Developing an effective way to deal with a persistent adversary or sophisticated criminal can be a daunting challenge for any organization, whether in the public or private sector. Many organizations find it difficult to keep pace with the rapidly changing cyber threat landscape. In order to meet and beat this challenge, a highly specialized expertise is required.

Cybersecurity Operations Service is a cybersecurity service offering for organizations who are looking to understand and reduce their exposure to the risks posed by today's targeted attacks from determined human adversaries and sophisticated criminal organizations. It is a proactive, discrete service that involves a team of highly specialized Microsoft resources providing analysis for one week for a fixed-fee. The service is, in effect, an incident response prior to an actual emergency.

Cybersecurity Operations Service is delivered by the same team of individuals who respond to cybersecurity incident response situations worldwide – the Microsoft Detection and Response team. Malware analysis, reverse engineering, tailored cyber threat intelligence, and the ability to create discreet, custom scanners suitable for high-value servers and endpoints provide a robust security assessment of your environment. With this Service, the Detection and Response team will provide the strategic guidance needed in order to properly harden environments against advanced and persistent attacks.
Microsoft’s experienced incident response professionals provide proactive diagnoses and potential mitigations before an unplanned emergency response is required by the customer.

Cybersecurity has become a crucial business risk that must be prioritized and actively addressed by all organizations today.

Overlooking a single security threat can create a serious event that could severely erode community and consumer confidence, can tarnish reputation and brand, negatively impact corporate valuations, provide competitors with an advantage, and create unwanted scrutiny.

Microsoft works with customers globally to identify risks and provide proactive solutions to help our customers manage their cyber risk especially in today’s dynamic threat environment.

How the Offering Works

Cybersecurity Operations Service is delivered by a team of four to five experienced Microsoft Incident Responders that perform analyses on selected high-value servers and endpoints. Leveraging a secure, dedicated Azure workspace to perform the investigation, the service will be remotely backed by the Detection and Response team’s hunting, reverse engineering, and forensic capabilities.

The team utilizes a proven toolset that leverages custom Microsoft capabilities including specialized detection tools, malware analysis, signature generation, and custom cyber intelligence for signs of advanced implants not typically found by commodity anti-virus or intrusion detection system technologies.

• Provides proactive analysis by incident response experts prior to detection of an emergency;
• Conducted by the same experienced Microsoft resources who help stop and mitigate attacks worldwide;
• Leverages Microsoft proprietary capabilities around Malware analysis, reverse engineering, tailored cyber threat intelligence, and the knowledge of how to create discreet, custom scanners;
• Suitable for IT operational scenarios involving high-value servers and endpoints used by executives or critical personnel; and
• Provides a unique understand of what adversaries are presently doing and what defenses are currently working in the real world.

Period of Performance & Outcome

Typical period of performance is one work-week, but this can be customized for large customers with multiple geographic sites or organizational components. Findings will be provided in the form of an outbrief presentation. All reports generated through the course of the engagement, including a Power BI dashboard to visualize and provide drill through capabilities, will be provided at the conclusion of the engagement.

Seasoned Expertise

Microsoft is a worldwide leader in providing IT products and solutions to both the public and private sectors. Microsoft has led the industry in key security initiatives such as the Trustworthy Computing initiative, the Security Development Lifecycle, botnet takedowns, and the Microsoft Windows Defender Security Intelligence. The Microsoft Services Cybersecurity Team is comprised of senior IT and IT Security leaders and experts with extensive experience in both the private sector and government. The Cybersecurity Operations Service is delivered by experienced cybersecurity professionals who devote 100% of their time to providing cybersecurity solutions to Microsoft and Microsoft’s customers worldwide.