SLAYING CYBER DRAGONS

LAB³ 2023 CYBERSECURITY GUIDE

A practical guide for C-suites in managing the responsibility of cybersecurity in a cloud world

Member of
Microsoft Intelligent Security Association
Microsoft

intel | irap | ISO 27001

LAB³
FEAR LESS
ACHIEVE MORE

TABLE OF CONTENTS

FOREWORD

Fearless Cybersecurity

by Maria Thomson
Director, Microsoft Intelligent Security Association

Welcome to the LAB³ Cybersecurity Guide, from which I hope you will gain some invaluable practical tips.

It might seem an obvious statement, but cybersecurity is a non-negotiable in today's day and age. Every organisation needs highly effective, high value cybersecurity solutions to protect their customers, their employees, and of course their businesses, not to mention the personal liability of board members. It's serious and I know adds to the stress of many in the C-suite and boards.

Organisations need partnerships with technology service providers like LAB³ who have the capability to ensure there is an *'always on'* motion. Potential threats need to be identified instantly with a rapid response.

Both Microsoft and LAB³ use the term *fearless*. It's not about disregarding the very real threats, but about being agile and modernising how you approach security to address current risk exposures with ever more sophisticated cyber-attacks.

We at Microsoft believe you can be fearless with a comprehensive approach to security that's end-to-end, best-in-breed, and AI-powered.

From our years of working collaboratively with LAB³ on innovative cloud solutions, I know LAB³ are driving to safeguard customers, people, data and infrastructure in a modern approach.

As you read through this highly practical guide, you will find the current challenges to look out for and the right questions to ask of your organisation's security teams.

As one our Microsoft Intelligent Security Association (MISA) MSSPs (Managed Security Services Providers) LAB3 are one of our 'go to' partners to help mutual customers have a secure and productive working environment. Security cannot be a blocker to achieving business goals, but rather an approach which enables organisations to move with agility yet be secure at the same time.

LAB³ are an inaugural partner from the ANZ region in the MISA. More information can be found here https://aka.ms/MISA. MISA is an ecosystem of ISVs and MSSPs that have integrated their solutions with Microsoft's security technology to better defend against a world of increasing threats. LAB³ have added AI and automation expertise to the equation.

I am so pleased LAB³ is helping to educate and empower organisations using Microsoft security solutions as the path forward to actively combatting cybersecurity threats. Their Security Insight solution automates the deployment and ongoing management of Microsoft Sentinel, and is leveraged by its Security Operations Centre.

Please don't hesitate to reach out to LAB³ for any advice in the context of your organisation's needs. Their MISA membership signifies our confidence in what will be delivered.

Warm regards
Maria

INTRODUCTION

Welcome to the LAB³ 2023 Cybersecurity Guide

A practical guide for C-suites & boards in managing the responsibility of cybersecurity in a cloud world

Maybe you can relate. The burden of responsibility for cybersecurity can be overwhelming in today's cloud world. C-suites and boards are very much in the front line of responsibility for protecting the data held by their organisations and for ensuring the continued operations of any critical infrastructure and services.

With increasingly sophisticated threats and potential for far-reaching consequences, comes new and increasingly complex measures to counter these – across both IT and OT environments. The technical language, latest security advice, and rate of change can be daunting, but it is something leaders nevertheless need to be across.

Knowing what to do to better protect your organisation, employees, customers, and citizens at large is now easier.

LAB³ has created this guide to help C-suites and boards quickly get up to date with the state of play in cybersecurity today, and to know the right questions to ask of your internal teams and the experts you engage.

LAB³ is a leader in providing modern cybersecurity solutions for clients in government, financial services, healthcare, utilities, major retail and more. Across Australia and New Zealand our experts work in tandem with organisations every day to help them stay on top of cybersecurity threats and actively meet regulatory requirements.

This guide covers the shared challenges and questions LAB³ has overcome for our clients over the past 12 months including for things like:

- Large Language Models (AI workloads)
- Reliance on cloud technologies
- Increase of asymmetric / dynamic attacks

We invite you to use this guide as a trusted resource. At any time, please don't hesitate to reach out for advice that takes your unique organisational context into account.

65%

of organisations experienced a SQL injection attack in the last 12 months

The average cost of a full data centre outage has increased

38%

since 2010

DID YOU KNOW?

CYBER THREATS ARE INCREASING IN NUMBER AND SOPHISTICATION

In 2020-21 the ACSC (Australian Cyber Security Centre) received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year. This equates to one report every 7 minutes, compared to every 8 minutes the previous year.

– *ACSC Annual Cyber Threat Report, July 2021 to June 2022*

UNDERSTANDING THE CYBERSECURITY THREAT LANDSCAPE

As the first step in reviewing your management of cybersecurity in today's world, it is important to understand the current state of cyber threats, including emerging trends, prevalent attack vectors, and notable incidents.

What are your 'crown jewels', what visibility do you have and how are you protecting them?

Having visibility into your organisation's crown jewels is of paramount importance in today's cyber landscape. Organisations must identify and understand their most valuable and sensitive assets, such as customer data, intellectual property, and financial information, to effectively protect them. However, achieving this visibility can be challenging due to the complex and dynamic nature of modern IT environments.

CHALLENGE

Creating a comprehensive asset inventory and classification, including data mapping and categorisation, can be a daunting task given the volume and diversity of data within an organisation.

60%

of clients have enabled data labelling for visibility

However only

10%

of clients have enabled Data Loss Protection (DLP)

RESOLUTION

Creating an asset inventory can be accelerated using automated labelling tools such as Microsoft Purview Information Protection. Leveraging additional tools such as Microsoft Insider Risk can enable you to have visibility of how your organisation is using the data without having to define strict rules and policies, enabling you to identify areas of concern. Once visibility is achieved protecting crown jewels from data loss is a critical aspect of cybersecurity. Organisations need robust Data Loss Prevention (DLP) strategies and technologies to prevent unauthorised disclosure or leakage of sensitive information. Implementing DLP solutions enables organisations to monitor data movement, enforce access controls, and detect and prevent data exfiltration attempts. By combining content inspection, contextual analysis, and user behaviour monitoring, organisations can obtain granular visibility into data flows and implement proactive measures to prevent incidents of data loss.

CHALLENGE

With the adoption of automation on the rise, source code security risk is increasing, and the protection of source code repositories is becoming crucial. Source code represents an organisation's intellectual property and forms the foundation of its applications and software products. Emerging risks in source code data protection include unauthorised access, tampering, or leakage of code, which can have severe implications for an organisation's security and reputation.

RESOLUTION

Implementing source code access management practices, such as role-based access controls, code review processes, and strong version control mechanisms, is essential to safeguarding source code and ensuring its integrity.

ACSC recognizes ageing data as a major risk for ransomware locally

52%

of data breaches are caused by malicious attacks

TAKEAWAY

In the ever-evolving cyber landscape, your organisation must first gain visibility into your crown jewels and then implement robust protection measures to safeguard sensitive data and valuable source code from loss, leakage, and unauthorised access.

DID YOU KNOW?

THE COMPROMISE OF A SINGLE EMPLOYEE EMAIL CAN BE A PRELUDE TO A MAJOR RANSOMWARE ATTACK.

BEC (Business Email Compromise) is when cybercriminals compromise organisations via email to scam businesses out of money or goods, pretend to be business representatives, or to trick employees into revealing confidential business information. BEC is also an entry point for malicious actors to move into higher value targets within networks.

In 2021–22, the number of reported losses increased significantly to over $98 million. Nationally, the average loss per successful BEC increased to over $64,000.

— ACSC Annual Cyber Threat Report, July 2021 to June 2022

How are you protecting your ageing data? (backups, hybrid file-shares)

In today's evolving cybersecurity landscape, it is essential for organisations to pay attention to the protection of your ageing data, which includes old file shares with minimal data access protections and exposed backup files. These ageing data repositories often contain sensitive information that, if left unprotected, can become an attractive target for threat actors.

CHALLENGE

Old file shares, which may have been established years ago, often lack proper access controls and permissions. As a result, sensitive data stored within these file shares can be easily accessed by unauthorised individuals, both internally and externally.

RESOLUTION

Organisations should conduct regular audits of their file shares, implementing stringent access controls and user permissions based on the principle of least privilege. Migrating to modern data solutions (Microsoft SharePoint) can incorporate centrally managed role-based access controls and data protection with a reduced risk of SAN (Storage Area Network) hardware and software exploitation.

CHALLENGE

Exposed backup files pose another significant risk to the security of ageing data. Backups are typically created as a fail-safe mechanism to restore data in the event of a disaster or system failure. However, if backup files are not adequately protected, they can serve as a gold mine for threat actors.

RESOLUTION

It is essential for organisations to ensure that backup files are stored securely, leveraging encryption and access controls to limit unauthorised access. Backups are big targets for cybercriminals to either corrupt and/or hold to ransom. Encrypting the backup with AES-256 encryption, while cycling the keys in accordance with the organisation's risk management / risk tolerance framework. For example, what length of time will you tolerate for data exfiltration?

TAKEAWAY

As your organisation focuses on protecting your critical assets, you must not overlook the significance of safeguarding ageing data stored in old file shares and exposed backup files, and ensure robust access controls, encryption, and vulnerability management to mitigate the risks posed by potential data breaches.

Have your security controls caught up with new cloud and modern vulnerabilities?

The cyber threat landscape has witnessed a significant increase in the exploitation of cloud misconfiguration vulnerabilities. Threat actors are capitalising on inadequate cloud security practices of organisations, targeting misconfigured tokens, weak or absent authentication and validation mechanisms, and publicly accessible storage and database services. These misconfigurations present a prime opportunity for unauthorised access, data exposure, and potential breaches. To ensure robust cloud security, organisations must prioritise continuous monitoring, adopt secure configurations, and implement stringent access controls to protect cloud environments and sensitive data from malicious actors.

CHALLENGE

In today’s fast-evolving application environments, limited vulnerability management practices encompassing application, OS and cloud infrastructure pose a significant challenge. With the rapid release of new features and updates, organisations often struggle to keep up with identifying and patching vulnerabilities in their environments. This creates a favourable environment for threat actors to exploit known vulnerabilities and gain unauthorised access.

RESOLUTION

To address this, LAB^3 incorporates both an agile and comprehensive vulnerability management program with Defender for Endpoint with Qualys and a Cloud Security Posture Management (CSPM) service with Defender for Cloud (extending to hybrid cloud). This performs regular scanning, prioritisation of vulnerabilities, and timely remediation to stay ahead of potential attacks and protect critical applications in addition to providing live for hardening the deployment of cloud services.

DID YOU KNOW?

RANSOMWARE REMAINS THE MOST DESTRUCTIVE CRIME.

Top-tier ransomware groups are continuing to target Australian ‘big game’ entities; organisations that are high profile, high value, or provide critical services. Global trends indicate a decline in ‘big game’ targeting and a shift towards targeting small and medium sized businesses.

In 2020-21 the ACSC responded to 135 cyber security incidents related to ransomware, an increase of over 75 per cent compared to 2019–20.

— ACSC Annual Cyber Threat Report, July 2021 to June 2022

CHALLENGE

One critical aspect that often lacks attention is the limited alignment of data management controls between different parts of a business. Organisations may have diverse data management practices across departments, business units, or subsidiaries, leading to inconsistent security controls and increased vulnerability. A fragmented approach to data management can result in data exposure, unauthorised access, and regulatory non-compliance.

RESOLUTION

Organisations should establish a unified and centralised approach to data management, encompassing data classification, access controls, encryption, and privacy policies, ensuring consistent security measures are applied throughout the entire organisation. This can be simplified by creating 'birth rights' with role-based access control associated with data privileges to reduce management overhead not just for new hires, but also for users who change roles within the organisation.

The majority of non-government and non-FSI clients don't have defined security controls and blueprints for developers.

Defining standards for deployment reduces DevOps rework and increases your security posture.

TAKEAWAY

In an increasingly interconnected and fast-paced digital landscape, organisations must ensure security controls, cyber-awareness, and policies keep up with the evolving cloud and modern vulnerabilities to effectively safeguard against data breaches and malicious exploitation.

Can one deception compromise your entire workforce?

The cybersecurity landscape has witnessed a concerning trend where the ability of the workforce to distinguish between real and fake is diminishing, thanks to increasingly sophisticated human-like attacks. Attackers are leveraging advanced social engineering techniques, such as spear-phishing and business email compromise, to trick employees into revealing sensitive information or performing unauthorised actions. Of further concern, an emerging area for phishing is with AI Voice using generative AI enabling digital call-centres to scale without the reliance on people to do the calls. To address this challenge, organisations need to focus on enhancing their workforce cybersecurity awareness through regular and comprehensive training programs. By educating employees about the latest attack techniques, emphasising the importance of scepticism, and providing practical examples, organisations can empower their workforce to recognise and respond effectively to these dynamic threats.

With the rise of sophisticated phishing attempts, compromised accounts are also on the rise.

Reduce external digital identity fraud by

95%+

using conditional access with device validation

CHALLENGE

The rise in automation has enabled threat actors to scale up their attacks, targeting multiple individuals simultaneously. Automated attack tools, coupled with sophisticated social engineering tactics, can create a formidable challenge for organisations.

RESOLUTION

To combat this, organizations must invest in advanced threat detection and response mechanisms, leveraging trusted 3rd party technologies which include artificial intelligence and machine learning such as Microsoft Sentinel. These technologies can help identify patterns and anomalies in user behaviour, detect potential malicious activities, and provide timely alerts, allowing security teams to respond swiftly and mitigate the impact of attacks. Leveraging services which use binary validations to verify threats is no longer sufficient, understanding the 'normal-use' of services is required to protect against modern-advanced threats.

CHALLENGE

It is crucial to acknowledge that attackers only need to successfully deceive a single person within a large corporation to gain unauthorised access or compromise sensitive information. This creates a significant advantage for attackers, as the odds of successfully infiltrating the organisation are in their favour.

RESOLUTION

To counter this, organisations should adopt a multi-layered security approach that combines technical solutions, such as robust email filtering and endpoint protection, with ongoing employee training and awareness programs. By strengthening the human element of cybersecurity defences, organisations can create a collective defence mechanism that enhances their ability to thwart dynamic, human-like threats. This, in addition to vendor consolidation, can extend the cohesiveness of the security tools for 'persona anomaly detection' and reduce management overhead with limited security teams.

TAKEAWAY

In a world where human-like cyber threats are increasingly sophisticated, your organisation must prioritise cybersecurity awareness training, leverage advanced threat detection technologies, and fortify your defences against attacks that require fooling just one person to facilitate a successful breach.

INDUSTRY RESPONSE TO CYBERSECURITY RISKS IN ANZ

There are common and unique cybersecurity challenges faced by different industries and every industry is exposed.

Which industries are truly prepared for the interconnected and technology-driven future?

As organisations leverage technology to streamline processes and enhance productivity, the need for robust cybersecurity measures becomes critical.

The difference in security requirements across industries is shrinking because all sectors increasingly rely on technology for their operations. With the growing trend of workforce automation and mechanisation leveraging compute power, organisations in every industry are embracing digital transformation to improve efficiency and competitiveness. The increased reliance on technology introduces cybersecurity risks that cut across sectors. Whether it's government, manufacturing, healthcare, finance, or retail, organisations are now interconnected and share common vulnerabilities stemming from their dependence on publicly accessible and interconnected systems.

While there are common vulnerabilities, the convergence of operational technology (OT, often critical infrastructure or supply chain) and information technology (IT) in industrial sectors brings unique challenges. In manufacturing, for example, the adoption of Internet of Things (IoT) devices and interconnected systems leads to increased vulnerability to cyber threats, potentially exposing critical infrastructure to malicious actors. Similarly, the healthcare industry's reliance on interconnected medical devices and electronic health records creates new attack vectors that can compromise patient safety and privacy.

Targeting clients' data: cybersecurity attacks spare no industry in Australia

66%

of employees downloaded mobile apps without permission

280 days

average time to identify and contain a data breach

CHALLENGE

The shrinking delta for security requirements among industries underscores the need for a holistic and proactive approach to cybersecurity. Organisations must recognise that their interconnectedness and reliance on technology exposes them to shared risks. Collaboration and information sharing across industries has become essential for developing effective cybersecurity strategies and best practices.

RESOLUTION

By fostering a culture of cybersecurity awareness and investing in robust defences, organisations can mitigate the evolving threats and safeguard their operations, reputation, and customer trust in this interconnected digital landscape. This is in addition to information sharing between organisations and Managed Security Service Providers (MSSP’s) regarding threats witnessed to bolster 'threat intelligence' but also defend against a common enemy.

TAKEAWAY

In an increasingly interconnected and technology-driven world, the convergence of industries and reliance on publicly accessible or interconnected systems narrows the gap for security requirements, necessitating a collaborative and proactive approach to cybersecurity across sectors.

Are you prepared for the rising tide of localised cyber attacks in Australia and New Zealand?

In recent years there has been a significant increase in localised cyber-attacks targeting organisations across Australia and New Zealand. Threat actors have demonstrated minimal prejudice when it comes to industry type, as they often exploit vulnerabilities within organisations that handle personal data. This poses a significant risk to organisations across sectors, including healthcare, finance, retail, and government, as the personal data of individuals becomes a prime target for cybercriminals. The frequency and sophistication of these attacks highlights the urgent need for organisations in Australia and New Zealand to prioritise cybersecurity measures and implement robust safeguards to protect sensitive customer information.

Growing trend: clients demand compliance certifications and evidence of ongoing validation of controls for those with confidential data access

What is particularly alarming is that a vast majority of citizens have been impacted not just once, but multiple times through these exposures. The interconnected nature of our digital lives has amplified the impact of cyber-attacks, resulting in a cascading effect where compromised data from one breach can lead to further attacks and data breaches. This emphasises the urgent need for individuals, organisations, and regulatory bodies to take collective responsibility for cybersecurity and adopt a proactive approach in safeguarding personal information. The implications of multiple exposures to personal data not only have financial and reputational consequences for individuals but also underline the importance of stringent data protection and privacy measures to mitigate these risks effectively.

REGULATORY SOLUTION

As a result of the growing cybersecurity challenges faced by both individuals and organisations, there have been proposals for changes to legislation regarding data security requirements. Governments and regulatory bodies are recognising the need to strengthen data protection laws to ensure adequate safeguards are in place to protect individuals' personal information. These proposed legislative changes include steep penalties, including up to 30% of a company's domestic turnover, that aim to hold organisations accountable for implementing robust cybersecurity measures, enforcing breach notification protocols, and imposing stricter penalties for non-compliance. It is a crucial step towards fostering a culture of cybersecurity resilience, where organisations are incentivised to invest in robust security practices and individuals can have greater confidence in the protection of their personal data.

TAKEAWAY

As localised cyber-attacks continue to rise in Australia and New Zealand, affecting individuals across multiple exposures, proposed legislative changes emphasise the urgency for your organisation to prioritise data security and for individuals to take an active role in protecting their personal information.

Is a tick box approach enough to protect your organisation?

Performing activities like penetration tests only once a year may have been sufficient in the past, but in today's rapidly evolving threat landscape, it is no longer enough. Cybersecurity threats and attack vectors are constantly evolving, and organisations must adapt to these changes. To effectively mitigate risks, organisations need to adopt a proactive approach by conducting regular and ongoing penetration testing exercises throughout the year. This ensures that vulnerabilities are identified and addressed promptly, reducing the window of opportunity for potential attackers.

CHALLENGE

Merely meeting the bare minimum requirements for certifications does not provide continual protection throughout the year. Certifications such as ISO 27001 or SOC 2 are valuable in demonstrating a baseline level of security compliance, but they should not be treated as a one-time achievement. Cybersecurity risks and threats are not static, and compliance requirements alone do not guarantee the ability to withstand emerging threats.

RESOLUTION

Organisations should strive for a continuous improvement mindset, regularly reviewing and updating security measures, and going beyond minimum compliance requirements. This includes implementing proactive monitoring, threat intelligence, and regular security assessments to stay ahead of potential risks.

TAKEAWAY

In the face of evolving cybersecurity threats, your organisations must move beyond a tick box mentality and embrace continual vigilance, incorporating ongoing penetration testing and surpassing minimum compliance requirements to truly protect your assets and data.

Are your internal procedures battle-tested?

In today's rapidly evolving threat landscape, it is not enough for organisations to merely have a cybersecurity plan in place. They must also ensure the plan has been thoroughly tested and ratified by the board of directors. This ensures that the organisation has a clear roadmap to respond to cyber incidents effectively, minimising the potential impact on operations, reputation, and customer trust.

Testing the cybersecurity plan is crucial as it helps identify any gaps or weaknesses in the organisation's defence mechanisms, response procedures, and incident handling capabilities. Through rigorous testing, organisations can evaluate their preparedness to address real-world cyber threats and make necessary improvements. It also provides an opportunity to assess the effectiveness of incident response processes, coordination among stakeholders, and the overall resilience of the organisation's security posture.

DLP provides a significant decrease of

95%

in data exfiltration attempts for clients who undergo questioning and validation prior to external data copying

CHALLENGE

Having a tested plan is not enough on its own. It is essential for the plan to be ratified by the board of directors. Board-level involvement and endorsement demonstrates a commitment to cybersecurity from the highest levels of the organisation.

RESOLUTION

Including the board in the testing process with a 'tabletop exercise', and by securing board approval, organisations gain the necessary resources, support, and prioritisation to implement the plan effectively. It also ensures that cybersecurity is a strategic consideration and aligns with the organisation›s overall risk management and business objectives.

TAKEAWAY

Without a thoroughly tested and board-ratified cybersecurity plan, your organisation may be ill-prepared to effectively respond to cyber incidents and mitigate industry-specific cybersecurity risks, leaving your organisation vulnerable to significant financial, operational, and reputational damage.

FUTURE TRENDS AND EMERGING TECHNOLOGIES

Explore upcoming cybersecurity trends and technologies that will shape the industry.

Data sovereignty: who controls your digital fortress?

As the rapid adoption of new technologies continues to shape the digital landscape, concerns regarding data sovereignty and intellectual property (IP) ownership are at the forefront of our clients' minds. They are seeking greater control over their security tooling and data, with real-time visibility and active participation in security discussions rather than passive monthly reports. Addressing these concerns requires innovative solutions that prioritise data protection and client engagement.

Rising demand: clients embrace modern MSSPs which offer data sovereignty, visibility, and control in the client's own environment

CHALLENGE

Organisations are increasingly apprehensive about the storage and management of their sensitive data (which is often extended to all data due to data visibility limitations), as well as the ownership and protection of their intellectual property. They want assurance that their security tools and data remain within their environment, guarded against unauthorised access or potential breaches when leveraging emerging technologies. To alleviate these concerns, organisations can implement security solutions that provide on-premises or client-owned cloud-tenant options, ensuring that data sovereignty is maintained, and IP ownership is safeguarded. By empowering organisations with control over their security infrastructure, they can feel confident that their sensitive information and valuable assets are protected within their designated environment.

RESOLUTION

To address the need for enhanced data sovereignty and IP ownership, a partner security approach can often be most effective. This approach combines the advantages of using a Managed Security Service Provider (MSSP) whilst retaining the data, controls, and response from within the client's own tenancy, thus providing ownership and control. The LAB³ SOC manages the security from within a clients Azure environment, using their instance of Microsoft Sentinel, with investigation tools hosted within. This approach enables clients to maintain visibility and control over their security posture whilst also benefiting from the latest tools and technologies.

CHALLENGE

Organisations no longer want to be passive recipients of monthly security reports; they want real-time visibility into their security posture and active participation in security discussions. This demand arises from a desire to have a proactive approach to cyber threats and a need to be continuously engaged in the decision-making process. To meet this requirement, organisations should invest in security solutions that offer live, interactive dashboards and collaboration platforms. By providing organisations with access to real-time security metrics, threat intelligence, and incident response capabilities, organisations can foster a collaborative environment with their MSSP where they feel involved and empowered to make informed security decisions.

RESOLUTION

To address the need of organisations for real-time visibility and active participation, organisations can deploy interactive security platforms that provide a unified view of security operations and enable direct engagement between themselves and their service provider. LAB^3 aggregates threat and platform service health reporting within a client's Microsoft tenancy. These platforms offer customisable dashboards with real-time analytics, automated alerts for potential threats, and secure channels for collaboration and communication. This enables us to involve clients in the conversation, so clients have live transparency into their security posture when this is needed. Additionally, interactive platforms facilitate timely communication, enabling clients to take immediate action in response to emerging threats or vulnerabilities.

TAKEAWAY

To navigate the challenges arising from the rapid adoption of new technologies and data sovereignty concerns, your organisation must be empowered by MSSPs with hybrid security approaches that preserve data control, while embracing interactive platforms that provide real-time visibility and facilitate active engagement, ultimately forging a collaborative ecosystem to combat evolving cyber threats.

Is consolidating security vendors the key to future success?

Consolidating security vendors is an emerging trend that offers heightened visibility and increased efficiency through platform integrations and data sharing. While Microsoft's E5 security services are in the top right quadrant with Gartner, adopting a consolidated platform can alleviate the burden on overworked security teams.

> “ Improving risk posture is the no. 1 benefit of consolidation ”
>
> **- Gartner 2022**

CHALLENGE

One concern with consolidating security vendors is that there may be unique features which the competition provides that Microsoft does not. Organisations may require specialised solutions that excel in particular areas of cybersecurity. Relying solely on a single vendor's platform might limit the availability of best-in-class tools that cater to unique threats and vulnerabilities.

RESOLUTION

LAB³ works with organisations to review options in consolidating security vendors. However, if a single vendor's platform cannot be achieved, LAB³ works with clients to adopt a hybrid approach, combining the benefits of a consolidated security platform with targeted solutions for specific needs. By integrating the chosen platform with specialised tools, clients can achieve a balance between broad visibility and management simplification, and access to best-in-class security solutions. This approach allows clients to leverage the strengths of their consolidated vendor while still benefiting from niche tools that provide superior protection in specific areas.

TAKEAWAY

Consolidating security vendors through a carefully balanced approach can provide heightened visibility and efficiency, but your organisation should ensure they strike a balance between a consolidated platform and specialised solutions to avoid compromising on best-in-class security capabilities and to minimise the risk of dependency on a single vendor.

CYBERSECURITY GOVERNANCE AND BOARD-LEVEL AWARENESS

Understanding the role of cybersecurity governance in organisations and the importance of board-level awareness.

Are boards equipped to safeguard cybersecurity governance?

In an ever-evolving cybersecurity landscape, organisations face the imperative of bolstering governance and board-level awareness to safeguard against risks and protect sensitive information. This section explores three critical aspects: first, the rise in adopting security duty and budget segregation aligned with ISO 27001 recommendations, second, concerns over new penalty fines for data and security mismanagement, and third, the growing personal security awareness fuelled by significant local incidents. These issues compel organisations to forge proactive and collaborative security cultures, transcending challenges and reinforcing their commitment to cybersecurity.

Growing demand: boards seek regular catchups with MSSPs for strategic guidance

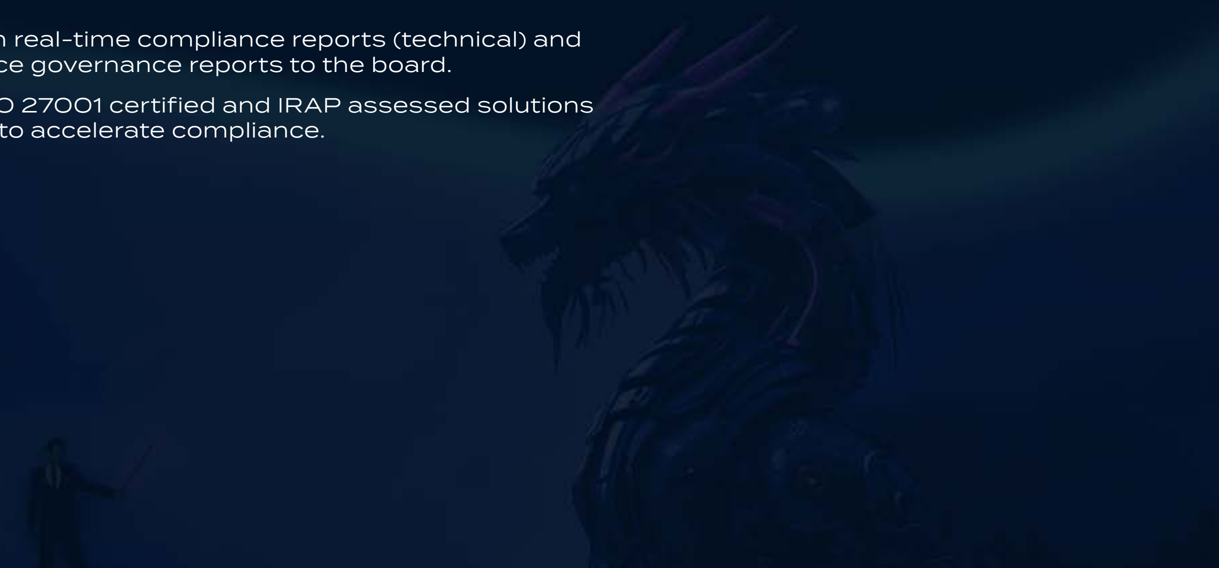
CHALLENGE

Organisations are recognising the importance of segregating security duties and budgets in line with ISO 27001 recommendations and Information Security Manual (ISM) controls. This approach ensures that responsibilities are clearly defined, reducing the risk of oversight or mismanagement. However, concerns may arise during implementation, as it requires a careful balance between accountability and collaboration. Organisations must establish effective communication channels and ensure that all stakeholders, including executives and board members, are well-informed about their respective roles and responsibilities.

RESOLUTION

Organisations should foster a culture of collaboration and knowledge sharing. By providing comprehensive training and awareness programs, they can empower employees at all levels to understand their roles in maintaining cybersecurity. LAB³ achieves this with two methods:

1. Providing both real-time compliance reports (technical) and ongoing service governance reports to the board.
2. Leveraging ISO 27001 certified and IRAP assessed solutions and products to accelerate compliance.



CHALLENGE

The establishment of new penalty fines for data and security mismanagement adds an additional layer of concern for organisations. While these fines aim to enforce accountability and encourage responsible cybersecurity practices, they can also create a sense of fear and uncertainty. The potential financial impact of such fines, coupled with potential damage to reputation, further underscores the importance of robust cybersecurity governance frameworks.

RESOLUTION

Organisations should prioritise proactive measures to prevent data and security mismanagement and continual validation in case of error. To reduce overhead LAB^3 incorporates comprehensive cybersecurity frameworks aligned with industry best practices into workplace and cloud solutions which are deployed with automation to ensure compliance. This is in addition to conducting regular risk assessments, and continuously monitoring and enhancing security controls. By taking a proactive approach and demonstrating a commitment to cybersecurity, organisations can minimise the risk of data breaches and security incidents, mitigating the potential impact of penalty fines.

CHALLENGE

The increase in major local incidents has raised the level of personal security risk among individuals. This heightened awareness presents a dual challenge for organisations. On one hand, it highlights the need for stronger security measures and increased investment in cybersecurity. On the other hand, it also introduces potential risks related to employee behaviour, such as increased susceptibility to phishing attacks or the use of personal devices on corporate networks.

RESOLUTION

Organisations should focus on comprehensive security awareness training programs that educate employees about potential threats and best practices for personal and organisational security. LAB^3 also implements segregation techniques for ‘home’ and ‘work’ life on resources that may be shared, such as mobiles. This segregation ensures protection for both the company (data exfil protection) and the employee (employee can’t see personal data). Emphasising the importance of strong passwords, multi-factor authentication, and the identification of phishing attempts can help individuals become more vigilant in their online activities. Additionally, implementing robust security measures, such as network segmentation and mobile device management policies, can help mitigate risks associated with personal devices.

TAKEAWAY

As your organisation strives to strengthen cybersecurity governance and board-level awareness, you must navigate the challenges posed by adopting security duty and budget segregation, mitigating the potential impact of penalty fines for data mismanagement, and addressing the growing personal security awareness stemming from major local incidents, all while fostering a proactive and collaborative security culture.

INSIDER RISK

There is no underestimating the potential damage of insider threats, including employees, contractors, or third parties with authorised access to sensitive systems and data.

Are your employees the weakest link or the strongest defence?

As organisations increasingly digitise their operations, the reliance on technology has grown, making the workforce a popular target for complex, human-exploitation attacks such as phishing. This poses a significant insider threat, as employees have greater access to sensitive data. To mitigate this risk, organisations need to prioritise comprehensive cybersecurity training, implement robust access controls, and foster a culture of vigilance and accountability among their employees.

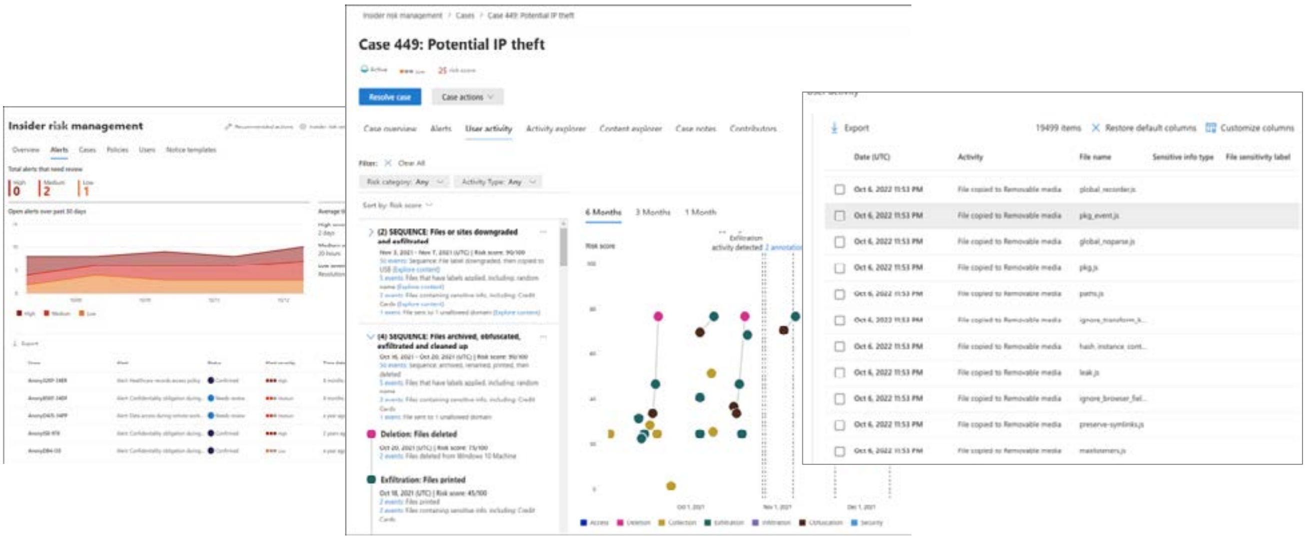
CHALLENGE

With the rapid advancement of technology, cybercriminals are employing sophisticated tactics to exploit the human element within organisations. Phishing attacks, for instance, have become increasingly nuanced and difficult to detect, posing a significant threat to the workforce. Cybercriminals may impersonate trusted individuals, craft convincing emails or messages, and manipulate employees into divulging sensitive information or granting unauthorised access. Such attacks can compromise not only individual employees but also the entire organisation's security posture.

RESOLUTION

To combat the rising threat of human-exploitation attacks, organisations must invest in comprehensive cybersecurity training for their workforce. This training should cover topics such as identifying phishing attempts, recognising social engineering tactics, and practicing secure online behaviour. By empowering employees with the knowledge and skills to identify and respond to these threats effectively, organisations can significantly reduce the likelihood of successful insider attacks. Regular training sessions and simulated phishing exercises will provide you with insight regarding the current risk factor, while also reinforcing these skills and fostering a security-conscious mindset among employees.

Insider Risk



Insider risk management

Overview · Alerts · Cases · Policies · Users · Notice templates

Total alerts that need review: High 0 · Medium 2 · Low 1

Open alerts over past 30 days

Insider risk management / Cases / Case 449: Potential IP theft

Case 449: Potential IP theft

Resolve case · Case actions

Case overview · Alerts · User activity · Activity explorer · Content explorer · Case notes · Contributors

Filter: Clear All · Risk category: Any · Activity Type: Any

Sort by: Risk score

(2) SEQUENCE: Files or sites downgraded and exfiltrated

(4) SEQUENCE: Files archived, obfuscated, exfiltrated and cleaned up

Deletion: Files deleted

Oct 20, 2021 (UTC) | Risk score: 75/100

Exfiltration: Files printed

Oct 18, 2021 (UTC) | Risk score: 45/100

Export · 19499 items · Restore default columns · Customize columns

	Date (UTC)	Activity	File name	Sensitive info type	File sensitivity label
□	Oct 6, 2022 11:53 PM	File copied to Removable media	global_recorder.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	pkg_event.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	global_noparse.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	pkg.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	paths.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	ignore_transform_k...		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	hash_instance_cont...		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	leak.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	ignore_browser_fiel...		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	preserve-symlinks.js		
□	Oct 6, 2022 11:53 PM	File copied to Removable media	maxlisteners.js		

Dashboard · Investigation · Deep Insights

CHALLENGE

As organisations embrace digital transformation, employees are granted greater access to sensitive data. While this facilitates collaboration and productivity, it also amplifies the potential damage that can be caused by insider threats. An employee with elevated privileges who decides to abuse their access or inadvertently falls victim to a cyber-attack can compromise critical systems, steal sensitive information, or disrupt operations. This places a premium on effective access controls and continuous monitoring to mitigate the risks associated with insider threats.

Redefining cybersecurity: Internal campaigns crucial in identifying vulnerabilities and strengthening protection against sophisticated attacks

RESOLUTION

To mitigate the risks posed by insider threats resulting from increased access to data, organisations must implement robust access controls and monitoring mechanisms.
This includes implementing the principle of least privilege, ensuring that employees only have access to the data and systems necessary to perform their roles. The barrier to entry is reduced using modern tools like Microsoft Insider Risk and Adaptive Data Loss Protection, which uses historical data from existing E5 security services to identify anomaly behaviour. This provides real-time monitoring and anomaly detection to identify any suspicious activities or unauthorised access attempts, enabling swift response and mitigation.

TAKEAWAY

As reliance on technology deepens and the workforce becomes a prime target for increasingly complex human-exploitation attacks, your organisation must proactively invest in comprehensive cybersecurity training, robust access controls, and vigilant monitoring to safeguard against the rising threat of insider abuses.

Are your data protection measures keeping pace with threats?

As organisations implement data protection activities to safeguard their sensitive information, the visibility of data theft incidents has increased. This section discusses two key concerns related to insider threats in this context: firstly, the rising cases of internal data theft, and secondly, the data loss caused by departing employees. Solutions to address these concerns involve the utilisation of modern data protection services, such as data labelling and monitoring tools like Microsoft Purview, and the implementation of endpoint and cloud service monitoring using adequate solutions like Defender for Endpoint and Defender for Cloud Apps.

Shocking results: across 100% of our new clients, LAB³ detected data exfiltration within 4 weeks of implementing Microsoft E5 Security (in FY22/23)

CHALLENGE

With the implementation of data protection activities and the utilisation of modern data protection services, organisations are increasingly detecting incidents of internal data theft. This rise in visibility can be attributed to improved monitoring and protection measures that now extend beyond traditional means of detecting and safeguarding against data loss caused by employees leaving. By leveraging data labelling and monitoring tools like Microsoft Purview, organisations can gain better insights into the movement and usage of their sensitive data, both within and outside the company network.

RESOLUTION

LAB³ recommends providing ongoing training for all employees and for all new starters to ensure the message is received. This can sometimes be seen as a cultural change, in which education to the employees regarding what data is theirs and how it should be managed is key.

CHALLENGE

Data loss resulting from departing employees or malicious actors has always been a concern - the implementation of data protection activities and the visibility provided by modern data protection services highlight the need for enhanced monitoring and protection measures. Organisations must ensure that data labelling and monitoring extends not only to USB devices but also to cloud services, where employees may transfer or store sensitive information before leaving the organisation.

RESOLUTION

To mitigate the risk of data loss, organisations should implement a data monitoring solution that includes data tagging, and usage of data with Workplace Services (Email, SharePoint), Endpoints, and Cloud Apps. Microsoft's E5 solution with Purview and the Defender suite enables a simple continuous monitoring solution that is already embedded into the existing services (Office365, Defender Suite). It provides monitoring of endpoints and applications used by employees, allowing organisations to detect and prevent unauthorised access, sharing, or leakage of sensitive data. By closely monitoring cloud services, organisations can proactively identify any suspicious or non-compliant activities, reducing the likelihood of data loss incidents associated with departing employees.

TAKEAWAY

With the increase in data theft incidents resulting from the implementation of data protection activities, your organisation must adopt strategies to encompass advanced monitoring and protection measures, leveraging data labelling and monitoring tools alongside endpoint and cloud service monitoring, to effectively combat insider threats and safeguard sensitive information.

CYBERSECURITY SKILLS AND WORKFORCE CHALLENGES

Understand the skills gap in the cybersecurity industry and strategies to address it.

Are cybersecurity teams equipped to handle the growing threat landscape?

The cybersecurity industry is facing significant challenges related to overworked employees and a lack of specialised skills. Security teams are overwhelmed with the constant need to juggle day-to-day defence activities and project work, further exacerbated by the increasing number of security tools and the resulting noise. However, there are potential solutions to address these concerns. Automation can play a crucial role in reducing the burden on security employees by assisting them in managing the workload. Additionally, partnering with a Managed Security Service Provider (MSSP) can offer flexibility and round-the-clock coverage, ensuring comprehensive security operations.

CHALLENGE

One of the major concerns in the cybersecurity industry is the high workload and constant firefighting that security teams experience. The need to balance ongoing defence operations (Business as Usual or BAU) with project work puts immense pressure on employees, leading to burnout and potential gaps in security coverage. This situation is further compounded by the proliferation of security tools, which generate a significant amount of noise that needs to be managed.

RESOLUTION

Automation can be a valuable ally in reducing the stress and workload for cybersecurity employees. By automating routine and repetitive tasks, such as log analysis, threat hunting, and vulnerability scanning, security teams can free up their time to focus on critical issues and strategic initiatives. Automation can also assist in handling the increased visibility created by multiple security tools, helping to streamline and prioritise alerts and incidents. In addition, this also increases governance and visibility while reducing human error. LAB^3 does this by using 'Security Orchestration, Automation and Response' (SOAR) playbooks deployed into client environments, reducing the operational workload by 30% on average. Implementing intelligent automation systems and leveraging machine learning algorithms can significantly enhance the efficiency and effectiveness of security operations, allowing employees to work smarter, not harder.

CHALLENGE

Another pressing concern in the cybersecurity industry is the significant skill gaps in specialised areas. As cyber threats become more sophisticated, organisations require professionals with advanced knowledge in areas such as threat intelligence, incident response, and cloud security. However, finding individuals with these specialised skills is a major challenge, leading to talent shortages and increased competition for skilled personnel.

Cyber skills shortage to hit 30,000 in four years

- AFR 2022

RESOLUTION

Collaborating with a Managed Security Service Provider (MSSP) can be an effective solution to overcome skill gaps and ensure 24x7 coverage. MSSPs have dedicated teams of cybersecurity experts with specialised skills and experience across various domains. By engaging an MSSP, organisations can access a broader range of expertise, including niche areas that are hard to find in-house. To accelerate self-growth from employees creating a training program and providing hands on experience accelerates the uplift in confidence and skills for security teams. LAB³ uses a lab environment called *Security Insight Cyber Lab* to perform blue and red teaming training exercises.

TAKEAWAY

By leveraging automation as a means to reduce workload, and partnering with Managed Security Service Providers (MSSPs) for specialised expertise and round-the-clock coverage, your organisation can alleviate the burden on overworked employees and bridge skill gaps, enabling effective cybersecurity defence in the face of increasing challenges.

SUPPLY-CHAIN RISK MANAGEMENT

Be aware of the risks associated with third-party vendors and supply chain vulnerabilities.

Are your vendor certifications truly securing your supply chain?

In today's rapidly evolving cybersecurity landscape, relying solely on vendor certifications is no longer sufficient to manage supply chain risks. Organisations must enhance their vendor onboarding and offboarding processes to prevent former partners from accessing sensitive data. Additionally, there is a growing need to closely scrutinise the extent of data shared with partners and implement robust mechanisms for continuous validation of data access and identity events. By prioritising these measures, organisations can mitigate the risk of data compromise and protect their customers from potential breaches.

Alarming surge in vulnerabilities detected among companies with extensive partner/broker networks and weak security protocols

CHALLENGE

Traditional reliance on vendor certifications has become inadequate as a standalone approach for managing supply chain risks. While certifications provide initial validation, they lack ongoing evaluation to ensure the vendors maintain necessary security standards. This poses a significant concern as cyber threats evolve rapidly, and vendors may become vulnerable to new attacks. To address this issue, organisations should augment their assessment process by conducting regular audits, vulnerability scans, and penetration tests to verify that vendors uphold the required security measures throughout the entire business relationship.

RESOLUTION

To bolster supply chain risk management, organisations need to focus on enhancing their vendor onboarding and offboarding processes. When onboarding vendors, thorough due diligence should be conducted, including comprehensive background checks, assessing their security posture, and evaluating their incident response capabilities. Equally important is establishing well-defined procedures for terminating vendor relationships and ensuring that all access privileges are promptly revoked. By implementing robust processes, organisations can minimise the chances of former partners retaining unauthorised access to sensitive data.

CHALLENGE

The increasing volume of data shared with partners amplifies the risk of compromise, particularly if a partner's security defences are breached. It is crucial for organisations to scrutinize the extent of data shared and assess the necessity of each data element. Additionally, continuous validation of data access and identity events becomes imperative to detect potential compromises early on. Without such validation, a compromised partner could unknowingly facilitate the compromise of the organisation's systems and compromise their data integrity.

RESOLUTION

To address the concern of compromised partners affecting their data, organisations should implement stringent controls to validate data access and identity events continually. This includes adopting multifactor authentication, monitoring access logs for suspicious activities, and implementing real-time alerts for any anomalous behaviour. LAB³ uses special dashboards deployed with our product Security Insight onto Microsoft Sentinel to show intercompany authentications and data usage to enable regular security assessments. This identifies potential vulnerabilities in partner systems, and incident response plans should be established to minimise the impact of a compromise. By implementing these measures, organisations can proactively detect and respond to any potential supply chain breaches, ensuring the protection of data.

TAKEAWAY

In an era where vendor certifications fall short and data breaches loom, organisations must rethink their supply chain risk management strategies to fortify their defences and safeguard client data from compromise.

SECURITY INCIDENT RESPONSE AND REMEDIATION

Discover incident response strategies and best practices to mitigate the impact of security incidents.

Are you ready to take charge of your data and security?

There has been an increased trend among our clients wishing to retain their data for both security and visibility purposes. One key aspect of this trend is the preference to host the Security Information and Event Management (SIEM) solution and data within their own environment. Clients are motivated by the need to maintain control over their sensitive information and reduce reliance on external vendors. By hosting the SIEM internally, organisations can closely monitor and safeguard their data, ensuring that it remains within their trusted infrastructure.

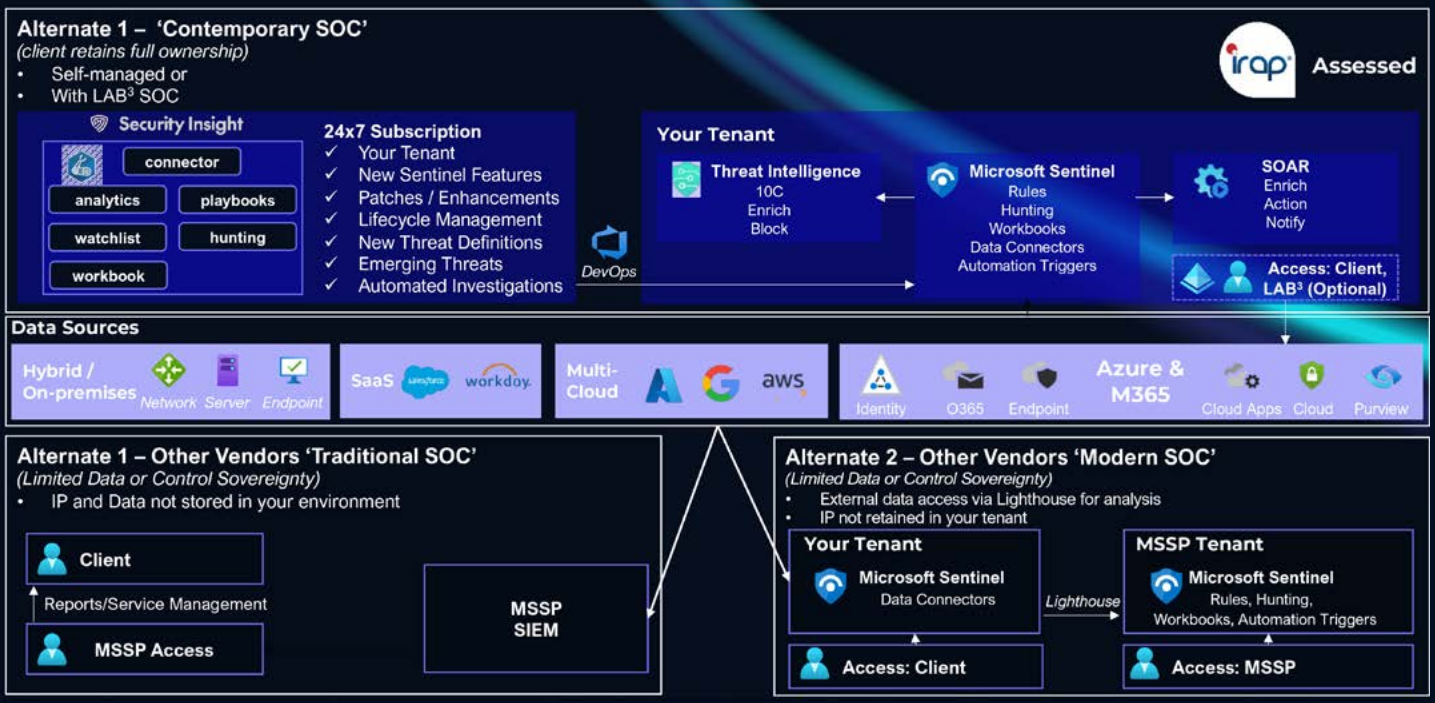
CHALLENGE

In addition to hosting the SIEM internally, clients working with Managed Security Service Providers (MSSPs) are insisting on the retention of intellectual property (IP) within their own environment. This includes critical components such as rule definitions, dashboards, and other configurations specific to their security environment. Retaining the IP provides clients with a greater sense of ownership and control, allowing them to tailor their security operations to their unique requirements and maintain the confidentiality of their security practices.

RESOLUTION

With the birth of Cloud technologies, it is now easier to have a shared responsibility model while retaining data and control sovereignty. LAB3 uses Security Insight to perform lifecycle management of client's Microsoft Sentinel environments that reside in their tenancy. This reduces the operational overhead of managing many SIEMs and provides transparency to clients. It extends beyond Security Event management (typical use of a SIEM) and provides Threat Intelligence for both proactive blocking of threats across the Microsoft security suite (typical home to Identity and Endpoint services) and SOAR capabilities, and so reduces incident fatigue and response time.

Data and Control Sovereignty



Alternate 1 – 'Contemporary SOC'
(client retains full ownership)
- Self-managed or
- With LAB³ SOC

irap Assessed

Security Insight: connector, analytics, playbooks, watchlist, hunting, workbook

24x7 Subscription
✓ Your Tenant
✓ New Sentinel Features
✓ Patches / Enhancements
✓ Lifecycle Management
✓ New Threat Definitions
✓ Emerging Threats
✓ Automated Investigations

DevOps

Your Tenant

Threat Intelligence: 10C, Enrich, Block

Microsoft Sentinel: Rules, Hunting, Workbooks, Data Connectors, Automation Triggers

SOAR: Enrich, Action, Notify

Access: Client, LAB³ (Optional)

Data Sources

Hybrid / On-premises: Network, Server, Endpoint

SaaS: salesforce, workday.

Multi-Cloud: Azure, Google, aws

Azure & M365: Identity, O365, Endpoint, Cloud Apps, Cloud, Purview

Alternate 1 – Other Vendors 'Traditional SOC'
(Limited Data or Control Sovereignty)
- IP and Data not stored in your environment

Client
Reports/Service Management
MSSP Access
MSSP SIEM

Alternate 2 – Other Vendors 'Modern SOC'
(Limited Data or Control Sovereignty)
- External data access via Lighthouse for analysis
- IP not retained in your tenant

Your Tenant: Microsoft Sentinel, Data Connectors
Lighthouse
MSSP Tenant: Microsoft Sentinel, Rules, Hunting, Workbooks, Automation Triggers
Access: Client
Access: MSSP

CHALLENGE

Clients are seeking to establish a partnership with MSSPs that goes beyond traditional vendor relationships. They aim to uplift internal visibility and enhance their own security capabilities by collaborating closely with MSSPs. This entails having access to skilled resources from the MSSP, enabling knowledge transfer and skill development within the client's organisation. By fostering this collaborative approach, clients can better leverage the expertise of the MSSP while simultaneously building their internal capabilities and gaining a deeper understanding of their security posture.

RESOLUTION

Clients provide access for the LAB³ SOC to work from within their environment. This provides transparency and ensures control for the client. There are live communications provided between both teams and both teams work as an extension of each other. This enables the client to enhance their own security capabilities and leverage LAB³ as the escalation expertise and to provide out of hours coverage.

TAKEAWAY

In the ever-changing cybersecurity landscape, it is time for your organisation to redefine your relationships with vendors and MSSPs. Seek and retain control, enhance visibility, and access skilled resources, all of which will empower your organisation to proactively protect your data and assets.

Is automation the answer to efficient incident response?

The cybersecurity landscape is constantly evolving, and organisations are facing an increase in security visibility and threats, leading to a surge in the number of alerts that need to be investigated. To effectively respond to incidents, organisations are now required to act faster to contain and reduce risk. However, limited security teams often struggle with the overwhelming volume of alerts, making it challenging to prioritise and respond in a timely manner. This has led to a growing demand for Security Orchestration, Automation, and Response (SOAR) solutions, which leverage automation to reduce noise and response time, enabling security teams to focus on what truly matters and enhance their incident response capabilities.

Automation-driven alert and incident tuning achieves over

60%

reduction in noise

CHALLENGE

Implementing a SOAR platform can be complex, as it requires a deep understanding of security operations and often collaboration with DevOps teams. It involves integrating threat intelligence to perform the initial enrichment tasks of Level 1 analysts, enhancing the accuracy and efficiency of incident response.

RESOLUTION

LAB^3, as a leading provider of cybersecurity solutions, leverages its Security Insight product in conjunction with a SOAR platform to effectively manage the entire lifecycle of the SOAR platform. Security Insight can perform the enrichment, action, and notification functions of the investigation to reduce response and containment times (typical investigation completed under 2 minutes from discovery). This does not replace the SOC team but adds value by performing repetitive activities and as such enables the SOC team to focus on investigating potential threats. Security Insight uses a micro-service integrated approach to not only streamline the implementation and management of the platform but also reduces the overall management overhead, allowing organisations to maximise the benefits of automation and orchestration.

TAKEAWAY

As your organisation faces a deluge of security alerts and strives to respond swiftly to incidents, the adoption of SOAR solutions becomes imperative, driving the need for intelligent automation and orchestration to reduce noise, expedite response times, and allow security teams to prioritise what truly matters in an increasingly complex threat landscape.

IT is not 9 to 5 anymore: How do you ensure 24x7 cybersecurity protection?

As the cybersecurity landscape evolves and threats become more sophisticated, there is a growing realisation among organisations that the standard 9-5 working hours are inadequate for addressing security incidents effectively. Organisations now recognize the need for true 24x7 coverage to ensure timely detection, response, and remediation of security incidents. This requirement stems from the understanding that technology and security do not operate within a defined schedule and that threats can arise at any time. In response to this need, organisations are seeking assistance from external Managed Security Service Providers (MSSPs) to augment their internal security teams and provide round-the-clock coverage.

CHALLENGE

However, organisations are not just looking for MSSPs that offer basic incident alerting through traffic lights on a Security Information and Event Management (SIEM) dashboard. They require MSSPs that go beyond these surface-level indicators and can provide comprehensive investigation and remediation services. Simply relying on automated alerts and traffic lights does not suffice in today's threat landscape.

RESOLUTION

To reduce noise to organisations and containment time, LAB³ recommends organisations provide their SOC with access to supporting security services such as Azure Active Directory and Defender for Endpoint. Organisations need MSSPs that can analyse and investigate security incidents, validate the severity and impact, perform forensic analysis, and provide actionable recommendations for remediation. The goal is for organisations to have a trusted partner who can actively respond to incidents, collaborate with internal teams, and help navigate the complex landscape of cybersecurity threats.

TAKEAWAY

In an ever-evolving threat landscape your organisation needs true 24x7 coverage. Consider external Managed Security Service Providers (MSSPs) that not only provide continuous monitoring but also go beyond surface-level alerts to investigate, validate, and remediate security incidents effectively.

THREAT INTELLIGENCE AND CYBER THREAT HUNTING

Explore threat intelligence sources, techniques, and the importance of proactive threat hunting.

Are you harnessing the power of threat intelligence to stay ahead of cyber threats?

Decoding reality: navigating >1M daily intelligence reports from >50 sources, to unravel the truth amidst information overload

In today's dynamic and ever-evolving cybersecurity landscape, threat intelligence plays a crucial role in defending against sophisticated cyber threats. Traditionally, threat intelligence has been utilised for validation purposes, helping organisations identify and understand the threats they face. However, the true value of threat intelligence lies in its ability to enable proactive blocking of threats before they can cause harm. By leveraging real-time threat intelligence feeds, advanced analytics, and automation, organisations can take proactive measures to block malicious activities, disrupt threat actors, and safeguard their digital assets.

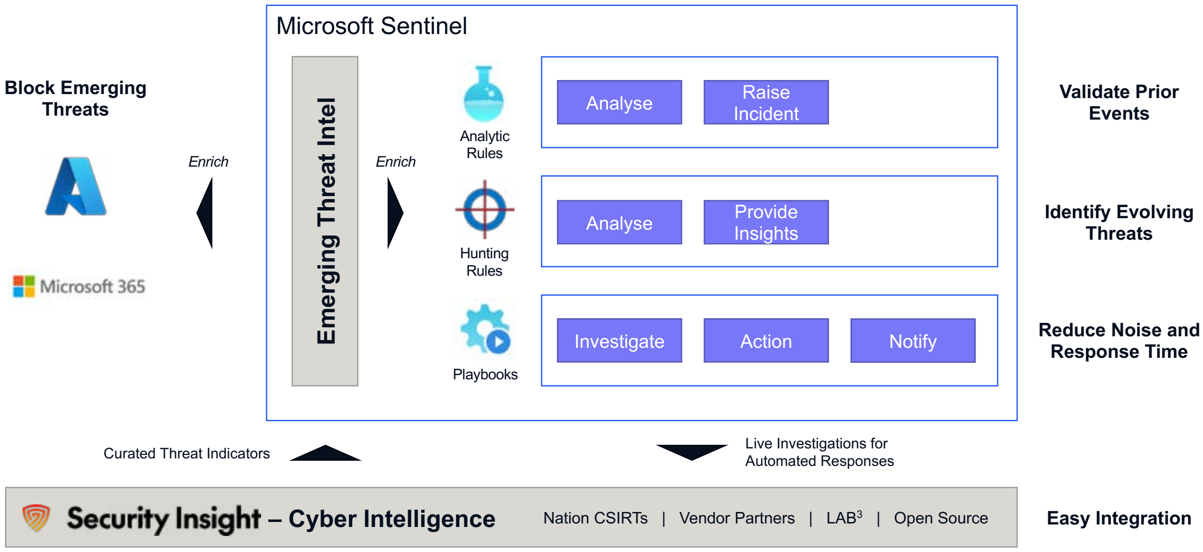
The shift from passive validation to proactive blocking allows organisations to stay one step ahead of cybercriminals. Rather than solely relying on post-incident analysis, organisations can use threat intelligence to implement proactive defence measures that enhance their overall security posture. This approach involves integrating threat intelligence into security solutions, such as intrusion prevention systems (IPS), firewalls, and security information and event management (SIEM) platforms, to automatically detect and block known threats in real-time. By leveraging threat intelligence for proactive blocking, organisations can effectively reduce their attack surface, minimize the impact of cyber threats, and improve their ability to thwart sophisticated attacks before they can exploit vulnerabilities.

TAKEAWAY

In the dynamic world of cybersecurity, leveraging threat intelligence for proactive blocking transforms organisations from passive defenders to proactive disruptors, enabling them to anticipate, block, and neutralise threats before they can cause significant harm.

LAB³ Cyber Intelligence And Response

Modern Technology



Are you seeing the full picture of cyber threats?

CHALLENGE

The traditional approach to Threat Intelligence has primarily focused on monitoring and analysing indicators of compromise (IOCs) from the clear web. However, as cybercriminals continue to exploit the anonymity and underground networks offered by the surface, deep, and dark web, organisations must expand their scope of Threat Intelligence to encompass these hidden realms.

RESOLUTION

By incorporating surface, deep-web, and dark-web monitoring into their Threat Intelligence programs, organisations gain valuable insights into emerging threats, malicious activities, and potential data breaches that may not be readily visible on the clear web.

Surface web monitoring provides visibility into publicly accessible websites and forums where cybercriminals may discuss tactics, share tools, or sell stolen data. Deep-web monitoring delves deeper into password-protected platforms, private forums, and marketplaces that require specific access credentials. Dark-web monitoring, which requires specialised tools and techniques, focuses on the encrypted and anonymous networks where illicit activities flourish, such as illegal marketplaces for stolen data, hacking tools, and other cybercriminal services. By monitoring and analysing activities across the surface, deep, and dark web, organisations can proactively identify threats, understand adversary tactics, and take appropriate measures to protect their assets.

TAKEAWAY

As cybercriminals increasingly operate in the hidden corners of the web, your organisation must extend your Threat Intelligence efforts beyond the surface, dive into the deep, and explore the darkness to stay ahead of evolving threats and protect your digital assets.

How can Threat Intelligence shield organisations against ever-evolving asymmetric and dynamic cyber-attacks?

CHALLENGE

Increased reliance on asymmetric attacks, such as zero-day exploits and polymorphic malware, has made traditional signature-based detection methods less effective in identifying and mitigating advanced cyber threats. Attackers are constantly evolving their tactics and employing sophisticated techniques to bypass signature-based defences, making it increasingly challenging for organisations to detect and respond to these threats. In this context, the role of Threat Intelligence becomes crucial in helping organisations stay one step ahead of attackers.

RESOLUTION

Threat Intelligence provides valuable insights into the tactics, techniques, and procedures (TTPs) used by threat actors. By leveraging Threat Intelligence feeds, organisations gain access to up-to-date information about emerging threats, indicators of compromise (IOCs), and attack patterns. This intelligence enables proactive identification of potential threats and the development of proactive defence strategies. It allows security teams to correlate real-time security events with threat intelligence data, enhancing the ability to detect and respond to sophisticated attacks that may not be identified by traditional signature-based detection methods.

In addition to identifying known threats, Threat Intelligence also assists in uncovering new and unknown threats. By analysing and correlating disparate data sources, including open-source intelligence, dark web monitoring, and information sharing platforms, organisations can identify patterns and indicators that may indicate the presence of previously unidentified threats. This proactive approach to threat hunting helps organisations anticipate and respond to emerging threats before they can cause significant damage.

TAKEAWAY

As attackers continuously evolve their techniques to bypass traditional defences, embracing Threat Intelligence will empower your organisation to proactively protect against advanced and asymmetric cyber threats by leveraging real-time insights and anticipating emerging attack patterns.

CLOUD SECURITY

Examine the security challenges associated with cloud computing and strategies for securing cloud environments.

Is your cloud security strategy evolving with cloud 2.0 transformation?

The rapid adoption of cloud services has prompted our clients to re-evaluate and rebuild their cloud environments, focusing on Cloud 2.0 Transformation rather than a simple transition. This transformation is driven by the need to enhance the scalability, governance, and security of cloud environments. Clients are realising that relying solely on traditional security views from on-premises infrastructure is insufficient to address the unique vulnerabilities and challenges presented by the cloud. To effectively secure their cloud environments, clients must embrace a modern approach that incorporates specialised tools such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP).

Unveiling the daunting security refactoring task in cloud environments: companies awaken to high-risk exposures in production services

CHALLENGE

In this era of Cloud 2.0 Transformation, clients are recognising the limitations of applying legacy security practices designed for on-premises environments to the cloud. The dynamic and elastic nature of the cloud introduces new vulnerabilities that require a different security perspective. It is no longer enough to rely on traditional perimeter-based security measures; instead, clients must adopt a holistic and scalable approach to cloud governance and security. By rebuilding their cloud environments with a cloud-native mindset, clients can leverage the inherent benefits of the cloud while proactively addressing the evolving threat landscape.

RESOLUTION

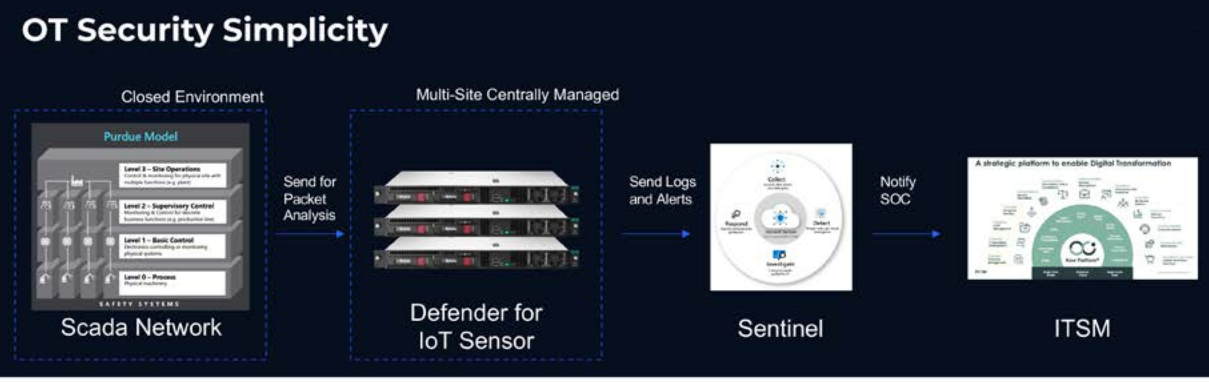
To achieve the desired level of governance and security in their cloud environments, clients must integrate specialised tools such as CSPM and CWPP. Cloud Security Posture Management tools provide continuous monitoring and assessment of cloud resources, enabling clients to identify misconfigurations, non-compliant resources, and security risks. On the other hand, Cloud Workload Protection Platforms help clients secure their cloud workloads, providing advanced threat detection, vulnerability management, and workload-specific security controls. By incorporating these new tools into their cloud security strategy, clients can enhance their ability to detect, protect, and respond to cloud-specific threats and vulnerabilities.

TAKEAWAY

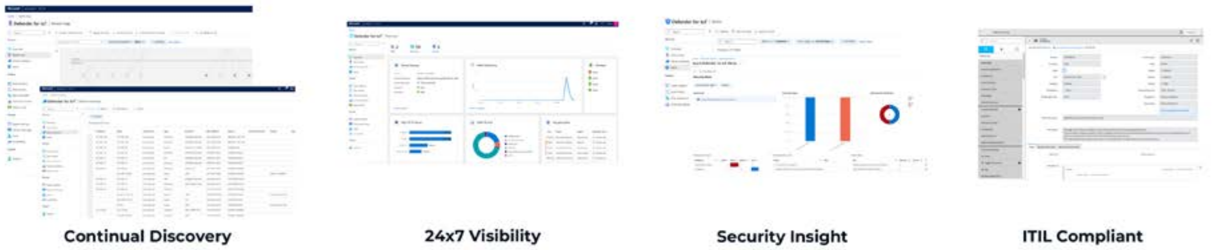
In the age of Cloud 2.0 Transformation, your organisation must rebuild your cloud environments with a cloud-native mindset and embrace specialised tools like CSPM and CWPP to uplift scalable governance and security, recognising that traditional security views from on-premises fall short in addressing the unique vulnerabilities and challenges of the cloud.

OPERATIONAL TECHNOLOGY (OT) SECURITY

Explore the security risks associated with Operational Technology (OT) systems and strategies for securing critical infrastructure.


OT Security Simplicity
Closed Environment
Purdue Model
Level 3 – Site Operations
Control & monitoring for physical site with multiple functions (e.g. plant)
Level 2 – Supervisory Control
Monitoring & Control for discrete business functions (e.g. production line)
Level 1 – Basic Control
Electronics controlling or monitoring physical systems
Level 0 – Process
Physical machinery
SAFETY SYSTEMS
Scada Network
Send for Packet Analysis
Multi-Site Centrally Managed
Defender for IoT Sensor
Send Logs and Alerts
Collect
Respond
Detect
Investigate
Sentinel
Notify SOC
A strategic platform to enable Digital Transformation
Now Platform
ITSM

LAB3 Security Fusion powered by Defender for IoT provides you with



Are OT environments vulnerable in the shadows?

In an increasingly interconnected world, boards must ensure that IT and Security teams are equipped to handle operational technology (OT) environments, despite their limited visibility and documentation. There are three key concerns. First, limited architecture and documentation for handover to IT teams. Next, ageing hardware and technology standards. And thirdly, the emergence of new problems stemming from different processes, including potential injury risks.

CHALLENGE

A major challenges in securing OT environments is the lack of comprehensive architecture and documentation available to IT teams. This limited visibility hampers their ability to understand and protect critical OT systems effectively. To address this concern, organisations should establish robust knowledge transfer processes that facilitate the transfer of information from OT teams to IT teams. This should include detailed documentation of OT infrastructure, network diagrams, system configurations, and standard operating procedures. By promoting knowledge sharing and collaboration between the two teams, organisations can enhance their understanding of OT systems and develop effective security measures.

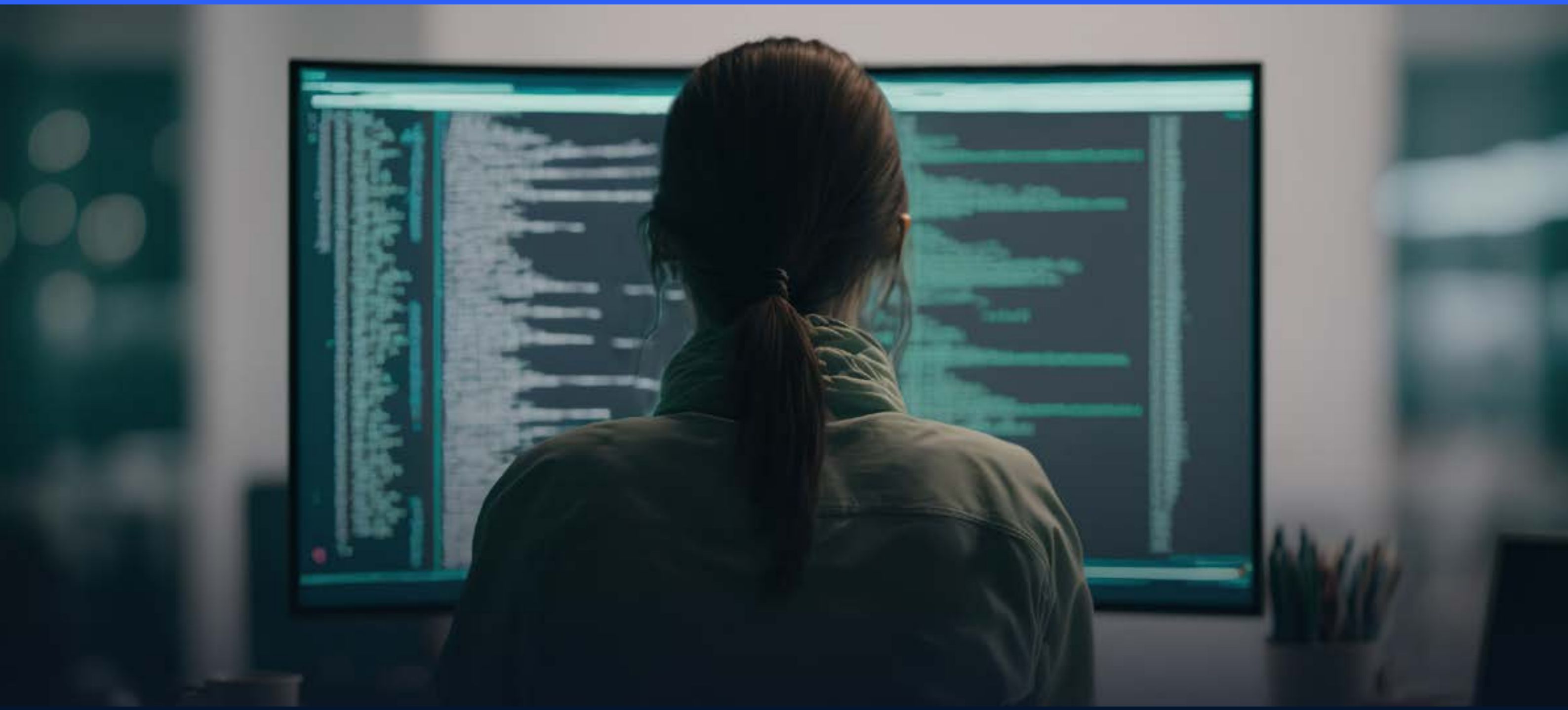
Further, many OT environments rely on ageing hardware and outdated technology standards, making them vulnerable to cyber threats. Legacy systems often lack the necessary security features and updates, increasing the risk of successful attacks.

RESOLUTION

If you are not able to modernise the OT infrastructure by replacing outdated hardware, upgrading software, and adopting industry-standard security practices, LAB³ recommends implementing continuous monitoring and vulnerability management programs which can help identify and address security gaps in a proactive manner. Solutions using technology like Microsoft Defender for IoT can provide visibility and protection even for entities with no internet access. By prioritising the modernisation of OT systems, organisations can improve their overall security posture and better protect critical assets.

TAKEAWAY

Embracing the complexities of securing operational technology (OT) environments requires your organisation's board to empower their IT and Security teams with comprehensive knowledge transfer, modernisation initiatives, and integrated risk management strategies, enabling your organisations to safeguard critical assets and protect against emerging threats.



Are large language models empowering cyber adversaries and making it easier for cybercriminals to attack critical infrastructure?

The increasing focus of state-based cybercriminals on critical infrastructure and operational technology (OT) environments poses a significant threat. Adding to this concern is the reduced skill gap of cybercriminals, as LLM (Large Language Models) and AI models enable anyone to exploit vulnerabilities in ageing OT systems. Addressing these challenges requires a multifaceted approach, including enhancing security measures, investing in skill development, and modernising OT environments.

CHALLENGE

One of the pressing concerns in OT security is the rise of state-based cybercriminals targeting critical infrastructure and OT environments. These malicious actors possess sophisticated resources and capabilities, making them a formidable threat. Their intent to disrupt essential services, compromise national security, or gain political leverage raises the stakes for protecting OT systems. As critical infrastructure becomes increasingly interconnected and reliant on digital technologies, the potential consequences of successful attacks are dire.

RESOLUTION

To mitigate the risks associated with state-based cybercriminals targeting critical infrastructure and OT environments, your organisation needs to enhance your security measures and build resilience. This involves implementing robust cybersecurity frameworks, conducting regular vulnerability assessments, and deploying advanced threat detection and response systems. Additionally, your organisation should adopt a proactive approach to threat intelligence and information sharing, collaborating with government agencies and industry partners to stay ahead of emerging threats.

CHALLENGE

Traditionally, the skill gap has acted as a deterrent against attacks on OT environments by inexperienced cybercriminals or "script kiddies." However, with the emergence of LLM and AI models, the skill gap is being rapidly reduced. These powerful technologies enable individuals to quickly acquire knowledge and expertise in exploiting vulnerabilities in ageing OT environments. This shift increases the likelihood of attacks on critical infrastructure and demands a proactive response.

RESOLUTION

To counter the evolving threat landscape, your organisation must invest in skill development initiatives to equip cybersecurity professionals with the knowledge and tools needed to address OT security challenges effectively. This includes training personnel on the latest OT security practices, conducting simulated exercises and red teaming to test defences, and fostering a culture of continuous learning and improvement. Furthermore, modernising ageing OT environments with up-to-date technologies, robust authentication mechanisms, and secure communication protocols is crucial for enhancing overall security posture.

TAKEAWAY

As state-based cybercriminals increasingly target critical infrastructure and OT environments, and the skill gap of cybercriminals diminishes with the rise of LLM and AI models, the imperative for your organisation in protecting critical assets lies in fortifying security measures, investing in skill development, and modernising OT environments to safeguard against the growing threat landscape.

SO, WHAT'S NEXT?

Thank you for taking the time to review this guide. We hope it proves to be a useful ongoing resource as you engage with your internal teams and external experts. There is no doubting the enormous burden in being responsible for an organisation's cybersecurity management, and understanding the cybersecurity landscape is crucial.

Here is what you might like to do as next steps:

- **Consult with your internal teams about the topics set out in the guide.**
- **Use the Takeaways to ask the right questions.**
- **Seek external counsel with a partner like LAB³ – a highly regarded expert in modern cybersecurity – who is best placed to give on point advice in the context of your organisation.**

The 2023 LAB³ Cybersecurity Guide was written and researched by Anthony Wales – Director of Network & Security at LAB³.

Anthony is a tenacious innovator who is driven to find new and better ways of doing things.

With a background in delivery, presales, and architecture across many industries, he understands both the common, and unique needs and frustrations of organisations.

Leading the security and network practices at LAB³, Anthony has been a champion of innovation, consistently pushing limits to provide clients with improved value, visibility, speed and reliability. Most importantly, Anthony works to ensure clients have the confidence necessary to invest in transformation for improved business outcomes.

CONNECTING WITH LAB³

At any time, feel welcome to contact us!
Rhiannon Tunstall, General Manager of
Client Engagement

rhiannon.tunstall@lab3.com.au

General enquiries:

Visit **www.lab3.com.au** or email **hello@lab3.com.au**

irap

ISO 27001 Certified

Member of
Microsoft Intelligent
Security Association
Microsoft

Microsoft

intel