



Microsoft Sentinel Accelerator

Establish a Gold Standard Security and Compliance solution on Microsoft Cloud

Capitalise on KPMG’s rich library of Sentinel and Compliance assets to build a Microsoft Sentinel service that delivers near real time threat detection, workflow automation for response, compliance monitoring and management, and centralised pane of visibility and orchestration.

Introduction

Microsoft Sentinel offers broad functionality for security monitoring and automation opportunities to allow organisations to centralise security information and incident management, and realise better incident handling efficiencies. However given the comprehensiveness of the tool, many organisations are daunted by the complexity in configuring all the necessary security features relevant to their business.

KPMG’s Microsoft Sentinel Accelerator service is designed to help organisations establish a comprehensive, industry specific best practice solution that takes their security and compliance posture in Microsoft Cloud to the next level.

Our accelerator service uses pre-configured assets, delivered by our multi-disciplinary team of Cyber professionals, can help you quickly deploy Sentinel and maximise your investment in Microsoft whether you are:

- **Deploying Sentinel for the first time;**
- **Aiming to unlock additional value** from your existing Microsoft Azure and Sentinel deployment; and/or
- **Looking to improve the efficiencies** in your security posture reporting and incident response

Solution Features

The combination of pre-configured assets and consulting services in the Microsoft Sentinel Accelerator provides a good balance between speed of deployment and tailoring for your needs, and includes:

Discovery – KPMG will conduct a discovery of your Microsoft Azure environment(s), establish a Sentinel architecture based on best practice patterns that aligns with your environment.

Industry Specific – Our industry subject matter experts (SMEs) will work with you to build views of your security posture against industry standards, regulations and key threat vectors relevant to the geographies you operate in.


Pre-configured Assets – Our Microsoft cloud workloads provide actionable security insights leveraging our KPMG’s IP/Asset library of pre-built rules for detection against key threat vectors, automation playbooks for incident response, threat and compliance reporting workbooks, data connectors for Microsoft native and external log ingestion, and workflow automation.

KPMG Risk-Based Approach – The service is built based on KPMG’s industry recognised risk-based approach with guidance on how to leverage Microsoft’s Sentinel solution to identify and respond to risks, supported by deployment and configuration assistance to meet the requirements of your unique situation.

Key Benefits




Utilise
Security features available in your Microsoft Azure environment




Obtain Value Quickly
through KPMG pre-configured assets



Gain Visibility
Of security posture against key industry standards and regulations

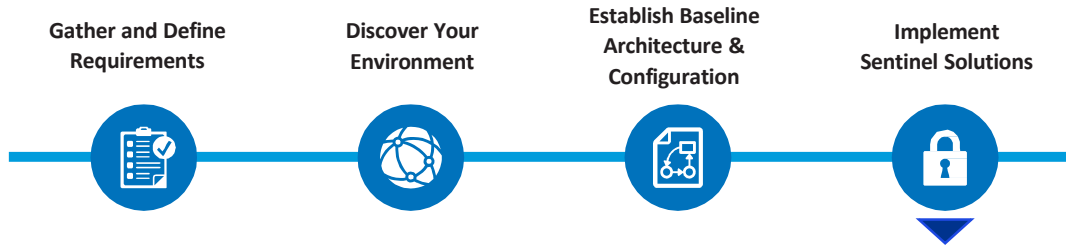


Centralise
Views with a single pane through Microsoft Sentinel



Respond
To threats in near real time with Sentinel playbooks

Our Approach



Based on your requirements and environment, we can deploy the below pre-configured assets on your Microsoft Azure environment. Our Cloud Security professionals can also work with you to develop additional custom data connectors and compliance / threat assets.

Policy Initiatives

Pre-configured for key regulatory requirements and industry standards, including:

Regulatory requirements

- CPS 234 (Australia)
- MAS TRG (Singapore)
- FISC (Japan)
- Among many others

Industry standards

- ISO 27001
- NIST
- PCI DSS

Sentinel Workbooks (Dashboards)

One platform to view key threat vectors relevant to your business and security posture against regulatory requirements and industry standards.

Threat-based Rules & Queries

To identify and detect suspicious activities across various stages of the MITRE attack framework, including but not limited to:

- DDoS
- Ransomware
- Command and Control
- Bruteforce
- Data Breach
- Business Email Compromise
- Vulnerability Exploitation

Automation Playbooks

To enable automation of notifications about suspicious activities in near real time and provision of recommendations to mitigate gaps. We will use the power of AI by integrating it with the solution to derive further efficiencies.

Workflow Automation with ServiceNow

By performing integration with Sentinel, creation of an ITSM profile, enable data flows and synchronisation and validation.

Why KPMG?

Our approach to cloud security emphasizes 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 experts pool include 4000+ certified professionals in cloud security with 1000+ certifications in Microsoft Cloud.

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.

Contact us

Matthew O'Keefe
KPMGAustralia
T: +61 3 9288 5430
E: mokeefe@kpmg.com.au

Krishna Manghat
KPMGAustralia
T: +61 2 9273 5028
E: kmanghat@kpmg.com.au

home.kpmg/socialmedia



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.

© 2023 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent member firms affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.