Threat IQ

Committed to keeping you secure, always.

AI Integration Risk Assessment Service

Leverage AI with Confidence
Secure and Resilient AI Adoption

The Business Challenge

Businesses are rapidly integrating Artificial Intelligence (AI) solutions to optimize operations, improve product quality, enhance decision-making, and drive efficiency. However, unsecured AI deployments can lead to safety and security risks, data privacy concerns, compliance challenges, and adversarial attacks. Without a structured risk assessment, AI adoption can lead to unexpected vulnerabilities, security risks, operational disruptions and unsafe conditions.

Threat IQ's AI Integration Risk Assessment Service ensures your AI systems are secure, ethical, and resilient, aligning with industry best practices.

Ensure your AI systems are secure and resilient:
Threat IQ's AI Cybersecurity Assessment identifies vulnerabilities, mitigates risks, and ensures AI systems are secure, resilient, and protected from evolving threats, misuse, and exploitation.

Assess the security of custom-built, embedded, and commercial AI applications for vulnerabilities:
AI Integration Security assessment helps protect against threats, ensures compliance, builds trust, and future-proof AI systems for business continuity and resilience.

Without a secure AI integration framework, organizations risk data breaches, compliance violations, and adversarial threats that can compromise business operations and decision integrity.

Business Benefits:

- ✓ Reduced Security Risks
- ✓ Strengthen AI Governance
- ✓ Optimize AI Deployment
- ✓ Enhance AI Trust & Adoption

Take the First Step

Are you confident your AI deployment is secure and compliant?

Let Threat IQ help you assess, mitigate, and optimize your AI risk posture.

Our Assessment Methedology

Identity: Scope & Objectives Definition:

- Identify the AI System(s) to be Assessed.
- Determine the Security Risk Assessment Objectives.
- Identify Stakeholders.

Assess: Risks associated with the AI integration:

- Evaluates the AI Model for Adversarial Vulnerabilities, Model Poisoning, Data Integrity Risks, Assess Exposure to Model Inversion or Extraction Attacks.
- Evaluates Data Protection and Access Controls Risks in AI Models.
- AI Deployment & API Integration to AI Solution and Third-Party AI Risks.

Mitigate: Develop mitigation plan based on risk levels

- Categorize Security Risks Based on Likelihood and Impact.
- Develop a Risk Remediation Roadmap with Prioritized Security Fixes.

What You'll Receive

Comprehensive AI Risk Assessment Report
A detailed analysis of your AI security, compliance, and risk posture.

Actionable Recommendations
Prioritized steps to mitigate risks and improve your AI Integration.

Risk Prioritization & Remediation Plan
Risk mitigation plan with prioritized risk treatment recommendation and residual risk level.

Business Benefits

Reduced Security Risks
Protect AI from cyber threats, bias, and adversarial attacks.

Strengthen AI Governance
Improve data integrity, decision transparency, and accountability.

Optimize AI Deployment
Securely integrate AI without disrupting business operations.

Enhance AI Trust & Adoption
Ensure AI is fair, ethical, and bias-free, fostering stakeholder confidence.