How Cranium helped a global life sciences company manage hidden AI risks while driving innovation

70,000
AI/ML REPOS SCANNED

14,000+
HOURS SAVED (YEARLY)

$1.3M
SAVINGS (YEARLY)

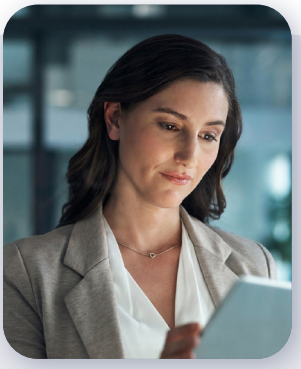
The challenge

Widespread AI initiatives generating unmanaged, and often hidden, risk.

Life sciences are making remarkable strides in AI innovation, delivering life-saving advancements. Yet, this rapid progress brings new risks for organizations.

With numerous business units and third-party vendors deploying AI daily, the company struggled to track where AI systems were used, increasing the risk of shadow AI and potential security breaches. Coupled with an evolving AI regulatory landscape, the company also faced the threat of non-compliance.

To address these challenges, they partnered with Cranium to improve transparency and security in AI development and deployment across all business units, ensuring innovation continued seamlessly.



The solution

Identifying AI/ML-enabled systems across the enterprise with Cranium's Detect AI

The team needed to sort through around 7,000 projects to identify repositories containing AI and machine learning code—an effort that would have taken nearly a year of manual work. In just a few hours, Cranium's Detect AI scanned all the projects and delivered a labeled directory, pinpointing 70,000 repositories containing AI/ML code.

Building a complete AI inventory with Cranium's Code Sensor

After identifying all repositories, the team used Cranium's Code Sensor to create an AI inventory through AI Bills of Materials (AI BOMs). These AI BOMs provided detailed insights into the libraries, models, and datasets composing each AI system. With this enhanced visibility, the team gained a comprehensive understanding of AI across business units, allowing them to conduct targeted vulnerability assessments on each system.

Beating AI security blind spots with Cranium's Vulnerability Assessment

For each AI BOM created, the team used Cranium's Vulnerability Assessment to identify potential threats to their AI systems. By leveraging threat intelligence sources like MITRE ATLAS, OWASP, OSV, and Cranium's own Threat Intelligence Database, the platform scanned each system for vulnerabilities that could increase security and compliance risks.

With a clear list of threats, the team implemented remediation strategies and rescanned to validate their effectiveness. Cranium's support simplified the monthly tracking and reporting process on vulnerabilities identified and resolved, keeping AppSec and CISO leadership informed every step of the way.

Accelerating internal & third-party compliance with Cranium's AI Card

Like many life sciences companies, this company faced challenges staying ahead of evolving regulations while maintaining a seamless R&D workflow. The introduction of the Cranium AI Card proved to be a game-changing solution.

This tool functions as a configurable and shareable "digital passport" for their AI systems, providing detailed insights into development, deployment, and compliance status. With Cranium, the team established clear security and compliance benchmarks tailored to their needs, aligning with industry-leading frameworks such as the NIST AI Risk Management Framework (AI RMF) and ISO/IEC 42001. Validating their systems against these benchmarks became straightforward and efficient.

Extending these controls to their third-party AI ecosystem was equally essential. The Cranium platform now serves as a centralized hub, enabling the creation, sharing, and requesting of AI cards across internal teams, partners, and vendors. This streamlined approach enhances compliance tracking, verification, and transparency throughout their entire AI ecosystem.

The result

Extended visibility, stronger security controls, and significant time saved.

With Cranium, the team achieved a fully automated, end-to-end inventory of their AI systems, eliminating manual discovery and saving over 2,000 hours annually. They have adopted a more proactive AI security posture by streamlining the process to identify and address vulnerabilities across their AI ecosystem. This approach also keeps key stakeholders informed on progress. Today, Cranium serves as their centralized source for tracking compliance across all AI repositories and third-party vendors, ensuring alignment with essential frameworks like the NIST AI Risk Management Framework (AI RMF) and ISO/IEC 42001.

These efficiencies go beyond saving time and resources—they empower this global innovator to focus on life-saving AI initiatives without compromising safety or progress.