Cyber Governance: A Legal Perspective and Best Practices

10 CPD Hours in One Day
Legalwise – March 2025

Incident Response
FORENSIC & CYBER

Todays Presentation – in 60 Seconds

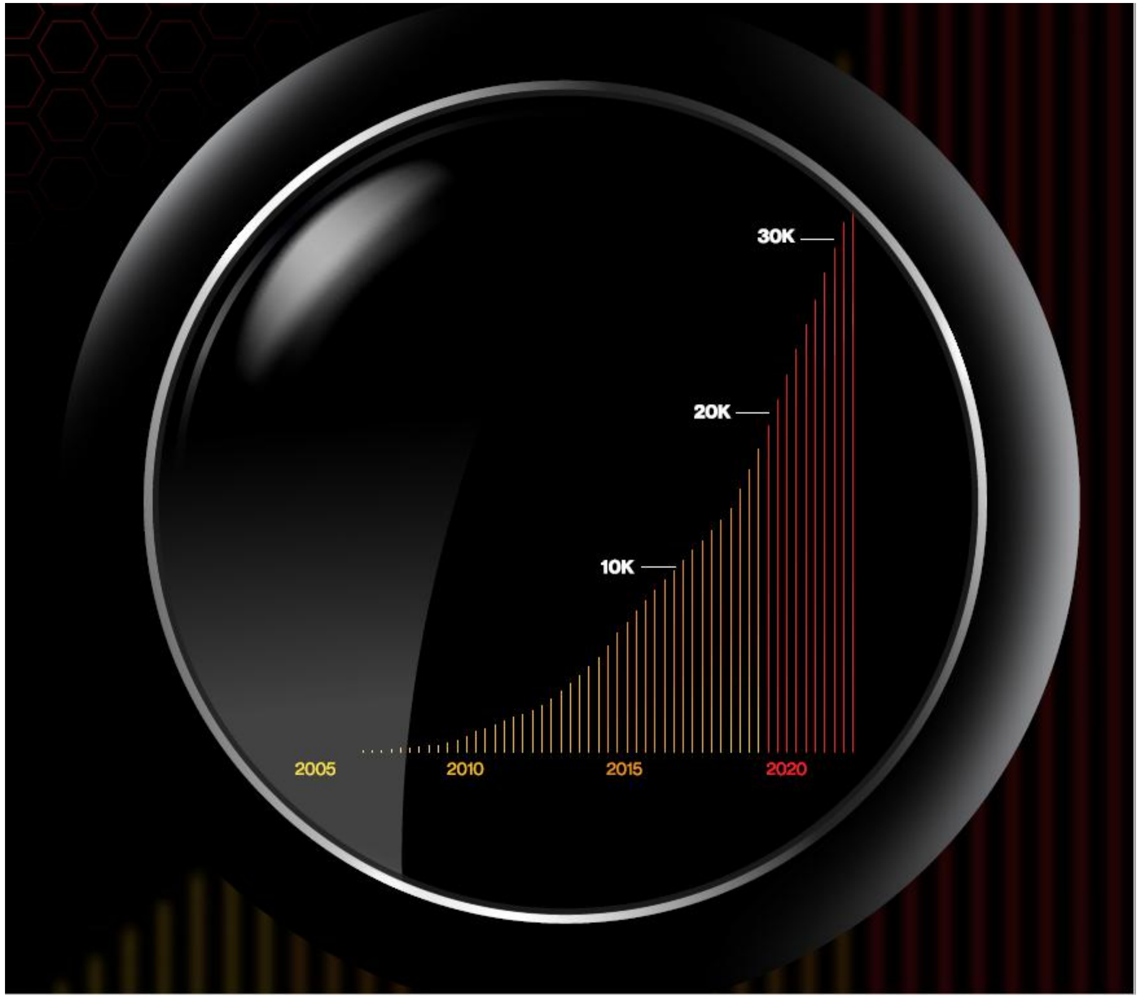
- Keeping your data secure, lessons from the increasing landscape targeting New Zealand law firms
- Cybersecurity controls
- Incident response
- Digital evidence
- Latest advancements in document analysis and review tools

Landscape

New Zealand Legal

Verizon 2024 Data Breach Investigations Report (17th Edition)

- 30,458 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 10,626 breaches that resulted in the confirmed disclosure of data to an unauthorised party.



verizon.com/dbir

What Verizon Found – Key Statistics

- **68%** of all breaches include the human element

  Error, stolen credentials or Social Engineering (Privilege Misuse removed)

- **>40%** of all Social Engineering incidents used pretexting

  Phishing and Pretexting via email make up 73% of social engineering attacks - targeting users with existing email chains and context

- **32%** of all breaches involved ransomware & extortion

  Maliciously encrypting data and demanding a ransom to return or unlock it

- **68%** increase in breaches involving a third party

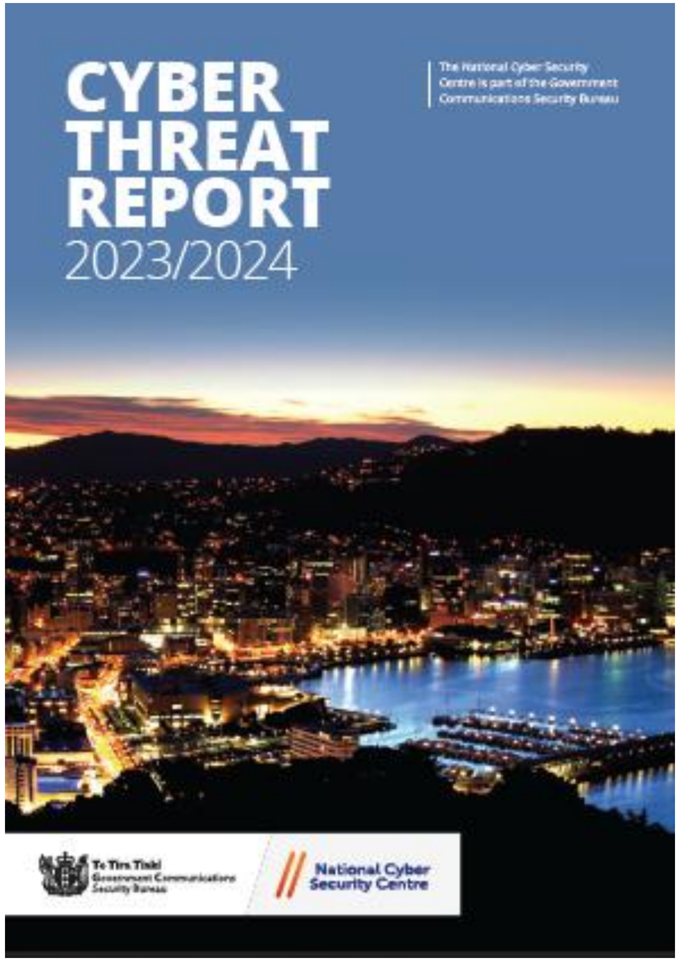
- **95%** of breaches are financially driven

  It's (almost) always about the money

Cyber Snapshot

The NCSC in a typical month:

- Detected 7 cyber incidents affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities.
- Received 22 new incident reports or requests for assistance for incidents of potential national significance.
- Recorded 565 incidents handled through the NCSC's general triage process, often affecting individual New Zealanders and small to medium businesses and organisations.



CYBER THREAT REPORT 2023/2024

The National Cyber Security Centre is part of the Government Communications Security Bureau

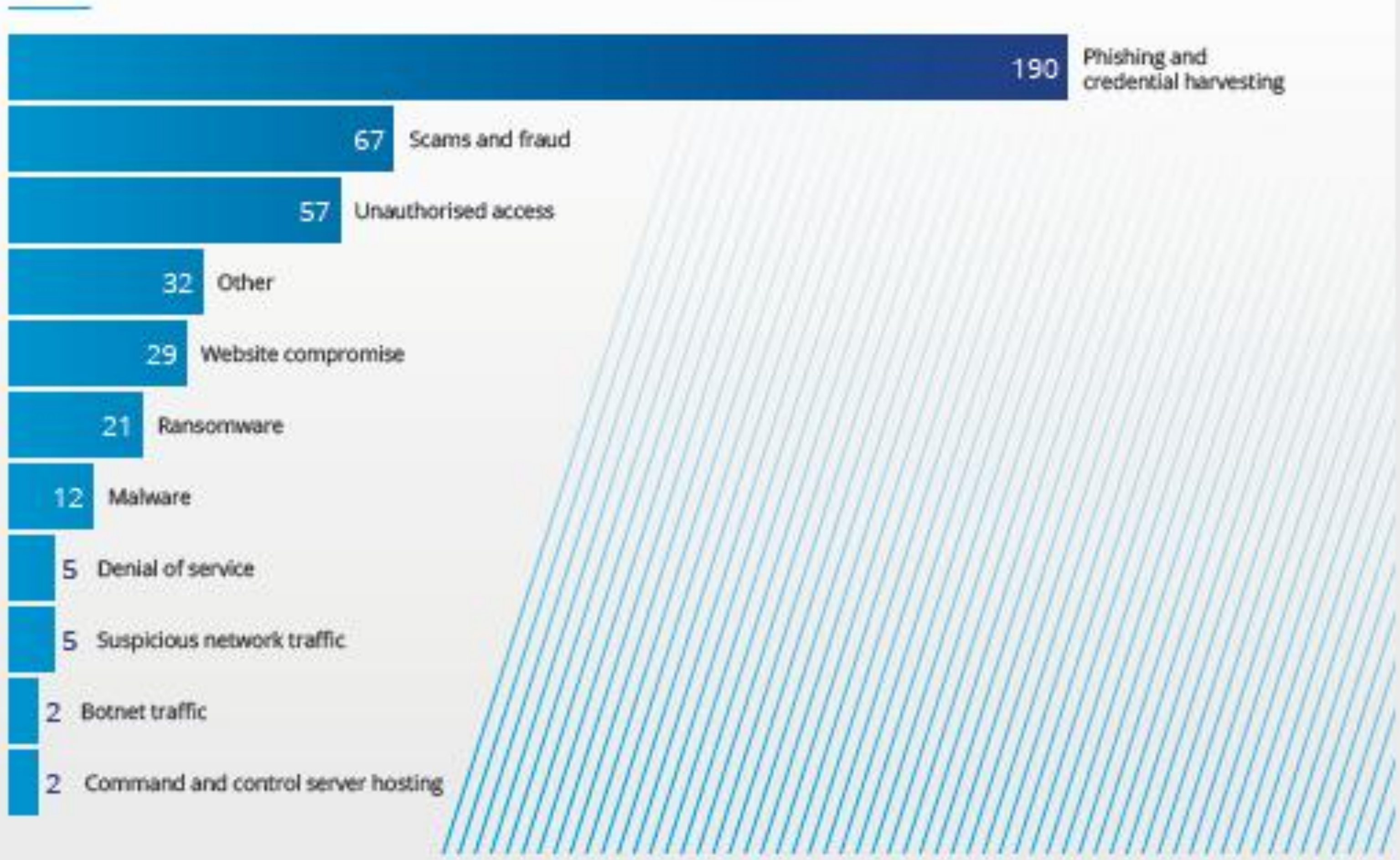
Te Tira Tiaki Government Communications Security Bureau

National Cyber Security Centre

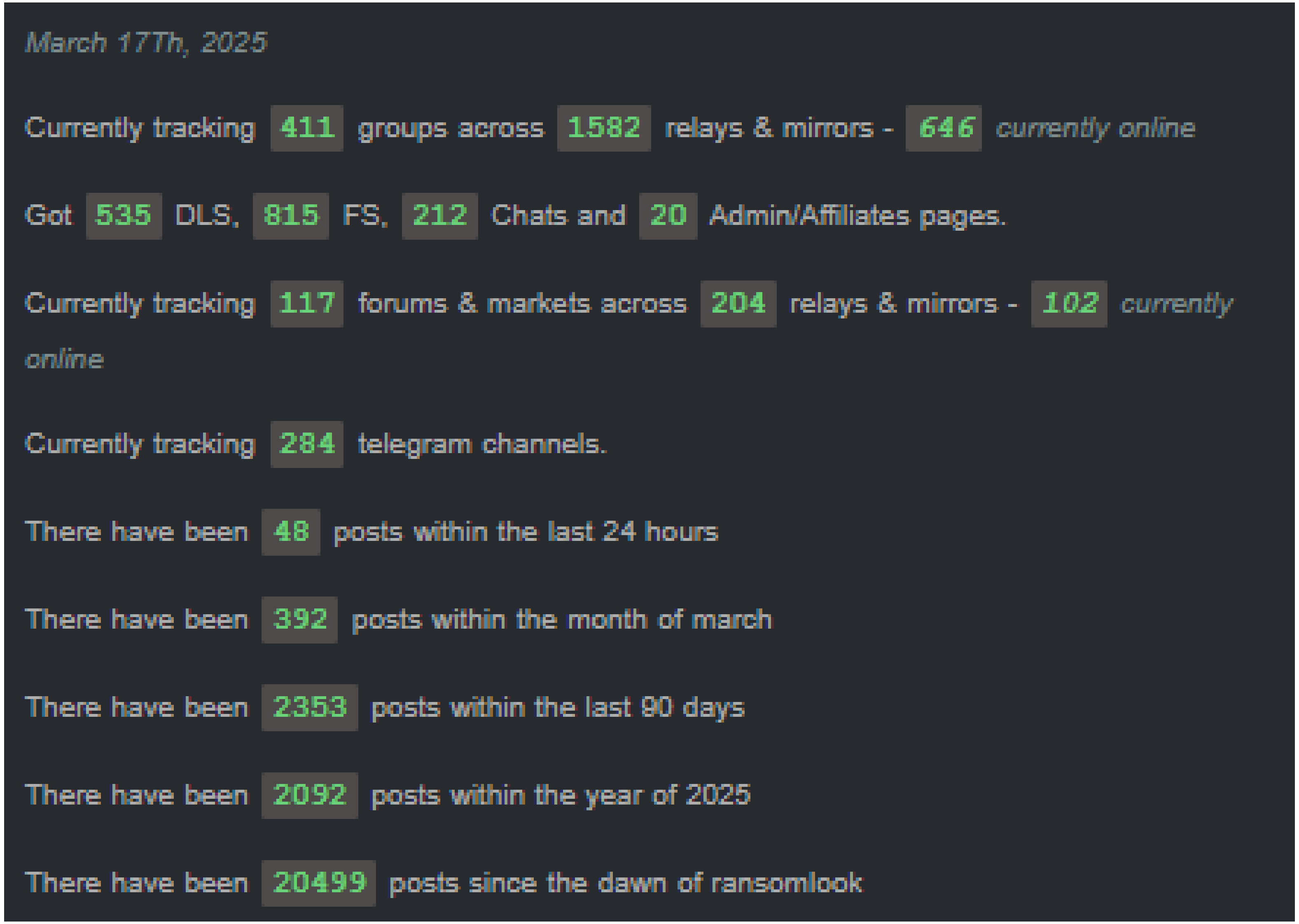
https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2024-FINAL.pdf

Cyber Snapshot

2023/2024 incidents handled through general triage process affecting organisations, primarily small to medium, by category



State of Ransomware



March 17Th, 2025

Currently tracking 411 groups across 1582 relays & mirrors - 646 *currently online*

Got 535 DLS, 815 FS, 212 Chats and 20 Admin/Affiliates pages.

Currently tracking 117 forums & markets across 204 relays & mirrors - 102 *currently online*

Currently tracking 284 telegram channels.

There have been 48 posts within the last 24 hours

There have been 392 posts within the month of march

There have been 2353 posts within the last 90 days

There have been 2092 posts within the year of 2025

There have been 20499 posts since the dawn of ransomlook

https://www.ransomlook.io

Cyber is Contextual – Law Firms

Incident
Response
FORENSIC & CYBER

INCIDENT RESPONSE
SOLUTIONS

Cyber Security Guide for NZ Law Firms

2020 Edition

https://incidentresponse.co.nz/cyber-security-for-law-firms

Law Firm Cyber Security at a Glance

- 27% have been breached (from a minor loss laptop to a major data breach). 42% of law firm business leaders rated security breaches, data loss, hacking and ransomware as a high risk to firm profitability. (*The American Bar Association's 2022 Legal Technology Survey Report)*
- 78% are extremely or somewhat concerned about cyber risk, leading to increased spend and appointments of dedicated Cyber Security Chief as it becomes more difficult to insure against cyber risk, managing cyber threats is likely to remain a key challenge with a heightened focus in the future. (*2022 Survey of Global Law Firms)*
- Every respondent suffered a security incident, with the most common attack being phishing. (*2019 Survey of Global Law Firm)*
- The most significant cyber threats to a law firm are phishing, data breaches, ransomware and supply chain compromise. (The *UK's National Cyber Security Centre 2018 Report)*

Cyber Security

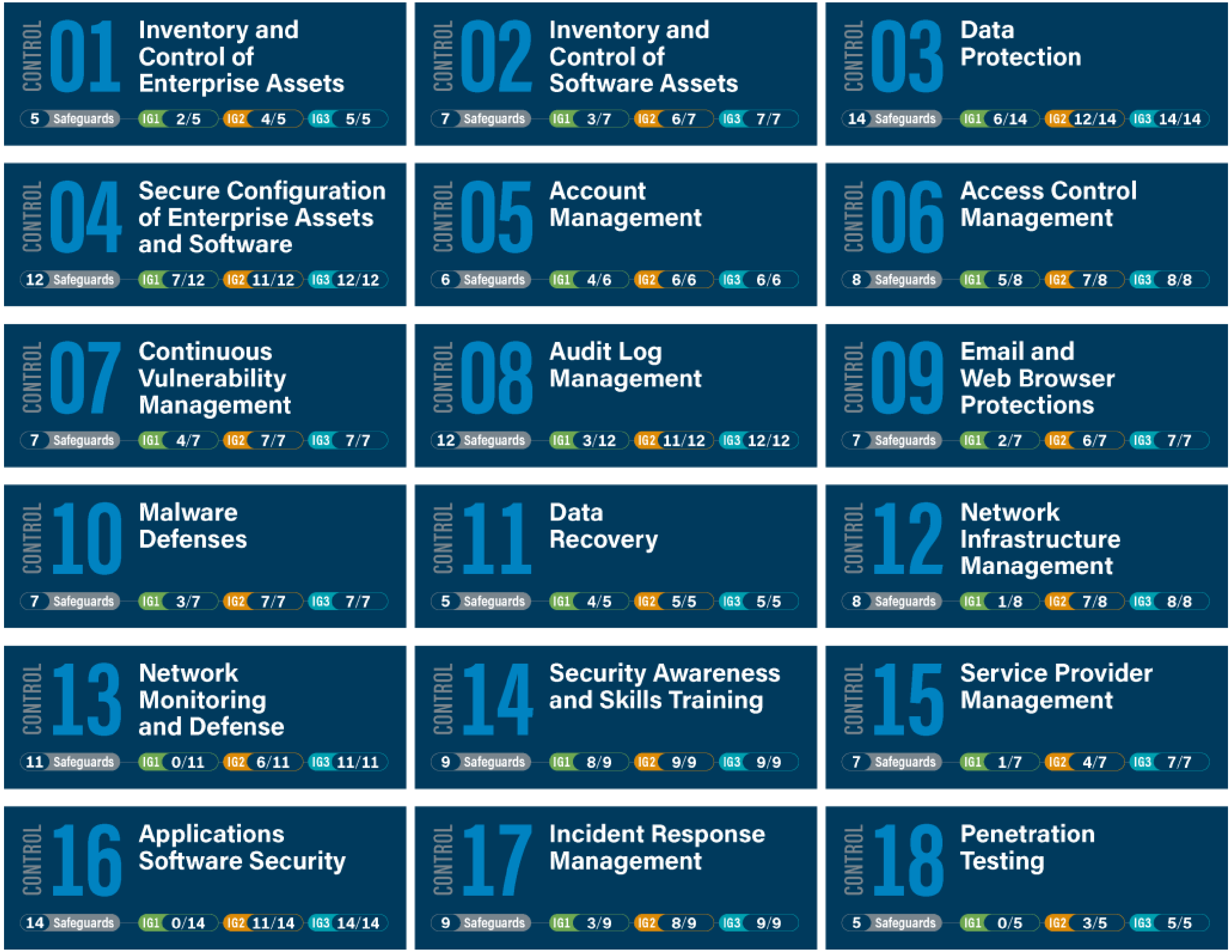
Governance and Controls

Cyber Risk Management - Controls

The CIS Controls are a set of 18 prioritised, well-vetted, and supported security actions that organisations can take to assess and improve their current security state.

The controls are designed using knowledge of actual attacks to help an organisation prioritise their investment in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented.

Cyber Risk Management - Controls



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

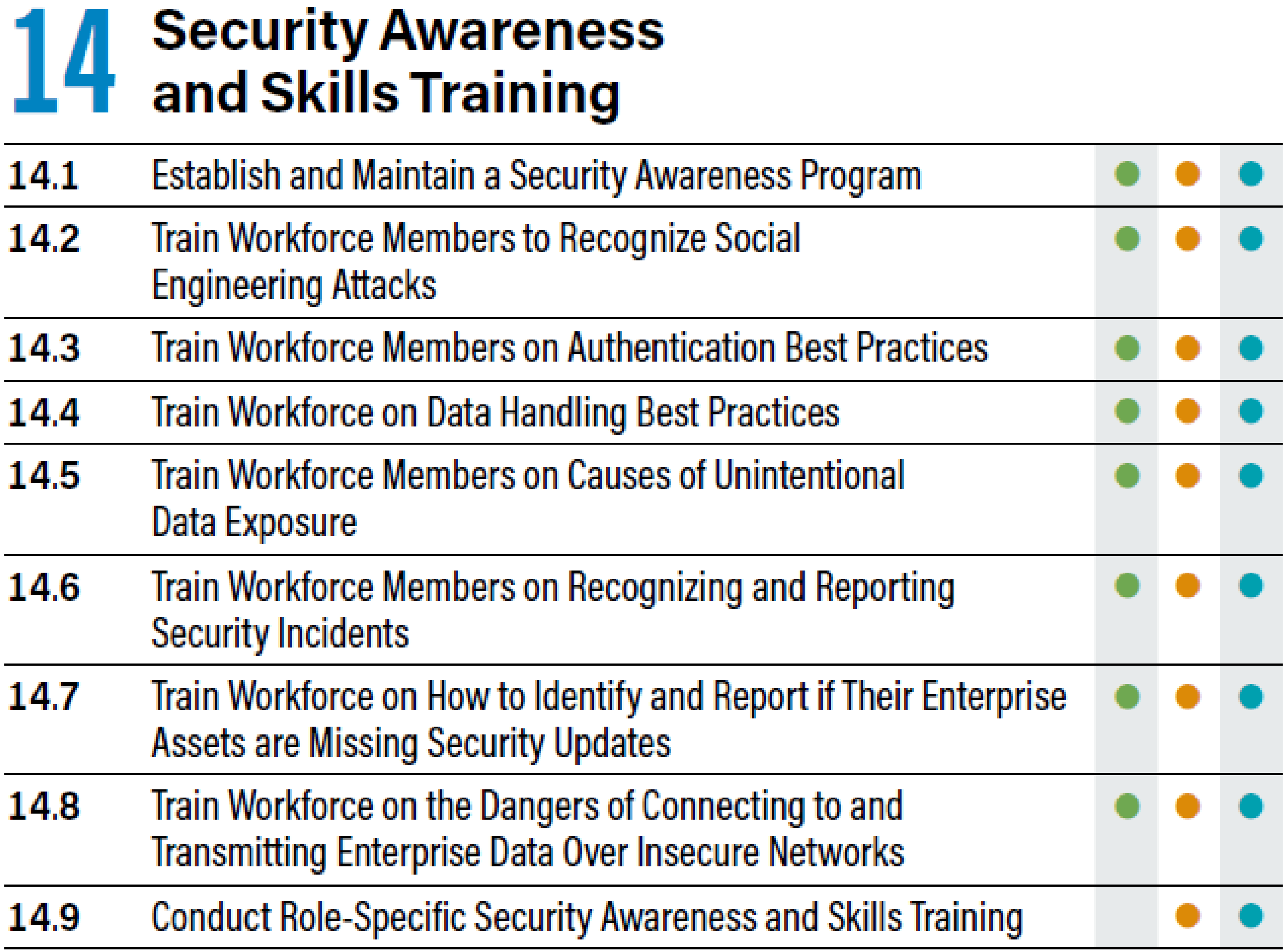
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

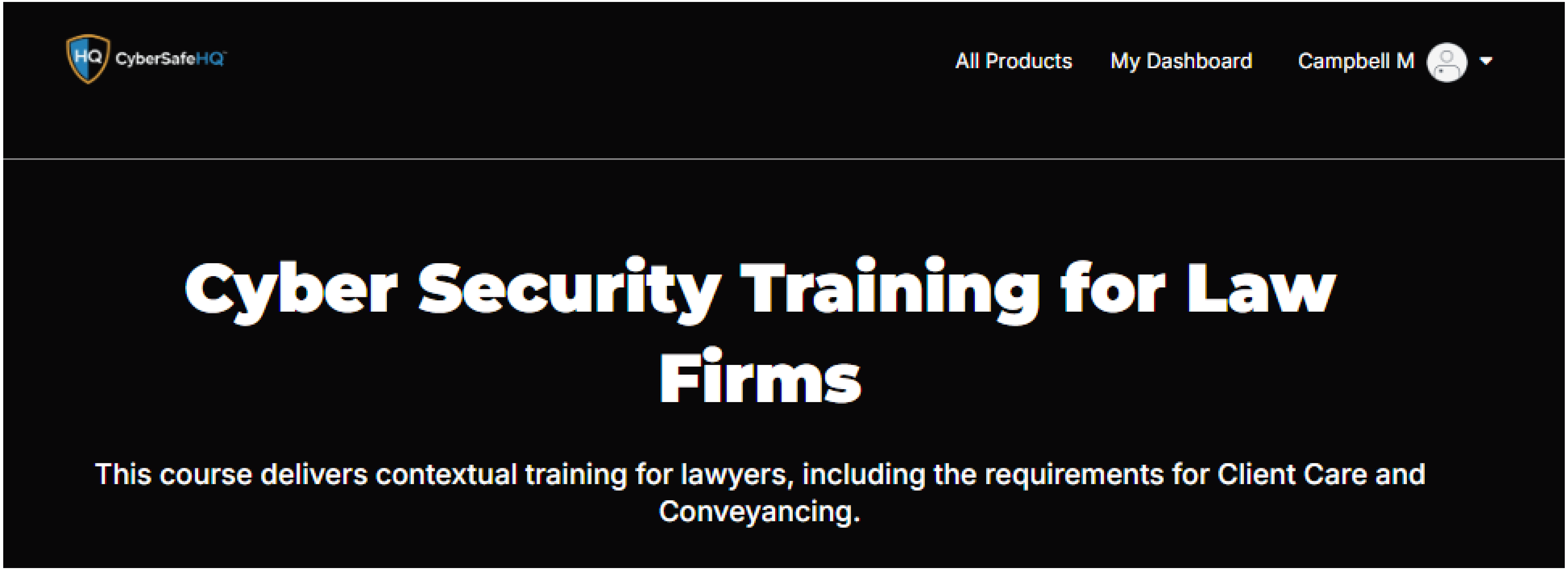
Cyber Risk Management – Security Awareness and Skills Training



14 Security Awareness and Skills Training

14.1	Establish and Maintain a Security Awareness Program	●	●	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●
14.3	Train Workforce Members on Authentication Best Practices	●	●	●
14.4	Train Workforce on Data Handling Best Practices	●	●	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●	●	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●
14.9	Conduct Role-Specific Security Awareness and Skills Training		●	●

Cyber Training and Awareness for Lawyers



Cyber Security Training for Law Firms

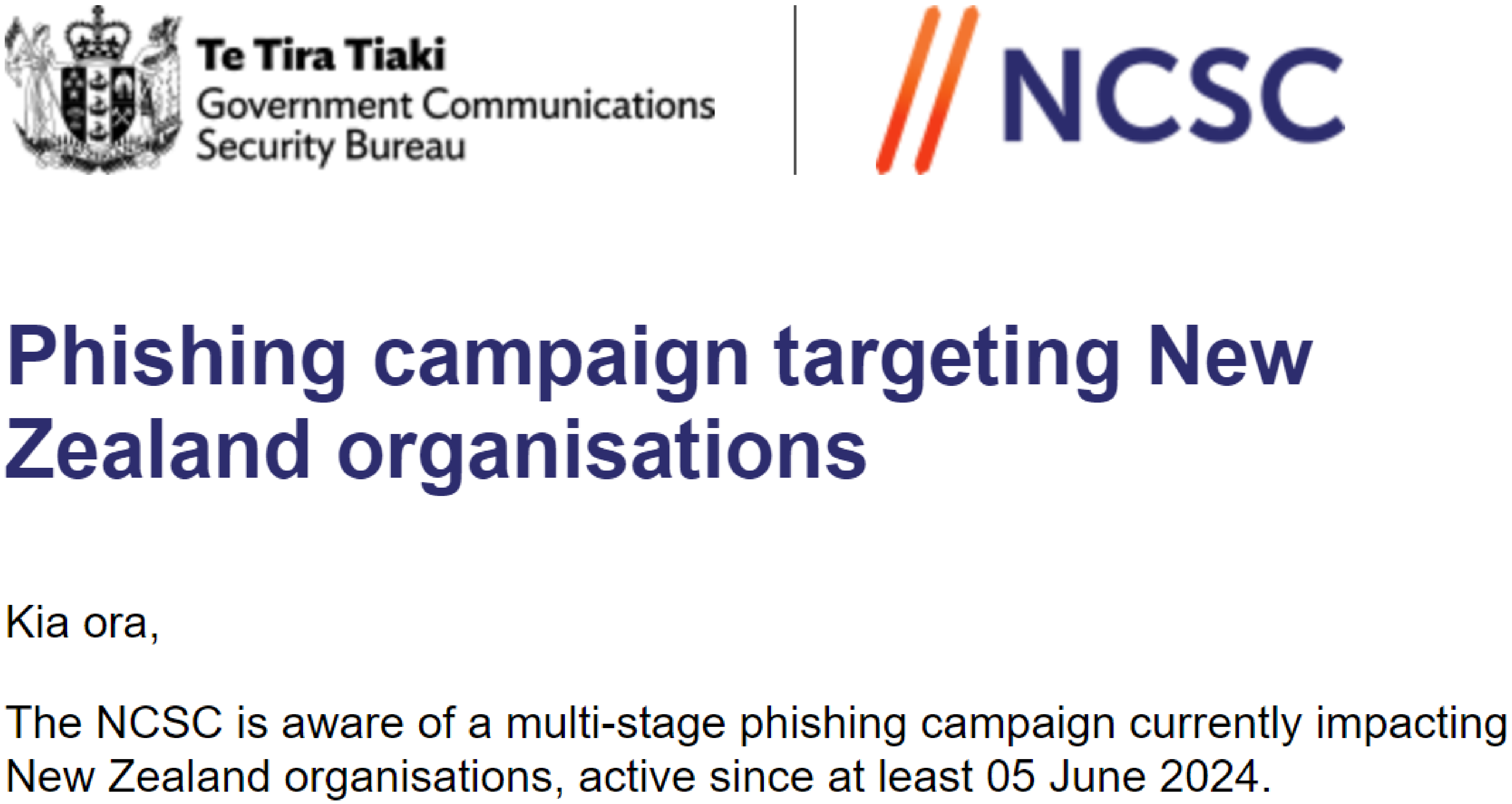
This course delivers contextual training for lawyers, including the requirements for Client Care and Conveyancing.

Cybersafehq.com

Cyber Security

Incident Response

Adversary-in-the-Middle (AiTM) – Business Email Compromise



Te Tira Tiaki
Government Communications
Security Bureau

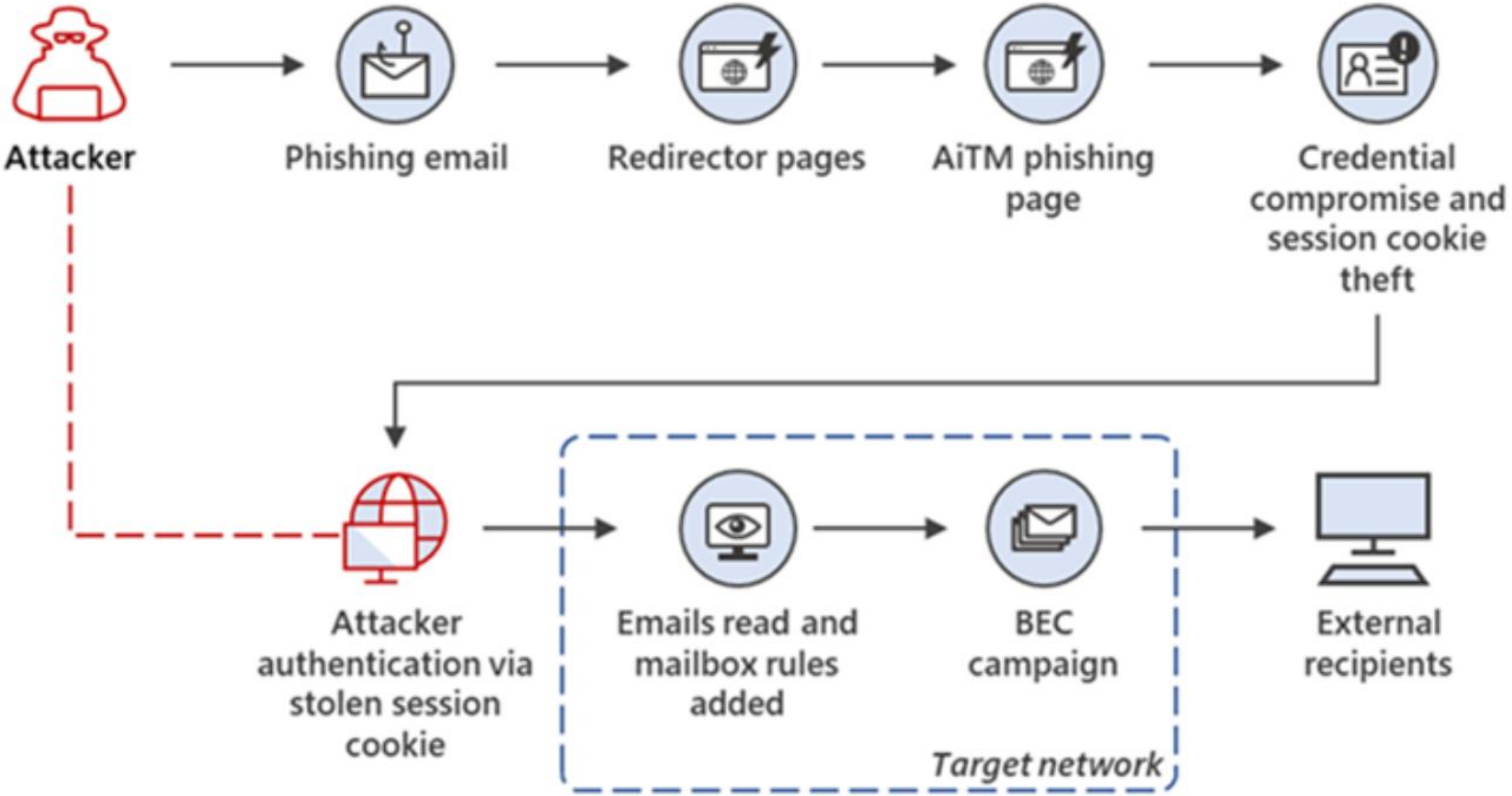
NCSC

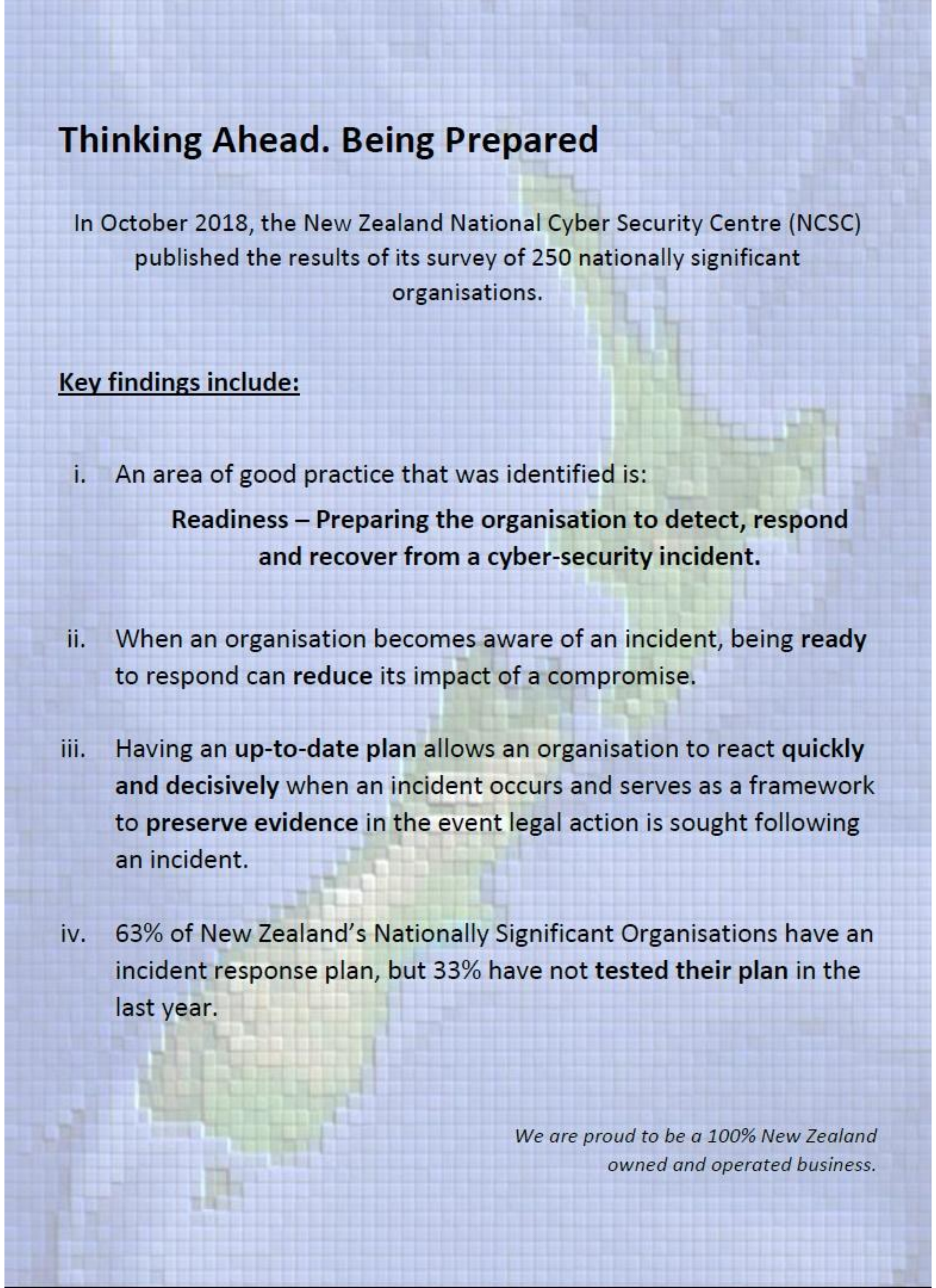
Phishing campaign targeting New Zealand organisations

Kia ora,

The NCSC is aware of a multi-stage phishing campaign currently impacting New Zealand organisations, active since at least 05 June 2024.

Adversary-in-the-Middle (AiTM) – Business Email Compromise


Attacker
Phishing email
Redirector pages
AiTM phishing page
Credential compromise and session cookie theft
Attacker authentication via stolen session cookie
Emails read and mailbox rules added
BEC campaign
External recipients
Target network



Thinking Ahead. Being Prepared

In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

<u>**Key findings include:**</u>

i. An area of good practice that was identified is:

Readiness – Preparing the organisation to detect, respond and recover from a cyber-security incident.

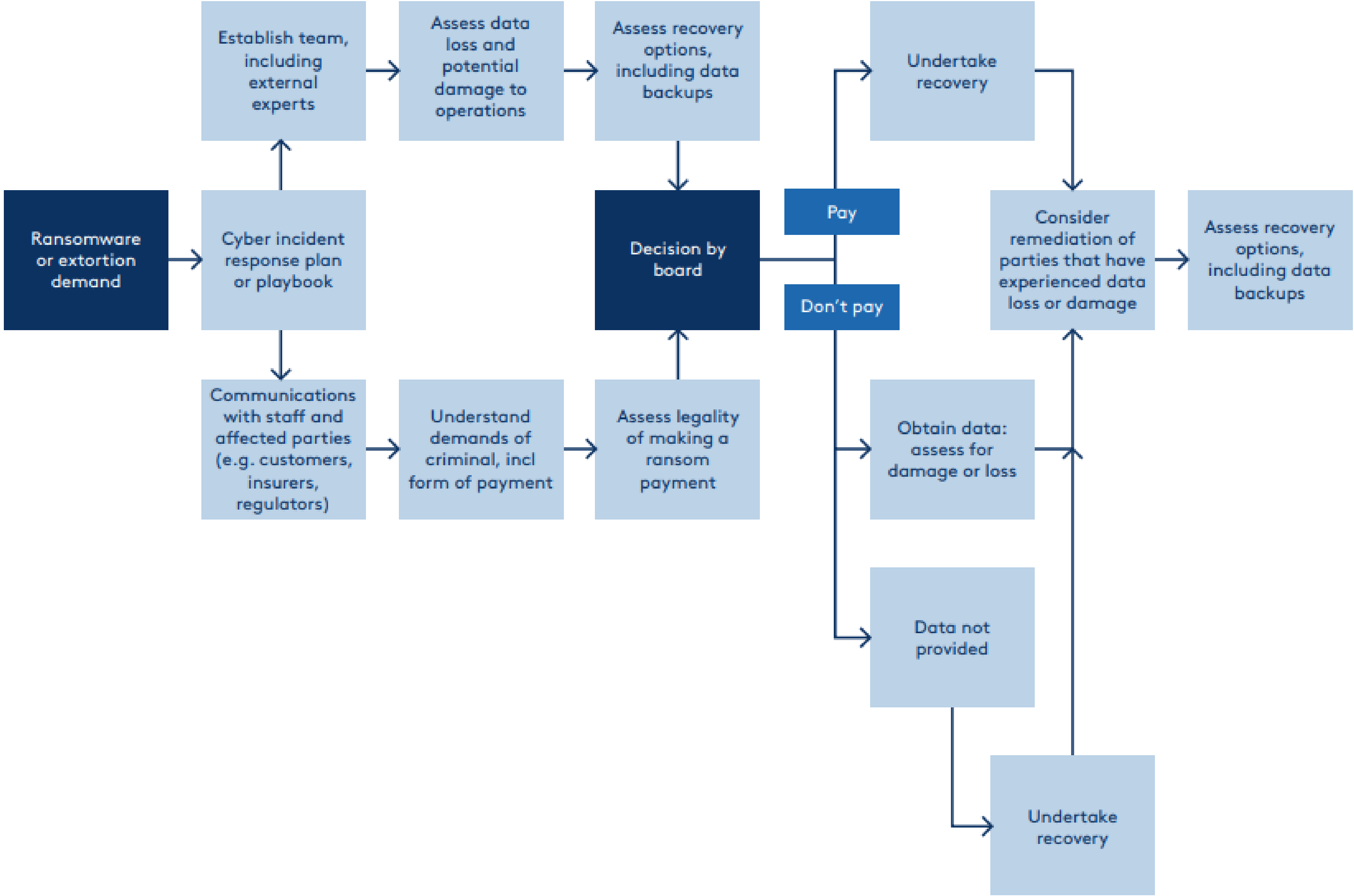
ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.

iii. Having an **up-to-date plan** allows an organisation to react **quickly and decisively** when an incident occurs and serves as a framework to **preserve evidence** in the event legal action is sought following an incident.

iv. 63% of New Zealand's Nationally Significant Organisations have an incident response plan, but 33% have not **tested their plan** in the last year.

We are proud to be a 100% New Zealand owned and operated business.

Example Ransomware Decision Making Process - AICD



Ransomware or extortion demand
Cyber incident response plan or playbook
Establish team, including external experts
Assess data loss and potential damage to operations
Assess recovery options, including data backups
Communications with staff and affected parties (e.g. customers, insurers, regulators)
Understand demands of criminal, incl form of payment
Assess legality of making a ransom payment
Decision by board
Pay
Don't pay
Undertake recovery
Obtain data: assess for damage or loss
Data not provided
Undertake recovery
Consider remediation of parties that have experienced data loss or damage
Assess recovery options, including data backups

Data Breach Response

Incident Response

FORENSIC & CYBER

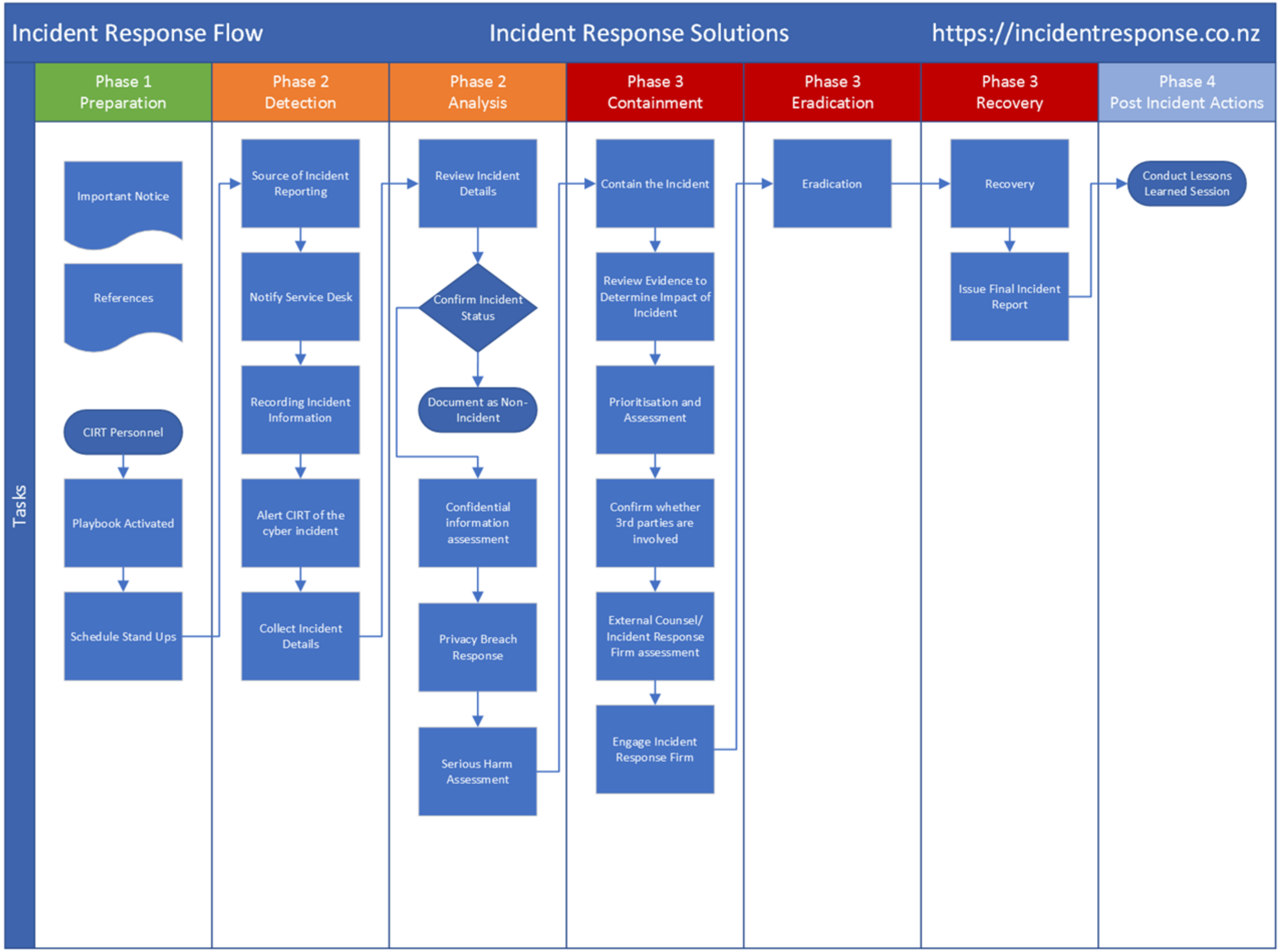
INCIDENT RESPONSE

SOLUTIONS

Data Breach Response

2020 Edition

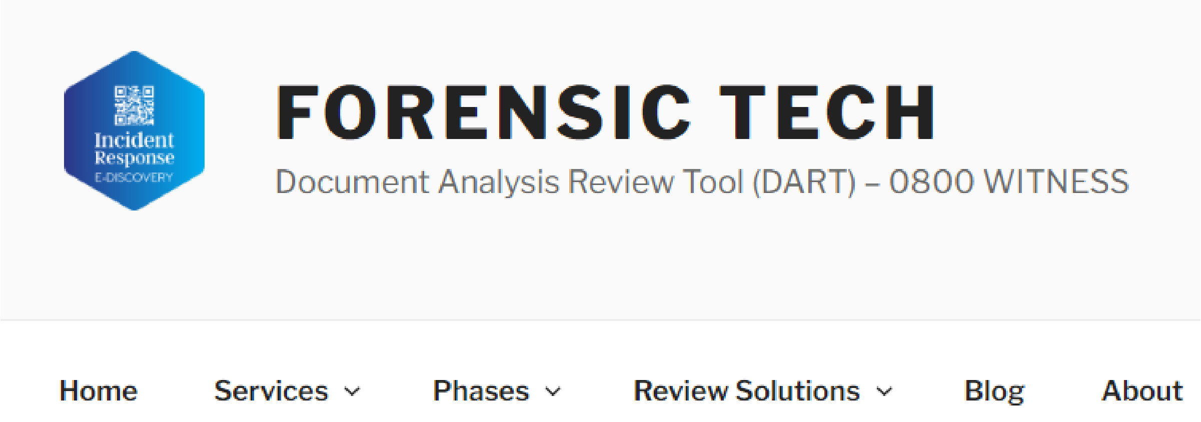
Routine Response and Investigation Methodology


Incident Response Flow
Incident Response Solutions
https://incidentresponse.co.nz
Tasks
Phase 1
Preparation
Phase 2
Detection
Phase 2
Analysis
Phase 3
Containment
Phase 3
Eradication
Phase 3
Recovery
Phase 4
Post Incident Actions
Important Notice
References
CIRT Personnel
Playbook Activated
Schedule Stand Ups
Source of Incident Reporting
Notify Service Desk
Recording Incident Information
Alert CIRT of the cyber incident
Collect Incident Details
Review Incident Details
Confirm Incident Status
Document as Non-Incident
Confidential information assessment
Privacy Breach Response
Serious Harm Assessment
Contain the Incident
Review Evidence to Determine Impact of Incident
Prioritisation and Assessment
Confirm whether 3rd parties are involved
External Counsel/ Incident Response Firm assessment
Engage Incident Response Firm
Eradication
Recovery
Issue Final Incident Report
Conduct Lessons Learned Session

Forensic Tech

Digital Evidence

Forensic Technology



FORENSIC TECH

Document Analysis Review Tool (DART) – 0800 WITNESS

Forensic Technology

Forensic Collection

eDiscovery Processing

Cloud Hosted Review

Technology Assisted Review (TAR)

Continuous Active Learning (CAL)

Government Inquiries and Independent Reviews

Case Management

Information Governance

Identification

Preservation

Collection

Processing

Review

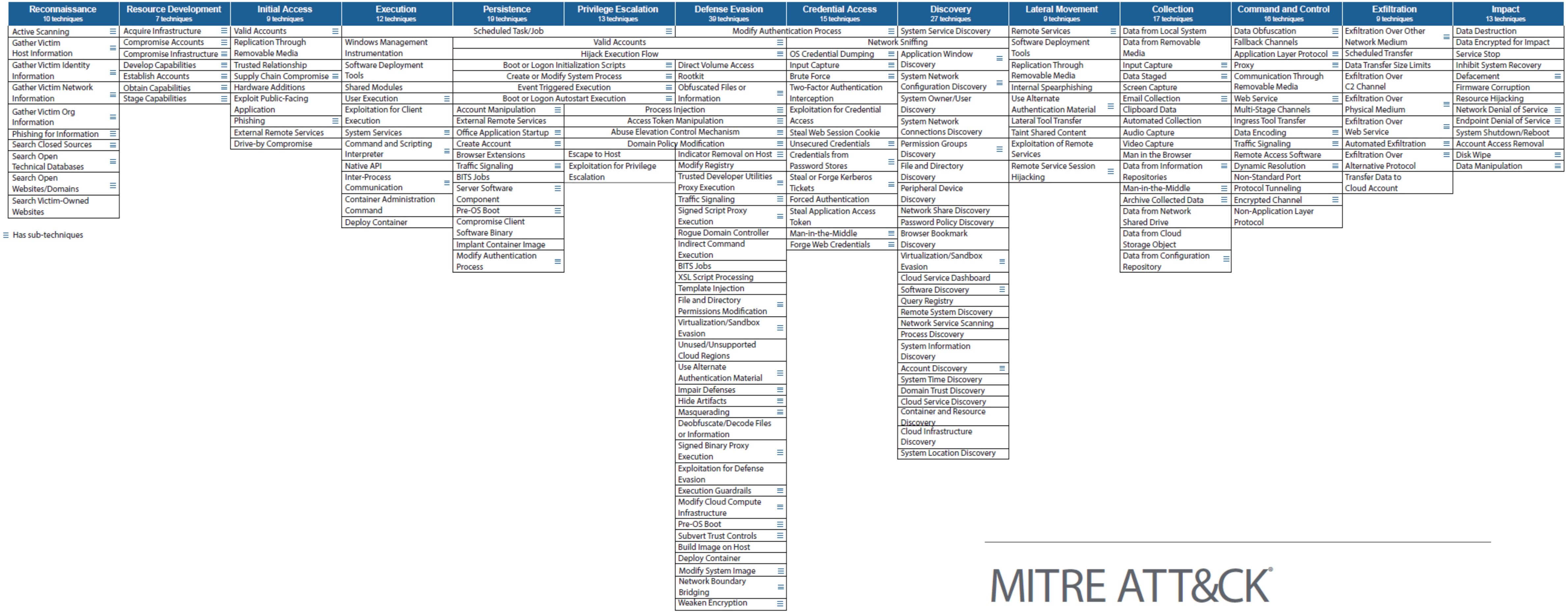
Analysis

Production

Presentation

https://forensictech.co.nz

MITRE ATT&CK®



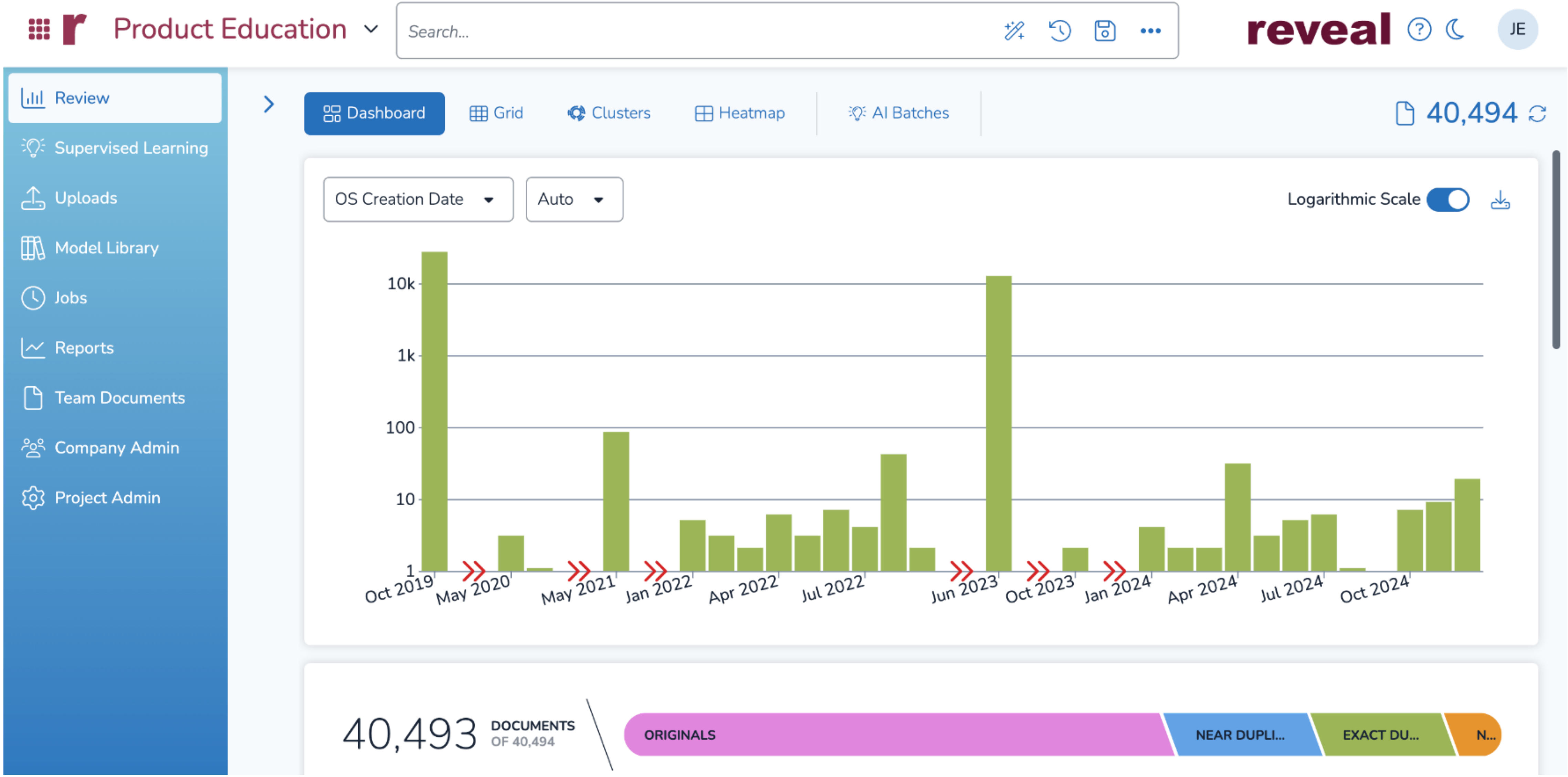
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning ☰	Acquire Infrastructure ☰	Valid Accounts ☰	Scheduled Task/Job ☰			Modify Authentication Process ☰		System Service Discovery	Remote Services ☰	Data from Local System	Data Obfuscation ☰	Exfiltration Over Other Network Medium ☰	Data Destruction
Gather Victim Host Information ☰	Compromise Accounts ☰	Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts ☰			Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Gather Victim Identity Information ☰	Compromise Infrastructure ☰	Trusted Relationship	Software Deployment Tools	Hijack Execution Flow ☰			OS Credential Dumping ☰	Application Window Discovery ☰	Replication Through Removable Media	Input Capture ☰	Application Layer Protocol ☰	Data Transfer Size Limits	Service Stop
Gather Victim Network Information ☰	Develop Capabilities ☰	Supply Chain Compromise ☰	Shared Modules	Boot or Logon Initialization Scripts ☰		Direct Volume Access	Input Capture ☰	System Network Configuration Discovery ☰	Internal Spearphishing	Data Staged ☰	Proxy ☰	Exfiltration Over C2 Channel	Inhibit System Recovery
Gather Victim Org Information ☰	Establish Accounts ☰	Hardware Additions	User Execution ☰	Create or Modify System Process ☰		Rootkit	Brute Force ☰	System Owner/User Discovery	Use Alternate Authentication Material ☰	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium ☰	Defacement ☰
Phishing for Information ☰	Obtain Capabilities ☰	Exploit Public-Facing Application	Exploitation for Client Execution	Event Triggered Execution ☰		Obfuscated Files or Information ☰	Two-Factor Authentication Interception	System Network Connections Discovery	Lateral Tool Transfer	Email Collection ☰	Web Service ☰	Exfiltration Over Web Service ☰	Firmware Corruption
Search Closed Sources ☰	Stage Capabilities ☰	Phishing ☰	System Services ☰	Boot or Logon Autostart Execution ☰			Exploitation for Credential Access	Permission Groups Discovery ☰	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Automated Exfiltration ☰	Resource Hijacking
Search Open Technical Databases ☰		External Remote Services	Command and Scripting Interpreter ☰	Account Manipulation ☰	Process Injection ☰		Steal Web Session Cookie	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Exfiltration Over Alternative Protocol ☰	Network Denial of Service ☰
Search Open Websites/Domains ☰		Drive-by Compromise	Native API	External Remote Services	Access Token Manipulation ☰		Unsecured Credentials ☰	Peripheral Device Discovery	Remote Service Session Hijacking ☰	Audio Capture	Data Encoding ☰	Transfer Data to Cloud Account	Endpoint Denial of Service ☰
Search Victim-Owned Websites			Inter-Process Communication ☰	Office Application Startup ☰	Abuse Elevation Control Mechanism ☰		Credentials from Password Stores ☰	Network Share Discovery		Video Capture	Traffic Signaling ☰		System Shutdown/Reboot
			Container Administration Command	Create Account ☰	Domain Policy Modification ☰		Steal or Forge Kerberos Tickets ☰	Password Policy Discovery		Man in the Browser	Remote Access Software		Account Access Removal
			Deploy Container	Browser Extensions	Escape to Host	Indicator Removal on Host ☰	Forced Authentication	Browser Bookmark Discovery		Data from Information Repositories ☰	Dynamic Resolution ☰		Disk Wipe ☰
				Traffic Signaling ☰	Exploitation for Privilege Escalation	Modify Registry	Steal Application Access Token	Virtualization/Sandbox Evasion ☰		Man-in-the-Middle ☰	Non-Standard Port		Data Manipulation ☰
				BITS Jobs		Trusted Developer Utilities Proxy Execution ☰	Man-in-the-Middle ☰	Cloud Service Dashboard		Archive Collected Data ☰	Protocol Tunneling		
				Server Software Component ☰		Traffic Signaling ☰	Forge Web Credentials ☰	Software Discovery ☰		Data from Network Shared Drive	Encrypted Channel ☰		
				Pre-OS Boot ☰		Signed Script Proxy Execution ☰		Query Registry		Data from Cloud Storage Object	Non-Application Layer Protocol		
				Compromise Client Software Binary		Rogue Domain Controller		Remote System Discovery		Data from Configuration Repository ☰			
				Implant Container Image		Indirect Command Execution		Network Service Scanning					
				Modify Authentication Process ☰		BITS Jobs		Process Discovery					
						XSL Script Processing		System Information Discovery					
						Template Injection		Account Discovery ☰					
						File and Directory Permissions Modification ☰		System Time Discovery					
						Virtualization/Sandbox Evasion ☰		Domain Trust Discovery					
						Unused/Unsupported Cloud Regions		Cloud Service Discovery					
						Use Alternate Authentication Material ☰		Container and Resource Discovery					
						Impair Defenses ☰		Cloud Infrastructure Discovery					
						Hide Artifacts ☰		System Location Discovery					
						Masquerading ☰							
						Deobfuscate/Decode Files or Information							
						Signed Binary Proxy Execution ☰							
						Exploitation for Defense Evasion							
						Execution Guardrails ☰							
						Modify Cloud Compute Infrastructure ☰							
						Pre-OS Boot ☰							
						Subvert Trust Controls ☰							
						Build Image on Host							
						Deploy Container							
						Modify System Image ☰							
						Network Boundary Bridging ☰							
						Weaken Encryption ☰							

☰ Has sub-techniques

MITRE ATT&CK®
Enterprise Framework

attack.mitre.org

Cloud Platform



40,494

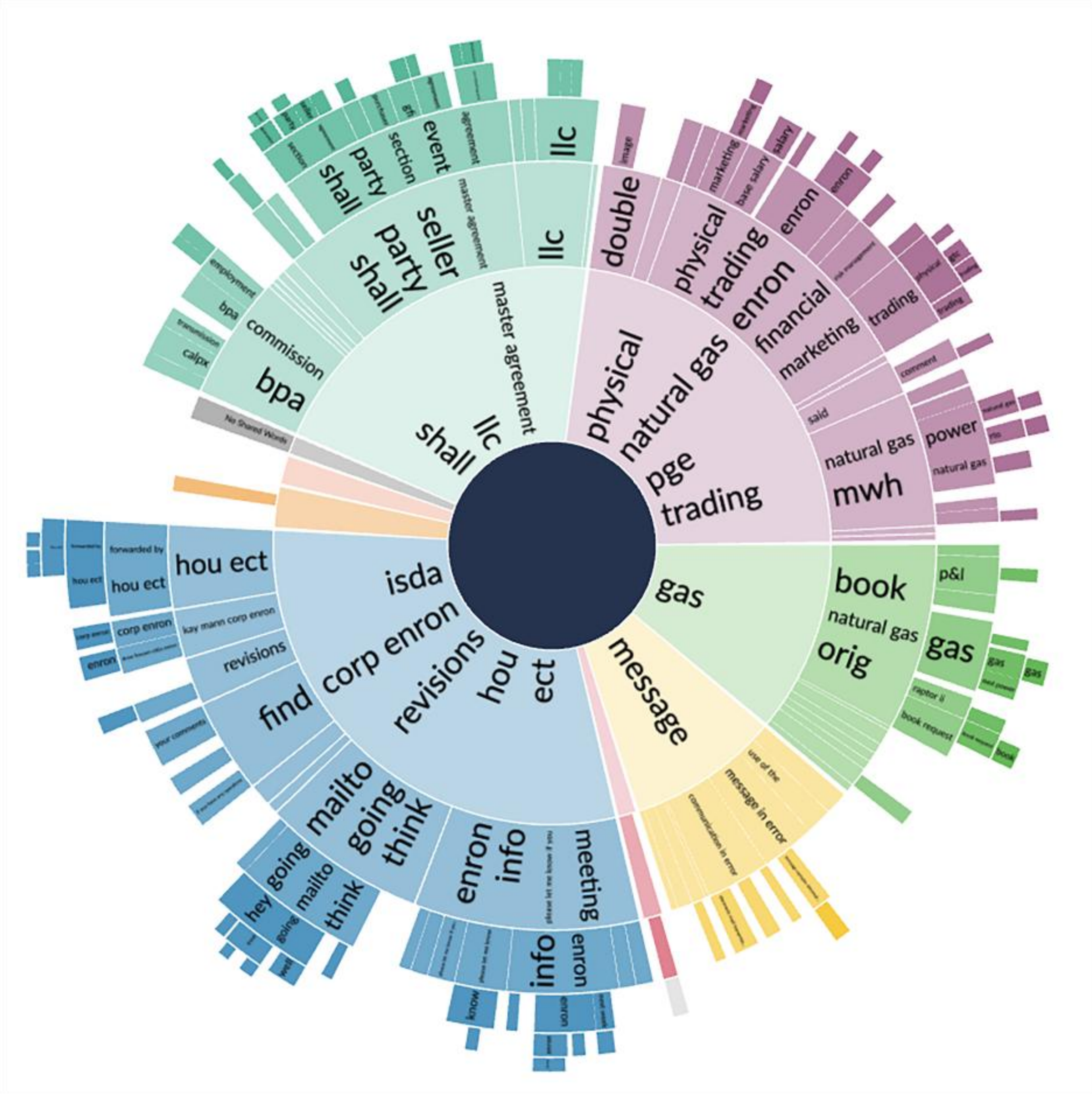
OS Creation Date

Auto

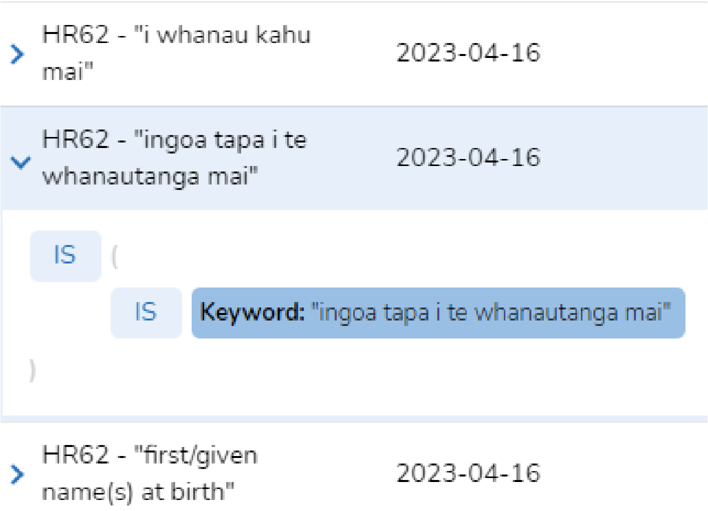
Logarithmic Scale

40,493 DOCUMENTS OF 40,494

Concept Searching and Clustering Technology



Preconfigured Search Sets – Privacy Breach

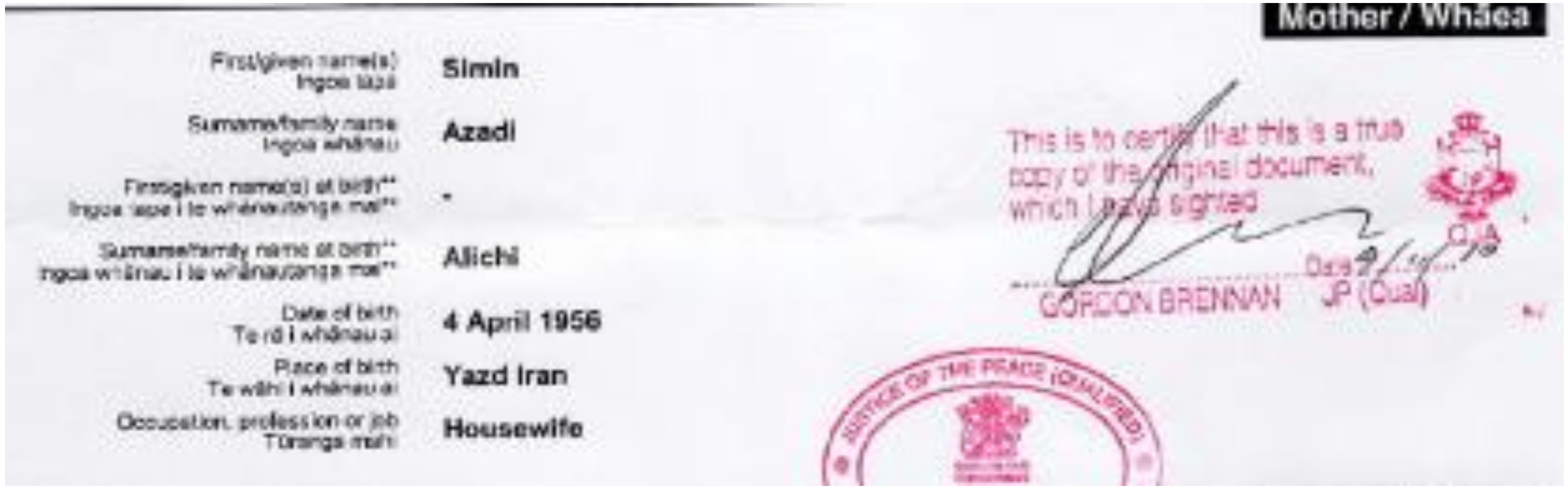


HR62 - "i whanau kahu mai" 2023-04-16

HR62 - "ingoa tapa i te whanautanga mai" 2023-04-16

IS (
IS **Keyword:** "ingoa tapa i te whanautanga mai"
)

HR62 - "first/given name(s) at birth" 2023-04-16



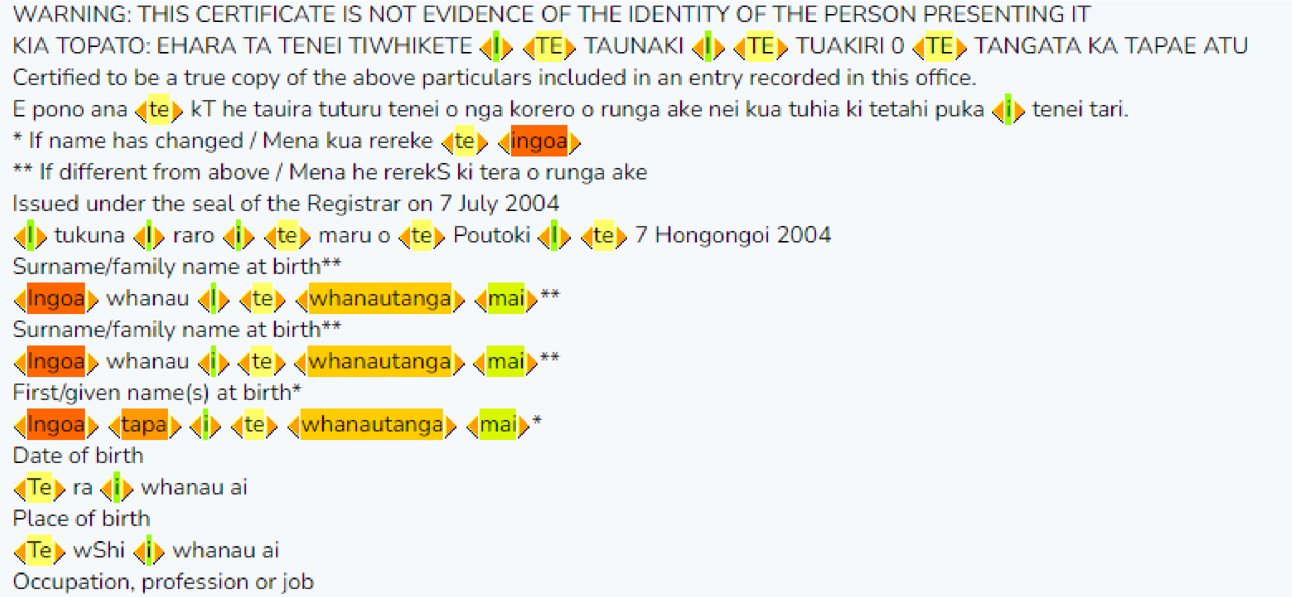
Mother / Whāea

First/given name(s) Ingoa tapa	Simin
Surname/family name Ingoa whānau	Azadi
First/given name(s) at birth** Ingoa tapa i te whānautanga mai**	-
Surname/family name at birth** Ingoa whānau i te whānautanga mai**	Alichi
Date of birth Te rā i whānau ai	4 April 1956
Place of birth Te wāhi i whānau ai	Yazd Iran
Occupation, profession or job Tūranga mahi	Housewife

This is to certify that this is a true copy of the original document, which I have sighted

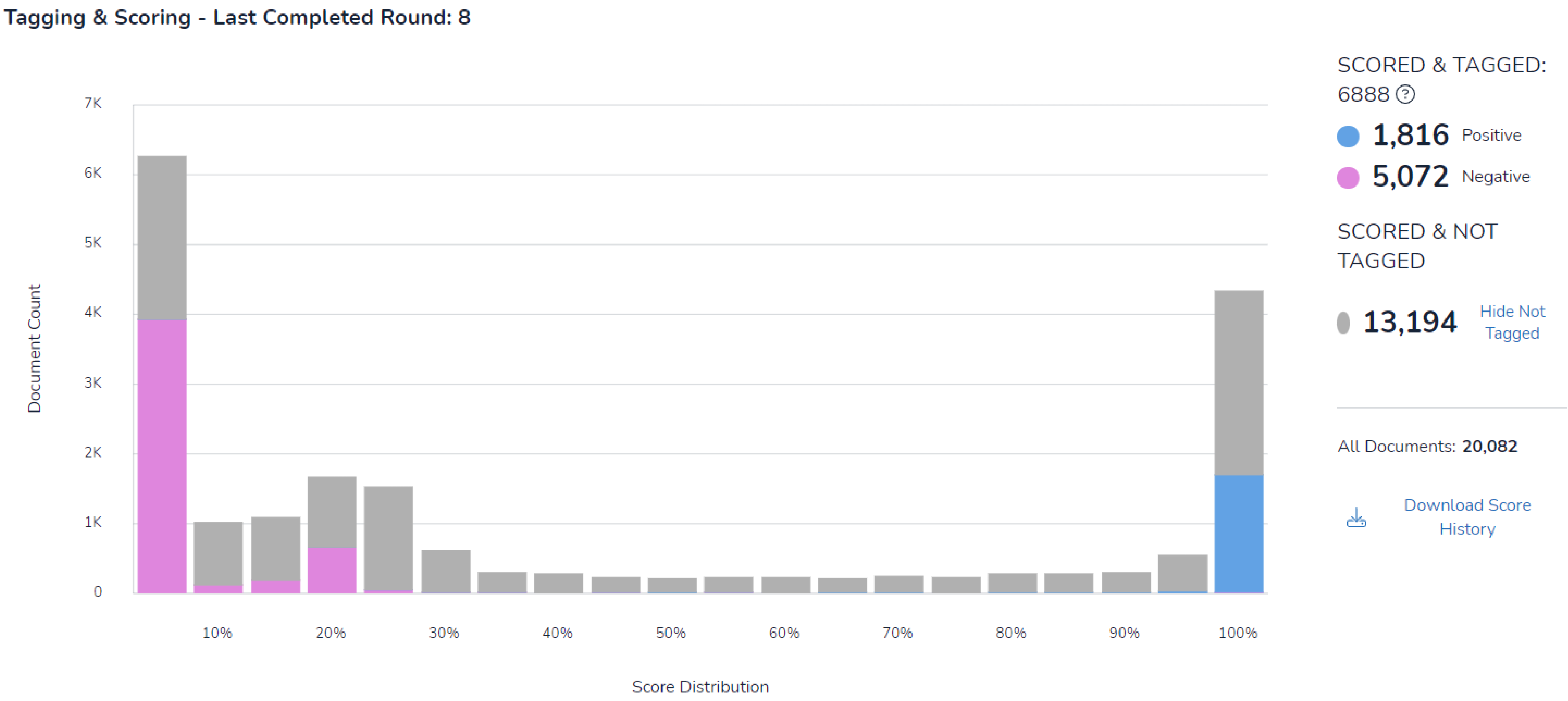
GORDON BRENNAN JP (Qual) Date 9/1/19

JUSTICE OF THE PEACE (QUALIFIED)



WARNING: THIS CERTIFICATE IS NOT EVIDENCE OF THE IDENTITY OF THE PERSON PRESENTING IT
KIA TOPATO: EHARA TA TENEI TIWHIKETE I TE TAUNAKI I TE TUAKIRI 0 TE TANGATA KA TAPAE ATU
Certified to be a true copy of the above particulars included in an entry recorded in this office.
E pono ana te kT he tauira tuturu tenei o nga korero o runga ake nei kua tuhia ki tetahi puka i tenei tari.
* If name has changed / Mena kua rereke te ingoa
** If different from above / Mena he rerekS ki tera o runga ake
Issued under the seal of the Registrar on 7 July 2004
I tukuna I raro i te maru o te Poutoki I te 7 Hongongoi 2004
Surname/family name at birth**
Ingoa whanau I te whanautanga mai**
Surname/family name at birth**
Ingoa whanau i te whanautanga mai**
First/given name(s) at birth*
Ingoa tapa i te whanautanga mai*
Date of birth
Te ra i whanau ai
Place of birth
Te wShi i whanau ai
Occupation, profession or job

Document prioritisation – Continuous Active Learning



Tagging & Scoring - Last Completed Round: 8

SCORED & TAGGED: 6888 ⓘ

● 1,816 Positive

● 5,072 Negative

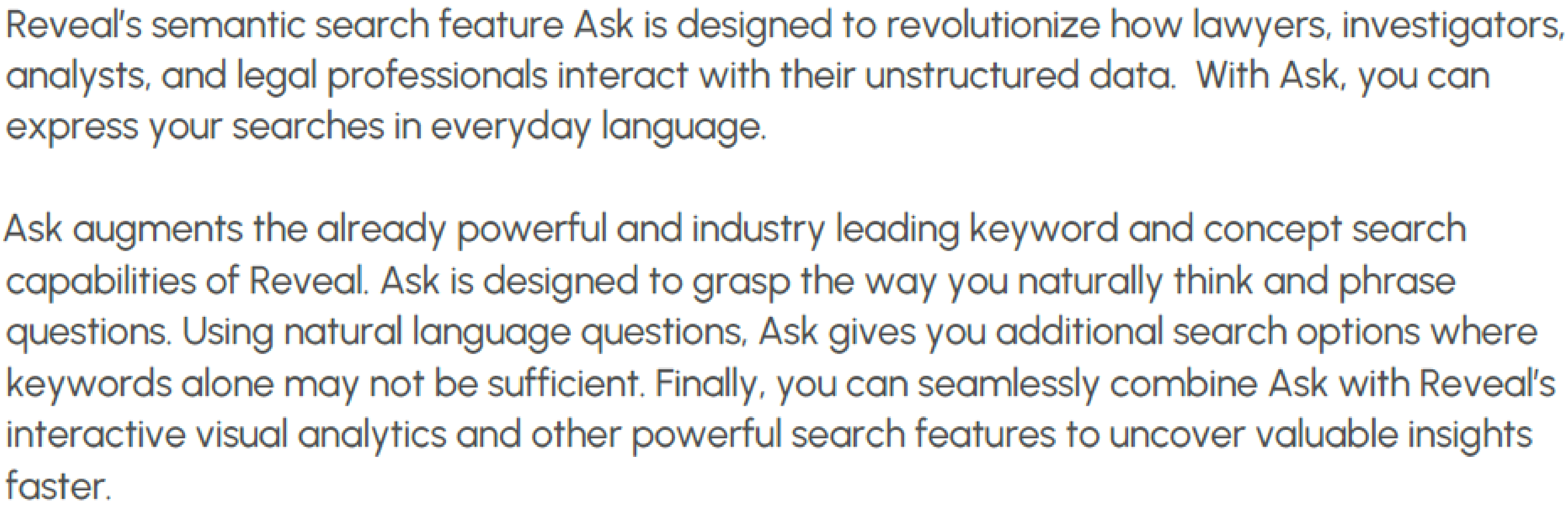
SCORED & NOT TAGGED

● 13,194 Hide Not Tagged

All Documents: **20,082**

Download Score History

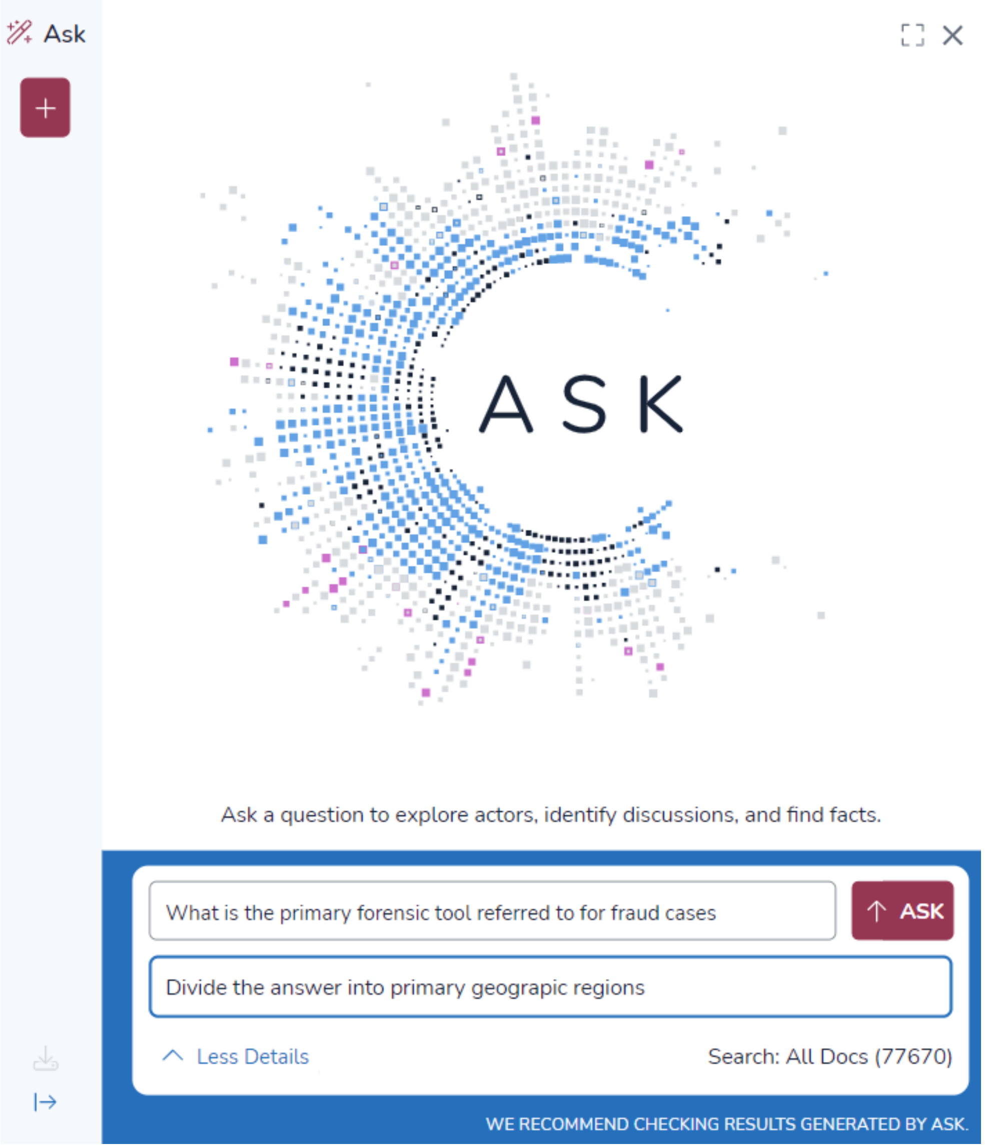
Semantic Search –Generate Results Securely



Reveal's semantic search feature Ask is designed to revolutionize how lawyers, investigators, analysts, and legal professionals interact with their unstructured data. With Ask, you can express your searches in everyday language.

Ask augments the already powerful and industry leading keyword and concept search capabilities of Reveal. Ask is designed to grasp the way you naturally think and phrase questions. Using natural language questions, Ask gives you additional search options where keywords alone may not be sufficient. Finally, you can seamlessly combine Ask with Reveal's interactive visual analytics and other powerful search features to uncover valuable insights faster.

Semantic Search –Generate Results Securely



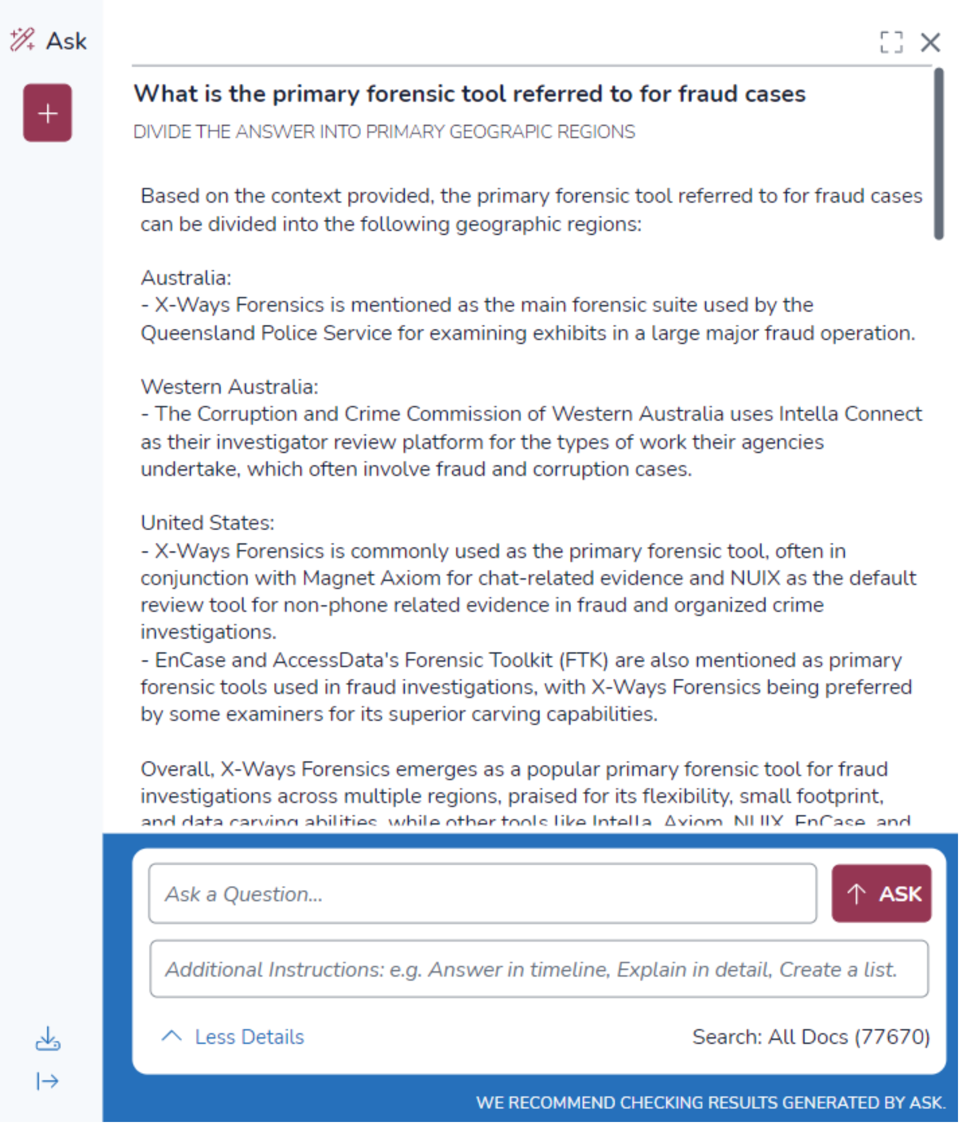
Ask a question to explore actors, identify discussions, and find facts.

What is the primary forensic tool referred to for fraud cases

Divide the answer into primary geograpic regions

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.



What is the primary forensic tool referred to for fraud cases

DIVIDE THE ANSWER INTO PRIMARY GEOGRAPIC REGIONS

Based on the context provided, the primary forensic tool referred to for fraud cases can be divided into the following geographic regions:

Australia:
- X-Ways Forensics is mentioned as the main forensic suite used by the Queensland Police Service for examining exhibits in a large major fraud operation.

Western Australia:
- The Corruption and Crime Commission of Western Australia uses Intella Connect as their investigator review platform for the types of work their agencies undertake, which often involve fraud and corruption cases.

United States:
- X-Ways Forensics is commonly used as the primary forensic tool, often in conjunction with Magnet Axiom for chat-related evidence and NUIX as the default review tool for non-phone related evidence in fraud and organized crime investigations.
- EnCase and AccessData's Forensic Toolkit (FTK) are also mentioned as primary forensic tools used in fraud investigations, with X-Ways Forensics being preferred by some examiners for its superior carving capabilities.

Overall, X-Ways Forensics emerges as a popular primary forensic tool for fraud investigations across multiple regions, praised for its flexibility, small footprint, and data carving abilities, while other tools like Intella, Axiom, NUIX, EnCase, and

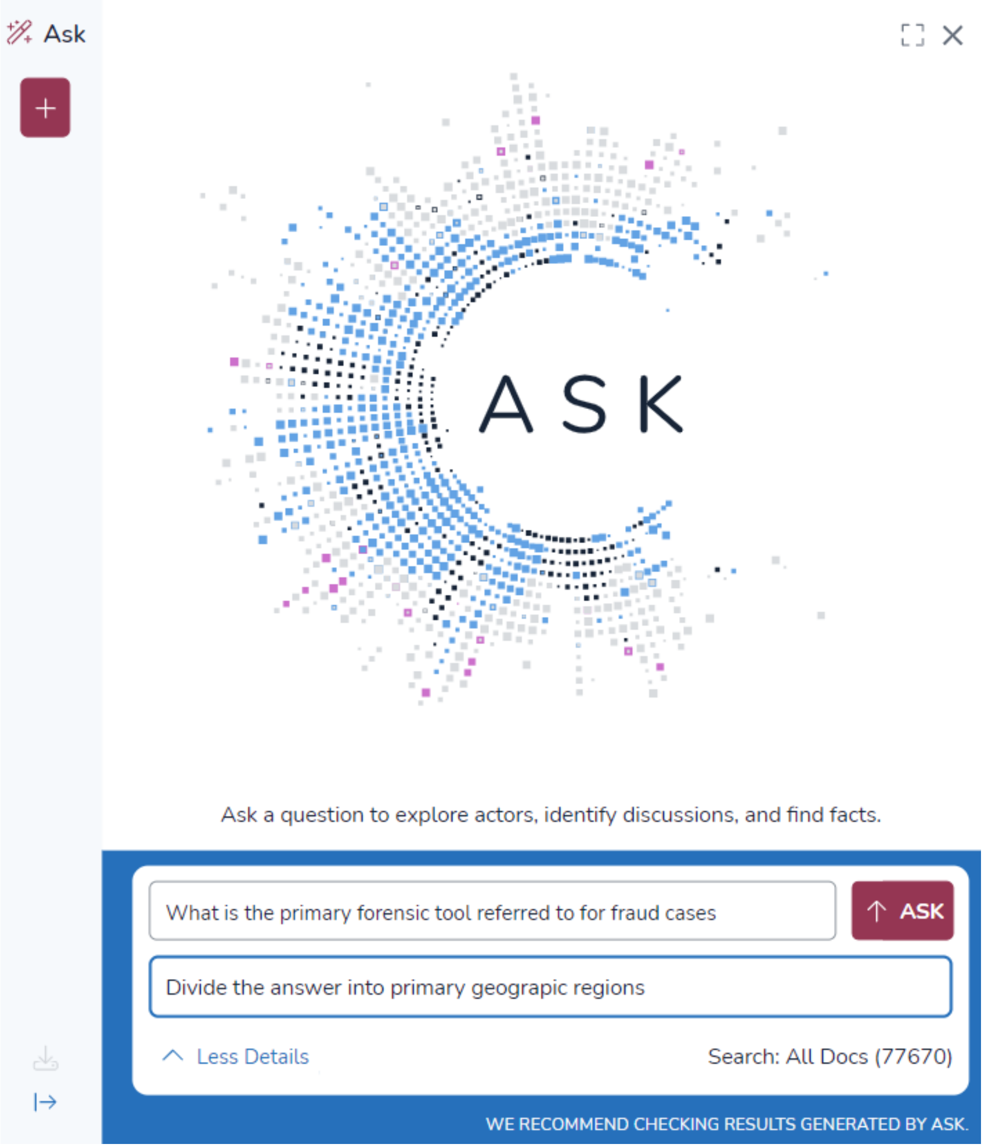
Ask a Question...

Additional Instructions: e.g. Answer in timeline, Explain in detail, Create a list.

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.

Semantic Search –Generate Results Securely



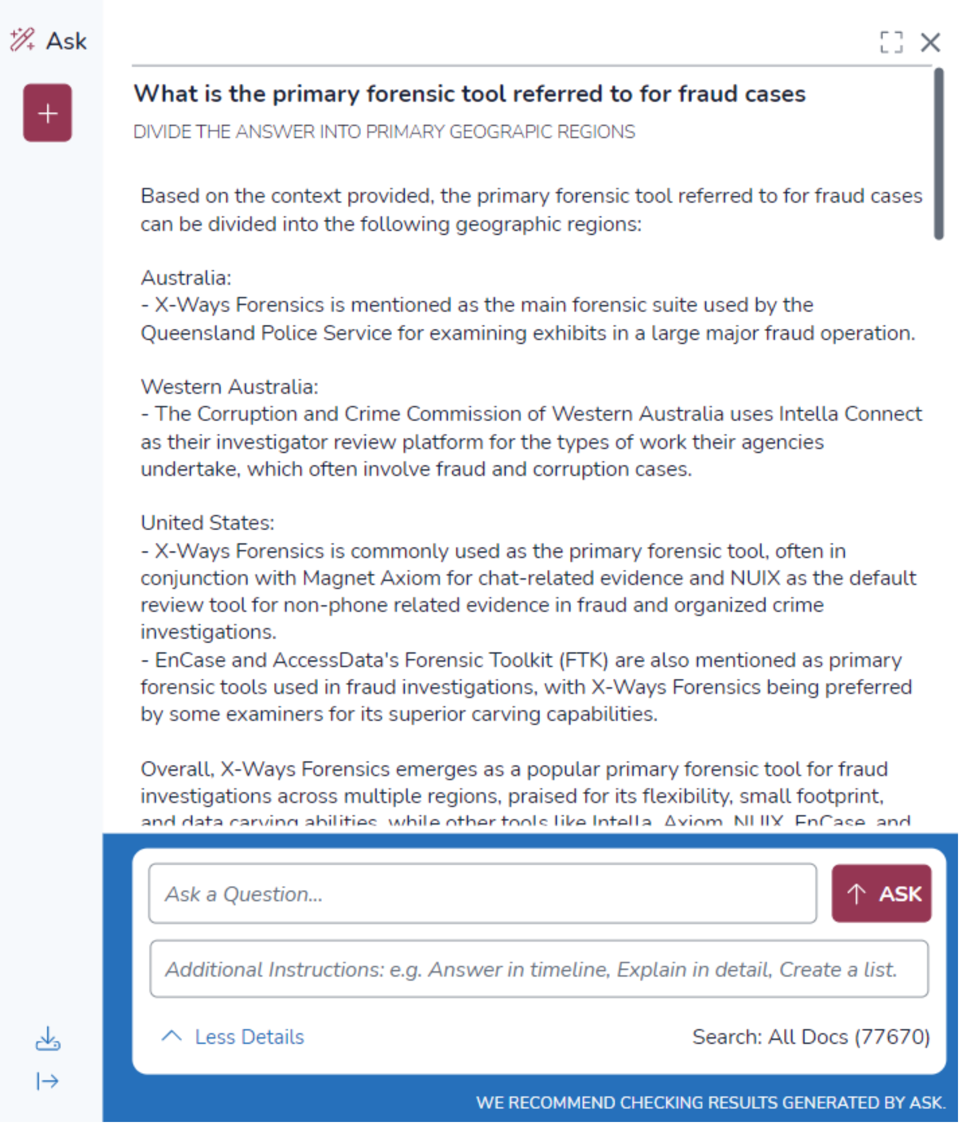
Ask a question to explore actors, identify discussions, and find facts.

What is the primary forensic tool referred to for fraud cases

Divide the answer into primary geograpic regions

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.



What is the primary forensic tool referred to for fraud cases

DIVIDE THE ANSWER INTO PRIMARY GEOGRAPIC REGIONS

Based on the context provided, the primary forensic tool referred to for fraud cases can be divided into the following geographic regions:

Australia:
- X-Ways Forensics is mentioned as the main forensic suite used by the Queensland Police Service for examining exhibits in a large major fraud operation.

Western Australia:
- The Corruption and Crime Commission of Western Australia uses Intella Connect as their investigator review platform for the types of work their agencies undertake, which often involve fraud and corruption cases.

United States:
- X-Ways Forensics is commonly used as the primary forensic tool, often in conjunction with Magnet Axiom for chat-related evidence and NUIX as the default review tool for non-phone related evidence in fraud and organized crime investigations.
- EnCase and AccessData's Forensic Toolkit (FTK) are also mentioned as primary forensic tools used in fraud investigations, with X-Ways Forensics being preferred by some examiners for its superior carving capabilities.

Overall, X-Ways Forensics emerges as a popular primary forensic tool for fraud investigations across multiple regions, praised for its flexibility, small footprint, and data carving abilities, while other tools like Intella, Axiom, NUIX, EnCase, and

Ask a Question...

Additional Instructions: e.g. Answer in timeline, Explain in detail, Create a list.

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.

Incident Response
FORENSIC & CYBER

Thank you

Campbell McKenzie
0800 WITNESS
021 779 310
campbell@incidentresponse.co.nz
incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents