Lodestone

SERVICE BRIEF FOR

ATTACK SIMULATION

Lodestone's Attack Simulation service, also known as the Red Team Engagement, 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.

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.

OVERVIEW

Lodestone Attack Simulations 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.

WHY LODESTONE

Lodestone is a global cybersecurity firm committed to helping clients prevent, investigate, and prepare for security incidents. It was built from the ground up to offer an innovative, behavior-based approach to proactive cybersecurity and digital forensics and incident response (DFIR). We are comprised of top investigative talent and offensive security experts from several of the world's largest cybersecurity firms, as well as military veterans and former members of national security organizations, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). We combine this expertise with our unique understanding of legal requirements through our relationship with our parent company, Beazley, which has been at the forefront of cyber insurance for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while preventing, preparing for, and responding to some of the toughest security challenges that industries face today.

Compliance

Since its founding as a subsidiary of Beazley in 2017, Lodestone has offered its customers insight into both cybersecurity and the cyber insurance industry. We help companies align and stay compliant with cyber insurance coverage requirements. In addition, we offer discounts to channel partners to form long-term relationships.

Security Focus

Lodestone's experts live and breathe cybersecurity and are committed to helping customers face some of the biggest challenges of their careers. We do not sell vendor security products – our offerings are purely service-focused, and any third-party tools we recommend are the product of genuine, vendor-agnostic, and tested endorsement, not business deals.

Expertise

Lodestone's approach to Incident Response is to have the top cybersecurity experts in the world, as the lead, and as the touchpoint, when responding to cybersecurity incidents. This is done with the backing of comprehensive, real-time threat intelligence to provide clients with protection across the life cycle of a potential security event or incident.

Tailored Approach

We understand the individual challenges of every situation and consider the human side of the equation, never taking a "one size fits all" approach. We blend design, threat intelligence, and technology with human insights to provide clients with the greatest cybersecurity advantage.

Threat Intelligence

Our deep understanding of threat actor tactics, techniques, and procedures (TTPs) is based on decades of experience in DFIR and the diligent gathering of threat intelligence from all possible sources.

Agility

Time is of the essence before, during, and after an intrusion. We stand ready to move in quickly and effectively at the first sign of an intrusion.

Team Experience

1000+
ENGAGEMENTS

200+ YEARS
COMBINED EXPERIENCE

50+
CERTIFICATIONS

Experts Unlike Anyone Else

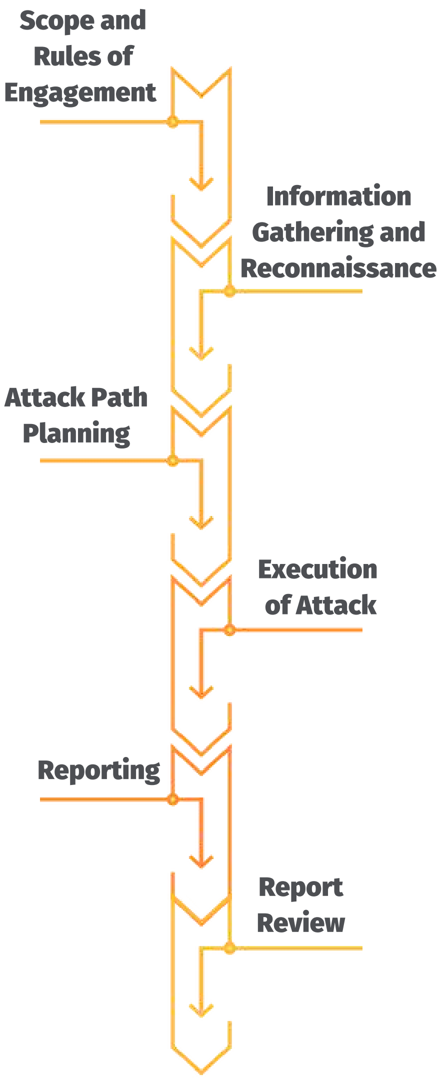
EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

As part of Attack Simulation, 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
Information Gathering and Reconnaissance
Attack Path Planning
Execution of Attack
Reporting
Report Review

- Scope and Rules of Engagement – Red team engagements 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

Attack Simulation Engagements 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.

Lodestone Security is a wholly owned subsidiary of Beazley plc. Lodestone provides computer security and cyber security consulting services. Lodestone does not provide insurance services and client information obtained by Lodestone is not shared with Beazley claims or underwriting. Likewise, client information obtained by Beazley claims or underwriting is not shared with Lodestone.