Persistent Adversary Detection Service

Leverage Microsoft's incident response professionals for proactive investigation

Microsoft's experienced incident response professionals can help investigate suspicious events to provide a diagnosis and potential mitigations before an unplanned emergency response is required.

Key Benefits

- Proactive analysis by incident response experts before an emergency occurs.
- Leverages Microsoft proprietary capabilities and the same experienced consultants who help stop and mitigate attacks worldwide.
- Malware analysis, reverse engineering, tailored cyber threat intelligence, and the ability to create discreet, custom scanners.
- Suitable for high-value servers and endpoints used by executives or critical personnel.
- Strategic guidance to harden against advanced and persistent attacks.
- Understand what leading adversaries are presently doing and what defenses are currently working in the real world.
- An outbriefing will be provided detailing the team's findings and recommendations to strengthen your environment and help disrupt attackers.

Overview

Persistent Adversary Detection Service (PADS) is a service offering for proactive clients who are looking to reduce the risk posed by today's targeted attacks from determined human adversaries and sophisticated criminal organizations.

The service is in effect a proactive, discreet incident response prior to an actual emergency and examines high value assets or a sample of systems for signs of advanced implants not typically found by commodity anti-virus or intrusion detection system technologies.

How the Offering Works

A team of Microsoft consultants travel to your location and perform the analysis on selected high-value servers or endpoints. The team utilizes a proven toolset that leverages custom Microsoft capabilities including specialized detection tools, malware analysis, signature generation, and custom cyber intelligence. Typical period of performance is one work week your location, but can be customized for large clients with multiple geographic sites or organizational components.

Microsoft PADS complements other proactive offerings which aim to reduce the risk posed by advanced actors before a crisis occurs.

Microsoft's PADS service has been utilized by leading defense, government, and commercial entities to help secure their most sensitive, critical environments.

PADS personnel have all undergone background checks and possess appropriate government security clearances.

Leverage our Experience

Many corporate information security teams only infrequently experience a major intrusion, especially targeted attacks by a determined human adversary. The Microsoft PADS team routinely investigates attacks of this nature and can bring in seasoned consultants to quickly supplement the existing skills of the team.

- Benefit from experienced, highly skilled responders
- Unsurpassed capabilities assessing Microsoft technologies
- Malware analysis and reverse engineering capabilities

From the Front Lines

Determined, sophisticated adversaries regularly change and modify their tools, tactics, and procedures (TTPs) to defeat organizational defenses. Microsoft's PADS team is uniquely positioned to see the most current attacks across the Windows platform worldwide and also understands how actors evolve over time. Such experience can be more powerful that any signature or tools-based approach.

- Know what the leading adversaries are currently doing
- Gain access to Microsoft's extended global security resources

Understand what Works in the Real World

The Microsoft PADS team is composed of seasoned incident responders who regularly investigate reactive intrusions. During these engagements, the team routinely encounters various defensive strategies – some more effective than others. The team understands what is currently effective for combatting current threats and can advise on what would be helpful in the event of an actual emergency response before one is necessary.

- Help identify deficiencies in key capabilities prior to an actual event
- Understand what defenses are effective against current threats

*For more information about Consulting and Support solutions from Microsoft, contact your Microsoft Services representative or visit **www.microsoft.com/services***

This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.