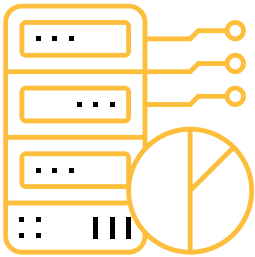


SERVICE BRIEF FOR **INCIDENT RESPONSE INVESTIGATION**



Lodestone's cyber incident response service is designed to help organizations quickly and effectively respond to security incidents, minimize damage, and restore normal business operations. We offer a comprehensive range of services, including incident investigation, threat assessment, containment, remediation, and post-incident analysis. Our team of experts is available 24/7 to provide rapid response and support, ensuring our clients have the best possible chance of minimizing the impact of a cyber-attack.

BENEFITS

- Providing your organization with technical information about the incident to help support any legal reporting, litigation, or cyber insurance considerations.
- The fastest approach to achieve a return to operations while still ensuring a thorough investigation of the incident aligned with business objectives and regulatory concerns.
- Identification of malicious activity and validation that threats and threat actors have been eliminated from your environment.
- Answers surrounding the malicious activity and impact on your environment, ensuring you have the information you need to know the threat has been eliminated and how to protect yourself from future attacks with the same vector.
- Demystification of threat actor tactics, techniques, and procedures (TTPs) and responding to ransomware demands with poise and confidence.
- Weekly updates from forensics experts and a comprehensive report that includes a timeline of the events surrounding the attack. We will work closely with your team to give visibility and answer questions throughout the progression of the incident, which will inform business decisions and provide final findings to support internal and external reporting needs.

METHODOLOGY

Lodestone Incident Response Investigation includes forensically sound evidence collection, expert analysis of evidence sources, clear communication of findings, and an understanding of the incident.

The Incident Response Investigation is comprised of these primary phases:

- **Initial Response** - We work with you to determine the scope of the environment, our initial impressions of the breadth of impact on the environment, business objectives, and steps that have been taken before we arrived to support the incident response.
- **Incident Containment** - We advise on the quickest path to stopping the threat actors from continuing their activity and additional damage being done to your environment. This occurs through the deployment of tooling and configurations with insight from our experts.
- **Mitigation** – We work with you to put controls in place to ensure the containment efforts are bolstered by actions to prevent further disruption during the response and restoration of the environment.
- **Recovery** – We advise you on the recommended actions necessary to restore the environment to not just a pre-incident, but a safer one.
- **Evidence Collection** – We work with you to collect the necessary evidence to complete the analysis and give you the answers you need. We provide several methods for this for ease and to prevent keeping your team from the important work of getting you back up and running. We use industry-standard tools and software and provide all necessary handling steps to address any legal considerations.
- **Investigation**
 - We analyze the evidence* collected to find all available indicators of compromise to achieve the objectives of the engagement.
 - We provide contextualization of the analysis to describe how the attack chain occurred and uncover as much information as possible about the timeline and progression of the incident.
 - We communicate with you to inform you not only of our progress, but also of any significant findings that can either help with intermediate actions or posture for future actions that may be necessary.
 - We provide the most thorough answers possible based on evidence as to how the incident was executed, what the total impact and scope of the incident were, and how to take steps to prevent future recurrence of similar attacks.
- **Reporting** – We provide a written final summary of the investigation with a concise description of the findings and details of the investigation for any historical preservation and reporting requirements you may have.
- **Case Conclusion and the Way Forward** – At the end of the investigation, we provide you with industry general cybersecurity best practices to aid you in moving forward. We remain available to deliver other services to further harden your environment

*Evidence Examples




While the total list of incident evidence items is ever-expanding with new technologies, these are the most common examples of evidence we collect during our investigation phase:

- Physical drives from workstations or servers
- Logical forensic images of workstations or servers
- Copies of security appliance logs (e.g., firewalls, network device management suites, VPN devices, copies of server logs)
- Alert histories from antivirus and endpoint detection solutions
- Threat actors lists of any claims surrounding data exfiltration
- Other sources of evidence as applicable that provide context or support of the investigation

DURATION AND DELIVERABLES

\The Incident Response Investigation varies in duration based on the size of your environment, the number of affected systems, and evidence delivery times, but typically takes four to six weeks. It can be delivered on-premises or remotely.

As part of the engagement, Lodestone will provide any or all of the following upon request:

	Executive Summary Report – A high-level summary report that provides an overview of the ransomware attack, including key findings identified during the investigative process.
	Executive Debrief – An overview of the investigation and key findings presented in person or via video conference with our Case Lead.
	Best Practices Overview – A generalized list of best practices that can help you strengthen your security posture against future attacks.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

©2023 Lodestone

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.