Lodestone

SERVICE BRIEF FOR
PROTECTED DATA BREACH RESPONSE

Accessing and exfiltrating protected data, including data covered under standards such as the Health Information Portability and Privacy Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS), is often the goal for many threat actors.

Whether the data breach began with a business email compromise (BEC), a ransomware event, insider threat, or another intrusion vector, Lodestone professionals turn the full force of their expertise towards investigating the source of these breaches and the extent of the effect they had on your environment.

BENEFITS

- Help eliminate uncertainty on what protected data may have been breached, to what extent, and how.
- Receive a detailed report that documents the circumstances and details surrounding unauthorized data access and exfiltration.
- Expert advice on enhanced auditing and data protection strategies to defend your company's most critical assets.

OVERVIEW

Lodestone's Protected Data Breach Response provides a thorough analysis of a threat actor's actions within your network and protected data stores. A Case Lead will lead an assessment of logs and evidence surrounding protected data stores and provide a thorough investigation into data access, manipulation, and theft.

Lodestone's experts will also provide detailed recommendations on improving internal data security to reduce the impact a threat actor may be able to have in the future.

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

Protected Data Breach Response is comprised of these primary phases:

- **Initial Response –** Lodestone works with you to determine the scope of the environment, our initial impressions of any potential impact on the environment, and business objectives your organization may have.
- **Evidence Collection –** Our experts work with you to understand how a threat actor may have accessed protected data and collect evidence accordingly. We use industry-standard tools and software and perform all necessary handling steps to address any legal considerations.
- **Investigation –** Lodestone analyzes the evidence collected to identify available indicators of compromise. We provide contextualization to the incident, including determining, if possible, the root cause, the malicious activity performed, and what unauthorized data may have been accessed or exfiltrated.
- **Reporting –** We provide a written final summary of the investigation with a concise description of the findings and details of the investigation for any historical preservation and reporting requirements you may have.

DURATION AND DELIVERABLES

Protected Data Breach Response times vary based on the size of the tenant and the systems involved. However, this typically takes a period of one to two weeks.

As part of Protected Data Breach Response, Lodestone will provide any or all of the following upon request:

- **Executive Summary Report** – A high-level summary report that provides an overview of the Protected Data Breach Response, including key findings identified during the investigative process.
- **Digital Forensics and Incident Response (DFIR) Report** – A detailed, technical breakdown of how the threat actor operated within your environment, including a granular list of affected systems and data, in addition to the information provided in an Executive Summary Report.
- **Executive Debrief** – An overview of the investigation and key findings presented in-person or via video conference with our Case Lead.
- **Best Practices Overview** – A generalized list of best practices that can help you strengthen your security posture against future attacks.

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