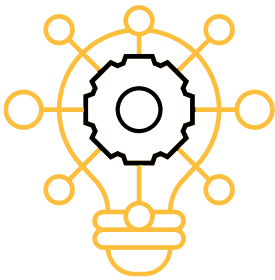


SERVICE BRIEF FOR

RED TEAM ASSESSMENT



Lodestone's Red Team Assessment service goes beyond the typical penetration test to show you how a real attacker would fare against your current security setup with none of the actual risks.

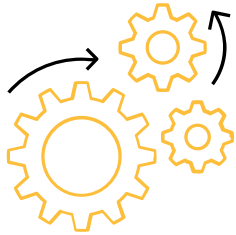
Lodestone professionals use the same tactics, techniques, and procedures (TTPs), scenarios, and tools employed by threat actors in the real world today to give your organization the most true-to-life experience without impeding your everyday business operations.

Lodestone Red Team Assessments are targeted and highly customized for your organization and its security goals. Our engineers will place pressure on your environment using common TTPs employed by threat actors today when targeting organizations in your industry. The end goal could be gaining access to specific pieces of Personally Identifiable Information (PII), access to a secure network within the organization, or other critical areas within your environment.

BENEFITS

- Understanding how your firewalls, endpoint detection and response (EDR), antivirus, and security information and event monitoring (SIEM) systems would shape up against a realistic attack.
- Invaluable experience for your internal IT teams as they test existing incident response procedures against simulated real-world threats.
- Insight into gaps in your organization's environment and what can be strengthened to protect your "crown jewels" and other high-value assets.

METHODOLOGY



As part of the Red Team Assessment, Lodestone engineers will test the maturity of your security program with real-world threat actor TTPs.

The phases of the engagement are as follows:

- **Scope and Rules of Engagement** – Red team assessments differ in scope from penetration tests due to the increased overall goal of the engagements. We will work with you to identify what systems, applications, employees, time frames, and more should be explicitly excluded from the engagement.
- **Information Gathering and Reconnaissance** – Lodestone engineers collect information of all types to identify your organization's footprint.
- **Attack Path Planning** – Our team utilizes the compiled information to develop various plans of attack to attempt to achieve the established assessment goals.
- **Execution of Attack** – Active exploitation will be performed during this phase of the engagement, including compromising found assets, executing phishing emails, and targeting personnel through social engineering.
- **Reporting** – Reports will be developed detailing the scope of the assessment, information found, narratives of the attack, and recommendations for remediation of found issues within your environment.
- **Report Review** – We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

ENGAGEMENT ARTIFACTS



The following artifacts will be obtained by our offensive security team as part of the assessment:

- Lists of external and internal assets
- Information gathered on personnel
- Logs for reconnaissance and exploitation activities
- Screenshots and information used for report deliverables

DURATION AND DELIVERABLES

Red Team Assessments will vary in duration based on the size of your environment, the number of systems, and the number of findings. Typically, these take two to three weeks, but may run longer depending on the goals of the testing.

Lodestone will provide the following deliverables to you as part of the engagement:

	Weekly Status Reporting – Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
	Executive Summary Report – Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable.
	Final Report – After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

©2023 Lodestone

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.

