Enterprise Capabilities Statement

Certifications

GIAC:
Security Expert (GSE)
Reverse Engineering Malware (GREM)
Certified Forensic Analyst (GCFA)
Security Essentials (GSEC)
Certified Incident Handler (GCIH)
Certified Intrusion Analyst (GCIA)
Security Leadership Certification (GSLC)
Certified Assessing and Auditing Wireless Networks (GAWN)
Certified Perimeter Protection Analyst (GPPA)
Certified Enterprise Defender (GCED)
Systems and Network Auditor (GSNA)

ISACA:
Certified Information Security Manager (CISM)

ISC²:
Certified Information Systems Security Professional (CISSP)

Offensive Security:
Certified Professional (OSCP)

PMI:
Project Management Professional (PMP)

Apple:
Certified Server Engineer
Certified Product Professional

Intel:
Security Product Specialist

Microsoft:
Certified Systems Engineer (MCSE)
Certified Technology Specialist (MCTS)

Palo Alto Networks:
Accredited Systems Engineer (PSE)

RSA:
Certified Systems Engineer
Archer Certified Associate

Symantec:
Certified Specialist (SCS)

Expertise

Phoenix Cybersecurity has been providing cybersecurity services 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 offers a set of **engineering**, **operations**, **sustainment**, and **managed security services** designed to deliver the solutions you need to meet today's cybersecurity challenges. Allesao, our exclusive SOC-as-a-Service offering, reduces your SOC workload by automating 80-90% of your incident response process. Our services and solutions are provided on-premises, remotely, or hosted within commercial cloud environments. This flexibility allows clients to rapidly procure and implement these sophisticated security offerings.

Cybersecurity Capabilities

- Security Automation & Orchestration (SAO/SOAR)
- Security Information and Event Management (SIEM)
- Threat Hunting
- Threat Intelligence
- User & Entity Behavior Analytics
- Data Protection
- Phishing Detection & Response
- Endpoint Security
- Network and Perimeter Security
- Vulnerability Management

Contact Us

Phoenix Cybersecurity
sales@phxcyber.com
(888) 416-9919 x2

Phoenix Cybersecurity provides cybersecurity engineering services, operations services, sustainment services, and managed security services to government agencies and large businesses determined to strengthen their security posture and enhance the processes and technology used by their security operations teams. Our clients include: Department of Defense agencies, federal civilian agencies, financial services companies, healthcare providers, and government prime contractors.

PHOENIX CYBERSECURITY

Past Performance

An Integrated Healthcare Delivery System

In late 2014, this client engaged Phoenix to provide a security gap analysis and external penetration assessment. Since then, Phoenix has worked to strengthen the gaps identified by that assessment.

This client is a private not-for-profit healthcare system and provider in he western United States that owns and operates eight hospitals and has over 2,000 employees.

Phoenix evaluated key aspects of the client's security program, computing systems, communications, physical security, personnel and operations in relation to NIST Cybersecurity Framework and ISO27001 security standards. Phoenix performed vulnerability assessment of the client's external facing systems, evaluating their external footprint, vulnerabilities and potential impacts.

The assessment included:

- Web Server Security Configuration
- Web Applications Security Configuration
- Web Security Gateway
- Identity and Authentication
- Host Security
- Perimeter Router and Firewall Configuration
- Adherence to security standards including OWASP

A detailed business benefits analysis with remediation plans and specific actionable procedures was developed and presented to the client's board of directors. This assessment enabled the client to identify strengths and weaknesses in their security program from an organizational, technical and procedural perspective. The assessment results drove a multi-year security program uplift that expanded the security services delivered, the organizational structure for delivery and the methods for measuring and reporting the security posture of the entire organization.

Major Credit Card Company

This client engaged Phoenix to define requirements and set company policies for mobile device usage and management, evaluate and recommend Mobile Device Management (MDM) platforms, and deploy the chosen solutions.

A major U.S. credit card company with tens of thousands of employees and millions of customers was expanding its alternate workspace program and needed to ensure that remote employees could securely access and store sensitive financial and customer personal information data on both corporate-issued and employee-owned mobile devices.

Phoenix evaluated current mobile device management (MDM) platforms and PCI and cybersecurity industry standards and best practices to determine what mix of features and company policies were necessary to ensure devices running a variety of operating systems (Blackberry, Android, iOS) would remain secure even if lost or stolen. The result was a set of requirements for encrypting data in motion and data at rest, over-the-air provisioning, remote wiping, and recommended configurations for all the tools the client selected.