MORPHISEC

Data Sheet

Incident Response Services

On-Demand Incident Response

Morphisec's on-demand incident response service is designed to assist organizations of all sizes contain, investigate, and remediate a security incident in-progress. The IR team, under the direct supervision of the CTO office, identifies, contains, and reports on security incidents in-progress as well as validating or verifying the lack of a breach.

Lock-Down and Investigate Incidents Quickly

Containment is the first priority for organizations experiencing a cyber-attack in order to minimize damage to the business. A specialized team with a skill set and experience in handling these critical situations is required for quick containment and rapid business recovery. They will leverage Morphisec's zero trust at runtime solution, which enables the IR team to quickly pinpoint and contain the threat.

Following containment, it is critical to gain an understanding of the root cause of the incident and, in turn, the required corrective actions to improve current tools and processes. Morphisec's IR teams assist organizations under attack to quickly contain the incident, ensuring business continuity, and minimize direct and indirect losses. They also identify and report on the root cause of the event, and will even provide assistance to validate or verify the lack of a breach.

At Morphisec we believe in rapid containment and prevention. Our aim is to provide immediate results even before forensic activities are finalized. During this time of uncertainty and a rapidly changing threat landscape, it is important that all businesses, even those without dedicated security professionals, have access to the expertise required to keep their businesses up and running in the event of a breach.

Deliverables

Executive Report and Technical Report with corrective actions to address any gaps in tools and processes.

Executive Report

High-level summary explaining the timing, investigative process, major findings, and containment/ eradication activities.

Technical Report

A detailed report highlighting the TTPs of the attack along with timelines and affected devices and suggested corrective actions to address the gaps in the environment.

Morphisec Incident Response Service Benefits

Experience and Expertise

Morphisec's team of experts has experience in analyzing, reversing, and fighting against the most complex cyber-attacks.

Technology

Leverage the scale and efficiency of Morphisec's threat hunting and containment agent to quickly protect your assets from backdoors and persistentent malware.

Malware Analysis

Constant analyses and investigation of the most harmful and sophisticated attacks from vast Morphisec deployments help our experts correlate, attribute, and identify root causes and TTPs of adversary groups.

Morphisec incident responders analyzed numerous human-operated ransomware attack chains all across the globe. They have helped customers to contain dozens of breaches, identify exploited vulnerabilities, find indicators for exploited supply chains, identify IP theft, and more.

The Morphisec IR Team for Incident Response services process includes:

- Deploying of containment agent within the compromised environment
- Forensic collection and investigation of affected assets, including the building of an activity timeline, supplying indicators of compromise (IOCs), scoping the impact, mapping of exfiltrated IP, and more.
- Malware analysis: In-depth analysis of a given malware, backdoor, or fileless code, to identify the potential impact.
- Working around the clock during the investigation, with availability whenever we're needed
- Executive report: Morphisec will provide a high-level report that will summarize the major findings and provide recommendations on remediation steps
- Forensics report: Detailed forensics report that includes IOCs, timeline, affected assets, and specific recommendations for mitigation.
- The option to develop customized scripts to minimize follow-up impact.

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Cipla, Citizens Medical Center, and many more. Learn more at www.morphisec.com