K·MICRO
THINK FORWARD

KMicro: Rapid Incident Response

Swift, expert-led incident containment and response

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

Microsoft
Solutions Partner

We Are KMicro

KMicro, seamlessly blends cutting-edge Microsoft business applications and technology prowess. Our seasoned experts, armed with Industry insights and implementation finesse, propel data-driven business modernization across the spectrum. From strategic advisors to end to end execution, we ignite transformation

Microsoft All In

KMicro is 100% focused on the Microsoft stack.

Specializations

- Modern Security
- Dynamics 365
- Modern Workplace
- Copilot & AI

Designations

- Business Applications
- Data & AI
- Digital & App Innovation
- Infrastructure
- Security
- Modern Work

Market Segments

Primary industries, Energy & Resources, Manufacturing, Healthcare Media & Entertainment, and Real Estate.

K•MICRO
THINK FORWARD

Microsoft Solutions Partner

Service Overview

Our Rapid Incident Response & Readiness service along with our Emergency Incident Response service is designed to provide immediate and effective support during cybersecurity incidents.

Leveraging Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Sentinel, and Azure Data Explorer, we deliver a comprehensive incident response and forensics solution to quickly identify, contain, and remediate threats.

Our service is adaptable, allowing us to deploy critical security tools even if the client does not have existing licenses, enabling rapid response during a crisis.

Rapid Incident Response & Readiness

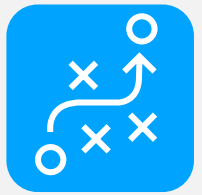
Incident Readiness enables organizations to be well-prepared to deal with relevant incident scenarios..

Emergency Incident Response

Immediate support during cybersecurity incidents for clients with no prior engagement to quickly identify, contain, and mitigate threats

Microsoft Security Integration

Leverages MDE, MDI, Microsoft Sentinel, and Azure Data Explorer for advanced threat detection and forensic analysis.



Flexible and Adaptable

Deploying critical security tools even without existing client licenses, ensuring a swift and effective response in any environment

Rapid Incident Response & Readiness

Increase Resilience

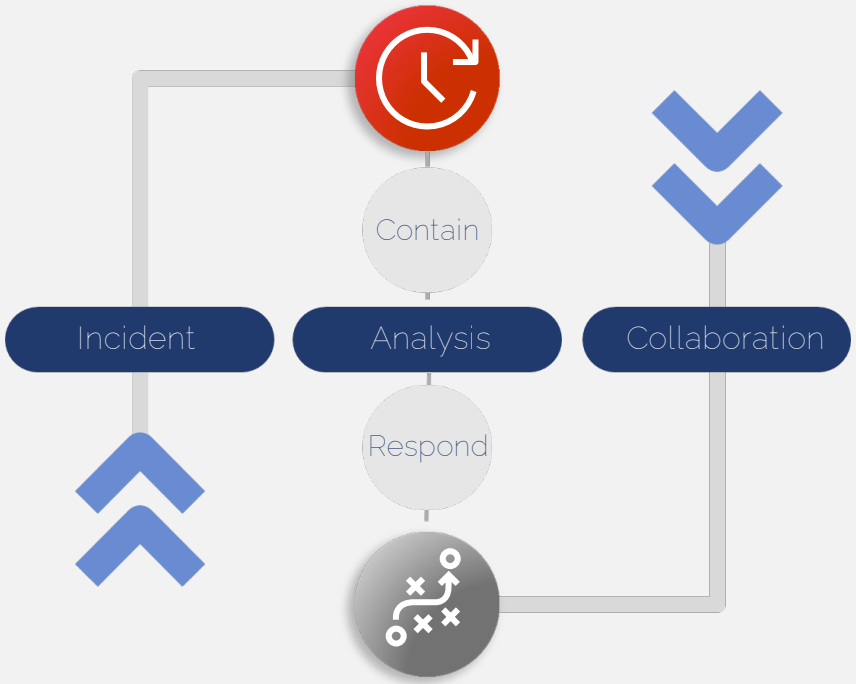
Maintain operations while under attack and minimize disruption.

Reduce Risk

Enable and support your response teams, minimizing response and recovery cost.

Achieve compliance

Comply with regulations and standards (e.g. ISO 27001, CIS20, NIST CSF).



K•MICRO
THINK FORWARD

Rapid Incident Response & Readiness

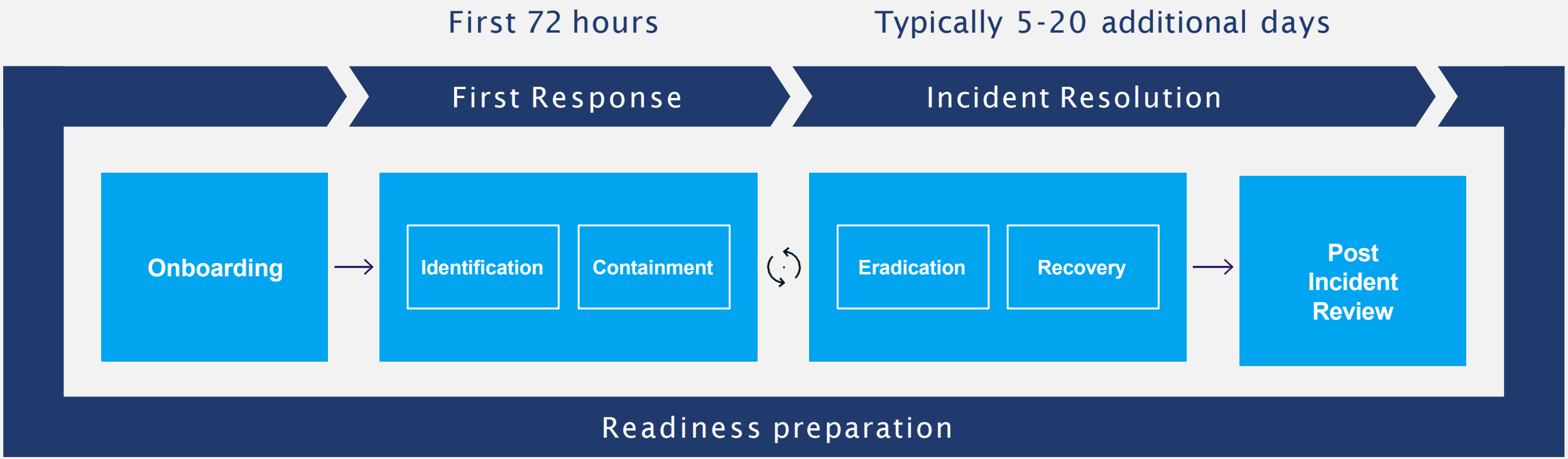
1. A subscription service offering priority access to incident response experts during the critical first 72 hours of an incident.
2. Prepares organizations for cyberattacks with tabletop exercises, simulations, and workshops to improve response strategies without disrupting operations.
3. Faster recovery, minimized risks, and confidence in handling incidents with expert support readily available.

Deliverables

- 24/7 Priority Access to IR teams
- IR Planning and Development
- Pre-arranged Incident Response Plans and Playbooks
- Specialized Support in the immediate aftermath of a breach
- Tabletop Exercises and Simulations
- Incident Response Maturity Assessments

K•MICRO
THINK FORWARD

Rapid Incident Response & Readiness



K•MICRO
THINK FORWARD

Rapid Incident Response & Readiness Service	Basic	Standard
Onboarding	Discovery & Preparation of Access & Permissions	Discovery & Preparation of Access & Permissions
Tooling deployment and Integration	Deployment of Microsoft Defender for Endpoint, Defender for Identity, and Sentinel	Deployment of Microsoft Defender for Endpoint, Defender for Identity, and Sentinel
Communication Channels Setup	Setup secure communication channels	Setup secure communication channels
Incident response playbooks	Create up to 3 playbooks	Create up to 5 playbooks
Major incident management playbook	-	Create or Review & Improve
Incident Response Plan	-	Create or Review & Improve
First responder training	-	Training for up to 5 participants
Incident response tabletop exercise	-	Once annually
Microsoft 365 & Defender Secure Posture Review	-	CIS Benchmark Report
Program governance	Bi-annual	Quarterly Meeting
Incident (Prepaid) IR Support	Includes 8 hours	Includes 8 hours
Locked in incident response hourly rate	$300 (USD)	$300 (USD)

Initial Assessment & Triage

Initial Assessment

Scoping

- Triaging the initial activity defines the incident's starting scope.
- As investigations progress, the scope will evolve, impacting containment and communications.
- Containment may need to expand to additional hosts or domains; communications may need updates for more stakeholders.
- Continuous re-evaluation and communication are essential to ensure response activities align with evolving risks and priorities.

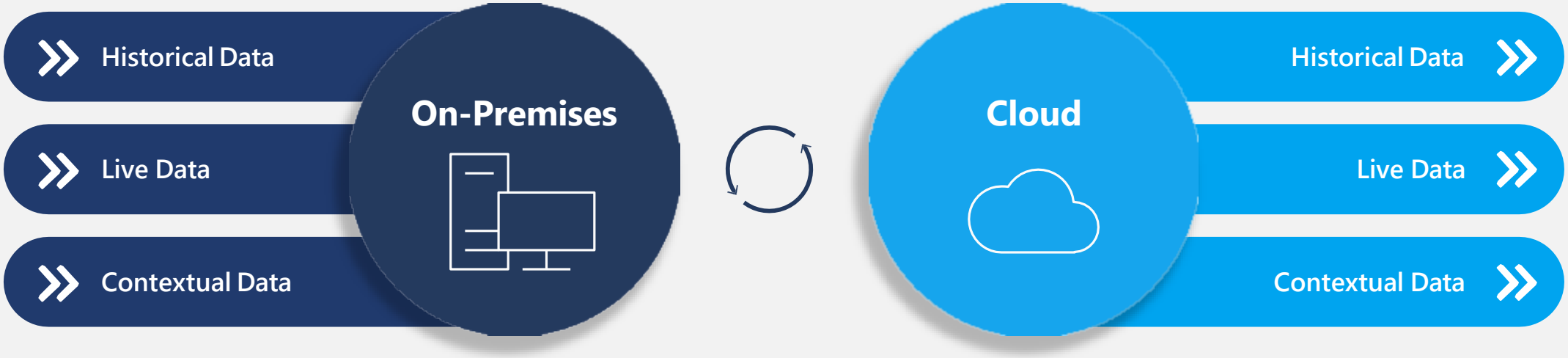
K•MICRO
THINK FORWARD

Microsoft
Solutions Partner

KMicro Incident Response & Forensics

- KMicro's approach to evidence collection is both tactical and scalable.
- It's not always practical to gather full disk images from every impacted host.
- Only the evidence that is required to help quickly paint a picture of what the Threat Actor did is gathered.

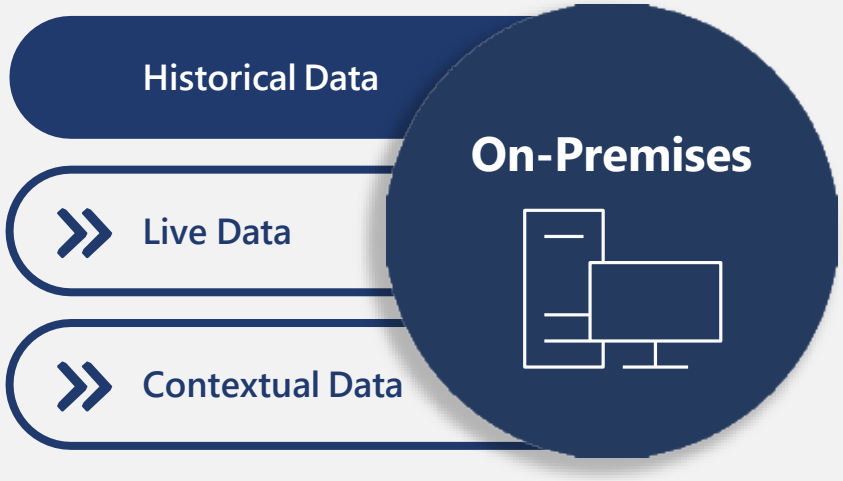
Be Aware: Often recovery efforts are prioritized, and hosts are rebuilt before forensic evidence can be collected. As a result, key pieces of intrusion timeline remain undiscovered, leaving the organization vulnerable to similar incidents in future



K•MICRO
THINK FORWARD

Microsoft
Solutions Partner

Historical Data: On-Premise



✓ Triage Images

Scalable, targeted collection of critical forensic artifacts and logs from compromised devices. These artifacts, such as system logs and memory data, are efficiently captured and securely transferred into KMicro's Azure Forensic Environment for in-depth analysis. This approach negates the need for full disk image acquisition, streamlining the investigation process and allowing rapid response while minimizing the impact on affected systems.

✓ Disk Images

A full disk image may be necessary when dealing with sophisticated attacks that involve advanced defense evasion or novel Tactics, Techniques, and Procedures (TTPs). Full disk images can be captured to gather more abstract and hidden artifacts critical for thorough analysis. These images are then securely transferred into KMicro's Azure Forensics Environment, where advanced tools and expert analysts can perform in-depth investigation to uncover the full scope of the attack.

✓ Memory Images

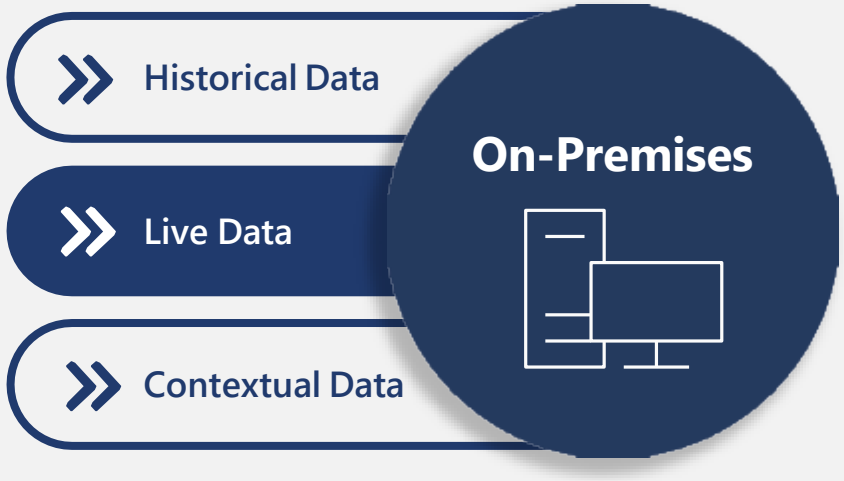
Memory images may be required for deeper analysis of key hosts, especially when dealing with novel malware or advanced Tactics, Techniques, and Procedures (TTPs) that do not leave evidence on disk. Memory images are captured and transferred can to KMicro's Azure Forensics Environment, where specialized tools and expert analysis can uncover hidden malicious activities that would otherwise go undetected in traditional disk-based forensics.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Live Data: On-Premise



✓ EDR Monitoring

If an endpoint detection and response (EDR) solution, such as Microsoft Defender for Endpoint (MDE), is not already deployed, it should be prioritized at the outset of an incident to ensure full visibility of ongoing activity within the network. MDE can be rapidly deployed across endpoints, and telemetry may be securely integrated into KMicro's Azure Incident Response Environment. This provides real-time monitoring and detection capabilities, enabling swift identification and containment of malicious activities.

✓ Active Blocking & Audit

Activating blocking mode in MDE with MDI integration is highly recommended in any incident. Combined with a robust triage process to deconflict block events, this allows real-time interdiction of malicious activity. These blocks and alerts will be securely monitored by KMicro's, enabling Incident Responders to swiftly contain threats and prevent further compromise while ensuring legitimate activities are unaffected.

✓ Custom Alerting

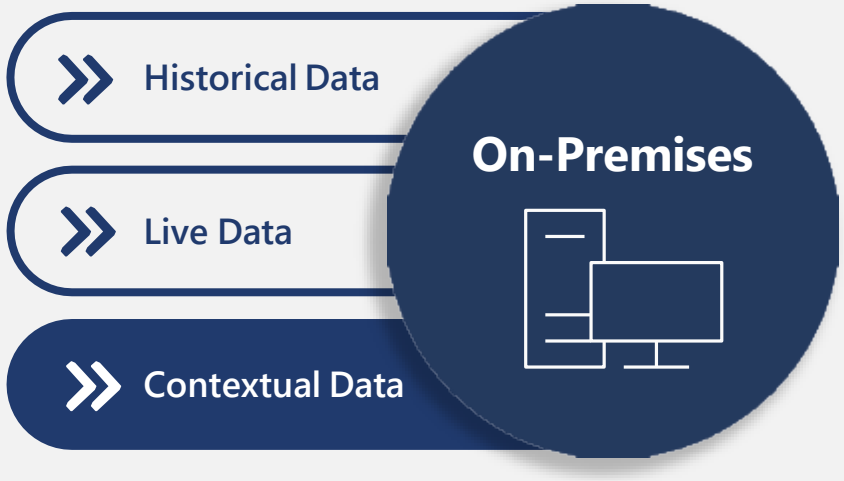
During the incident response process, responders will have the ability to create and deploy custom indicators and detections within MDE and Microsoft Sentinel. These custom alerts are seamlessly integrated, allowing for real-time monitoring and tailored detection as the analysis evolves, ensuring that emerging threats are promptly identified and addressed.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Contextual Data: On-Premise



✓ Boundary Device Logging

Network logging should be thoroughly analyzed to determine how the threat actor gained remote access to the network. This includes scrutinizing boundary devices such as firewalls, VPNs, proxies, and internet-exposed servers. By integrating this data with MDE and MDI, KMicro's Incident Response services will ensure centralized visibility, enabling comprehensive analysis of these boundary devices to trace the attacker's entry points and movement across the network.

✓ Centralized SIEM

It is a best practice to centralize key logs from across the environment into a SIEM solution, such as Microsoft Sentinel. By integrating these logs within Client's tenant or KMicro's Azure Incident Response Environment, where KMicro will enable real-time monitoring, correlation, and analysis, ensuring comprehensive visibility across the network. This centralized approach allows for faster detection, investigation, and response to emerging threats during an incident.

✓ Remote Access

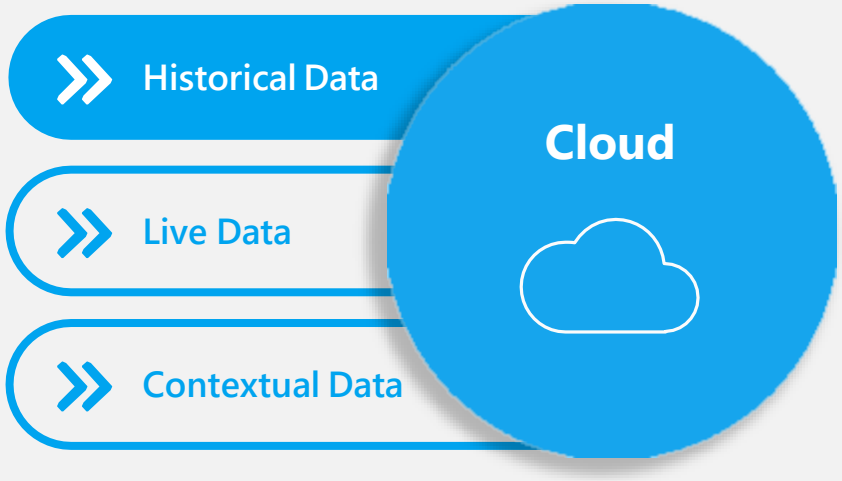
When paired with Boundary Device Logging, understanding the remote access architecture is critical. Analysts must have clear visibility into how traffic flows through the network to determine the appropriate logs to request and identify relevant indicators. With Microsoft Sentinel and KMicro's Azure Incident Response Environment, traffic patterns are analyzed in real time, enabling precise detection and monitoring of potential threats across remote access points and network boundaries.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Historical Data: Cloud



✓ Sign-in & Audit Logging

Sign-in data and admin actions performed by compromised identities are critical to cloud incident analysis. If not centralized, this data is limited to the past 30 days in Microsoft security portals (and may vary for other cloud platforms).

By integrating this logging into Microsoft Sentinel or KMicro's Azure Incident Response Environment, we ensure long-term retention and comprehensive visibility, enabling in-depth investigation of identity-based threats and admin activities beyond default logging window.

✓ Application & Activity Logs

Non-human identities and actions within cloud workloads should be scrutinized just as closely as traditional user activities. Without centralization, this logging may only be available for the past 30 days in Microsoft security portals (and may vary for other cloud platforms), potentially making it unrecoverable.

By centralizing application and activity logs in Sentinel, we ensure comprehensive, long-term retention and full visibility for in-depth analysis of all cloud-based activities, including those linked to non-human identities.

✓ Cloud Resource Artifacts

The preservation of cloud resource artifacts follows the same principles as on-premises environments: ensure resources are isolated but not deleted once identified.

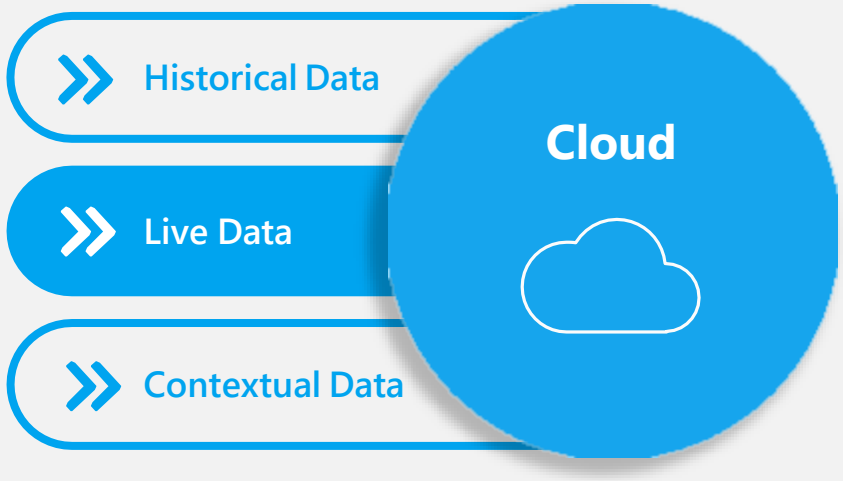
Deleting these artifacts may make them unrecoverable. By utilizing Sentinel, and KMicro's Azure Incident Response Environment, we ensure that evidence is securely preserved, enabling thorough investigation and analysis without risking the loss of critical data.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Live Data: Cloud



✓ Identity & Email Alerting

Many identity and email platforms, such as Microsoft Entra ID Identity Protection, provide alerting functionality backed by advanced algorithms to detect anomalous activity.

By integrating these alerts into Microsoft Sentinel, and KMicro's Azure Incident Response Environment, we ensure real-time monitoring and comprehensive analysis of identity and email-based threats, enabling swift detection and response to suspicious activities.

✓ Custom Alerting: Sign-in

Sign-in events for compromised identities, whether successful or failed, must be closely scrutinized for additional indicators or signs of re-compromise.

By leveraging Microsoft Sentinel and KMicro's Azure Incident Response Environment, custom alerting can be configured to monitor these events in real time, ensuring that any suspicious activity is promptly identified and mitigated, reducing the risk of further breaches.

✓ Custom Alerting: Admin

As the investigation progresses and activities performed by the threat actor are identified, custom queries and alerting mechanisms should be established to detect any additional instances of those actions.

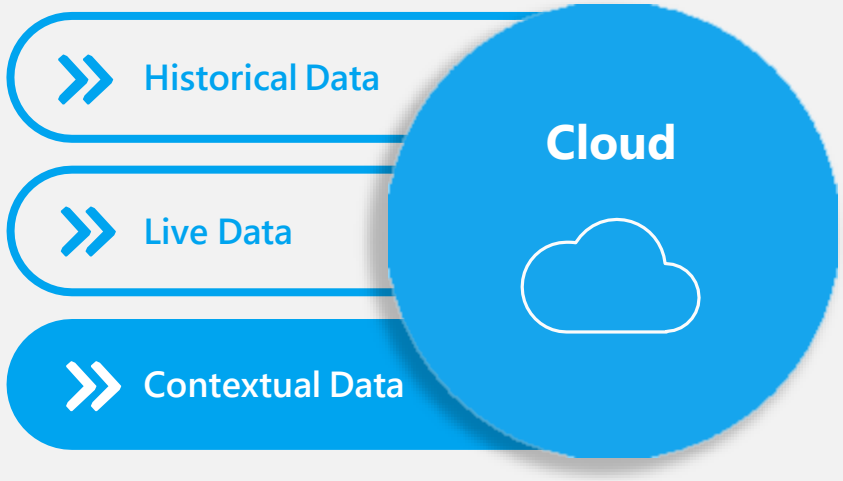
With Microsoft Sentinel and KMicro's Azure Incident Response Environment, these admin events can be monitored in real time, ensuring continuous detection of malicious activities and enabling swift containment of any further compromise.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Contextual Data: Cloud



✓ Auth & Email Flow

Understanding authentication and email flows is crucial for identifying the most relevant logging sources during an investigation.

KMicro leverages Microsoft Sentinel with integration to KMicro's Azure Incident Response Environment, where Incident Responders gain clear visibility into these flows, ensuring that the appropriate logs are captured and utilized effectively to trace threat actor activities and support a thorough investigation.

✓ Centralized SIEM

Centralizing key logs from across the multi-cloud environment into a SIEM solution, such as Microsoft Sentinel, is a best practice for effective incident response.

By integrating these logs into KMicro's Azure Incident Response Environment, Incident Response teams can interrogate data from a variety of sources in real time, enabling comprehensive threat detection, investigation, and response.

✓ Secure Posture

Understanding the boundaries between on-premises and cloud environments is critical for identifying which artifacts need to be collected and what areas may be targeted by a threat actor seeking to maintain a foothold.

Guided deployments for secure posture of M365 & Defender as part of KMicro's IR services, ensures visibility across hybrid environments, enabling proactive security best practices to be applied along with collection and monitoring of key artifacts to swiftly mitigate potential threats.

K•MICRO
THINK FORWARD

Microsoft Intelligent Security Association

Microsoft | Microsoft Verified Managed XDR Solution

Contact Info.

Let's connect! Contact us for your Managed Security Services needs.

PHONE :

(855) 564-2761

E-MAIL :

dwhite@kmicro.com
jhaifa@kmicro.com

WEBSITE :

https://kmicro.com

ADDRESS :

3525 Hyland Ave, Suite 265
Costa Mesa, CA 92626

K·MICRO

THINK FORWARD

THANK YOU