apiphani

Advisory Cybersecurity Program

AI adoption is accelerating across the enterprise. Governance, risk, and security frameworks must evolve just as quickly.

As organizations embed AI into core operations, analytics, and decision-making, new considerations emerge around data protection, accountability, monitoring, and resilience. These aren't theoretical risks. They're operational realities that require structure and clarity.

Apiphani's AI Cybersecurity Assessment provides a disciplined, enterprise-ready evaluation of your AI security postur, helping you strengthen controls, clarify ownership, and move forward with confidence.

What **We Examine**

Our AI Cybersecurity Assessment evaluates five domains that determine whether AI is secure, governed, and enterprise-ready.

Data Security	How your AI data is protected across ingestion, training, deployment, and inference — including exposure from shadow AI usage.
Governance, Compliance & Audit	Where AI risk sits within your enterprise risk framework — and whether ownership, documentation, and regulatory alignment are clearly defined.
Threat Detection	How effectively you monitor for model drift, compromise, adversarial activity, and anomalous AI behavior.
Operational Security	Whether AI systems are fully integrated into resilience planning, incident response, and secure deployment standards.
Employee Training & Awareness	How clearly policies, usage boundaries, and cross-functional accountability are understood and enforced.

What You **Receive**

Aligned to NIST CSF, ISO 27001, and CIS Controls, our assessment provides:

- **Actionable Gap Analysis**
- **AI Risk Heat Map**
- **Maturity Scoring Across the Five Domains**
- **Executive-Ready Summary**
- **Prioritized Security Roadmap**

Beyond assessment, apiphani supports vulnerability management, incident response readiness, and compliance alignment so your AI governance model remains durable over time.

Sample **Use Case**

A mid-sized enterprise deploys AI-driven forecasting using sensitive operational data

Our assessment identifies:

- Unmonitored shadow AI usage
- Inadequate controls around model retraining
- Vendor contract gaps around data liability

Within 60 days, leadership gains:

- Clear risk ownership
- Hardened data governance
- Defined monitoring controls
- A roadmap aligned to regulatory expectations

Why **apiphani**

Combining enterprise cybersecurity rigor with deep AI platform expertise, our approach is structured, executive-focused, and prioritizes operational reality over abstract theory.

Our goal is to do more than simply surface risk. It's to help you quantify it, own it, and most importantly, reduce it.

apiphani.io | One Financial Center 16th Floor, Ste. 1640 Boston, MA 02111 | @apiphani | @apiphani.io | info@apiphani.io | +1 (617) 917 5335