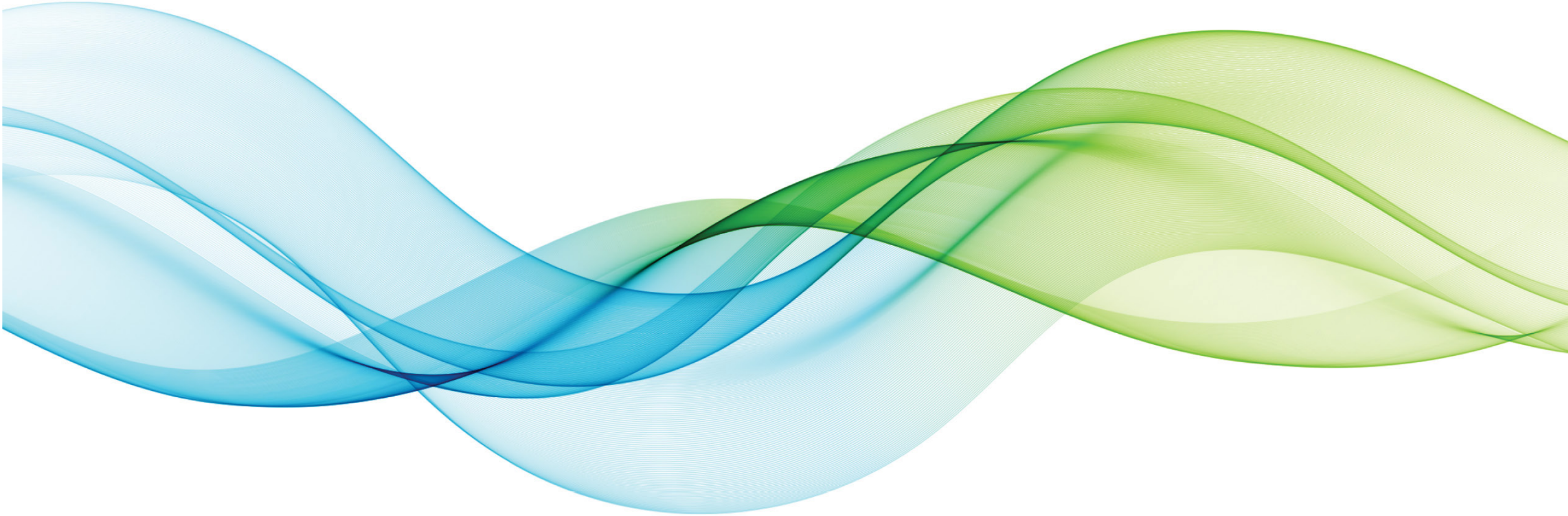
TAG CYBER

RETURN ON INVESTMENT (ROI) ANALYSIS:

SWIMLANE SECURITY AUTOMATION

LARGE ENTERPRISES EXPERIENCE 240% ROI WITH SWIMLANE



DR. EDWARD AMOROSO, TAG CYBER

SWIMLANE

RETURN ON INVESTMENT ANALYSIS OF SWIMLANE SECURITY AUTOMATION

LARGE ENTERPRISES EXPERIENCE 240% ROI WITH SWIMLANE

DR. EDWARD AMOROSO

RETURN ON INVESTMENT STUDY FINDINGS

The return on investment (ROI) analysis and practical case studies included in this report suggest that customers should achieve major savings by deploying Swimlane Turbine to support security automation. Specifically, we show the following:

- **Mid-Sized Retail:** A midsized[1] retail company running a midsized security operations center (SOC) under a set of reasonable operating condition assumptions could expect to see a **160% ROI** in one year by investing in Turbine.
- **Large Financial Services Company:** A large financial services company running a larger SOC under reasonable operating condition assumptions could expect to see a **240%** ROI in one year by investing in Turbine.

TAG Cyber analysts generated these case studies by using conservative estimates that did not include any contributions from qualitative benefits accrued upon deployment of the Turbine platform. The report below justifies the ROI analysis, case studies and ROI conclusions drawn.

EXECUTIVE SUMMARY

This report provides a quantification of the financial returns and benefits that enterprise security teams should expect when they deploy Swimlane Turbine for security automation. Turbine works by orchestrating the data collection, integration and analysis tasks demanded in a typical security operations center. Benefits include major savings in staff, tools and response efficiencies. Swimlane customers should expect to find the platform extensible beyond legacy security orchestration automation and response and can thus extend security automation beyond SOC use cases, which increases their ROI by delivering value to the broader security organization.

The analysis uses TAG Cyber's ROI methodology, which we developed for use with commercial cybersecurity solutions in the context of modern enterprise security protection programs for CISO-led teams. The analysis, which we have tailored to Swimlane and its usage scenarios, revealed that, under reasonable assumptions for a typical enterprise, investment in Swimlane's Turbine can result in significant positive financial returns beginning in-year with the investment. This ROI is demonstrated for enterprise teams of varying sizes.

Using this TAG Cyber ROI methodology, an enterprise security team can easily adjust the equation variables included here to tailor their own estimated impacts based on more local assumptions.

OVERVIEW OF THE SWIMLANE SOLUTION

Swimlane offers a next-generation security automation solution that features low-coding, thus removing any dependency on security teams and software developers to build their own integrations and set up their own automation. Turbine instead allows enterprise teams to create automation in a simple manner to improve their productivity and analysis results.

The Turbine platform offers the following four value-driven functions for security organizations and their associated SOC operations teams:

- **Active Sensing Fabric Extends Visibility and Actionability:** Turbine includes the capability to ingest relevant data at scale for security processing. This is essential for larger environments with Big Data implementations that require automated security orchestration.
- **Autonomous Integrations Enable Connections to any Application Programming Interface:** Turbine includes advanced automated support for security teams to enable autonomous integrations that can connect different technologies and systems via their application programming interface.
- **Adaptable Low-Code Playbooks Make Automation Approachable:** Turbine supports the creation of security automation and orchestration playbooks without depending on developers to build integrations or write complex scripts. This is essential for creating an adaptable implementation that matches the needs of the local environment.
- **System of Record Provides Actionable Intelligence:** Turbine also offers support for actionable intelligence based on the assessment of key performance indicators and risk posture assessments that it embeds in a system of record for security and management teams.

RETURN ON INVESTMENT METHODOLOGY

The TAG Cyber ROI methodology follows a simple equation-based approach where the investment and the quantified returns are normalized into a common financial basis. Qualified returns are not included in the analysis but are considered separate dividends.

Three possibilities emerge for a given investment case, and technically only the accretive case is a balanced equation. In the investment case, the costs incurred exceed the qualified returns, and in the positive return case, the costs incurred are lower than the qualified returns.

***Accretive Case*:**
Incurred Costs = Quantified Returns

***Investment Case*:**
Incurred Costs > Quantified Returns
Incurred Costs = Quantified Returns + Investment

Positive Return Case:
Incurred Costs < Quantified Returns
Incurred Costs + ROI = Quantified Returns

APPLYING THE ROI METHODOLOGY TO SWIMLANE

The specifics of incurred costs and quantified returns will vary based on the platform selected, existing systems in the local environment and other factors. For Swimlane Turbine customers, we expect that different SOC teams, tools and other local conditions will drive different assumptions. Nevertheless, we make the following general estimates for our analysis:

Incurred_Costs:
1. Platform Licensing Fees (for Turbine)
2. Deployment Costs (costs to support Turbine deployment)
3. Maintenance Costs (costs to maintain Turbine annually)

Quantified_Returns:
1. Staff Salary Savings (reduced costs via efficiency and productivity gained from Turbine automation)
2. Staff Support Savings (fewer staff implies less support cost)
3. Tool Savings (Swimlane automation saves on support tools)
4. Response Cost Savings (automation reduces number of incidents that impact company profitability)

Using this methodology, enterprise teams can select their own preferred values to determine the ROI for local deployment and use of Turbine. In this report, we will make some reasonable general estimates to illustrate the corresponding results.

The equation that results from this overall approach can be represented using the factors introduced above:

Incurred_Costs = Platform Licensing Fees + Deployment Costs + Maintenance Costs

Quantified_Returns = Staff Salary Savings + Staff Support Savings + Tool Savings + Response Cost Savings

The ROI implementation thus supports the following three use cases for accretive, investment and positive return scenarios:

> ***Accretive Case*:**
> **Platform Licensing Fees + Deployment Costs + Maintenance Costs = Staff Salary Savings + Staff Support Savings + Tool Savings + Response Cost Savings**
>
> ***Investment Case*:**
> **Platform Licensing Fees + Deployment Costs + Maintenance Costs = Staff Salary Savings + Staff Support Savings + Tool Savings + Response Cost Savings + Investment**
>
> ***Positive Return Case:***
> **Platform Licensing Fees + Deployment Costs + Maintenance Costs + ROI = Staff Salary Savings + Staff Support Savings + Tool Savings + Response Cost Savings + Investment**

The remainder of this document provides a detailed analysis of these factors with justification for our proposed reasonable estimations of the financial effects of a Turbine deployment and use in a typical enterprise. We show that under reasonable assumptions, the use of Turbine will result in a positive return use case for many typical enterprise environments. As mentioned above, enterprise teams can adjust our factor assumptions to tailor the ROI to local conditions.

SUMMARY OF SWIMLANE TURBINE COST FACTORS

We categorize the costs to deploy Turbine at a high level into the following four specific budgeted areas on an organizational income statement:

- **Platform:** These are costs incurred by an organization that involves a payment to an external platform vendor. These are direct payments from a security team's budget and can be significant for larger platforms.
- **Infrastructure:** These are costs incurred by an organization for services, software and other related resources required for a given platform. These are sometimes not direct payments incurred by the security team but are IT or hosting costs.
- **Staff:** These are the loaded costs incurred by an organization that involve the salaries, benefits and related costs for full- and part-time employees. This is typically the largest line item on a CISO's annual budget.
- **Consulting:** These are the fees paid externally to consultants to augment work being done by the team's full- or part-time employee staff. Consultants do not come with loaded benefits but are often more expensive than employees on an hourly basis.

The result of this cost grouping is a 4 X 7 matrix (Figure 1) that we can use to demonstrate which types of costs an enterprise will incur before and after using Turbine.

	***Costs Additions* to Deploy Swimlane** *(Above Normal Run Rate)*			***Costs Reductions* from Swimlane Deployment** *(Below Normal Run Rate)*			
	Licensing	**Deployment**	**Maintenance**	**Staff Hiring**	**Staff Support**	**Tool Costs**	**Response Costs**
Platform	*License Fees to Swimlane*	*N/A*	*Maintenance Fees to Swimlane*	*N/A*	*N/A*	*Lower Tool Related Costs*	*Lower Response Platform Costs*
Infrastructure	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*Lower Infrastructure Related Costs*	*N/A*
Staff	*N/A*	*N/A*	*N/A*	*Reduced New Staff Salaries*	*Reduced Staff Related Costs*	*N/A*	*N/A*
Consulting	*N/A*	*Consulting Fees for Deployment Assist*	*N/A*	*Reduced Consulting Fees*	*Reduced Consulting Related Costs*	*N/A*	*Lower Response Service Fees*

Figure 1. Cost Unit Matrix for Swimlane

We include the explanations and rationale for these cost additions and reductions in the next sections, along with the ROI equation.

SWIMLANE TURBINE COST ADDITIONS

Turbine cost additions (i.e., costs incurred by a customer when they purchase and deploy the product) include the following items from Figure 1:[2]

1. **License Fees to Swimlane:** This is the payment made to Swimlane for the Turbine platform, which will vary based on terms and conditions.

2. **Consulting Fees for Deployment Assistance:** It is not uncommon for teams to hire consultants to help with deployment since these are one-time events.

3. **Maintenance Fees to Swimlane:** Ongoing maintenance paid to Swimlane will vary based on terms and conditions.

In the case studies (below) we make broad financial estimates of these cost additions to support a more tangible ROI analysis. Readers can change or tailor the estimates to their own local conditions.

SWIMLANE TURBINE COST REDUCTIONS

Turbine cost reductions (i.e., reduced costs a customer can achieve when they purchase and deploy the product) include the following items from Figure 1):

1. **Reduced New Staff Salaries:** This includes reductions in the need for additional salaries once Turbine is deployed, thus reducing the need for new SOC team members or other security functions.

2. **Reduced Consulting Fees:** This includes reductions that occur when Turbine is deployed, thus reducing the need for additional new security consultants.

3. **Reduced Staff-Related Costs:** This includes all the various support costs that come with having larger security teams that demand costly training, tools and other services.

4. **Reduced Consulting-Related Costs:** This includes all the various support costs that come with having more consultants who need costly training, tools and other services.

5. **Lower Tool-Related Costs:** This includes any tool or platform costs that are reduced by installing Turbine.

6. **Lower Infrastructure-Related Costs:** This includes any infrastructure costs that are reduced by installing Turbine.

7. **Lower Response Service Fees:** This includes reduced incident response costs that occur by lowering the likelihood of incidents via Turbine's low-code automation.

As with the cost additions, we will make broad financial estimates of these cost reductions in our case studies to support a more tangible ROI analysis. Again, readers can change or tailor the estimates to their own local conditions.

SWIMLANE ROI EQUATIONS

Establishing ROI for Swimlane Turbine involves an equation with payment-made on the left side and savings-out on the right side. Swimlane customers will see savings each year, so this will be shown as an annual ROI. The equation that results will be arranged as follows:[4]

Annual ROI:
Annual_Incurred_Costs + ROI = Annual_Quantified_Returns

The specific variables for cost additions and cost reductions will follow the factors discussed in the sections above. Rather than show the equations generally, we will use the case studies below to exemplify the types of ROIs that might be expected. Any readers interested in obtaining an Excel spreadsheet representation of the equations so that they can perform calculator-type tailored analysis should contact Swimlane directly.

CASE STUDY 1: MIDSIZED RETAIL COMPANY

This first case study assumes that a midsized (sub-Fortune 500) retail company deploys Turbine to obtain the benefits of security automation.[3] The estimated annual costs for the platform licensing, maintenance, and deployment beginning in 2023 are as follows:

Swimlane Turbine License	**$500K**
Total	**$500K**

The annual estimated savings for the platform are offered under the assumption that three meaningful incidents are avoided each year (due to the automated support) that would have normally required forensic, response or legal support, and that two new SOC hires are avoided by installing Swimlane Turbine, are as follows:

Reduced New Staff Salaries (2 FTE)	**$400K**
Reduced Staff-Related Costs	**$300K**
Lower Response Costs	**$600K**[5]
Total	**$1.3M**

These costs and savings imply that this midsized retail company would experience a significant annual ROI. **In this case, the return on a $500K investment for a midsized company is 160%.**[6] This ROI analysis leaves out 100% of the qualitative benefits that come with improved and streamlined automation across the security infrastructure for the retail company. Such qualitative benefits would justify the financially accretive investment in this case.

CASE STUDY 2: LARGE FINANCIAL SERVICES COMPANY

This second case study assumes that a much larger (Fortune 100) financial services company deploys the Swimlane Turbine solution to obtain the benefits of security automation.[3] The estimated annual costs for the platform licensing, maintenance and deployment beginning in 2023 are as follows:[7]

Swimlane Turbine License	**$800K**
Total	**$800K**

The annual estimated savings for the platform assume that IT service management (ITSM) costs for workflow, inventory and related tasks are reduced, three major incidents are avoided (due to implementing Turbine) that require forensic, response or legal support, and that three FTE hires are avoided due to the automation support. The result is the following:

Reduced ITSM Platform Savings	**$500K**
Reduced New Staff Salaries (3 FTE)	**$700K**
Reduced Staff-Related Costs	**$600K**
Lower Response Costs	**$900K (at $300K/incident)**[8]
Total	**$2.7M**

These costs and savings imply that this large financial services company would experience annual savings of $2.7M. **In this case, the return on an $800k investment for a larger company rounds to 240%.** Note that this ROI analysis also leaves out 100% of the qualitative benefits that come with the security automation benefits of Turbine.

FOOTNOTES

[1] Return on investment (ROI) analyses must consider the size, scale and scope of the target enterprise in determining the impact of the security solution under consideration. While it is difficult to specify the differences between large, midsized and smaller enterprise companies, one can generally agree that larger firms will have well-funded security budgets with teams using most if not all available security tools. Midsized companies will have more modest teams which must be more discerning about their budget. Small businesses will often have little or no in-house security support, generally opting to use the security features available from their cloud, IT service or even network service providers.

[2] While the cost reductions in this section apply to the SOC, where most Turbine customers would expect to start with a platform ROI analysis, the flexibility and extensibility of Turbine enable organizations to apply security automation beyond standard SOC use cases. As a result, the benefits and returns apply more broadly than just within the SOC, and as such, Turbine customers should expect to experience a higher ROI than presented in the more conservative estimate shown in this section.

[3] Using Turbine, SOC teams can expect to automate large numbers of actions which will result in saving many human-hours. SOC teams can also expect to reduce the number of manual interventions taken by a meaningful percentage which will result in their mean response times going down considerably. This will reduce the number of breaches they can avoid.

[4] Readers should note that license, deployment and maintenance fees will vary significantly between different organizations. No present or future customer of Swimlane, for example, should use the case studies here as representative of the pricing they should expect or seek. Detailed information on platform pricing must be obtained from Swimlane directly. The values used here are for representational purposes only to demonstrate the ROI concept using concrete values.

[5] To vary the analysis, we assume that response costs are $600K for three incidents. Larger firms will experience higher response costs (as demonstrated in the second case study). Organizations should use local numbers for their response costs, but the numbers used here are typical of most modern corporations and government agencies.

[6] ROI is calculated by subtracting the initial cost of the investment from its final value, then dividing this new number by the cost of the investment and then multiplying this number by 100.

[7] Readers should note that license, deployment and maintenance fees will vary significantly between different organizations. No present or future customer of Swimlane, for example, should use the case studies here as representative of the pricing they should expect or seek. Detailed information on platform pricing must be obtained from Swimlane directly. The values used here are for representational purposes only to demonstrate the ROI concept using concrete values.

[8] As noted previously, we assume a higher response cost for the larger firm at $300K per incident, which is reasonable given empirical evidence over the past decade. Also as noted previously, organizations are encouraged to insert their actual numbers to localize the ROI analysis.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Swimlane Inc. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.