

# Enterprise Services and Capabilities

## CAPABILITIES

- Security Operations Center
- Security Engineering & Architecture
- Security Automation
- Cyber Threat Intelligence & Threat Hunting
- Incident Response
- Zero Trust Security
- DevSecOps & DevOps
- Data Protection
- Risk Assessment & Mitigation
- Vulnerability Management
- Network & Endpoint Security
- Identity Management
- Privacy Risk Management & Compliance
- Cloud Security



## EXPERTISE

Phoenix Cyber has been providing cybersecurity services to Fortune 500 companies, U.S. Federal Government agencies, and service providers since 2011. Our team is comprised of senior cybersecurity consultants and engineers with expertise in architecting results-oriented, cybersecurity solutions and the operational processes to ensure accurate incident detection, enrichment, and response.

## TEAM CERTIFICATIONS

### ISC2:

- Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP)

### CompTIA:

- Security+, Cybersecurity Analyst (CySA+), Cloud+, PenTest+, CompTIA Advanced Security Practitioner (CASP), Network+, Server+, Linux+

### EC-Council:

- Certified Ethical Hacker (CEH)

### GIAC:

- Reverse Engineering Malware (GREM), Security Essentials (GSEC), Certified Incident Handler (GCIH), Certified Intrusion Analyst (GCIA), Security Leadership Certification (GSLC), Certified Perimeter Protection Analyst (GPPA), Systems and Network Auditor (GSNA), Certified Windows Security Administrator (GCWN), Certified Detection Analyst (GCDA)



## SERVICES

Phoenix Cyber delivers engineering, operations, and technical expertise to help you meet today's cybersecurity challenges. We reduce security operations workload by automating 80–90% of the incident response process and strengthen your security posture to defend against threats, attacks, and data loss. Our experts help identify, assess, and mitigate enterprise risks while building operational processes and deploying technical solutions. We ensure your security tools are seamlessly integrated and set up to deliver immediate ROI.



## ABOUT US

Phoenix Cyber is an ISO-9000, ISO 20001, ISO 270001, and a CMMI Level 3-certified leading cybersecurity solutions company providing architecture, engineering, and operations technology expertise to organizations determined to mitigate risk and safeguard their business. Since 2011, we have delivered cybersecurity solutions to the Federal Government as a certified small business.

### ISACA:

- Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA)

### Scrum Alliance:

- Certified ScrumMaster (CSM)

### Vendor:

- RSA (Archer), Forcepoint, Splunk, Swimlane

## CONTACT

sales@phoenixcyber.com | (888) 416-9919



# Enterprise Services and Capabilities

## Past Performance

### U.S.-based Integrated Health System Assessment

A Southwestern U.S.-based Integrated Health System had many security tactics already in place to reactively defend against cyber attacks.

However, facing newly evolved threats and challenges to further ensure the security of their critical healthcare information and data, they desired a more proactive approach.

The health system realized financial savings by rapidly migrating to new, more scalable products and removing outdated third-party solutions.

The Phoenix Cyber team assessed their current security practices, built a framework to manage their overall security posture and maintain compliance with regulatory requirements, as well as provided direction for their day-to-day in-house cybersecurity projects. For over a decade, we have assisted with several high-profile initiatives for the healthcare organization to fortify their security defenses, including: cybersecurity program assessments and build outs, identity and access management, data security, network security, security automation, endpoint security, and governance, risk, and compliance (GRC).

After conducting an initial security program assessment, the health system gained a comprehensive understanding of their risks and potential weaknesses. Implementing foundational security controls reduced vulnerabilities and enhanced the organization's overall security posture. The focus on network, data, and authentication security controls, including multi-factor authentication and data loss prevention provides robust protection of critical patient data. By implementing a GRC practice and aligning technology and security operations with business objectives, the organization can more effectively manage risk, meet regulatory compliance requirements, and improve governance processes.

### Driving a Fortune 100's Strategic SOAR Transformation

Phoenix Cyber was part of a joint venture to assist in migrating a Fortune 100's existing security automation, orchestration, and response (SOAR) solution from Palo Alto XSOAR to Swimlane Turbine. The primary focus was to perform a lift-and-shift in replicating the current platform's capabilities, along with the expansion of new playbooks within Swimlane. Ingestion points included Splunk ES, Palo Alto, Microsoft Security and several homegrown solutions. The overall scope of work included migrating 70+ active integrations, 20 incident types, 200 playbooks, 150 custom automations, and 25 dashboards. Additionally, the engagement required 2.5+ years of data and over 1 million indicators of compromise be migrated to the new SOAR platform.

The Phoenix Cyber team successfully led the complex migration within the customer's enterprise environment, overcoming technical constraints, limited resources, and aggressive deadlines while delivering measurable value. Leveraging a lift-and-shift strategic, the team closely mimicked the XSOAR environment in Swimlane Turbine, ensuring continuity while unlocking the strength of Swimlane's platform. Through this approach, our engineers delivered a MVP featuring seven core playbooks with comprehensive application and playbook inventories, detailed developer notes, and a Turbine upgrade.

Beyond execution, Phoenix Cyber provided hands-on security automation expertise, supporting parallel development efforts, and resolving integration challenges in real time. This project resulted in a fully deployed and operational Swimlane Turbine SOAR platform for the customer's SOC complete with executive-level dashboards that enhances visibility, streamlines response workflows, and accelerates incident resolution.