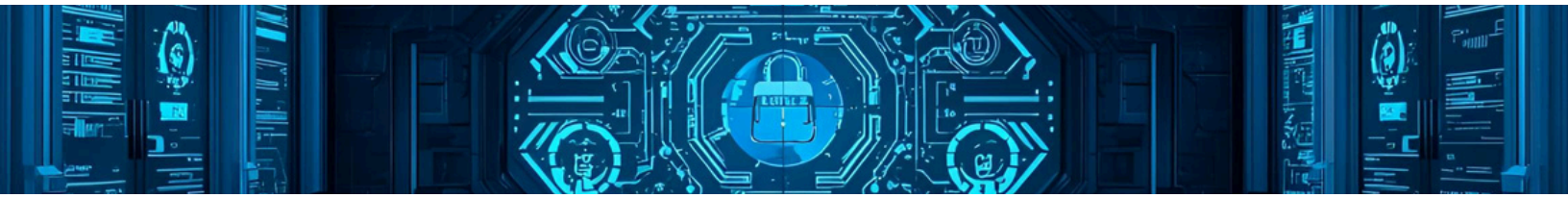
PHOENIXCYBER

CASE STUDY



Phoenix Cyber Transforms a Major DHS Agency with Security Automation

Efforts resulted in over $40 million in labor hours saved

THE CHALLENGE

A major Department of Homeland Security (DHS) agency's Security Operations Center (SOC) is responsible for 24x7x365 protection, monitoring, detection, analysis, and response to cybersecurity threats. The SOC faced a range of operational inefficiencies that hindered its ability to respond to cybersecurity threats effectively. These included fragmented communication due to disparate inboxes, a lack of standardized documentation and processes, and inconsistent task prioritization. The absence of unified IT and security systems created onboarding and training challenges, while manual workflows led to wasted time and effort. These issues collectively resulted in a reactive security posture and increased risks across the incident response process.

THE PHOENIX CYBER SOLUTION

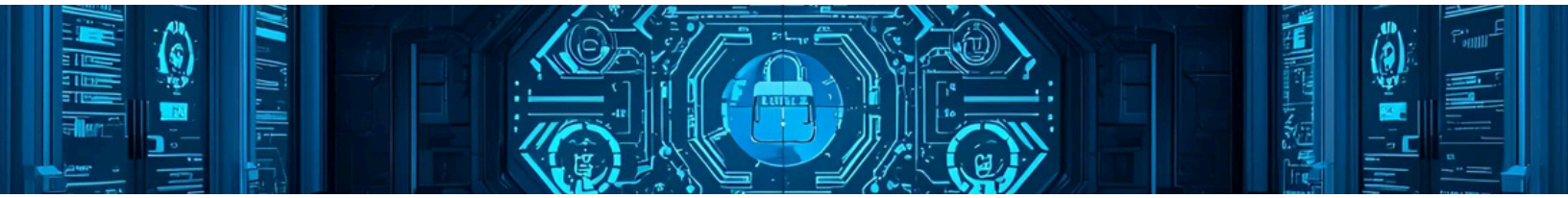
Since 2013, Phoenix Cyber has supported the agency's global SOC operations. The SOC transformation included the full implementation of a tailored security orchestration, automation, and response (SOAR) platform. This platform centralized incident management and enabled automated workflows to identify, triage, and remediate cybersecurity incidents at machine speed.

Phoenix Cyber first interviewed and documented the current use cases for the SOC, including many processes which had never been previously documented. This included identifying risks and gaps within the processes, along with prioritizing recommendations for automation use cases. Many use cases were not necessarily candidates for full automation, but key components of the process were identified for partial automation. The team focused on use cases with the highest impact to the security operations team.

Throughout the contract, the SOAR platform became the operational backbone of the SOC to automate incident response, enrich alerts with contextual data, and even contain compromised systems directly from within the platform. This eliminated the need for analysts to switch between tools.

PHOENIXCYBER

CASE STUDY



The SOAR platform was further integrated with other systems, enabling seamless ticket creation, status tracking, and email notifications. Phoenix Cyber utilized an integrated tool for interdepartmental requests including automating the creation of tickets, pulling the data necessary from the SOAR platform, and providing prompts within the SOAR platform for any other additional information needed. Ticket status was also pulled into the SOAR platform to ensure SOC analysts can quickly and easily monitor these updates. To make things even easier, the Phoenix Cyber team used an API to provide bilateral integration with Microsoft, allowing the SOAR platform to send, capture, and ingest notification emails sent by the ticketing system. These integrations vastly streamlined interdepartmental collaboration and reduced the burden of manual data entry.

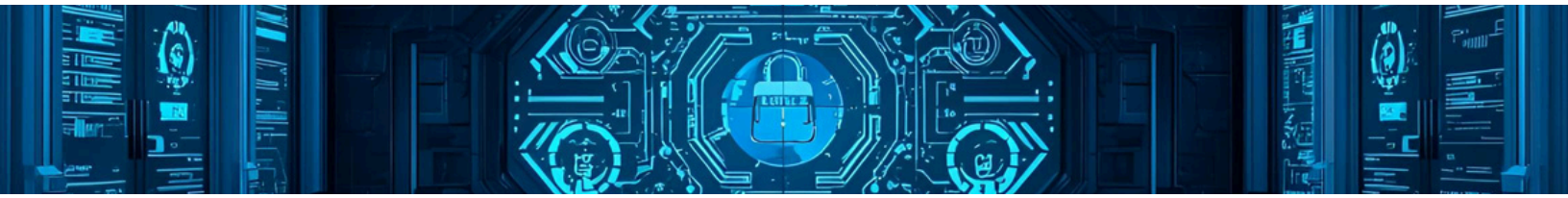
Interdepartmental requests from those outside of the agency's SOC were also enhanced. For incoming requests, like FOIA requests and forensics reporting, Phoenix Cyber built a web form for authorized users in other departments to submit requests. These incoming requests go directly into the SOAR platform, which is also used as the ticketing system. The team built a task tracking system within the SOAR platform that provides a dashboard of outstanding tasks, including their status and the system automatically logs the tasks completion date and owner.

At the DHS agency, Phoenix Cyber manages daily security operations and coordinates with the DHS ESOC. The support of the SOC also included security program assessment, solution evaluation, integration, testing, documentation, maintenance, and security operations to ensure uninterrupted security service availability. The team developed, implemented, and trained DHS staff on internal security response plans and security training programs to ensure the SOC could rapidly onboard and enable analysts to be effective in performing security triage and incident management.

In addition, Phoenix Cyber completed the implementation, operation, and sustainment of a wide variety of security tools, including the first endpoint detection and response (EDR) product at the agency, as part of a cross-functional team collaborating with other tool owners. The initial objective also involved fine-tuning the aggregation of log information from its SIEM, which accumulates around one terabyte of log data daily. The team tailored custom objects, including dashboards, alerts, and reports, to expedite the detection process of unusual events for the SOC. This brought relevant data forward and enabled SOC analysts to react to the full threat landscape. The calibration of alerts resulted in a substantial enhancement in the accuracy of alerts and a noteworthy decrease in false positives.

PHOENIXCYBER

CASE STUDY



Throughout the contract, Phoenix Cyber used APIs from another tool to automate standard incident response and forensics processes, as well as to contain a compromised endpoint right from the ticket within the SOAR platform. This increased response time by eliminating multiple interfaces and system logins as well as redundant copy and paste actions. For other tools, license costs were reduced as most SOC users were now only accessing the tool via the API.

DevOps Excellence

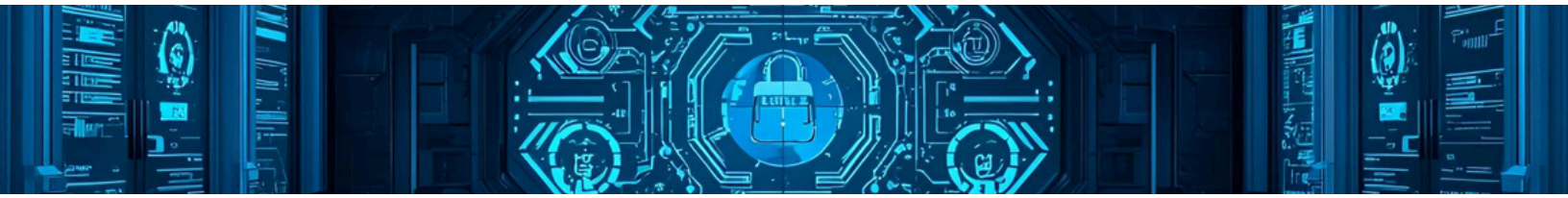
To facilitate optimized SOC operations, Phoenix Cyber's DevOps team developed and matured the SOAR processes and the technologies that support them. The team utilizes Agile processes with sprint planning kicking off each two-week sprint and concluding with a stakeholder-attended sprint review as well as a team-centric retrospective. Stand-up meetings occur daily throughout the sprint. Proper DevSecOps processes introduced into the security environments involve user research, continuous improvement, and feedback loops. The cross-functional team is comprised of senior and junior SOAR developers and engineers adept in relevant scripting languages as well as UI/UX, web design, and functional specialists who integrate seamlessly with SOC operations. All DevOps leads are Certified Scrum Masters to enable efficient facilitation of sprint management.

The DevOps team has implemented key infrastructure upgrades including migrating the SOAR platform back-end to containerized microservices, the development and implementation of the next generation engine and full-scale code migration to the latest version. These critical enhancements continue to promote toolset efficiency by improving integrations with all relevant SOC tools.

Recently, the DevOps team improved the integration between the SIEM and SOAR. SIEM alerts now instantly populate within the SOAR platform to include all pertinent event and asset details for immediate incident response action. In addition to infrastructure development, the team developed numerous dashboards and reporting mechanisms to streamline delivery and provide real-time metrics into the performance and ongoing efforts of the SOC. An example key deliverable provided by the team was the state-of-the-art CISO Dashboard developed with minimum guidance from senior leadership, and which exceeded expectations for the CISO. The dashboard enables actionable visualization with an array of incident, vulnerability, and risk metrics, all updated in real-time, allowing for faster executive decision-making.

PHOENIXCYBER

CASE STUDY

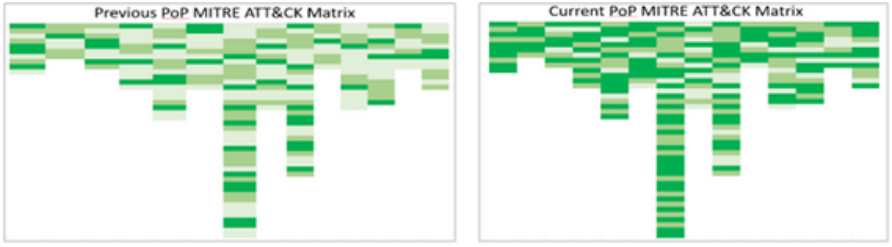


Advanced Threat Hunting (ATH)

While the incident response team primarily focuses on Indicators of Compromise (IOCs) before, during, and after a security incident, Phoenix Cyber's ATH team concentrates on attacker behaviors, or Tactics, Techniques, and Procedures (TTPs), throughout the course of an event. By receiving TTPs both from the team's intelligence gathering practices as well as their own research and knowledge base, they have provided expert insight into potential future attack patterns. With this knowledge in hand, the ATH team has built dozens of customized predictive alerting and detection mechanisms within the toolsets.

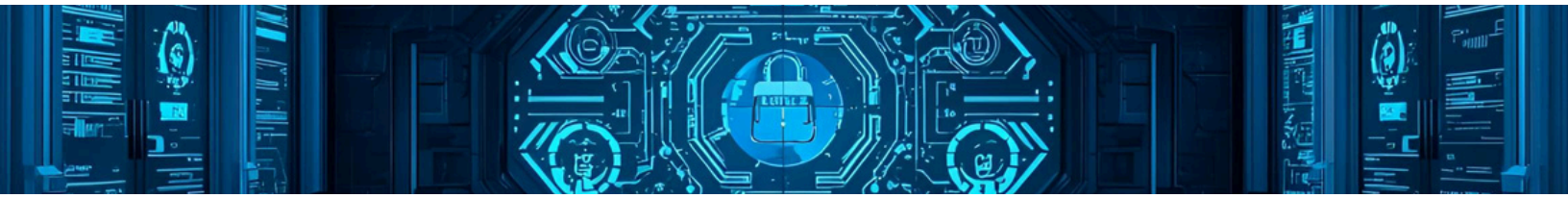
The ATH team leverages open-source and classified threat intelligence to identify threats. For each vulnerability, the team assigns risk levels relevant to the current security posture. By utilizing capabilities such as network monitoring tools, customized SIEM alerting mechanisms, and automations, the ATH team leverages data from the network, running processes, files, and relationships. The team is proficient at profiling rogue systems, identifying C2 channels, developing detections for payload delivery techniques, obtaining artifacts from memory, and deconstructing the obfuscation, encryption, and anti-analysis techniques used by self-defending malware. Discovered vulnerabilities are categorized by recency, criticality, and severity. These vulnerabilities are then managed alongside gathered threat intelligence in dedicated custom-built applications residing within the existing COTS platform utilized by the SOC. This approach allows for near-real time detections and monitoring for the latest threats prioritized by enterprise risk level, thus substantially mitigating interruption to business operations.

ATH has implemented patterns from over 100 different TTPs into these customized mechanisms and leverages the MITRE ATT&CK framework, the Diamond Model, and the Kill Chain process as part of their threat hunting responsibilities. The agency's ATH processes have matured by drastically increasing alignment to the MITRE ATT&CK Framework to ensure that no category of threat activity goes without predictive monitoring techniques in place. The progress in this effort is shown in the diagram below. The shades of green indicate the number of predictive monitoring techniques already developed for each tactic.



PHOENIXCYBER

CASE STUDY



Testing goes beyond “black box” testing and includes engagements designed to identify gaps in security practices and controls not readily apparent from conducting standard technical tests. These tests may also include information and direction from hunt team scenarios. The team analyzes and maps potential vulnerabilities and provides analysis artifacts and reports for all penetration tests. The ATH team also contributed to blue-team penetration testing, identifying vulnerabilities and enhancing the SOC’s threat posture through behavioral analysis and forecasting.

ONGOING CUSTOMER BENEFITS

Phoenix Cyber's work at the SOC has been nothing short of transformative. Their core system automations laid the groundwork for the SOC’s fast and effective incident detection and response capabilities, which continue to support operations today. These automations are now recognized across the agency as an example for future SOC efficiency programs and have set a new benchmark for federal SOC operations.

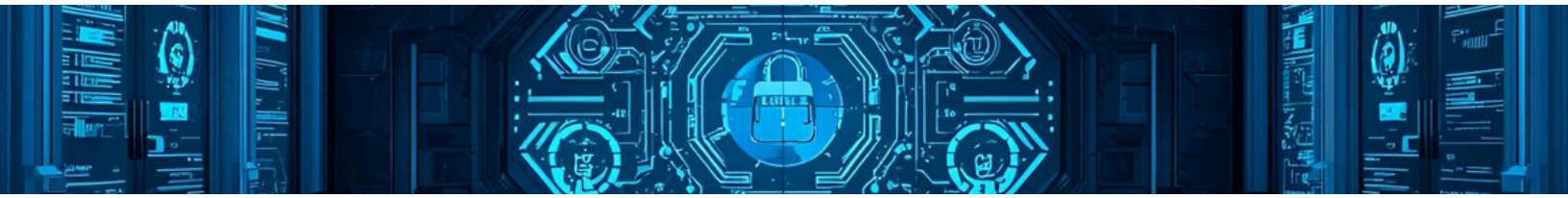
To date, Phoenix Cyber has automated more than 2 million actions and over 50,000 records. This has saved over 100,000 labor hours annually and delivered a return on investment of more than $9 million each year. Over five years, the DHS agency has reported more than $40 million in labor-hour savings thanks to security automation. The SOC has also advanced to Cybersecurity Maturity Model Certification (CMMC) Level 4, with many processes meeting Level 5 standards.

Phoenix Cyber developed automations that handle most monitoring functions 24x7x365. These include response actions such as escalation and some approved remediations that occur in real time based on toolset data. As a result, mean time to detect (MTTD) and mean time to resolve (MTTR) have both decreased by 90 percent. MTTD dropped from four hours to under one minute, and over 90 percent of initial alerts are now resolved without needing additional review by personnel.

With these automations in place, SOC personnel shifted from reactive tasks to proactive ones, such as investigating anomalies. This shift has reduced backlogs and lowered costs. The agency estimates the efficiency gain is equal to a 50 percent increase in staff. Staff turnover also declined, which is attributed to improved morale. Phoenix Cyber continues to refine its SOC and security automation expertise, delivering NIST-compliant and operationally efficient solutions within federal agency security environments.

PHOENIXCYBER

CASE STUDY



These improvements have led to national recognition. The agency's SOC was named the "2023 Security Operations Center Team of the Year" by Cybersecurity Insiders. Phoenix Cyber also contributed to the SOC being named the DHS SOAR Center of Excellence (COE). As a COE, the SOC is responsible for developing, vetting, and advising on requirements for security architecture and policy recommendations across all DHS components.

Phoenix Cyber's combination of engineering skill, user-focused design, and operational insight helped modernize the agency's cybersecurity capabilities. Their work demonstrated the value of automation, DevOps, and advanced threat hunting in protecting mission-critical environments. The deployment of enhanced security solutions and advanced orchestrations allowed the agency to exceed the integration capacity of the hang-fire task engine originally included in the agency's procurement.

Phoenix Cyber's work at the SOC has delivered measurable and lasting impact. They have significantly reduced detection and response times, cut operational costs, and enhanced overall security posture. The results include millions in labor-hour savings, national recognition, and a more resilient, proactive cybersecurity environment. Their approach has modernized the SOC and set a strong example for how federal agencies can scale security operations most effectively.

> **AUTOMATION HAS ALLOWED OUR SECURITY OPERATIONS CENTER TO FREE UP INCIDENT ANALYSTS TO FOCUS ON RESPONSE ROLES.**
>
> -DHS Agency's CISO

CONTACT US AT **SALES@PHOENIXCYBER.COM**

Phoenix Cyber *is a leading cybersecurity services company providing security engineering, operations, and technical cybersecurity expertise to federal agencies and enterprsies determined to mitigate risk and safeguard their business.*