Lodestone

SERVICE BRIEF FOR

BREACH SIMULATION

Lodestone's Breach Simulation, also known as the Assumed Breach Assessment, is Lodestone's response to an unfortunate truth in cybersecurity: it is often not a matter of if an organization will experience a breach, but when. From misconfigurations, an accidental click within a phishing email, a disgruntled employee looking to cause harm, and beyond, it can only take one gap in your company's armor for a threat to slip through. All isn't lost, however, and it is certainly no time to give up.

We work with your team to create the most accurate simulation of a breach possible so that you will be prepared to handle more than just hypotheticals. Our experts help you identify gaps and provide the experience and training to enable your personnel to respond to future security concerns with confidence and poise.

BENEFITS

- Gaining the experience and lessons learned from an insider threat or compromise without going through the incident.
- Technology control testing using the tactics, techniques, and procedures (TTPs) of real threat actors to give you the real-world advantage.
- Insight into whether existing plans and policies allow your company to detect and fully address insider threats and other incidents.

OVERVIEW

Lodestone's Breach Simulation gives your company access to an experienced offensive security team as we identify gaps in your defenses and prepare your personnel to respond to insider threats and other types of compromise. Our engineers will attempt to enumerate resources and pivot within your network using the existing infrastructure in the same way an actual threat actor would, but without the damage to your business. There's no better training than real life – we simulate a breach and response scenario as realistically as possible to maximize your company's ability to respond.

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

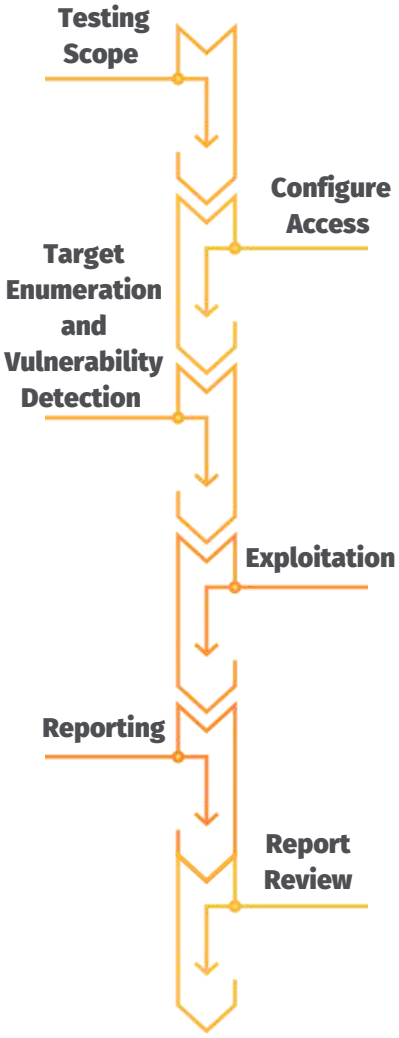
EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

As part of Breach Simulation, Lodestone engineers will simulate the behavior of actual threat actors to provide a true test of your company's readiness to respond.

The phases are described in the subsections below.



- Testing Scope – Lodestone will work with you to determine the best scenario to test your response abilities. This includes identifying in-scope areas of your environment for testing, such as email portals, web applications, portals, or file-sharing applications. Our goal is to provide the most realistic experience possible without damaging or interrupting your business's everyday operations.
- Configure Access – We plan the "rules of engagement" of the assessment, including where our engineers will begin. This could the simulation of a breach caused by an internal threat, or planning to begin at the outside of your environment and attempt to work our way in.
- Target Enumeration and Vulnerability Detection – Engineers will begin to enumerate potential resources and services running on open ports discovered from open-source intelligence (OSINT). Testers and threat actors use this research to formulate attack paths and identify potential methods for exploitation.
- Exploitation – Lodestone engineers test findings from the previous phase to determine if they can be exploited. If so, our offensive security team will carry out these exploits and determine what information and systems they can access. From there, they will attempt to escalate privileges, exfiltrate data, and pivot to other devices and services.
- Reporting – We provide a written final summary of the Breach Simulation that includes an executive summary of the engagement and a detailed description of the findings and any remediation procedures to strengthen your security posture.
- 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:

- Internal IP address ranges
- Credentials captured during testing
- Gathered data
- Screenshots and information used for report deliverables

DURATION AND DELIVERABLES

Breach Simulation will vary in duration based on the size of your environment, the number of systems, and the number of findings, but typically takes two to three weeks.

This service can be delivered on-premises or remotely, and 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.

Learn more at www.lodestone.com

Connect with us:

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com