GUIDEPOINT® SECURITY

PENETRATION TESTING

Gain Real-World Results to Understand Security Gaps and Prioritize Investments

Remove the Hypothetical and Gain Actionable Insights About Your Security Posture

Our highly-certified team uses controlled exploitation, detailed evidence and concise reporting to give meaningful insights to prioritize tactical remediation and plan strategic investments. We strive to uncover unique and obscure vulnerabilities that automated tools fail to detect.

Penetration Testing Tailored to Your Objectives for Actionable Results

Our teams have a "defender first" mentality that guides any penetration testing engagement. Whether it's internal or external networks, applications, cloud, security awareness or facilities, our cross-functional teams are poised to focus on your top priorities with the right combination of expertise. Our approach, focus and priorities are tailored to your organization's threats and environment to ensure our penetration testing meets your objectives.

Our penetration testers prioritize the manual aspects of a robust assessment methodology, leveraging hands-on expertise to identify even complex, multi-step vulnerabilities. We only use automated tools to augment our consultants and ensure that we identify as much as possible in the allotted time and budget.

## Benefits of GuidePoint's Pentesting Services:

Our pentesting engagements will provide visibility into areas such as:

Security Program Management Effectiveness

- Inventory missing patches and systems/applications that have reached EOL status
- Harden operating systems and third-party applications
- Evaluate security monitoring and IR capabilities
- Locate rogue devices in your environment
- Expose deficiencies in authentication measures
- Identify gaps in data egress filtering
- Discover publicly accessible information that could be used in targeted social engineering attacks

Business Impacts

- Demonstrate the true impact of compromise
- Demonstrate ROI of internal security initiatives
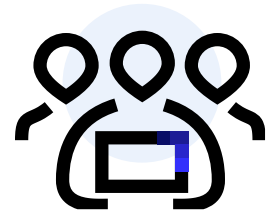
Put an ELITE Team of Cybersecurity Practitioners on Your Side

GuidePoint's Threat & Attack Simulation team is staffed by professionals who are technically adept and possess a diverse set of collective skills, enabling them to be extraordinarily adaptable to all security assessments.

Hundreds of Industry and Product Certifications

GuidePoint Security Penetration Testing Services

GuidePoint's Threat & Attack Simulation team provides customizable internal and external penetration testing services.
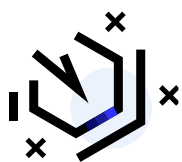
Internal Penetration Testing

This assessment simulates an attacker on the internal network (i.e. insider threat or a compromised end-user system) that will actively exploit vulnerabilities and leverage configuration deficiencies to provide a tangible demonstration of the associated business impacts in clear, repeatable steps. Our internal penetration test not only helps you demonstrate to leadership the impact of a successful internal attack, but also provides you with a real-world test of your security monitoring and incident response capabilities so you understand the areas with the greatest need of improvement.
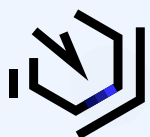
External Penetration Testing

We go beyond standard host, service and vulnerability scanning to uncover the vulnerabilities present in your perimeter systems. We not only uncover the active vulnerabilities affecting your perimeter systems, but also discover and present the Open Source Intelligence ("OSINT") that is available to an attacker before they ever even need to touch your systems.

Scenario-Based Penetration Testing

If there are specific attack vectors or threat models that are of particular concern, we will work with you to define a plan to simulate those scenarios. This approach places heavy emphasis on providing assurance that your defenders are properly equipped to adequately respond to a given incident. These types of assessments can be performed in similar fashion as traditional penetration testing or we can collaborate with our incident response team and your defenders in a Purple Team Assessment to ensure you have the visibility you need to effectively detect and respond to advanced threats.

Penetration Testing Deliverables

For either type of engagement, you will receive the following:

- **Executive Summary:** We will summarize the assessment approach, scope and findings in a manner that is appropriate for executive consumption. This summary will clearly communicate business risk and impact as well as provide a general understanding of the resources that will likely be required for both short- and long-term remediation.

- **Technical Analysis:** Each finding will include a description of the problem, a description of the impact, a list of hosts affected by the issue, specific steps for remediation, links to supporting reference data for independent research, and clear, step-by-step instructions on how to reproduce the finding on your own.

- **Custom:** We can address specific requests and requirements as needed.

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.