vCISO for AI Deployments

SECURE YOUR AI FUTURE WITH EXPERT CYBERSECURITY LEADERSHIP

Why Choose a vCISO for AI?

As AI, LLMs and voice automation become central to how businesses operate, the risks scale just as fast. From hallucinations and prompt injection to data leakage and compliance gaps, most organisations are underprepared.

ETT's vCISO services provide specialist cybersecurity leadership tailored for AI-first environments, so you can innovate safely and scale with trust.

FOR MORE INFO
EMERGINGTT.COM

RISKS CREATED BY AI DEPLOYMENTS

AI models producing unsafe or incorrect outputs

LLMs are non-deterministic by nature. Without proper grounding and oversight, they can hallucinate facts, make up customer responses, or take unsafe actions. We help you identify, mitigate, and monitor these risks before they impact customers or compliance.

Regulatory confusion (GDPR, PCI, HIPAA, SOC2)

Voice assistants and LLMs often collect and process personal or sensitive data. We guide you through what applies, what's at risk, and how to align to relevant laws without slowing innovation.

Hidden risks from third-party model providers (e.g. PolyAI, OpenAI)

Just because a model is hosted by a vendor doesn't mean it's risk-free. We assess model provenance, supply chain risk, API controls, change management policies, and provider SLAs—so you don't inherit hidden vulnerabilities.

Gaps in AI incident response and audit readiness

When something goes wrong, most organisations lack the right playbooks or monitoring. We build custom breach response frameworks for AI, help you maintain evidence trails, and prepare for regulator scrutiny.

Gaps against AI-specific ISO frameworks (ISO/IEC 42001, ISO/IEC 27001:2022)

With new standards like ISO/IEC 42001 (AI Management Systems) and updates to ISO/IEC 27001 introducing AI-relevant controls, most organisations aren't ready. We deliver comprehensive gap analysis and remediation roadmaps to align your security posture with these global benchmarks.

CHOOSING THE RIGHT VCISO PACKAGE

Our services are designed to meet you where you are — whether you're just starting your AI journey, scaling fast, or operating across complex, regulated environments.

Foundational

Is for teams launching their first AI or voice assistant use case. It helps identify security gaps, define safe deployment parameters, and ensure you're compliant from day one.

AI-Readiness Assessment & Risk Baseline

- Gap analysis - ISO 27001, 42001, SOC 2, OWASP LLM Top 10
- Threat modelling (voice + LLM)
- Regulatory readiness review (GDPR, PCI, HIPAA)
- Draft AI Use Policy

3–4 weeks | Fixed-fee engagement

Operational

Is for organisations actively scaling AI. You get ongoing access to a dedicated vCISO, hands-on integration security reviews, red team testing, and the strategic oversight needed to expand safely.

vCISO-as-a-Service for Scaling AI Safely

- Everything in Foundation
- Monthly strategic security sessions
- API/CRM/CCaaS integration reviews
- Red team testing (prompt injection, hallucination)
- AI incident response playbooks

Monthly Services | Monthly Retainer

Leadership

Is for large-scale operations running AI across departments, markets, or countries. It delivers end-to-end governance, live model monitoring, ISO/IEC alignment, and executive reporting — giving your C-suite the assurance that AI risk is under control.

Full-Scale AI Command & Control

- Everything in Operational
- Live threat detection for AI models
- Executive/board risk briefings
- AI governance framework for global ops
- Real-time observability & rollback planning

Annual engagement | Custom pricing

The Outcomes You Can Expect

AI deployments you can trust, scale, and explain

We help you implement guardrails, governance, and transparency—so AI doesn't feel like a black box.

Faster rollouts with guardrails built in from Day 1

Security shouldn't slow down deployment. With our guidance, you launch faster—with fewer rework loops, missteps, or post-deploy risks.

Executive-level visibility into model performance and risk

Boards and regulators want evidence—not vague reassurances. We translate technical risks into clear metrics, scorecards, and business-level dashboards.

Reduced exposure to fines, outages, and customer trust erosion

Preventative controls, monitoring, and defined response plans keep small issues from becoming brand-damaging events.

Confidence from board to frontline

Your technical team knows what to secure. Your legal team knows what to report. Your execs know where the risk sits. Everyone's aligned—and confident.

Why Partner with ETT?

- Cyber leadership for AI-first businesses
- Aligned to ISO 27001, 42001, SOC 2, OWASP LLM Top 10
- Customised to your model stack & risk posture
- Real results, not just theory

"AI will only scale with trust. We help you build it."
— Marius Poskus, CISO

FOR MORE INFO
SALES@EMERGINGTT.COM
EMERGINGTT.COM

71-75 SHELTON STREET,
COVENT GARDEN, LONDON,
WC2H 9JQ