KPMG

Overcoming overconfidence

Companies tap managed services to address evolving cyber threats

As the pandemic spawned new ways of working, it also spawned new security considerations across remote offices, mobile devices and everything in between. Meanwhile, it accelerated the journey toward a digital business model, spurring enterprise transformation to meet the needs of a changing marketplace.

Therefore, if you're like many chief information security officers (CISOs), you probably bought new security technology—like endpoint detection and response, next-gen firewalls, cloud security tools, and upgrades to your security information and event management (SIEM) system. You may even have seen a drop in cyberattacks at your organization, providing a fair amount of confidence in your security posture.

But imagine getting hit out of nowhere by a hacking campaign from an organization like FIN7 that, while appearing benign in your SIEM, proceeds to lock employees out of their systems and pilfer confidential data for ransom. All of a sudden, you have to tell the board of directors that despite the recent investments, your security operations center (SOC) wasn't able to detect the attack or respond in time.

This kind of scenario is becoming all too common, due to a false sense of confidence in cybersecurity. Indeed, while recent investments in security technology may deter known threats, they are less effective for emerging threats such as ransomware, cloud attacks, supply chain sabotage and advanced hacking.

To protect the enterprise, build resilience and make cybersecurity an enabler of ongoing business transformation, CISOs must go beyond basic security investments.

Rising risk

Cybercrimes are increasing in volume and sophistication, leaving even the most tech-savvy organizations feeling outmatched. Companies face risk of reputational damage, financial loss and business disruption.

83% of companies have suffered at least one cyberattack over the past 12 months.

80% expect cyber risk to rise in the next 12 months.

Source: KPMG Fraud Outlook 2022

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Stretched thin

New security tools sharply increase the amount of data coming in from disparate sources, but most cybersecurity teams lack the technical skills to analyze it.

Some fail to understand the difference between threat feeds and threat intelligence, while others simply don't have the resources to manage a wide variety of isolated security tools—nor to integrate new tools with legacy security processes.

As a result, many cybersecurity organizations are facing staff burnout, missed alerts, ineffective analytics, increased adversary dwell time and slow incident response.

In addition, the investments that many CISOs are making could be considered a mere baseline for a cybersecurity tool stack, and serious challenges remain. For example, a SIEM is a basic data-in-events-out approach that is often too simplistic for modern security. To prevent the time-consuming analysis of extraneous data, a SIEM requires a lot of human input—such as developing use cases, flagging irrelevant data sources, configuring the system to ingest only the relevant intel, and managing storage—but how can teams do that when they're already stretched thin?

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

An emerging answer: as-a-service security

To respond to these kinds of challenges, companies must move from reactive security monitoring to more proactive cyber operations. One growing solution is managed detection and response (MDR).

With this model, CISOs can transfer day-to-day security operations and 24/7 monitoring—including low-level analysis, hypothesis-driven hunting for new threats, and cybersecurity engineering—to an expert managed services provider.

In addition to cutting total cost of operations, leading providers combine deep subject-matter expertise, artificial intelligence and leading practices to deliver other strategic outcomes—such as faster detection, faster remediation, improved operational resilience and stakeholder trust.

In fact, according to the KPMG and HFS Managed Services Outlook, a global survey of 800 executives conducted in October 2021, 80 percent of organizations plan to increase their use of managed services for information technology and cybersecurity over the next two years. Already, over 40 percent of respondents use managed services for more than half of their organization’s cybersecurity activities, and cybersecurity is one of the areas where respondents expect managed services to deliver the most value.

Companies are also tapping managed services providers for specialized, hard-to-find talent. In a recent HFS Research Cybersecurity Pulse*, more than three-quarters of cybersecurity executives said the shortage of qualified cyber professionals had intensified their staff workload, led to human errors, and hampered the ability to prioritize or investigate alerts in a timely manner. Eighty-one percent said this shortage is driving their increased use of managed services in areas like network security, threat intelligence and threat hunting.

Meanwhile, MDR enables companies to free their overstretched cyber staff to focus on the bigger picture and conduct major incident investigations that are escalated to the internal team.

80%

of organizations plan to increase managed services for cybersecurity in the next two years.

Source: KPMG and HFS Managed Services Outlook

*HFS Research, Cybersecurity Pulse, October 2021

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Five key strengths to look for

To effectively drive transformation through managed services, CISOs must look far beyond staff augmentation and basic use case management. Instead, seek out MDR providers who bring new thinking on security controls and networking, along with big data analytics for better insights, detection and rapid response.

In particular, look for providers who provide five key strengths.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

01

Create a holistic view of the threat landscape

Technology moves at the speed of the business, and that can create compromises you’re not aware of.

For example, consider that with every deployment to a public cloud, the attack surface expands by 2X to 3X. One company, in trying to fail fast with a new application, was deploying it about six times per day and, unbeknownst to the SOC, those deployments left behind privileges for confidential data repositories that were still connected to the on-premises environment.

Your MDR provider should have the knowledge and experience to help you prevent these kinds of remnants, while also monitoring every application running on the servers in your environment. Indeed, SOC operators rarely know which version of software is running, nor the access levels and vulnerabilities of the associated application programming interfaces (APIs). For example, an attacker could compromise the service account for an application, elevate its access privileges on that system and every connected system, and move laterally across the network.

Look for providers who offer proactive, hypothesis-driven hunting for these and other kinds of threats, while drawing from their threat intelligence in addition to yours. Providers should have a deep understanding of your on-premises, cloud and hybrid environments, while providing services like enhanced intelligence to understand an actor’s motives, identity access management to prevent lateral movement, and rapid root cause analysis beyond alerting.

Also seek a provider who will take responsibility for tuning your technology to thwart false positives, ensure proper configurations, and prevent blind spots.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02

Make cybersecurity a transformation forethought

In many enterprises, profit tends to outweigh security, so the cybersecurity function—typically viewed as a profit-inhibitor—is often called to the table only after an initiative has been deployed.

But a savvy MDR provider can help you establish your SOC as a transformation enabler and accelerator, not a blocker.

For example:

— What is the hardening baseline for every server?

— What is the role of that server?

— What is its core functionality?

— Is it a database server or a basic server?

Using inquisitive analytics around security and access controls, leading MDR providers serve as the expert bridge between the SOC and transformation teams.

These providers can help you achieve the right balance between fast development and high security—thanks to secure DevOps that embed trust and security into the heart of your processes.

With the right MDR partner, you don't have to put agile development on hold for security or retrofit your technology to resist new threats.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

03

Offer a collaborative relationship with a single-pane view

Your MDR partner should be just that: a partner in the transformation journey who provides appropriate metrics and security analysis to drive skillful business decisions.

Therefore, instead of using “black box providers” who operate out of sight, seek a provider with the expertise and automation to correlate multiple SIEMs, data sources, threat feeds, controls, alerts, and investigations across different environments—all presented in a clear dashboard that’s accessible by both parties.

Your provider should also be able to offer a 360-degree view that gives visibility across an organization, including:

- C-Suite: Executive view of the over all security posture of the enterprise
- Compliance Team: A view of security data that allows for a continuous audit of operations of security controls
- Security Ops: A view of prioritized list of threats that impacts the business resiliency
- DevOps: A view of architecture security weakness and vulnerabilities for backlog management

This enables one source of cybersecurity truth instead of multiple portals.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

04

Deliver predictable costs and outcomes

Traditional MDR often focuses on reactive threat analysis, meaning variable costs and outcomes. Leading providers, on the other hand, package proactive detection and response in a subscription-based offer with predictable costs—with the option to flex up or down to meet fast-changing needs.

Importantly, that package should not be a one-size-fits-all solution. Instead, your provider should offer a security model that's tailored to your business strategy, operations and environment.

For example, a "pay as you grow" model can incorporate the analytics of the following for more predictive service:

- Business Requirements: Predictive needs based upon digital transformation strategy
- Infrastructure analytics: Connected services consumed within the enterprise
- External attack surface: Analytics of external attack patterns and un-managed services deployed (e.g. Shadow IT)

The best providers also deliver predictable, measurable outcomes, from dwell time reduction to speed of containment. Outcomes should also relate to enterprise transformation—such as accelerated innovation, brand trust and operational resilience—while giving CISOs a seat at the transformation table.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

05

Have deep knowledge of your industry

To drive those kinds of enterprise outcomes, MDR providers should be experts not only in cybersecurity but also in business—including your industry.

Considerations include:

- What industry-specific threats are emerging?
- What are the latest considerations in cloud and mobile applications?
- What does a good security posture look like in your business model?

Seek a managed services provider who brings robust industry expertise to your cybersecurity challenges.

Providers also need to be able to help organizations identify "indicators of compromise" by industry. This should include:

- Knowing your adversaries
- Understanding attack patterns that are leveraging weaknesses within the enterprise by industry
- Proactive defense: Understanding of industry weakness patterns that can be provided by a trusted MDR service provider to proactively identify weaknesses before they become concrete security incidents.

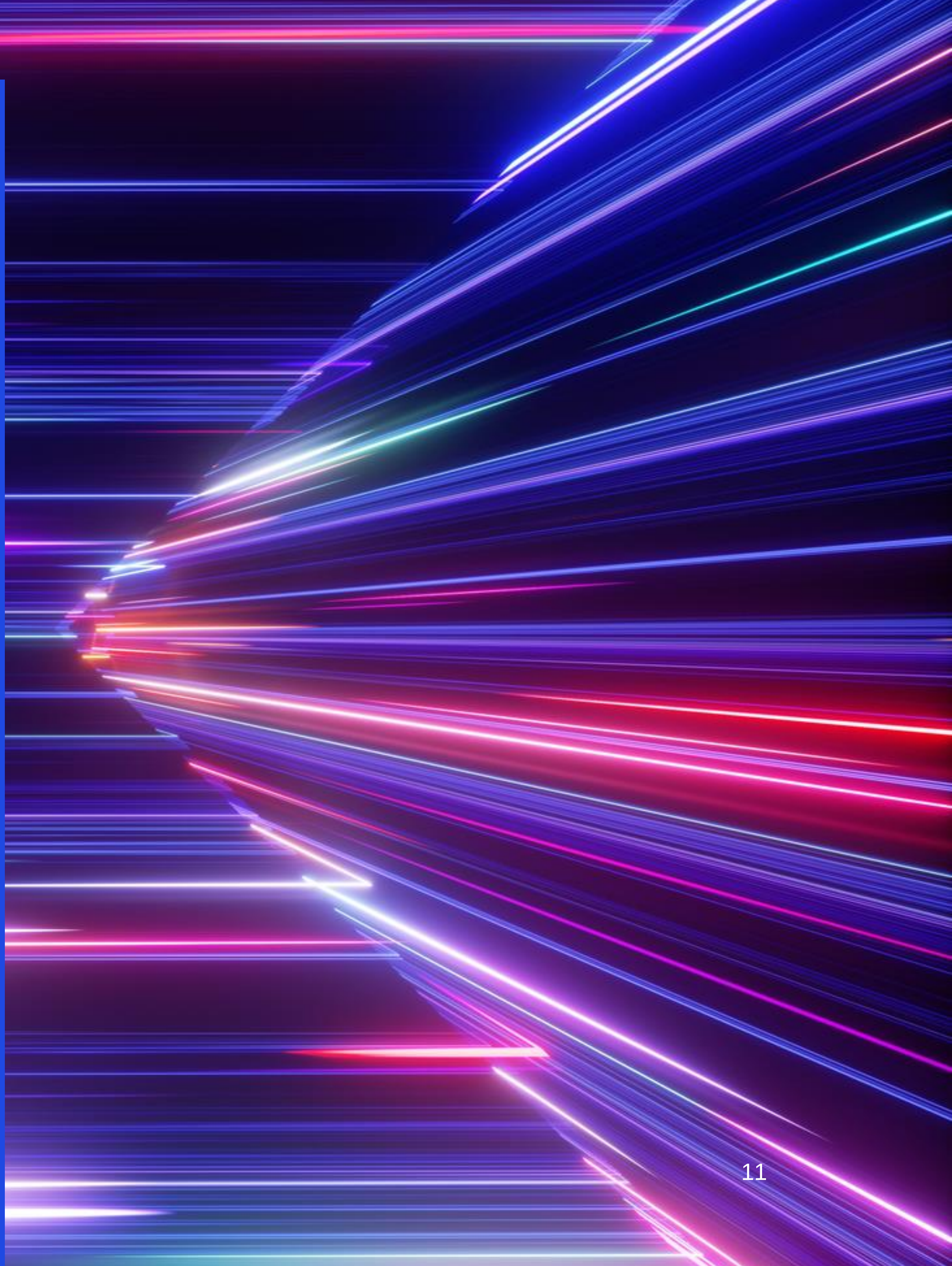
© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Shaping the future

Technology makes many things possible, but possible doesn’t always mean safe.

Indeed, transformation initiatives—from innovative sales channels to new customer experiences—create exciting opportunities not only for the business but also for cyber criminals. How can you build a resilient and trusted digital world, even in the face of evolving threats?

As one part of their approach, forward-looking CISOs are partnering with leading service providers for managed detection and response. This is how companies can adapt to ever-changing risks, safely operationalize their growth agenda, scale security across the enterprise, and get an edge with technology that is secure and trusted.



© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

About KPMG Managed Services

Business transformation is the path to sustained advantage. But transformation is not a fixed destination; it's an ongoing journey. How can you continually evolve your business functions to keep up with ever-changing targets?

KPMG Managed Services can help.

We combine advanced technology with functional and sector expertise to handle knowledge-intensive processes across your enterprise—on a subscription, as-a-service basis. In addition to reducing your costs, we drive outcomes like resilience, customer retention, stakeholder trust, and competitive advantage. We help you operationalize your growth ambition, so you can accelerate your transformation journey while minimizing disruption and risk.

Learn more about KPMG Managed Services.

Learn more about KPMG Managed Detection and Response.

About KPMG Cyber Security Services

KPMG helps you create a resilient and trusted digital world—even in the face of evolving threats. We bring a combination of technological expertise, deep business knowledge, and creative professionals who are passionate about protecting and building your business. Together, we can create a trusted digital world so you can push the limits of what's possible.

Learn more about KPMG Cyber Security Services.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contacts:

Rajesh Ahuja, CISSP
Managing Director, Advisory KPMG
Managed Services
KPMG U.S.
ajeshahuja@kpmg.com

Jerry Nguyen
Director, Advisory
KPMG Managed Services
KPMG U.S.
jerrynguyen1@kpmg.com

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.