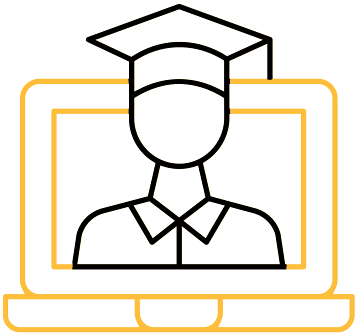
SERVICE BRIEF FOR

ASSUMED BREACH ANALYSIS



Are you worried that the call is coming from inside the house? If your company is concerned that they have already been breached, Lodestone professionals will help you get to the truth of the matter with a forensic investigation of your environment.

Our experts will hunt for evidence of compromise across all in scope systems and report back with insights into your current state of security. Whether we can prove that a security incident has occurred, there is no evidence of a compromise or anything in between; Lodestone is prepared to equip you with the knowledge you need to make your next move.

Lodestone's Assumed Breach Analysis service takes a holistic and widespread look across your organization's entire network to assess any current or historical threats that may be present in your environment. We are prepared to identify indicators of compromise from everything from commodity malware and spyware to nation-state threat actors and advanced ransomware actors.

Lodestone utilizes an easy-to-deploy agent and industry-leading knowledge to quickly search for threats and abnormal activity, as well as poor security practices and potentially unwanted software.

BENEFITS

- Rapidly assess the health of your entire network with expert knowledge on what threats are lurking based on experience gained from hundreds of real-world attack investigations.
- Be ready to pivot to incident response at a moment's notice if an incident is confirmed.
- Obtain recommendations based on findings and years of experience to strengthen the security of your environment.

METHODOLOGY

Assumed Breach Analysis is comprised of these primary phases:

- Preparation – Lodestone works with your personnel to deploy a lightweight agent across all of your organization's endpoints with minimal impact on performance and day-to-day activities.

- Analysis – Our experts run a full suite of artifact collection based on the MITRE ATT&CK framework, searching for evidence of compromise from all stages of the attack lifecycle. We perform deep dives into suspicious activity and assess whether findings represent false positives, evidence of a previous event or incident, or evidence of an active event or incident.

- Reporting and Recommendations – Lodestone professionals create and present to your stakeholders a detailed report of our findings, including any vulnerabilities or areas of particular concern. Recommendations are also provided to maximize the hardening of your environment while minimizing the level of effort needed to make those changes.

DURATION AND DELIVERABLES

The time required for an Assumed Breach Analysis depends upon the size of the environment and the breadth of suspicious activity detected within the environment. This typically takes two weeks from the time of agent deployment across all in-scope endpoints.

As part of the engagement, Lodestone will provide a report that details our methodology, the scope of the environment, and a complete explanation of all threats and risks detected over the course of the analysis, all under the lens of the industry-accepted MITRE ATT&CK framework.

©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.