AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

How a Global Enterprise Secured AI Adoption Across Multiple Business Units

letsconnect@ampcuscyber.com
www.ampcuscyber.com

01 Overview

Ampcus Cyber helped a Fortune 500 Global Manufacturing & Industrial Technology enterprise move from fragmented, ungoverned AI experimentation to a validated, board-approved AI security program spanning 12 business units and 4 continents.

60 Days	58%	12 BUs
From engagement kickoff to full AI use-case inventory.	Reduction in unsanctioned "shadow AI" tool usage.	Brought under a unified AI governance framework.

Client Snapshot

- **Industry:** Global Manufacturing & Industrial Technology.
- **Engagement type:** AI risk assessment, governance framework design, and security validation.
- **Engagement duration:** 6 months (phased rollout).

02 The Challenge

Like many global enterprises, the client found itself moving faster on generative AI adoption than its security, risk, and compliance functions could keep pace with. Individual business units were independently piloting large language model (LLM) copilots, AI-assisted coding tools, and customer-facing chatbots, often through consumer-grade or unvetted third-party platforms.

This decentralized adoption pattern created several converging risks:

- **Shadow AI:** Employees pasting proprietary code, customer records, and financial data into public LLMs with no data-handling guarantees.
- **No unified inventory:** Security and compliance teams could not answer a basic question, which AI systems and models were in use, where, and by whom.
- **Regulatory exposure:** Emerging obligations under frameworks such as the EU AI Act, NIST AI Risk Management Framework, and sector-specific data protection laws had no clear internal owner.
- **Untested attack surface:** New AI-enabled applications were being pushed to production without adversarial testing for prompt injection, model manipulation, or data exfiltration paths.
- **Vendor risk blind spots:** Third-party AI vendors were being onboarded without a consistent security or privacy review process.

Leadership recognized that innovation could not be allowed to outrun governance, but they also did not want to slow the business down with a blanket ban on AI. They needed a partner who could bring structure and security without becoming a bottleneck.

03 The Ampcus Cyber Approach

Phase 1: AI Discovery & Risk Assessment

Our team deployed a combination of technical discovery (network and SaaS traffic analysis, API and browser-extension telemetry) and structured stakeholder interviews across all 12 business units to build a complete inventory of AI tools, models, and use cases, sanctioned and unsanctioned.

- Cataloged all in-use AI/LLM tools, internal models, and AI-embedded SaaS products.
- Classified each use case by data sensitivity, business criticality, and regulatory relevance.
- Scored risk exposure for every use case using a custom AI risk matrix.

Phase 2: AI Governance Framework & Policy Design

Working with legal, privacy, and business-unit stakeholders, we co-designed an AI governance framework mapped to recognized standards, including the NIST AI Risk Management Framework and ISO/IEC 42001 and tailored to the client's regulatory footprint.

- Established an AI Governance Council with clear ownership and escalation paths.
- Defined acceptable-use policies, data-handling rules, and an AI vendor risk assessment process.
- Created a tiered approval workflow so low-risk AI use cases could move quickly, while high-risk use cases received deeper review.

Phase 3: Security Validation of AI Systems

Our security validation team conducted adversarial testing against the client's highest-risk, customer-facing AI deployments, simulating real-world attacker behavior against AI-specific and traditional attack surfaces alike.

- Prompt injection and jailbreak testing against production and pre-production LLM applications.
- Assessment of data leakage paths between AI systems and sensitive internal data stores.
- Traditional application and API penetration testing of AI-integrated systems and infrastructure.
- Red team exercises simulating misuse of internal AI copilots for social engineering and data exfiltration.

04 Results & Business Impact

Within the first two quarters of the engagement, the client moved from having no consolidated view of its AI risk posture to a governed, monitored, and board-reportable AI security program.

- Full inventory of AI use cases across 12 business units completed within 60 days.
- Reduced unsanctioned "shadow AI" usage by 58% within 120 days through policy, tooling controls, and employee awareness.
- Closed 17 high- and critical-severity vulnerabilities identified during AI security validation before production release.
- Established a standing AI Governance Council with representation from security, legal, privacy, and business leadership.
- Achieved audit-ready alignment with the NIST AI Risk Management Framework ahead of an external regulatory review.
- Cut average AI use-case approval time by 75% from 6 weeks to 4 business days through the new tiered review workflow.

Perhaps most importantly, the client's business units retained the ability to innovate with AI, just within a framework that gave security, legal, and executive leadership confidence and visibility they previously lacked.

Ready to secure your organization's AI adoption?

Ampcus Cyber helps global enterprises govern, validate, and defend AI adoption at scale, without slowing the business down.