Category

Data & AI

AI Identity, Access & Model Security Management Playbook

Securing AI systems and models with the same rigor you'd apply to any other production infrastructure

- Practitioner
- Advanced
- Template Included

- Administrator
- 25 November 2021
- 3 minute(s)

Overview

A framework for AI identity, access, and model security management — access control for training data and model artifacts, protecting against model theft and extraction attacks, and securing AI-specific attack surfaces — treating AI systems as production infrastructure requiring dedicated security discipline, not an afterthought relative to traditional application security.

Does standard application security cover AI system security

adequately? Standard application security addresses infrastructure and access concerns AI systems share with other software, but AI introduces distinctive attack surfaces — model

extraction, training data poisoning, prompt injection — that require dedicated security consideration beyond traditional application security practices.

What's "model extraction" and why does it matter for AI security?

Model extraction refers to attacks that attempt to reconstruct or steal a proprietary model's behavior through systematic querying, a risk specific to AI systems that traditional application security practices don't typically address, requiring dedicated access control and monitoring for query patterns.

{ "@context": "https://schema.org", "@type": "FAQPage", "mainEntity": [{ "@type": "Question", "name": "Does standard application security cover AI system security", "acceptedAnswer": { "@type": "Answer", "text": "adequately?\nStandard application security addresses infrastructure and access\nconcerns AI systems share with other software, but AI introduces\ndistinctive attack surfaces — model extraction, training data\npoisoning, prompt injection — that require dedicated security\nconsideration beyond traditional application security practices." } }, { "@type": "Question", "name": "What's \"model extraction\" and why does it matter for AI security?", "acceptedAnswer": { "@type": "Answer", "text": "Model extraction refers to attacks that attempt to reconstruct or steal\na proprietary model's behavior through systematic querying, a risk\nspecific to AI systems that traditional application security practices\ndon't typically address, requiring dedicated access control and\nmonitoring for query patterns." } }] }

Subscriber access

Unlock this playbook

This playbook — including every framework, template, and step-by-step section — is available free to Think Insights subscribers. Enter your email to unlock it instantly and get our weekly insights newsletter. No account needed, and access is remembered on this device.

First Name

Last Name

Email

Country - Select -

■ I agree to data processing in accordance with GDPR

Submit

Leave this field blank

References

Related playbooks

Data & AI

AI in Data Engineering & Pipelines Orchestration Playbook

A framework for using AI in data engineering and pipeline orchestration — AI-assisted pipeline code generation, automated data quality monitoring, and intellige

- Practitioner
- Intermediate
- Template Included

Read playbook

Data & AI

AI Data Readiness & Foundation Models Input Quality Playbook

A framework for assessing and building AI data readiness — data quality, completeness, and structure appropriate for foundation model input — recognizing that A

- Practitioner
- Intermediate
- Template Included

Read playbook

Data & AI

AI for Design, Prototyping & Experimentation Workflows Playbook

A framework for using AI in design, prototyping, and experimentation workflows — accelerating prototype generation and iteration speed while maintaining genuine

- Practitioner
- Intermediate
- Template Included

Read playbook

Talk to us about AI security

Tags

- AI Security
- Model Security
- Identity and Access Management

Author

Administrator

Think Insights Administrator