SERVICE BRIEF FOR
POST-INCIDENT REHABILITATION

Lodestone's Post-Incident Rehabilitation helps businesses recover from security incidents – particularly ransomware and ransomware-related events.

Our experts will help you pinpoint weaknesses in your security posture that were or could be exploited by threat actors and address them in a way that complements and safeguards your network.

BENEFITS

- Best implementation of security measures through the guidance of experts with years of experience in incident response and restoration.
- A full external analysis of security gaps and practices that gives you an outsider's perspective into your security posture.
- Receiving best-fit models and strategies for your organization that help you build security into every aspect of your business without hindering flow.

OVERVIEW

Lodestone's Post-Incident Rehabilitation equips organizations that have been targeted by ransomware with the ability to identify those small gaps in network security that can have devastating consequences. Lodestone experts use industry-standard best practices to evaluate your environment and make specific and targeted recommendations to improve your entire security posture.

Once you have chosen a path, we will work with you to implement and configure the security measures you select and test them to ensure they address the identified vulnerabilities. Our experts assist you through the entire process to help you refine your security practices with confidence.

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
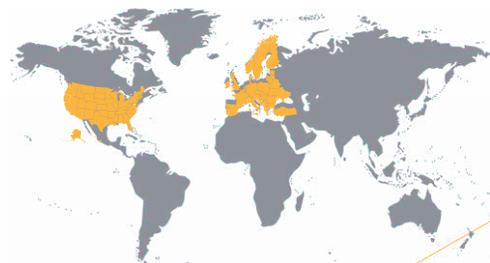
METHODOLOGY

The Lodestone Post-Incident Rehabilitation includes industry best practices and recommendations tailored specifically for your environment to give you the best, most secure return on your investment.

Lodestone employs a standard methodology that includes multiple phases:
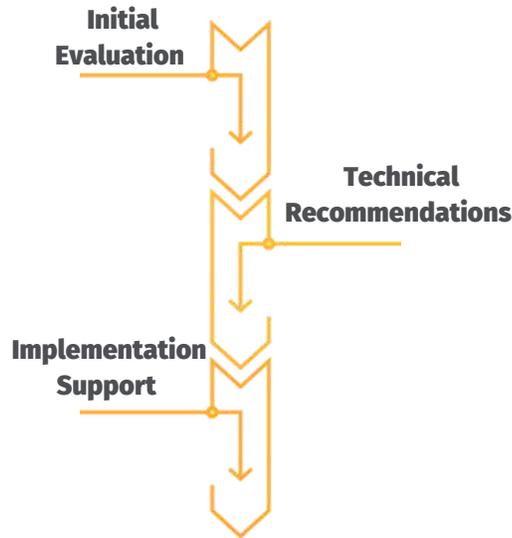
- **Initial Evaluation** - The first phase of Lodestone's Post-Incident Rehabilitation involves gathering details on your business and its unique needs and security requirements. This includes what best serves your business and will minimize disruption while protecting against recurrence and similar threats.
- **Technical Recommendations** - Lodestone engineers collaborate with your company's IT personnel to identify the best recommendations for security based on your company's unique posture. We understand that effective security solutions must carefully balance usability and protection. We work to give you the most impact and benefit without disrupting your business.
- **Implementation Support** - Once Lodestone experts have pinpointed our recommendations and you have confirmed the strategy you want to pursue, we work with your personnel throughout the installation and configuration phases. Whether on-premises, in the cloud, or stored at a colocation, we help ensure that everything works and has as minimal of a negative impact on your business as possible.

DURATION AND DELIVERABLES

Post-Incident Rehabilitation varies in duration based on the size of your environment and the scope of installation, configuration, testing, and equipment delivery times. However, it typically takes six to eight weeks and can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement.
- **Technical Recommendations Report** – A list of custom security measures and implementations ranked from most to least impactful to the security of your environment. This includes recommended vendors based on industry performance, quality, and our understanding of your unique environment and its needs.

Learn more at www.lodestone.com