GUIDEPOINT® SECURITY

SECURITY OPERATIONS CENTER (SOC) SERVICES

Manage Evolving Threats and Security Operations Effectively and Efficiently

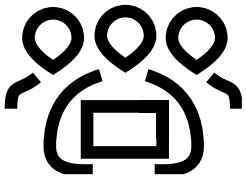
Security teams are trying to manage and secure complex IT environments that are often hybrid and distributed. They also must secure increasingly larger volumes of data and applications while maintaining compliance.

Unlock the power of your SOC, reduce "noise", gain greater visibility to quickly remediate incidents, and improve your overall security posture with GuidePoint Security. As your trusted advisor and partner, we design, deploy, operationalize and continuously optimize modern Security Operations programs — integrating leading security platforms with structured detection engineering, data normalization, and intelligence — to deliver measurable performance.

A Security Operations Center (SOC) is the operational core of an organization's cybersecurity program — responsible for detecting, investigating, and responding to threats across the enterprise. Modern organizations have complex IT systems that operate across hybrid environments including a mix of on-premises infrastructure, cloud platforms, SaaS applications, and distributed workforces. As environments become more distributed and data volumes increase, maintaining consistent monitoring, reliable detection coverage, and disciplined incident response becomes more complex.

GuidePoint Security helps reduce "noise" and unlock the full potential of the modern SOC. We design, deploy, and operationalize SOC programs to unleash intelligence-driven, metrics-oriented, automation-enabled operations that are tightly aligned to your business risk tolerances. As your trusted technology advisor and partner, we ensure your SOC platforms perform as intended — from implementation through continuous optimization to provide greater visibility, quickly remediate incidents, and improve your overall security posture.

- **Threat-Focused Prioritization** - Focus your SOC on the adversaries, tactics, and risks most relevant to your environment with GuidePoint Security. We ensure your security efforts are aligned with the threats most likely to impact your organization.
- **Stronger Visibility** - Improve telemetry coverage and log consistency with GuidePoint SIEM, observability, and data onboarding services. These offerings help reduce blind spots and give analysts a more complete view of activity across the environment.
- **Higher-Quality Detection** - By improving normalization, use case alignment, and content quality, we help SOC teams strengthen detection fidelity, reduce noise, and support faster, more confident investigations.
- **Reduced Operational Risk** - Structured deployment, migration, and admin support help maintain platform stability, preserve monitoring continuity, and lower the risk of gaps caused by misconfiguration or unmanaged change.
- **Improving Results for Lean Teams** - Give your team stronger monitoring foundations, actionable threat context, and expert support without requiring them to carry every engineering and platform challenge internally.



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly trained SOC and cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War and U.S. intelligence agencies.

We excel with the platforms and tools that support your needs, including:

CROWDSTRIKE elastic

DATADOG sumo logic

splunk> a CISCO company paloalto NETWORKS

Google Security Operations

And more...

Maximize SOC Performance and Efficiency

As your trusted advisor, we take a vendor objective approach. This ensures clients have the comprehensive, adaptable solutions their unique environment requires.

Threat Intelligence Profiling (TAP) – Provides an intelligence-driven analysis of threat actors most relevant to the client's industry, technology stack, and business operations.

Detection Coverage & Gap Assessment – Evaluates the alignment between existing threat detection capabilities and the threat landscape to identify gaps in detection coverage.

Threat Intel Monitoring As-a-Service – Continuously tracks a client's technology stack for emerging threats, including actively exploited vulnerabilities, credential exposure, and relevant dark web activity. This helps identify relevant risk earlier and focus remediation efforts on the issues most likely to affect the organization.

SIEM Data Engineering Services – Designs, implement, and migrate the foundational data engineering components required to operationalize a SIEM platform, including onboarding, normalization, validation, and initial data quality controls.

SIEM Admin-on-Demand – Provides on-call access to senior SIEM engineers to help keep SIEM platform stable, optimized, and audit-ready without the cost of a full-time administrator. This service reduces operational risk, strengthens day-to-day platform management, and helps to maintain consistent SIEM performance.

Detection Engineering Services – Designs, develops, and optimizes detection logic to improve alert fidelity, coverage, and operational effectiveness.

Platform Optimization & Health Assessment – Evaluates ingestion health, parsing quality, data volume and cost drivers, platform performance, and detection effectiveness to identify operational issues and optimization opportunities.

Telemetry Data Strategy – Evaluates current pipeline architecture, identify inefficiencies, evaluate governance and cost controls, and produce a strategic plan for pipeline expansion, optimization, and standardization.

Telemetry Data Engineering – Onboard data sources into pipeline technologies, implement routing and filtering logic, apply enrichment, masking, and normalization as required. This is to control data flow, improve data quality, and reduce SIEM costs.

Security Data Governance & Normalization – Establishes logging standards, field consistency, schema alignment, and data quality expectations required to support security operations and analytics.

SOC Strategy, Maturity & Roadmap – Establishes a comprehensive Security Operations strategy aligned to business objectives, threat landscape, and regulatory requirements. It evaluates current SOC maturity across people, processes, and technology, and defines a target-state operating model with a prioritized roadmap for improvement.

SOAR Data Engineering Services – Designs, implements, optimizes, and migrates SOAR capabilities to support incident response automation and operational efficiency.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.

GUIDEPOINT® SECURITY

1900 Reston Metro Plaza, Suite 701 • Reston, VA 20190
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132