Accelerating cloud security monitoring & incident response

KPMG Cloud Responder

As the digital revolution continues, cybersecurity is a core business requirement to protect critical business processes, assets and data from cyber attacks. While not a matter of if but when a cyber security incident occurs, the need to quickly identify, contain, remediate, and report a security incident is crucial to an organization's financial, reputational, legal, or operational risk. As more IT systems shift to the cloud, organizations continue to push more cloud technologies and solutions into their digital transformation portfolio requiring security teams to secure not only existing infrastructure; but also learn, train, and adopt new approaches to incident response.

Challenges of security monitoring and incident response (IR) for the cloud

New tools are needed for analyzing cloud resources

Monitoring and response needs to support multi-cloud approaches

Incident response techniques must operate at cloud scale

Capabilities need to continuously adapt to meet evolving threats

KPMG Cloud Responder with Microsoft Azure Sentinel

KPMG Cloud Responder with Microsoft Azure Sentinel leverages Microsoft's cloud-based SIEM/SOAR solution to enable incident response at cloud speed and scale, combined with AI and the built-in orchestration and automation of common tasks. KPMG Cloud Responder is combination of accelerators that help clients rapidly implement Azure Sentinel and quickly adopt industry leading processes for security monitoring, digital forensics & incident response.

Through our accelerators, KPMG can help organizations transform their security operations, incident response and digital forensics capabilities to become cloud-ready during the transformation of its security monitoring capabilities.

	Accelerators		
People	Network defender training	Shift resources to high-value tasks	Standardized investigation handling
Process	Target Operating Model	Refined process flows	Integration & orchestration
Technology	Sentinel configuration	Analytic rule & playbook libraries	Digital forensics & IR automation

KPMG Cloud Responder helps speed the adoption of Microsoft Azure Sentinel

Sentinel Configuration

KPMG professionals help plan, architect and deploy Azure Sentinel for single and multi-tenant enterprises, leveraging Azure Lighthouse as needed.

Analytic Rule Library

KPMG leverages pre-configured analytic rules to help speed the adoption of security monitoring. During implementation, rules are tailored to the environment as well as new rules are created to match the most relevant use cases.

Investigation Playbooks

KPMG developed an approach to automated investigations leveraging Azure Logic Apps, allowing your environment to change investigation techniques as the threat landscape changes.

Digital Forensics & Incident Response Environment

KPMG extends Microsoft Azure Sentinel with automation and orchestration to enable triage, processing and reporting of digital forensic artifacts for cloud resources. We enable security detections to trigger orchestration that transforms the time consuming process of isolating and triaging cloud resources into an automated process. Integrated with **KPMG Digital Responder**, an **automated forensic collection and processing pipeline**, forensics artifacts are converted from data into actionable information in hours rather than days.

Why KPMG and Microsoft?

People

Our respective cyber security teams include recognized industry leaders and highly experienced digital forensics and incident response professionals.

Experience

Both Microsoft and KPMG 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, 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.

Contact us

Jordan Barth
Director, Cyber Security Services
KPMG United States
T: (202) 533-3989
E: jbarth@kpmg.com

David Nides
Principal, Cyber Security Services
KPMG United States
T: (312) 665-3760
E: dnides@kpmg.com

Ed Goings
Principal, Cyber Security Services
KPMG United States
T: (312) 665-2551
E: egoings@kpmg.com

Steve Barlock
Principal, Cyber Security Services
KPMG United States
T: (415) 963-7025
E: sbarlock@kpmg.com

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

www.kpmg.com

kpmg.com/socialmedia