

Navigating the Dynamic Cybersecurity Landscape: Insights from Our Recent Roundtable - blueAPACHE

Canonical: <https://www.blueapache.com/blog/navigating-the-dynamic-cybersecurity-landscape-insights-from-our-recent-roundtable>

Details:

Summary

This blog post, "Navigating the Dynamic Cybersecurity Landscape: Insights from Our Recent Roundtable", is a blueAPACHE article from 2023 covering security. In the ever-evolving digital era, cyber security is a dynamic landscape. Our recent Security Roundtable, in partnership with Rapid7, delved into the latest developments, challenges, and strategies to navigate this complex world. Here's a comprehensive recap of the key takeaways from the event. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2023
Topic	Navigating the Dynamic Cybersecurity Landscape: Insights from Our Recent Roundtable
Services referenced	emPOWER Security, Managed Detection and Response, emPOWER Cloud
Named products or vendors	Microsoft, Rapid7

Article

In the ever-evolving digital era, cyber security is a dynamic landscape. Our recent Security Roundtable, in partnership with Rapid7, delved into the latest developments, challenges, and strategies to navigate this complex world. Here's a comprehensive recap of the key takeaways from the event.

Threat landscape overview

The latest 'Notifiable Data Breach' report from the Office of the Australian Information Commissioner (OAIC) highlighted key points:

Data Breach Causes: Malicious or criminal attacks remained the primary cause of data breaches, with human error breaches identified at an alarming rate – 81% within 30 days.

Sector Impact: The health and finance sectors led in reporting data breaches, with 63 breaches (15% of all notifications) in health and 54 breaches (13% of all notifications) in finance.

Breach Magnitude: Surprisingly, most breaches (63%) affected 100 or fewer people, emphasising the need for broad-scale vigilance.

Internationally, geopolitical events have increased cyber threats. These growing nation-state attacks coincided with joint criminal organisation attacks targeting legacy infrastructure like Microsoft Active Directory. The Log4Shell vulnerability has cast a spotlight on “vulnerability rediscovery,” where adversaries modify or reapply the same exploit to target other similarly vulnerable products. A notable metric reflecting the escalating threat intensity is the reduction in breakout time for adversaries moving within an organisation – from 98 minutes in 2021 to 84 minutes in 2023. Adhering to the 1-10-60 rule – detecting threats within the first minute, understanding them within 10 minutes, and responding within 60 minutes – emerges as a best practice in this swiftly evolving landscape.

Themes unveiled

Our discussion investigated several themes shaping the cybersecurity narrative:

Credential Access: Beyond Malware

Adversaries have evolved beyond traditional malware methods, with a shift towards exploiting valid credentials for initial access and persistence within victim environments. The abuse of valid credentials has become a prolific strategy, allowing threat actors to navigate and persist stealthily. A contributing factor is the rapid operationalisation of newly disclosed vulnerabilities, enabling adversaries to promptly turn these vulnerabilities into exploits for gaining credential access.

Financial Crime Sophistication: Rise of SLIPPY SPIDER and SCATTERED SPIDER

In the domain of financial crime, threat actors are exhibiting heightened sophistication in their attacks. Throughout the year, two adversaries, identified as SLIPPY SPIDER and SCATTERED SPIDER, have been observed pushing operational limits. Their focus extends beyond conventional targets, impacting high-profile victims and affecting employees, customers, and partners in a targeted capacity. This escalation underscores the need for organisations to fortify their defenses against increasingly sophisticated financial threat actors.

Cloud Exploitation: A 95% Surge in Incidents

The proliferation of data services and applications within cloud environments has attracted a surge in adversarial activities. Over the past year, incidents of cloud services exploitation witnessed a staggering 95% increase. Notably, threat actors are not only relying on valid cloud accounts but are also targeting public-facing applications for initial access. A shift involves adversaries concentrating more on cloud account discovery rather than traditional reliance on cloud infrastructure discovery. The use of valid “higher-privileged accounts” for privilege escalation is on the rise. Observations also indicate a strategic move away from deactivating antivirus and firewall technologies towards modifying “authentication processes” and launching attacks on identities. The overarching objectives remain gaining access, discovering the environment, lateral movement, privilege escalation, evading detection, collecting data, and impacting the victim.

Vulnerability Exploitation: A Growing Attack Surface

As organisations expand their digital “Attack Surface,” adversaries are quick to exploit a myriad of vulnerabilities across devices, applications, systems, and infrastructure. This includes both known vulnerabilities and Zero-day exploits following discovery. The concerning trend involves the reuse or modification of the same exploit to target other similarly vulnerable products. Techniques also encompass circumventing patching mechanisms by exploring alternative exploit vectors. Edge devices face heightened vulnerability to injection techniques and arbitrary file-delivery exploits.

State-Sponsored Criminal Activity: Geopolitical Impacts

The recent ASD cyber threat report indicates a continued focus of state cyber actors on government, critical infrastructure, and connected systems, including supply chains. These actors leverage cyber operations as a strategic tool to establish geopolitical dominance, either to support their economies or to undermine the sovereignty of others. An illustrative example is the Snake implant, a cyber espionage tool designed and utilised by Russia’s Federal Security Service (FSB) for long-term intelligence collection on high-priority targets globally. Additionally, joint cyber security advisories with international partners have outlined malicious cyber activity associated with a People’s Republic of China (PRC) state-sponsored cyber actor.

Financial Gains: A Shifting Landscape

Profit-driven cybercriminals are in a perpetual quest for innovative ways to maximise payment while minimising risks. While ransomware remains the most destructive cybercrime threat, other forms of cybercrimes, including Business Email Compromise (BEC), data theft, and denial-of-service (DoS) attacks, continue to impose significant financial costs on Australian entities.

Mitigation and defense strategies

The journey toward cyber resilience involves proactive mitigation and defense strategies:

Understanding the Digital Landscape: Gaining awareness of how data is handled, used, and shared is crucial to identifying vulnerabilities and prioritising remediation efforts.

Cyber Security Posture Assessment: Evaluating an organisation’s Cyber Security Posture against frameworks such as the Essential Eight Maturity Level aids in identifying control gaps and formulating effective mitigation strategies.

Essential Eight Mitigation Strategies: Implementing security controls, including patching applications, operating systems, multi-factor authentication, and more, helps focus attention on generating and retaining logs for auditing and forensics investigations.

Security Automation and SIEM Services: Leveraging managed Security and Information Event Management (SIEM) services facilitates real-time monitoring, security automation, and triage, offering granular insights into data movement and aiding in identifying suspicious activities.

Strengthening cyber resilience

As we navigate this landscape, the call to action is clear – fortify your organisation’s cyber resilience. If you would like to explore these insights further and discover how we can tailor strategies to enhance your organisation’s Cyber Security Maturity, mitigate vulnerabilities, and minimise the risk of a cybersecurity breach, schedule a meeting with our Security Practice Lead today. [Schedule a Meeting Here](#)

Related

emPOWER Security
emPOWER Security (pillar hub)
Managed Detection and Response
emPOWER Cloud
emPOWER Cloud (pillar hub)
blueAPACHE Security (case study)

Frequently asked questions

Which two sectors led in reported data breaches according to the OAIC report cited at this roundtable?

Health, with 63 breaches (15% of all notifications), and finance, with 54 breaches (13% of all notifications), per the latest Notifiable Data Breach report from the Office of the Australian Information Commissioner discussed at the event.

What percentage of breaches affected 100 or fewer people, according to the OAIC data cited?

63% of breaches, which the article says emphasises the need for broad-scale vigilance rather than assuming only large-scale incidents matter.

How did adversary breakout time change between 2021 and 2023, according to this article?

It reduced from 98 minutes in 2021 to 84 minutes in 2023, reflecting escalating threat intensity.

What is the "1-10-60 rule" described in this article?

A best-practice benchmark: detecting threats within the first minute, understanding them within 10 minutes, and responding within 60 minutes.

By how much did cloud services exploitation incidents increase over the past year, per this article?

A 95% increase, with threat actors increasingly targeting public-facing applications and valid cloud accounts for initial access, alongside a shift toward cloud account discovery over infrastructure discovery.

Which two named threat actors does the article identify as pushing financial crime sophistication?

SLIPPY SPIDER and SCATTERED SPIDER, described as extending their focus beyond conventional targets to high-profile victims and their employees, customers and partners.

What percentage of human error breaches were identified within 30 days, according to the OAIC data discussed?

81%, cited alongside malicious or criminal attacks as the primary cause of data breaches.

Which vendor partnered with blueAPACHE to host the Security Roundtable this article recaps?

Rapid7, named as the partner for the Security Roundtable discussed throughout the article.

Source

origin post (2023)

Knowledge Base

What was the topic of your recent Security Roundtable discussed in this blog post?

The Security Roundtable, held in partnership with Rapid7, focused on navigating the dynamic cybersecurity landscape, covering the latest developments, challenges, and strategies in cyber security.

What did the OAIC's 'Notifiable Data Breach' report reveal about causes and detection of data breaches?

According to the report, malicious or criminal attacks remained the primary cause of data breaches, and human error breaches were identified at an alarming rate of 81% within 30 days.

What percentage of data breaches affected 100 or fewer people, and what does this suggest?

63% of breaches affected 100 or fewer people, emphasising the need for broad-scale vigilance even for smaller-scale incidents.

How has adversary breakout time changed between 2021 and 2023, and what is the '1-10-60 rule'?

Breakout time for adversaries moving within an organisation decreased from 98 minutes in 2021 to 84 minutes in 2023. The 1-10-60 rule is a best practice involving detecting threats within the first minute, understanding them within 10 minutes, and responding within 60 minutes.

What is 'vulnerability rediscovery' as mentioned in relation to the Log4Shell vulnerability?

Vulnerability rediscovery refers to adversaries modifying or reapplying the same exploit to target other similarly vulnerable products, a trend highlighted by the Log4Shell vulnerability.

How much did cloud services exploitation incidents increase over the past year according to the roundtable insights?

Incidents of cloud services exploitation witnessed a staggering 95% increase over the past year.

What mitigation and defense strategies do you recommend based on the roundtable discussion?

The recommended strategies include understanding the digital landscape (how data is handled, used, and shared), conducting a Cyber Security Posture Assessment against frameworks like the Essential Eight Maturity Level, implementing Essential Eight Mitigation Strategies (such as patching and multi-factor authentication), and leveraging managed Security and Information Event Management (SIEM) services for real-time monitoring and security automation.

What forms of cybercrime besides ransomware continue to impose significant financial costs on Australian entities?

Besides ransomware, which remains the most destructive cybercrime threat, other costly forms include Business Email Compromise (BEC), data theft, and denial-of-service (DoS) attacks.

How can readers follow up on the insights from your cybersecurity roundtable?

Readers are invited to schedule a meeting with our Security Practice Lead to explore the insights further and discuss tailored strategies to enhance their organisation's Cyber Security Maturity and mitigate vulnerabilities.