KPMG Microsoft Sentinel Accelerator

Enable best practice security and compliance with a single pane of glass via Microsoft Sentinel.

The challenge

The digital environment leaves us all exposed. Not only can it disrupt business operations, but it can cause significant financial and reputational damage.

Microsoft Sentinel offers broad functionality for security monitoring and automation opportunities to allow organisations to centralise security information and incident management, and achieve incident handling efficiencies. However given the breadth and depth of the tool, many organisations are daunted by the complexity of configuring and customising the necessary security use cases critical to their business.

Key Benefits

Utilise security features with a powerful SIEM built on the cloud, and enriched by AI.

Maximise time-to-value with KPMG's pre-configured assets to protect your hybrid, multi-cloud, multi-platform business.

Gain visibility of your organisation's security posture across your entire enterprise with intelligent security analytics.

Centralise alerts through a single pane of glass with a unified security operations platform.

Detect and disrupt threats in near real-time to streamline investigation and response with our playbooks.

The KPMG solution

KPMG's Microsoft Sentinel Accelerator offering is designed to help organisations establish a comprehensive, industry specific best practice solution that takes your security and compliance to the next level.

Our Accelerator offering uses pre-configured assets, delivery by our multi-disciplinary team of cyber professionals, to help you quickly deploy Sentinel and maximise your ROI when you are:

- Deploying Sentinel for the first time;
- Unlock additional value from your existing Microsoft Azure and Sentinel investments; and
- Looking to increase efficiencies in your security posture, reporting, threat detection and incident response.

Our approach

Scope
Gather & define SIEM and XDR requirements.

Customise
Discover & tailor use cases for your multi-cloud, multi-platform environment.

Define
Establish baseline & architecture configuration for deployment.

Activate
Implement Sentinel solution for end-to-end visibility across your resources.

Enable best practice security & compliance

Based on your environment, compliance and regulatory requirements, we can help you deploy these pre-configured assets to Microsoft Sentinel to have you onboarded and detecting threats in as little as 30-days.

Our cloud security professionals will also help you customise use cases, develop custom data connectors and additional assets.

We provide:

Policy Initiatives	Pre-configured for key regulatory requirements & industry standards, including but not limited to: Regulatory requirements: • CPS 234 (Australia) • MAS TRG (Singapore) • FISC (Japan) Industry standards: • ISO 27001 • NIST • PCI DSS
Threat-based Rules & Queries	To identify and detect suspicious activities across various stages of the MITRE attack framework, including but not limited to: • DDoS • Bruteforce • Vulnerability Exploitation • Ransomware • Data Breach • Command and Control • Business Email Compromise
Automation Playbooks	Enable automation of notifications about suspicious activities in near real time and provision of recommendations to mitigate gaps. We will leverage the power of AI by integrating it with the solution to derive further efficiencies, specific to your environment.
Workflow Automation with ServiceNow	Integrate with Sentinel by creating an ITSM profile to enable data flows, synchronisation and validation.
Sentinel Workbooks (Dashboards)	Single, centralised platform to evaluate key threat vectors relevant to your organisation, and understand your security posture against regulatory requirements and industry standards.

Why KPMG?

Our approach to cloud security emphasises integration. Successful cloud security implementation is inherently multi-disciplinary – so we combine architecture, engineering, operations, business and IT skillsets to deliver secure and compliant cloud transformation.

We are a Global Microsoft partner with specialisations across 12+ areas and have received partner recognition from Microsoft at global and local levels. Our expert pool includes over 4,000 certified professionals in cloud security with 1,000+ certifications in Microsoft Azure.

The KPMG Microsoft Alliance

Together we have the capacity and capability to achieve valuable business insights, make smarter decisions faster, and quickly adapt to change – while also managing risk, compliance and security for you.

Contact

Ross Widdows
Microsoft Cyber,
Lead Partner
rosswiddows@kpmg.com.au

Christie Chan
Microsoft Cyber Lead
cchan33@kpmg.com.au

kpmg.com.au/socialmedia
kpmg.com.au

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.