Lodestone

An elite cybersecurity force

You've heard it all before

It's a tale as old as the Internet: with every year, the world becomes increasingly dependent on technology and its advantages. We are more connected than ever before, and the complexity and depth of those connections continue to increase. With these advantages, however, come new risks humanity has never faced before. Cybersecurity incidents have gone from niche news to front-page headlines, where they can affect millions of people and bring industry giants to their knees with astronomical financial, legal, and reputational consequences. It is the unfortunate truth that it is not a matter of if a company will be compromised, but when. That doesn't mean, however, that all hope is lost.

Digital defenses

The explosion of technological advances from mobile devices and apps to cloud services, wireless networks, data analytics, and beyond has created uncertainty about lurking dangers. In the face of this, cybersecurity experts like Lodestone have committed themselves to fighting the good fight – and helping companies prepare themselves to stand up to digital threats. A mature cybersecurity program is critical in helping companies combat threat actors, whether they come from outside or within. This begins with an understanding of one's own attack surface – that is, where a company's environment may be vulnerable to adversaries. While there is no such thing as a silver bullet or a flawless defense, reducing this attack surface as much as possible and closely monitoring vulnerable points that cannot be eliminated can stop would-be cybersecurity incidents in their tracks or minimize the damage they cause.

About us

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection. Lodestone has a unique understanding of the intersection between cyber insurance and cybersecurity while responding to some of the toughest security challenges that industries face today. In other words, we know what insurance providers care about as we offer them expert recommendations on what risk to accept. Being product-agnostic, we focus on practical, actionable solutions that are based on real-world scenarios and modify our services to suit each client's needs.

Governance, Risk and Compliance Advisory

- CIS-18 Gap Analysis
- Incident Response Plan Development
- Security Policy Review and Development
- Security Awareness Training
- Tabletop Exercises
- Virtual CISO

Offensive Security

- Active Directory Hardening Assessment
- Email Hardening Assessment
- Penetration Testing
- Phishing Campaign Assessment
- Red Team Assessment
- Vulnerability Assessment
- Web Application Penetration Testing

Digital Forensics and Incident Response

- Assumed Breach Analysis
- Digital Forensics Investigation
- Incident Response Investigation
- Ransomware Readiness Assessment

Restoration

- Post-Incident Rehabilitation

Security Operations Center

- Attack Surface Monitoring
- Managed Detection and Response

Digital Forensics and Incident Response

The Lodestone Digital Forensics and Incident Response (DFIR) team is built to respond to potential and confirmed security events and incidents with the speed and precision necessary to support analysis, containment, and recovery. Our methodology is driven by extensive, real-time threat intelligence gained from our experience responding to thousands of incidents, as well as up-to-the-minute intelligence garnered from other prime sources. When an incident occurs, Lodestone experts provide a thorough analysis of the cause and extent of a breach through the use of advanced tools and techniques in memory, network, and file system forensics. We then work with you to go beyond restarting business operations and expediting recovery by strengthening your security posture and proactively assessing for further threats.

Offensive Security

Lodestone Offensive Services make threat actor tactics, techniques, and procedures (TTPs) work for you by testing your environment against real-world attacks without the risk to your critical data and business flow. Our penetration tests go beyond standard vulnerability assessments with proof-of-concept exploitations of vulnerabilities performed safely by our team of white hats. Lodestone's experts set you up for success by hardening your environment with TTPs seen in the wild, identifying potential security weaknesses, and providing recommendations for remediation. Strengthen your company's security posture from Active Directory to physical security, insider threats, and beyond, including key components of your business such as web applications. We also work with you to put your mind at ease by testing against headline-making cyberattacks like ransomware and phishing.

Security Operations Center

The Security Operations Center (SOC) is the heart of Lodestone's managed detection and response (MDR) services and stands ready to monitor your company's environment for threats 24/7 and 365 days a year. Our experts analyze events and detect potential threats before they become more serious, enabling you to respond quickly and decisively to possible incidents. Lodestone's SOC team can deploy attack surface monitoring and endpoint detection and response (EDR) tools in your environment to gain a broad view and a basis for threat hunting. While monitoring often produces high volumes of data to sift through, we use a security information and incident response (SIEM) system to collect, analyze, and pinpoint the events that are essential to your company's security. We help you defend your business from the inside out, working side-by-side with you to assess situations and devise the best next steps.

GRC - A

Lodestone's Governance, Risk and Compliance Advisory services team delivers cumulative decades of experience in security consulting to give you the advantage when pursuing or maintaining key certifications such as Health Information Portability and Accessibility Act (HIPAA) requirements, Protected Health Information (PHI) requirements, or those set by the Payment Card Industry Security Standards Council (PCI-SSC). Our experts offer everything you need to be proactive about your security in a world where cyberattacks are more common – and devastating – than ever. This includes customized assessments and professional guidance to identify your attack surface, strengthen your security policies, test your readiness, and provide training to your personnel to create layers of defense that protect your business and its critical resources long before a threat actor targets you.

Mission

Lodestone provides cybersecurity through partnership for businesses that recognize the connection between revenue, reputation, and security. We empower our clients to prepare for, detect, and respond to evolving cyber threats and enhance the trust of their customers.

Vision

Lodestone will lead the way to a more secure digital future through knowledge transfer, meaningful collaboration, and intelligent solutions.

Values

- Leadership – We serve as trusted experts that guide our clients through their worst days.
- Common Sense – We value effectiveness and clarity without ambiguity and lengthy processes.
- Agility – We adapt and move quickly in response to challenges.
- Inclusivity – We assemble diverse teams of strong leaders with interdisciplinary expertise.
- Initiative – We empower each other to experiment with new approaches and solutions.
- Balance – We care about each other and know that balance, not burnout, allows us to flourish.

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 foundation 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.

Keeping the world's critical infrastructures safe

We know what keeps senior leaders awake at night and what threat actors are looking for when they attempt to breach the defenses of hospitals, universities, retailers, manufacturers, and government offices, among others.

Actors don't target specific industries but rather specific vulnerabilities. Virtually every industry faces some level of risk. Add to that the nuanced requirements of organizations in securing their operations and information while meeting regulatory compliance — the challenge of protecting valuable assets and reputations can be daunting.

Our technical skills and deep understanding of sector-specific requirements combined with our industry-leading threat intelligence enable us to partner with clients to minimize losses, mitigate risk, control costs, and keep reputations intact.

Healthcare
Securing patient privacy, clinical research, and healthcare infrastructure.

Higher Education
Protecting the institution and its students in an increasingly threatening environment.

Retail
Maintaining high-quality customer service while securing valuable data.

Financial Services
Managing and orchestrating a growing security portfolio as attacks proliferate.

Manufacturing
Protecting and enhancing value with dynamic cyber risk management.

Government & Non-Profit
Protecting critical infrastructure from cyberattack.

For inquiries, contact us.

lodestone.com

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com

What we offer

DFIR

The Lodestone Digital Forensics and Incident Response (DFIR) team is built to respond to potential and confirmed security events and incidents with the speed and precision necessary to support analysis, containment, and recovery. Our methodology is driven by extensive, real-time threat intelligence gained from our experience responding to thousands of incidents, as well as up-to-the-minute intelligence garnered from other prime sources. When an incident occurs, Lodestone experts provide a thorough analysis of the cause and extent of a breach through the use of advanced tools and techniques in memory, network, and file system forensics. We then work with you to go beyond restarting business operations and expediting recovery by strengthening your security posture and proactively assessing for further threats.

Governance, Risk and Compliance Advisory

Lodestone's Governance, Risk and Compliance Advisory services team delivers cumulative decades of experience in security consulting to give you the advantage when pursuing or maintaining key certifications such as Health Information Portability and Accessibility Act (HIPAA) requirements, Protected Health Information (PHI) requirements, or those set by the Payment Card Industry Security Standards Council (PCI-SSC). Our experts offer everything you need to be proactive about your security in a world where cyberattacks are more common – and devastating – than ever. This includes customized assessments and professional guidance to identify your attack surface, strengthen your security policies, test your readiness, and provide training to your personnel to create layers of defense that protect your business and its critical resources long before a threat actor targets you.

Offensive Security

Lodestone Offensive Services make threat actor tactics, techniques, and procedures (TTPs) work for you by testing your environment against real-world attacks without the risk to your critical data and business flow. Our penetration tests go beyond standard vulnerability assessments with proof-of-concept exploitations of vulnerabilities performed safely by our team of white hats. Lodestone's experts set you up for success by hardening your environment with TTPs seen in the wild, identifying potential security weaknesses, and providing recommendations for remediation. Strengthen your company's security posture from Active Directory to physical security, insider threats, and beyond, including key components of your business such as web applications. We also work with you to put your mind at ease by testing against headline-making cyberattacks like ransomware and phishing.

Security Operations Center

The Security Operations Center (SOC) is the heart of Lodestone's managed detection and response (MDR) services and stands ready to monitor your company's environment for threats 24/7 and 365 days a year. Our experts analyze events and detect potential threats before they become more serious, enabling you to respond quickly and decisively to possible incidents. Lodestone's SOC team can deploy attack surface monitoring and endpoint detection and response (EDR) tools in your environment to gain a broad view and a basis for threat hunting. While monitoring often produces high volumes of data to sift through, we use a security information and incident response (SIEM) system to collect, analyze, and pinpoint the events that are essential to your company's security. We help you defend your business from the inside out, working side-by-side with you to assess situations and devise the best next steps.

Digital Forensics and Incident Response

- Assumed Breach Analysis
- Incident Response Investigation
- Digital Forensics Investigation
- Post-Incident Restoration

Governance, Risk and Compliance Advisory

- CIS-18 Gap Analysis
- Tabletop Exercises
- Security Policy Review and Development
- Virtual CISO
- Security Awareness Training
- Incident Response Plan Development

Offensive Security

- Vulnerability Assessment
- Penetration Testing
- Web Application Penetration (WAP) Testing
- Email Hardening Assessment
- AD Hardening Assessment
- Phishing Campaign Assessment
- Red Team Assessment

Security Operations Center

- MDR
- Attack Surface Monitoring
- 15-Day Containment and Monitoring
- 30-Day Containment and Monitoring

About us

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specialized in incident response, digital forensics, offensive security, risk management, and threat detection. Lodestone is a subsidiary of Beazley, an international organization that has been at the forefront of cyber insurance and breach response for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while responding to some of the toughest security challenges that industries face today.

Digital Forensics and Incident Response

- Assumed Breach Analysis
- Incident Response Investigation
- Digital Forensics Investigation
- Post-Incident Restoration

Security Operations Center

- MDR
- Attack Surface Monitoring
- 15-Day Containment and Monitoring
- 30-Day Containment and Monitoring

Offensive Security

- Vulnerability Assessment
- Penetration Testing
- Web Application Penetration (WAP) Testing
- Email Hardening Assessment
- AD Hardening Assessment
- Phishing Campaign Assessment
- Red Team Assessment

Governance, Risk and Compliance Advisory

- CIS-18 Gap Analysis
- Tabletop Exercises
- Security Policy Review and Development
- Virtual CISO
- Security Awareness Training
- Incident Response Plan Development

About us

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection. Lodestone has a unique understanding of the intersection between cyber insurance and cybersecurity while responding to some of the toughest security challenges that industries face today. In other words, we know what insurance providers care about as we offer them expert recommendations on what risk to accept. Being product-agnostic, we focus on practical, actionable solutions that are based on real-world scenarios and modify our services to suit each client's needs.

Digital Forensics and Incident Response

- Assumed Breach Analysis
- Incident Response Investigation
- Digital Forensics Investigation
- Post-Incident Restoration

Governance, Risk and Compliance Advisory

- CIS-18 Gap Analysis
- Tabletop Exercises
- Security Policy Review and Development
- Virtual CISO
- Security Awareness Training
- Incident Response Plan Development

Offensive Security

- Vulnerability Assessment
- Penetration Testing
- Web Application Penetration (WAP) Testing
- Email Hardening Assessment
- AD Hardening Assessment
- Phishing Campaign Assessment
- Red Team Assessment

Security Operations Center

- MDR
- Attack Surface Monitoring
- 15-Day Containment and Monitoring
- 30-Day Containment and Monitoring