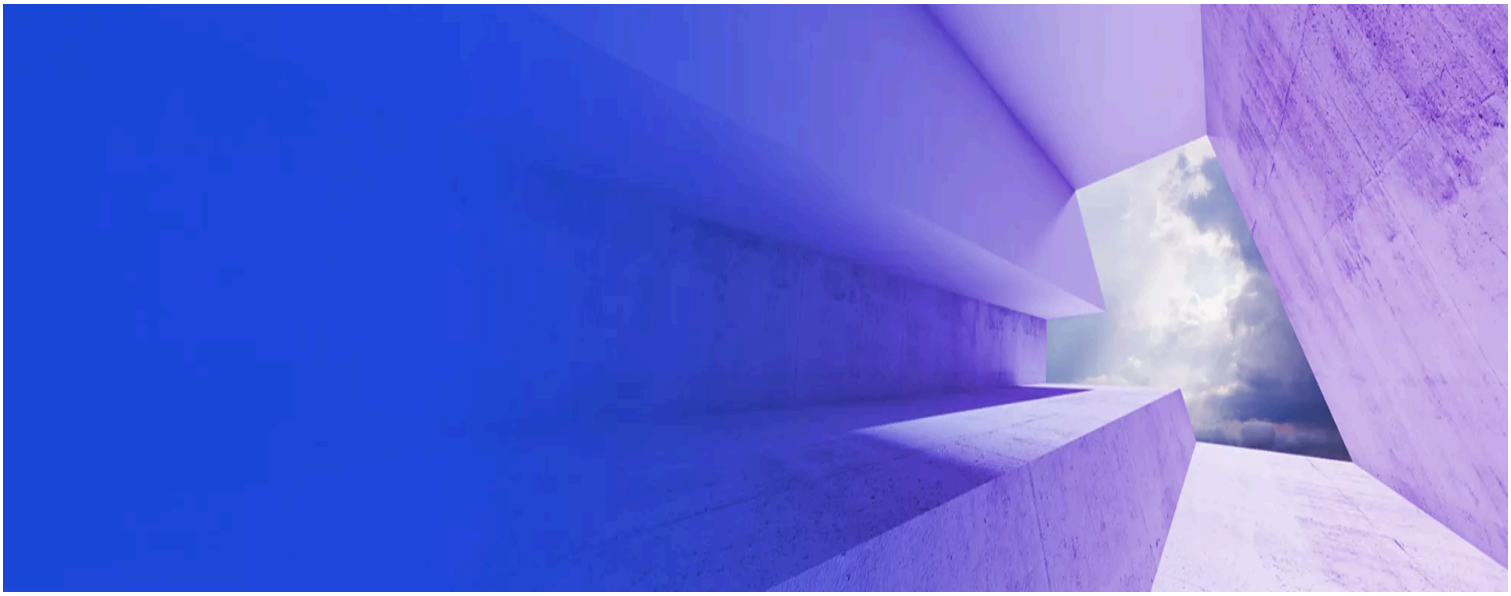


Global businesses face a paradigm shift demanding revolutionary new capabilities to detect and respond to today's fast-expanding cyber threat landscape. As emerging technologies such as artificial intelligence (AI) and automation redefine cyber threat detection and response, they also unleash new advantages for malicious attackers who are 'upping their game' to become more agile than many of today's large enterprises.

Many businesses are discovering that traditional threat detection and response capabilities may not be able to effectively manage the flow of proliferating data and threat alerts. Forward-looking organizations are pursuing rapidly emerging AI capabilities to combat today's expanding and increasingly sophisticated threat environment. The time is now, as CISOs spend significant time and resources sorting through logs amid the endless wave of positive and negative threat alerts.

The overarching challenge for CISOs is how best to apply new AI technologies and the capabilities of today's cloud hyperscalers to enable automation that can dramatically enhances alert accuracy and fidelity in an increasingly complex threat environment.

The good news, as more are discovering, is that there are finally powerful core automation and AI capabilities which can address gaps in skills and resources amid the data overload. Today's hyperscaler and AI advances offer a deeper unlocking potential for automation that was not previously available — ultimately forging a new era for security orchestration and automated response (S.O.A.R.).

Automation to combat evolving threats is the inevitable way forward

Unfortunately, while many businesses embrace technology to advance some cybersecurity capabilities, they may also rely on aging and increasingly vulnerable legacy systems and a lack of modern skills – constraints that cannot be quickly or cost-effectively remediated.

Automating detection and response using today's newest AI and hyperscaler capabilities is the inevitable way forward to identify, analyze and respond to real and potential security threats. This *cloud-centric* approach relying on hyperscalers includes elements of key detection and response such as endpoint detection and response (EDR) and extended detection and response (XDR).

The key is to unlock the growing potential of cloud providers to deliver game-changing capabilities for automated visibility, threat detection and data-driven analytics and mitigation tools. Proactive organizations are wisely looking to AI's evolving power to create a secure environment and remain ahead of malicious actors.

KPMG professionals advice to clients is to work to 'make every endpoint a sentry versus a target.' With modern automation, threat detection can be done within seconds instead of hours or days, taking level-one noise detection to new levels while replacing labor-intensive manual processes prone to human error. This allows security teams to focus on level-two and level-three activities, enabling them to respond, remediate and recover much more quickly.

Hyperscale cloud service providers have many platform-native technologies to enhance the detection of potential threats. To build modern effective security monitoring, businesses need to apply a modern threat and signal monitoring program enterprise-wide using the following approach that focuses on people, processes and technology enablement:

- **Build the foundation** with your maturity level defined and a single cloud that is service provider native.
- **Enhance and extend** your maturity level with managed multi-cloud that is native and cloud service provider (CSP) agnostic.
- **automate and integrate** to optimize the maturity level with multi-cloud enterprise integration that is enterprise-centric.

Apply a strategic AI playbook to the cloud 'canvas'

In the race to synthesize proliferating data from multiple sources into clear, actionable insights and drive rapid incident responses, hyperscaler solutions such as Microsoft Security Copilot are advancing triage capabilities and empowering security teams to combat threats as never before. Cloud providers can offer the critical functionality needed to defend against sophisticated threat actors. That said, not enough businesses are effectively leveraging their power.

It's important to stress that hyperscalers driving much needed automation progress will provide the 'canvas' onto which businesses must strategically apply a precise playbook of algorithms, telemetry, capabilities and tactics suited to their unique operations and needs. Success demands more than a 'plug-and-play' game plan to maximize AI's advantages. Also critical is combining modern skills with strategic change management to integrate humans with automated threat-detection capabilities effectively.

Automation, AI and machine learning (ML) will be pivotal to easing today's typical skills and resource constraints while revolutionizing processes, capabilities, speed and efficiency. Businesses can gain an indispensable new window into data alerts and the crucial ability to instantly determine, for example, where a threat may have moved within the organization and how to drive rapid containment. Implementing proactive, adaptable defenses is now indispensable to combat evolving threat actors.

The good news is that more investment is being dedicated to enabling this paradigm shift. Leading organizations, for example, in the financial and telco sectors, are committed to investing in AI and automation tools, typically to reduce level-one alerts in their security operations centers by as much as 50 percent in the short term. Ensuring regulatory compliance and secure, trustworthy AI implementation along the way will be essential to success.

Where to begin? A well-timed approach is imperative

A strategic approach to automation is key. That includes mapping out a progressive and gradual journey that avoids adopting too many different automation tools and technologies at once, as some of them may not be appropriate for your organization's unique and evolving requirements. A smart roadmap should include three key steps:

- **Don't automate a mess.** Incorporate automation, AI and ML into your three-year business strategy. Getting the basics of your security architecture right at the outset — along with the standard detective incident management processes and response playbooks — is imperative.
- **Tailor targets and cloud tools.** Set specific targets suited to your unique business needs to enable automation, AI and ML in your overall detection and response capabilities. Choosing the right cloud (native) tools for the job is essential.
- **Cost-effective use cases for timely capability growth.** Drive an initial set of use cases to methodically and cost-effectively evolve your capabilities in a timely manner.

For enhanced detection, centralize and correlate data across known sources like SIEM, cloud logs, firewalls, EDR / XDR, vulnerability scanning, threat intelligence, identity and asset inventories. Also, enhance enrichment across those data sources so that security incident tickets have more data – ultimately reducing how many 'panes of glass' security analytics teams need to review in order to triage. Machine learning and automation can help reduce the number of false positives that come to your level 1 team and automatically escalate more severe incidents to the level 2 team.

For enhanced responses, rationalize and optimize the number of response playbooks and leverage an appropriate security orchestration and automated response (S.O.A.R.) platform to automatically isolate and contain known threats and bad activity.

As noted, success in advancing detection and response is not about simply 'plugging in' to today's cloud and technology tools. Understanding how to engineer new technologies provided by hyperscalers to fit your organization and bringing in the right skills to drive progress is pivotal. The right mix of human and virtual analysts should be a mainstay. And from the hyperscaler perspective, automated forensics and misconfiguration correcting will be critical.

It's clear that as today's threat landscape and the incidence of costly and disruptive cyberattacks multiply and evolve, there is no time to lose in adopting an advanced S.O.A.R. approach to detection and response capabilities.

Get in touch

Charles Jacco

Principal

KPMG in the U.S.

Profile | Email | Phone

Brian Geffert

Global CISO & Head of Informatior Protection Group

KPMG International

Profile | Email | Phone

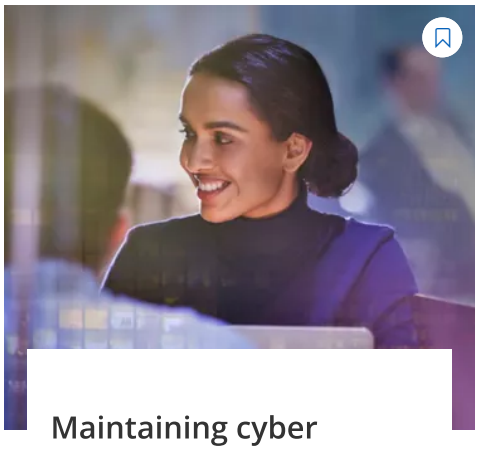
Jordan Barth

Managing Director and Cyber Resilience Leader

KPMG in the U.S.

Profile | Email | Phone

Related content



Maintaining cyber vigilance and staying resilient

How to recover from a cyberattack, rebuild effectively and avoid complacency

KPMG global tech report 2023

Discover how leaders are securing value by navigating uncertainty with confidence.

Learn more

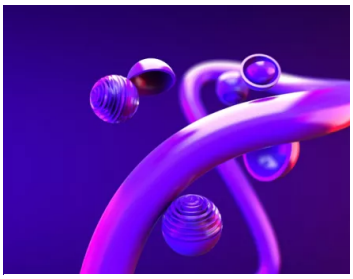
CYBER SECURITY

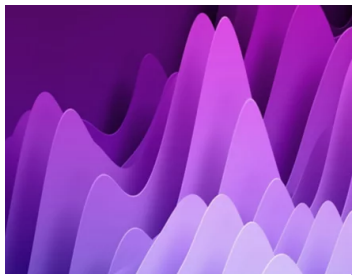
Cyber Security Services

Use cyber security to protect your future.

Transforming for a future of value

Connected. Powered. Trusted. Elevate. KPMG firms' suite of business transformation technology solutions can help you engineer a different future – of new opportunities that are designed to create and protect value.





ADVISORY

Submit RFP