RESPONSE TO CSA CYBERSECURITY CODE OF PRACTICE 2026

Show the evidence. Meet the deadline.

Singapore's Cybersecurity Code of Practice 2026 requires designated CII owners to demonstrate board governance, asset visibility and continuous monitoring across CII and interconnected systems by 29 July 2027. Vectra AI aligns to 31 of the 38 clauses reviewed in this brief, helping CIIOs build the detection and investigation evidence auditors expect.

TRANSITION DEADLINE
29 JUL 2027
Existing CIIOs must meet new governance, asset-oversight, and interconnected-system controls.

TIER 5 DEADLINE
31 DEC 2027
Cyber Trust Market Advocate, Tier 5, or equivalent certification required.

WHERE VECTRA AI ALIGNS
31 OF 38 CLAUSES
Vectra AI directly aligns with Detect & Respond and Interconnected clauses.

Where Vectra AI maps to CCoP 2026 requirements

Summary view of where the Vectra AI Platform contributes operational capability or supports the clauses.

17 of 18 clauses
Identify & Protect
Asset visibility, access, identity, segmentation, hardening

7 of 7 clauses
Detect & Respond
Records, monitoring, threat hunting, incident response

7 of 13 clauses
OT, Domain, & Interconnected
OT architecture, DNS, interconnected systems

Direct Alignment | **Supporting Alignment** | **Other control owner / Not core**

Audit & governance	2.1	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9
	3.10									
Identify & Protect	4.1	5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.8	5.9
	5.10	5.11	5.12	5.13	5.14	5.15	5.16	5.17		
Detect & Respond	6.1	6.2	6.3	6.4	7.1	7.2	7.3			
Resilience & Training	8.1	8.2	9.1	9.2						
OT, Domain, & Interconnected	10.1	10.2	10.3	10.4	11.1	11.2	12.1	12.2	12.3	12.4
	12.5	12.6	12.7							

Where Vectra AI Helps: Identify & Protect

Asset visibility, access, identity, segmentation, and hardening.

CCoP Area	Item	Action Item Detail	What Vectra AI Does	Practical Outcome
4 – Identification	4.1	Maintain CII and interconnected-system inventories, dependencies, links, location, providers and topology.	Asset Visibility and Inventory; HostID context.	Continuous passive discovery can reconcile communicating assets and unmanaged devices. Asset Inventory is not an authoritative CMDB.
5 – Protection	5.1	Authorize and authenticate access; monitor anomalous sessions.	Network and identity behavioral detections; native response actions and response integrations.	Detects suspicious use of valid access and can trigger supported containment; does not provision or authenticate users.
	5.2	Manage account lifecycle, least privilege, anomaly monitoring and reviews.	Identity behavior threat detection and response; entity prioritization.	Finds risky account behavior and supports review evidence; IAM lifecycle and recertification remain external.
	5.3	Control privileged accounts, MFA, sharing, inventory and break-glass logging/review.	Privilege-related identity and network behavior analytics; identity observability analytics.	Can reveal suspected privilege abuse; no PAM vault, MFA enforcement or privileged-account register.
	5.4	Secure domain controllers and monitor trust or configuration anomalies.	Active Directory connector; network and identity detections for signatures and behaviors.	Provides behavioral visibility into suspicious AD operations where configured; hardening remains with AD owners.
	5.5	Segment by risk; minimize communications; detect, block and isolate unauthorized activity.	Observed-flow analytics; exposure findings; native traffic lockdown and integration responses; network segmentation visibility.	Validates actual communication and assists containment; does not design or administer firewall segmentation.
	5.6	Define and enforce network-access rules across internal and external boundaries.	Network threat detection and response; signature-based detections; exposure evidence and prioritization.	Detects malicious or unexpected network activity; is not the network access-control or firewall enforcement plane.
	5.7	Secure remote access with MFA, encryption, intermediaries and minimum required flows.	Network and identity behavioral detections; exposed-RDP exposure findings.	Highlights risky remote behavior and externally exposed services; does not provide VPN, MFA or encryption enforcement.
	5.8	Authorize and secure wireless networks and devices.	Analysis of wireless traffic only when forwarded or mirrored.	
	5.9	Maintain secure configurations; disable unnecessary services/ports; anti-malware and patching.	Exposure findings for weak protocols, TLS and exposed services.	Network-validated findings help prioritize hardening; Vectra AI does not scan configuration baselines or manage endpoints.
	5.10	Operate risk-based patching with monitoring, testing, tracking, compensating controls and rollback.	No patch-management capability, but visibility into patch-related exposures.	May prioritize observed exposure or compensating monitoring; no CVE scanner, patch deployment or rollback management.
	5.11	Control portable and removable media, encryption and malware risk.	No device-control capability, but visibility into device-related exposures.	Network analytics may see subsequent behavior, but cannot authorize USB use or enforce removable-media controls.
	5.12	Control applications, integrity, tier separation, secure development and web protection.	No application control or multi-tier review capability, but visibility into application and web-related exposures.	Can detect exploitation and post-compromise behavior; not application allowlisting, SAST, software integrity or WAF.
	5.13	Protect databases, segregate duties and monitor anomalous or bulk queries.	Network behavior analytics where database traffic is visible.	May surface unusual access patterns; does not provide comprehensive database activity monitoring or DB access control.
	5.14	Identify, track and remediate vulnerabilities; assess periodically and after material change.	Exposure Findings.	Continuously validates selected network exposures and remediation status; complements vulnerability scanning.
	5.15	Conduct periodic and post-change penetration tests through qualified providers and remediate findings.	Detection, investigation and coverage evidence during testing.	Shows what attacks were observed and supports closure validation; does not perform or accredit the penetration test.
	5.16	Plan and run red/purple exercises at least every 24 months; report and remediate.	Detections; ATT&CK context; Investigative and response integrations.	Directly supports blue-team validation and evidence; exercise governance, provider choice and remediation plan remain external.
	5.17	Protect cryptographic keys and manage their lifecycle and review.	TLS/certificate-related exposure findings; visibility into post-quantum cryptography communications.	Can identify selected protocol/certificate and cryptography risks; no KMS, HSM or key lifecycle management.

Where Vectra AI Helps: Detect & Respond

Assurance testing, records, monitoring, and threat hunting and incident response.

CCoP Area	Item	Action Item Detail	What Vectra AI Does	Practical Outcome
6 – Detection	6.1	Retain and protect required access/network/security records; synchronize time, analyze and share.	Metadata, detections, audit events, API and SIEM connector.	Feeds operational evidence to a retention platform; does not collect every required log or guarantee 12-month centralized retention.
	6.2	Monitor the whole network, establish baselines, correlate, alert, investigate and support CSA sensors if requested.	Network, cloud, and identity threat detection and response; Attack Signal Intelligence; correlation of signature-based detections.	Core capability for monitored telemetry: behavior analytics, correlation and prioritized entities. Does not replace a CSA-supported sensor under 6.2.4.
	6.3	Conduct proactive threat hunting at least every 24 months.	Investigate search; AI-enriched metadata; guided/prebuilt threat hunts; MDR options.	Directly enables hypothesis-led hunting subject to edition, retention and telemetry coverage.
	6.4	Obtain, process and act on cyber-threat intelligence; share with Commissioner as required.	Threat intelligence; signature-based detections; behavioral detections; APIs.	Operationalizes indicators and behavior context; CTI governance and regulatory sharing remain CIIO responsibilities.
7 – Response & Recovery	7.1	Maintain IR plan/CIRT, escalation, containment, investigation, forensics and root-cause actions.	AI-prioritization; attack progression; AI-assisted investigations; EDR/account/firewall response; SIEM/SOAR integrations.	Strong detection-to-containment support; does not own the IR plan, statutory reporting or full forensic/RCA process.
	7.2	Maintain and exercise crisis-communications arrangements.	Incident timeline and evidence exports.	Provides facts to communications teams; does not manage stakeholder communications or the crisis plan.
	7.3	Maintain comprehensive exercise plan, scenarios, participants, reports, improvements and CSA exercises.	Purple-team validation; detections; investigations; workflow evidence.	Supports realistic technical exercises and proof of response; plan ownership and mandated participation remain with CIIO/CSA.

Where Vectra AI Helps: OT and Interconnected Systems

OT architecture, DNS, and controls for systems that communicate with CII.

CCoP Area	Item	Action Item Detail	What Vectra AI Does	Practical Outcome
10 – OT Security	10.2	Secure OT architecture, restrict enterprise flows, monitor anomalies, separate authentication and fail safely.	Passive network detection and response across mirrored OT traffic and observed-flow baselining.	Direct fit for 10.2.2 anomaly monitoring when traffic is visible; supports architecture validation but not one-way gateways, credentials or fail-safe engineering.
	10.3	Apply secure coding to OT software.		Vectra AI may detect exploitation after deployment; it does not provide SAST, code review or secure-SDLC controls.
	10.4	Protect field-controller code/register integrity and safety functions.		
11 – Domain Practices	11.1	Establish applicability of domain-name requirements.		
	11.2	Implement and maintain DNSSEC.		Vectra AI can reveal suspicious DNS behavior, but does not sign zones, validate DNSSEC deployment or manage keys.
12 – Interconnected Systems	12.1	Inventory and oversee interconnected systems and their communications with CII.	Asset inventory; HostID; observed network communications.	Strong reconciliation evidence for communicating assets.
	12.2	Manage accounts and least privilege for interconnected systems.	Identity and network behavior analytics.	Detects risky use where identity/traffic telemetry exists; no account lifecycle or access recertification.
	12.3	Control privileged accounts, MFA, sharing and break-glass use.	Privilege-abuse detections and investigation context.	Behavior evidence supports oversight; PAM, MFA and privileged-account administration remain external.
	12.4	Segment interconnected systems and enforce minimum, authorized communications.	Observed-flow analytics; exposure findings; traffic lockdown response action and integrations.	Validates actual paths and can assist containment; segmentation design and firewall enforcement remain external.
	12.5	Harden interconnected systems and disable unnecessary services.	Exposure findings for exposed services, weak protocols and TLS.	Provides network-validated hardening evidence; not a configuration-compliance scanner.
	12.6	Patch interconnected systems through governed, risk-based processes.		Can prioritize compensating monitoring, but does not inventory CVEs, deploy patches or manage rollback.
	12.7	Monitor network-management, endpoint and virtualization activity; detect and report suspicious events.	Network detection and response; Attack Signal Intelligence; signature-based detections; investigations; SIEM/API export.	Directly covers visible network behavior and supports correlation; endpoint logs, vSphere checks, retention and CSA reporting need other controls.
Annex A	A	Enterprise cybersecurity posture guidance outside mandatory CII scope.	Network, identity, and cloud platform coverage where deployed.	Can extend consistent detection and investigation to enterprise environments; Annex A is guidance and coverage depends on telemetry.

Direct Alignment **Supporting Alignment** **Other control owner / Not core**

Clause mappings and alignment grades are Vectra AI's interpretation of the Cybersecurity Code of Practice 2026 in relation to platform capability. They are provided for informational purposes and do not constitute legal or regulatory advice.
Source: Cyber Security Agency of Singapore, Cybersecurity Code of Practice 2026 (CCoP 2026).

Pressure-test your CCoP readiness with Vectra AI.

Know what is considered normal. Investigate quickly. Trigger response. Prove what the SOC saw and did.

Build your action plan >

About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world.

For more information please contact us: Email: info@vectra.ai | vectra.ai

© 2026 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and the Vectra Threat Labs, Threat Certainty Index and Attack Signal Intelligence are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Version: 100526