SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE

Executive Summary

Security Orchestration, Automation, and Response (SOAR) has emerged as a phrase that cybersecurity practitioners immediately recognize and understand in terms of the overall concept and its importance to an effective cyber defense. However, attempts to implement SOAR have faced challenges as technology vendors have co-opted the term to carve out their own product segment, causing implementations to almost exclusively center on a point product implementation. Many organizations have been unable to capitalize on the promise of SOAR and have decided to invest in long-term budget commitments on other technology purchases. Tyto Athene's approach places Security Operations Center (SOC) functions and capabilities at the center of the discussion and positions SOAR as a methodology, rather than as a technology purchase, which increases the security posture of an organization in the most cost-effective manner.

Introduction

Agencies throughout the federal Government are tasked with maintaining and securing some of the largest, most geographically disparate, and complex Information Technology (IT) infrastructures while being targeted by well-resourced, technically advanced adversaries. The rapid evolution of cyber threats, increasing regulatory demands, and explosive growth of Internet of Things (IoT) and Operational Technology (OT) is beginning to intersect with a dynamic geopolitical environment. This environment is expanding the range of adversaries that target civilian Government agencies and the Department of Defense (DoD). Government agencies are required to be resilient, adaptive, and innovative, even while being outnumbered by these adversaries. SOAR has the ability to transform security operations, deliver measurable operational benefits, and strengthen resilience across mission-critical systems.

Challenges

We outline the challenges facing the modern SOC below:

Environmental Complexity

Modern IT environments are becoming increasingly complex. Teams must understand, defend, and respond to attacks against a labyrinth of cloud architectures, microservices, and AI-driven solutions while also grappling with legacy systems that are often poorly documented and supported.

Adversary Advantage

Each organization faces an array of highly-resourced adversaries, which do not have to support customers, meet regulatory requirements, or support complex mission sets. As a result, they can rapidly innovate and continually evolve their Tactics, Techniques, and Procedures (TTPs).

Proposed Solution

Tyto Athene approaches SOAR as a methodology that maximizes existing cybersecurity investments. This wholistic approach to SOAR delivers on the promise of faster threat detection, triage, and remediation. Our approach places the processes, procedures, and business functions carried out by the SOC as the central point of focus, and applies a repeatable methodology to identifying, prioritizing, and developing automation and orchestration opportunities. The process is designed to maximize the automation capabilities of existing investments, many of which are already capable of supporting automation. The result is best-fit integration of existing tools such as Splunk, Elastic, JIRA, ServiceNow, and even sensors, into cohesive and automated workflows. In most cases, there is no need to buy a dedicated SOAR product, which ultimately can still only support a portion of the existing automation/orchestration opportunities. Our process provides its own operations and overhead maintenance to support existing engineering teams.

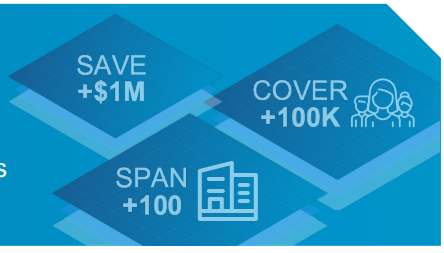
Tyto Athene's SOAR process follows a structured, metrics-driven pipeline that begins with the intake of automation candidates. Each is evaluated for impact, level of effort, and Return on Investment (ROI) to prioritize high-value initiatives. We form baselines on selected efforts with meaningful metrics, and upon initial release, reviews and outcome evaluations capture the lessons learned. This disciplined approach ensures every automation delivers measurable value and aligns with operational objectives. At its core, Tyto's SOAR methodology is a process-first approach, emphasizing clearly defined, actionable security workflows before automations are applied. It adopts a software development mindset with version control, testing, and feedback loops to ensure maintainability and resilience. This also ensures that automations and workflow orchestrations evolve with the threat landscape and delivers real operational value while reserving high-impact decisions for expert human analysis.

Path Forward

Agencies must avoid the lure of technology vendors promising to address their challenges in the form of a product. CISOs and CIOs must focus on outcomes, and set the vision for a SOAR implementation as a solution that is capable of delivering outcomes via a well integrated set of people, process, and technology. CISOs and CIOs should demand accountability in implementing SOAR because SOAR is fundamentally about eliminating work that is not value-adding for existing processes and procedures and making the routine execution of those processes and procedures more efficient. Establishing performance baselines for existing tasks, processes, and procedures ensures that organizations can demonstrate the measurable value of efforts to automate and orchestrate each task, process, and procedure.

Case Study Snapshot

A federal agency was able to save more than $1M annually while increasing SOC capabilities by applying Tyto Athene's SOAR approach in a SOC tasked with overseeing the cyber defense of dozens of component agencies, offices, and divisions spanning more than 100 offices and covering more than 100,000 users and assets.



Call to Action

Agencies approaching the implementation of SOAR as establishing a wholistic framework for automating SOC processes, as opposed to taking a product-centric perspective, can realize greater benefits while spending less money. It requires placing the processes and procedures carried out by the SOC at the forefront, and establishing a lightweight methodology for applying automation and orchestration in a prioritized manner. Tyto Athene's approach, grounded in federal expertise and real-world operations, provides organizations with a scalable, adaptive, and measurable strategy for defending critical systems and data.

For more information about our cybersecurity services, please email bd@gotyto.com

https://gotyto.com

Tyto GSI is registered in System for Award Management (SAM) as a Large Business under NAICS Code 541519.

TYTO Athene
DATA TO DOMINANCE