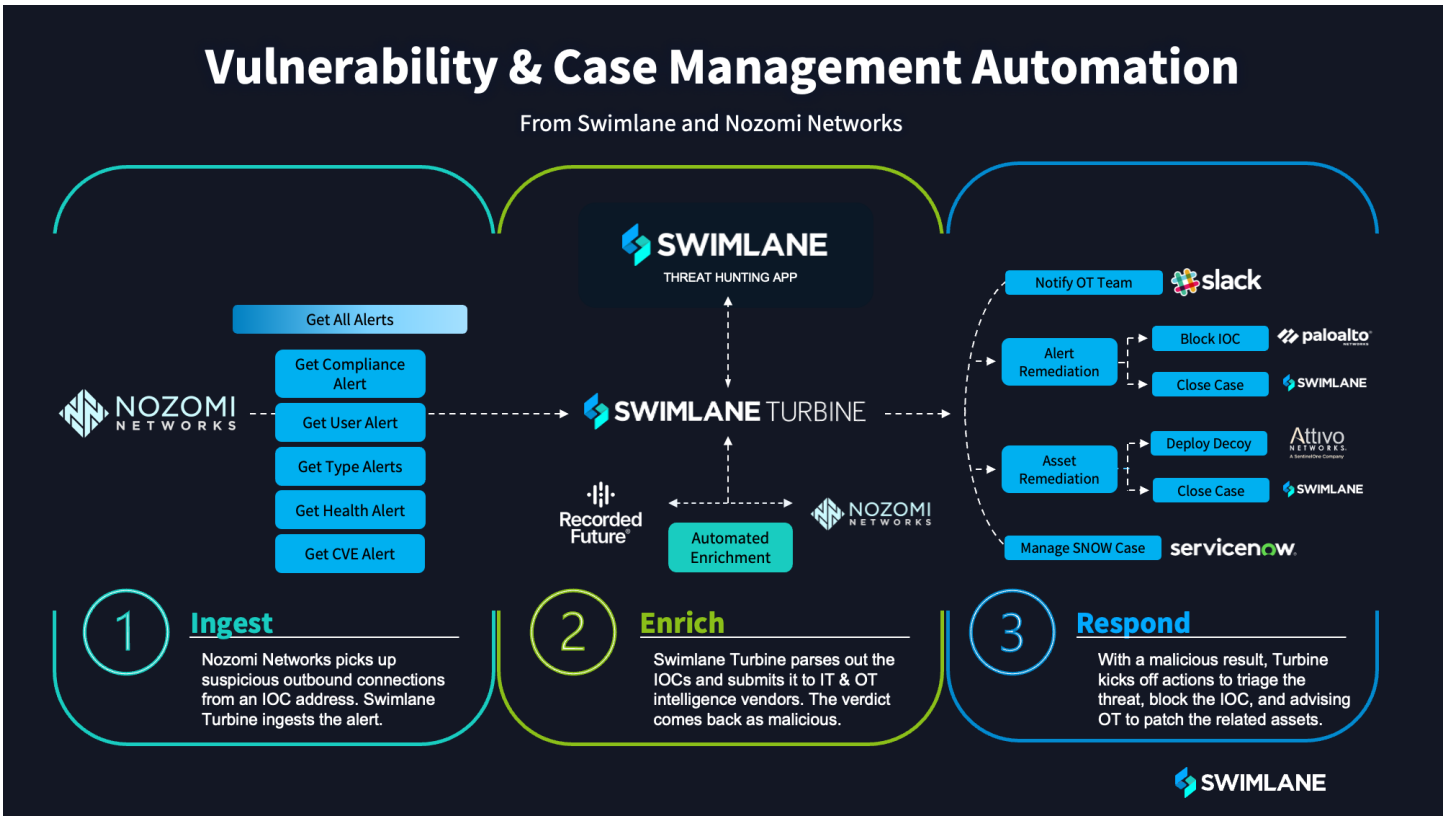
Swimlane and Nozomi Networks have spoken with many customers in the OT space and have heard first hand the struggles these challenges create. Those conversations helped drive Swimlane and Nozomi Networks to partner together, creating a joint solution customized specifically with OT teams in mind and the increasingly complex IT/OT convergence.

How It Works

The first challenge to address is the complexity around vulnerability management and patching. With thousands of assets being monitored for new vulnerabilities, and limited sharing between tools, OT teams have been jumping back and forth between products trying to find the information they need. Swimlane Turbine and Nozomi have centralized all of this intelligence, both IT and OT enrichment, into a single system designed to facilitate streamlined vulnerability management and simplified collaboration with IT. Having all of this information in one system makes it easy to quickly understand the details of a case or alert, enabling the analyst to quickly diagnose the situation and launch a response with a single click.

The Swimlane Turbine and Nozomi Networks integration also enables automated responses or single click responses across any Swimlane Turbine connected product. Leveraging Turbine's low code automation can be a major force multiplier across enrichment actions, greatly reducing the time wasted on manual investigations or building out a case.

Using the integration between Swimlane Turbine and Nozomi, IT and OT teams are now able to reconnect their processes through a common lens. Not only can teams leverage greater visibility across joint initiatives, they can easily pass cases back and forth as situations dictate. This leads to greater efficiency across cases, a large reduction in risk for the organization, and greater visibility for management across their IT and OT security landscape.



Featured Use Case

- **Step 1:** An alert is generated within the Nozomi Networks Guardian sensor that an outbound connection attempt has been made to a specified IP address.
- **Step 2:** Swimlane Turbine ingests the alert from Guardian, parses the IP address, and automatically submits queries to intelligence sources (both IT and OT). The IP in this case returns as highly malicious, so an incident within the IT case management system is automatically created.
- **Step 3:** As Swimlane Turbine creates the IT case, it then kicks off multiple automated actions. The first is to notify OT team members of the incident and to pass on details of the case.
- **Step 4:** After that, Swimlane Turbine deploys a decoy host to the asset's IP in preparation for an attack. Should one come, the decoy will take the hit and provide further forensics on the attacker.
- **Step 5:** The next action Turbine takes is to update the firewall rules, as this device should not be talking to the internet or this malicious IP address.
- **Step 6:** The final step in this workflow is to open an OT ticket within ServiceNow with details on the actions taken and further information to be passed to the OT team.

Integration Features

- Live Asset Intelligence
- VIP Asset Tagging, tracking, and prioritization
- Continuous Compliance Checking
- Automated IT, CPS, User Alert Enrichment
- Third Party Threat Intelligence
- Real-time discovery of newly introduced assets
- Automated Response Capabilities, Single click triage actions

To learn more about this solution or how it can provide lift across your organization, reach out to your Swimlane or Nozomi representative to schedule a demonstration.

SWIMLANE

Corporate Headquarters
363 Centennial Pkwy Suite 210
Louisville, CO 80027
1-844-SWIMLANE

Learn more at: swimlane.com

Better Together

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders.

About Nozomi Networks

We accelerate digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience. Learn more at nozominetworks.com