Security Automation and Orchestration (SAO) Readiness Assessment

As cyberattacks continue to rise, organizations invest heavily in attack identification, threat intelligence and the staff required to protect the enterprise. However, alerts are still going unresolved and often unseen. The solution is a Security Automation and Orchestration (SAO) system to standardize the incident response process, improve consistency, decrease mean time to resolution (MTTR), and lower operating costs by integrating workflow automation with dynamic case management.

A SAO Readiness Assessment from Phoenix Cybersecurity (Phoenix) will identify security operational processes that can be automated to lower your MTTR, lower your risk profile, and increase the return on your investment in security operations. On average, SAO systems resolve 80-90% of their alerts without human intervention—drastically reducing the workload on analysts.

Phoenix Cybersecurity's SAO Readiness Assessment is a four-week engagement with one week spent on site analyzing your security operations capabilities, one week off site compiling the results and generating the report, and an optional two-week proof-of-concept of a single SAO workflow working within your organization.

Phoenix has extensive experience performing SAO integrations with vendors including McAfee, Cisco, Forcepoint, Symantec, RSA, Carbon Black, CrowdStrike and many more.

Scope

- Focused assessment of Security Operations
- People, process, technology
- Policies, procedures, guidelines
- Metrics, key performance indicators
- Aligns with industry standards (CSF, NIST, FISMA)

Benefits

- Identification of opportunities for efficiency gains and cost savings
- Improved staff utilization
- Improved security metrics and situational awareness
- Improved security capability & posture

About the Assessment

This isn't a basic maturity assessment. Phoenix will focus specifically on your Security Operations Center (SOC) and delivery of security response and recovery services. When on site, we use a "day in the life" approach that combines data collection, interviews, and observation to study your operations. We will review your documentation, architecture, rule-sets, and system configurations to determine what automation options are available with your current security tools and infrastructure. Once the assessment is delivered, Phoenix Cybersecurity can set up a SAO proof-of-concept and is available to work with you to implement any of the recommendations.

About Phoenix Cybersecurity

Phoenix Cybersecurity (Phoenix) is a national provider of cybersecurity engineering services, operations services, sustainment services, and managed security services to organizations determined to strengthen their security posture and enhance the processes and technology used by their security operations teams. Since 2011, Phoenix has been serving clients in the private, public, and defense sectors including clients in the Fortune 500, the US Department of Defense, and the U.S. Department of Homeland Security.

Our team comprises senior cybersecurity consultants and engineers with expertise in architecting results-oriented, cybersecurity frameworks; and the operational processes to ensure accurate incident detection, enrichment and response. Our experts are the trusted advisors to cybersecurity leaders in the Department of Defense, Department of Homeland Security, and hold a variety of industry certifications including (ISC)2 CISSP, GIAC Information Security Expert, SANS, ISACA and ITIL.

Our unique blend of security automation, orchestration and proven best practices differentiates Phoenix-architected solutions from traditional cybersecurity services.

For more information or to schedule an assessment, call us at (888) 416-9919 or email us at sales@phxcyber.com.

39506 N. Daisy Mountain Drive
Suite 122-121
Phoenix, AZ 85086
(888) 416-9919

https://www.phxcyber.com
https://twitter.com/phxcyber
https://www.linkedin.com/company/phxcyber/