Deloitte.

Superannuation Sector

Navigating challenges posed by cyber criminals

2022 Edition

Foreword

In this third instalment focused on the Superannuation industry, we take a closer look at the recent cyber events related to the Early Release scheme and SMSF rollover in the context of the COVID-19 pandemic. This industry holds Australia's $3.4 trillion of superannuation assets and is facing increased cybercrime activity due to large account balances, low member interactions and low cyber maturity.

There has been a steady increase in the rate of these cyber incidents and the tradecraft has evolved. Initially, incidents tended to be isolated to individual members, but now they are impacting society as a whole. ACCC and ASIC have released multiple super scam alerts, with recent examples related to the Early Release Scheme and SMSF Rollover.

In 2021, the AFP has stopped cyber criminals from stealing $24 million from the superannuation accounts of hard-working Australians and launched counter strikes to stop millions of dollars from being siphoned offshore[13].

While supporting the Australian Super community navigate the challenges posed by cyber criminals, The Deloitte Cyber Intelligence Centre has observed organised crime groups sharing and trading in tradecraft specific to the targeting of superannuation funds.

As the awareness spreads, we have also observed the trading of credentials referencing specific wealth balances as cyber criminals seek to maximise value at each stage of the dark web supply chain. A number of similarities between events were identified, which would be explained by a consortium working in collaboration. Our investigations also identified the likelihood that Australians were involved, given the accent observed in reviewing contact centre recordings where staff were manipulated or coerced to make a fraudulent payment or alter member data.

The more frequent and sophisticated cyber attacks means that the superannuation sector (Trustees and Administrators) need to take a holistic approach to uplift cyber resilience capabilities by implementing layered security controls across their people, technologies and process.

What is the magnetic pull between cyber criminals and the super funds?

AUSTRAC have found many reported offences are fraud related cases linked to cybercrime. It was identified by AUSTRAC that cybercrime is the single biggest threat they have faced with regular hacking attempts into many individuals funds[14].

The Gateway Network Governance Body (GNGB), investigated 80 executives across the super sector and discovered a lack of leadership and ownership when it comes to managing cyber risk[1]. Strongly encouraging all Australia's super funds to review their current cybersecurity controls to ensure they are consistent and up to date.

According to APRA Cyber Security Survey, 75% of respondents encountered an incident that required escalation to executive management and identified that the super industry had little preparedness to address an incident[2].

A number of unique characteristics explain why the industry is becoming an attractive target for cybercrime:

- **More opportunities to access money.** During the Covid-19 outbreak, many Australians have used the financial assistance provided by the Australian Government, for eligible individuals to withdraw $20,000 in super. However, scammers saw this initiative as an opportunity to scam and take advantage of many Australians superannuation resulting in a loss of over $6 million[3].
- **Oversized money pools.** Australia has the world's fourth-largest superannuation market[4], with assets over $3.4 trillion, with a growth of 9.7% for the period of 2021-22.
- **Low member engagement.** In general, members infrequently check their superannuation accounts or read the statement. This can significantly increase the period of time between a successful fraud event (e.g. withdrawal or rollover) and the detection of that event by the member.
- **A complex third-party environment.** As a whole, the industry has a high reliance upon third-parties such as administrators, financial planners and other outsourced providers who perform services or engage with members on their behalf. This increases the range of potential attack points that cyber criminals can target and commit fraud through, without the fund itself directly having visibility.
- **Digital experience.** The industry is rapidly improving the functionality of online member portals and mobile apps so that members can interact and perform transactions from a range of devices on a 24/7 basis. This is in turn increasing the inherent risk that an attacker can access member information or initiate transactions if they have the member's log-in details.
- **Faster payments.** Technology adoption and regulations such as SuperStream and the New Payments Platform (NPP) are driving a transformation of the superannuation industry towards a fully interconnected environment with faster velocities on withdrawals and rollovers. These faster velocities can mean that outbound payments or rollovers are made promptly, with limited human oversight, and can reduce the time window for detection of a fraud or recovery of funds paid in error.
- **Weak detection and mitigation strategies.** AUSTRAC identified that organised crime is actively targeting funds with weak systems and controls. Once the ability to access funds without detection is confirmed (typically via a single fraudulent transaction), threat actors would step up their attack to a number of compromised identities. The elevated risk rating for the sector and the target areas from the regulator has made control weaknesses from outsourced Anti-Money Laundering /Counter-Terrorism Financing (AML/CTF) processes a focal point for third party providers.

Covid-19 superannuation early release scheme scam

Background

Superannuation assists Australians to prepare for a comfortable retirement, by putting aside money through the duration of an individual's working life until they decide to retire from work.

Due to the impact and implications of the Covid-19 pandemic unfolded to many Australians in 2020, the Australian Government took the initiative to provide financial assistance to those who in need by allowing eligible individual gain early access to their superannuation funds.

Eligible individuals were allowed to apply online through myGov and withdraw $10, 000 of their super prior to 1 July 2020 and apply for another instalment after 1 July 2020.

Unfortunately, this initiative created an opportunity for cyber criminals to take advantage of the government's early-release measures.

Attack vectors used by malicious actors

Phishing was the most common technique used to steal individuals superannuation through cold-calling or email and text messages during early access super scheme. Cyber criminals used the technique of cold calling by claiming to be from an organisation and offering the individual early access to their super.

Another method that was used was by email or text messages, this is where cyber criminals would use fake links to get the victim to enter personal information which was later on used by the cyber criminal to access their account.

Cyber criminals were able to compromise numerous super accounts due to the lack of configuration to limit multiple myGov accounts under one account. Many false accounts were made through the identity theft method, this involved retrieving personal information which was then used to gain access to individuals personal accounts.

Insight

$1.2 Million

ATO allowed 3.05 million Australians to access their Superannuation Funds early due to severe financial hardship during 2020. It was believed that Australians have sought to withdraw nearly $37.8 billion from retirement as Covid-19 financial aid[5].

$9.8 Million

Since the outbreak of Covid-19, Scamwatch captured over 6415 scam reports were logged related to identity theft and superannuation scams. Ultimately accumulating a loss of $9,800,000 million dollars[6].

$120 Thousand

According to Reece Kershaw (Commissioner of the Australian Federal Police), $120, 000 in retirement savings had been allegedly accessed as part of financial hardship scheme, resulting with all bank accounts being frozen for further investigation[7].

Self-Managed Super Fund (SMSF) rollover scam

Background

Australians are offered an alternative to using a traditional superfund and instead have the option to use a self-managed super fund (SMSF). A SMSF allows an individual to invest their super the way they want. While an effective way to take control of your superfund, using an SMSF statistically leads to lower returns compared to APRA-regulated funds. Due to the structure of the SMSF, individuals who fall victims to scams do not have access to compensation schemes and are not able to make a complaint through Australian Financial Complaints Authority (AFCA). Unfortunately cyber criminals take advantage of this system to the detriment of Australians.

Attack vectors used by malicious actors

Cyber criminals cold call the victims impersonating a registered financial advisor. These cyber criminals are convincing victims to open a SMSF account promising high returns from 8% to 20% on their balance. There are a variety of techniques used by the cyber criminals to convince the victim that they are legitimate including using company names, emails and addresses that are similar to licensed Australian companies. Legitimate companies are also used to establish the SMSF so that it is complaint with Australian laws and regulations so that it is less likely to raise suspicion by the ATO and super companies.

To create the SMSF, cyber criminals will either use documents given by the customer and open it with the customers knowledge and consent or use personal information stolen using a phishing email and create a fraudulent SMSF without the customers knowledge. After the SMSFs have been created the cyber criminals will either get the customer to roll over their superannuation balance into the SMSF, or impersonate the customer and roll the balance over fraudulently.

After the funds are in the SMSF the cyber criminals then transfer the balance into their own personal accounts, leaving little recourse for victims to get their money back.

Insight

$1.5 Million

Ahmed Saad a financial advisor in Glenroy, Victoria accessed over $1.5 million dollars on behalf of 168 of his clients. He used his position as an authorised representative of Apogee Financial Planning Limited (Apogee) to illegally rollover funds out of the clients superannuation[8].

$7 Million

One crime syndicate was able to steal over $7 million from superannuation and bank accounts of unsuspecting victims. They stole personal information from victim's mailboxes and used it to replicate high quality, fraudulent identification documents. These documents were then used to operate SMSFs in the victim's names and used to rollover funds from their legitimate superfund accounts into fraudulent accounts[9].

23,000

The Australian Taxation Office has risk models in place to assess every individual that enters the SMSF system to ensure that it is being used for the correct purpose. The ATO has many components that contribute to the identification of SMSFs being used to fraudulently roll over funds, including the non-lodgement of tax returns and inactivity of funds. It is estimated that there is over 23,000 fraudulent SMSFs[8].

$145 Thousand

One man discovered that he was the victim of identity theft when he was rejected when applying for a car loan. Months after this discovery he was sent his annual superannuation statement where he was notified that his entire superannuation balance of $145,000 was rolled over into a fraudulent SMSF account in his name[10].

Current Landscape

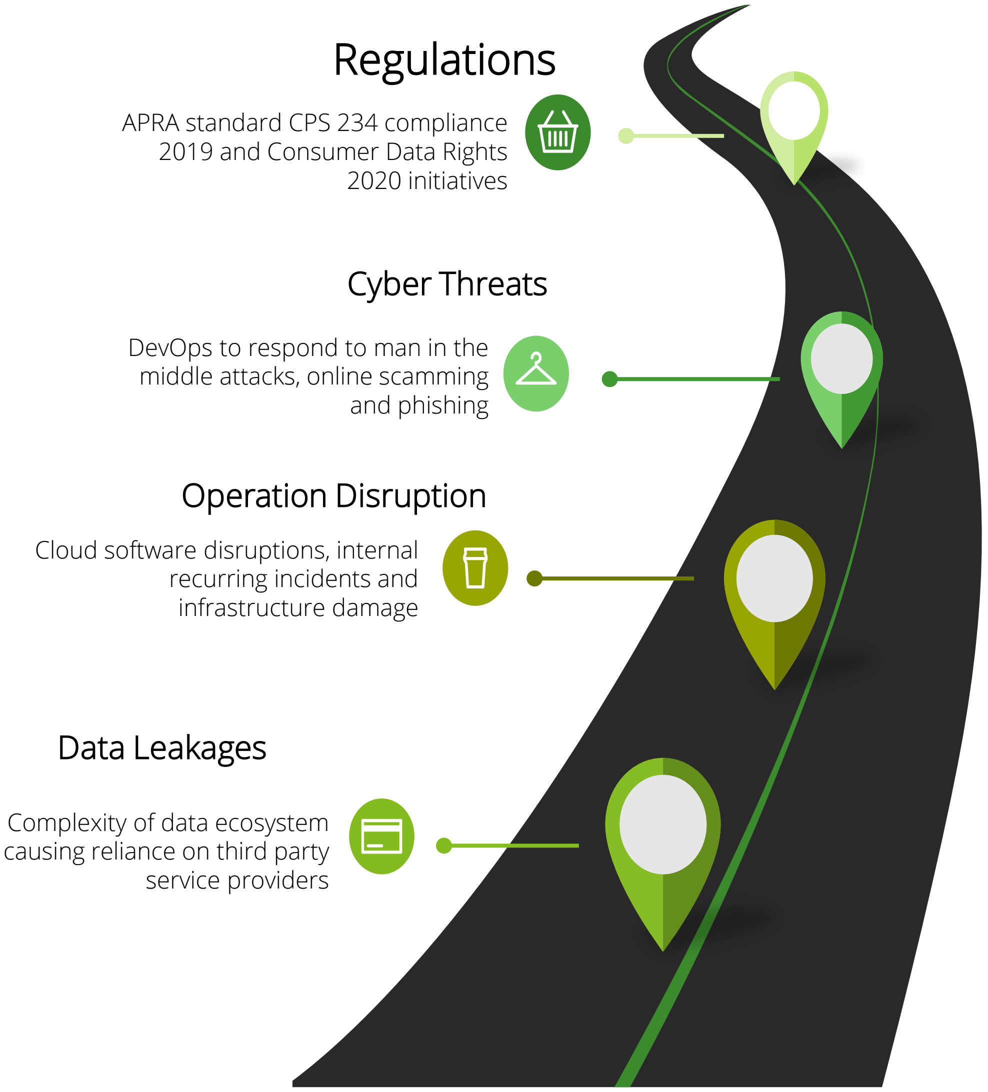
Some of the most common cyber threats seen across superannuation are as follows:

- Phishing Emails
- Identity Theft
- Cyber Enabled Fraud
- Human Error and
- Third-Party / Supplier Risk

Superannuation sector are also facing challenges related to increased regulatory requirements, emerging cyber threats, data theft/misuse and operational disruptions relating primarily to the digital platforms used. It highlights the importance of taking a holistic approach to uplift cyber resilience capabilities by implementing layered security controls.

Reported Superannuation Scams

- From 2020 to 2021, there was a 323% Increase of superannuation scam reports[11]
- As of 2020, over $35.9bn payments have been made as part of the Early Release Scheme[12]
- Over 23,000 SMSF accounts are suspected to be fraudulent[8]
- In 2020 $6.4 million was lost to superannuation scams[3]



Regulations

APRA standard CPS 234 compliance 2019 and Consumer Data Rights 2020 initiatives

Cyber Threats

DevOps to respond to man in the middle attacks, online scamming and phishing

Operation Disruption

Cloud software disruptions, internal recurring incidents and infrastructure damage

Data Leakages

Complexity of data ecosystem causing reliance on third party service providers

Raising the bar

The multi-stage nature of cyberattacks means that super funds and administrators need to consider a risk management approach that directly maps mitigation techniques to each stage of the attack scenarios – and also ensure they can join the dots between stages.

Seven key areas that organisations in the superannuation industry should consider are:

1. **Perform cyber risk assessment based on real-world scenarios.** Cyber risk assessments should be based on a set of realistic attack scenario pathways that are based on how cyber criminals actually seek to attack the fund (or the third-party landscape)[15].

2. **Threat intelligence.** External threat intelligence can help monitor both the public internet and the dark web to identify emerging cyber threats and attack groups that are currently targeting super companies and their members. Moreover, this capability can also be used to identify compromised usernames/passwords and correlate this against the current passwords of members that use the member portal – which can be used for proactive outreach to members (e.g. to choose a stronger password).

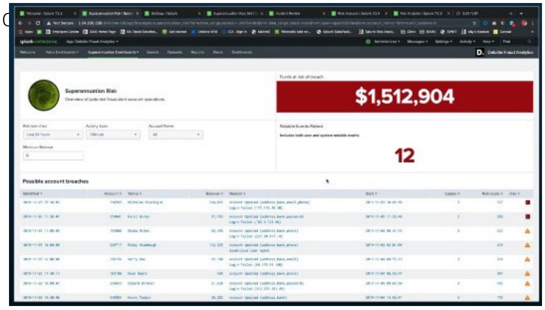
3. **Human resilience.** A significant number of cybercrime events still involve some degree of coercion of staff, third-parties or members. Modern organisations are developing role-based cyber risk assessments and learning needs analysis to develop targeted training that is specific to the risks associated with each role and includes practical examples.

4. **Effective cyber detection.** In a significant number of cyber breaches, there is an extended period of time between the initial infiltration and the risk event. However, most organisations have millions of security log events which presents an extreme 'needle in the haystack' scenario. Mature organisations are investing in sophisticated detection capability, which includes skilled analysts, and detection use-cases/behavioural analytics that are mapped to the specific financial crime risks.

5. **Incident and crisis response.** An increasing reality is that organisations experience malicious significant cyber events on a recurring basis. Significant events often put pressure on an organisation to make effective decisions under time pressure, and recent regulatory reform means that organisations are sometimes expected to perform outreach to thousands of impacted individuals. For these reasons, it's particularly important that the incident and breach response process is well defined and practiced to the point where there is familiarity across the whole organisation.

6. **Financial crime framework.** An increased focus on enforcement by financial services regulators within Australia across the superannuation sub-sector has called for a more holistic and proactive approach for linking cyber-related threats and the risk-based approach of superannuation funds' AML/CTF Programs. Enhanced maturity and maintenance of programs will be expected to be driven by a continuous feedback loop from real events and suspicious matters relevant to the industry into the organisation's AML/CTF risk assessments. The need for funds to demonstrate a parallel movement with the maturing of their financial crime prevention efforts needs to remain proportionate to the risks they face.

7. **Converged cyber & fraud capabilities.** Consolidated cyber, fraud and compliance capabilities (that all benefit from interrelated data sets) like Deloitte's Fusion platform based on our CAMS(Cyber Analytics Managed Service) architecture, can significantly improve



Deloitte Fusion platform, based on CAMS

How Deloitte can help

Data and Privacy

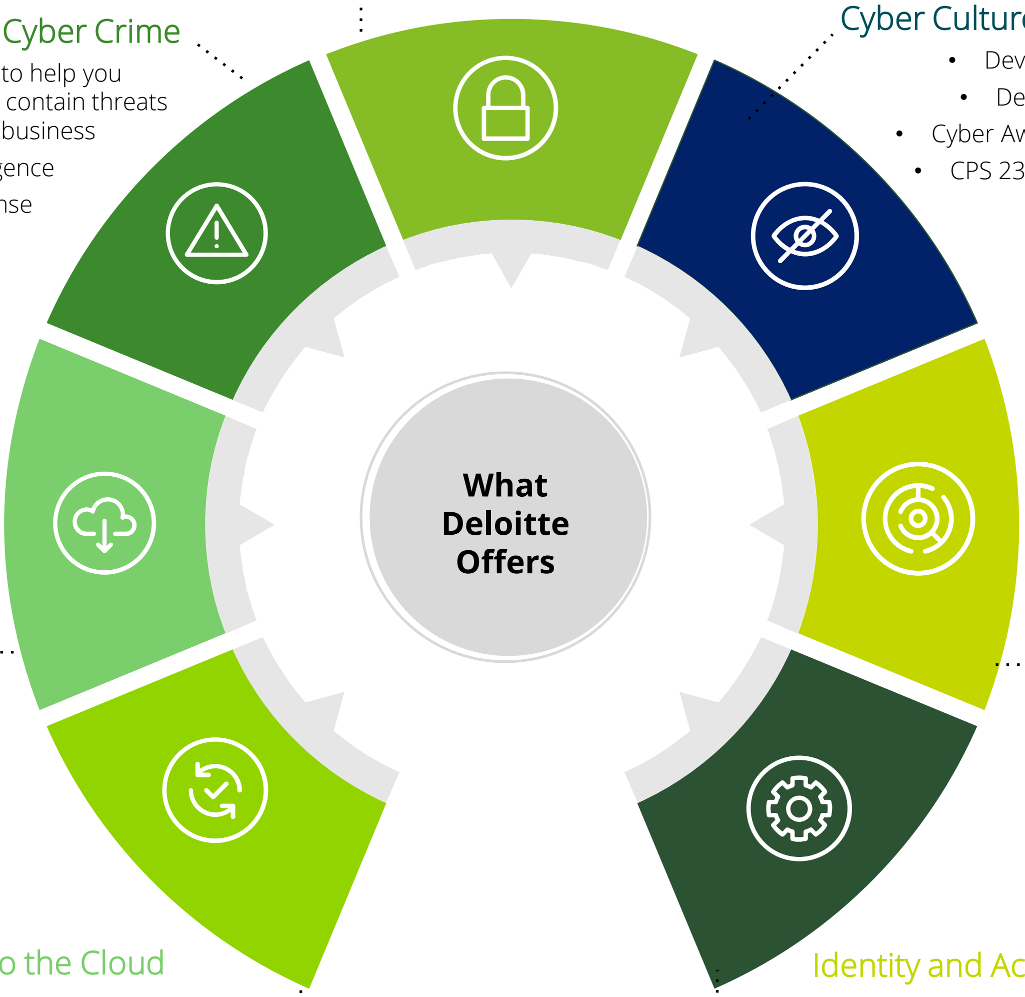
- Trust Experience Model with Responsible Data use
- Privacy Assurance
- Data Management and Protection

Cyber Crime

- Human Intelligence to help you detect, analyse, and contain threats before they disrupt business
- Cyber Threat Intelligence
- Incident and Response

Cyber Culture and Governancee

- Develop Cyber Risk Programs
- Develop Strategic Objectives
- Cyber Awareness and Governance
- CPS 234 Readiness Assessments



Transformation to the Cloud

- Cloud Governance and Compliance
- Cloud Infrastructure Security
- Security Management
- Security Strategy and Planning

Identity and Access Management

- Advanced Authentication tools
- Privileged Access and Control
- Identity Analytics and Logging

Application Security

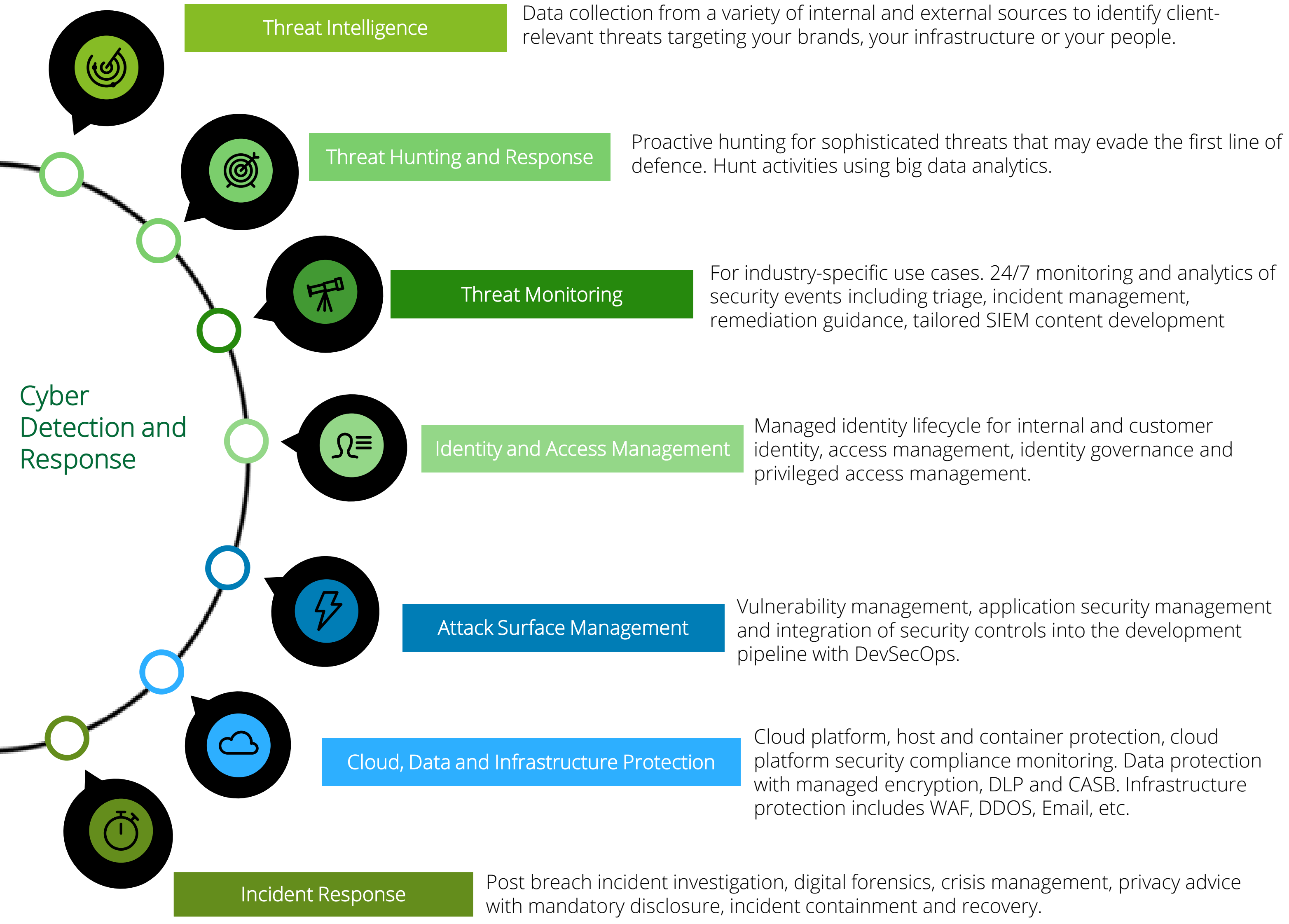
- Application and Penetration testing
- Design and Development Transformation
- GRC dashboards to deal with emerging threats

Infrastructure Security

- Asset Management
- Core Infrastructure Security
- Mobile and Endpoint Security
- Modernize and Integrate Supply Chains

Cyber managed services catalogue

Deloitte also offers the following Cyber Detection and Response services



Cyber Detection and Response

Threat Intelligence

Data collection from a variety of internal and external sources to identify client-relevant threats targeting your brands, your infrastructure or your people.

Threat Hunting and Response

Proactive hunting for sophisticated threats that may evade the first line of defence. Hunt activities using big data analytics.

Threat Monitoring

For industry-specific use cases. 24/7 monitoring and analytics of security events including triage, incident management, remediation guidance, tailored SIEM content development

Identity and Access Management

Managed identity lifecycle for internal and customer identity, access management, identity governance and privileged access management.

Attack Surface Management

Vulnerability management, application security management and integration of security controls into the development pipeline with DevSecOps.

Cloud, Data and Infrastructure Protection

Cloud platform, host and container protection, cloud platform security compliance monitoring. Data protection with managed encryption, DLP and CASB. Infrastructure protection includes WAF, DDOS, Email, etc.

Incident Response

Post breach incident investigation, digital forensics, crisis management, privacy advice with mandatory disclosure, incident containment and recovery.

Contacts

Caroline Cui
Partner
Risk Advisory
Sydney
E. carolcui@deloitte.com.au

Dinesh Santhiapillai
Partner
Risk Advisory
Melbourne
E. dsanthiapillai@deloitte.com.au

Simon Gribble
Partner
Cyber Risk
Melbourne
E. sgribble@deloitte.com.au

Evan Carvouni
Partner
Cyber Intelligence Centre
Sydney
E. ecarvouni@deloitte.com.au

Endnotes

1. https://www.gngb.com.au/wordpress/wp-content/uploads/2021/02/Securing-the-future_GNGB-Feb-2021.pdf
2. https://www.apra.gov.au/sites/default/files/Information-Paper-Cyber-Security-2016-v4.pdf
3. https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202020%20v2.pdf
4. https://treasury.gov.au/publication/p2020-super
5. https://www.ato.gov.au/uploadedFiles/Content/SPR/downloads/covid19_early_release_of_super_report_infographic.pdf
6. https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams
7. https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z
8. https://www.afr.com/policy/tax-and-super/ato-to-crack-down-on-self-managed-super-scams-20220104-p59lsi
9. https://www.abc.net.au/news/2010-05-07/identity-fraud-ringleader-arrested-in-sydney/426206
10. https://www.theaustralian.com.au/business/wealth/one-call-all-it-takes-for-superannuation-savings-to-vanish/news-story/7ca6590ed24611937b1d29ab645f31f0
11. https://www.moneymanagement.com.au/news/superannuation/323-increase-super-scam-reports
12. https://www.apra.gov.au/covid-19-early-release-scheme-issue-35-accessible-version
13. https://www.afp.gov.au/news-media/media-releases/cyber-criminals-stopped-stealing-tens-millions-dollars-afp-unleashes-new#:~:text=Museum-,Cyber%20criminals%20stopped%20from%20stealing%20tens%20of%20millions%20of,AFP%20unleashes%20new%20cyber%20punch&text=The%20AFP%20has%20stopped%20cyber,dollars%20more%20being%20siphoned%20offshore.
14. https://www.austrac.gov.au/sites/default/files/2019-06/super-annuation-risk-assessment-WEB2.pdf
15. https://www.canstar.com.au/superannuation/avoiding-superannuation-scams/
16. https://www.austrade.gov.au/news/economic-analysis/australias-pension-funds-shine-in-2021-global-rankings
17. https://www.superannuation.asn.au/resources/superannuation-statistics
18. https://ministers.treasury.gov.au/ministers/jane-hume-2020/media-releases/there-138-billion-lost-and-unclaimed-super-could-any-it-be