RESPONSE TO ECB SUPERVISORY LETTER SSM-2026-0301, JULY 2026

Assume the breach. Prove the defense.

The European Central Bank has asked significant institutions to submit an action plan by 31 October 2026, showing how they will strengthen defenses against AI-enabled cybersecurity threats. Vectra AI aligns to 12 of the 21 action items in Annex 1, helping banks reduce exposure, strengthen defense in depth and respond faster when prevention fails.

ACTION PLAN DUE
31 OCTOBER 2026
Immediate and proactive action required

WHY NOW
LESS TIME TO ACT
As attacks move at machine speed, defenders have less time to understand attacker behavior and act before business impact.

WHERE VECTRA AI ALIGNS
IMMEDIATE AI-ENABLED DEFENSE
- Enhance monitoring & detection
- Reinforce defense in depth
- Deploy AI-enabled defense

Where Vectra AI maps to ECB SSM action items, DORA and NIST CSF functions

ECB SSM ACTION ITEM — Direct alignment | Supporting alignment | Not covered
DORA ARTICLE — Direct alignment | Supporting alignment | Not covered

NIST CSF 2.0 FUNCTIONS

DORA CHAPTER	Govern	Identify	Protect	Detect	Respond	Recover
II ICT risk management	Art. 5, Art. 6, Art. 7, Art. 9, Art. 10, Art. 11, Art. 12, Art. 13, Art. 16, SSM 4.1, SSM 4.2, SSM 4.3, SSM 2.2, SSM 2.3, SSM 5.4	Art. 8, Art. 11.5, Art. 13.1, Art. 13.6, SSM 1.1, SSM 2.1, SSM 5.3, SSM 5.6	Art. 9.1, Art. 9.2, Art. 9.3, Art. 9.6, Art. 10, Art. 12.1, Art. 12.2, Art. 12.3, Art. 12.4, Art. 12.5, Art. 12.7, Art. 13.6, Art. 13.7, SSM 1.2, SSM 1.4, SSM 2.1, SSM 1.3	Art. 10.1, Art. 10.2, Art. 10.3, Art. 15.3, Art. 16.2, SSM 1.4, SSM 3.1, SSM 5.1, SSM 5.2, SSM 5.3, SSM 5.5	Art. 11.2, Art. 11.3, Art. 13.2, Art. 13.3, Art. 14, Art. 16.4, SSM 6.1	Art. 11.4, Art. 11.6, Art. 12.2, Art. 12.4, Art. 12.6, Art. 12.7
III Incident monitoring and reporting	Art. 17.1, Art. 23		Art. 12.3, Art. 12.7	Art. 17.1, Art. 17.2, Art. 18	Art. 17.3, Art. 17.6, Art. 19, SSM 6.1	
IV Operational resilience testing	Art. 25	Art. 24, Art. 26		Art. 25.1, Art. 25.2, Art. 25.3, Art. 26, Art. 27, SSM 6.2		
V ICT third-party risk	Art. 30.3, Art. 33	Art. 28, Art. 29, Art. 30, SSM 4.3	Art. 28.7, Art. 28.8, Art. 29.2			
VI Information sharing	Art. 45, SSM 6.3					

Where Vectra AI helps, by ECB action area

ECB ACTION AREA	ITEM	ACTION ITEM DETAIL	DORA MAPPING	WHAT VECTRA AI DOES	PRACTICAL OUTCOME
1 **Protect attack surfaces**	1.1	Identify ICT assets, including third-party software and open-source components	Art. 8 ICT asset management	Detects active assets and enriches inventory with observed network, identity and cloud activity.	A reliable asset inventory, with high-value exposed systems ranked first.
	1.2	Minimize and continuously monitor internet-facing, externally exposed, cloud and third-party VPN assets	Arts. 8–10 ICT asset management; protection/prevention; detection	Detects suspicious post-login and post-compromise behavior on exposed assets and identities.	Help the SOC identify where compromise is unfolding and contain it sooner.
	1.3	Prioritize perimeter technologies in remediation, then critical cloud and on-premises systems and security infrastructure	Arts. 9–10 Protection/prevention; detection	*Outside Vectra AI's scope.*	
	1.4	Consider internal as well as external threat vectors	Arts. 9–10 Protection/prevention; detection	Detects threat activity independent of its origin: compromised identities, privilege misuse, lateral movement.	Assume-breach coverage for internally originating threats.
2 **Vulnerability and patch management**	2.1	Use prioritized vulnerability scanning; use AI-based tools only with safeguards and human oversight	Arts. 9, 13 Protection/prevention; learning and evolving	Discovers active attack paths and shows evidence of exploitation and attacker progression.	Remediation and detection sensitivity focused on prioritized entities.
	2.2	Prepare for more frequent and higher-volume patching across vendor, open-source and internally developed software	Arts. 9, 13 Protection/prevention; learning and evolving	*Outside Vectra AI's scope.*	
	2.3	Enable rapid, risk-based emergency change for critical fixes; reflect this in provider contracts and SLAs	Arts. 9, 28, 30 Protection/prevention; third-party risk; contractual arrangements	*Outside Vectra AI's scope.*	
3 **Monitoring, detection and AI-enabled defense** Strong Vectra AI alignment	3.1	Strengthen monitoring of application and access logs, network traffic and compromise indicators	Arts. 10, 17, 18 Detection; incident management; incident classification	Attack Signal Intelligence: behavioral detections, enrichment and correlation across network, identity and cloud.	Enable the SOC to detect, prioritize and investigate critical attacker activity across network, identity and cloud, without deploying agents.
4 **Governance, funding and supply-chain assurance**	4.1	Assess whether budgets, staffing, tooling and change capacity support accelerated patching and AI-enabled defense	Arts. 5–6 ICT risk management and governance; ICT risk-management framework	*Outside Vectra AI's scope.*	
	4.2	Provide risk-appropriate training and awareness across employees, counterparties, third parties and ICT lines of defense	Arts. 6, 13 ICT risk-management framework; learning and evolving	*Outside Vectra AI's scope.*	
	4.3	Assure supplier preparedness for accelerated vulnerability disclosure and patching	Arts. 28–30 ICT third-party risk; contractual arrangements	*Outside Vectra AI's scope.*	
	4.4	Update risk-appetite metrics, tolerance thresholds and controls for increased patching and frontier-AI exposure	Arts. 5–6 ICT risk management and governance; ICT risk-management framework	*Outside Vectra AI's scope.*	

ECB ACTION AREA	ITEM	ACTION ITEM DETAIL	DORA MAPPING	WHAT VECTRA AI DOES	PRACTICAL OUTCOME
5 **Defense in depth and modernization** Strong Vectra AI alignment	5.1	Assume perimeter defenses will be breached, including through faster zero-day exploitation	Arts. 9–10 Protection/prevention; detection	Built on assumed compromise: tracks attacker progression after initial access, privileged activity and command and control.	A technical second line of defense for when preventive controls fail.
	5.2	Strengthen segmentation, micro-segmentation and zero-trust verification across users, devices, APIs and service accounts	Arts. 9–10 Protection/prevention; detection	Detects compromised identities, AI agent and service-account abuse, and lateral movement.	Granted access compared with observed activity, so segmentation and least privilege are validated in practice.
	5.3	Maintain accurate inventory, secure configuration, least privilege, MFA and comprehensive logging	Arts. 8–10 ICT asset management; protection/prevention; detection	Agentless discovery of shadow IT, AI services and identities. Network and authentication logs stay searchable for six months.	Independent, high-fidelity evidence for cyber hygiene and investigation.
	5.4	Apply security-by-design software-development practices	Art. 9 Protection/prevention	*Outside Vectra AI's scope.*	
	5.5	Deploy AI-native and AI-assisted defense with governance, validation and human oversight	Arts. 5–6, 9–10 Governance; ICT risk-management framework; protection/prevention; detection	AI-driven detection, triage and prioritization, paired with analyst-led investigation and response.	The signal that matters, not more automated noise.
	5.6	Replace or update legacy, unsupported and end-of-life systems, or add compensating controls	Arts. 8–10 ICT asset management; protection/prevention; detection	Provides compensating detection for legacy platforms and evidence for modernization priority.	Legacy risk reduced and visibility maintained while migration is under way.
6 **Response, recovery and information sharing**	6.1	Maintain and regularly test crisis management, incident response, backup, failover and recovery arrangements	Arts. 11–13, 17–23 Response/recovery; learning and evolving; incident management and reporting	Supplies attack timelines, investigation context and detection-to-containment measures.	Faster response and recovery, with lessons learned.
	6.2	Exercise high-speed, high-volume, zero-day, ransomware, destructive, supply-chain and cloud-disruption scenarios	Arts. 24–26 Digital operational resilience testing	Powers realistic exercises with live detections, attack paths and measurable response outcomes.	Operational resilience tested against severe, fast-moving scenarios.
	6.3	Establish secure information-sharing arrangements for vulnerabilities, threat intelligence and remediation	Art. 45 Information-sharing arrangements	*Outside Vectra AI's scope.*	

Direct alignment Vectra AI directly supports the ECB action item.
Supporting alignment Vectra AI helps strengthen or validate the action item.
Not covered Outside Vectra AI's scope.

DORA mappings are Vectra AI's interpretation of relevant Regulation (EU) 2022/2554 requirements in relation to the ECB Annex 1 focus areas. They are provided for informational purposes and do not constitute legal or regulatory advice.

Source: European Central Bank, "Addressing AI-enabled cybersecurity threats," SSM-2026-0301, July 2026.
DORA: Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.

Pressure-test your readiness before 31 October

Start from an assumed breach and ask: can we detect what the attacker does after initial access, recognize compromise when valid credentials are used, follow progression across identity, network and cloud, and show that our controls hold under an AI-speed scenario?

Build your action plan with us

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

Version: 091426