

Cyber Governance: A Legal Perspective and Best Practices



Privacy Law, Cyber Governance and AI Forum
Legalwise – August 2024



**Incident
Response**

FORENSIC & CYBER

Today's 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



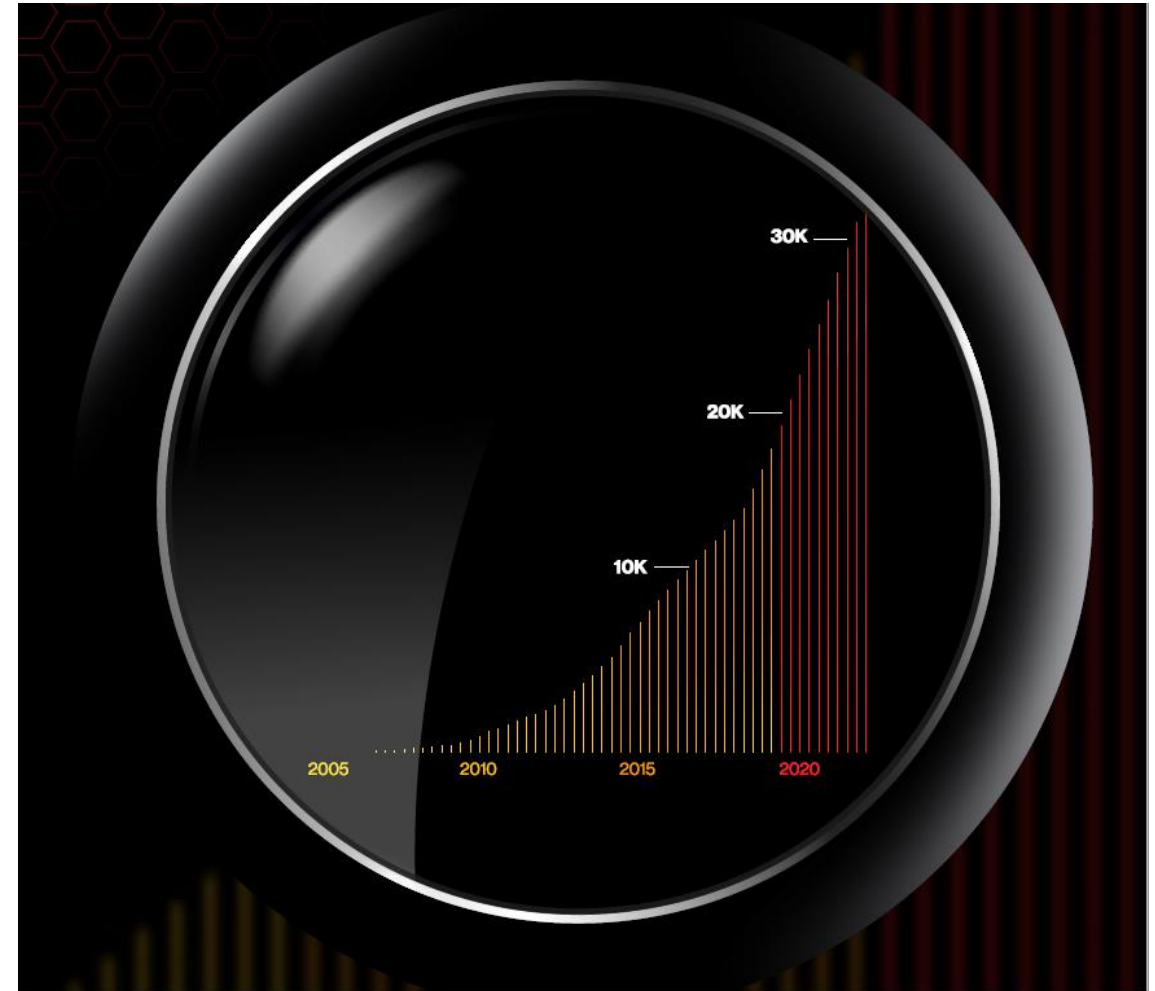


Landscape

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.



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

State of Ransomware

Welcome to 🦖 RansomLook 🦖 !

August 1st, 2024

Currently tracking **216** groups across **466** relays & mirrors - **173** currently online

Currently tracking **75** forums & markets across **116** relays & mirrors - **51** currently online

Currently tracking **245** telegram channels.

There have been **16** posts within the last 24 hours

There have been **14** posts within the month of august

There have been **1447** posts within the last 90 days

There have been **3100** posts within the year of 2024

There have been **15463** posts since the dawn of ransomlook

There are **126** custom parsers indexing posts



<https://www.ransomlook.io>

State of Ransomware in New Zealand

Year	Date	Company Name	Industry	Ransomware Strain
2018	Jul, 2018	Hawera High School	Education	Unknown
2020	Oct, 2020	Altus NZ Ltd	Business	Egregor
2020	Jun, 2020	Fisher & Paykel Appliances	Business	Nefilim
2020	Dec, 2020	Staircase Financial Management	Business	
2020	Nov, 2020	New Zealand Bloom	Business	Egregor
2021	Jul, 2021	Search and Rescue Base at Aoraki/Mount Cook	Government	Unknown
2021	Aug, 2021	Haydn	Business	LockBit
2021	Aug, 2021	Inline Plumbing	Business	LockBit
2021	Jul, 2021	Phoenix Services	Business	LockBit
2021	May, 2021	Volunteer Service Abroad	Business	Unknown
2021	May, 2021	Waikato District Health Board	Healthcare	Conti
2022	Feb, 2022	iTCo	Business	Unknown
2022	Jan, 2022	New Zealand Uniforms	Business	Conti
2022	Jan, 2022	NZ Uniforms	Business	Conti
2022	Sep, 2022	Pinnacle Midlands Health Network	Healthcare	ALPHV/BlackCat
2022	May, 2022	Enlighten Designs	Business	Unknown
2022	Nov, 2022	Mercury IT	Business	LockBit
2023	Sep, 2023	Auckland Transport	Government	Medusa
2023	Sep, 2023	Auckland University of Technology	Education	Monti
2024	May, 2024	Smith & Cagheys	Business	LockBit
2024	Jun, 2024	Elite Fitness	Business	DragonForce
2024	Jul, 2024	Competenz	Business	LockBit

Cyber is Contextual – Law Firms



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



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 Security

Incident Response

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



Te Tira Tiaki
Government Communications
Security Bureau

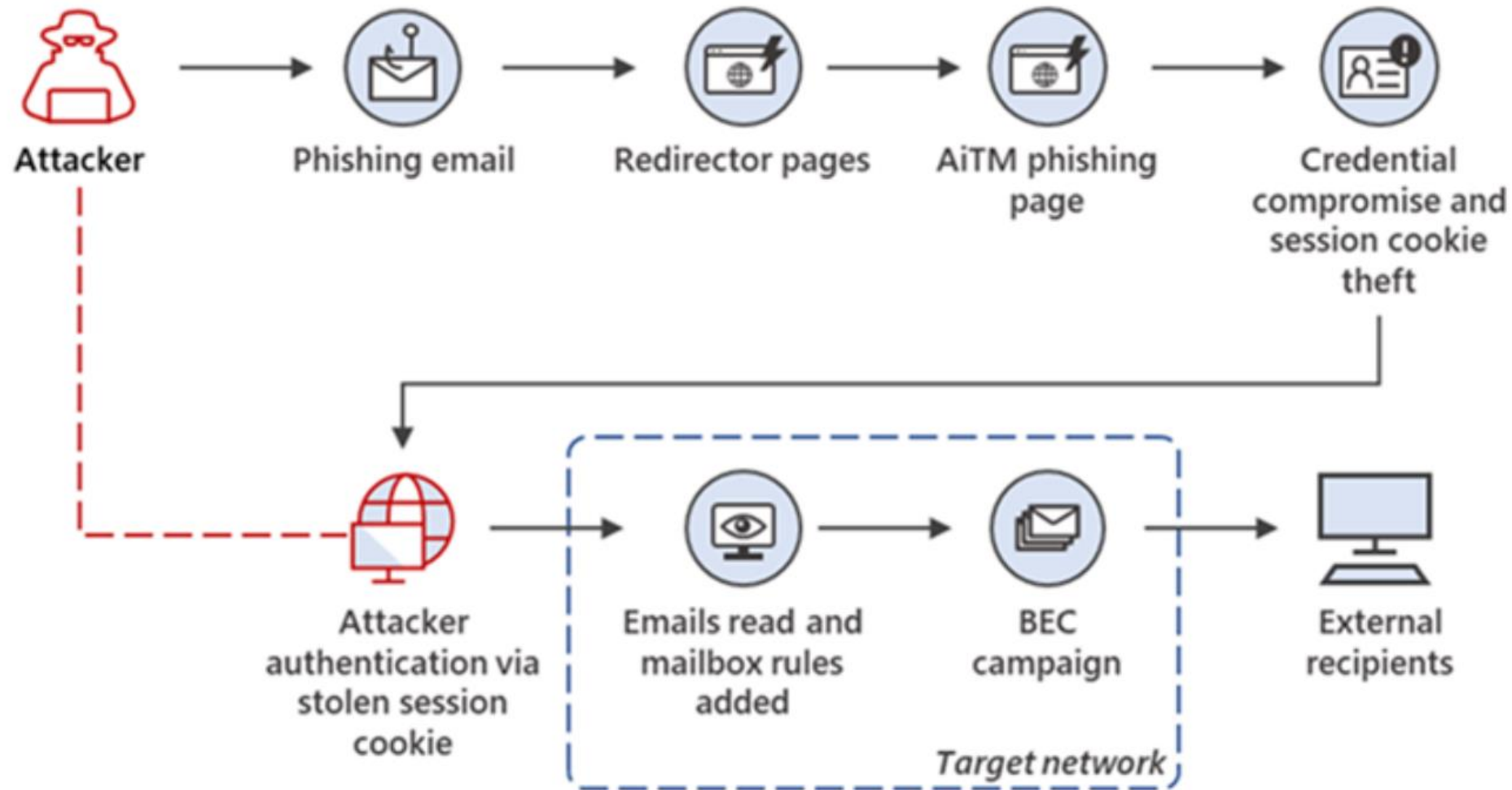


Phishing campaign targeting New Zealand organisations

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



Thinking Ahead. Being Prepared

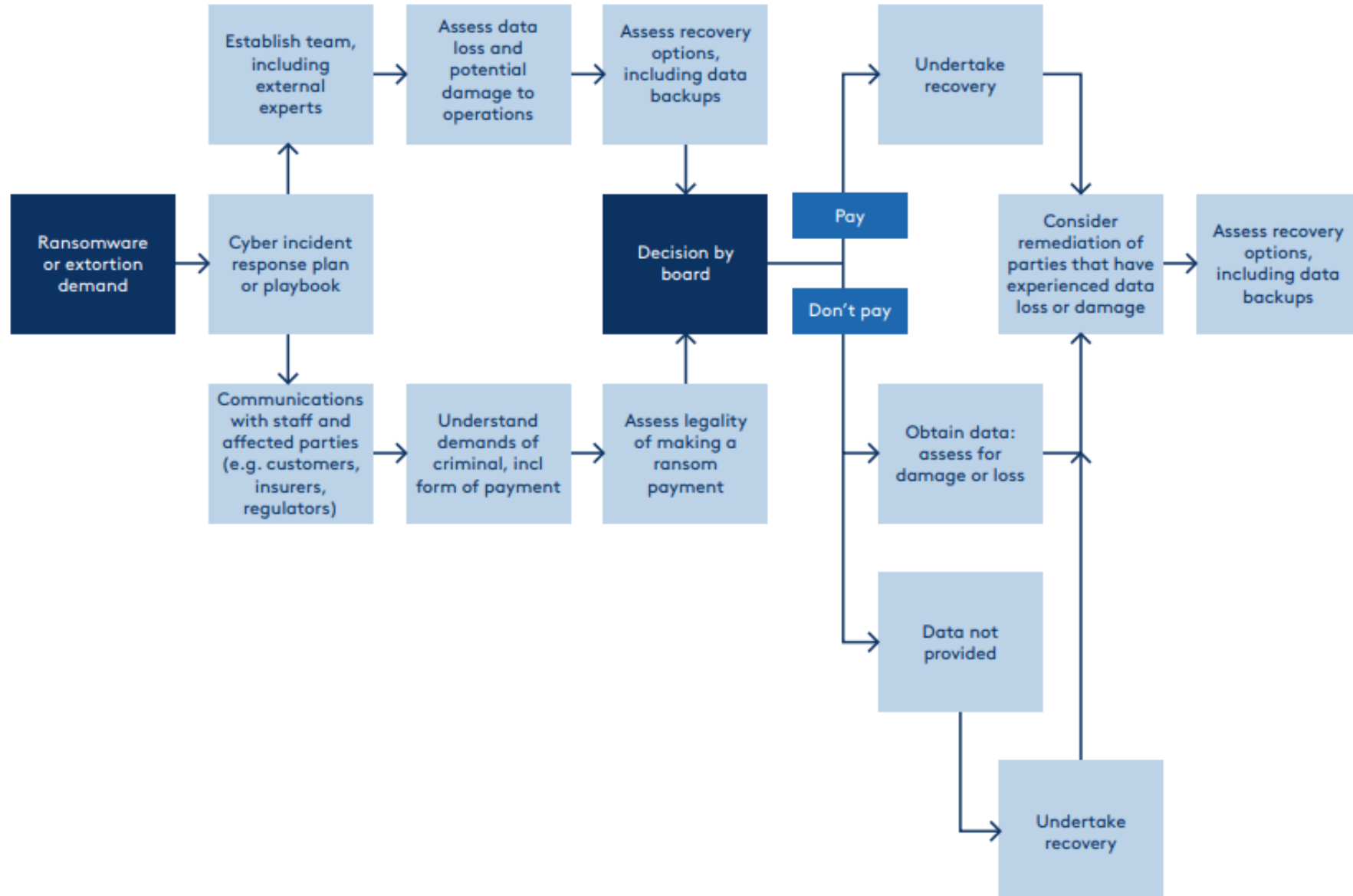
In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

Key findings include:

- 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.*

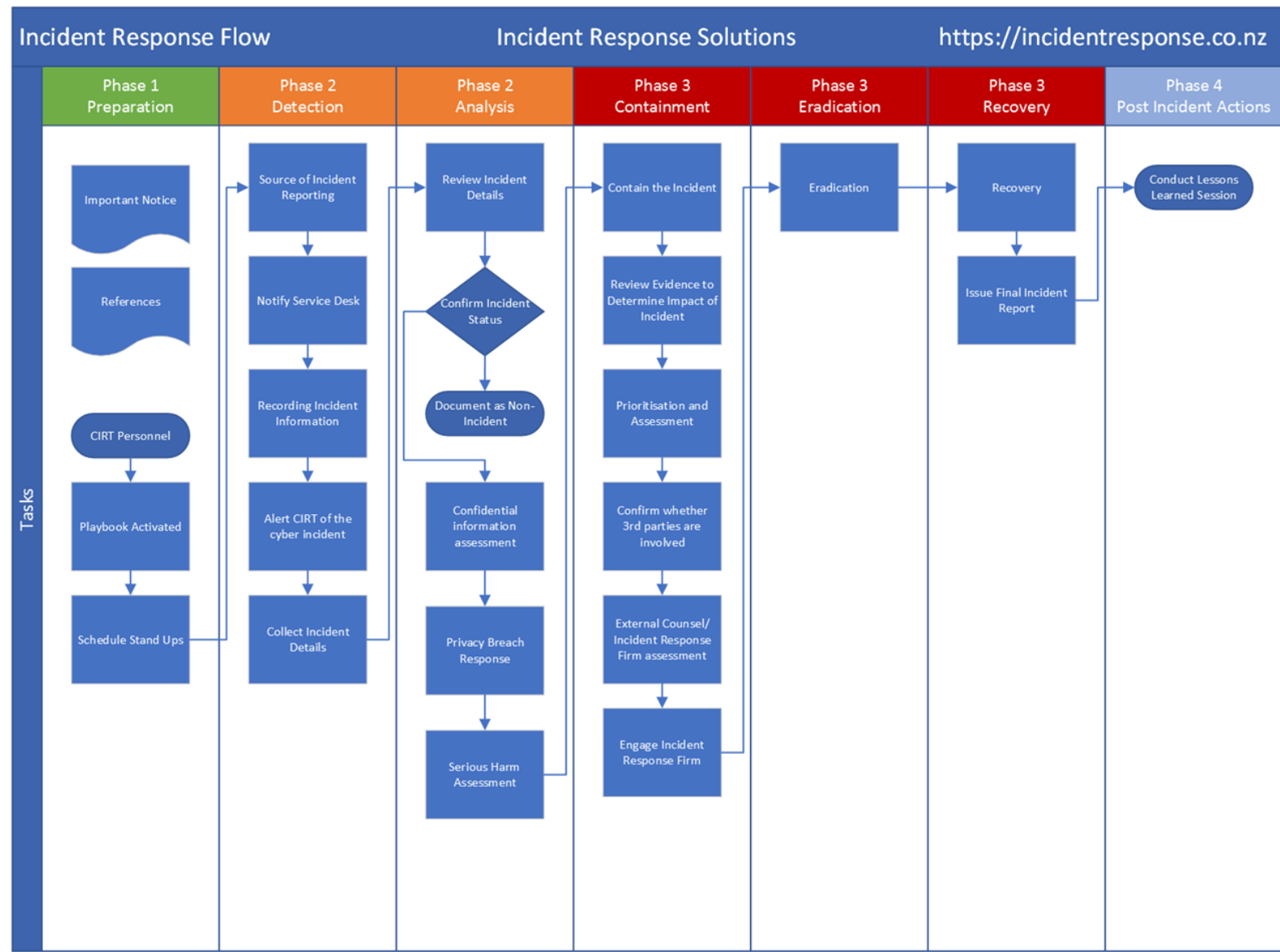
Example Ransomware Decision Making Process - AICD



Data Breach Response



Routine Response and Investigation Methodology



Forensic Tech

Digital Evidence

Forensic Technology



FORENSIC TECH

Document Analysis Review Tool (DART) – 0800 WITNESS

Home Services ▾ Phases ▾ Review Solutions ▾ Blog About

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

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

MITRE ATT&CK® Enterprise Framework

attack.mitre.org

Document Analysis Review Tool

DART

reveal

b r a i n s p a c e

Cloud Platform

Product Education

Search...



reveal



JE

Review

Supervised Learning

Uploads

Model Library

Jobs

Reports

Team Documents

Company Admin

Project Admin



Dashboard

Grid

Clusters

Heatmap

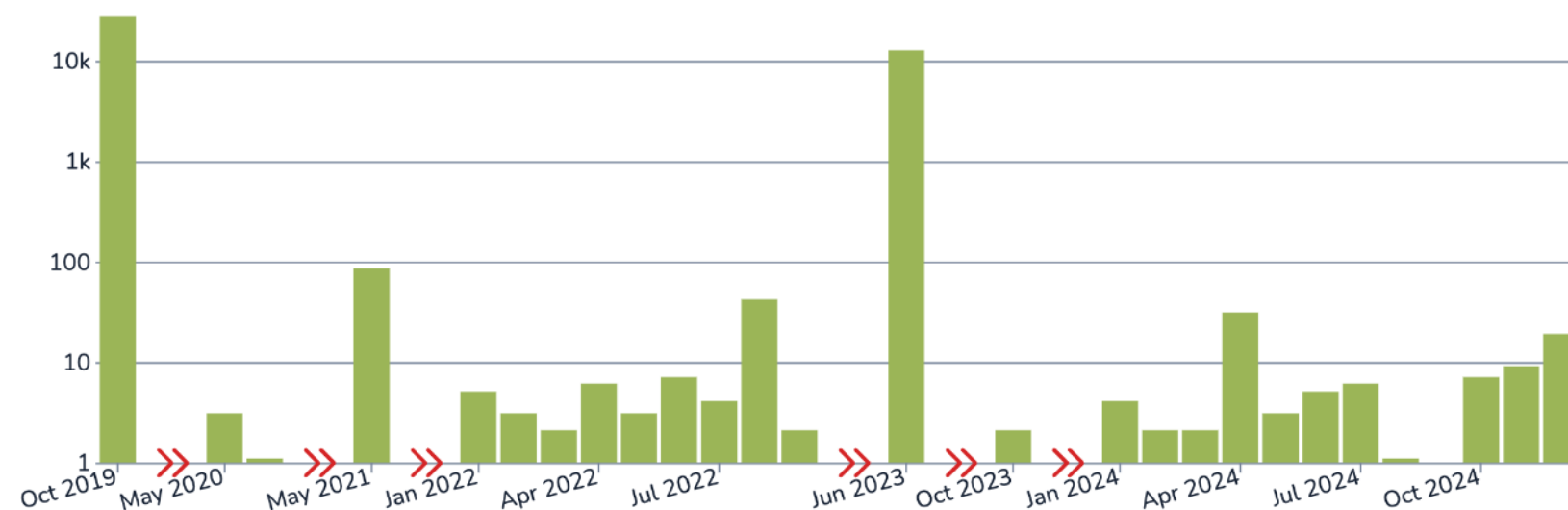
AI Batches

40,494

OS Creation Date

Auto

Logarithmic Scale



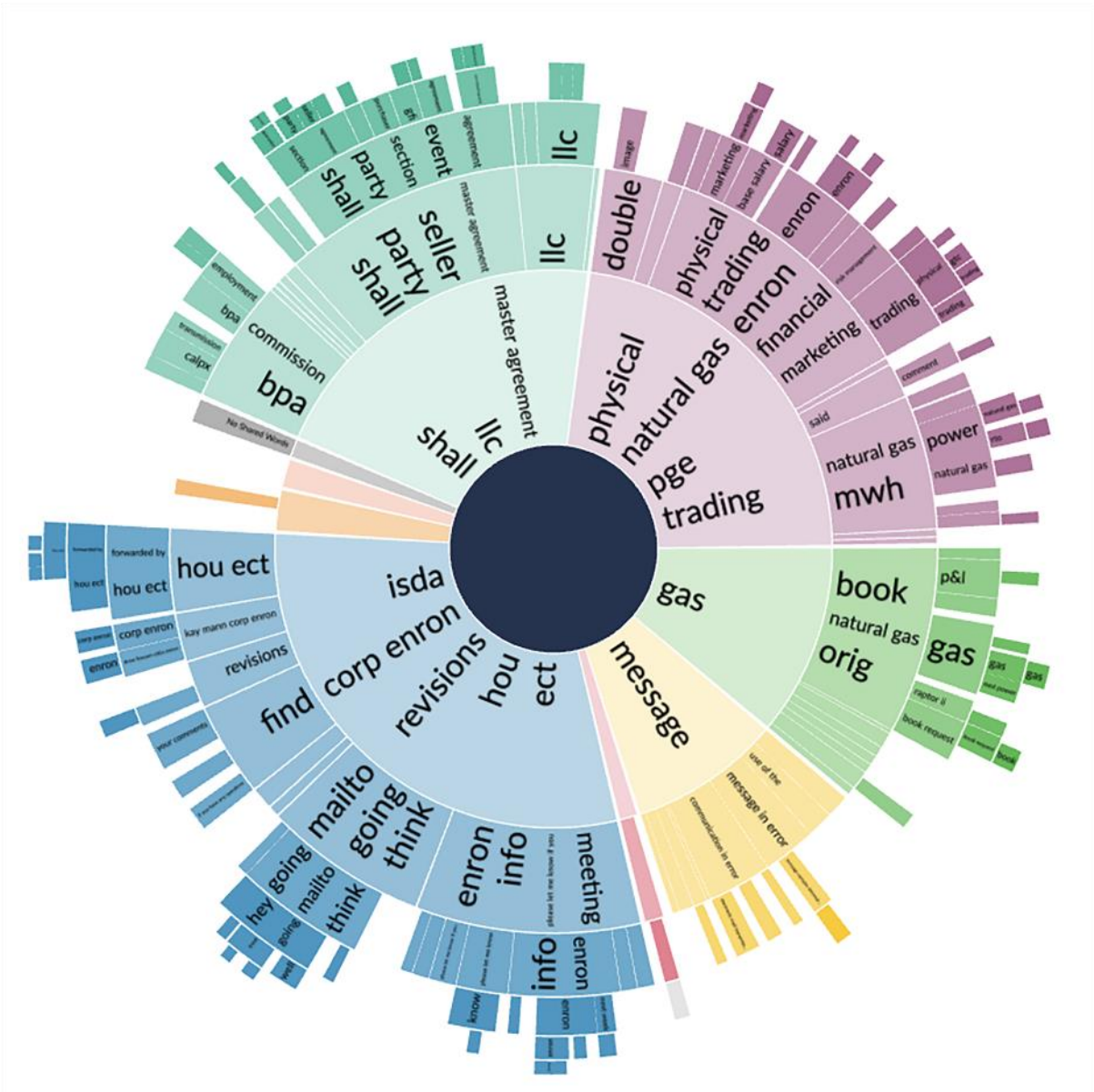
40,493 DOCUMENTS OF 40,494

ORIGINALS

NEAR DUPLI...

EXACT DU...

N...



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")

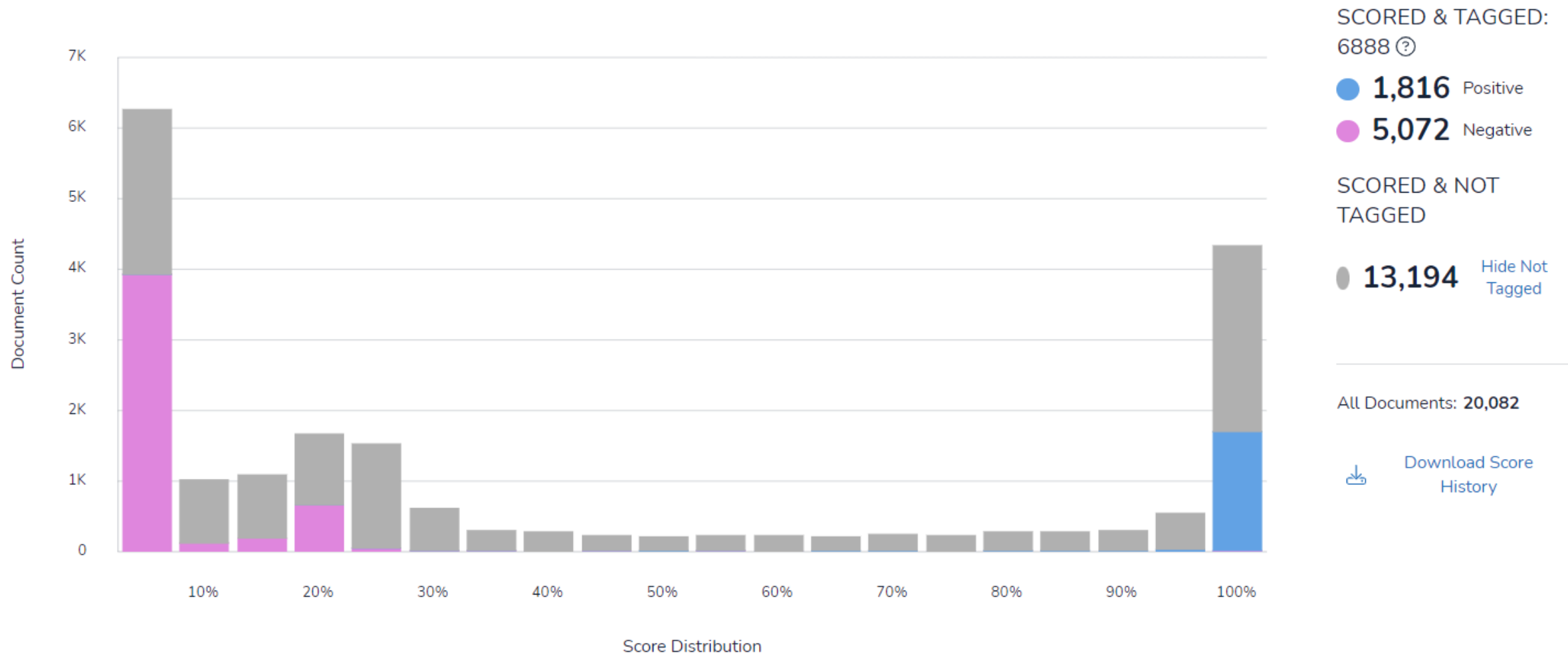
> HR62 - "first/given name(s) at birth" 2023-04-16



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

Document prioritisation – Continuous Active Learning

Tagging & Scoring - Last Completed Round: 8





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







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


What is the primary forensic tool referred to for fraud cases


↑ ASK

Divide the answer into primary geographic regions


^ Less Details


Search: All Docs (77670)






WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.

 Ask





What is the primary forensic tool referred to for fraud cases

DIVIDE THE ANSWER INTO PRIMARY GEOGRAPHIC 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...


↑ ASK

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

^ Less Details

Search: All Docs (77670)





WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.

Services lawyers are engaging IRS to assist with

- Cyber Governance
- Cyber IR plans and simulations
- Breach response
 - Incident controller
 - Data Breach assessment (DART)
 - Communications
 - Ransomware response
 - Dark web and data leak monitoring
- Post Incident Reviews (PIR)
- Forensic technology
- Hosting / eDiscovery





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