The AI Frontier:
Next-Gen Cyber and Forensic Response

July 2026
CAANZ - Management

Incident Response
FORENSIC & CYBER

Todays Presentation – in 60 Seconds

- Key Takeaways from the Cyber Incident Response conference in Denver, June 2026
- Adopting responsible AI Governance - Digital Forensic and Incident Response Examples
- Practical application of AI in New Zealand employment forensic matters
- Insights into the use of AI tools to prepare this presentation and other work

Topic

Cyber Incident Response Conference, June 2026

AI & LLMs in Modern Defense

LLM-Powered Forensics

Deploying AI models to parse and logs dynamically. Solutions like StealerLens demonstrate how specialised LLMs drastically accelerate InfoStealer triage.

Adaptive AI Defense Models

Developing protective guardrails and adaptive threat models as adversaries pivot. Implementing robust prompt validation frameworks protects core detection models from ingestion poisoning.

Simulations & Active Readiness

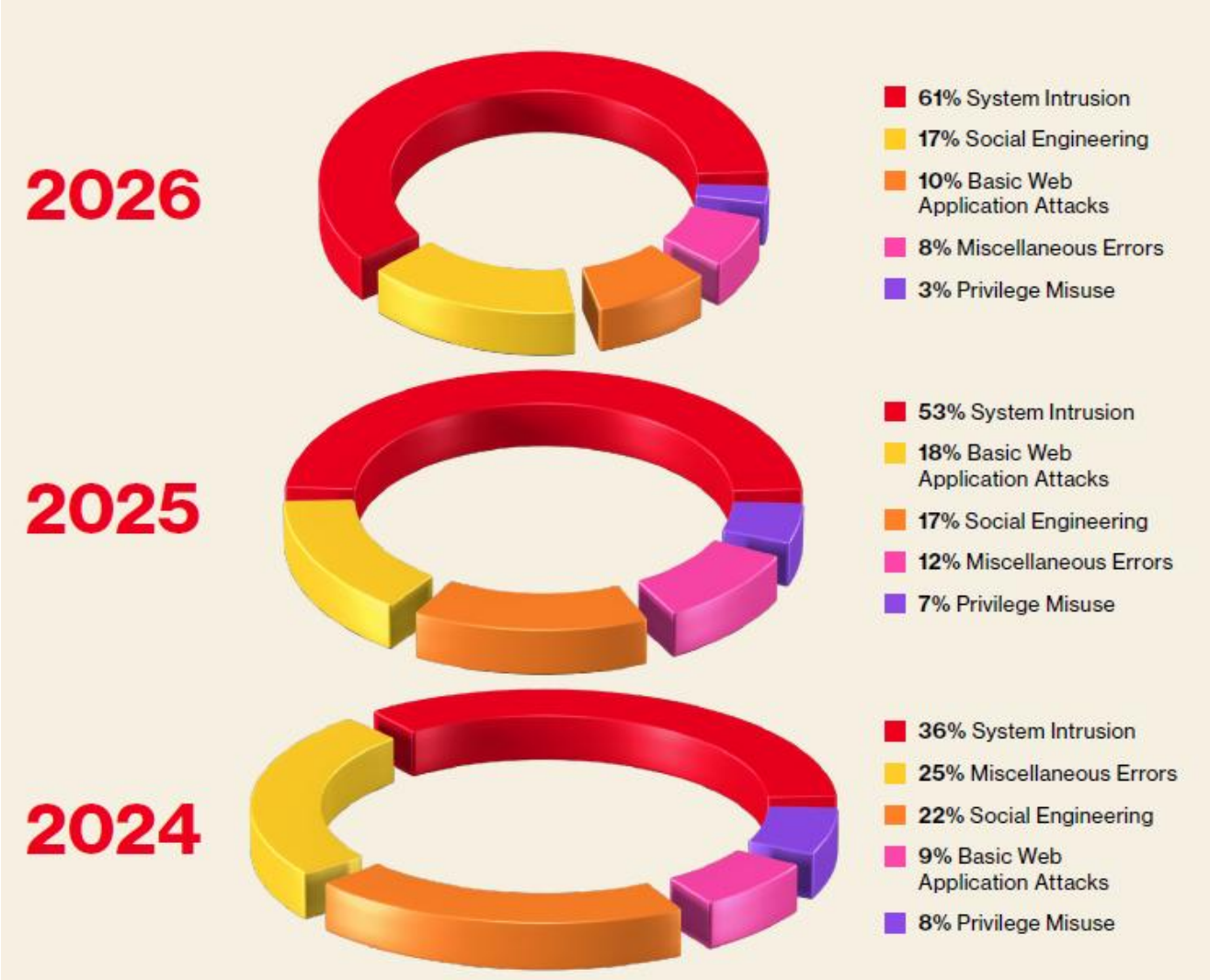
- National Simulations: Insights from complex operations highlight the need for scaled, stress-tested playbooks.
- Layered Tabletops (TTX): Modern training demands multi-tiered tabletop exercises modeling complex supply chain failure chains.
- Frontline Recovery Lessons: Front-line briefings assert that continuous rapid recovery simulation is as vital as intrusion detection.

The Human & Operational Pivot

- Reframing heavy technical jargon into strategic, business-coherent reporting to elevate executive buy-in during active incidents.
- Mitigating systemic operational burnout by transitioning analysts away from alert verification and toward autonomous containment engineering.
- Advanced approaches to stitching disparate digital artifacts into integrated, unified timelines for accelerated root-cause analysis.
- Solidifying FIRST's core mission of fostering global cross-border trust loops to dismantle advanced adversarial infrastructure.

Verizon 2026 Data Breach Investigations Report

- 19th Edition
- 31,861 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 22,625 breaches that resulted in the confirmed disclosure of data to an unauthorised party.
- System Intrusion increasing as an Incident Classification



https://www.verizon.com/dbir/

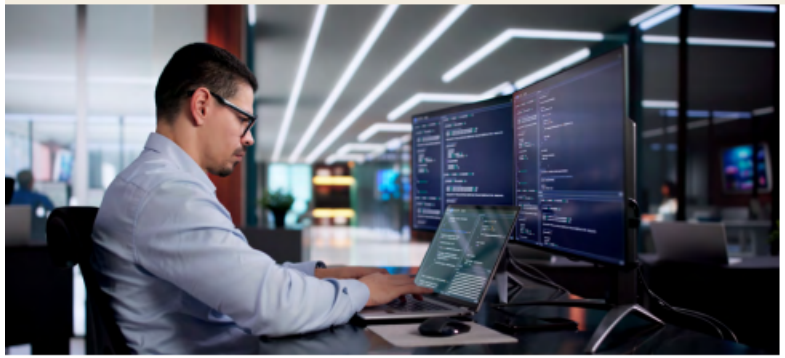
Key Findings

Breaches have become more costly.

$60K → $110K

In cyber claims made from 2019 to 2024, insurable losses went from roughly $60,000 to around $100,000.[1]

With the development of artificial intelligence (AI) in the cybersecurity landscape, mitigating this loss could become increasingly difficult.



In this new world of AI-driven cyberthreats, vulnerabilities continue to be exploited as entry points.

31%

The percentage of vulnerability exploitation as an initial access vector is now up to 31% – a 55% jump from last year.[2]

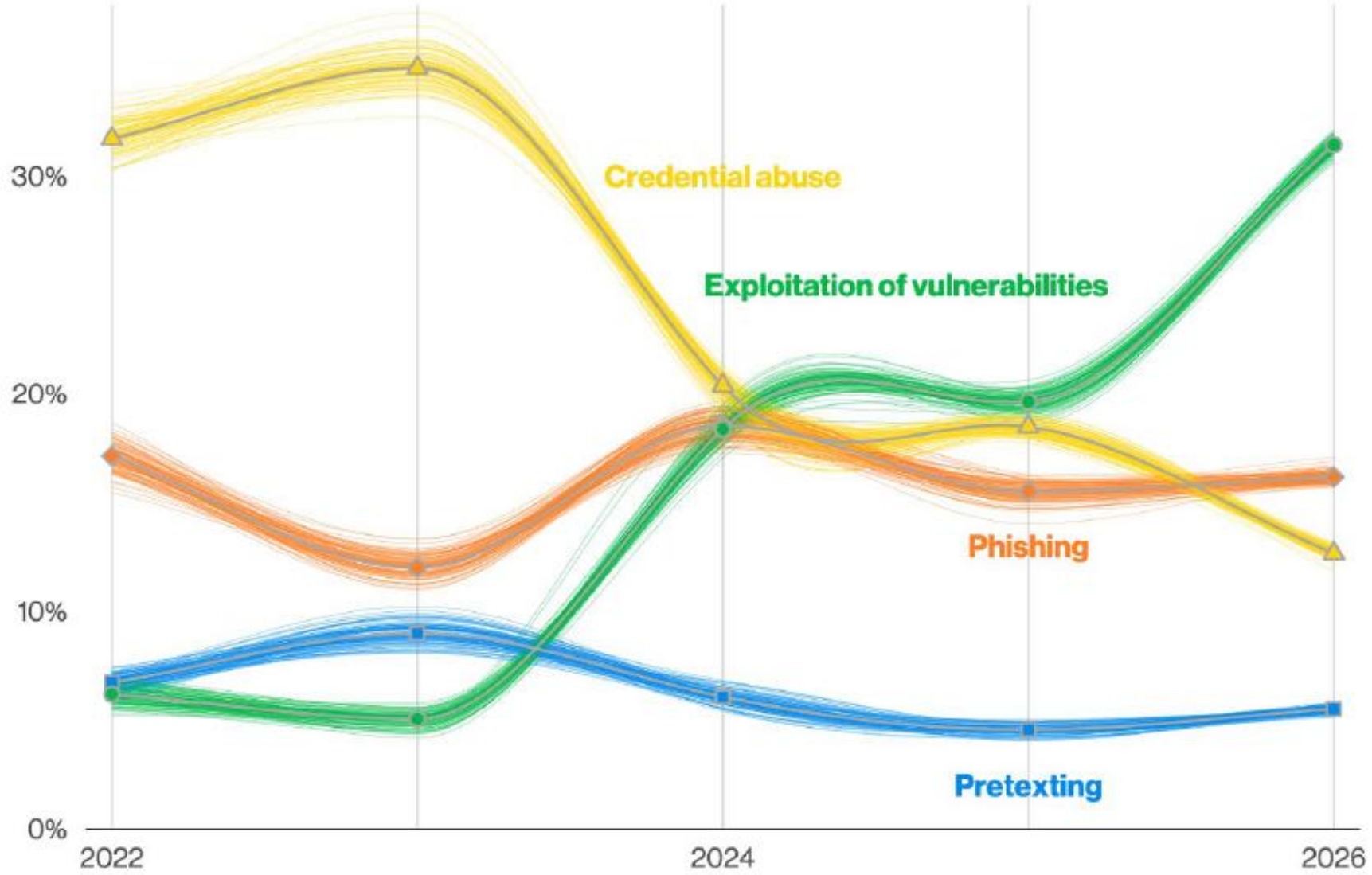
15

In the median case, threat actors verifiably researched or used generative AI to help with 15 distinct attack techniques.[2]

43 days

This is the median time to full resolution of a critical vulnerability – an almost two-week increase from the previous year.[2]

Verizon - Initial Access Vectors



Topic

Adopting responsible AI Governance
Digital Forensic and Incident Response Examples

DIGITAL FORENSICS & AI — INVESTIGATION FRAMEWORK

Safe AI Integration Points Mapped to the SWGDE Guidelines & Expert Best Practices

Contributors: Heather Barnhart, Ovie Carroll, and Josh Hickman

AI Recommended — Low Risk | AI Optional — Elevated Risk | AI Never — High Risk | Human Driven — AI Supports Only

01 IDENTIFICATION

✓ AI RECOMMENDED

Recognizing potential sources of digital evidence such as laptops, portable devices, media, cloud, logs, and artifacts

- AI scans environments to identify potential evidence sources
- Automated device & artifact discovery across endpoints
- AI-assisted scope definition & evidence mapping

02 COLLECTION / PRESERVATION

⚠ AI OPTIONAL

Acquiring forensic copies, maintaining chain of custody, and protecting evidence integrity

- AI may assist with automated imaging workflows
- Hash verification support can be automated
- Chain of custody must remain human-controlled

03 TRIAGE

✓ AI RECOMMENDED

Rapidly prioritizing evidence, assessing severity, and determining investigative focus areas

- AI rapidly scores & prioritizes evidence by relevance
- Automated IoC matching & threat scoring
- AI-assisted keyword & pattern flagging at scale

04 EXAMINATION / ANALYSIS

✓ AI RECOMMENDED

Deep forensic examination of artifacts, timeline reconstruction, and drawing investigative conclusions

- AI-assisted artifact parsing & timeline building
- Pattern recognition across large evidence datasets
- Human must validate ALL AI conclusions to mitigate inaccuracies

⚠ AI CANNOT PUT A HUMAN BEHIND AN ARTIFACT TO PROVE ATTRIBUTION

05 VALIDATION

✕ AI NEVER

Verifying findings are accurate, repeatable, and defensible to ensure forensic integrity of conclusions

- A human must validate AI findings
- Human examiner must independently verify all conclusions
- Legal & evidentiary integrity requires human accountability

06 REPORTING / PRESENTATION / ACTION

HUMAN DRIVEN

Documenting findings, presenting evidence, and driving investigative or legal action

- AI may assist with report drafting but a human must author & own
- Expert witness testimony is always human responsibility
- All legal conclusions & actions require human authority

✓ AI RECOMMENDED — LOW RISK

- Discover, map, and scope evidence sources
- Prioritize, score, and flag evidence at scale during the Triage phase
- Parse artifacts, build timelines, and find patterns
- Surface insights; Human in the Loop required
- AI involvement must be fully documented

⚠ AI OPTIONAL — ELEVATED RISK

- AI may assist workflows during the Collection/Preservation phase; Human in the Loop required
- Chain of custody must remain human-controlled at all times
- Hash verification may be automated
- AI involvement must be fully documented

✕ AI NEVER — HIGH RISK

- AI should not be the final source of validation; Human in the Loop required
- Be the sole author of a forensic conclusion
- AI cannot associate an artifact to a human to prove attribution
- Make legal determinations or drive investigative action
- If AI is used, all involvement must be fully documented

INCIDENT RESPONSE & AI — INVESTIGATION FRAMEWORK

Suggested Safe AI Integration Points Mapped to NIST CSF 2.0

Contributors: Heather Barnhart, Steve Anson, David Bianco, Josh Hickman, and Taz Wake

AI Recommended — Low Risk | AI Optional — Elevated Risk | AI Never — High Risk | Human Driven — AI Supports Only

INCIDENT RESPONSE — NIST CSF

Detect — ✓AI RECOMMENDED

Timely discovery, event analysis, continuous monitoring, and anomaly detection

- AI-assisted
- AI anomaly detection & log correlation
- Automated IoC triage & enrichment
- Pattern recognition across large datasets
- AI-assisted timeline construction

Respond — ⚠ AI OPTIONAL

Taking actionable steps to contain and mitigate impact for incidents

- When AI suggests a response and automation performs it, Human in the Loop is required
- AI-suggested containment actions
- Automated evidence preservation tasks
- AI-assisted report drafting

Recover — ⚠ AI OPTIONAL

Minimize impact while restoring assets and normal operations affected by an incident

- Human judgement required

↑ ↓ ↑ ↓ ↑ ↓

LESSONS LEARNED — NIST CSF

(Identify) Improvement

Identify what was learned from all phases of the incident

- Human decision points
- Decision points should not be purely AI

⚠ AI MAY BE A COLLABORATOR BUT A HUMAN MUST MAKE THE FINAL DECISION

↑ ↓ ↑ ↓ ↑ ↓

PREPARATION — NIST CSF

✓AI RECOMMENDED

Govern

Establish and monitor cybersecurity risk management strategy, policies, and expectations across the organization

- Policy gap analysis
- Playbook drafting

Identify

Understand the business context, assets, and risks to prioritize cybersecurity efforts aligned to objectives

- Automated asset inventory & classification
- AI-driven threat intelligence & risk scoring

Protect

Implement safeguards to limit impact to include access controls, training, and data security

- AI-assisted training simulations/tabletop exercises

✓AI RECOMMENDED — LOW RISK

- AI is easily integrated into the Preparation phase of an incident
- AI can assist in the Detection phase, which may require both Human in the Loop (Act) and Human on the Loop (Monitor)
- AI is recommended for training exercise creation and simulations
- All AI involvement must be fully documented

⚠ AI OPTIONAL — ELEVATED RISK

- AI-suggested containment actions requires Human in the Loop
- AI-assisted report collaboration and drafting requires human approval
- A human must validate all AI outputs before actions are taken
- AI involvement must be fully documented

✕ AI NEVER — HIGH RISK

- Lessons Learned should not be purely AI at decision points
- AI should not be used in legal and evidentiary conclusions
- AI should not determine attribution
- AI output requires Human in the Loop or Human on the Loop
- If AI is used, all involvement must be fully documented

Topic

Practical application of AI in
New Zealand employment forensic matters

Topic

Insights into the use of AI tools
to prepare this presentation and other work

Sample Output

Cybersafehq.com

Sample Output

KiwiGen.AI

Home Services Solutions Insights Templates About Contact

A Template Worth Copying: What New Zealand's Public Service AI Policy Template Signals About Practical AI Governance

Most organisations know they need an AI policy. Far fewer know what one should actually say....

Generative AI in New Zealand's Courtrooms: What the Judiciary's Guidelines Mean in Practice

Generative AI (GenAI) has moved from novelty to everyday tool with remarkable speed, and the legal...

Who's in charge of your AI? Governance and accountability under New Zealand's Responsible AI Guidance

AI adoption in New Zealand businesses is accelerating, but a familiar question keeps surfacing in boardrooms:...

From Principles to Practice: What the Public Service AI Toolkit Means for Government Agencies

An insights article on the GCDO's Public Service AI Toolkit — digital.govt.nz New Zealand's public service...

Trust Before Tools: What New Zealand's Public Service AI Framework Means for Government Agencies

New Zealand has set out its stall on artificial intelligence in government. The Public Service AI...

The AI Shift in Cyber Risk: What the Five Eyes Call to Action Means for Your Organisation

An insights article on the joint statement issued by the Five Eyes cyber security agencies, 22...

Where to Start with Responsible AI: The Government's Curated Guidance, Decoded

Key Takeaway: New Zealand's Centre for Data Ethics and Innovation has published a shortlist of AI...

New Zealand's First AI Strategy: What "Investing with Confidence" Means for Your Business

Key Takeaway: New Zealand now has a national AI strategy — and its message to businesses...

KiwiGen.AI

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