



Navigating cyber threats in Aged Care

Threat intelligence for a sector under pressure

CI-ISAC Australia | Health Cyber Sharing Network (HCSN) | May 2026

50%

of public hospital beds
under protection

35%

of public hospital beds
under protection

60+

of public hospital beds
under protection

Federally Funded

an initiative of the Australian
Cyber Strategy

Three Converging Pressures on Aged Care

Healthcare most targeted sector in 3 of 4 quarters in 2025 — more than financial services or government



State actors. Organised Crime. Accelerating campaigns.

In 2025, State-sponsored groups MuddyWater ran simultaneous campaigns across healthcare, financial services and higher education.

Ransomware groups fragmenting & reforming faster than attribution-based defence can track



Aged Care Act 2024. Board Obligation. Criminal penalties.

Since November 2025, cybersecurity is now a board-level legal obligation. Failures carry criminal penalties.

Security of Critical Infrastructure (SCI)
Act reforms propose bidirectional threat sharing as national priority



More capability. More attack surface. Legacy risk.

Telehealth, remote monitoring, AI tools for clinical health – more technology means more doors into your building.

Legacy clinical systems create persistence vulnerabilities that don't disappear when you buy something new.

Complexity of the Cyber Threat Landscape

AI matters. But the infrastructure we rely on to make sense of it is breaking down

Complexity of the Cyber Threat Landscape

NIST / NVD Global Public Goods

US pulling back from global vulnerability triage at the worst possible moment

Hours

window between vulnerability discovery and weaponisation down from days

THE CORE QUESTION FOR AGED CARE:

How can we ensure the safety and security of our residents and staff in the face of a cyber threat?

Signal-to-noise ratio worsening

Increasing number of alerts and incidents, making it difficult to identify and respond to threats

Common mistakes chasing every CVE alert • buying products that don't integrate • treating compliance as security • underestimating people as threat vectors



Fitri

{ ! [9 {

Falls for a low effort
crypto scam on
LinkedIn—
credentials harvested



Fitri

{ ! [9 {

Falls for a low-effort crypto scam on LinkedIn— credentials harvested



a $\check{\text{A}}\text{n}^{\text{r}}\hat{\text{j}} \ell$

EXECUTIVE PA

Buy gift cards after a WhatsApp impersonation scam targeting the CEO



Graham

HR

Inadvertently hires a foreign intelligence asset—no background check conducted



t'nHÄ

CIO

wś Ć ŋ ħ ž Ǻ
l' z s n s Ö Å
و ا x r j l' c c ä c
c s t n ä s l ö c
c c c | c c c s l c ä p

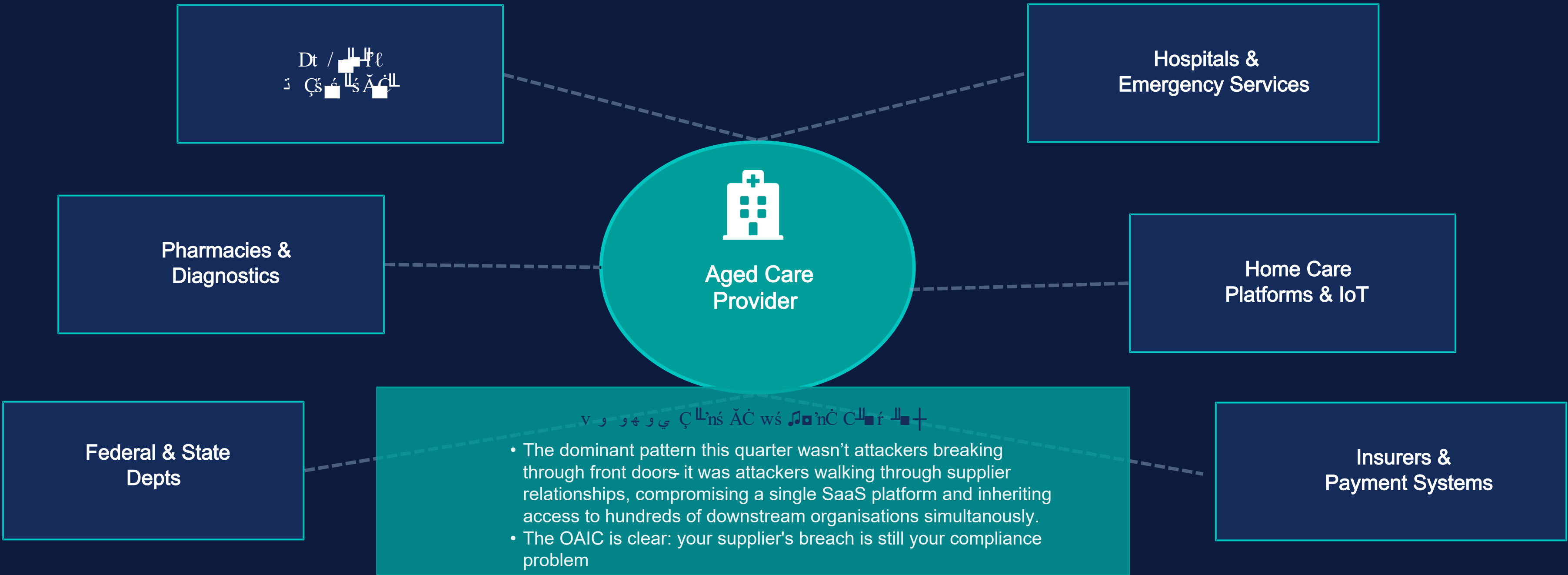


Tariq

FINANCE

Opens phishing email,
convinces helpdesk to
bypass controls, runs
malware manually

Incident Response & Aged Care Provider



- Incident Response & Aged Care Provider
- Ransomware on a GP clinic disrupts medication management for residents the same day home IoT devices expand your attack surface into patients' homes.
 - Supply chain compromise via shared MSP can affect dozens of providers simultaneously. Intelligence siloed to one provider is a cross-sector pattern.

The useful question: not 'should we worry' but 'what matters most right now?'

— REAL OUTCOMES

í ś 𐀀 𐀁 𐀂 𐀃 𐀄 𐀅 𐀆 𐀇 𐀈 𐀉 𐀊 𐀋 𐀌 𐀍 𐀎 𐀏 𐀐 𐀑 𐀒 𐀓 𐀔 𐀕 𐀖 𐀗 𐀘 𐀙 𐀚 𐀛 𐀜 𐀝 𐀞 𐀟 𐀠 𐀡 𐀢 𐀣 𐀤 𐀥 𐀦 𐀧 𐀨 𐀩 𐀪 𐀫 𐀬 𐀭 𐀮 𐀯 𐀰 𐀱 𐀲 𐀳 𐀴 𐀵 𐀶 𐀷 𐀸 𐀹 𐀺 𐀻 𐀼 𐀽 𐀾 𐀿 𐁀 𐁁 𐁂 𐁃 𐁄 𐁅 𐁆 𐁇 𐁈 𐁉 𐁊 𐁋 𐁌 𐁍 𐁎 𐁏 𐁐 𐁑 𐁒 𐁓 𐁔 𐁕 𐁖 𐁗 𐁘 𐁙 𐁚 𐁛 𐁜 𐁝 𐁞 𐁟 𐁠 𐁡 𐁢 𐁣 𐁤 𐁥 𐁦 𐁧 𐁨 𐁩 𐁪 𐁫 𐁬 𐁭 𐁮 𐁯 𐁰 𐁱 𐁲 𐁳 𐁴 𐁵 𐁶 𐁷 𐁸 𐁹 𐁺 𐁻 𐁼 𐁽 𐁾 𐁿 𐂀 𐂁 𐂂 𐂃 𐂄 𐂅 𐂆 𐂇 𐂈 𐂉 𐂊 𐂋 𐂌 𐂍 𐂎 𐂏 𐂐 𐂑 𐂒 𐂓 𐂔 𐂕 𐂖 𐂗 𐂘 𐂙 𐂚 𐂛 𐂜 𐂝 𐂞 𐂟 𐂠 𐂡 𐂢 𐂣 𐂤 𐂥 𐂦 𐂧 𐂨 𐂩 𐂪 𐂫 𐂬 𐂭 𐂮 𐂯 𐂰 𐂱 𐂲 𐂳 𐂴 𐂵 𐂶 𐂷 𐂸 𐂹 𐂺 𐂻 𐂼 𐂽 𐂾 𐂿 𐃀 𐃁 𐃂 𐃃 𐃄 𐃅 𐃆 𐃇 𐃈 𐃉 𐃊 𐃋 𐃌 𐃍 𐃎 𐃏 𐃐 𐃑 𐃒 𐃓 𐃔 𐃕 𐃖 𐃗 𐃘 𐃙 𐃚 𐃛 𐃜 𐃝 𐃞 𐃟 𐃠 𐃡 𐃢 𐃣 𐃤 𐃥 𐃦 𐃧 𐃨 𐃩 𐃪 𐃫 𐃬 𐃭 𐃮 𐃯 𐃰 𐃱 𐃲 𐃳 𐃴 𐃵 𐃶 𐃷 𐃸 𐃹 𐃺 𐃻 𐃼 𐃽 𐃾 𐃿 𐄀 𐄁 𐄂 𐄃 𐄄 𐄅 𐄆 𐄇 𐄈 𐄉 𐄊 𐄋 𐄌 𐄍 𐄎 𐄏 𐄐 𐄑 𐄒 𐄓 𐄔 𐄕 𐄖 𐄗 𐄘 𐄙 𐄚 𐄛 𐄜 𐄝 𐄞 𐄟 𐄠 𐄡 𐄢 𐄣 𐄤 𐄥 𐄦 𐄧 𐄨 𐄩 𐄪 𐄫 𐄬 𐄭 𐄮 𐄯 𐄰 𐄱 𐄲 𐄳 𐄴 𐄵 𐄶 𐄷 𐄸 𐄹 𐄺 𐄻 𐄼 𐄽 𐄾 𐄿 𐅀 𐅁 𐅂 𐅃 𐅄 𐅅 𐅆 𐅇 𐅈 𐅉 𐅊 𐅋 𐅌 𐅍 𐅎 𐅏 𐅐 𐅑 𐅒 𐅓 𐅔 𐅕 𐅖 𐅗 𐅘 𐅙 𐅚 𐅛 𐅜 𐅝 𐅞 𐅟 𐅠 𐅡 𐅢 𐅣 𐅤 𐅥 𐅦 𐅧 𐅨 𐅩 𐅪 𐅫 𐅬 𐅭 𐅮 𐅯 𐅰 𐅱 𐅲 𐅳 𐅴 𐅵 𐅶 𐅷 𐅸 𐅹 𐅺 𐅻 𐅼 𐅽 𐅾 𐅿 𐆀 𐆁 𐆂 𐆃 𐆄 𐆅 𐆆 𐆇 𐆈 𐆉 𐆊 𐆋 𐆌 𐆍 𐆎 𐆏 𐆐 𐆑 𐆒 𐆓 𐆔 𐆕 𐆖 𐆗 𐆘 𐆙 𐆚 𐆛 𐆜 𐆝 𐆞 𐆟 𐆠 𐆡 𐆢 𐆣 𐆤 𐆥 𐆦 𐆧 𐆨 𐆩 𐆪 𐆫 𐆬 𐆭 𐆮 𐆯 𐆰 𐆱 𐆲 𐆳 𐆴 𐆵 𐆶 𐆷 𐆸 𐆹 𐆺 𐆻 𐆼 𐆽 𐆾 𐆿 𐇀 𐇁 𐇂 𐇃 𐇄 𐇅 𐇆 𐇇 𐇈 𐇉 𐇊 𐇋 𐇌 𐇍 𐇎 𐇏 𐇐 𐇑 𐇒 𐇓 𐇔 𐇕 𐇖 𐇗 𐇘 𐇙 𐇚 𐇛 𐇜 𐇝 𐇞 𐇟 𐇠 𐇡 𐇢 𐇣 𐇤 𐇥 𐇦 𐇧 𐇨 𐇩 𐇪 𐇫 𐇬 𐇭 𐇮 𐇯 𐇰 𐇱 𐇲 𐇳 𐇴 𐇵 𐇶 𐇷 𐇸 𐇹 𐇺 𐇻 𐇼 𐇽 𐇾 𐇿 𐈀 𐈁 𐈂 𐈃 𐈄 𐈅 𐈆 𐈇 𐈈 𐈉 𐈊 𐈋 𐈌 𐈍 𐈎 𐈏 𐈐 𐈑 𐈒 𐈓 𐈔 𐈕 𐈖 𐈗 𐈘 𐈙 𐈚 𐈛 𐈜 𐈝 𐈞 𐈟 𐈠 𐈡 𐈢 𐈣 𐈤 𐈥 𐈦 𐈧 𐈨 𐈩 𐈪 𐈫 𐈬 𐈭 𐈮 𐈯 𐈰 𐈱 𐈲 𐈳 𐈴 𐈵 𐈶 𐈷 𐈸 𐈹 𐈺 𐈻 𐈼 𐈽 𐈾 𐈿 𐉀 𐉁 𐉂 𐉃 𐉄 𐉅 𐉆 𐉇 𐉈 𐉉 𐉊 𐉋 𐉌 𐉍 𐉎 𐉏 𐉐 𐉑 𐉒 𐉓 𐉔 𐉕 𐉖 𐉗 𐉘 𐉙 𐉚 𐉛 𐉜 𐉝 𐉞 𐉟 𐉠 𐉡 𐉢 𐉣 𐉤 𐉥 𐉦 𐉧 𐉨 𐉩 𐉪 𐉫 𐉬 𐉭 𐉮 𐉯 𐉰 𐉱 𐉲 𐉳 𐉴 𐉵 𐉶 𐉷 𐉸 𐉹 𐉺 𐉻 𐉼 𐉽 𐉾 𐉿 𐊀 𐊁 𐊂 𐊃 𐊄 𐊅 𐊆 𐊇 𐊈 𐊉 𐊊 𐊋 𐊌 𐊍 𐊎 𐊏 𐊐 𐊑 𐊒 𐊓 𐊔 𐊕 𐊖 𐊗 𐊘 𐊙 𐊚 𐊛 𐊜 𐊝 𐊞 𐊟 𐊠 𐊡 𐊢 𐊣 𐊤 𐊥 𐊦 𐊧 𐊨 𐊩 𐊪 𐊫 𐊬 𐊭 𐊮 𐊯 𐊰 𐊱 𐊲 𐊳 𐊴 𐊵 𐊶 𐊷 𐊸 𐊹 𐊺 𐊻 𐊼 𐊽 𐊾 𐊿 𐋀 𐋁 𐋂 𐋃 𐋄 𐋅 𐋆 𐋇 𐋈 𐋉 𐋊 𐋋 𐋌 𐋍 𐋎 𐋏 𐋐 𐋑 𐋒 𐋓 𐋔 𐋕 𐋖 𐋗 𐋘 𐋙 𐋚 𐋛 𐋜 𐋝 𐋞 𐋟 𐋠 𐋡 𐋢 𐋣 𐋤 𐋥 𐋦 𐋧 𐋨 𐋩 𐋪 𐋫 𐋬 𐋭 𐋮 𐋯 𐋰 𐋱 𐋲 𐋳 𐋴 𐋵 𐋶 𐋷 𐋸 𐋹 𐋺 𐋻 𐋼 𐋽 𐋾 𐋿 𐌀 𐌁 𐌂 𐌃 𐌄 𐌅 𐌆 𐌇 𐌈 𐌉 𐌊 𐌋 𐌌 𐌍 𐌎 𐌏 𐌐 𐌑 𐌒 𐌓 𐌔 𐌕 𐌖 𐌗 𐌘 𐌙 𐌚 𐌛 𐌜 𐌝 𐌞 𐌟 𐌠 𐌡 𐌢 𐌣 𐌤 𐌥 𐌦 𐌧 𐌨 𐌩 𐌪 𐌫 𐌬 𐌭 𐌮 𐌯 𐌰 𐌱

[illegible]

A national health insurer caught 2 critical cases their own internal systems missed entirely—intelligence the sector network surfaced first.

! b s Cc'n||z Cn lC

COMMERCIAL THREAT INTEL VENDORS

- ×

Generic global feeds
Not calibrated to Australian critical infrastructure or aged care sector
- ×

Point-in-time products
You pay for the tool; you're still responsible for connecting the dots
- ×

Siloed intelligence
9Ar ll-ös r anls l C-s-hlj lG s'nf □ ■ P'no llLs P'G'n,ACS' n-ll-L-FF
- ×

Cost vs. coverage tradeoff
Small and midsize providers often priced out of meaningful capability
- ×

Integration complexity
a j Cll'4 J'or j P' C'ACr ■ Cc' ll G s Ar ll-C's'n □ ls P'j n'FC's AG's

CHSAC COLLECTIVE DEFENCE MODEL

- ✓

Shared intelligence network
What one member sees, all members benefit fromthe network gets smarter with every incident
- ✓

Australian sovereign capability
Purposebuilt for AU critical infrastructure; no offshoring the triage problem
- ✓

Crosssector visibility
! Cc' ll-ös r anls l C-s-hlj lG s'nf □ ■ P'no llLs P'G'n,ACS' n-ll-L-FF
- ✓

Scales to all maturities
From single site residential facilities to 14,000ed national operators—same intel feed
- ✓

Bidirectional sharing
! ■ s' r G {h / L P'Cs z'n ll-ös r Ls'nf L-C's'ls-ös Ar P'G'n ll G s-ll-G-ll's ■ ls

Cyber Threat Intelligence

Case Study - CLICK FIX

Member Flags

Victorian health provider notices unusual ClickFix advisory. Reports through the HCSN network.



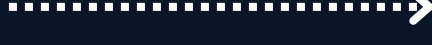
Analysis

CHSAC analysts run assessment. Identify 70 indicators of compromise.



Structured advisory distributed

to all members. Total time: 1 day.

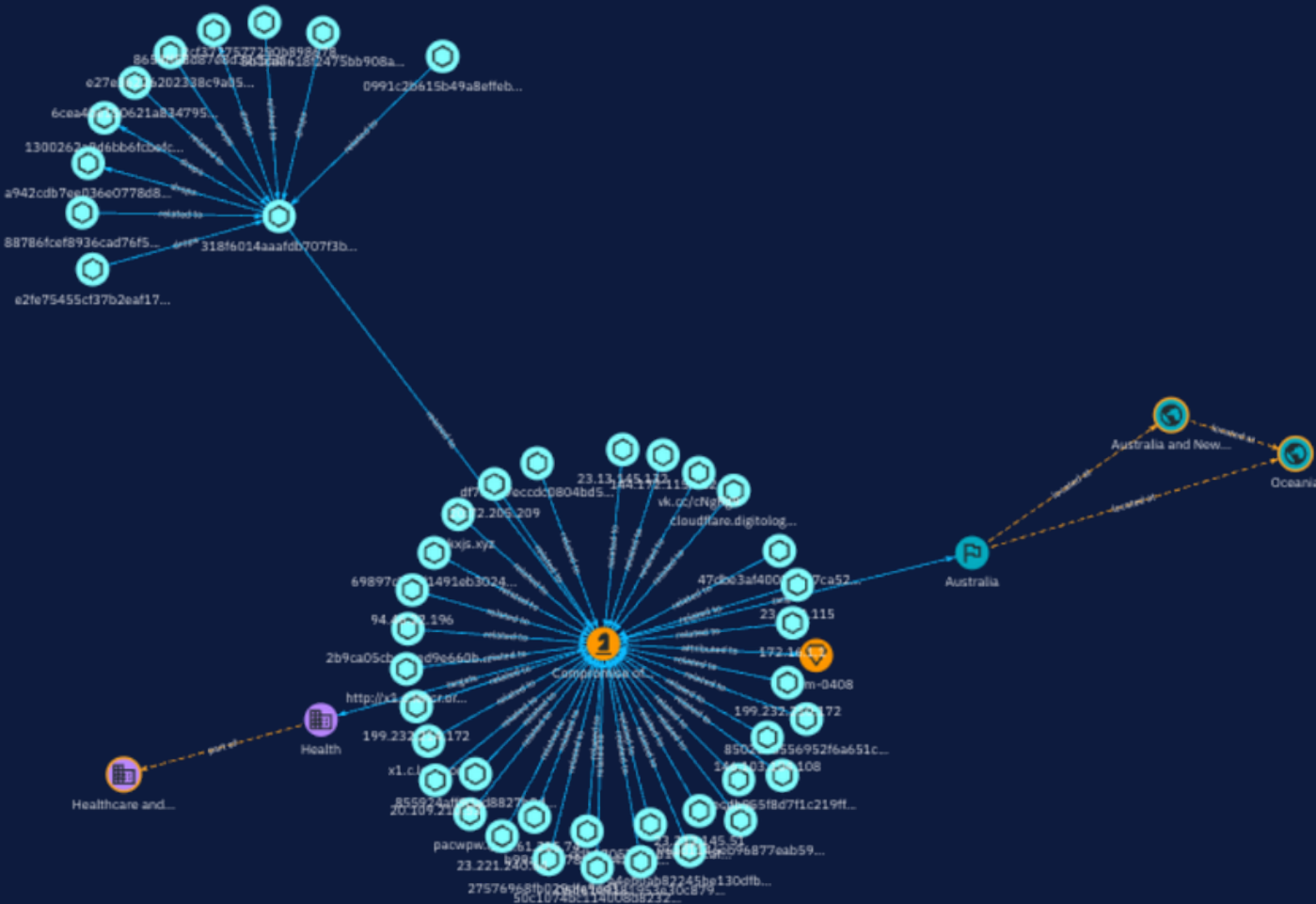


Emergency service provider

revealed similar analysis took their team many weeks to complete independently.

1 Day

vs many weeks for an independent team to produce the same analysis



For Every Level of Maturity

í I ò I / {b í h wY{ ! / wh {{ ÇI 9 {t 9/ ÇwÜa

Small providers:

wśl's-ōś ĆnA's Ćs Ąr F-Ćś ĆśFl'qĵ ģ ■śōś'n
Āzz'nr Ć ģś ■ś'nĀś Ā■ś □ ■□ / Lh 'rs ijĵ -ĥśr Ć
śśĆĀ'ĆōĀĥś ž■ Ćś žśśr □

Mid-tier regionals:

Build towards active cyber defence posture;
HCSN membership is auditable evidence of
active governance for the Aged Care Quality &
Safety Commission.

Large nationals:

Full bidirectional sharing: contribute sector
level visibility; gain cross-sector pattern
intelligence unavailable from commercial
vendors.



AGED CARE ACT 2024



{L's و b oś L's'n یو و l'HL's'nls j' n'F-L ČÄ IC llj s C-Č ÄlČÄĜ Ġn'FL-Äń
oL'ÄG-CÄk's l-zoÄG-Ä-Ä's Čl'Änn'l'n-Ä's-l özj Ů Ġ و
Ts Änl-n-s ČÄ-r l'Ä's lj-č's oal'ÄG-öz n-o-l's'n's-lČnÄG-

. 4 4 6 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Patch internet-facing systems. Enforce MFA on every account. Fix cloud permissions and segment your networks. These controls predate enabled threats—and they remain the most effective defence.

[illegible]

The question isn't 'how fast can we patch?' It's 'which patch matters to aged care systems?' Intelligence that helps you prioritise beats faster tools that point you in every direction at once.

Phishing, BEC, fake contractors, social engineering. Consistent, scalable, and completely independent of whatever AI announces next. User awareness and sensible access controls are your most cost-effective defence.

Many will emerge. Most won't integrate with your stack, improve your posture, or justify their cost. Add capability deliberately—the best test is: 'Does it help us prioritise?'

What's in it for Aged Care? I share / I don't

Aged care providers at every scale of maturity are building Australia's collective cyber defence through HCSN.

Start a 6Month Pilot

Federally funded via Home Affairs. Zero upfront cost.

ci-isac.org.au/hcsn



What you get from day one:



Access to the HCSN platform, including the HCSN dashboard, HCSN portal, and HCSN API.



Triage-ready intelligence — know what to prioritise in your environment, not just globally



Access to the HCSN platform, including the HCSN dashboard, HCSN portal, and HCSN API.



Visibility across threat actors, CVEs, malware, and affected Australian sectors



Auditable evidence of active cyber governance under the Aged Care Act 2024 & SOCI