Revolutionising cybersecurity for tomorrow’s threats

Part 1: The shifting sands of cyber threats

Businesses are facing an unprecedented challenge: securing their assets against an rapidly evolving array of cyber threats. The cybersecurity battlefield is no longer confined to simple firewalls and antivirus software, and therefore traditional network based cyberdefences are no longer adequate. Instead, the threats have expanded into a complex, multidimensional space where threats emerge and mutate at an alarming rate.

The evolving threat landscape

The speed at which cyber threats are evolving is staggering. Consider these statistics:

In 2023, the average cost of a data breach reached **$4.45 million, a 15% increase over 3 years** *(IBM Cost of a Data Breach Report 2023).*

Ransomware attacks occur every 11 seconds since 2021, up from every 40 seconds in 2016 *(Cybersecurity Ventures 2022).*

95% of cybersecurity breaches are caused **by human error** *(World Economic Forum)*

The number of IoT devices is projected to **reach 29 billion by 2030, each a potential entry point for attackers** *(Statista).*

These figures illustrate a clear trend: cyber threats are becoming more frequent, more costly, and more diverse. For businesses, this means that traditional, static security measures are no longer adequate to protect them. They are facing an avalanche of threats ranging from Advanced Persistent Threats (APTs), AI-powered attacks, supply chain compromises, Cloud security vulnerabilities and often misconfigurations, IoT device exploitation and Insider threats.

Common gaps exposing businesses to cyber risks

Despite the growing sophistication of cyber threats, many businesses continue to struggle with fundamental security issues. Here are some common gaps that expose organisations to unnecessary risks:

1 **Outdated security infrastructure**

Many companies continue to rely on legacy systems that weren't designed to handle modern threats. They struggle with burden of technical debt and many find it difficult to move away from their legacy systems.

2 **Lack of comprehensive strategy**

Too often, cybersecurity is treated as an IT problem rather than a business-wide concern. Most businesses do not have a cybersecurity strategy or plan, but rather "band-aids", where cybersecurity is an afterthought and applied in pockets while leaving wide attack surfaces undefended.

3 **Insufficient employee training**

While human error is a leading cause of breaches, many organisations neglect regular, comprehensive security awareness training. Many of the most recent successful cyber-attacks have Often, even with security awareness training, it does not reduce human fallacy to zero.

4 **Inadequate third-party risk management**

As supply chains become more complex, many businesses fail to properly vet and monitor their partners' security practices. Some of the most damaging cyber-attacks in recent history were attributed to vulnerabilities in organisation's supply chain and vendor eco-system.

5 **Poor incident response planning**

Many organisations lack a well-defined, practiced plan for responding to security incidents. Even if they do, very few actually test their plans to check for effectiveness. Often, these plans are made at a point in time in history and are not updated/ refreshed to incorporate changes in corporate network/ IT setup or evolving nature of cyber threats.

6 **Neglect of cloud security**

As businesses rapidly adopt cloud services, many fail to properly secure their cloud environments or have the capability to monitor and detect for vulnerabilities, threats, or understand their cloud security posture.

7

Lack of continuous monitoring and testing

Point-in-time assessments are insufficient in a rapidly changing threat landscape. The reality is that cybersecurity is never a point-in-time thing.

8

Failure to keep pace with compliance requirements

As regulations evolve, many businesses struggle to stay compliant.

9

Insufficient focus on data privacy

With increasing privacy regulations, many organisations fail to properly manage and protect sensitive data.

10

Insider threats

Many organisations are focused on external threats alone, and do not have mechanisms to detect and thwart the threat of an insider acting with malicious intent. Password-based access controls are not sufficient to stop breach of priviledged access or an insider exporting sensitive data or such other cyber threats.

These gaps represent more than just technical oversights; they reflect a broader failure to adapt to the realities of modern cybersecurity. Traditional cybersecurity practices designed around a relatively reactive approach are not adequate for today's landscape where every traffic can potentially be malicious. We need to pivot our cybersecurity strategies to be on an offensive against the threats by assuming a breach and actively hunting threats. In the following chapters, we'll explore how a proactive, holistic approach to cybersecurity can address these gaps and prepare businesses for the threats of tomorrow.

As organisations continually expand their reliance on the use of technology to support their business, naturally, their IT infrastructure footprint will grow with new devices, assets and services. This makes their potential attack surface increasingly porous, necessitating more robust security measures.

A critical challenge in this complex landscape is the lack of complete asset visibility. Large organisations often grapple with an incomplete view of their assets and sometimes shadow IT or unauthorised devices. These elements, operating outside the purview of official IT management, pose substantial risks that are difficult to quantify and mitigate.

In the broader context of digital transformation, organisations in APAC are increasingly integrating suppliers and vendors from diverse regions into their supply chains, often with varying levels of security maturity. This integration, while necessary for growth and efficiency, introduces new vulnerabilities that are challenging to assess and manage effectively. The absence of unified insights into these complex, interconnected systems make it difficult for security professionals to make fully informed decisions regarding supply chain vulnerabilities, further complicating the already intricate landscape of cybersecurity risk management.

By understanding the evolving threat landscape and identifying common security gaps, businesses can begin to shift their cybersecurity strategies from reactive to proactive, from siloed to integrated, and from static to dynamic. This shift is not just about adopting new technologies—it's about fundamentally changing how we think about and approach cybersecurity in the digital age.

Part 2: a proactive and holistic approach to cybersecurity

Businesses have come to accept the fact that it is not a matter of IF but WHEN they will be the next victim of a cyber-attack, but many of them still are underprepared to effectively tackle the risk of cyberthreats. To address their challenges, organisations need to adopt a proactive and holistic approach to cybersecurity.

Shifting from reactive to proactive

A proactive approach to cybersecurity means anticipating and preparing for threats before they materialise, rather than simply reacting to incidents as they occur. Usually this is achieved by having, at the bare minimum, the following:

Continuous monitoring

Implementing 24/7 monitoring of all systems, networks, and endpoints.

Threat intelligence

Leveraging up-to-date threat intelligence to stay ahead of emerging risks.

Threat hunting

Assuming that one has been breached and hunt for the threats within the network to uncover them before they unleash the damage

Regular security assessments

Conducting frequent vulnerability scans and penetration tests. This includes also running simulations with the employees to guage their alertness levels to spot phishing and other such benign appearing malicious links

Predictive analytics

Using AI and machine learning to analyse and predict potential security incidents.

Adopting a holistic security posture

A holistic approach recognises that cybersecurity is not just an IT issue, but a business-wide concern. Businesses must view cybersecurity as an integral part of the entire organisation, rather than just an IT function. It recognises that effective security requires a comprehensive strategy that encompasses all aspects of the business. Afterall, cybersecurity strategies exist to support your business goals.

This means that as part of your cybersecurity program, it is necessary to be:

Closely coupled integration with business

Aligning cybersecurity with business objectives and integrating it into all processes. Such alignment includes incorporating security considerations into business decision-making processes.

Cultivating a security-aware culture

Fostering a security-aware culture throughout the organisation, including encouraging employees at all levels to take responsibility for security.

Comprehensive governance

Establishing clear security policies and procedures that apply across the entire business. There should be a corporate-wide framework for risk management that includes cyber risks and embracing accountability for security at all levels, including the C-suite and board room.

Ecosystem security

Extending security considerations to partners, vendors, and the entire supply chain. As an example, implementation of a robust vendor risk management process and ensuring security standards are maintained throughout the supply chain.

Continuous adaptation

Regularly reassessing and updating security measures and controls to address evolving threats, implementing agile security processes that can quickly adapt to new challenges and fostering a culture of continuous improvement in security practices.

Cross-functional collaboration

This means breaking down silos between IT, security, and other departments, encouraging collaboration between security teams and other business units and ensuring security is a consideration in all major business initiatives.

Human-centric security

Recognising that people are both the greatest vulnerability and the first line of defense, i.e. they are our "human firewall". We need to implement security measures that are user-friendly and don't impede productivity, which means we must balance technical controls with human factors and usability.

Metrics and reporting

Developing comprehensive security metrics that provide insights across the organisation to allow regular reporting on security status to all levels of the organisation and to drive continuous improvement.

Addressing common gaps

A proactive and holistic approach to cybersecurity addresses the common gaps exposing businesses to cyber risks by creating a comprehensive, forward-thinking security posture. By implementing continuous monitoring and threat intelligence, organisations can keep their security infrastructure up-to-date, addressing the issue of outdated systems.

The holistic nature of this approach ensures cybersecurity is treated as a business-wide concern rather than just an IT problem, fostering a security-aware culture through regular, comprehensive employee training. This strategy also emphasises robust third-party risk management and incident response planning, closing critical gaps in supply chain security and crisis preparedness.

By integrating cloud security as a fundamental component and positioning cybersecurity as a business enabler, it justifies appropriate investment and resources. The proactive stance enables continuous monitoring, testing, and adaptation to evolving compliance requirements, while also prioritising data privacy. This approach transforms cybersecurity from a reactive, siloed function into a dynamic, integrated part of business operations, effectively preparing organisations for both current and emerging threats.

Addressing these gaps systematically can enable businesses to significantly reduce their exposure to cyber risks and build a more resilient security posture.

Managed detection & response (MDR)

Managed Detection and Response (MDR) is a comprehensive cybersecurity service that combines advanced technology, analytics, and human expertise to provide continuous threat monitoring, detection, investigation, and rapid response capabilities. MDR services utilise sophisticated tools and techniques to identify potential threats, analyse suspicious activities, and respond to confirmed incidents quickly and effectively. This approach offers organisations 24/7 monitoring, access to cybersecurity experts, integration of threat intelligence, and the ability to detect and mitigate threats before they cause significant damage.

However, while MDR is a powerful tool in a cybersecurity arsenal, it is not sufficient on its own to fully protect businesses. MDR primarily focuses on detection and response, which are crucial but represent only part of a comprehensive cybersecurity strategy. It may not address other critical aspects, for example, preventive controls like access management systems, or security awareness training, or vulnerability management, or the need for long-term cybersecurity strategy development.

For example, an organisation relying solely on MDR might detect and respond to a phishing attack quickly, but without proper employee training and email filtering systems, they remain vulnerable to future attacks. Similarly, MDR might identify a breach caused by an unpatched vulnerability, but without a robust vulnerability management program, the organisation remains at risk of similar incidents. Therefore, while MDR is a valuable component, it needs to be part of a broader, holistic cybersecurity approach to truly protect businesses from the full spectrum of cyber threats.

Part 3: the future of cybersecurity: embracing proactive defense

As we've explored in previous sections, the cybersecurity landscape is constantly evolving, demanding more sophisticated and proactive approaches to defense. In this section, we'll examine how Lumen has taken the concept of Managed Detection and Response (MDR) to the next level, morphing it into what we termed as Advanced MDR, incorporating enhanced asset visibility, continuous vulnerability management, and proactive threat hunting.

The evolution from MDR to advanced MDR

While traditional MDR services have proven valuable in detecting and responding to threats, the increasing complexity of modern IT environments and the sophistication of cyber-attacks have necessitated a more comprehensive approach. An advanced MDR solution that combines capabilities of traditional MDR with the means for proactive threat detection & hunting represents an evolutionary next step in cybersecurity services.

Key Components of Advanced MDR:

1 Enhanced asset visibility

Advanced MDR begins with a foundation of comprehensive asset visibility. Combining sophisticated tools and processes to provide a more accurate and real-time view of an organisation's entire digital estate.

Comprehensive asset discovery

Advanced MDR employs a real-time, continuous discovery of all devices in an organisation's environment, including IoT, OT, IT (on cloud and on-premise) and IoMT devices. You can't protect what you can't see.

Classification and risk assessment

Automated classification of discovered assets and assessment of their risk based on factors such as their device type, behavior, and known vulnerabilities.

Asset Context

Beyond mere identification, Advanced MDR enriches asset information with contextual data, including ownership, purpose, criticality, and security posture.

2 Continuous vulnerability management

Building on enhanced asset visibility and with a comprehensive configuration details of the assets, Advanced MDR allows a continuous vulnerability management by:

Vulnerability identification

By maintaining an up-to-date database of known vulnerabilities and comparing it against the discovered assets, we can quickly identify devices with potential vulnerabilities.

Integration

We can integrate with existing vulnerability management solutions, providing them with accurate, real-time asset information to enhance their effectiveness as well as to support prioritisation through contextual information.

3 Proactive threat hunting

Perhaps the most significant value offered by an Advanced MDR solution is the value of proactive threat hunting:

Hypothesis-driven hunting

Skilled analysts develop and test hypotheses about potential threats based on the latest threat intelligence and observed patterns.

Advanced analytics

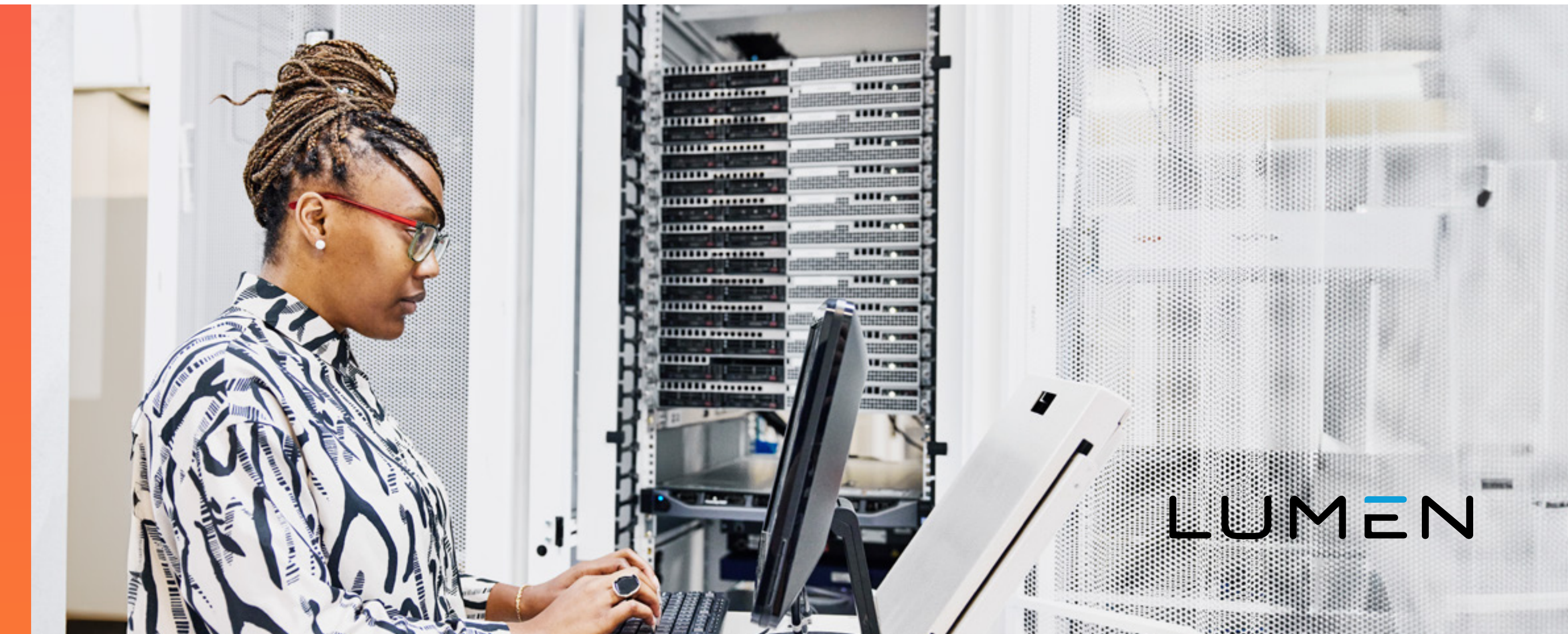
The system leverages machine learning and behavioral analytics to identify subtle indicators of compromise that might evade traditional detection methods.

Retrospective analysis

Advanced MDR can analyse historical data to uncover previously undetected threats or to investigate the full scope of an identified incident.

Customised hunting

Threat hunting activities are tailored to each organisation's specific threat landscape and risk profile.



Why advanced MDR by Lumen?

As a leading managed security service provider, with extensive experience in proactive threat detection, hunting and managed security offerings, Lumen pioneered the Advanced MDR service to help improve the overall cyberrisk posture of enterprises and help them confidently tackle the myriad of cyberthreats challenging them.

Positive impact from proactive threat hunting

Imagine your organisation as a digital city, with you as its cyber guardian. Your role is to detect and neutralise cyber threats before they cause significant damage. This process begins with forming hypotheses based on the latest threat intelligence, like a detective theorising about a case. You then test these hypotheses against your network's data flow, searching for anomalies.

In one example, Lumen's SOC detected a security anomaly on a client's firewall. A Romanian IP, known for malware, was connecting through the client's network to another external IP via Telnet. Investigation revealed this was likely related to TrickBot C2 malware distribution. The incident exposed a firewall misconfiguration allowing threat actors to use the client's network for attacks. Lumen quickly identified the issue and took corrective actions. It is important to minimise the potential damage by identifying and neutralising the threat quickly, significantly reducing the attacker's dwell time.

In some scenarios, it is important to comprehend the different types of evasion techniques. On one occasion, we detected suspicious DNS requests resembling Domain Generation Algorithm (DGA) patterns through a client's domain controller. DGAs are commonly used by threat actors for malware delivery and C2 communication. Investigation revealed the traffic originated from a device on the client's BYOD guest network. The DNS destination was flagged as malicious. Lumen escalated the issue to the client to determine if the device was a corporate asset or visitor-owned. Analysis of DNS payloads to detect malicious activities like DNS tunneling and DGA use. It demonstrates Lumen's thorough investigation process and alignment with the MITRE ATT&CK framework, enabling effective threat detection and response.

The power of integration

What sets Lumen's Advanced MDR apart is not just these individual components, but how they work together to create a truly proactive defense system:

- Asset visibility informs vulnerability management, ensuring no assets are overlooked in the security process.
- Vulnerability data enhances threat hunting by highlighting potential attack vectors.
- Threat hunting findings feed back into the asset visibility and vulnerability management processes, creating a continuous improvement cycle.
- All of these components work in concert with our MDR capabilities, 24/7 monitoring and rapid incident response.

There was another case where we suspected an elusive APT had infiltrated our client's environment. Armed with cutting-edge tools and a keen intuition, our threat hunter embarks on a digital cat-and-mouse game. Using advanced network analysis, we detected faint traces of encrypted communication during odd hours. Anomaly detection systems flag subtle changes in user behavior across multiple endpoints. Diving deeper, we uncovered a sophisticated malware strain lurking in seemingly innocuous system files. It's a hallmark of advanced persistent threats. The hunter cross-references this with the latest threat intelligence, confirming our suspicions. We traced the APT's command and control infrastructure, exposing a months-long espionage campaign. Thanks to their relentless pursuit, the company swiftly isolates compromised systems and collaborates with cybersecurity authorities to dismantle the operation, turning a potential disaster into a major victory for digital security.

There were many other occasions where the use of enhanced asset visibility were able to identify and secure several forgotten legacy systems that were putting our clients at risk.

Diverse technological landscapes, unified security

Every organisation's technological infrastructure is unique, resulting in varied attack surfaces that demand tailored security approaches. Lumen's Advanced Managed Detection and Response (AMDR) solution addresses this diversity with a flexible, cloud-centric architecture.

Conclusion

Lumen's evolution of MDR into Advanced MDR represents a significant step forward in proactive cybersecurity. By combining enhanced asset visibility, continuous vulnerability management, and proactive threat hunting with traditional MDR capabilities, Advanced MDR provides a more comprehensive, proactive, and effective approach to cybersecurity.

As we look to the future, it's clear that such proactive, integrated approaches will be crucial in defending against increasingly sophisticated cyber threats. Organisations that embrace these advanced methodologies will be better positioned to not just respond to threats, but to anticipate and prevent them, creating a more resilient and secure digital environment.

apac.lumen.com apac.mail@lumen.com

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

LUMEN