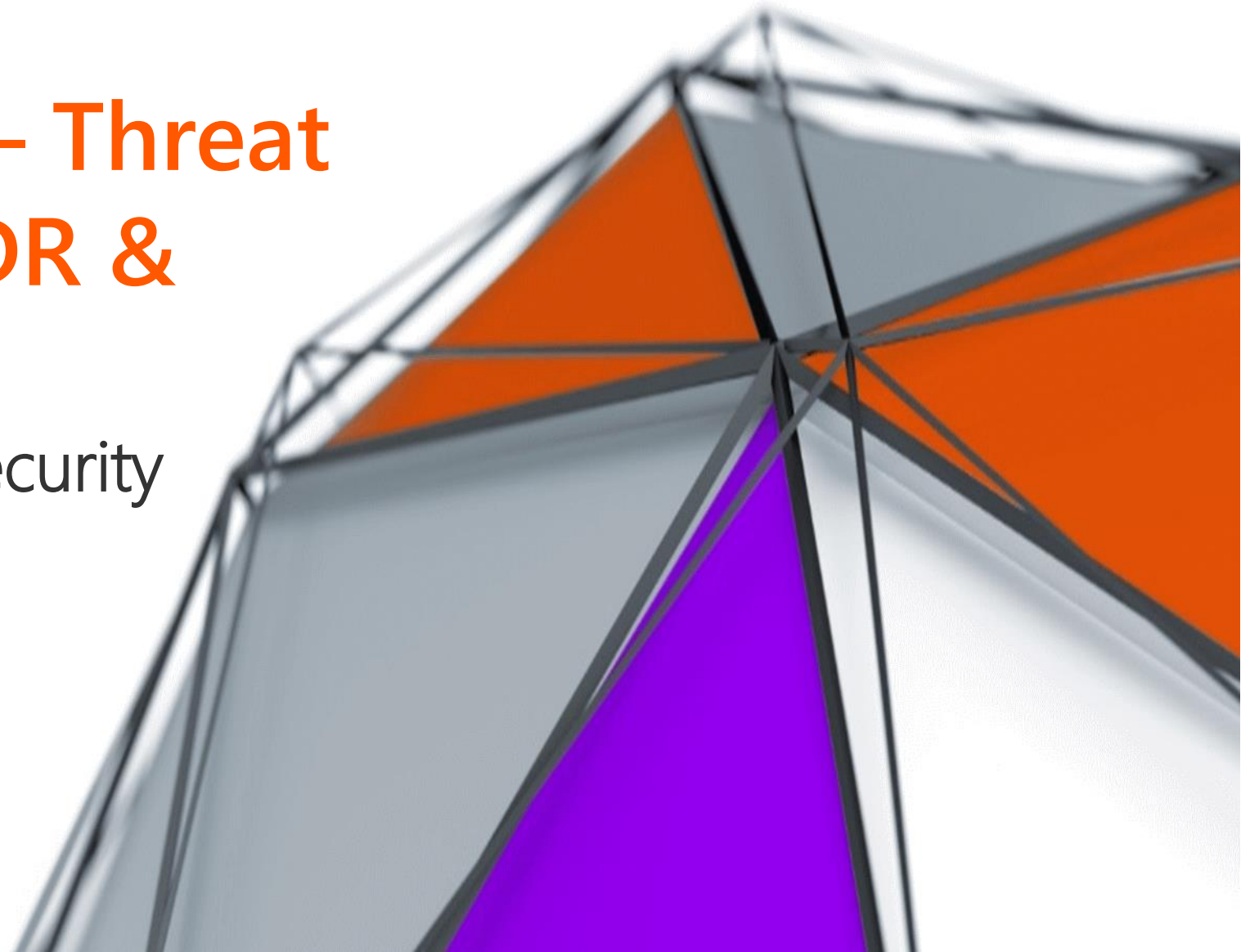




Avanade Security – Threat Protection with XDR & SIEM

Accelerate our Microsoft Security Business Together

January 2024



Sales Play: Threat Protection with XDR & SIEM

Why now?

In the last year, accelerated digital transformation has outpaced security. Organizations are facing a growing and constantly evolving security threat.

- The attack surface has increased
- Hybrid remote working is exposing organizations
- Platforms are susceptible
- Microsoft security and platform capability has never been stronger

Our Differentiated Services

- **MDR across the Microsoft Platform & Hybrid environments** – continuous security monitoring, detection and response in partnership with Microsoft. Cost effective security monitoring at scale using Sentinel SIEM providing advanced analytics and automated response to threats. Avanade are an approved MXDR partner.
- **Build & manage Microsoft Sentinel** – we help clients to onboard and connect services to Microsoft Sentinel to protect, detect, and respond to threats for the entire Microsoft Platform and extended security landscape
- **Microsoft Co-pilot for Security Integration** - Assess readiness for organisation, pilot Security co-Pilot, upskill your existing security champions
- **Managed Cloud & Infrastructure Security** - Leverage managed cloud security to operate cost-effectively and securely at scale.



46% of Global 500 companies as clients



Security CoPilot Advisory Council Member



100+ Microsoft Partner of the Year awards, including Microsoft Global Alliance SI Partner of the Year for the 17th time



2x

Microsoft Security **Winner** as "Zero Trust Champion – SI" (2024 & 2024)

Winner: Microsoft Entra Partner Excellence award in the 'External Identities' category (2024)

The business outcomes we drive

- **Protect against advanced threats** and attacks and leverage the power of the Microsoft's advanced cybersecurity capabilities such as automated remediation and predictive threat intelligence. This enables clients to optimize their SOC.
- **Provide additional security and visibility** for recently deployed services and infrastructure. A key focus is protecting endpoints from Ransomware.
- **Augment the Cybersoc team's capability** with advanced analysis to prioritise on the right issues
- **Assess and mitigate potential vulnerabilities** that the client isn't aware of within their environment. Enable Secure Collaboration and prevent phishing.
- **Runbooks and use cases built dynamically** based on clients business context and priorities

MXDR across the Microsoft Platform & Hybrid environments

Managed Extended Detection & Response Overview

To truly defend your organization against cyber-attacks, you need to prepare for threats – both known and unknown – and ensure continuity in the face of disruption.

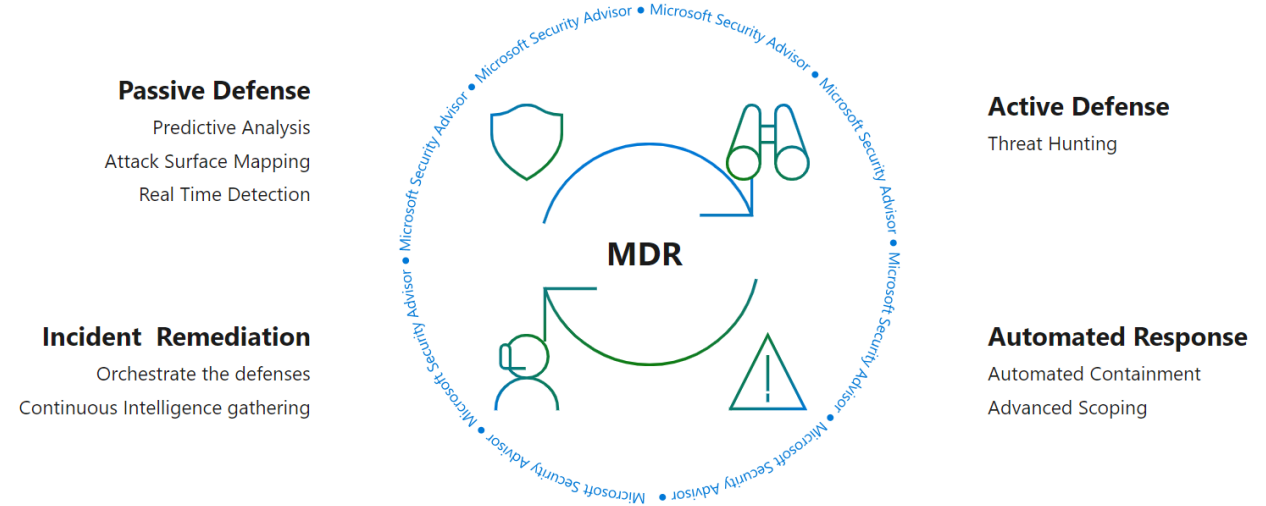
- Microsoft Sentinel, a modern SIEM for entire Microsoft platform and extended security ecosystem covering modern workplace, digital platforms and cloud.
- Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Client Outcomes

- Modernize your Security Operations Center (SOC)
- Unify security posture across your entire IT infrastructure , Reduce downtime, exposure, and risks
- Modernize customers SOC moving away from point solutions and tradition log ingestion
- Enable a customer to inventory, assess, and respond to ransomware across all types of Endpoint devices
- Providing secure collaboration in O365, Teams, and M365 Apps and prevent phishing

Case Study : Requirement for 24*7 SOC Monitoring and Managed Security Operations including Incident response

- Provide client with a dedicated 24/7/365 Managed Extended Detection and Response (MXDR) service that provides L1 and L2 security monitoring, Threat Hunting, and Incident Response support services and escalation of complex security incidents to Microsoft L3. This managed service will be performed remotely from Avanade/Avanade delivery centre with an onshore SDM from Avanade.



Technology in scope

- Defender for Cloud
- Microsoft Sentinel
- Microsoft 365 Defender

Results :

- Provided the capability to proactively identify and respond quickly to threats, mitigate damage
- Proactively support incident investigation and response
- Microsoft Sentinel
- M365/Defender for Cloud dashboards
- M365 Defender Suite
- Defender for Cloud Suite

Build & manage Microsoft Sentinel

Enhance and Optimize your Enterprise Security with Microsoft Sentinel

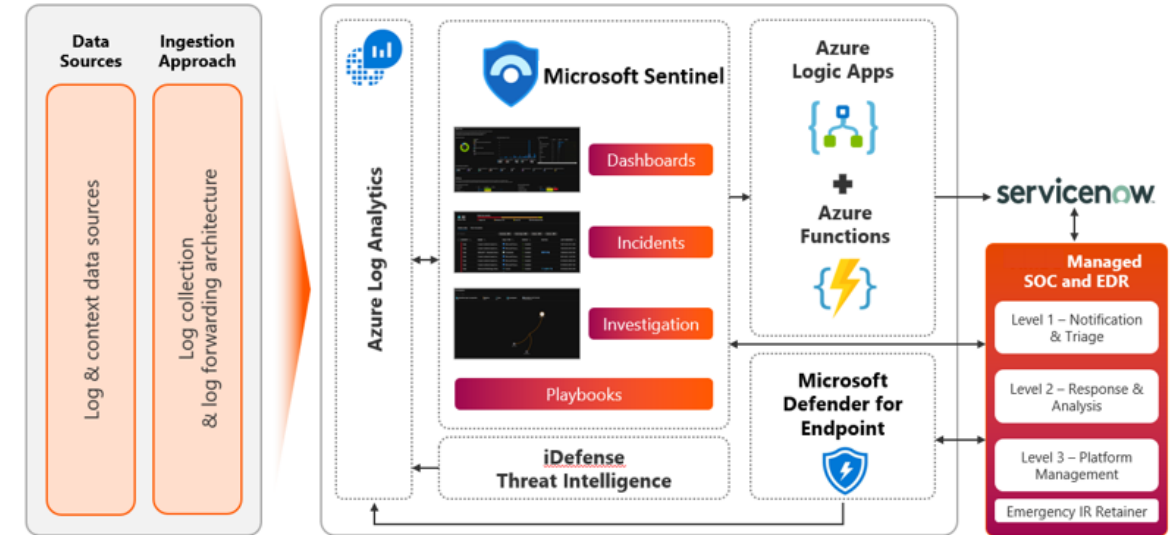
- To truly defend your organization against cyber-attacks, you need to prepare for threats – both known and unknown – and ensure continuity in the face of disruption.
- Microsoft Sentinel is a modern, scalable, cloud-native, SIEM and SOAR solution to protect-detect-respond for the entire enterprise including Microsoft platform and extended infrastructure, both on-premises and in multiple clouds.
- We integrate off-the-shelf Microsoft tools and ecosystem and all third-party security sources for comprehensive SOC monitoring on the cloud.

Client Outcomes

- Cost effective security monitoring at scale using Azure Sentinel SIEM providing advanced analytics and automated response to threats
- Provide setup, ongoing monitoring, response and managed service for customers using Sentinel as their SIEM of choice
- 20-40% run operations cost savings vs. legacy approach
- 50% average time reduction for SIEM go-live operations

Case Study : Enhanced experience and increased security

- We supported the client to become the best-connected in a secure way by providing continuous security monitoring and incident response services leveraging the Microsoft Sentinel platform.
- SOC Monitoring: Avanade delivers 24*7 monitoring services to support in the detection and response to Security incidents.
- Delivered engineering services focused on use case development leveraging our Sentinel Use Case Library.



Results :

- We support the client by continuously monitoring the IT infrastructure. Also by providing best practice use cases and runbooks. Together, we have implemented +100 use cases. The data ingestion in the platform is +1000GB per day resulting from a growing set of data sources including: Microsoft data sources (Defender for endpoint, identity and office, Defender for Cloud Apps), Firewall log sources and Symantec AV.
- With the client team we work in a collaborative, agile way. The client knows our analysts and engineers and we are working together to keep everyone happy.

Microsoft Security Co-Pilot Integration

End-to-end defense at machine speed and scale

To truly defend your organization against cyber-attacks, you need to prepare for threats – both known and unknown – and ensure continuity in the face of disruption.

- Microsoft Sentinel is a modern, scalable, cloud-native, SIEM and SOAR solution to protect-detect-respond for the entire enterprise including Microsoft platform and extended infrastructure, both on-premises and in multiple clouds.
- We integrate off-the-shelf Microsoft tools and ecosystem and all third-party security sources for comprehensive SOC monitoring on the cloud.
- As an adopter and builder of AI technology, we have the necessary tools, knowledge and foundation to help our clients rapidly and responsibly modernize security operations with our Security Copilot rapid deployment approach.

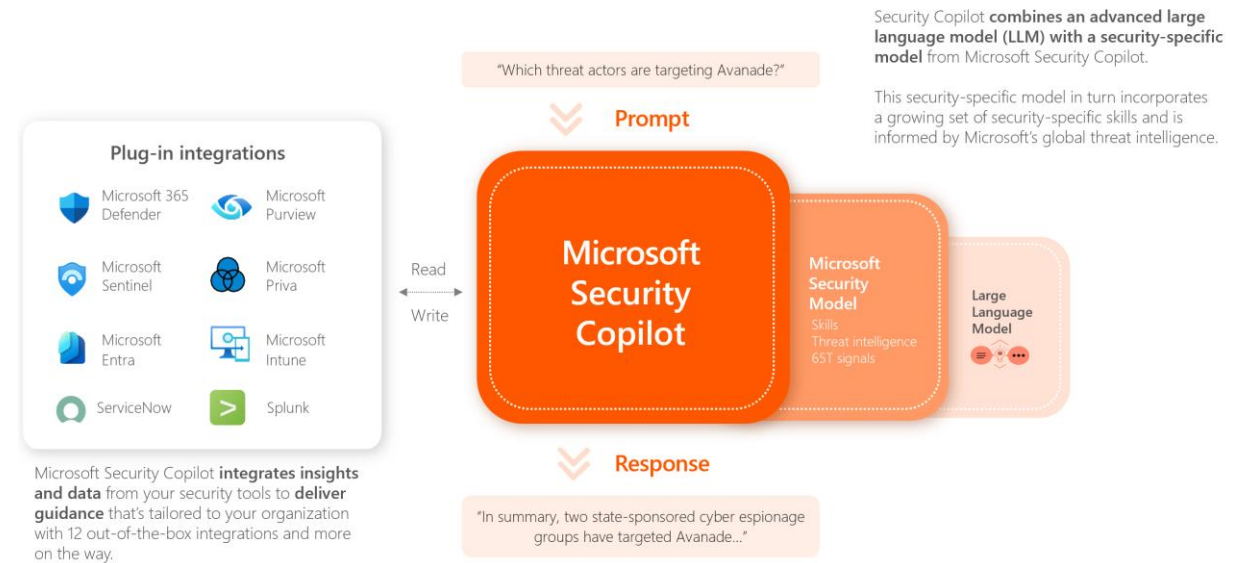
Client focus & outcomes

- Avanade will join your team on-site (or remote) to go in-depth on the business value of Security Copilot as well as an overview of the capabilities Microsoft can bring. We'll then workshop to identify the business scenario that drives the most benefit and provide a comprehensive product/tool enablement.
- Important focus areas: Security remediation Process optimization, Security threat hunting efficiency, Automation to scale security operations, Security Platform Maturity

Case Study : Avanade is the only company on both the partner and customer private preview for Security Copilot. We use it ourselves and we bake it into what we bring to our clients.

Real-world experience

- Avanade shares information between our internal security operations team and our client facing organization, bringing together resources to help improve and make the most of Microsoft's technology internally, then leveraging those lessons learned with our clients.



Starting with a blank sheet

- Security Copilot can drastically help analysts draft Kusto Query Language (KQL) to meet their needs or help provide a draft incident summary based on relevant data. Rather than starting with a blank slate or performing an internet search, describe what you're looking for in plain language. The results will help you get started and aid your learning of what's possible.

Lessen the talent gap

- Finding, training and retaining good security analysts is hard. Security copilot has the potential to close the talent gap. It doesn't replace the need for quality mentorship and experience, but it can help your team scale and get more junior analysts up to speed faster.

Managed Cloud & Infrastructure Security Services

Detect and respond to advanced cyber attacks across the environment.

- Make informed security decisions with Microsoft's unique global threat intelligence and growing set of security skills informed by more than 65 trillion daily signals.
- Make informed security decisions with Microsoft's unique global threat intelligence and growing set of security skills informed by more than 65 trillion daily signals.

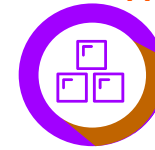
Client Outcomes

- Comprehensive MSS capabilities that grow with the business and allow visibility across client's environment
- Effective and efficient real-time protection against threats across the industry and geography
- Matured service operating model for integrated processes
- Continuous improvement and innovation across cybersecurity services, low-risk, zero-disruption transition
- Measurable and flexible operations, scalable delivery model

Case Study : Azure Managed Security Services focuses on key services

- Client is a large UK Energy provider who had invested in a new Cloud Infrastructure but also wanted to put service monitoring in place.
- Having a managed service was aligned with their cloud strategy and seen as an alternative to having their own datacentre and managing it.

What we hear from our Clients



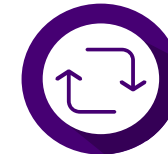
Cloud Native Integration

Ensure Proper integration and configuration of Cloud –native Security tools into Security Operations



Manage Continuous Compliance

Meet Regulatory and Compliance requirements with clear understanding of Shared security responsibility



Visibility of Dynamic Workloads

Get visibility into cloud activities and manage risk through automated controls there by protecting dynamic workloads




Shadow IT

Identify Shadow IT and prevent data leakage through unsanctioned apps

Results :

- The client moved its sensitive data and applications into the cloud and leverages the Microsoft Azure platform for secure access and document management.
- A dedicated support service based nearshore to the client was setup to provide infrastructure support for the Azure infra and Security Cloud service
- Within the managed service the team focused on the main infrastructure, a separate team focused on continuous improvement, reducing overhead of simple tasks

Avanade Global Team – Who to contact

Region	 avanade
Global	Rajiv Sagar Rajiv.Sagar@Avanade.com
APAC	Anand Manoharan anand.a.manoharan@avanade.com
EU	David Adde David.Adde@Avanade.com
NA	Justin Haney Justin.Haney@avanade.com
LATAM	Anand Manoharan anand.a.manoharan@avanade.com
