Lodestone
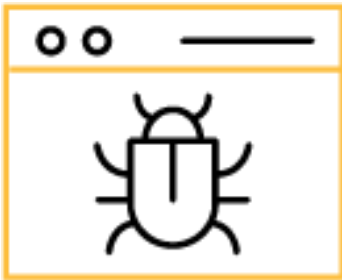
SERVICE BRIEF FOR
VULNERABILITY ASSESSMENT

Lodestone Vulnerability Assessment is an expert analysis of vulnerabilities in your company's information systems – that is, weaknesses, flaws, or errors that could be exploited or triggered by a threat actor to gain access to your network. Vulnerabilities in network infrastructure, system security procedures, and internal controls are common entry points for threat actors. We equip you with insight into weaknesses in your environment so you can be better prepared for whatever cyber threats might come your way.

In the event of critical findings that need immediate remediation, we will work with you to develop a detailed remediation strategy that helps keep your environment safe and your critical assets protected.

BENEFITS

- Identification and mitigation of security vulnerabilities before attackers can find them, reducing your company's likelihood of falling victim to a cyberattack.
- In-depth analysis of your environment and elimination of false positives without disruption to your daily business operations to help you make your environment stronger, faster.
- Critical visibility into your network, including an inventory of all systems on your network to address device-specific vulnerabilities, plan upgrades and future assessments, and establish a business risk/benefit curve to optimize your company's security investments.

OVERVIEW

Lodestone's Vulnerability Assessment combines automated scanning with manual assessment techniques and open-source intelligence (OSINT) to evaluate your company's security posture. These activities can be performed externally by targeting all Internet-exposed systems and devices, or internally, with one of Lodestone's proprietary vulnerability testing devices on your network.

Our experts identify potential security weaknesses in your environment and report our findings and recommendations to strengthen your company's security posture and deter would-be attackers. We use industry-standard techniques to assess internal and external weaknesses and categorize our findings based on criticality.

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 Vulnerability Assessment provides direction on reducing the risk created by vulnerabilities in your environment and yielding a better understanding of assets, severity, and overall risk to your organization.

The Vulnerability Assessment is comprised of these primary phases:

Initial Assessment

Defining a Baseline

Vulnerability Scanning

Reporting

Report Review

- **Initial Assessment** - We work closely with you to gain a deep understanding of the devices on your network and its nuances, including the 6Ps (Patch, Ports, Protect, Policies, Probe, and Physical). This collaborative effort helps Lodestone engineers determine which systems are accessible from the Internet, their criticality, and their roles. It helps prepare and prioritize the remainder of the assessment and establish the optimal order for vulnerability assessment scans.
- **Defining a Baseline** - For each system to be assessed, we help you determine a baseline – that is, whether its configuration meets basic security best practices or not. The most common baseline factors we identify include:
  - Operating system (OS)
  - Version
  - Service pack or build, if applicable
  - Approved software
  - Installed services and required ports
  - Unnecessary open ports
  - Any additional security configurations, as applicable
- **Vulnerability Scanning** - We deploy automated vulnerability scanning tools and perform manual testing to discover any vulnerabilities in your environment. During the external portion of a Vulnerability Assessment, Lodestone engineers evaluate Internet-facing web applications, URLs, servers, and workstations. During the internal portion of the Vulnerability Assessment, Lodestone engineers evaluate servers and workstations in the environment and behind your firewalls Organizations subject to regulations like the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and others should look to perform scans that confirm adherence to compliance regulations. As part of this step, we perform the following activities:

  - Information Gathering and Discovery: Lodestone engineers gather information through publicly available OSINT on compromised credentials, and breached databases. We gather information on your external network footprint by gathering IP addresses and other publicly available information.
  - Review and Enumeration: After determining which hosts are live on each network, we use various scanning techniques on these hosts to find services listening on TCP and UDP ports. The scans are initially run against more than 1,000 ports to search for specific services, including SMTP, FTP, telnet, NetBIOS, HTTP, and many less well-known services. Additionally, a few servers scattered throughout the addresses provided ran other services such as SSH, FTP, and Telnet.
- **Reporting** - We manually verify the vulnerabilities we identify in your network and develop recommendation strategies to mitigate those vulnerabilities. The assessment includes the external-facing web application, URLs and servers, and internal vulnerable servers and workstations. Our reports include pertinent details that can be used to respond to found vulnerabilities, including:
  - Vulnerability discovered
  - The date of discovery
  - Common Vulnerabilities and Exposures (CVE) database reference and score
  - A list of vulnerable systems and devices
  - Detailed mitigation steps, including patching and the reconfiguration of operating systems or applications
- **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

The Vulnerability Assessment varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

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

◆	**Weekly Status Reporting –** Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
◆	**Executive Summary Report –** Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable.
◆	**Final Report –** After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings.

Learn more at www.lodestone.com