Lodestone

SERVICE BRIEF FOR

EMAIL HARDENING ASSESSMENT

Lodestone Email Hardening Assessment targets Microsoft 365 (M365) tenants, in particular, to reduce risk by proactively reviewing and addressing common misconfigurations. M365 is a highly targeted resource by threat actors due to its prevalence as a business solutions service and value if infiltrated. A compromised M365 tenant can allow threat actors to remotely access sensitive and business-critical data, even without the need to breach your network's actual perimeter.

We work with you to identify risks in the most critical component of your M365 tenant: its security configuration. Our experts offer solutions that align with your business needs and help you optimize security and increase visibility into events occurring in a critical part of your workflow.

BENEFITS

- Identification of potential security challenges and their risks to your organization, including misconfigurations that could leave data exposed or susceptible to unauthorized access.
- Improvement of security posture through configuration evaluation and recommendations on security hardening and best practices.
- Insight into your current M365 tenant, including a high-level overview of your current configuration.

OVERVIEW

Lodestone's email hardening assessment is a structured engagement designed to help you understand your security posture within the context of what is often one of the most frequently used components of a business: the M365 tenant. We identify gaps and misconfigurations and connect with your personnel to create a customized roadmap for security controls that will reduce your risk of compromise.

We evaluate your organization's M365 tenant against the following security control areas:

- Account/Authentication
- Application Permissions
- Data Management
- Email security / Exchange Online
- Data security and storage
- Auditing
- Mobile device management (MDM)

Included in our findings are recommendations that balance industry best practices with your organization's productivity needs.

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

As part of our email hardening assessment, Lodestone consultants will review your M365 configurations and settings for critical security control areas.

The Email Hardening Assessment is comprised of these primary phases:

- Initial Consultation – A brief overview of what the email hardening assessment entails, where we walk you through the security controls that will be assessed and how we will conduct the assessment.
- Configuration Review – We provide a thorough configuration review of your M365 tenant to ensure that security configurations follow industry guidelines and are optimized to your business's unique needs.
- Reporting – We provide a written final summary of the email hardening assessment with an executive summary of the engagement and a detailed description of the findings and any remediation procedures to better protect your M365 tenant.
- Report Review – We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

DURATION AND DELIVERABLES

An email hardening assessment takes approximately one week. As part of the engagement, Lodestone will provide the following:

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

- Executive Summary Report – This report will provide a high-level overview of the process, methodology used, and overall risk to the organization based on the results of the assessment of your M365 tenant.
- A snapshot of the existing M365 security configurations.
- Prioritized and detailed recommendations for further hardening your organization's M365 tenant.
- An executive debriefing call to discuss findings and provide clarity on any lingering questions or concerns.

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