

## SOAR SERVICES

# Jumpstart your SOC's ability to respond via automation

Help your SOC soar to new heights by leveraging automated response

A SOAR solution is the automation hub of your SOC to help you effectively manage incidents in a more efficient manner. With over half a decade of SOAR experience in various platforms, we can help you quickly operationalize your SOAR platform and help you respond more quickly to the noisiest and most time-consuming alerts.

## SOAR Advisory Services

Unsure how to start your SOAR solution journey? Moving on to your next SOAR solution? Through our portfolio of SOAR Advisory services, we can help you select the most compatible solution for your SOC based on our proven SOAR platform evaluation criteria.

SOAR Advisory Services include:

- ✓ SOAR SME Advisory
- ✓ SOAR Planning and Development
- ✓ SOAR Evaluation Services

## SOAR Health Check

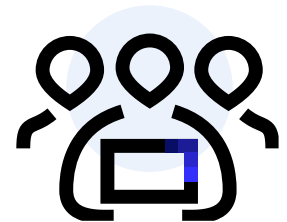
Need to check the pulse of your existing SOAR solution? Unsure if your SOAR solution is still effective? Not getting the expected ROI out of your SOAR solution? Leverage our comprehensive Health Check services to see how to maximize the value from your existing SOAR solution and to check the vitals of your platform and its operationalized use cases.

- ✓ Platform
- ✓ Playbooks
- ✓ Integrations

## SOAR Implementation and Development

Leverage GuidePoint's SOAR implementation services to build automations for your most crucial SOC workflows to allow your analysts to DECIDE and ACT faster.

- ✓ Install and Configure
- ✓ Use Case Planning Workshops
- ✓ Playbook Development
- ✓ Integrations Configuration and Development



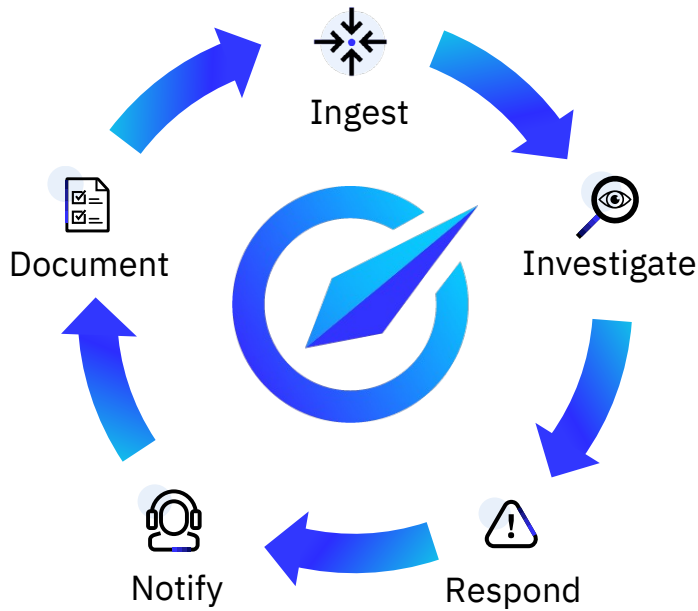
Put an **ELITE** Team of Cybersecurity Practitioners on Your Side

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



Using GuidePoint's Security Automation Workflow, we can dissect, build, and operationalize the simplest to most complex use cases for your SOAR solution.



-  **Ingest:** All Notable Events and Alerts
-  **Investigate:** Reputation/Enrichment, SIEM & EDR Searches, Asset Lookups, CMDB Searches, etc.
-  **Respond:** Incident Response – Containment/Blocking, Remediation, and Lessons Learned
-  **Notify:** SOC Analysts/Manager, Executive Leadership, System Owners, Help Desk, etc.
-  **Document:** Case Management – Analyst/Manager Notes, Reputation/Enrichment Results, Investigation Results, etc.

In order to gain the many benefits of a SOAR solution, you must customize it to your environment and processes. **Our team of experts can help you quickly take advantage of your SOAR solution through popular use cases that we have implemented for many of our customers:**

- ✓ Phishing
- ✓ Business Email Compromise
- ✓ Ransomware
- ✓ Malware
- ✓ Command and Control
- ✓ Credential Compromise
- ✓ Threat Hunting
- ✓ Threat Intelligence
- ✓ Insider Threat
- ✓ Unauthorized Access

## 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.