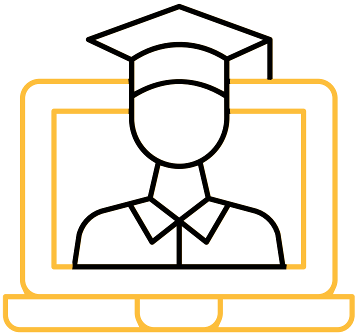
SERVICE BRIEF FOR

ASSUMED BREACH ANALYSIS



Are you worried that the call is coming from inside the house? If your company is concerned that they have already been breached, Lodestone professionals will help you get to the truth of the matter with a forensic investigation of your environment.

Our experts will hunt for evidence of compromise across any and all desired systems and report back with insights into your current state of security. Whether we can prove that a security incident has occurred, there is no evidence of a compromise or anything in between; Lodestone is prepared to equip you with the knowledge you need to make your next move.

BENEFITS

- Rapidly assess the health of your entire network with expert knowledge on what threats are lurking based on experience gained from hundreds of real-world attack investigations.
- Readiness to pivot to incident response at a moment’s notice if an incident is confirmed.
- Recommendations based on findings and years of experience to strengthen the security of your environment.

OVERVIEW

Lodestone’s Assumed Breach Analysis service takes a holistic and widespread look across your organization’s entire network to assess any current or historical threats that may be present in your environment. We are prepared to identify indicators of compromise from everything from commodity malware and spyware to nation-state threat actors and advanced ransomware actors.

Lodestone utilizes an easy-to-deploy agent and industry-leading knowledge to quickly search for threats and abnormal activity, as well as poor security practices and potentially unwanted software.

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

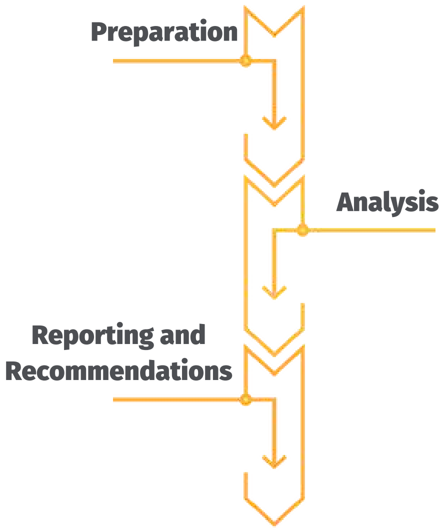
Experts Unlike Anyone Else

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

Global Presence - NA/Europe

METHODOLOGY

Assumed Breach Analysis is comprised of these primary phases:



- **Preparation –** Lodestone works with your personnel to deploy a lightweight agent across all of your organization's endpoints with minimal impact on performance and day-to-day activities.
- **Analysis –** Our experts run a full suite of artifact collection based on the MITRE ATT&CK framework, searching for evidence of compromise from all stages of the attack lifecycle. We perform deep dives into suspicious activity and assess whether findings represent false positives, evidence of a previous event or incident, or evidence of an active event or incident.
- **Reporting and Recommendations –** Lodestone professionals create and present to your stakeholders a detailed report of our findings, including any vulnerabilities or areas of particular concern. Recommendations are also provided to maximize the hardening of your environment while minimizing the level of effort needed to make those changes.

DURATION AND DELIVERABLES

The time required for an Assumed Breach Analysis depends upon the size of the environment and the breadth of suspicious activity detected within the environment. This typically takes two weeks from the time of agent deployment across all in-scope endpoints.

As part of the engagement, Lodestone will provide a report that details our methodology, the scope of the environment, and a complete explanation of all threats and risks detected over the course of the analysis, all under the lens of the industry-accepted MITRE ATT&CK framework.

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

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.