Exposure Management & Telemetry: You Can’t Defend What You Can’t See - blueAPACHE

Canonical:
https://www.blueapache.com/blog/exposure-management-telemetry-you-cant-defend-what-you-cant-see

Details:

Summary

This blueAPACHE post reports: October 2025 October is Cyber Security Awareness Month, and blueAPACHE is proud to support the ACSC’s national initiative by aligning each week’s content to the official CSAM themes. This year, we’re taking a lifecycle approach by mapping each blog to a critical stage in the Threat Lifecycle. It concerns emPOWER Security, Exposure Management, Managed Detection & Response. It names IBM in connection with the announcement. Published in 2025. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2025
Services referenced	emPOWER Security, Exposure Management, Managed Detection & Response
Named products or vendors	IBM

Article

October 2025 October is Cyber Security Awareness Month, and blueAPACHE is proud to support the ACSC’s national initiative by aligning each week’s content to the official CSAM themes. This year, we’re taking a lifecycle approach by mapping each blog to a critical stage in the Threat Lifecycle. We’ll begin with Exposure Management and Telemetry (preventive steps like vulnerability and patch management, and understanding your attack surface), then move to Defense (security operations and incident response), followed by Human Risk Management, the “human firewall” (security awareness, phishing, and MFA). We’ll conclude with a forward-looking perspective from our vCISO Barry Sollitt on quantum computing and AI-driven threats. While our sequence differs from the ACSC’s weekly order, every topic is directly aligned to their 2025 themes, ensuring our guidance is both timely and relevant for Australian organisations. We invite you to follow along each week as we explore the evolving threat landscape and practical steps to strengthen your cyber resilience.

Barry Sollitt – vCISO – blueAPACHE

In cybersecurity, the adage “you can’t defend what you can’t see” has never been more relevant. Modern businesses are built on sprawling digital ecosystems, a potential mix of local systems to cloud systems and multiple SaaS platforms. As attack surfaces expand, it is critical to understand where blind spots exist. This is where Exposure Management and real-time telemetry step in.

Why Visibility is the New Battleground

Most cyber intrusions don’t start with a Hollywood-style hack. They begin with the ordinary: an unpatched browser, an end-of-life VPN, or a forgotten web service. These overlooked assets become easy entry points for attackers, especially as automated exploits and ransomware crews weaponise known vulnerabilities. Exposure management and real-time telemetry are now essential for any organisation serious about cyber resilience. They offer the comprehensive view across operations needed to identify vulnerabilities before attackers do, prioritise what matters most, and enable dynamic, continuous defence.

The Business Case for Exposure Management

Proactive Risk Reduction: By mapping your entire attack surface—including public cloud, branches, home offices, and third-party platforms—you can spot and remediate vulnerabilities before they’re exploited.

Contextual Prioritisation: Exposure management isn’t about drowning in endless vulnerability lists. It’s about focusing on risks with the greatest business impact, aligning remediation with what truly matters to your organisation.

Continuous Improvement: Real-time telemetry from endpoints, networks, and cloud feeds exposure management with actionable insights, moving you from periodic, static scanning to dynamic, always-on defence.

Compliance and Resilience: Structured remediation cycles and continuous visibility are vital for meeting regulatory frameworks like the Essential Eight, ISO27001, and more.

The Risks of Poor Visibility

Blind Spots Become Breach Points: Unmonitored assets, shadow IT, or endpoints from acquisitions can create invisible entryways for attackers, often going undetected until after a breach.

Static Defence Fails Modern Attacks: Point-in-time assessments leave organisations exposed between scans, while threat actors exploit new vulnerabilities in real time.

Overwhelmed Security Teams: Outdated inventories and fragmented data make it hard to prioritise and act, increasing both risk and operational costs.

Regulatory Penalties: Missed exposures make it harder to demonstrate compliance, risking sanctions and reputational damage.

These risks often undermine even the most robust security strategies. The good news: with the right approach, organisations can regain visibility and control. Here’s how to get started:

Practical Steps for Business Leaders

Map Your Attack Surface: Build a comprehensive inventory of all assets—internal and external—to ensure nothing escapes your line of sight. Define and prioritise business critical information assets.

Adopt CTEM and Telemetry Solutions: Deploy Continuous Threat Exposure Management platforms that integrate real-time telemetry for constant, automated risk assessment for critical assets.

Prioritise by Context: Perform business impact analysis on critical assets to filter exposures not just by technical severity, but by organisational risk value.

Validate Before Mobilising: Confirm which exposures are truly exploitable, using automated breach simulations or red team validation.

Mobilise Remediation and Measure Progress: Coordinate patching, configuration changes, and compensating controls, integrating IT, security, and business functions for optimal results.

Extending Security Beyond Your Walls

Your suppliers' risks are your risks which is a reality highlighted by recent supply chain breaches in Australia and reinforced by ACSC guidance. To reduce your exposure, build security into your procurement process: require that vendors use supported software versions, provide secure-by-design assurances, and share a Software Bill of Materials (SBOM) so you know what's in their products. Prioritise patching for known exploited vulnerabilities (KEVs), and ensure your suppliers commit to timely updates. Require multi-factor authentication (MFA) and single sign-on (SSO) support for any third-party access. Regularly review and revoke unnecessary vendor access to your systems. By making these steps part of your standard vendor management, you'll align with Australian best practice and reduce the risk of a breach spreading through your supply chain.

Measure What Matters

Track key metrics such as time-to-patch for known exploited vulnerabilities (KEVs)—for example, aim to reduce your average patch time from 30 days to under 7 days. Monitor your coverage across servers, endpoints, and SaaS platforms, and set targets to reduce the number of unknown or unmonitored assets each quarter. Document any exceptions and ensure compensating controls are in place. Map your progress to your chosen cyber security framework (such as the Essential Eight), so boards and executives can see tangible improvement over time. Exposure management, powered by robust telemetry, is the foundation of organisational cyber resilience in 2025. For business leaders, it's not simply about technical defence, it's about ensuring every critical asset is visible, every risk is quantified, and every action leads to measurable risk reduction. In the digital age, visibility isn't optional: it's a strategic imperative for every modern business. Call to Action: Discover how a Patch & Exposure Uplift Plan from blueAPACHE can help you close security gaps, automate your defenses, and give your board the confidence of an executive scorecard which are all aligned to ACSC guidance. Contact us today to get started.

Sources (for editor/reference)

ACSC – Cyber Security Awareness Month 2025 (weekly themes): https://www.cyber.gov.au/business-government/cyber-security-awareness-month

ACSC – Essential Eight maturity model: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model

ACSC – Annual Cyber Threat Report 2023–24: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

IBM – Cost of a Data Breach Report 2025: https://www.ibm.com/reports/data-breach

FBI IC3 – Business Email Compromise PSA (losses): https://www.ic3.gov/PSA/2024/PSA240911

Related

emPOWER Security

emPOWER Security (pillar)

Exposure Management

Managed Detection & Response

Frequently asked questions

Who authored this post, and what is their role?

The post is written by Barry Sollitt, vCISO at blueAPACHE, as the first instalment of blueAPACHE's Cyber Security Awareness Month 2025 series.

What five practical steps does the post recommend for exposure management?

It recommends: mapping the attack surface, adopting Continuous Threat Exposure Management (CTEM) and telemetry solutions, prioritising exposures by business context, validating exploitability before mobilising, and coordinating remediation while measuring progress.

What patch-time target does the post recommend for known exploited vulnerabilities?

It recommends tracking time-to-patch for known exploited vulnerabilities (KEVs) and aiming to reduce the average from 30 days to under 7 days.

What supply-chain security measures does the post recommend for vendor management?

It recommends requiring vendors to use supported software versions, provide secure-by-design assurances, share a Software Bill of Materials (SBOM), and support MFA and SSO for third-party access.

Is this post still current?

It reflects CSAM 2025 content and sources current at publication, including references to the ACSC 2023-24 Annual Cyber Threat Report and the IBM Cost of a Data Breach Report 2025. For current exposure management services, see the Exposure Management page linked below.

Source

https://www.blueapache.com/blog/exposure-management-telemetry-you-cant-defend-what-you-cant-see/

Knowledge Base

How does this blog post relate to Cyber Security Awareness Month (CSAM) 2025?

October is Cyber Security Awareness Month, and we are supporting the ACSC's national initiative by aligning weekly content to a Threat Lifecycle approach: starting with Exposure Management and Telemetry, then Defense (security operations and incident response), followed by Human Risk Management, and concluding with a forward-looking piece from vCISO Barry Sollitt on quantum computing and AI-driven threats.

how do most cyber intrusions typically begin?

Most cyber intrusions don't start with a Hollywood-style hack; they begin with ordinary oversights like an unpatched browser, an end-of-life VPN, or a forgotten web service, which become easy entry points for attackers as automated exploits and ransomware crews weaponise known vulnerabilities.

What are the key business benefits of Exposure Management ?

four benefits: Proactive Risk Reduction (mapping the entire attack surface—public cloud, branches, home offices, third-party platforms—to spot and remediate vulnerabilities before exploitation); Contextual Prioritisation (focusing on risks with the greatest business impact rather than endless vulnerability lists); Continuous Improvement (using real-time telemetry from endpoints, networks, and cloud to move from static scanning to dynamic, always-on defence); and Compliance and Resilience (structured remediation cycles and continuous visibility to meet frameworks like the Essential Eight and ISO27001).

What risks does poor visibility create for organisations, per the blog?

Poor visibility creates four risks: Blind Spots Become Breach Points (unmonitored assets, shadow IT, or acquisition endpoints create invisible entryways for attackers); Static Defence Fails Modern Attacks (point-in-time assessments leave gaps between scans); Overwhelmed Security Teams (outdated inventories and fragmented data hinder prioritisation and increase costs); and Regulatory Penalties (missed exposures make it harder to demonstrate compliance, risking sanctions and reputational damage).

What five practical steps do you recommend for business leaders to improve exposure management?

The five steps are: 1) Map Your Attack Surface—build a comprehensive inventory of all internal and external assets and prioritise business-critical information assets; 2) Adopt CTEM and Telemetry Solutions—deploy Continuous Threat Exposure Management platforms with real-time telemetry for constant automated risk assessment; 3) Prioritise by Context—filter exposures by business impact analysis, not just technical severity; 4) Validate Before Mobilising—confirm which exposures are truly exploitable using automated breach simulations or red team validation; 5) Mobilise Remediation and Measure Progress—coordinate patching, configuration changes, and compensating controls across IT, security, and business functions.

What metrics do you suggest organisations track to measure exposure management progress?

The post recommends tracking time-to-patch for known exploited vulnerabilities (KEVs)—for example, aiming to reduce average patch time from 30 days to under 7 days—monitoring coverage across servers, endpoints, and SaaS platforms, setting quarterly targets to reduce unknown or unmonitored assets, documenting exceptions with compensating controls, and mapping progress to a chosen cyber security framework like the Essential Eight for board visibility.

What sources are referenced in the blog post for editors and readers?

The referenced sources include: ACSC – Cyber Security Awareness Month 2025 weekly themes; ACSC – Essential Eight maturity model; ACSC – Annual Cyber Threat Report 2023–24; IBM – Cost of a Data Breach Report 2025; and FBI IC3 – Business Email Compromise PSA on financial losses.