PHOENIXCYBER

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

TEAM CERTIFICATIONS

ISC2:
- Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP)

CompTIA:
- Security+, Cybersecurity Analyst (CySA+), Cloud+, PenTest+, CompTIA Advanced Security Practitoner (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)

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

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.

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.

ISO AGS AMERICAN GLOBAL STANDARDS 9001 CERTIFIED

ISO AGS AMERICAN GLOBAL STANDARDS 27001 CERTIFIED

ISO AGS AMERICAN GLOBAL STANDARDS 20000 CERTIFIED

ML3 CMMI APPRAISED SVC

PHOENIXCYBER

Enterprise Services and Capabilities

Past Performance

U.S.-based Integrated Health System Assessment

The health system realized financial savings by rapidly migrating to new, more scalable products and removing outdated third-party solutions.

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 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.

Rapid SOAR Solution Migration for Fortune 100 Retailer

A Fortune 100 retailer engaged Phoenix Cyber, along with Trace3, to assist in migrating their existing security automation, orchestration, and response (SOAR) solution from Palo Alto XSOAR to Swimlane Turbine. The primary focus of the initiative was to replicate the current capabilities of the platform in Swimlane, with a primary ingestion point from Splunk ES. The overall scope of work included migrating over 70 active integrations, 20 incident types, 200 playbooks, 150 custom automations, and 25 dashboards. Over 2.5 years of data and over 1 million indicators of compromise also needed to be migrated to the new SOAR platform.

The Phoenix Cyber team overcame technical constraints, limited resources, and tight deadlines during the migration within the company's enterprise environment. They successfully collaborated with stakeholders across multiple teams and procured new third-party services to meet the migration requirements.

The migration focused on a lift-and-shift approach to closely mimic the XSOAR environment in Swimlane Turbine. With this approach, Phoenix Cyber identified and developed an MVP that included seven core playbooks with full application and playbook inventories, playbook developer notes, and a Turbine upgrade. Additionally, the Phoenix Cyber team shared its expertise in security automation with the retailer's team, successfully navigated parallel development efforts, and fully engaged with Swimlane to rectify any hurdles that arose during the migration.

This project resulted in a fully developed and deployed new Swimlane Turbine SOAR platform for the SOC, as well as high-level reporting dashboards for the team.