Lodestone

SERVICE BRIEF FOR

FORENSIC DATA COLLECTION

Lodestone's Forensic Data Collection places our seasoned teams directly in charge of collecting data from your environment prior to investigation, especially for ransomware and suspected ransomware events.

Our experts work with your personnel to collect evidence in a manner that preserves key artifacts and securely transfers data with minimal disruption to your business flow.

BENEFITS

- Precise collection based on investigation requirements by personnel that work alongside our Incident Response team.
- Protection of sensitive and potentially volatile data by having them retrieved by technical experts with years of experiences.
- Reduction of impact to staff, IT personnel, or your remote managed service provider (MSP) to maximize evidence gathered while minimizing disruptions.

OVERVIEW

Lodestone's Forensic Data Collection equips organizations that suspect they have been the target of a cyberattack with the knowledge and confidence to recover quickly and effectively without hindering future investigations. Organizations often begin the recovery process before securing all evidence, hindering the efforts of internal or external incident responders to understand the incident and prevent recurrence. Lodestone experts work with incident responders as they evaluate the impact of the attack on your environment and retrieve any additional forensic artifacts should the need arise.

The information gathered is compiled into a summary that details the evidence gathered, including hash values and other forensic details. This record lets your personnel understand exactly what was collected and when.

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

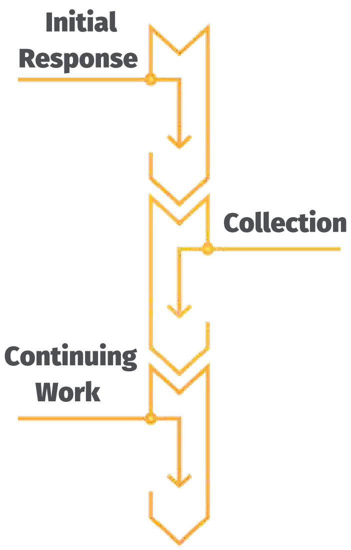
EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

Lodestone's Forensic Data Collection partners our restoration experts with your incident responders, be they internal, from Lodestone, or from another third party. The goal is to maximize the potential of the investigative process and set your incident responders up for success.

Lodestone employs a standard methodology that includes multiple phases:



- Initial Response - During the first phase of Lodestone's Forensic Data Collection, we work with you to determine the scope of the environment and identify indicators of the breadth of impact of the suspected incident on your environment. We determine what your business objectives and primary concerns are, along with what steps have been taken prior to our arrival.
- Collection - Based on the understanding of the potential incident and your business needs, we collect all evidence deemed applicable and assist the incident response team with analysis to provide you with the critical answers you need. We use industry-standard tools and software to ensure that all evidence handling considerations are accounted for and address any legal considerations.
- Continuing Work - Once the initial evidence collection is complete, we will continue to work closely with the incident responders as the investigation progresses. We will be prepared to retrieve any additional evidence needed to further the investigation quickly and with as little disruption to your business as possible.

DURATION AND DELIVERABLES

The delivery of Forensic Data Collection varies in duration based on the size of the environment and resources, as well as the duration of the incident response efforts that are being supported.

Lodestone will provide the following deliverable to you as part of the engagement:

- Evidence Summary – Lodestone will provide detailed documentation of the actions our engineers have taken to collect evidence from within your environment. This includes location, time, type, and hash values.

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

©2022 Lodestone
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.