

CISO Command Center — Daily Executive Brief

As of: 2026-01-12T17:00:57.035Z+00:00

Consensus: 0

Top Risks: 5

Executive Summary

Weekly intelligence update completed January 12, 2026. CRITICAL: Q-Day timeline ACCELERATED by 1 year (now 6 years). OpenAI reduced estimate from 8 to 6 years based on latest quantum hardware developments. All organizations should expedite PQC migration planning. 197 AI threat articles tracked across 14 categories. AI-Powered Attacks surged with 123 incidents (+35 this week). 4 new CISA KEV entries require immediate patching. Priority actions: (1) Accelerate PQC certificate migration given reduced timeline, (2) Patch 4 new KEVs immediately, (3) Review AI attack surface given 64 new threat articles.

Top Emerging Risks (Projected Escalation, next 30d)

DOMAIN	SEVERITY	IMPACT	TREND	PROJECTED	OWNER	SLA
AI Model Security	Critical	\$5,500,000	Worsening	<div style="width: 92%;"><div style="width: 100%;">9.2/10</div></div>	security@org	14 days
Post-Quantum Readiness	High	\$4,500,000	Worsening	<div style="width: 85%;"><div style="width: 100%;">8.5/10</div></div>	crypto@org	30 days
KEV Exposure	High	\$3,000,000	Worsening	<div style="width: 78%;"><div style="width: 100%;">7.8/10</div></div>	infra@org	7 days
Deepfake Detection	Medium	\$2,000,000	Stable	<div style="width: 62%;"><div style="width: 100%;">6.2/10</div></div>	soc@org	45 days
AI Social Engineering	Medium	\$1,800,000	Stable	<div style="width: 58%;"><div style="width: 100%;">5.8/10</div></div>	security@org	30 days

30-Day Forecast

- **AI Attack Escalation** — 78.0% escalation probability
- **Critical KEV Exploitation** — 62.0% escalation probability
- **Quantum Timeline Shift** — 45.0% escalation probability
- **Deepfake Incident** — 38.0% escalation probability

Operational Snapshot

KEV

New: 4, Modified: 0, Removed: 0

PQC

Coverage: 32% • Hybrid pilot ETA: 2190 days

AI Attack Status

{"AI Bias \u0026 Fairness": 2, "AI Data Poisoning": 1, "AI Governance Gaps": 2, "AI Infrastructure Compromise": 1, "AI Social Engineering": 7, "AI Supply Chain": 2, "AI-Powered Attacks": 123, "Backdoor": 2, "Deepfake \u0026 Synthesis": 9, "Ethical AI Violations": 2, "Output Manipulation": 1, "Privacy Inference": 1, "Regulatory Compliance": 8, "Uncategorized": 36}

Generated by AI PQC Audit — 2026-01-15 08:18:12Z UTC