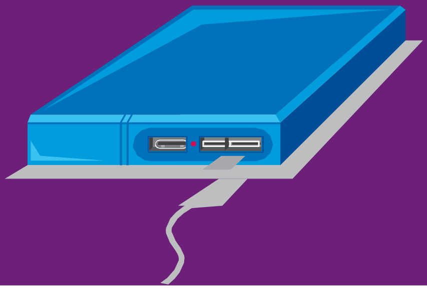
Cyber Defense

Simplifying the Security Operations Ecosystem with Microsoft Azure Sentinel



As the digital revolution continues, cybersecurity is a core business requirement to protect critical business processes, assets and data from cyber attacks. A key component of cybersecurity is security monitoring. Moving business operations to the cloud has become ever more popular, a consequence of which is a diverse attack surface and the fragmentation of security tooling, making it more expensive and difficult to manage. Traditional on-premises SIEM solutions hinder the digital revolution. They're often unsuitable for taking in and analyzing logs from multi-cloud environments, are costly to buy and maintain and difficult to scale.

By combining Microsoft technology with KPMG member firm's security operations advisory services, the security operations tooling of your organization can be right on track.

Outcomes

Assess
Assessments carried out to determine current state.

Design
A custom SecOps transformation program tailor-made for you.

Build
Seamless customization and integration tailored to your environment and requirements.

Operate
Training, incident response, tuning, threat hunting and operations.

Capabilities

The KPMG Cyber Defense Framework allows KPMG professionals to work with you to identify key focus areas to design and implement a custom SecOps transformation program centering around Azure Sentinel. This program will include a simplified architecture, operational model and direction to integrate your existing tooling and processes to manage the migration to Azure Sentinel.

KPMG: Cyber Defense Framework
The framework focuses on the key security operations capabilities within Identify, Protect, Detect, Respond and Recover to provide your current and desired maturity level using identified gaps to establish a program to improve your security posture.

Microsoft Azure Sentinel
Azure Sentinel is a cloud-based SIEM-SOAR solution offering limitless cloud speed and scale combined with AI and built-in orchestration and automation of common tasks. Azure Sentinel can simplify your security operations ecosystem and save time with automation and orchestration.

Scope

ASSESS

- Review of existing implementation
- Purple team/red team in the cloud

OPERATE

- Training to use the solution
- On-call incident response
- Tuning of alerts to a point only L3 required
- Managed operations
- Managed threat hunting

CLOUD
CYBER
DEFENSE

DESIGN

Develop the SecOps Transformation program, including

- Simplified architecture
- Migration from legacy security tooling
- Requirements (log sources, use cases)
- Integration with existing legacy security tooling

BUILD

- Ready-to-go playbooks for common use cases (O365, Phishing, Defender)
- Create custom playbooks
- Integration with ticketing systems
- Integration with other solutions
- AI/ML queries/models to detect
- Creation of connectors
- Integration of automated process
- Integrate into legacy SOC processes and procedures

Why KPMG and Microsoft?

People

Our respective cyber security teams include recognized industry leaders and highly experienced professionals.

Experience

Both Microsoft and KPMG member firms have supported clients advising on niche security challenges to delivering compliance and identity integration in complex and highly-regulated industries.

Global, local

Between Microsoft and KPMG's worldwide reach, we're able to work in a consistent manner with global organizations and their entities across multiple territories at a local level.

Approach

Using a tried and tested proprietary approach, Microsoft and KPMG professionals can help cut through complexity and expedite your information security activities.

Simplifying your Security Operations Ecosystem with Microsoft Azure Sentinel

To find our more about the power of the KPMG and Microsoft alliance, contact:

Koos Wolters
Partner, Cyber Security and Privacy
KPMG in the Netherlands
T+31 20 656 4048 | M+31 6 533 37 486
wolters.koos@kpmg.nl

kpmg.com
kpmg.com/socialmedia

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.