GUIDEPOINT SECURITY

SOC ADVISORY SERVICES

Maximize the value from your existing SOC investment to ensure better outcomes

Gain more signal and less noise for your SOC

Our team of security operations experts and engineers will help you optimize your SOC to effectively respond to the latest and most relevant threats to your organization while driving efficiencies in automated and human response, processes, and technologies.

SOC Assessment Services

GuidePoint's SOC Assessment services provide an in-depth look at your SOC processes and capabilities, as well as the overall maturity of your SOC. Know the visibility your SOC has against the latest threats and your SOC's response capabilities against those threats by leveraging our assessment methodology.

Security Posture Gap Analysis
Technology Stack Analysis
Use Case and Workflow Analysis
Cyber Threat Intelligence (CTI) Analysis

Security Posture Gap Analysis

- Identify Relevant Threats
- SOC Maturity Assessment

Technology Stack Analysis

- Identify SIEM Detection Gaps
- Map SIEM Detection Gaps to Relevant Threats

Cyber Threat Intelligence (CTI) Analysis

- CTI Lifecycle Analysis
- Threat Feeds, Integrations, Workflow Analysis

Use Case and Workflow Analysis

- End-to-End Use Case Review
- SOC Runbooks, Policies, & Procedures Review

SOC Assessment Key Outcomes

- ✓ Build an Enterprise Framework for Defense to advance cyber protection and detection capabilities
- ✓ Build a SOC Maturity Roadmap by determining your SOC's current maturity and identifying areas of needed growth
- ✓ Identify "real world" threats targeting your organization based on CTI research
- ✓ Increase your SOC's visibility by identifying new detection and response capabilities to protect against the latest threats
- ✓ Determine the efficacy of existing detection capabilities, and identify detection gaps based on the latest threats
- ✓ Assess the fidelity of existing log and data sources and identify those missing from detection capabilities
- ✓ Improve CTI capabilities, workflows, and integrations
- ✓ Consolidate and improve existing response workflows and/or runbooks

Put an ELITE Team of Cybersecurity Practitioners on Your Side

More than 70% of our workforce consists of tenured cybersecurity engineers, architects, and consultants

Many have managed security within the DoD and U.S. intelligence agencies and Fortune 500 companies

Hundreds of Industry and Product Certifications

SOC Staff Augmentation

GuidePoint can provide expert SOC and Cyber Advisory Staffing Services to provide organizations with the right level of expertise to keep your SOC operational and assist with special projects.

SOC Health Check

GuidePoint's SOC Health Check assists organizations to quickly assess and gauge the maturity of their SOC to help identify areas of growth and/or improvement.

- **Operations:** The day-to-day function of a SOC, including leadership and analyst activities and how they respond to daily threats
- **Procedures:** Formal guidance meant to inform and dictate a SOC analyst's behavior during real-world situations
- **Tooling:** Technology and data supplied to a SOC to support ongoing operations
- **Collaboration:** The people interactions within a SOC, and collaboration with other internal and external stakeholders

Benefits of our SOC Advisory Services

- Validate and improve your existing processes and procedures
- Curate existing and new threat intelligence resources and tools
- Increase your SOC maturity level based on industry best practices
- Remediate security operations gaps
- Enhance your visibility based on MITRE ATT&CK
- Decrease time to resolution of an incident
- Increase security data visibility
- Facilitate better communication and collaboration between SecOps teams
- Improve tooling and automation maturity
- Gain external validation of regulatory compliance laws/certifications

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.

GUIDEPOINT
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132