KAITIAKI IT

Sentinel v3.0

Threat Intelligence & Compliance Assessment — Sample Preview

83

CRITICAL RISK /100

AUDIT ID	KAI-SAMPLE-2026
DATE	03 May 2026
LOG SOURCE	Zscaler Zia Web Proxy
RECORDS	100,000
AI ENGINE	NVIDIA NIM — Nemotron / Kimi-K2 / LLaMA-4
GUARDRAILS	NeMo Guardrails — Active
DATA EGRESS	Zero — All processing on-premises
CLASSIFICATION	SAMPLE — Full reports available via kaitiaki-it.com

// 01 — OVERVIEW

Executive Summary

This sample report demonstrates the output of a Kaitiaki Sentinel forensic analysis. A full audit processed 100,000 log records and identified a Board Risk Score of **83/100** — indicating a **critical security posture**. The analysis identified 10,822 CRITICAL-severity events, of which 7,891 were actively allowed through security controls.

20 confirmed AI tool access events were detected, triggering Australian Privacy Act 2026 APP 1.7 obligations. 6 attack chains were correlated — sequences consistent with data staging and exfiltration.

REGULATORY OBLIGATIONS TRIGGERED

OBLIGATION	DEADLINE	PENALTY	STATUS
Australian Privacy Act 2026 — APP 1.7	10 Dec 2026	$50,000,000	TRIGGERED
Privacy Act — APP 8.1 (cross-border)	Immediate	Civil penalty	TRIGGERED
NDB Scheme — Notifiable Data Breach	30 days	OAIC notification	TRIGGERED
APRA CPS 234 — Material Cyber Incident	72 hours	APRA notification	ASSESS

FINANCIAL EXPOSURE

SCENARIO	ESTIMATED EXPOSURE (AUD)	BASIS
Conservative	$2,250,000	Minimum regulatory penalties only
Most Likely	**$10,875,000**	Penalties + incident response + reputational
High Case	**$19,500,000**	Maximum APP 1.7 + NDB + APRA enforcement

BOARD MUST ACT — NEXT 24 HOURS

1. Convene an emergency security meeting with CISO, Legal counsel, and CEO.
2. Block all access to unsanctioned AI tools (ChatGPT, Claude, Gemini, DeepSeek) at the network perimeter.
3. Identify and interview the 3 highest-risk individuals listed in the full report.
4. Engage privacy legal counsel to assess NDB Scheme notification obligations.
5. Preserve all log data as potential legal evidence.

// 02 — FINDINGS

Key Findings & Evidence

Finding 01

7,891 CRITICAL-severity sessions ALLOWED through security controls with 149.9 MB confirmed transmitted. Applications: Pi AI (Inflection), Poe AI, Grok/xAI. These are confirmed policy breaches — not detections.

TIMESTAMP	USER	APPLICATION	ACTION	BYTES SENT	THREAT
2026-03-10 06:35	User_3EAA82AD	Pi AI (Inflection)	ALLOW	9.5 MB	—
2025-10-05 08:55	User_B555ADA7	Poe AI	ALLOW	8.2 MB	—
2026-02-05 19:38	User_64C527D1	Replicate API	ALLOW	7.1 MB	Trojan.Emotet
2025-11-20 19:34	User_31ECCC58	Microsoft Copilot	ALLOW	9.3 MB	Ransomware.BlackCat

Finding 02

Malware/threat families detected: Ransomware.LockBit3 (289 events); Trojan.QakBot (285 events); Trojan.Metasploit (284 events); Ransomware.BlackCat (276 events).

THREAT NAME	EVENT COUNT	AFFECTED USERS	CATEGORY
Ransomware.LockBit3	289	User_5383ADCB, User_A8743935, +4 others	Malware
Trojan.QakBot	285	User_1AAA03C4, User_31ECCC58, +3 others	Malware
Trojan.Metasploit	284	User_37AACF19, User_73E3779C, +4 others	Malware
Ransomware.BlackCat	276	User_75580F7F, User_1B1153F2, +3 others	Malware

Finding 03

APP 1.7 BREACH: 20 confirmed AI tool access events. Services: replicate.com, perplexity.ai, character.ai. 53.4 MB transmitted to external AI services crossing Australian borders without data processing agreements.

TIMESTAMP	USER	AI SERVICE	JURISDICTION	BYTES SENT	ACTION
2025-04-01 00:10	User_B181440D	replicate.com	US — CLOUD Act	7.0 MB	Allowed
2025-04-01 00:58	User_AF521931	perplexity.ai	US — CLOUD Act	2.3 MB	Allowed
2025-04-01 03:18	User_1AAA03C4	claude.ai	US — CLOUD Act	1.7 MB	Allowed
2025-04-01 04:00	User_7C89D2FF	copilot.microsoft.com	US — CLOUD Act	3.2 MB	Allowed

// 03 — COMPLIANCE

Compliance Framework Analysis

FRAMEWORK	STATUS	CONTROLS TRIGGERED	MAXIMUM PENALTY
Australian Privacy Act 2026	FAIL	17	Up to $50,000,000
Essential Eight (ACSC)	FAIL	13	Regulatory enforcement
ISO 27001:2022	FAIL	16	Certification revocation
SOC 2 Type II	FAIL	11	Audit qualification
PCI-DSS v4.0	FAIL	6	Card scheme fines

IMMEDIATE ACTIONS REQUIRED

Each framework failure represents a current, ongoing compliance gap. The Australian Privacy Act 2026 failures trigger mandatory regulatory obligations with deadlines running from the date of discovery of these findings.

PRIORITY	ACTION	OWNER	DEADLINE
CRITICAL	Block unsanctioned AI tools at perimeter	IT Security	24 hours
CRITICAL	Interview high-risk individuals	CISO + HR	24 hours
HIGH	OAIC notification assessment	Legal + CEO	10 days
HIGH	AI governance policy	CISO + Legal	14 days
HIGH	MFA enforcement	IT Security	30 days
MEDIUM	Staff awareness training	HR + CISO	30 days