Lodestone

SERVICE BRIEF FOR
MANAGED DETECTION AND RESPONSE

Lodestone's MDR service gives organizations all of the advantages of a 24/7/365 SOC without the fees and coordination required to find, train, and maintain top security talent. Our experts work with you to perform custom deployments of monitoring tools within your environment that maximize visibility and reduce the time it takes to respond and recover to potential threats.

We get to know your unique needs and operations to eliminate false positives and reduce the burden of security considerations on your personnel. Our SOC team hunts for threats within your environment and is equipped with the experience and security tools to help you quickly address vulnerabilities and even roll back your environment to a known-good state if an incident does occur.

BENEFITS

- 24/7/365 monitoring with a defined escalation path to your organization that reduces your level of effort to eliminate false positives.
- Reduced detection time and increased detection coverage, meaning fewer chances for threat actors to gain a foothold or exploit a vulnerability in your network.
- Reduced response time so that any threat actor accessing your network has less time to cause damage to your network or exfiltrate data.
- Improved vulnerability management that gives you immediate access to known vulnerabilities in your network and recommendations on how to prioritize and remediate them.
- Reduced chances of a historical threat via threat hunters that constantly search your environment for threat actors may have already gained access before MDR began.
- Mitigation of damage to your business and the ability to contain and remediate threats to minimize negative effects to your environment.
- Reduced recovery times for incidents via security tools that enable our SOC to quickly restore your environment to its last known good state.
- Reduced burden on your personnel with an experienced, external SOC that conducts day-to-day security management without interruptions from off-hours, weekends, sick days, and holidays.
- Obtaining the advantages of a SOC without paying for hiring, training, salaries, or retaining security professionals. Lodestone's software agent licenses also carry over to your company, eliminating the need to independently purchase them.

METHODOLOGY

Lodestone MDR includes gaining a deep understanding of an organization's environment, implementing a symbiotic monitoring solution that minimizes disruption to everyday workflow, and flexible and agile detection and response capabilities for potential threats.

MDR is comprised of these primary phases:

- **Requirements Gathering –** We work with you to determine the types of devices, operating systems, and applications in your environment to ensure that we deploy the best tools to suit your needs in your environment.

- **Rules of Engagement, Escalation Path, and Communication Methods –** We collaborate to set up initial rules, policies and procedures for how you want us to react to alerts and events, which threats can be handled by automation, and which require human intervention before a response is made. We also discuss which of your assets are business-critical and what requires the most protection.

- **Fine Tuning –** We get to know your environment and its unique needs to reduce the need to perform tuning after deployment. We ensure that there are no conflicts between security applications and perfect our configurations so that defense in depth works seamlessly.

- **Provisioning –** We coordinate with you to determine the best time for deployment to minimize impacts on your business flow. Our experts provide software agents to you and walk your personnel through the deployment of those agents, troubleshooting any issues that arise. Agents are then validated to confirm that they are working properly.

- **Tune Alerts with Clients –** We establish normal, expected behavior in your environment to minimize false positives and make true alerts more readily apparent.

- **24/7/365 Monitoring –** We provide continuous monitoring, continuous tuning, and continuous threat hunting. We coordinate actions taken against alerts with you and automate them to reduce alert fatigue after the initial occurrence and strengthen your security posture.

- **Reporting –** We provide ad hoc reporting upon request, as well as monthly reporting, communicated via email that provides a visualization of the previous month's alerts and activities and any outstanding issues. We also provide quarterly reporting, typically via teleconference to review trends and plan for future changes with your key personnel.

DURATION AND DELIVERABLES

Standard MDR is provided as an annual service, but multi-year options are also available. We begin with a few days to a few weeks of preparation for deployment, followed by an approximately two-week tuning phase. Once setup is complete, you receive constant access to our tools, dashboards, and our SOC staff via email and phone.

As part of the engagement, Lodestone will provide some or all of the following:

⬢	**Software Agents –** MDR instances compatible with the operating systems in your environment or environments.
⬢	**Instructions –** Detailed guidance on any security settings that must be made in your environment, such as firewall rules needed to allow for monitoring and reporting and how to whitelist our agents with your existing security devices and appliances.
⬢	**Alerts –** Detailed explanations of triggered alerts via email or phone depending on the severity of the alert and the escalation paths you specify.
⬢	**Monthly Reports –** Summaries of vulnerabilities, alerts, incidents, and trend analysis.
⬢	**Quarterly Meetings –** An avenue for both Lodestone and your organization to discuss upcoming changes (e.g., a cloud migration) and MDR maintenance.

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.