**Microsoft**

# Cybersecurity Operations Service (COS)

## Assess

### Protect your investments, people, and reputation.

*Leverage Microsoft's incident response professionals for proactive investigation, and to perform an end-to-end review of your Windows environment.*

*Microsoft's Cybersecurity Operations Service is utilized globally by leading defense, government, and commercial entities to help secure their most sensitive, critical environments.*

#### Duration
*Starting at one week*

#### Outcome
*Findings will be provided in the form of an outbrief presentation, including a Power BI dashboard to visualize and provide drill through capabilities.*
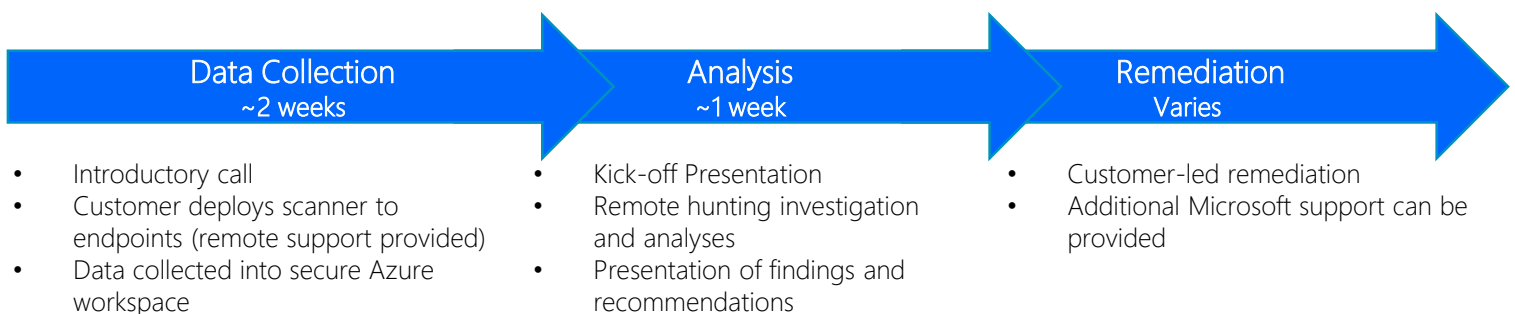
# Overview

Developing an effective way to deal with a persistent adversary or sophisticated criminal can be a daunting challenge for any organization. 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 skillset is required.

Cybersecurity Operations Service (COS) is a service offering for organizations that 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, discreet service that involves a global team of highly specialized resources providing remote analysis for a fixed-fee. This service is, in effect, a proactive approach to identifying emergencies before they occur.

COS is delivered by the Microsoft Detection and Response Team, the same team of individuals who respond to cybersecurity incident response situations globally. This robust security assessment is comprised of forensic analysis, reverse engineering, tailored cyber threat intelligence, and proprietary scanners suitable for high-value servers and endpoints. With COS, the Detection and Response Team will provide strategic guidance and recommendations to harden your environment against advanced and persistent threats.

## How the Offering Works
COS is delivered by a remote team of experienced Microsoft incident responders that perform analyses across your Windows estate. The team will provide a secure, dedicated Azure workspace to perform the investigation and will partner with your organization to assist in deploying scanners across your environment. Scanners will be provided by the COS team.

| Data Collection ~2 weeks | Analysis ~1 week | Remediation Varies |
|---|---|---|
| • Introductory call<br>• Customer deploys scanner to endpoints (remote support provided)<br>• Data collected into secure Azure workspace | • Kick-off Presentation<br>• Remote hunting investigation and analyses<br>• Presentation of findings and recommendations | • Customer-led remediation<br>• Additional Microsoft support can be provided |

# Solution Details

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, 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.*

## Scope
*All currently supported Microsoft operating systems are in scope for this engagement.*

## Primary Advantages
- Conducted by the same experienced Microsoft resources who help stop and mitigate attacks worldwide;
- Provides proactive analysis by incident response experts prior to detection of an emergency;
- Leverages Microsoft proprietary capabilities around Malware analysis, reverse engineering, tailored cyber threat intelligence, and the knowledge of how to create discreet, custom scanners;
- Provides a unique understanding of what adversaries are presently doing and what defenses are currently working in the real world.

## Why Microsoft
- Significant investments in cybersecurity – over $1 billion per year as of 2017 and  $15 billion invested in Microsoft cloud infrastructure
- One of the largest threat intelligence networks globally, with 22+ years of experience in cloud services:
    - 450B authentications per month across all cloud services
    - 400B emails analyzed for malware and malicious sites
    - 18B+ Bing web-page scans per month
    - 1B+ Windows devices updated monthly
    - More than $1B invested each year on security
    - More than 70 million Office 365 commercial monthly active users
- Agentless scanners designed for easily deployed, non-disruptive analysis
- Direct access to product development teams utilizing Microsoft's latest security and identity products and capabilities
- Delivered by a global team of experienced cybersecurity professionals, who devote 100% of their time to providing cybersecurity investigative services to Microsoft enterprise customers worldwide

Microsoft is a worldwide leader in providing IT products and solutions to both the public and private sectors - leading the industry in key security initiatives such as Trustworthy Computing, the Security Development Lifecycle, botnet takedowns, and the Windows Defender Security Intelligence group. The Microsoft Services Detection and Response 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 employs a highly skilled, diverse group of resources to defend the world's largest enterprise organizations in the fight against cybercrime.

For more information, visit //aka.ms/cyberoperationsservice