Lodestone

SERVICE BRIEF FOR

FORENSIC CHECKUP

Whether your company is preparing for a merger or simply looking to maintain a strong security posture, health checks can help keep you, your partners, and your customers safe. As part of a health check, Lodestone experts use investigative tools to perform a highly technical forensic analysis of your environment. This includes triage and searching for telltale indicators of compromise to determine whether your environment can be considered clean of malicious activity.

We reflect our findings in a health report that gives you a clear look into your current security hygiene and allows you to take control of your cyber health.

BENEFITS

- Confirm whether or not a system or systems are compromised and, if so, to what extent. Understand how your wider environment might be impacted.
- Actionable recommendations based on any findings to harden your security.
- Receive a detailed report documenting any actions performed on the system, including a clean bill of health, if applicable.

OVERVIEW

Lodestone's Forensic Checkup helps organizations concerned that one or more systems or devices in its networks may have been compromised or inappropriately accessed. A Case Lead supported by a team of Lodestone experts uses industry-standard forensic techniques to investigate the environment and identify any signs of malicious activity.

We will work to identify whether systems or devices have been compromised and, if so, to what extent. Should a compromise have occurred, Lodestone will additionally work to identify what risk or threat may be posted to the rest of the network and whether a full-scale breach has occurred.

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

The Forensic Checkup 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 collect the necessary evidence to complete an analysis that gives you the answers you need. We provide several methods for this for ease and to prevent keeping your team from important day-to-day work. We use industry-standard tools and software and provide all necessary handling steps.
- Investigation – Lodestone analyzes the artifacts collected to find any available indicators of compromise and other key information. We contextualize any findings and communicate with you to inform you of our progress and any significant findings. Our experts provide the most thorough answers possible based on the available sources, including the potential impact and scope if an incident is suspected and how to take steps to prevent future attacks.
- Reporting – We provide a written final summary that includes a concise description of any findings and details for historical preservation and reporting requirements. If no evidence of a security event or incident is found, our experts will instead provide a clean bill of help that details the thorough techniques used to assess the condition of your environment.
- Conclusion and Future Planning – In addition to the delivery of the report, our experts provide you with industry general cybersecurity best practices to aid you in hardening your environment. We remain available to answer any questions and deliver other services to help you continue on your security journey.

DURATION AND DELIVERABLES

The Forensic Checkup varies in duration based on the size of your environment, the number of systems, and evidence delivery times, but is typically complete within one week of evidence collection. It can be delivered on-premises or remotely.

As part of the engagement, Lodestone will provide the following deliverables:

- Executive Summary Report – A high-level summary report that provides an overview of the activities performed, including any key findings identified over the course of the forensic checkup.
- Best Practices Overview – A generalized list of best practices that can you're your company strengthen its 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