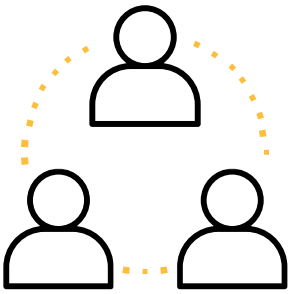
Lodestone

SERVICE BRIEF FOR

# INSIDER THREAT RESPONSE



When a suspected breach comes from within your company, Lodestone experts can serve as your trusted advisor to determine the scope of the investigation.

Whether we deliver evidence or report on a lack of evidence to support insider threat activities, Lodestone professionals can help arm you with the knowledge you need to make key decisions. Lodestone is experienced with numerous cases, and various insider threat techniques, including thumb drives, web portal exfiltration, and beyond, and has the experience to detect any evidence of potentially nefarious behavior and deliver our findings in a clear and easy-to-reference format.

## BENEFITS

- Comprehensive, yet discreet, support in making a determination on whether an insider threat event has occurred and the individuals involved.
- An in-depth understanding of what data was affected and actions performed by an insider threat during a given time period.
- An assessment of abnormal activities, including off-hours events, abnormal web browsing and file searches, and high volumes of data download or upload.

## OVERVIEW

Lodestone's Insider Threat Response service provides a discreet and thorough analysis of an insider's actions within your network. A Case Lead will lead a methodical collection of data and provide a detailed summary of abnormal actions taken by an insider.

Lodestone's experts will also provide detailed recommendations on improving internal data security to reduce the impact an insider threat 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

An Insider Threat Response is comprised of these primary phases:


- **Initial Response –** Lodestone works with you to determine the scope of the investigation, 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 discreetly collect evidence and complete analysis that gives you the answers you need without alerting personnel to an investigation underway. 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 insider threat, including determining, if possible, the individuals involved, the time frame of the activity, 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

Insider Threat Response services vary based on the size of the tenant and the accounts potentially involved. However, this typically takes a period of one to two weeks.

As part of Insider Threat 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 Insider Threat 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 tenant, 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