SWIMLANE

ORGANIZATION
United States Federal Government Agency

INDUSTRY
Federal Government

SCOPE
19,000 employees & contractors in 200+ offices worldwide

KEY IMPACTS

- Efficiency improvements equivalent to 50% staffing increase
- Significantly lowered mean time to resolution (MTTR)
- Increased the opportunity to be proactive
- Greatly improved staff satisfaction and quality of life

U.S. Government Agency Improves Efficiency to Keep Pace with Increasing Threats

Federal agencies are massive and highly distributed organizations that represent the U.S. government in the eyes of many people worldwide. As such, each agency has an outsized threat profile and an ever-growing number of daily attacks.

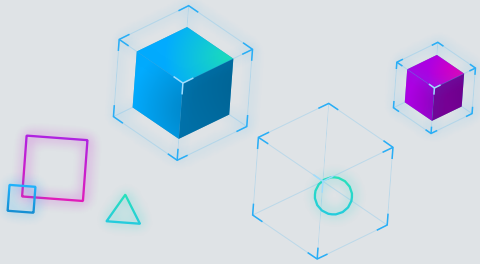
To counter these threats, this federal agency has a 24/7 Security Operations Center (SOC) with a large staff. They rely on dozens of point security systems as well as sophisticated SIEM and network security platforms. They are tasked with typical SOC functions like:

- Monitoring
- Looking for anomalous activity
- Malware alerts
- Basic intelligence gathering
- Forensic, end-point, and network investigations
- SIEM management
- Phishing
- PII & classified data spills
- Reporting

THE CHALLENGE

All of these point solutions and responsibilities generate tens of thousands of alerts every day. Prior to bringing on Swimlane, each alert had to be manually triaged and investigated. Much of the SOC's time was spent on rote manual tasks like cutting and pasting information to and from ticketing systems or manually searching for information stored on various separate databases. Staff was becoming simultaneously frazzled and bored with their jobs.

In the meantime, the number of both false alarms and genuine threats kept increasing. As a government agency, it has a fixed headcount and could not just throw additional bodies at the problem. Eventually, the SOC simply would not be able to keep up with the ever-increasing number of both true threats and false alarms.



"We were paying a lot of money for high-level data entry people."

SWIMLANE

"Swimlane has completely revamped how we handle incident response."

THE SOLUTION

The Security Operation Center Section Chief started to explore the possibilities of Security Automation, Orchestration and Response (SOAR) solutions. He realized that much of the mundane and repetitive work that was clogging up their processes could be automated.

After doing his homework and looking at competing solutions, the Section Chief selected Swimlane as the best solution.

The agency deployed the solution quickly, and they are in the process of plugging in at least ten separate point solutions into Swimlane, including the SIEM and ticketing system.

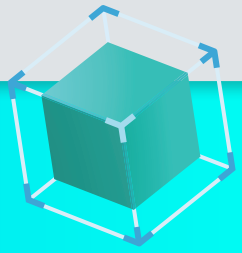
"I liked that with Swimlane we didn't need to devote a lot of resources to deploy or maintain new point solutions, integrations, or use cases. It's incredible how agile the system is and how little we have to invest in getting it up and running. The new functionality in Swimlane 3.0 will increase that agility even further."

THE RESULT

Swimlane provides the analysts all the data they need upfront—as soon as the alert triggers—which allows for much faster analysis and remediation. Since implementing Swimlane, the agency has seen dramatic improvements in mean time to resolution. **For some routine types of threats, the agency is seeing reductions of 75-90% in both staff and response time.**

This speedy time to response and resolution is enabled by giving analysts an instant global view of the threat while simultaneously relieving them of tedious manual work such as ticket generation, updates, and looking up information in separate systems.

The Section Chief estimates that **the overall increase in efficiency is like a 50% increase in staff.** This empowers security staff to be more proactive and really dig into anomalous issues. The new-found respect for the analysts' time and expertise has additionally improved the morale for the entire security operations staff and will undoubtedly lower staff turnover.



On the investigation of unauthorized software:

"We used to spend hours manually digging into multiple systems and looking through approved software lists… now unauthorized software is usually a 15-20 minute incident. It's all been automated."