

SERVICE OFFERING

Building Custom Playbooks to Maximize Splunk and CrowdStrike

Phantom enables teams to work smarter by executing automated actions across their security infrastructure in seconds, versus minutes when performed manually. Teams can codify workflows into Phantom's automated playbooks using the visual editor (no coding required) or the integrated Python development environment.

Integrating your Phantom with CrowdStrike allows you to enrich indicators coming from your environment with additional context. Empowering analysts to make faster and smarter informed decisions. Taking the repetitive, grunt work out of being an analyst and improving their quality of work productivity.



Automate the enrichment of indicators with:

- Known vulnerabilities
- Threat Actors
- Reputation Scores
- Hash Details
- Domain Details
- File Details
- Detonate Files
- Get Indicators of Compromise
- Quarantined Devices
- and much more....



Create faster and effective decision making for the front-line analyst

GuidePoint Security Government Solutions has extensive security expertise in playbook buildout and tailor plays to your organization's use cases. Some examples that have been implemented to date include:

- Compromised Indicator Hunting (IOC ingestion)
- Malware Triage
- Ransomware Investigate and Contain
- Checkpoint Malicious File Response
- Checkpoint Hunt and Block URL



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

Our highly-certified, operational cybersecurity experts have lived and breathed your job.

- 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**

Reach out to the following
POC's from GuidePoint Security
to schedule a meeting to discuss:

John Trojanowski

John.trojanowski@guidepointsecurity.com
630.770.4892

Yuri Shabanowitz

yuri.shabanowitz@guidepointsecurity.com
814.303.9874

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help agencies 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.