Lodestone

SERVICE BRIEF FOR POST-INCIDENT MONITORING

When the worst comes to pass, Lodestone’s SOC professionals stand ready to support you with effective monitoring and alerting that protects your environment during the investigation and restoration processes. We work with you to reduce the mean time to resolve (MTTR) for incidents and get critical information to the right members of your team more quickly.

Detect if a threat actor is still in your environment or if malicious files have been left behind with 24/7 monitoring, detection, identification, and threat hunting. Our experts work to bring you the ease of mind on your worst day so you can focus on minimizing business continuity disruptions and combating further loss.

BENEFITS

- Prevent instances of re-infection by threat actors after a compromise.
- Ensure that any and all lingering threats within your environment are eradicated.
- Instill confidence in partners and customers that your network is clean and secure.

OVERVIEW

Lodestone’s Post-Incident Monitoring Services utilizes indicators of compromise identified in incident analysis as well as tactics, techniques, and procedures (TTPs) gleaned from years of recorded attack patterns analyzed by our experts. Following a security event or incident, put your mind at ease with monitoring from Lodestone professionals to eliminate lingering threats and prevent recurrence.

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

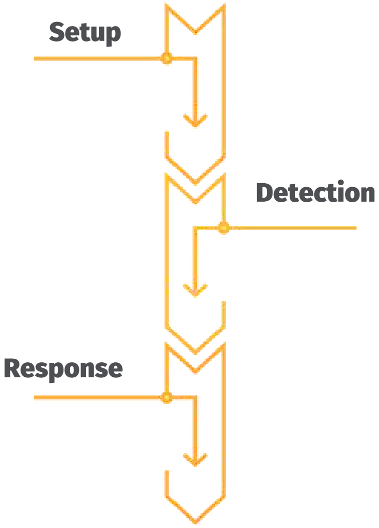
EX-

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

Global Presence - NA/Europe

METHODOLOGY

Lodestone's Post-Incident Monitoring service is comprised of these primary phases:



- **Setup** – Lodestone experts work with your personnel to deploy endpoint detection and response (EDR) within your environment with minimal disruption to day-to-day functionality.
- **Detection** – Under 24/7 monitoring by our experienced SOC staff, your environment will be scanned regularly for any lingering threats. In addition, Lodestone will perform advanced searches to ensure that threat actors do not have the opportunity to re-enter your environment.
- **Response** – We routinely deliver our findings to you, providing alerts via email or phone, depending on the urgency of the issue at hand. As threats are detected, Lodestone will take immediate action if feasible or advise you on how to remove the threat.

DURATION AND DELIVERABLES

Lodestone's Post-Incident Monitoring service is performed for a period of 30 days. Reports or deliverables are not included in this engagement type, but alerts will be provided via email or phone, depending on the urgency and severity of what has been detected.

DEFINITIONS

See the definitions below for an explanation of some of the Lodestone SOC team's methodologies:

- Evidence assessment – This process involves interviewing personnel to understand what data is available. Based on the data available, Lodestone will request any additional data needed to perform the required assessment or analysis.
- Evidence collection – This process involves the collection of data for analysis. Where applicable, Lodestone will facilitate the collection process by providing tooling and support or requesting access to perform the full collection.
- Analysis – Processing, reviewing, and organizing all data sources to answer key questions and gather information.
- Report findings – The results of assessment and analysis, often presented in a meeting with key stakeholders. This information may be provided through a presentation.
- Report writing – Documenting all factual findings into a report that accurately represents the assessment or analysis performed.
- Recommendations – Suggestions based on industry-leading experience to harden technologies, reduce attack surfaces, enhance policies, and promote a security-minded culture.

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.