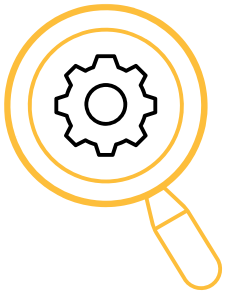
Lodestone

SERVICE BRIEF FOR

THREAT HUNTING



Take an active role in detecting advanced threats in your company's network with Lodestone's threat-hunting capability.

Our experts use automation and tools that leverage machine learning and user and entity behavior analytics (UEBA) to identify potential risks and then investigate further, iteratively tracking suspicious behavior in your environment. Results are also stored to serve as a foundation for future analysis. With a proactive analysis of threats, Lodestone can help you interrupt attackers at the earliest possible stage and strengthen your security posture with the results of robust threat hunts.

BENEFITS

- Fill security gaps left behind by even the most advanced software platforms.
- Ensure that threat actors are detected and removed from your environment as quickly as possible to minimize their ability to do damage.
- Maintain a layered threat detection model necessary for today's advanced threat landscape.

OVERVIEW

Lodestone's Threat Hunting service brings our experts' years of real-world investigation experience to close critical gaps in modern security appliances. While modern security appliances offer great protection and detection, Lodestone's Threat Hunting goes a step further and adds human intelligence to eliminate blind spots.

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

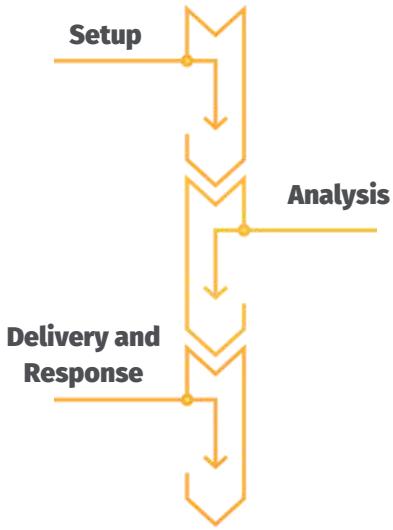
Experts Unlike Anyone Else

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

Global Presence - NA/Europe

METHODOLOGY

Lodestone's Threat Hunting service is comprised of these primary phases:



- **Setup** – Lodestone experts work with your personnel to assess your existing technology stack. If the current technology cannot support Lodestone's threat hunting, we will assist with deploying a new version or alternate solution.
- **Analysis** – Leading threat intelligence and attacker techniques are used to continuously identify and assess the severity of potential threats within your environment.
- **Delivery and Response** – We routinely deliver our findings to you, creating a list of potential threats within the environment with detailed information on each threat's severity and ability to negatively impact your environment. Lodestone also stands by to immediately assist with the removal of threats as they are discovered.

DURATION AND DELIVERABLES

This service is paired with Lodestone's Managed Detection and Response service, with the same length of service and same deliverables. See Managed Detection and Response for additional details.

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