SWIMLANE TURBINE

Product Overview

Introducing Swimlane Turbine

Low-code security automation that extends visibility and actionability to deliver on the promise of XDR

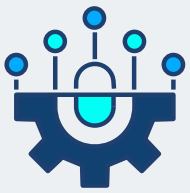
Swimlane Turbine is a breakthrough low-code security automation platform that captures hard-to-reach telemetry and expands actionability beyond the closed extended detection and response (XDR) ecosystem. It is different from the traditional security orchestration, automation and response (SOAR) platforms that are notoriously complex and used exclusively to automate basic security operations center (SOC) workflows like SIEM alert triage, phishing, and threat intelligence.

While these SOC use cases are important, security teams really need the ability to ingest telemetry and apply automation to all aspects of security operations inside and outside of the SOC. This can include automating workflows around privacy, audit, compliance, legal eDiscovery, vulnerability patch management, and user on/off-boarding.

Swimlane has spent the past decade helping the world's largest and most demanding organizations automate security use cases both within and beyond the SOC. Through this experience, Swimlane has harnessed the institutional knowledge and expertise needed to deliver outcomes that satisfy the increasing demands of our customers:

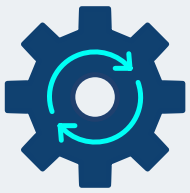
EXTEND VISIBILITY AND ACTIONABILITY

Customers need solutions capable of ingesting , enriching and actioning on large and diverse data sets, allowing security teams to respond to threats the instant they occur.



INTEGRATE WITH ANYTHING

Customers need to unify any type of complex environments by autonomously connecting with tools that are typically siloed from a security perspective, like cloud, IoT, and edge computing.



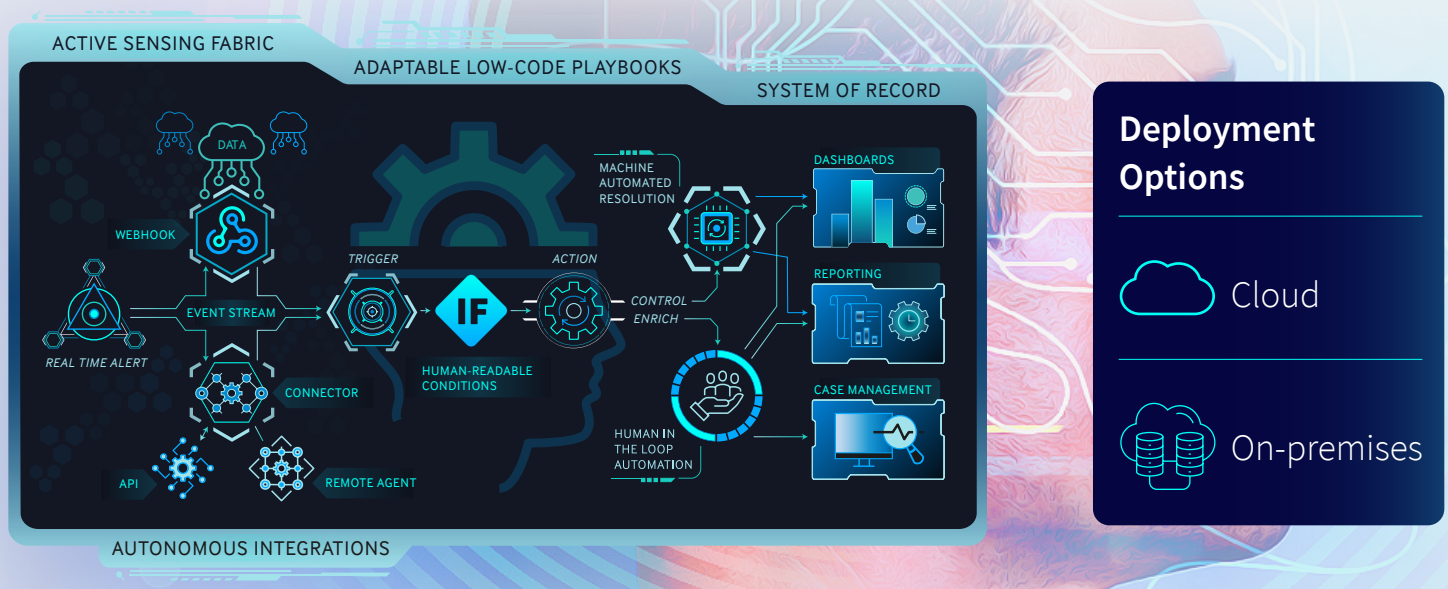
MAKE AUTOMATION APPROACHABLE

SOAR has earned a reputation for requiring a mature SOC team, yet less-mature security organizations are in need of flexible security automation tools to improve the ROI of their security programs.

With the industry's first true system of record for security operations, Turbine Swimlane enables security teams to gain actionable intelligence through KPI metrics like mean-time-to-detect (MTTD), mean-time-to-respond (MTTR), and MITRE ATTACK framework benchmarks.

- Fortune 100 financial company **saves $900k per year** by using Swimlane to automate security use cases outside of the SOC.
- Another fortune 100 Swimlane customer **saves $160,000/month** in labor costs by automating 3,700 hours of work.

Swimlane Turbine Architecture



Action at the Point of Inception

In order to speed MTTR and reduce dwell time, organizations need the ability to identify and take action on changes in their environment closer to the point of inception. Actions taken can either be passive or more aggressive, like isolating an endpoint, turning off an application, or revoking a user's account access. In order to accomplish this, security automation technologies need to be much more present at the time when events occur and new telemetry data is created.

Today, most SOAR technologies are dependent on underlying infrastructure, like SIEM, to get an alert. This causes latency in the response process. It means that before the SOAR takes action, an endpoint agent on a workstation must generate an alert, send it to the centralized manager for the endpoint agent product, then log data is sent to and processed by the SIEM, which then runs analytics, creates an event, and finally sends that alert to the SOAR for response. In examples like this, where the alert has high fidelity, the SIEM does not add enrichment necessary for enabling action. This data aggregation lifecycle makes threat detection and incident response (TDIR) slower and more expensive than it should be.

Swimlane Turbine changes the game of traditional security automation by providing the security industry with the first low-code automation solution capable of handling big data at scale and connecting with broader integration sets. Its groundbreaking capabilities enable security leaders to re-think their SIEM and data analytics strategy so that they find a more cost-effective solution to achieve their goals. Moreover, Turbine delivers a centralized management hub and simplified visualizations of complex attacks in order to unlock the promise of XDR. Security teams who use Turbine to make this shift from a detection strategy to an action-centric strategy will be more successful at identifying sophisticated attackers in near-real time.

Active Sensing Fabric

Reduce Dwell Time with Distributed Big Data Ingestion

The Swimlane Turbine Active Sensing Fabric makes the evolution of security operations possible. Swimlane Turbine is built to ingest data from distributed big data sets. This is important because modern infrastructure must account for various data streams with webhooks, poll requests, pub/sub, file creation, SMS messages, email messages, and IoT. Swimlane Turbine ingests from all of these sources, in addition to SIEM logs as needed, in order to move action closer to the source to reduce dwell time. The Active Sensing Fabric listens across the security ecosystem, taking immediate action directly at the source.

Immediate Actionability with Powerful Pre-processing and Inline Enrichment

Turbine executes on thousands of concurrent automations in order to eliminate noise in the customer environment and mitigate analyst burnout that stems from receiving too many alerts fatigue. The organization's business logic and processes inform the application of custom data filtering, pre-processing, deduplication and inline enrichment in order to reduce data overload so that analysts can respond faster.

Secure Distributed Organizations with Remote Agents

Creating a secured architecture, Remote agents make it easy to connect Turbine to internal applications and systems without spending time configuring complicated networks or multiple VPNs. It enables companies to connect internal applications and systems to Turbine in a highly-secure and frictionless manner. This is especially beneficial for larger, distributed organizations with multiple business units or segmented environments. It is also uniquely valuable for MSSPs who need to manage multiple infrastructures representing a diverse customer base.

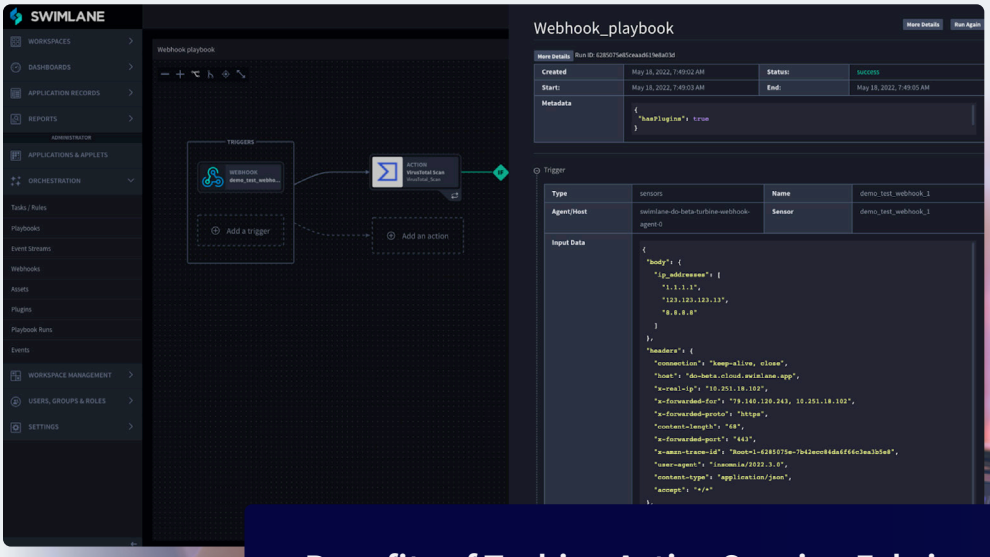
DID YOU KNOW?

Remote agents are dynamic sensors that enable the intelligent collection of hard-to-reach telemetry sources.

"Swimlane Turbine has given us the tools to help our customers accelerate security response by actioning the event at the source," said Cody McGehee, SOAR Engineering Team Lead at ECS Enterprise Managed Services (MSSP). "The remote agent feature is a game-changer as we seek to efficiently manage multiple infrastructures for our diverse customer base."

Simplify Data Ingestion with Webhooks

Extended actionability is made possible by the Turbine webhooks feature. Flexible webhooks enable products, vendors or services to push real-time communication into Turbine. New webhook listeners can be created for any technology that supports webhooks, and can be plugged directly into the playbook building experience within seconds. They are easily managed with flexible authentication options to cover a wide variety of capabilities found in third-party tools. Use of webhooks in playbooks gives analysts real-time visibility into events, so that security teams can drastically improve MTTD and MTTR security metrics.



Benefits of Turbine Active Sensing Fabric

- *Accelerate MTTD, MTTR and time-to-value*
- *Reduce dwell time*
- *Minimize noise from contextless alerts*
- *Mitigates analyst burnout*
- *Simplifies and connects complex and diverse environments*

Integrate Anything

No security vendor has an integration to every version of every product that has ever been made - This is a pipe dream to accomplish. Every organization's infrastructure will always be unique, and when it comes to security, customers cannot afford to wait on a vendor to build new integrations. There is simply no way to keep up with all of the integrations or hire enough people to deliver the breadth and depth of integrations that customers need. — Swimlane is thinking about this differently!

Swimlane understands that to meet customer needs in an ever-changing environment the best way is to build technology capable of enabling security practitioners to integrate with anything, without dependency on the security automation vendor.

Autonomous Integrations

Swimlane Turbine changes the way that API integrations work by delivering autonomous integrations. This innovation will enable customers to conduct real-time discovery on any new integration. This enables security teams to connect to any API without assistance or development resources. Once this instant connection is established, the customer is able to see the list of actions that the connector is capable of, the data and identity types it can send, and pull these actions or triggers into a playbook.

With Turbine, anyone can be an automator – and a truly creative one at that. Domain experts like compliance managers, fraud teams, legal, or HR will be able to build a playbook without waiting for a library, integration, or connector. Better yet, when a connector API definition changes, Turbine will update the connector in real-time from the source provided. Instead of needing to spend precious time developing integrations, security teams can focus on what matters – utilizing integrations to automate any task.

Save Time Deploying and Managing Integrations with Connectors

Swimlane Turbine connectors provide a stable, portable and reliable connection to any API in a customer environment. Turbine enables customers to layer on business logic through playbooks. Turbine connectors are hosted in a new curated marketplace which are accessible to all Swimlane customers.

While connectors will deliver immediate value to customers, this capability is just the beginning for Turbine Autonomous Integrations. The innovation is made possible by years of focus and dedication to the security automation market.

Swimlane built the first integration in 2012. Since then, the company has established a team of developers who build integrations. The company then built specialized tooling to make the work of integrations easier, which has been supported by building out lab environments and automated testing around this process.

Benefits of Turbine's Autonomous Integrations

- *Easily and quickly connect siloed technologies*
- *Minimize dependency on development resources*
- *Achieve the promise of extended detection and response*

Softcat

"With Swimlane, we don't have to try to fit our outcome into a preconceived box that had already been developed. Swimlane allowed us to build something that worked for us and how we operate." - Matt Helling, Head of Cyber Security at Softcat

Make Automation Approchable

SOAR has earned a reputation for requiring mature SOC teams to be equipped enough to handle the technology, but that does not mean less-mature security teams don't need security automation. In fact, it's actually the less sophisticated security organizations who need automation the most because they have smaller teams and are those likely to feel the challenges of the industry's talent shortage more acutely. To multiply the workforce and overcome the security talent shortage, organizations need security automation solutions that democratize automation so that domain experts are able to become citizen automators.

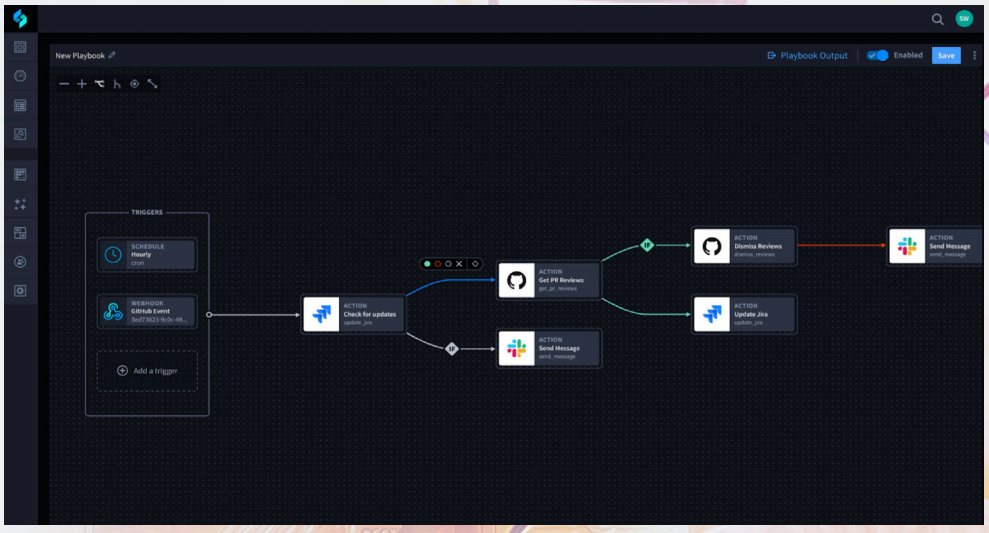
Why Adopting Low-Code Security Automation?

Swimlane's low-code approach to automation sets it apart from other vendors who remain on the no-code or traditional SOAR ends of the spectrum. No-code providers limit power users, marketplaces and partners, while also lacking key automation functionality like case management, dashboards and reporting. Full-code SOAR offerings leave customers dependent on highly-experienced developer resources, and are associated with lengthy error-prone execution cycles.

Adaptable Low-Code Playbooks

The Turbine platform from Swimlane is the first and only solution to enable Security Operations teams (SecOps) to realize the full potential of XDR through a low-code security automation platform that is both approachable enough for those with no coding experience, and sophisticated enough to satisfy the world's most demanding security teams.

Adaptable playbooks in Turbine make it easy to quickly build modular, repeatable playbooks that enrich and process real-time data that is then presented through an ultra-configurable case management system. As a result, humans are brought into the loop of automation when necessary. By automating enrichment, data gathering and standard controls, security teams are able to take action faster and regain time to focus on decisions only humans can make.



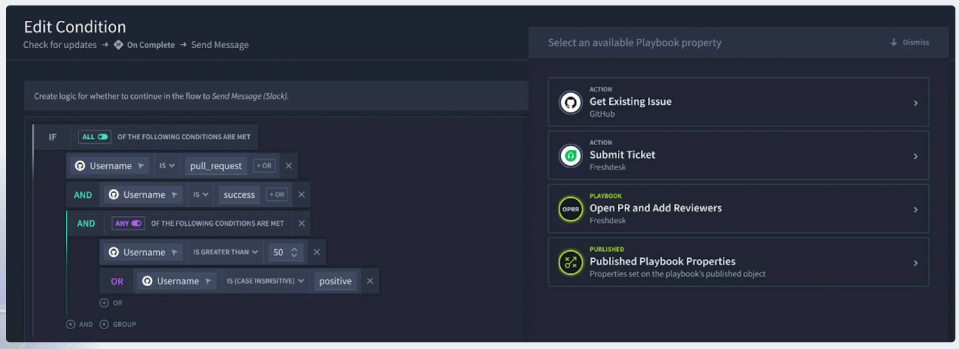
Codeless Conditions Provide a Force Multiplier for SecOps and Beyond

Turbine playbooks enable powerful codeless conditions that make it easy to codify business logic and best practices into playbooks. This human-readable user experience is how Turbine makes playbook-building adaptable and approachable for domain experts and new security analysts. As a result, Turbine customers are able to build playbooks in half the time that it would take with a traditional SOAR tool. It also enables them to more effectively scale security automation beyond SecOps, so that functions like vulnerability management, fraud prevention and data loss prevention teams can benefit from the force multiplier that Swimlane security automation delivers.

Simplify Technology Interactions with Playbook Actions and Assets

Anyone who has built a SOAR playbook knows how complex and rigid this process can be. Turbine makes this process approachable by simplifying technology interactions with playbook actions and assets. The drag-and-drop user interface makes it simple for customers to configure connector actions in playbooks. This ease of use means that automation builders can spend more time building robust response actions instead of worrying about maintaining complex architectures.

Swimlane Turbine customers can use assets as predefined configurations to standardize and accelerate how they authenticate or send data to other systems. An intelligent playbook editor also helps to minimize potential misconfigurations by preventing race conditions in accessible properties. These capabilities make it possible for security professionals with minimal configuration experience to create effective playbooks without first having to learn all of the intricacies of their architecture or struggle through the ordering of data.



Benefits of Low-Code Adaptable Playbooks

- *Quickly and easily build playbooks*
- *Effectively scale business logic and response best practices*
- *Reduce complexity when building playbooks*
- *Regain time to dedicate to new use cases*

Unify Workflows, Telemetry and Teams

The reality is, security teams today lack a centralized management hub. Other industries have this, but security is lagging behind. For sales operations, it's Salesforce; for IT, it's ServiceNow; for HR, it's Workday; but for security, it's not the SIEM. The SIEM offers a solution for big data analytics, compliance and audit purposes. But security leaders really need a system of record that shows them where systems are weak and how operationally efficient their programs are. Such a system should help security practitioners manage everything from vulnerabilities to misconfigurations. It should help leaders measure risk posture improvements, ROI and key security metrics like MTTD and MTTR.

Turbine is the System of Record for Security

Speed Investigations with Robust Case Management

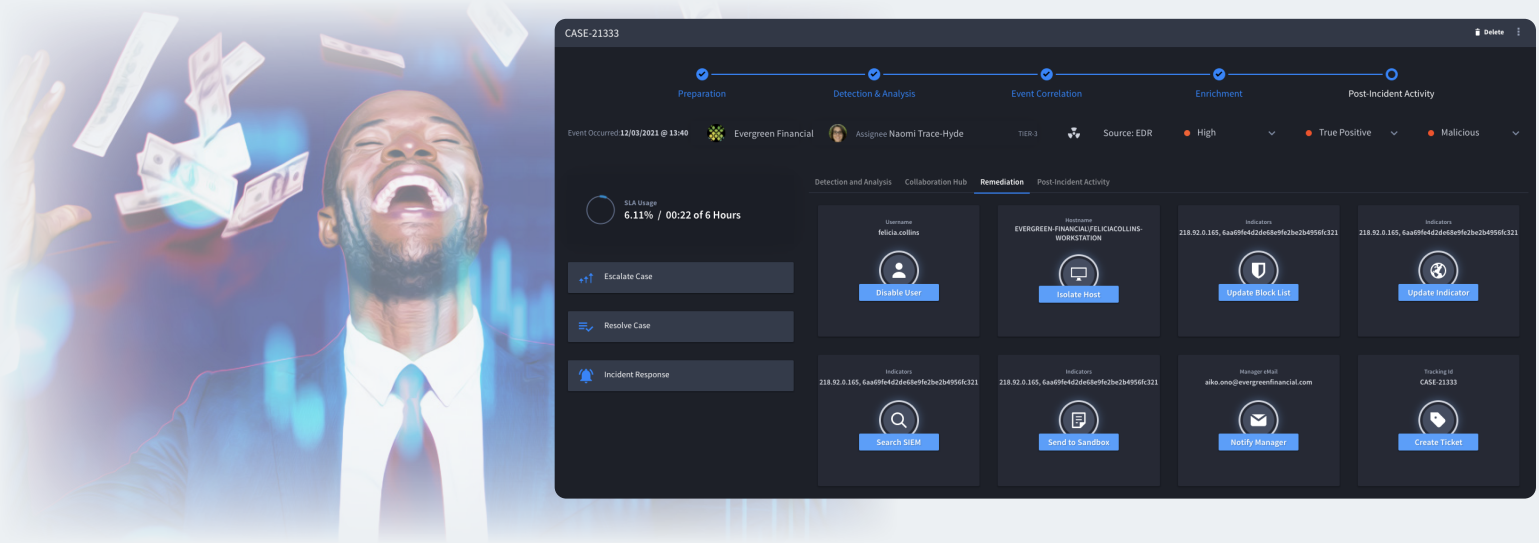
The dynamic case management in Turbine provides direct interaction with all data and actions related to an incident. This provides analysts with the flexibility needed to respond faster. Turbine analyzes and enriches incident data in real-time so that analysts can instantly execute an array of actions specific to the case. For example, from a single case management record, an analyst can click one button to initiate a search using their SIEM, or trigger a control in their EDR platform.

Incident response investigations are the most time-consuming process for SOC analysts. Turbine speeds this process while also enforcing security standards and compliance. With Turbine case management, unique business processes can be institutionalized into the workflow in order to ensure that analysts are working with the right data at the right time.

Maximize People, Process and Technology Efficiency with Customizable Dashboards

In the past decade, security has made the shift from a backroom to a boardroom type of conversation. With elevated visibility, security leaders are more accountable than ever for outcomes and investments. This means organizations need to maximize their people, process and technology efficiencies in order to deliver business outcomes. Leaders need to demonstrate a continuous return-on-investment through key performance indicators like speeding MTTR, MTTD, and the overall maturing of security programs. Doing so is often a difficult talk with complex and distributed environments.

Turbine dashboards provide security teams with actionable insights for assessing performance and optimizing critical operations. These come out-of-the-box with built-in SOC dashboards so leaders can quickly see where they need to reallocate resources to avoid employee burnout,
or understand which employees may need additional training. With Turbine, security leaders are empowered to easily identify trends over time by looking at historical records, other tools or observables across multiple business units. Dashboards provide a centralized management hub for security teams to gain an end-to-end view of their security posture.

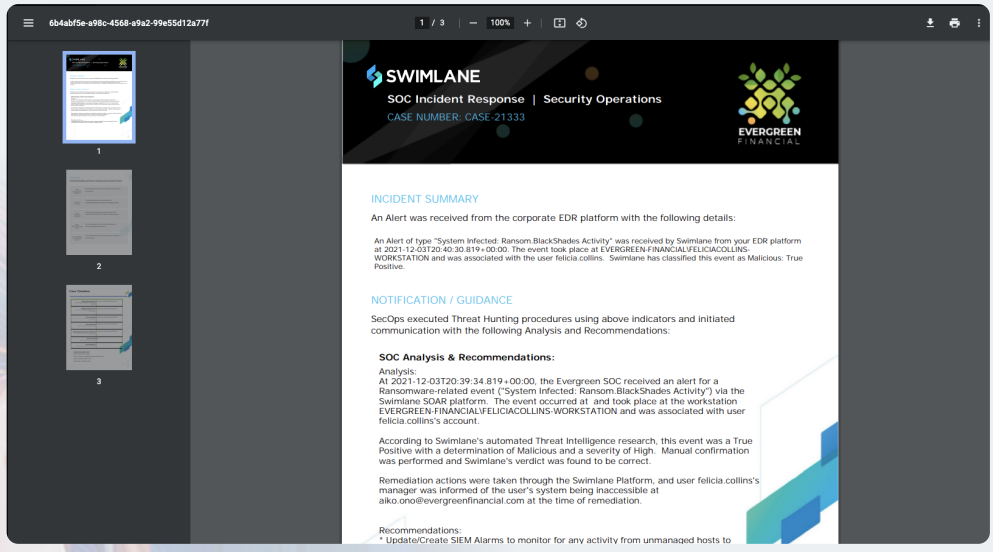


Track Mean-Time-to-Resolution (MTTR) and Establish ROI

Turbine makes it easier than ever to measure the ROI of individual security tools and to efficiently manage budgets. Understanding technology effectiveness at this level means that security leaders are able to methodically improve MTTR. self-documenting playbooks in Turbine track every step in the incident response process so that dashboards are populated with real-time data that illustrates security operations trends. These details make it clear to see how much time and money is saved by automating previously manual tasks.

Increase Collaboration with Real-Time Reporting

While dashboards are great for real-time data and managing operations, there is also a need for point-in-time reporting. Turbine's low-code visualization studio enables SOC managers to build custom reports that can be exported on a scheduled cadence to inform the CISO or other stakeholders. When critical situations occur, Turbine can create real-time reports with detailed insights that pinpoint problematic areas of security operations. This makes it easier to analyze retrospectives and develop a counter strategy.



Benefits of System of Record

- *Efficiently and effectively resolve cases with real-time enriched incident data*
- *Make better and faster decisions with comprehensive incident context*
- *Accelerate defined and repeatable incident response processes*
- *Quantify key performance metrics like ROI, MTTR and MTTD*

SWIMLANE

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

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. For more information, visit swimlane.com or join the conversation on LinkedIn, Twitter and YouTube.