GUIDEPOINT® SECURITY

THREAT DISCOVERY SERVICES

Prepare For, Respond To and Efficiently Resolve Security Incidents to Minimize Business Impact.

Engagements Focus On Identifying Anomalous and Suspicious Behaviors

Our Threat Discovery engagements determine if there are any ongoing threats present within your environment, including targeted threat actor activities potentially going unnoticed or unidentified.

We will leverage existing data sources and toolsets within your infrastructure, supplemented with additional solutions that can be deployed to ensure the full visibility needed for the identification of potential threats acting within your environment.

Our engagement frequency ranges from a one-time engagement to quarterly, or even weekly sustainment services, aligned with your specific needs.

Visibility & Methodology

During our Threat Discovery engagements, we'll leverage your existing toolsets and data sources in conjunction with supplemental solution that can be deployed as part of the engagement to achieve the necessary environmental visibility.

Full visibility across network, endpoint, logs, and other data sources allows our team to obtain current and historical situational awareness that ensures a holistic view of any potential threats acting within your environment.

Engagement Findings

Your Threat Discovery engagement results can range from insecure controls and identification of vulnerabilities to the extended presence of advanced threat actors working within the environment.

Regardless of the findings, our Incident Response experts will be working closely with your team throughout the engagement to communicate findings, provide tactical recommendations, and longer-term strategic recommendations that will increase your overall security posture.

Put an ELITE Team of Cybersecurity Practitioners on Your Side

Typical Threat Discovery activities will include all of the below components to ensure the required environmental awareness:

1. Network traffic analysis
2. Host analysis and mass triage of forensic artifacts
3. Log collection and review
4. Malware analysis and reverse engineering
5. Integration of threat Intelligence

Hundreds of Industry and Product Certifications

GCFE · GSE · GCFA · GSEC · GREM · CISSP · GCIH · GCIA

Customer Discovery Needs

Our customers leverage our Threat Discovery services to fulfill a wide variety of requirements, including:

M&A Activities

Perform due diligence and ensure the environmental health of recent acquisitions before integration into your existing infrastructure or organization

Penetration Testing

Supplement penetration testing engagements to not only tell you how a threat actor could get into your environment, but if they already have as well

Internal/External Analyst Support

Enhance the capabilities of your internal team or external service providers that might be performing standard monitoring or threat hunting services, by including periodic sessions specific to the identification of advanced threat and targeted attack activity

3rd Party Validation

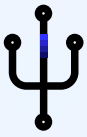
Confirm and assess the capabilities of your current analysis resources or visibility that is being provided by existing solutions

Investigation of Suspicious Activities

Validate preliminary findings or reports of suspicious activity, or mitigate concerns of a recent incident or breach

Post-Incident Confirmation

Ensure that remediation efforts associated with previous incidents have been effective and there is no subsequent adversary access



Sustained Hunting Expertise

Weekly hunting sessions to fulfill internal requirements for proactive threat hunting capabilities

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