SANS | Research Program

PRODUCT REVIEW

SOC AI Automation Masterclass: How Swimlane Enhances Incident Response and Visibility

Written by **Mark Jeanmougin**

August 2025

SWIMLANE

©2025 SANS™ Institute

Introduction

Swimlane Turbine is a proven AI automation platform built on more than a decade of expertise and deep integration with a wide range of enterprise tools.[1] Designed to enhance productivity, efficiency, and effectiveness across multiple teams, Turbine is especially impactful in security operations (SecOps) within large enterprises and managed security service providers (MSSPs).

Many organizations begin their automation journey by targeting the alert management life cycle. Even with best-in-class tools, operational efficiency can suffer if systems don't communicate seamlessly. Turbine bridges that gap, enabling your SIEM, EDR/XDR, firewalls, EPP, cloud, SaaS, and on-prem tools to share alert data and coordinate incident response (IR) efforts—without leaving the Turbine platform.

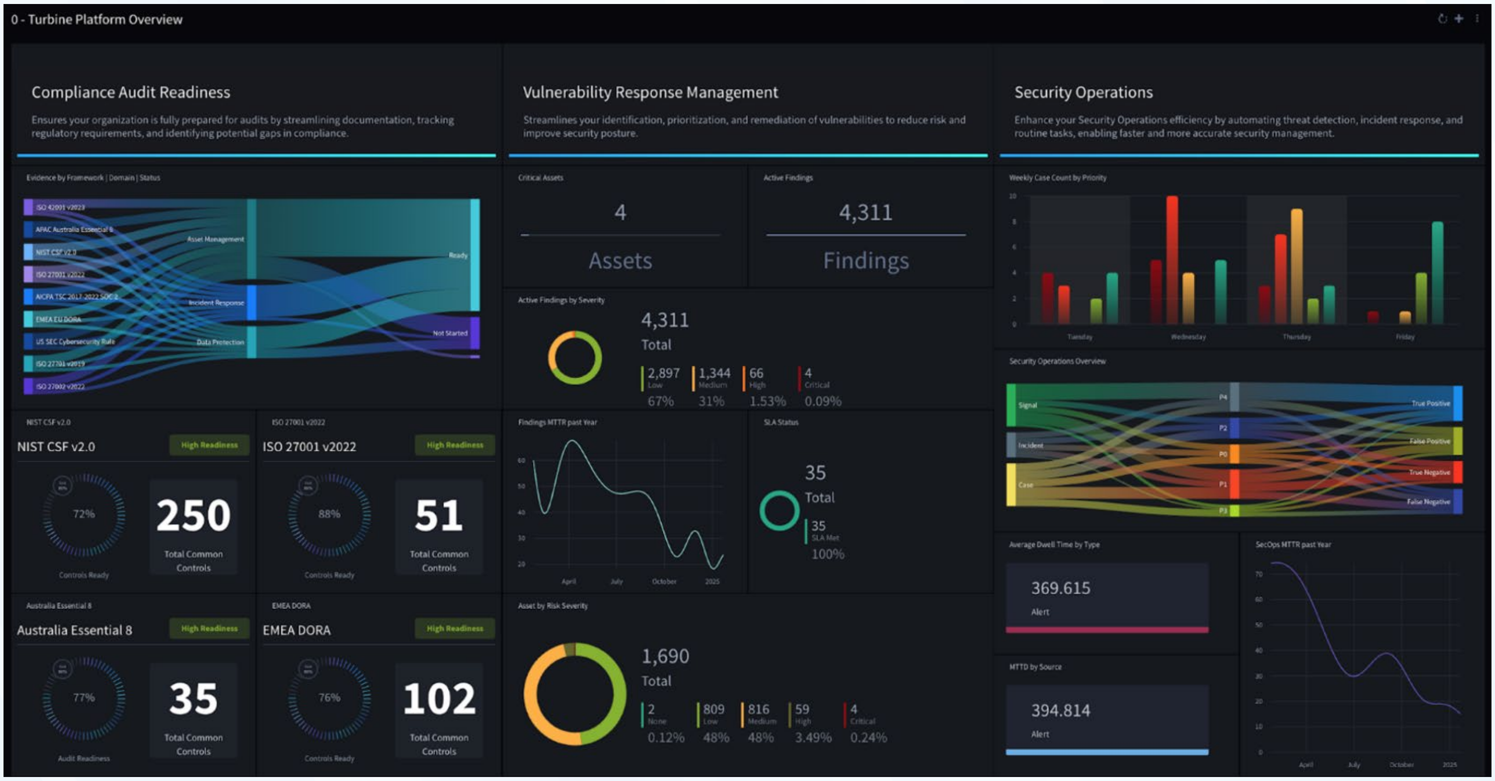
Once an incident is declared, Turbine can automatically collect relevant data from across your security ecosystem and attach it to the corresponding Turbine ticket. For teams handling phishing threats, Turbine integrates with Microsoft 365 and other enterprise email platforms to streamline investigation and resolution—delivering a faster, higher-quality user experience. Turbine also can deliver that same experience with 500-plus connectors to other platforms to automate complex workflows. Turbine wraps all this up with a complete set of dashboards and reporting. The following sections explore these capabilities in greater detail.

Swimlane Turbine helps unify disconnected security tools—finally delivering on the promise of seamless automation.

[1] https://swimlane.com/swimlane-turbine

Integrations

A core strength of Turbine is its ability to integrate with virtually any API. As most enterprise security tools provide network-based APIs, Turbine can seamlessly connect with them to streamline workflows and facilitate efficient data sharing. The Swimlane Marketplace serves as the primary resource for discovering existing integrations (called connectors) for third-party tools.[2] In many cases, the required connector is already available for download, as other users have likely implemented similar integrations. In addition to connectors, the Marketplace offers widgets, prebuilt playbooks, and end-to-end automation solutions tailored to common use cases (see Figure 1). For custom-built or internal applications, Turbine supports script-based integrations using Python, PowerShell, Secure Shell (SSH) connections, and other languages.



0 - Turbine Platform Overview

Compliance Audit Readiness

Ensures your organization is fully prepared for audits by streamlining documentation, tracking regulatory requirements, and identifying potential gaps in compliance.

Vulnerability Response Management

Streamlines your identification, prioritization, and remediation of vulnerabilities to reduce risk and improve security posture.

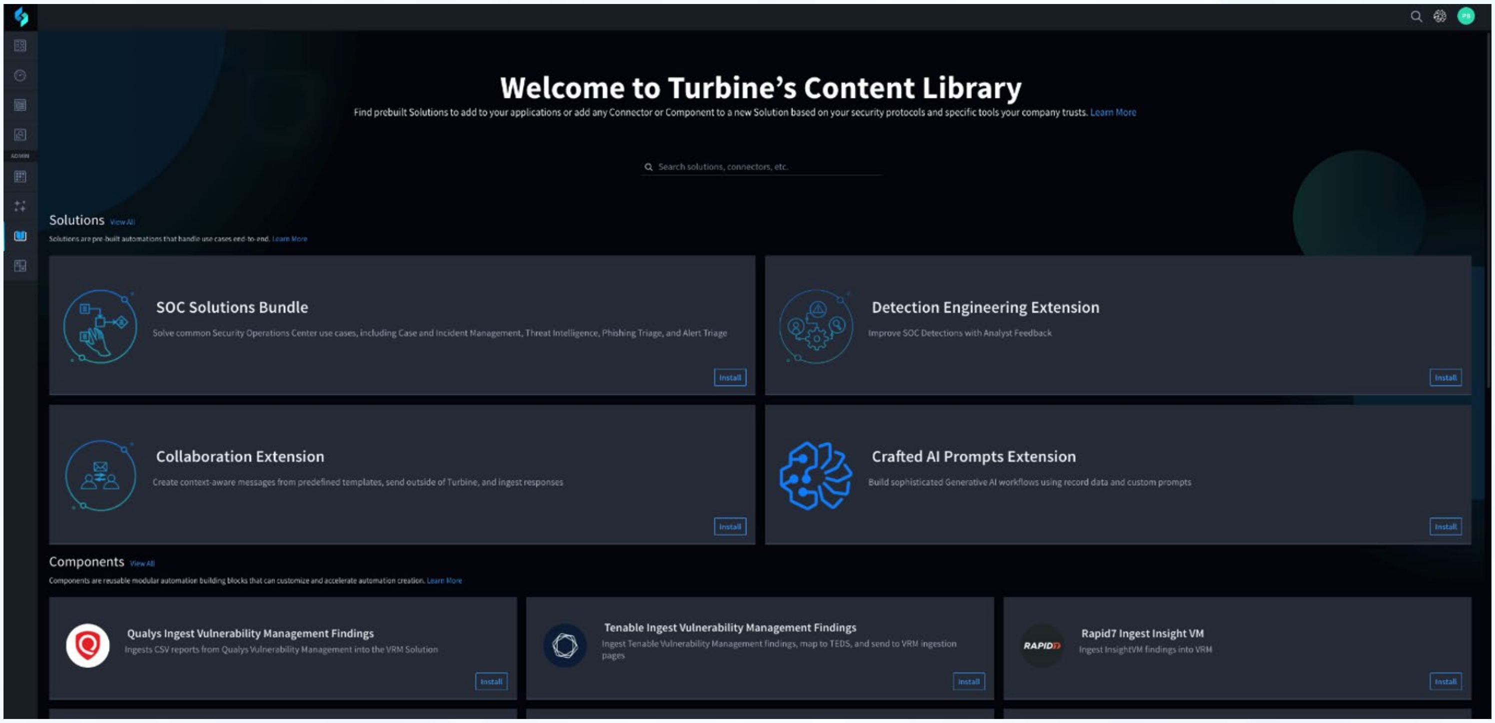
Security Operations

Enhance your Security Operations efficiency by automating threat detection, incident response, and routine tasks, enabling faster and more accurate security management.

Figure 1. Swimlane Turbine Platform Overview

[2] https://turbine-marketplace.swimlane.com/en-US/home

Swimlane Turbine also includes the Turbine Library, an in-platform resource that simplifies the sharing and reuse of automation content across multiple tenants, enabling greater collaboration and consistency in security operations (see Figure 2).



Welcome to Turbine's Content Library

Find prebuilt Solutions to add to your applications or add any Connector or Component to a new Solution based on your security protocols and specific tools your company trusts. Learn More

Search solutions, connectors, etc.

Solutions View All

Solutions are pre-built automations that handle use cases end-to-end. Learn More

SOC Solutions Bundle

Solve common Security Operations Center use cases, including Case and Incident Management, Threat Intelligence, Phishing Triage, and Alert Triage

Install

Detection Engineering Extension

Improve SOC Detections with Analyst Feedback

Install

Collaboration Extension

Create context-aware messages from predefined templates, send outside of Turbine, and ingest responses

Install

Crafted AI Prompts Extension

Build sophisticated Generative AI workflows using record data and custom prompts

Install

Components View All

Components are reusable modular automation building blocks that can customize and accelerate automation creation. Learn More

Qualys Ingest Vulnerability Management Findings

Ingests CSV reports from Qualys Vulnerability Management into the VRM Solution

Install

Tenable Ingest Vulnerability Management Findings

Ingest Tenable Vulnerability Management findings, map to TEDS, and send to VRM ingestion pages

Install

Rapid7 Ingest Insight VM

Ingest InsightVM findings into VRM

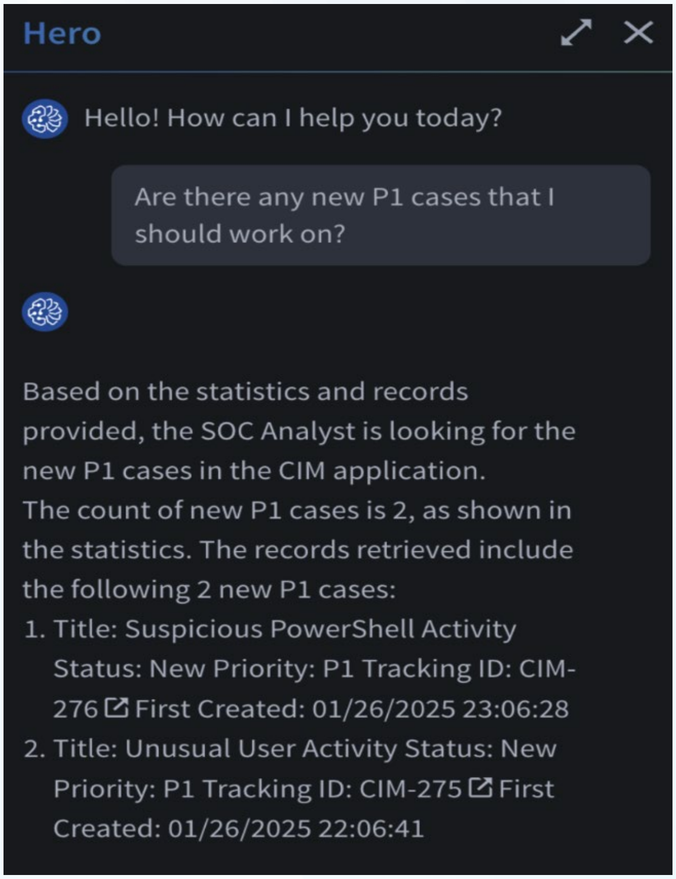
Install

Figure 2. Swimlane Turbine Library

Agentic and Generative AI

Hero AI is Turbine's advanced AI feature, built on a foundation of large language models (LLMs), generative AI (GenAI), and agentic AI (see Figure 3).[3] Unlike companies that simply capitalize on the latest AI buzzwords, Swimlane has been developing and refining these capabilities over years of focused investment, delivering real, tangible benefits to SecOps teams. Swimlane has recently earned the ISO 42001 certification for Artificial Intelligence Management System, which joins their existing ISO 27001 (Information Security Management System) and ISO 27701 (Privacy Information Management System).

What ChatGPT is to the internet, Hero AI is to the SOC.



Hero

Hello! How can I help you today?

Are there any new P1 cases that I should work on?

Based on the statistics and records provided, the SOC Analyst is looking for the new P1 cases in the CIM application.
The count of new P1 cases is 2, as shown in the statistics. The records retrieved include the following 2 new P1 cases:

1. Title: Suspicious PowerShell Activity Status: New Priority: P1 Tracking ID: CIM-276 First Created: 01/26/2025 23:06:28
2. Title: Unusual User Activity Status: New Priority: P1 Tracking ID: CIM-275 First Created: 01/26/2025 22:06:41

Figure 3. Swimlane Hero AI

[3] https://swimlane.com/platform/ai

Hero AI enables analysts to interact with Turbine using natural language, asking context-aware questions about individual cases, open investigations, recent activity, or even the overall environment. For example:

- Have we found this vulnerability on other devices?
- Which case should I work on first?
- Give me a quick summary of the three most recent cases.
- How many of our NIST 800-53r5 controls are ready for an audit?

In organizations operating under a follow-the-sun model, Hero AI significantly simplifies the preparation of handover reports, making them faster, more accurate, and easier to produce. It helps eliminate critical omissions during transitions, reducing the need for follow-up communications after hours. It's a common scenario where an analyst forgets to brief a case during a handover call, only to receive a follow-up phone call on their way home!

Hero AI is powered by a private Swimlane LLM, ensuring that user queries and organizational data remain confidential. None of this information is used to train future models or shared outside the environment, reinforcing trust and data privacy. As an agentic AI assistant, Hero AI uses the full context of Turbine's platform data to provide intelligent, situation-aware responses. Whether summarizing audit readiness or recommending next steps in an incident, it adapts to the analyst's needs. Beyond the interactive chat interface, Hero AI also can be embedded directly into automation playbooks, allowing teams to harness its capabilities in no-code, programmatic workflows.

Properly deployed tools like Hero AI enable security teams to operate faster, more efficiently, and with greater satisfaction. In an industry historically understaffed and underfunded, GenAI allows teams to extract more value from their automation investments, freeing analysts to focus on higher-impact activities like incident response, threat prevention, and strategic planning.

One of Hero AI's most transformative advantages is how it supports junior analysts. By guiding them through investigations, showing what data matters, how to use specific tools, and how to document tickets correctly, Hero AI helps new team members become productive faster and with minimal reliance on senior staff. This elevates the efficiency of the entire team, improving collaboration, knowledge transfer, and operational maturity.

Case and Incident Management

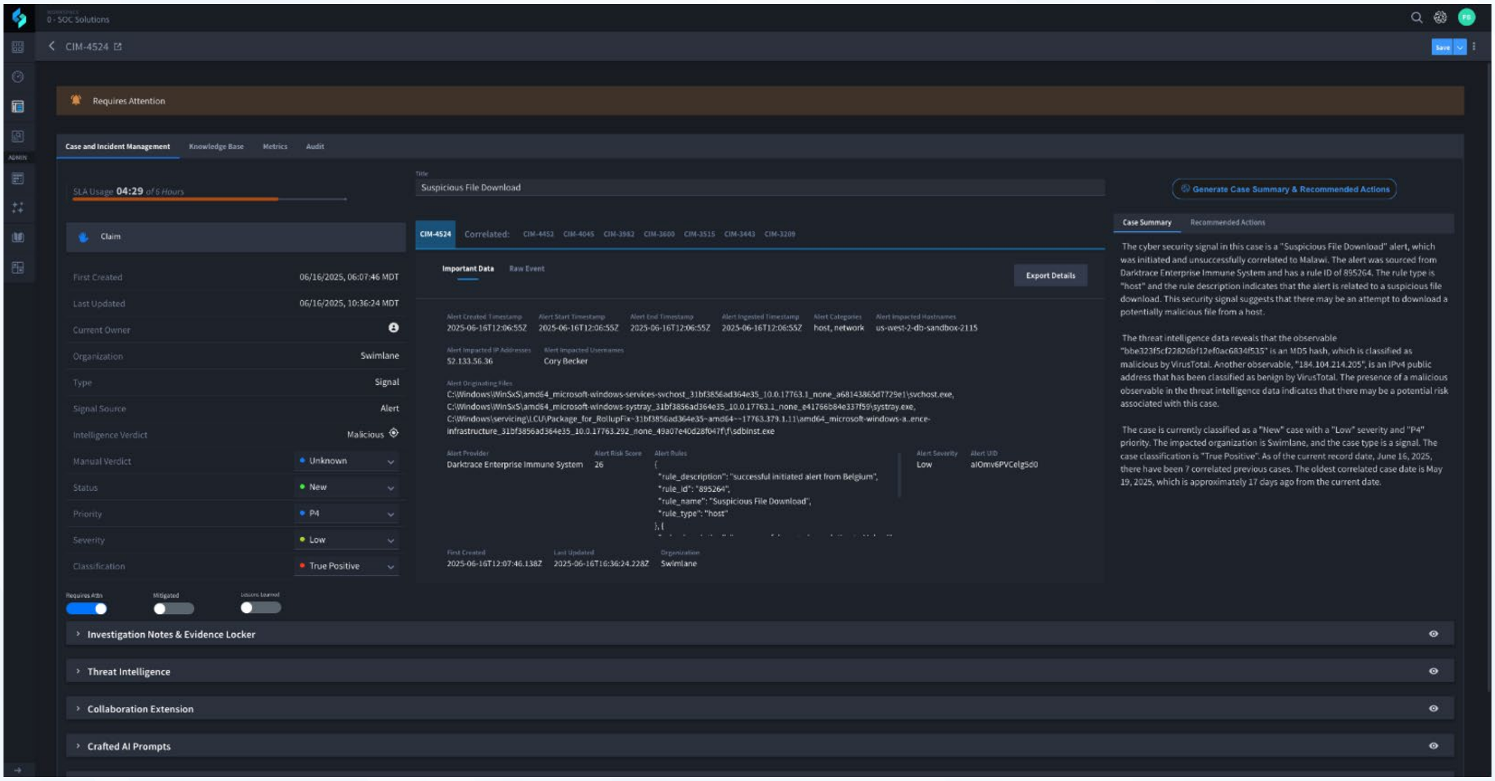
Swimlane Turbine includes case and incident management (CIM), which is a fully integrated incident management system (IMS) as part of its broader security automation platform.[4] For organizations currently relying on basic incident tracking modules embedded within other tools, Turbine offers a significant upgrade in both capability and user experience. Analysts can manage cases for their enterprise or MSSP customers through a centralized, intuitive user interface (UI).

Turbine simplifies operations across complex environments, for example, if one team or customer uses Amazon Web Services (AWS) while another relies on Google Cloud Platform (GCP), Turbine automatically normalizes log data, eliminating the need for analysts to manually interpret tool-specific differences. This not only reduces onboarding time for new analysts, but also minimizes long-term risk caused by inconsistent interpretation of platform-specific details.

Each incident ticket in Turbine includes a comprehensive audit trail of automation artifacts, providing full visibility into every action taken. Turbine seamlessly uses connectors to make API calls to SIEM platforms to gather context from EDR, email systems, on-prem infrastructure, cloud environments, custom applications, and more. Turbine also can receive high-fidelity alerts directly from EDRs and other tools. It also pulls intelligence from connected threat intelligence platforms (TIPs) to deliver real-time insight into threat actors, their tactics, and their motivations.

[4] https://swimlane.com/platform/case-management

What truly differentiates Turbine's CIM application is its deep integration with Hero AI (see Figure 4). Powered by advanced generative and agentic AI models, Hero AI delivers real-time case summaries, allowing analysts to quickly grasp key incident details. It also can proactively identify patterns or gaps, generating insights such as "No post-exploitation activity observed." Most importantly, Hero AI provides context-aware recommendations, such as advising when to reimage a compromised machine or rotate exposed credentials, which helps streamline decision-making and accelerate response. Swimlane Turbine provides a composable UI, which is a modular, drag-and-drop interface that allows users to build case views that interact with dashboards and workflows by assembling reusable visual components without writing code. This approach enables rapid customization and scalability of security operations across different use cases and teams. Swimlane Turbine's CIM empowers SecOps teams with a smarter, more cohesive approach to incident management, which allows for better accuracy, speed, and clarity at scale.



SLA Usage **04:29** *of 6 Hours*

First Created	06/16/2025, 06:07:46 MDT
Last Updated	06/16/2025, 10:36:24 MDT
Current Owner	
Organization	Swimlane
Type	Signal
Signal Source	Alert
Intelligence Verdict	Malicious
Manual Verdict	Unknown
Status	New
Priority	P4
Severity	Low
Classification	True Positive

Title
Suspicious File Download

CIM-4524 Correlated: CIM-4452 CIM-4045 CIM-3982 CIM-3600 CIM-3515 CIM-3443 CIM-3209

Alert Created Timestamp	Alert Start Timestamp	Alert End Timestamp	Alert Ingested Timestamp	Alert Categories	Alert Impacted Hostnames
2025-06-16T12:06:55Z	2025-06-16T12:06:55Z	2025-06-16T12:06:55Z	2025-06-16T12:06:55Z	host, network	us-west-2-db-sandbox-2115

Alert Impacted IP Addresses	Alert Impacted Usernames
52.133.56.36	Cory Becker

Alert Originating Files
C:\Windows\WinSxS\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_10.0.17763.1_none_a68143865d7729e1\svchost.exe, C:\Windows\WinSxS\amd64_microsoft-windows-systray_31bf3856ad364e35_10.0.17763.1_none_e41766b84e337f59\systray.exe, C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.379.1.11\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_10.0.17763.292_none_49a07e40d28f047f\f\sdbinst.exe

Alert Provider	Alert Risk Score	Alert Severity	Alert UID
Darktrace Enterprise Immune System	26	Low	aIOmv6PVCelg5d0

Alert Rules
```
{
 "rule_description": "successful initiated alert from Belgium",
 "rule_id": "895264",
 "rule_name": "Suspicious File Download",
 "rule_type": "host"
}, {
```

First Created	Last Updated	Organization
2025-06-16T12:07:46.138Z	2025-06-16T16:36:24.228Z	Swimlane

The cyber security signal in this case is a "Suspicious File Download" alert, which was initiated and unsuccessfully correlated to Malawi. The alert was sourced from Darktrace Enterprise Immune System and has a rule ID of 895264. The rule type is "host" and the rule description indicates that the alert is related to a suspicious file download. This security signal suggests that there may be an attempt to download a potentially malicious file from a host.

The threat intelligence data reveals that the observable "bbe323f5cf22826bf12ef0ac6834f535" is an MD5 hash, which is classified as malicious by VirusTotal. Another observable, "184.104.214.205", is an IPv4 public address that has been classified as benign by VirusTotal. The presence of a malicious observable in the threat intelligence data indicates that there may be a potential risk associated with this case.

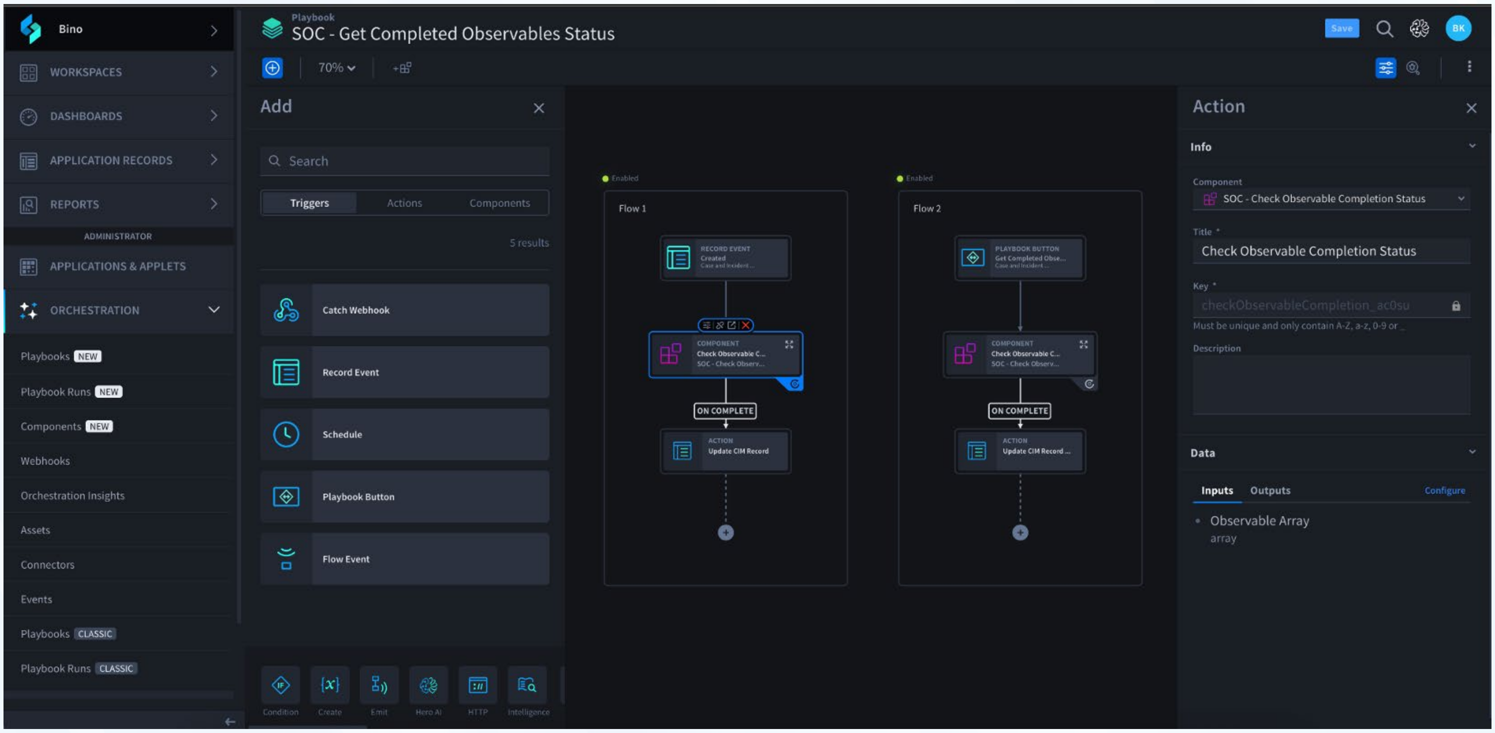
The case is currently classified as a "New" case with a "Low" severity and "P4" priority. The impacted organization is Swimlane, and the case type is a signal. The case classification is "True Positive". As of the current record date, June 16, 2025, there have been 7 correlated previous cases. The oldest correlated case date is May 19, 2025, which is approximately 17 days ago from the current date.

Figure 4. Swimlane AI-Driven Case and Incident Management

Low-Code Playbooks

Turbine Canvas is a low-code playbook development environment, designed to simplify and accelerate security automation. Within Canvas, users can deploy editable playbooks downloaded from the Turbine Library or build and customize their own in-house workflows. Whether streamlining repetitive tasks or building advanced automation strategies, Canvas enables organizations to put their tools to work, freeing analysts to focus on higher-value activities.

Canvas strikes the ideal balance between ease of use for beginners and robust functionality for power users (see Figure 5). Its intuitive drag-and-drop interface allows playbooks to be created directly in the web UI, with no coding required. Playbooks can be triggered in multiple ways, including webhooks, scheduled events, or requests from other playbooks. Development is quick and user-friendly, thanks to a no-code design that enables dynamic interaction with Hero AI—no Python or complex scripting required.



Playbook
SOC - Get Completed Observables Status

Action
Info
Component: SOC - Check Observable Completion Status
Title *: Check Observable Completion Status
Key *: checkObservableCompletion_ac0su
Must be unique and only contain A-Z, a-z, 0-9 or _
Description
Data
Inputs Outputs Configure
Observable Array
array

Figure 5. Turbine Canvas

Canvas offers a robust range of actions and logic, including:

- Conditional flows
- Loops and iterations
- Variable management
- HTTP/HTTPS requests
- Data transformation and schema inference
- Parallel execution
- Record interaction
- Hero AI integration enables a user to send playbook data to the AI without complex scripting

Every Swimlane Turbine subscription includes access to comprehensive training resources, helping new users quickly become proficient in building and managing automated workflows.

The Turbine Library provides an extensive collection of ready-to-use playbooks, ideal for both getting started and addressing more advanced operational needs.[5] For custom workflows, users can take advantage of Hero AI's text-to-code capabilities, enabling even junior developers to generate functional Python scripts. These scripts can support file transformation, integration with on-prem or cloud tools, and virtually any task requiring advanced logic. Advanced developers, meanwhile, can use their own Python code to craft highly tailored automations.

One of the standout features of Turbine Canvas is its component system. Unlike traditional automation platforms where users must manually copy and paste reusable logic across multiple workflows, components enable true modular development. A single component can be created, maintained, and reused across countless playbooks. Updates are made in one place and automatically reflected wherever that component is used, reducing maintenance overhead and dramatically lowering the risk of introducing errors.

With Turbine Canvas, teams can truly build once and reuse anywhere, scaling their automation efforts efficiently and securely.

[5] https://turbine-marketplace.swimlane.com/en-US/listing?pl=3401&pl=3158&order=NEWEST&page=1&locale=en-US

Real-World Playbook Use Cases

Playbooks in Swimlane Turbine can be applied across a wide range of security operations scenarios. The following are a few specific examples demonstrating how they can be tailored to automate and streamline complex workflows:

- **Palo Alto Networks firewalls—**A playbook can be triggered when the SIEM detects a command and control (C2) threat, identified through Palo Alto's Advanced Threat Prevention subscription. Although the organization may want to block this traffic immediately, an approval process ensures caution. The playbook sends an email containing details of the threat and a request for action. The recipient can review and approve the request by clicking a link directly from their mobile device. Upon approval, Turbine sends the appropriate command to Panorama, distributing the block rule across all relevant firewalls—no need to log in to multiple tools.
- **Amazon AWS WAF (web application firewall)—**When the SIEM logs malicious web traffic targeting a business-to-business API gateway—originating from a subnet with a successful login in the past week—a playbook can be used to automatically apply a "tight configuration" policy for that source IP for a 96-hour window. Simultaneously, the playbook creates a ticket for customer support to contact the client and investigate possible misconfiguration. This approach ensures continued service while addressing security concerns.
- **CrowdStrike Falcon—**If a suspicious file is identified, a playbook can automatically submit it to CrowdStrike's sandbox for analysis. Based on the result—malicious, suspicious, or benign—the playbook can respond accordingly. For malicious files, actions might include adding the file to a block list and pushing indicators of compromise (IoCs) to email and web security tools to prevent reentry into the environment.
- **DFIR evidence gathering—**For digital forensics and incident response (DFIR), a manually triggered playbook allows analysts to initiate evidence collection from a web interface. By entering a hostname, the playbook connects to the machine in question, captures a memory image, collects ephemeral data (e.g., DNS cache), and retrieves relevant logs and key files. The memory image is analyzed using Volatility plugins, with the output summarized into a report that assists analysts in understanding the machine's recent activity.

Swimlane Turbine users are limited only by their imagination when it comes to automation. In practice, analysts and engineers often draw inspiration from one another, sharing automation workflows that eliminate tedious, repetitive tasks. Over time, this collaboration leads to increased productivity, freeing up teams to tackle long-standing projects that deliver meaningful improvements across the security program.

Dashboards and Reporting

It's been said, "If you spend more than five seconds reading your car dashboard, you're going to hit something." Although this statement originally applied to driving, the principle holds true in the fast-paced SecOps world. Situational awareness must be immediate and actionable. Turbine enables this with real-time, wall-mounted dashboards that help teams instantly recognize high-priority alerts, attacks on critical assets, team workloads, DDoS events, and any other metrics that matter to your organization.

Turbine supports both high-level visual dashboards and detailed, analyst-focused views, ensuring the right people see the right data at the right time (see Figure 6). For example, teams can monitor open alerts by severity to ensure prompt attention to the most critical issues. Dashboards can be customized to track specific APT groups, monitor threat activity on key IoCs, or prepare for the next zero-day event, such as Log4Shell.

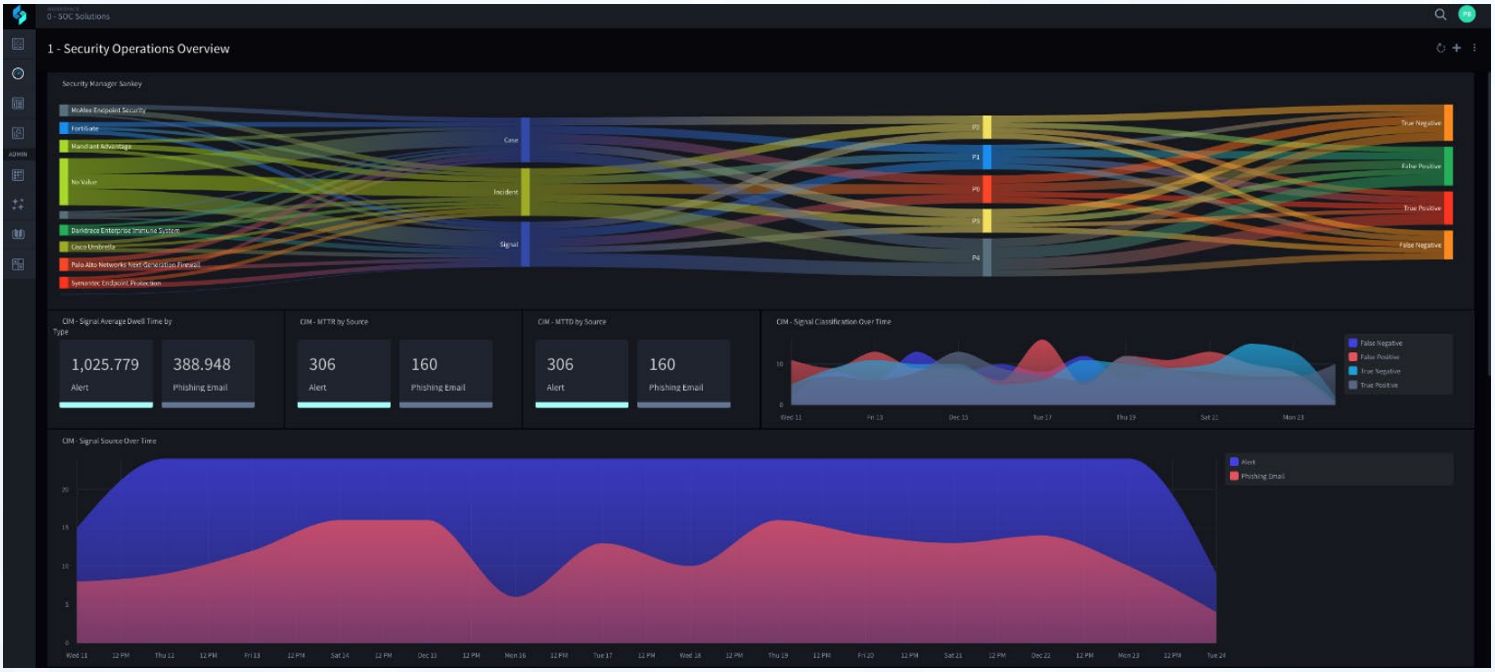


Figure 6. Turbine Dashboard

Operational dashboards also can be used for infrastructure health monitoring. For instance, if a firewall hasn't generated logs in over 120 seconds, it may be experiencing an outage. With Turbine, that anomaly can automatically trigger a playbook to begin troubleshooting or remediation—delivering proactive service assurance without manual intervention.

In addition to dashboards, Turbine offers comprehensive reporting capabilities. These support both operational needs and compliance requirements. One notable example involved a compliance mandate requiring the review of all failed logins on systems handling customer-sensitive data. Initially, analysts were being alerted every time an admin mistyped a password, creating frequent interruptions and lost productivity. The solution: a daily automated report generating a CSV of all failed logins, satisfying the audit requirement without disrupting the team's workflow.

Turbine also delivers value through unexpected and intelligent reporting capabilities, including:

- Automatically generating after-action reports, streamlining post-incident documentation
- Translating reports into other languages on demand, supporting multilingual customers
- Executing ready summaries, such as incident reports from the past six months involving unpatched systems, ahead of critical meetings with leadership

Whether it's delivering fast, actionable visuals for the SOC floor or fulfilling complex reporting requests in seconds, Swimlane Turbine ensures teams are always equipped with the insights they need to act decisively.

Incident Response Workflow Example

Swimlane Turbine automates everything from IoC blocking to forensic collection and user notification—no tab-hopping, no guesswork, just consistent, audit-ready action.

The following illustrates the day-to-day operational efficiency of a mature Swimlane Turbine deployment within a large enterprise SecOps team. Although vendor-neutral in approach, the following scenario references specific integrations to demonstrate real-world capabilities. (For a complete list of supported integrations, refer to **marketplace.swimlane.com**).

In this illustration, Swimlane Turbine is fully integrated with the organization's threat intelligence platform (TIP). IoCs are automatically pulled from the TIP and pushed to the enterprise's EDR system, firewalls, SIEM, and other critical security tools. These "bad lists" are applied in real time to block known malicious activity at the EDR and firewall level, providing preventive controls, while the SIEM leverages the same data for detective controls, scanning both real-time and historical logs for matches.

A typical incident begins when the SIEM ingests a log event indicating that Microsoft Defender has detected potentially malicious behavior on a user's laptop. This triggers a DFIR playbook in Turbine. The playbook orchestrates the following actions:

- Tanium is called to collect forensic artifacts from the host, including OS and firewall logs, ephemeral data (e.g., DNS cache), and a full memory image.
- Turbine queries the CrowdStrike Falcon API to retrieve process execution data, identifying any deviations from the known baseline.
- The file's SHA256 checksum is submitted to VirusTotal for public reputation analysis and also shared with the internal TIP to access proprietary threat intelligence.
- Falcon logs confirm that malware execution was successfully blocked.
- Turbine queries the Microsoft 365 API to validate that no phishing emails were sent from the compromised endpoint.
- Windows Firewall with Advanced Security logs are scanned for any signs of outbound C2 activity.
- The organization's HR system is queried to obtain the user's identity and manager details.

All of this information is compiled into a centralized incident ticket within Turbine. Hero AI summarizes the findings, identifies gaps, and recommends next steps—all of which are reviewed by the assigned analyst.

This streamlined, automated workflow saves valuable time. Analysts no longer need to manually log in to multiple systems, navigate different UIs, juggle varying search languages, or pass multiple MFA checks. If corrective action is required, such as reimaging the affected machine, the analyst already has all the context and the relevant contact information needed to notify the user and their manager of potential disruptions. Swimlane Turbine ensures that incident response is not only faster but also more consistent, comprehensive, and auditable, enabling SecOps teams to operate at peak effectiveness.

Conclusion

Swimlane Turbine enhances analyst productivity by automating evidence collection and orchestrating actions across the entire security stack. This time savings enables security analysts to focus on high-value tasks like analyzing data, making informed decisions, and responding to threats, all before adversaries can achieve their objectives.

Swimlane was originally built with SOC challenges in mind. Over the years, additional functionality has been built on top of the Turbine AI automation platform. The Vulnerability Response Management (VRM) Solution leverages data from your existing vulnerability scanner to enable smarter risk prioritization, leading to faster vulnerability patching. The Compliance Audit Readiness (CAR) Solution reduces your manual spreadsheets, enabling easier evidence collection to produce controls for multiple frameworks. Each Swimlane Turbine module works with the others to make them all more effective.

In far too many security programs, skilled analysts spend more time hunting down data than analyzing threats. Swimlane Turbine changes that.

This paper covered a few of the many ways a SOC can use Swimlane Turbine. We focused on these areas:

- **Integrations—**The Swimlane Marketplace contains 500-plus connectors (at no extra cost!), enabling Turbine to easily talk and listen to the other technologies you already have in your environment.
- **Agentic and generative AI—**Swimlane's Hero AI is integrated into all areas of the product. Analysts can ask interactive questions as they work a case, use it to help write a playbook, and more.
- **Case and incident management—**Turbine's CIM provides an IMS that has more features than some of the dedicated IMS tools on the market. More feature rich, integrated automation features and Hero AI are all included.
- **Low-code playbooks—**The Swimlane Marketplace enables users to download from a selection of more than 2,500 playbooks, which can be customized to meet your specific needs. You also can use Hero AI to create them. More advanced users can write their playbooks in Python or other languages.
- **Dashboards and reporting—**Swimlane Turbine has a robust set of tools to create custom dashboards to improve analyst efficiency or PDF reports.

Turbine also addresses a common issue in larger security teams: inconsistency in incident handling. Analysts often take varied approaches to similar problems, leading to inefficiencies and uneven results. Turbine provides a collaborative platform where teams can define best practices and translate them into standardized, reusable playbooks. This ensures consistent, high-quality execution across all analysts, regardless of their experience level, while significantly reducing the time spent on manual processes.

Beyond improving individual workflows, Turbine fosters stronger team collaboration. Analysts communicate more effectively, align on standards, and accelerate task completion. The result is a more unified, high-performing SecOps team.

Sponsor

SANS would like to thank this paper's sponsor:

SWIMLANE