GOOD SECURITY

Security Baseline Assessment

Current posture, priority gaps, and the first actions the business should take.

CLIENT	ASSESSMENT DATE	ASSESSOR
Kiwi Manufacturing Ltd	**21 March 2026**	**Castelyn Security vCISO**

OVERALL SCORE	CRITICAL FINDINGS	90-DAY ACTIONS
81/100	**0**	**8**

LEADERSHIP SUMMARY

Kiwi Manufacturing Ltd is sitting at 81/100. The baseline shows 0 critical findings and 7 high findings, with the clearest pressure points concentrated in the lowest-scoring domains below.

Executive summary

This report gives leadership a current-state view of the security baseline, the business impact of the most material gaps, and the actions that should be funded or delegated first.

Eliminate shared SCADA admin accounts and implement individual credentials

Enable M365 DLP policies to protect employee PII

Develop OT-specific incident response playbook with CERT NZ notification

Scope and evidence base

Item	Detail
Systems assessed	All IT systems, OT/SCADA network, Microsoft 365 tenant
Frameworks used	ISO 27001:2022, NZ Privacy Act 2020, NZISM
Evidence base	Knowledge graph, Azure AD tenant, Sophos Central
Assessment date	21 March 2026

Assessment methodology and frameworks

Initial Security Baseline Assessment using ISO 27001:2022 control-based methodology, supplemented by CIS Controls v8 and NZISM where applicable.

Domain-by-domain scoring

Domain	Score	Status	Maturity	Key gap
Iam	78	Amber	Defined	Shared admin account used for SCADA system maintenance
Endpt	85	Green	Managed	Warehouse barcode scanners running legacy Android not covered by XDR
Email	90	Green	Managed	DMARC policy set to quarantine rather than reject
Net	80	Green	Defined	VPN split-tunnelling enabled by default for remote workers
Datap	78	Amber	Defined	No data classification scheme for production line documentation
Bkup	88	Green	Managed	No immutable backup copy (vulnerable to ransomware encryption)
Cloud	76	Amber	Defined	No Cloud Access Security Broker (CASB) for SaaS monitoring
Vndr	72	Green	Defined	No formal vendor risk assessment process for supply chain partners
Ir	78	Amber	Defined	No documented incident response plan specific to manufacturing OT
Gov	82	Green	Managed	Security committee minutes not consistently documented
Aware	82	Green	Managed	Production floor staff exempt from phishing simulations

Target-state priorities

- Vndr: lift from 72 to at least the managed threshold through Establish vendor risk assessment questionnaire for critical suppliers.
- Cloud: lift from 76 to at least the managed threshold through Enable Microsoft Defender for Cloud Apps for CASB coverage.
- Iam: lift from 78 to at least the managed threshold through Eliminate shared admin accounts for OT/SCADA systems.
- Datap: lift from 78 to at least the managed threshold through Implement data classification (Public/Internal/Confidential/Restricted).
- Ir: lift from 78 to at least the managed threshold through Develop OT-specific incident response playbook.

Key risks / heatmap

Risk	Score	Priority	Treatment
Supply chain ransomware via OT network	15	L3 / I5	Mitigate
Shared SCADA admin account compromise	12	L3 / I4	Mitigate
Employee PII breach via unencrypted shares	8	L2 / I4	Mitigate
Vendor supply chain data exfiltration	6	L2 / I3	Accept

Gap analysis against target state

Domain	Current state	Target state	Priority action
Vndr	No formal vendor risk assessment process for supply...	Lift Vndr into the Defined to managed range with evidence-...	Establish vendor risk assessment questionnaire for critical...
Cloud	No Cloud Access Security Broker (CASB) for SaaS monitoring	Lift Cloud into the Defined to managed range with evidence-...	Enable Microsoft Defender for Cloud Apps for CASB coverage
Iam	Shared admin account used for SCADA system maintenance	Lift Iam into the Defined to managed range with evidence-...	Eliminate shared admin accounts for OT/SCADA systems
Datap	No data classification scheme for production line...	Lift Datap into the Defined to managed range with evidence-...	Implement data classification...
Ir	No documented incident response plan specific to...	Lift Ir into the Defined to managed range with evidence-...	Develop OT-specific incident response playbook

Prioritised roadmap

Phase	Action	Owner	Timing	Success measure
1	Eliminate shared SCADA admin account	Kiwi Manufacturing IT / MSP	Eliminate shared SCADA admin account (1-2 weeks)	Domain IAM improvement verified
1	Enable M365 DLP policies for PII detection	Kiwi Manufacturing IT / MSP	Enable M365 DLP policies for PII detection (1-2 weeks)	Domain DATAP improvement verified
2	Establish vendor risk assessment questionnaire	Kiwi Manufacturing IT / MSP	Establish vendor risk assessment questionnaire (3-6 weeks)	Domain VNDR improvement verified
2	Develop OT-specific incident response playbook	Kiwi Manufacturing IT / MSP	Develop OT-specific incident response playbook (3-6 weeks)	Domain IR improvement verified
2	Deploy Microsoft Defender for Cloud Apps (CASB)	Kiwi Manufacturing IT / MSP	Deploy Microsoft Defender for Cloud Apps (CASB) (3-6 weeks)	Domain CLOUD improvement verified
3	Deploy 802.1X NAC for wireless networks	Kiwi Manufacturing IT / MSP	Deploy 802.1X NAC for wireless networks (7-12 weeks)	Domain NET improvement verified
3	Add role-based BEC training for finance team	Kiwi Manufacturing IT / MSP	Add role-based BEC training for finance team (7-12 weeks)	Domain AWARE improvement verified
3	Implement data classification scheme	Kiwi Manufacturing IT / MSP	Implement data classification scheme (7-12 weeks)	Domain DATAP improvement verified

90-day action plan

Window	Focus	Named owner	Expected outcome
1	Eliminate shared SCADA admin account	Kiwi Manufacturing IT / MSP	Domain IAM improvement verified
1	Enable M365 DLP policies for PII detection	Kiwi Manufacturing IT / MSP	Domain DATAP improvement verified
2	Establish vendor risk assessment questionnaire	Kiwi Manufacturing IT / MSP	Domain VNDR improvement verified
2	Develop OT-specific incident response playbook	Kiwi Manufacturing IT / MSP	Domain IR improvement verified
2	Deploy Microsoft Defender for Cloud Apps (CASB)	Kiwi Manufacturing IT / MSP	Domain CLOUD improvement verified
3	Deploy 802.1X NAC for wireless networks	Kiwi Manufacturing IT / MSP	Domain NET improvement verified

Leadership checkpoints

- Confirm owners and due dates for all quick wins within the first governance cycle.
- Use one evidence pack for customer, insurer, and audit follow-up rather than recreating material under pressure.
- Track domain movement monthly so the next scorecard can prove uplift rather than restating intent.

Evidence appendix

Domain	Strengths already in place	Primary recommendation
Iam	Azure AD Conditional Access enforces MFA for cloud apps; Named user...	Eliminate shared admin accounts for OT/SCADA systems
Endpt	Sophos XDR deployed to 100% of corporate endpoints; Automated...	Extend Sophos Mobile protection to warehouse handheld devices
Email	SPF, DKIM and DMARC all configured and enforced; Microsoft Defender...	Upgrade DMARC policy to reject after 3-month monitoring period
Net	Managed firewall with IPS/IDS via MSP; IT/OT network segmentation...	Disable split-tunnelling or implement always-on VPN
Datap	Privacy Act 2020 privacy officer appointed	Implement data classification (Public/Internal/Confidential/Restricted)
Bkup	Veeam Backup with daily snapshots and weekly fulls; Off-site...	Enable Veeam immutable repository or Wasabi Object Lock
Cloud	Azure AD used for SSO across all cloud services; Microsoft Secure...	Enable Microsoft Defender for Cloud Apps for CASB coverage
Vndr	MSP contract includes SLA and security obligations	Establish vendor risk assessment questionnaire for critical suppliers