Automate to Elevate:

13 Automation Use Cases for Your SOC and Beyond

The Need for Automation in and Beyond the Security Operations Center (SOC)

SWIMLANE

Introduction

One-third of organizations surveyed in the 2023 Cyber Threat Readiness Report believe that they will never have a fully-staffed team. As attacks continue to escalate in frequency and sophistication, security teams need automation to mitigate alerts, connect siloed telemetry sources, and ensure overall security operations (SecOps) efficacy.

Analysts are dealing with up to 150,000 alerts per day, with 64% going unaddressed. The time-intensive nature of having to manually triage alerts and large volumes of security data means that valuable hours end up being spent on routine and repetitive tasks. This leaves little room for proactive threat hunting and critical analysis. As a result, analysts struggle to see clear signals across the security operations center (SOC), resulting in slower mean-time-to-respond (MTTR) and an elevated risk.

Automation is the only way to overcome these common SOC challenges. A low-code security automation platform is the key to improving threat detection and incident response, while also automating security operations processes outside the SOC. This is enabling many organizations to use security automation today to maximize the return on investment (ROI) of their entire cybersecurity stack.

Continue reading this ebook to learn about common, strategic, and even unconventional automation use cases that organizations are adopting today.

SOC Automation Essentials

- Phishing
- Alert Triage
- Threat Intelligence

Automate Beyond SOC Basics

- Insider Threats
- Employee Off-boarding
- Identity & Account Management
- Ransomware
- Vulnerability Management

ROI Maximizing Automation

- Supply Chain Integration
- Anti-Cheat
- Physical Security
- Fraud

Table of Contents

Don't Take the Bait: Why **Phishing** is the Most Common Automation Use Case

Phishing is a continuous challenge for organizations worldwide. Despite robust security measures and training programs, attackers continue to bypass these defenses. As a result, phishing causes 33 billion security incidents annually. The potential financial losses associated with phishing is estimated to reach a staggering 8 trillion dollars.[1]

> "To get solutions to help us process those phishing emails faster was the number one thing we needed inside automation. We found Swimlane to be one of the few products that actually allowed us a more versatile and custom build into automation"
>
> Zac Tielkin, Chief Cyber Forensicator
>
> DIGITAL INVESTIGATIVE GROUP

Most phishing attacks occur within 43 minutes of the email being opened. It takes analysts an average of 30 minutes to manually triage just one phishing email. The process of triaging phishing alerts is often associated with a high percentage of false positive alerts. This combination of high threat frequency and low alert fidelity amounts to phishing being an impossible use case to manually maintain.

This is why leading organizations like the Digital Investigative Group rely on low-code security automation to triage phishing alerts. These automation platforms offer pre-built phishing solutions that help customers quickly resolve phishing alerts. After implementation, organizations are able to respond to all phishing events in less than three minutes.

1 *The State of Email Security 2023, Mimecast*

Stay Afloat: Achieve Efficient **Alert Triage**

Security teams must deal with multiple detection sources, each with its own contextual information. This complexity requires analysts to be proficient in a range of tools, including Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Threat Intelligence. This creates a high barrier to entry for new analysts, as they must become experts in multiple systems before they can triage alerts effectively.

Manual processes are becoming less effective today's rapidly evolving threat landscape. Human error is a persistent issue that results in 70% of alerts going unnoticed during manual investigations. This failure rate is compounded by an overwhelming alert volume that can be as high as 150,000 alerts per day with a 50% false positive rate.[1]

This creates an additional burden on security teams, as analysts must spend precious time sifting through false positives, reducing their capacity to identify and address true positives.

As an example, NTT Data automates up to 90% of incident response processes across their security operations with low-code automation. This saves analysts up to 14 minutes per alert while reducing the risk of missing critical security incidents.

> "I'm 100% convinced that every customer that is operating a SIEM system, that's operating a log management solution, a SOC whatsoever—if they want to survive, they need some kind of automation."
>
> Patric Schraut
> SVP Cybersecurity
> NTT DATA

1 https://swimlane.com/blog/too-many-siem-alerts-use-sao/

From Reactive to Proactive: **Threat Intelligence**

Manual processes impose significant time constraints on security teams, forcing them to react to threats instead of hunting them. Effectively harnessing and correlating cyber threat intelligence data from disparate sources is essential to stay ahead of the expanding threat landscape.

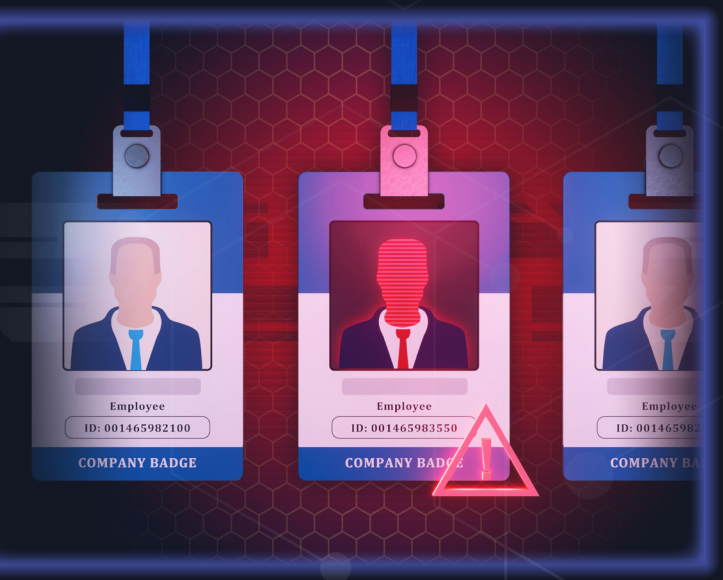
Organizations can improve their threat intelligence by analyzing indicators of compromise (IOCs). However, the manual process of delving into logs, scrutinizing packet captures, and accessing third-party systems is not only time consuming, but is also susceptible to human errors. The solution lies in the ability to efficiently consolidate, enrich, and correlate Telemetry from siloed sources.

Companies such as RV Connex rely on low-code security automation to bring together intelligence sources and enhance their SOC maturity.

> "In order to mature our security operations, we knew it was necessary to advance how we monitor and respond to threat intelligence by taking a more proactive approach to security operations."
>
> Tanajak Watanakij, CISO
> **RV CONNEX**

Insider Threats:
The Danger Within

Insider threats pose a significant challenge for businesses globally. More than 50% of organizations have faced insider threats in the past year.[1] Common insider threat scenarios include malicious data exfiltration and intellectual property theft. Insider attacks can cause a wide range of negative impacts on affected organizations, such as brand damage, operational disruption and customer attrition.



Insider threats can be even more difficult to detect and prevent than external cyber attacks. Trusted insiders have approved access to the network and services. This makes it challenging for analysts to distinguish legitimate employee behavior from malicious data leaks. The increased use of cloud applications, home networks and personal devices with access to corporate resources make organizations increasingly vulnerable to insider threats.

Security teams who leverage low-code automation to detect and take action on insider threats are able to accelerate insider threat investigations and remediation. Automation platforms with collaboration features also help to bring stakeholders like HR and legal teams into the loop of security automation for investigations.

1 *The 2023 Insider Threat Report by Cybersecurity Insiders*

How to Safeguard the Exit: **Employee Offboarding**

The annual employee turnover rate in the US is 18%,[1] yet 71% of organizations don't have a formal offboarding program.[2] Employee offboarding is a critical process to ensure credentials and data do not walk out the door with the individual, creating a compromise for the organization.

32% of organizations have a partially automated offboarding process, while only 5% have a fully automated process. 50% of insider compromise is due to failed employee offboarding and revoking access to internal systems.

The manual offboarding process often involves time-consuming and error-prone tasks, such as disabling user accounts, revoking access privileges, and collecting company assets. Most of these tasks are often delayed or overlooked, leaving security gaps and exposing sensitive data. 90% of employee offboarding processes can be automated and visualized into a customized system of record, enabling IT, HR and SecOps teams to efficiently collaborate.

1 *Aberdeen Strategy & Research*
2 *https://www.zippia.com/employer/offboarding-statistics/*

"What we like about Swimlane is the fact that it also allows our internal IT department to automate certain processes like JMLs (joiners, movers, leavers)."

Matt Helling,
Head of Cyber Services

Softcat

Access Granted:
Identity and Access Management (IAM)

Identity and access controls are a critical Zero Trust principle. Automation can help identify vulnerabilities and potential attacks, accelerate responses to compromised accounts, streamline remediation processes, and revoke elevated access privileges in a fast-paced technology environment.

Many SecOps teams lack visibility into IAM and privileged access management (PAM) tools. This blindspot hampers analysts' ability to effectively monitor user accounts, privileges, and access rights across systems and applications. Complex remediation processes involving multiple teams and siloed technology can result in further delays and errors.

Security automation is a practical necessity for managing identity and access controls in alignment with Zero Trust. It drives efficiency and empowers analysts to react promptly to compromised accounts which minimizes the impact of security incidents.

Lock Down Data's Fate: **Ransomware** Prevention

Ransomware is a significant challenge for analysts due to its ever-evolving nature and its potential to cause severe damage to organizations. 49% of analysts state that Ransomware is the most common incident they face.[1] Many organizations have made ransomware preparedness one of their top five business priorities.

Despite the attention and prioritization that ransomware receives, it is still a huge challenge for security teams to overcome. It is difficult to manually prevent because attackers exploit vulnerabilities and develop new variants constantly.

It is impossible for security analysts to stay ahead of this threat on their own. Swift identification, containment, and crucial decisions are essential to minimizing the impact. While traditional incident response processes and siloed SOC tools fall short, automation is the only way that organizations can strengthen their defenses and decrease their ransomware risk exposure.

1 *2022 Vulnerability Intelligence Report, Rapid 7*

Stay Ahead of the Threats: **Vulnerability Management**

Unpatched, unrecognized, and misconfigured hardware, applications, security stacks, systems, endpoints, and cloud services can result in massive security breaches via open ports, configuration settings, and unpatched vulnerabilities.

Security teams need the ability to prioritize and address multiple concurrent vulnerabilities based on severity. Limited technology integration and team collaboration hinders SOC visibility and timely actions. Even if an organization already has qualified staff in place, manual scanning is time-consuming and error prone. Employees' time and talent can be better utilized by removing the significant leg work associated with manually monitoring and managing vulnerabilities 24×7.

Low-code security automation solutions streamline vulnerability scans and provide security teams with human-readable vulnerability reports. Automation adds important contextual data like prior vulnerability scan results, analyst notes, and known and accepted risk elements so that analysts can make the right decision when it comes to vulnerability management.

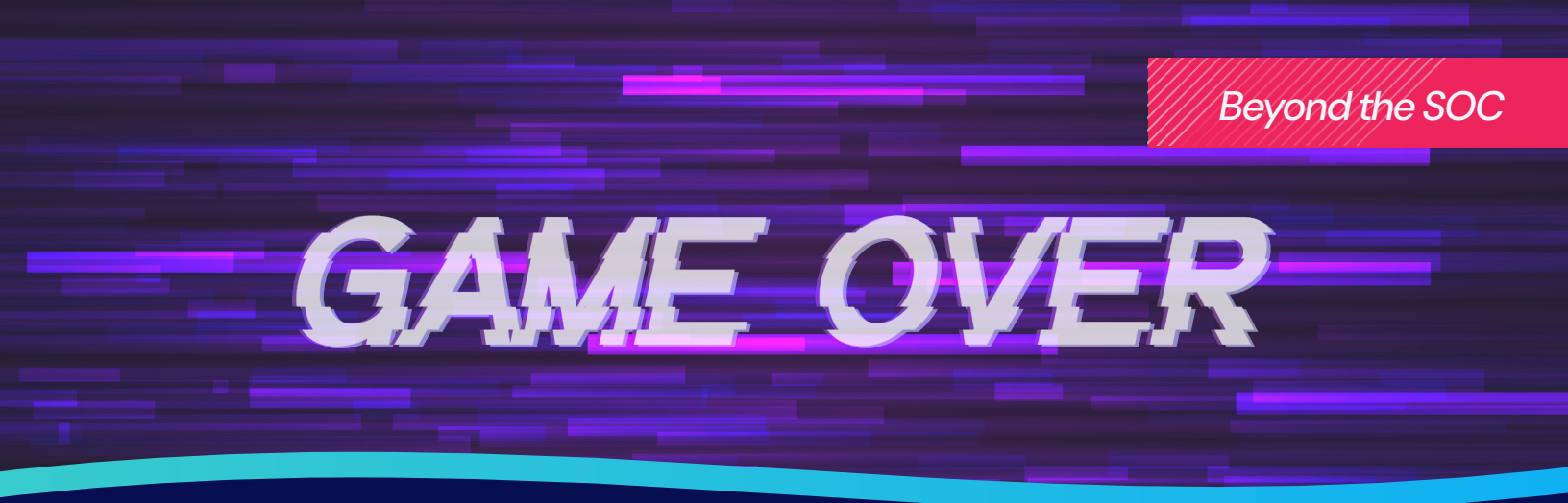
Beat **Open Source Threats** at Their Own Game: **Software Supply Chain** Defense

The use of open source software (OSS) has become an integral part of software supply chain management. To address threats specific to OSS consumption, the S2C2F (Software Supply Chain Cybersecurity Framework) has been developed. The S2C2F framework focuses on identifying, assessing, and mitigating risks associated with OSS usage in software supply chains.

Open source software (OSS) consumption introduces various threats that can be exploited by malicious actors and jeopardize its security. For example, accidental vulnerabilities within OSS code can serve as entry points for malicious actors.

Attackers may compromise the compiler used during the OSS build process, enabling the introduction of backdoors and compromising the entire software supply chain.

Without low-code security automation, SOC teams would need to individually log into every security tool to be able to search for and block IOCs that were used as part of this phishing campaign. Low-code security automation and proper case management help to quickly respond to any threat by bringing down the mean time to resolution (MTTR), reducing errors and false positives during the investigation process.



Ready Player One?
Anti-Cheat Investigations & Response

The gaming industry is expected to grow at a 13.19% CAGR by 2030.[1] Gaming and betting companies recognize the critical importance of preventing player exploitation on their platforms. The negative consequences of cheating and exploitation can significantly impact companies operations and reputation. Therefore, it is essential for gaming and betting companies to prioritize fair play, prevent system exploitation, and uphold the trust of their user base while preserving the overall integrity of their platforms.

Efficiently identifying and addressing cheating or suspicious activity is a significant challenge. Manually investigating reports from users and sifting through massive amounts of telemetry data is a time-consuming and daunting task. The burden of this process is why only 5% or less of investigations are completed.

With low-code security automation, organizations can make quick decisions on whether to suspend, ban, or classify an issue as a false positive. This proactive approach to cheating methods ensures fair game-play which enhances the overall gaming experience. As a result, organizations preserve player trust and the integrity of the gaming environment.

1 *Market Research Future (MRFR)*

DLPower Your Defenses: Automate Breach and Data Loss Prevention

In the contemporary business landscape, data loss prevention (DLP) continues to be a pivotal concern for most companies. Data is the linchpin of operations and its vulnerability holds far-reaching consequences, including financial losses, reputational harm, legal penalties, and erosion of trust.

Analysts are swamped as threats emerge from all directions. The combination of hybrid work models, changing regulations, and rising cyber dangers like insider breaches, cyberattacks, ransomware, and phishing intensify the daunting task of securing sensitive data for businesses. As companies digitalize operations and embrace cloud platforms, vulnerabilities multiply, complicating the protection of proprietary data. These challenges arise due to the surge in storing and sharing confidential information online.

These factors underscore the importance of implementing effective DLP strategies to safeguard sensitive information and maintain the integrity of businesses in this data-driven age. By leveraging the power of security automation, organizations can streamline real-time threat detection, policy enforcement, intelligent data classification, proactive risk mitigation, and compliance management.

Conquer Real-World Threats with **Physical Security Automation**

Physical threats can have terrible consequences for individuals and companies. Yet, many organizations are less prepared to detect and respond to physical threats than to cybersecurity attacks.

Robbery, the use of counterfeit money, and natural disasters are all forms of physical vulnerabilities. Most organizations don't have teams dedicated to preventing and responding to all types of physical risks. In lieu of physical security teams, SecOps teams are in the best position to address a physical crisis. However, alerting and remediation of physical threats is often disconnected from cyber-threat workflows. This cyber-physical gap leaves businesses, and often employees, vulnerable.

With the right tools, processes, and automation in place, businesses can monitor risk in real-time and gain critical visibility throughout the reporting, investigation, and response to any incident. Low-code security automation platforms leverage human-readable form-fills to make it easy and convenient for physical threats to be reported. Once reported, case management applications can be leveraged to direct a customized response process, speed analysis or investigations, or generate incident reports.

From Con Artists to 'Code' Artists: Automate **Fraud** Protection

In today's corporate landscape, the impact of fraud reaches far beyond the immediate impact of public disclosure and extends to bottom-line profits and shareholder value. Financial institutions cannot afford to experience any business downtime, as the impact extends far and wide to reputation and customer trust.

Fraud is one of the leading security challenges that causes downtime and risk for financial institutions today. The annual financial impact of fraud now amounts to $42 billion, and this number is growing year over year. The digitalization of payment methods (virtual cards and Apple Pay) and the increase of online shopping has led to an increase in technical complexity.

When it comes to fraud, detection and monitoring are the best plans to put in place for a counter-attack. Fraud management teams lack visibility into security operations and cannot manually identify all malicious threats.

With security automation, it's much easier to fight back. Low-code security automation helps solve these challenges by detecting 10x more fraud risk and enabling collaboration across different teams. This comprehensive approach and the capability to connect incidents and patterns can lower MTTD and MTTR by half.

Request a Demo

First Name: *

Last Name: *

Business Email: *

Company: *

Title

Phone *

I consent to receiving emails from Swimlane including newsletters, best practices and promotions.

REQUEST DEMO

Take the Next Steps

Automation enables security teams to streamline and orchestrate tasks that would otherwise demand extensive and time-consuming manual intervention. This technology has the potential to significantly alleviate the problems associated with the increasing volume and complexity of cyber threats. From fundamental operational tasks to industry-specific applications, automation offers a solution to the overwhelming challenge of alert fatigue and information overload. This takes the burden off of security teams so that they can focus their expertise on strategic decision-making and high-priority threats.

To witness first-hand how automation can transform security operations, request a demo today.

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 reduce process and data fatigue, overcome chronic staffing shortages, and quantify business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com.

SWIMLANE