avanade

G-Cloud 14

Avanade Managed Security Services - **MXDR**

March 24

Table of Contents

1. Scope of Services

Avanade understands that organisations face a number of key challenges around security and risk functions supporting the achievement of business objectives. Threats are growing and becoming more sophisticated, business models are continuously evolving, and regulatory requirements are increasing along. We have formed a market-leading Security Practice offering the services to help organisations address all of their security needs.

Our Managed Security Services (MSS) provide organisations with the ability to rapidly scale security and compliance operations. MSS supports the digital enterprise by providing innovative technologies, top security talent, and an operating model that is designed to provide measurable business outcomes.

It provides integrated end-to-end security services for large enterprise clients at the global and regional levels. Our unique approach is based on consulting led transformation for optimised and high performing security operations aligned to our client's respective industries.

2. Approach

We provide end to end security operations center services, which utilize the latest Extended Detection and Response capabilities from Microsoft to detect, protect and respond to cyber-risks, helping to ensure the continuity of your business and avoiding disruption.

Maturity	Focus areas
Foundational: **Core Security + Monitoring**	• Core Security Compliance • Cyber Awareness & Training • Vulnerability Management • SIEM Integration • Defender AV - Endpoint Security
Modernised: **SOC > MXDR**	• Incident Response • Identity Protection Detection & Response • Defender for Endpoint Detection & Response • Network Detection & Response • Defender for Office – Advanced Anti Phishing & Email Protection
Optimised: **Automation and Analytics**	• C-Level Dashboards • User and Entity Behaviour Analytics • Threat Hunting • Automated Response Playbooks • Threat Intelligence
Leading: **AI Powered Predictive Security**	• Adversary Deception • Attack Path Analysis • Defensive AI powered by Security Copilot • Adversary Simulation & Tabletop Exercises • Enhanced Threat Intelligence

3. Assets & Tools

Core Service Capability	Description
Security Monitoring & Incident Response (L1, L2)	▪ Security Event Monitoring & Incident Handling on a 24x7 basis ▪ Maintenance of use cases / Log Source Tracking ▪ Service Review & Reporting ▪ Sentinel Management and Evolution
Advanced Threat Protection	▪ Correlation with other monitored security alerts and activity ▪ Analysis & recommendations ▪ Service Review & Reporting
FIM & DLP	▪ Manage file integrity monitoring configuration policies and fine tuning ▪ Correlation with other monitored security alerts and activity ▪ Analysis & recommendations
Vulnerability management	▪ Perform scheduled vulnerability scanning of assets. ▪ Configuration for vulnerability scans ▪ Service review & reporting ▪ Vulnerability remediation tracking
Threat Intelligence	Integration of external Threat Intelligence information and provision of Threat Intelligence portal to enhance cyber awareness
Threat Hunting	Scheduled and ad-hoc Threat hunting activities to help us to identify latent risks and to build familiarity with your network.
Digital Forensics & Incident Response	Proactive activities including • Threat Assessment • Incident Response Plans • Ransomware and Major Incident Playbooks • Table-top exercises • Purple Team exercises • Bespoke support Reactive activities including: • Technical Incident Response • Crisis Management • Engagement Management / Engineering • Executive Breach Coaching

Platform Management for Azure Security Tooling	• Sentinel
	• Defender XDR
	  ○ Defender for Cloud
	  ○ Defender for Cloud Apps
	  ○ Defender for Endpoint
	  ○ Defender for Identity
	• Purview

avanade

	• Entra ID

4. Pricing

5. Contacts

Name	Title	Email	Phone
Paul Marsh	Head of Avanade UK Health & Public Services	uk.hps.support@avanade.com	+44 20 7025 1000

6. About Avanade

Avanade, a joint venture between Accenture and Microsoft, is a privately held company was founded in 2000 with the goal of delivering innovative services and solutions to enterprises worldwide using the Microsoft platform. Avanade's main business focus is to purely deliver innovative services and solutions to enterprises worldwide on Microsoft technology. Avanade is a global organisation with over 56,000+ professionals worldwide, serving our clients in major geographic business areas in 26 countries.

This vast network of highly skilled resources is further complemented by our network of delivery centres that we refer to as Advanced Technology Centres (ATCs). This complementary capability provides the agility, cost efficiency and diversity of skills that today's businesses demand. This construct underpins the results we generate for our clients and forms the foundation for our long-term relationships with them.