KROLL

Microsoft Solutions Partner
Security

Member of
Microsoft Intelligent
Security Association
Microsoft

Microsoft Threat Detection and Response:

Five Key Pitfalls (and How to Address Them)

Microsoft Threat Detection and Response: Five Key Pitfalls (and How to Address Them)

Authors

Rafael De Lima
Cyber Security
Solutions Architect

Michael Cowley
Head of Solution
Engineering

Thomas Hind
Vice President
Platform Architecture

Organizations are increasingly turning to the cloud in their attempt to become more agile and efficient. Many will choose the Microsoft ecosystem and consequently will need to become familiar with Microsoft Security Products, how these technologies can be leveraged to their full potential, and what will need to be supplemented to avoid unnecessary risk. Drawing on Kroll's experience gained by responding to thousands of incidents each year, this guide outlines:

- Common security challenges organizations face when moving to a Microsoft cloud environment
- Practical steps to help accelerate threat detection and response across your Microsoft estate
- How to get the most value from solutions such as Microsoft Sentinel and the Microsoft XDR solutions, of Microsoft 365 Defender and Microsoft Defender for Cloud
- Insights from a real-life case study
- How Managed Detection and Response (MDR) services can help get the most value from the Microsoft Security stack and what to consider what evaluating their experience, approach and technical scope

Risk Vs. Opportunity: Threat Detection and Response in the Microsoft Ecosystem

As the drive to move business operations to the cloud continues at pace, the expanded attack surface generated by digital transformation continues to present new opportunities for threat actors—and considerable risks for organizations.

For businesses ambitious to maintain a robust security posture in an ever-evolving threat landscape, there is a lot to consider technically. Not only must threat detection in the Microsoft ecosystem leverage native tooling and telemetry but also, at the same time, it must be supplemented with intelligence-driven detections specific to cloud threats.

Added to this, the rapid and effective detection of a genuine cyber threat is futile without a corresponding rapid and effective response that addresses not only containment but also remediation and forensic analysis to prevent reinfection. Not having these processes in place can pose a significant risk to a business. However, by recognizing the potential obstacles and working with trusted experts, organizations can maximize both their Microsoft investment and level up their cybersecurity.

5 Key Microsoft Threat Detection and Response Pitfalls to Avoid

Pitfall 1. | Not Understanding Where to Prioritize with Your E5/ Microsoft Defender License

A common challenge for many organizations is a lack of certainty around which products of Microsoft Defender/E5 they should prioritize for threat detection and response. For those that have the EMS E5 or Microsoft 365 Enterprise plan that could mean deciding which solution they need to onboard first out of Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint, Defender for Cloud Apps. That's not taking into account the separate licensing structures of Microsoft Sentinel and Defender for Cloud.

Outside of carefully considering the type of license you have, it is important to keep an eye on what is cost effective. For example, additional data ingestion and storage charges can be created by consuming too much data. Including extra assets and endpoints to monitor, such as additional servers, workstations and virtual machines may incur additional licensing charges, while some teams spend too much time configuring sensors.

Of course, every organization faces different threats and has a different risk tolerance. However, in our experience, if you have invested in Microsoft for your IT estate, you can prioritize aspects of the security stack that are best value through what Gartner calls a "Security Operations Center (SOC) triad perspective": gaining essential visibility of logs, endpoint and network infrastructure telemetry.

Recommendations

Start by gaining a clear understanding of the type of Microsoft license you have. We recommend making sure you have the solutions listed below and prioritizing them for threat detection and response. They offer cost-effective licensing while providing that vital combination of prevention and detection capabilities in the key environments exploited by threat actors in the early stages of attack:

Microsoft Defender for Endpoint (DfE)

A critical solution to detect advanced threats on endpoints such as workstations, virtual machines and servers as well as mobile devices to access network resources. Microsoft DfE provides great integrations with the wider Defender suite of solutions, offering visibility over an attack's common lifecycle and valuable insight into what is accessed, who it's accessed by, and from where.

Microsoft Defender for Identity - Azure Active Directory (AD)

With the traditional network perimeter now being replaced by the authentication boundary for your trusted resources, Azure AD enables organizations to leverage a central identity and authentication source across third-party resources and Software-as-a Service (SaaS) environments, including those outside of Azure and the Microsoft ecosystem. Microsoft Defender for Identity provides an identity-centric view of users' activity and behaviour to highlight malicious activity.

Microsoft Defender for Office 365

Protects you against malicious threats posed by email messages, links (URLs) and collaboration tools. This acts not only as the secure email gateway in front of your exchange servers but also provides threat investigation and response capabilities such as alerting of malicious or suspicious activity affecting your email or users, identifying malicious IP addresses, resetting passwords or blocking the user account.

By prioritizing Microsoft Defender solutions that cover endpoint, identity and O365—and putting them all into Microsoft Sentinel—you will begin pulling in data not only from the underlying Azure environment but also from third-party cloud sources such as AWS and Google Cloud. Using Sentinel in this way also means that everything is in the same place for dashboarding, rules and Microsoft 365 Defender. An advanced Managed Detection and Response (MDR) for Microsoft service like Kroll Responder MDR for Microsoft will be able to pull relevant alerts from Microsoft's Defender products, whilst leveraging the data within those platforms for detailed investigation and remediation on your behalf. The Microsoft Reference Architecture for Security Operations leverages Microsoft Defender as a detection layer for the relevant areas (cloud workloads, identity, endpoints, etc), passing alerts onto Microsoft Sentinel. Microsoft Sentinel can then also carry out additional correlation based on those alerts or from traditional log sources.

"An advanced Managed Detection and Response (MDR) for Microsoft service like Kroll Responder MDR for Microsoft will be able to pull relevant alerts from Microsoft's Defender products, whilst leveraging the data within those platforms for detailed investigation and remediation on your behalf."

Pitfall 2. | Buying Microsoft Security Solutions Before Understanding How to Configure Them

Many organizations make the error of committing financially to adopting security solutions before fully understanding the breadth of time and insight required to optimize them. Failing to ensure that effective configuration is in place, to identify the right telemetry and activity, can cause monitoring to become redundant. The good news is that Microsoft has made it simple to integrate Microsoft Defender and other E5 security solutions into Microsoft Sentinel. The bad news is that, without proper configuration and implementation of these underlying features, you won't gain value from them.

Recommendations

Let's look at one example of this with Microsoft 365 Defender solutions, for which you need to consider:

Data retention

While data retention can be extended to assist with compliance and threat hunting use cases, it's worth noting that telemetry for advanced features in this product is generally not available after 30 days. Organizations may therefore need to identify other methods of hunting this data.

Threat policies

Ensure that relevant policies are configured for each Defender solution. Examples include policies for anti-malware, anti-phishing, anti-spam, etc.

Automations (in terms of notifications or remediation actions)

You will need to enable features such as Live Response, Automated Investigation and Auto Remediation.

Permissions and roles

Ensure correct admin roles, permissions and assigned Azure Active Directory groups for tier-based/role-based access to assign and authorize access to different teams.

Rules and relevant components

These include alerts suppression, indicators and web content filtering.

An effective MDR service provider can help to integrate these solutions to give you visibility across the tools in which you've already invested, multiplying your return on investment. Ask your MDR provider to advise on the minimum requirements and standards for specific features and policies. A good provider should proactively guide you on which logs, policies and rules will be needed for each of the solutions you've invested in, particularly in deployment. They should be able to work with you to define logs worth ingesting for detections and logs worth ingesting for compliance or retrospective forensics and threat hunting. These different log categories do not need to be stored in the same expensive storage as one another—and a pragmatic approach can be to align storage platforms and performance considerations to query and recall cadences, to ensure that you are optimizing budgets.

"With the move to the cloud showing no sign of slowing down, it is imperative that organizations fully understand how best to optimize their investments in both Microsoft solutions and MDR services to get the most security value."

Marc Brawner
Head of Cyber Managed Services, Kroll

Pitfall 3. | Not Leveraging Response Automation and Native Integrations

Organizations don't frequently automate response playbooks with on-premise environments because of the negative impacts this can have on more legacy technology which also demands specific on-site forensics. However, as the cloud is both highly accessible and fast-moving, response should be highly automated.

Recommendations

Explore opportunities to leverage native Microsoft tools such as Azure Logic Apps and Power Automate to set up automated cloud responses. Also, look at opportunities to build playbooks that are native in Microsoft Sentinel such as:

Notification playbooks

Triggered when an alert or incident is created, a notification is sent to a configured destination, such as Microsoft Teams, Slack or Outlook email.

Blocking playbooks

Triggered when an alert or incident is created, they gather entity information like the account, IP address and host, and block them from further actions.

Change an incident's severity

Triggered by an incident or alert when attached to an automation rule or analytics rule, the incident severity is changed based on a specific username that is part of the incident user entity.

When combining Microsoft Sentinel with a Microsoft Defender solution, more comprehensive playbooks include:

Compromised machine

An analytics rule indicates a compromised machine, as discovered by Microsoft Defender for Endpoint. An incident is created in Microsoft Sentinel that includes related alerts and entities. Use the **Entities - Get Hosts** action in Microsoft Sentinel to parse the suspicious machines that are included in the incident entities. Issue a command to Defender for Endpoint to isolate the machines in the alert.

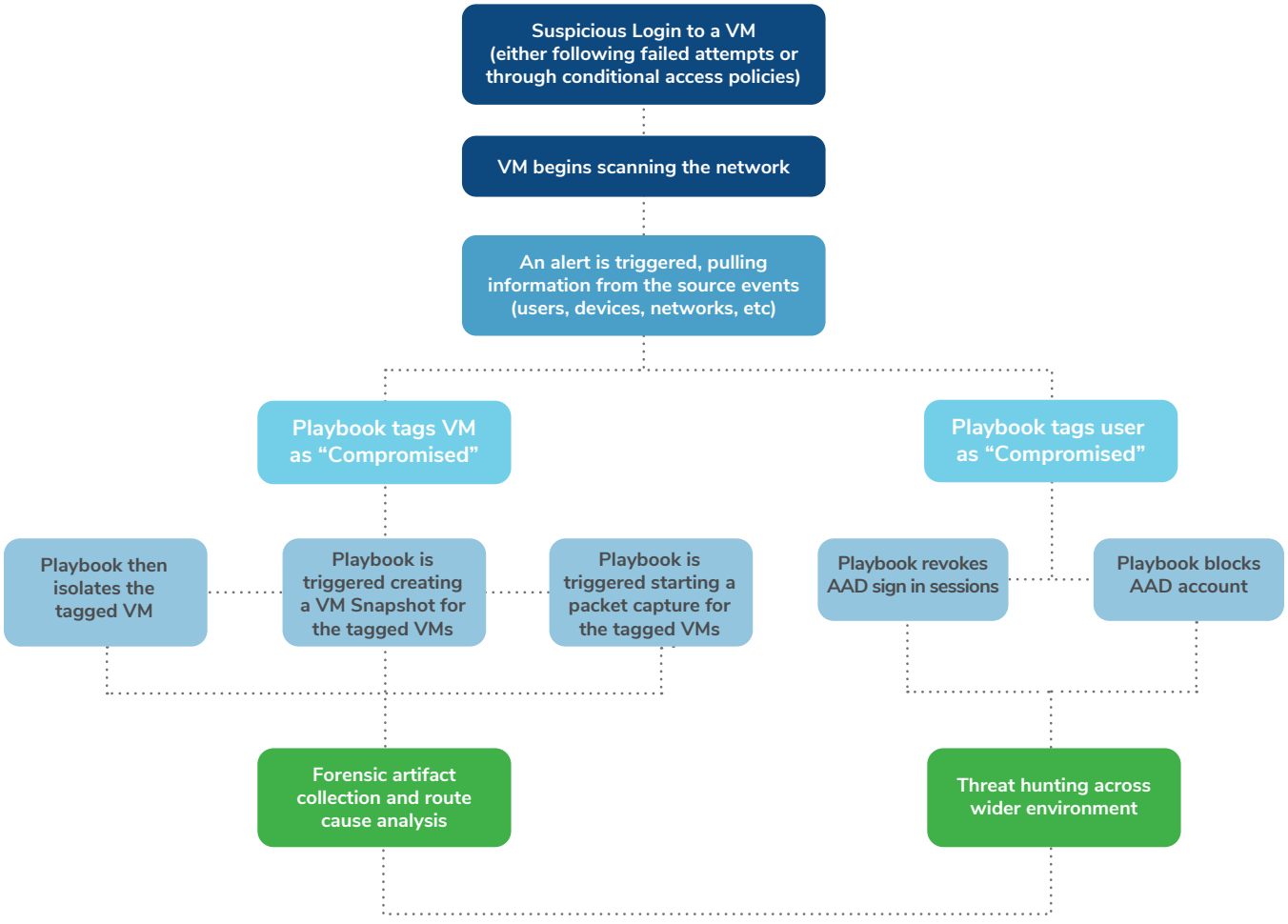
Activity from infrequent country

Triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. It also uses Power Automate to contact users detected as connecting from infrequent locations, and their managers, in order to verify their activity.

It is important to understand the difference between Microsoft Sentinel automations and broader SOC automations. While Microsoft Sentinel will help automate API integrations with other technologies, a broader SOC workflow automation is needed to cover triage, enrichment of threat intelligence Indicators of Compromise (IOCs) and containment. This should be supplemented with frontline intelligence and strategic response that uses digital forensics and incident response (DFIR) techniques such as root-cause analysis, reverse engineering, threat hunting and malware removal.

Example Playbook

In the example playbook below, an attacker aims to access a virtual machine (VM) and starts scanning the network to get a lay of the land. This triggers an alert, pulling user, device and network information (1). From here, various response actions can be triggered such as tagging the VM as compromised (2) and taking a snapshot of that VM (3). That snapshot can be used to run point-in-time forensics and, in parallel with the automation of packet capture enabled on the VM, conduct root-cause analysis as well as ongoing hunting of the deep network activity (4) that the endpoint continues to exhibit.



Pitfall 4. | Not Addressing the Costs and Complexities of Log Ingestion

As organizations start adopting Microsoft Sentinel, they can suddenly find themselves overwhelmed with vast quantities of data collected from an ever-increasing number of new data sources. This can significantly increase the costs of log storage and ingestion, leaving security teams with the reactive and risky task of reducing their coverage or having to suppress log collection altogether.

Recommendations

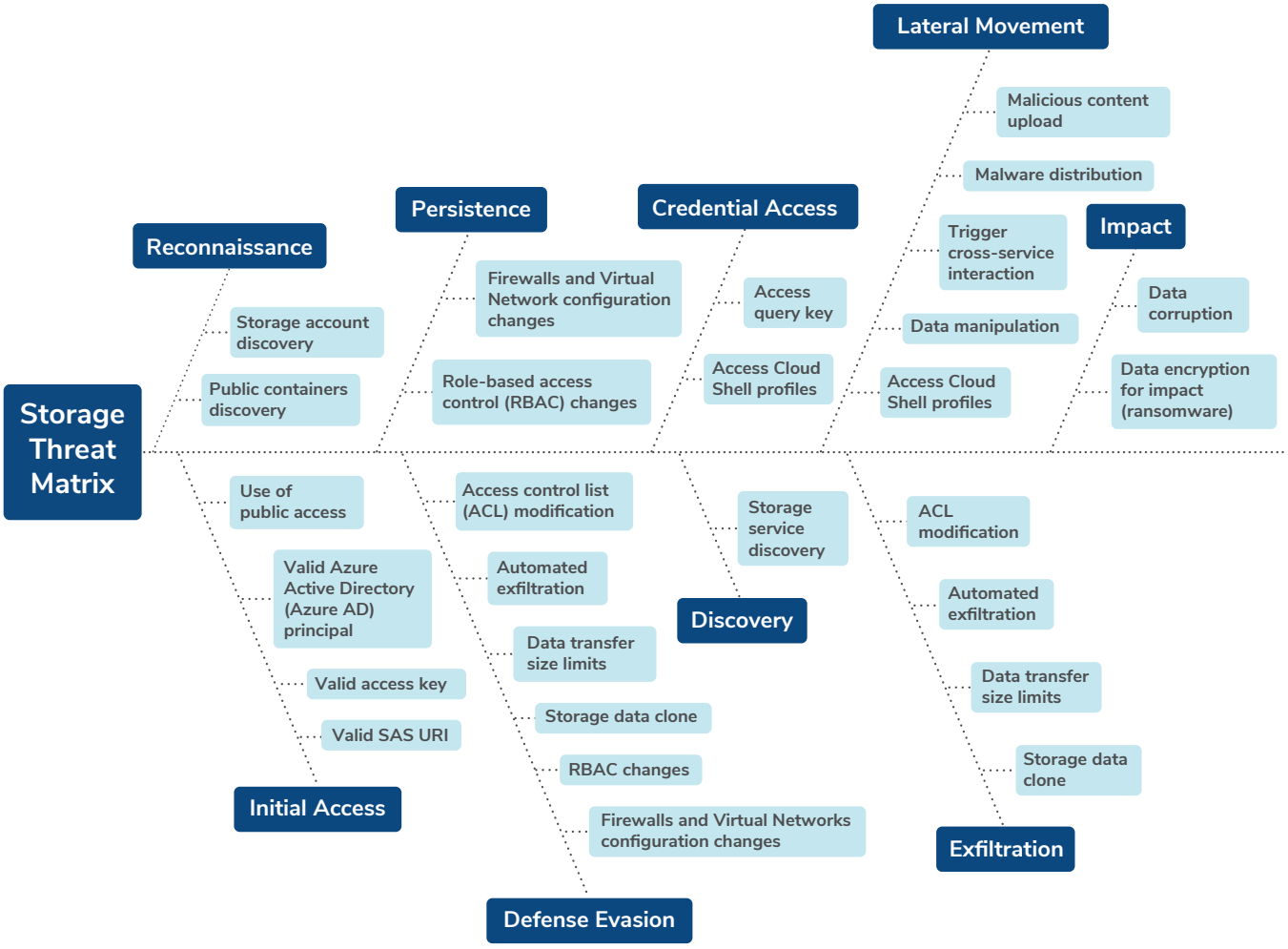
While it's important to maintain coverage of your estate, you can reduce costs by scrutinizing which logs are essential for ingestion compared with those that can be archived. To achieve this, we recommend filtering data at ingestion to archive compliance-related and lower fidelity data into a long-term cloud data lake, such as Azure Data Explorer (ADX), and routing high-fidelity data—specific for threat detection use cases—into Microsoft Sentinel (Log Analytics). Microsoft Sentinel uses the same query language as ADX, which means you can focus on addressing high-fidelity alerts in your Security Information and Event Management (SIEM) while continuously hunting across your data lake for related data and generating detailed analytics reports at the same time.

Organizations also need to understand how the different types of logs can benefit their security in the cloud. While analytic logs provide insights for traditional SIEM correlation, lower value security telemetry can be ingested as basic logs, which can be used for threat hunting and provide additional context as part of investigations.

> **“We recommend filtering data at ingestion to archive compliance-related and lower fidelity data into a long-term cloud data lake, such as Azure Data Explorer.”**

Pitfall 5. | Not Harnessing Opportunities Presented by Defender for Cloud

Too many organizations continue to overlook the many advantages of leveraging Defender for Cloud for environments such as Azure and AWS, not least its ability to break down into more granular solutions covering monitoring for SQL, storage, containers, etc. One example of this is clicking “Enable” in Defender for Cloud, which immediately covers you for data points needed for alerting on all types of threats without any further configuration required, as demonstrated in the diagram below:



Source: Ben Mansheim, 2023, Microsoft Defender for Storage Classic

Recommendations

If your organization is looking to move to the cloud or to operate in an Azure or AWS environment, start connecting Microsoft Defender for Cloud to your servers to benefit from features such as application control and compliance monitoring. This will also help to protect Platform as a service (PaaS) and cloud-native resources which are traditionally difficult to secure.

In terms of response, your organization should then be able to pivot into Microsoft Sentinel and give cloud logs to incident response specialists, enabling them to sift through via a cloud compromise engagement and providing valuable forensic information for making effective and timely remediations.

Case Study: Seamless Microsoft Azure Migration

Company: BSM

With ransomware increasing and a complex, business-critical cloud migration on the horizon, one of the world's largest shipping companies BSM was seeking a solution to monitor its environment for potential threats. It was looking to do this by building a long-term partnership with an experienced MDR provider. This was particularly important given BSM's planned cloud migration to Microsoft Azure, aimed at achieving a more centralized IT approach for both its primary and smaller offices, many of which were small maritime centers.

BSM recognized that the diverse challenges it was facing could be addressed by working with Kroll. Kroll's MDR solution, Kroll Responder, enriches Microsoft's technology by applying frontline threat intelligence drawn from thousands of cyber incidents handled every year, enabling deeper and more effective threat hunting. This is supported by Kroll Responder's global SOC professionals, who operate as a virtual extension of the team, providing the high-quality insight and mitigation guidance that BSM's IT team needs to respond to incidents whenever they arise. To further ensure that BSM's security is as robust as possible, Kroll also conducts managed vulnerability scanning and CREST-accredited penetration testing to help identify and address vulnerabilities across its global infrastructure.

BSM was able to successfully migrate from a legacy security information and event management (SIEM) solution to cloud-native security monitoring with Microsoft Sentinel. This was achieved through Kroll's technology-agnostic approach and deep integration with Microsoft. BSM's IT team is now able to swiftly identify threats and gain the help it needs to respond when threats arise, from phishing attempts that are prevented in collaboration with the Secure Email Gateway (SEG) vendor to stopping fully-fledged ransomware attacks before detonation. The company also has greater visibility across its global network of offices and ships to better detect and respond to threats. Teams within Kroll help BSM to navigate and deploy appropriate security controls and processes, including those related to its Microsoft Security strategy.

By working closely with Kroll and drawing on its close links with Microsoft, BSM is now better prepared for the future evolution of the security market and threat landscape.

View more customer stories at the Kroll Case Study Hub.

Alleviating the Challenges of Cloud Threat Detection and Response: What to Look for in an MDR for Microsoft provider

Organizations often start by adopting Microsoft Security products but struggle to stay on top of the fast-moving changes in their portfolio. Yet another challenge is gaining access to the right team of experts and processes to achieve the best from these products and their capabilities. Effective MDR services can deliver the talent, processes and expertise to ensure your organization gains the greatest value from solutions such as Microsoft Sentinel, Microsoft 365 Defender and Microsoft Defender for Cloud. However, not all Microsoft MDR providers are capable of delivering the caliber of experience and insight required to address the potential pitfalls. To avoid the risks, assess potential MDR providers on the basis of the criteria outlined below:

Microsoft-certified security specialists

Look for a provider whose services are delivered by security experts certified in Microsoft Security competencies such as AZ-500 Microsoft Azure Security Technologies (security engineers capable of implementing, managing and monitoring security for resources in Azure, multi-cloud and hybrid environments as part of an end-to-end infrastructure) and SC-200: Microsoft Security Operations Analyst (security analysts certified in investigating, responding to and hunting for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender and third-party security products).

Microsoft Commercial Marketplace

Check that your prospective provider is in the Microsoft Commercial Marketplace containing the 'Get it Now' button in their offering overview page. This makes it easier for existing Microsoft businesses to select and onboard MDR service providers using their existing enterprise plans.

Field-proven experience

Aim to identify an MDR provider with a proven track record of investigating Microsoft-related security incidents of all sizes, types and complexity. This ensures that, as well as being able to demonstrate relevant experience, they will have the threat intelligence and detection rules needed to detect these threats. A good first point of call is to look at providers who carry the Microsoft Gold Partner, Microsoft Security Solutions Provider or the Microsoft Intelligent Security Association badge. This demonstrates their high standard of expertise and investment in Microsoft Security.

Continual engagement with Microsoft

Verify whether your potential provider is actively engaged with Microsoft on a continual basis. This level of insight will ensure that they can track the trajectory that Microsoft is developing with certain products, enabling them to plan for and make the most of new capabilities as they become available.

Response beyond containment

While MDR has become an effective approach to addressing the security skills gaps around detection and response, organizations have been disappointed with the "response" provided by most MDR vendors. This is because it often stops at containment, putting the onus on the client to remediate and investigate. Some providers may even help eradicate a threat but, due to the lack of a complete response, they leave the door open to reinfection.

More traditional MDR providers will rely on your technology stack to carry out effective response. For example, their response capabilities would be limited to what your EDR tool can achieve. Although this is of course important, having dedicated incident response teams involved would enable you to go beyond the capabilities of your EDR. Rather than leaving your organization hanging, response should cover the whole incident response lifecycle and enable continuous improvement. This means closing the gap between merely containing the threat to actively removing it across all affected systems and quickly understanding the root cause, so that it doesn't happen again.

Ongoing insight

Ensure that your potential MDR provider can deliver ongoing insight into the latest threats that may impact your business, while also turning this intelligence into active detection, hunting and response efforts. Threat intelligence needs to be as wide-ranging as it is deep; wide enough to include a variety of organic, open-source and proprietary sources, yet deep enough to identify not just known attacker indicators such as an IP address, internet domain or file hash—referred to as IOCs—but also actual methods and behaviors used by attackers—known as tactics, techniques and protocols (TTPs). This kind of intelligence requires access to dark web forums, live incident response and forensic analysis, and exposure to both cybercriminal and nation-state level activity.

An adversary-driven mindset

It is critical to check that your potential MDR provider has an offensive perspective or teams beyond its core SOC that engage with live attacker campaigns and use this information to frequently update detections. This requires tight integration between threat intelligence analysts, malware analysts and detection engineers.

The advantages of working with an effective MDR for Microsoft partner

- Greater ROI on native endpoint and cloud technology
- Enhanced threat visibility
- Faster detection, more effective response
- Enriched telemetry
- Frontline threat intelligence

Maximizing Your Microsoft Security Investment: Key Takeaways

In the rush to benefit from Microsoft Security tools, organizations are putting themselves at risk by failing to fully understand the scope of technology they are adopting. This isn't surprising, considering the many issues they need to consider. When assessing or planning your own use of Microsoft security technologies, stay vigilant about falling into common traps that affect many organizations. These range from a lack of uncertainty around which features of your license to start with, not leveraging automation and native integrations, and failing to addressing the costs and complexities of log ingestion.

Working with a good MDR provider plays a key role in not only enabling companies to address the potential pitfalls but also significantly enhancing the impact of their Microsoft Security products. In assessing the best MDR provider for your requirements, it is important to assess potential vendors against key criteria, such as a proven track record of investigating Microsoft-related security incidents of all sizes, types and complexity, the scope to go beyond containment, and an offensive perspective.

The rewards of Microsoft Security tools are significant but without an effective MDR provider on the side, the potential risks are too high to ignore. That's why, at Kroll, we enable organizations to unlock the full power of their Microsoft security stack with Kroll Responder, our MDR solution. Kroll Responder MDR for Microsoft provides 24/7 visibility of threats and complete response across your network, endpoint, cloud and email environments, allowing you to maximize your entire Microsoft security technology investment.

Responder Managed XDR for Microsoft

Responder MDR for Defender for Endpoint

Responder MDR for Sentinel

Responder MDR for Office 365

Get a custom demo of Responder MDR for Microsoft

KROLL

Microsoft and Kroll
The Perfect Partnership

- Telemetry from Microsoft as well as third-party security tools gets enriched with frontline threat intel from

  3,000+ cyber incidents

  handled by our team every year.

- This unified telemetry helps deliver enhanced visibility, and at the hands of our seasoned IR pros, enables

  threat hunting, containment, eradication, and remediation.

$1M INCIDENT PROTECTION WARRANTY

- The entire service is covered by a complimentary $1 million Incident Protection Warranty, not dependent on specific hardware or software choices, which includes ransomware, business email compromise, and other potential issues.

KROLL

END-TO-END SOLUTIONS TO STOP CYBERATTACKS NOW

TALK TO A KROLL EXPERT TODAY

Rafael De Lima
Cyber Security
Solutions Architect
rafael.delima@kroll.com
+44 2045069771

Michael Cowley
Head of Solution Engineering
michael.cowley@kroll.com
+44 7827251673

Thomas Hind
Vice President
Platform Architecture
thomas.hind@kroll.com
+44 7824606854

Additional hotlines at:
kroll.com/hotlines

Or via email:
CyberResponse@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.