Lodestone

SERVICE BRIEF FOR

ACTIVE DIRECTORY HARDENING ASSESSMENT

Lodestone's Active Directory Hardening Assessment addresses one of the most complex, yet least understood components of the vast majority of enterprise environments. Threat actors know the potential for exploitation in a misconfigured or otherwise vulnerable Active Directory, and often utilize this critical infrastructure as a common path of attack when targeting organizations.

Our engineers stand ready to dive into your AD setup and give you an understanding of this key component within your environment that many organizations lack. We will equip you with knowledge and recommendations to better secure your valuable data and strengthen your security posture.

BENEFITS

- Identification of potential attack paths within your environment to enable you to create an environment that limits your attack surface and helps stop threat actors in their tracks.
- Identification and classification of system and application-level vulnerabilities that could pose internal threats to your organization.
- Findings and recommendations for addressing misconfigurations and vulnerabilities in your Active Directory based on level of importance to give your personnel a custom roadmap to a stronger security posture.

OVERVIEW

Lodestone's Active Directory Hardening Assessment gives you a comprehensive view of your Active Directory setup. This overview includes the identification of any misconfigurations or attack paths that threat actors could exploit within your environment, optimization of group policy controls, a listing of privileged accounts, and other valuable information. Lodestone will assess your environment and help you prioritize changes to your Active Directory that can significantly increase security and lower risk.

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 Lodestone's Active Directory Hardening Assessment, Lodestone engineers will get to know the nuances of your organization's Active Directory setup to pull back the curtain on a key piece of your infrastructure.

Active Directory Hardening Assessment is comprised of these primary phases:

- Testing Scope – Lodestone will work with you to understand your environment and determine the best course of action for assessing AD-related components.
- Information Gathering – Our engineers will utilize security resources and automated testing tools to gather user information, privilege levels, groups, and policies to combine with data collected over the course of the assessment.
- Analysis – The above-gathered information will be reviewed to determine risks within your environment due to misconfigurations, overreaching policies, and unaddressed vulnerabilities.
- Reporting – All findings will be compiled into a report that includes issues and misconfigurations, potential paths to exploitation in Active Directory, and recommendations for remediation.
- Report Review – We will 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 will be scheduled to ensure that all of your concerns are addressed.

ENGAGEMENT ARTIFACTS

The following artifacts will be obtained by our offensive security team as part of the assessment:

- List of internal IP address ranges
- Credentials for accounts used in testing
- Screenshots and information used for report deliverables

DURATION AND DELIVERABLES

Active Directory Hardening Assessments vary in duration based on the size of your environment, the number of systems, and the number of findings, but typically take two to three weeks.

This service can be delivered on-premises or remotely, and 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 detailing the engagement, findings, and recommendations for mitigating the findings.

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