HIDDENLAYER

AI THREAT LANDSCAPE REPORT

Overview

To help understand the evolving cybersecurity environment, we developed the 2024 AI Threat Landscape Report as a practical guide to understanding the security risks that can affect every industry and to provide actionable steps to implement security measures at your organization.

SURVEY FINDINGS

We commissioned a survey of 150 security and data science leaders to reveal the current state of securing AI. The survey uncovered AI's widespread utilization by today's businesses, **but there's still a lot of work to be done to implement proper security measures.**

On average, companies have a staggering

1,689

AI models in production.

98%

of IT leaders consider at least some of their AI models crucial to their business success.

77%

of companies reported identifying breaches to their AI in the past year. The remaining were uncertain whether their AI models had seen an attack.

In response, security for AI has become a priority, with

94% of IT leaders allocating budgets to secure their AI in 2024

Yet only **61%** are highly confident in their allocation

and

92%

are still developing a comprehensive plan for this emerging threat.

These findings reveal ***the need for support in implementing security for AI.***

RISKS INVOLVED WITH AI USE

Adversaries can use a variety of methods to utilize AI to their advantage. The most common include:

- **Manipulation** to give biased, inaccurate, or harmful information.
- **Creation of harmful content**, such as malware, phishing, and propaganda.
- **Development** of deep fake images, audio, and video.

COMMON TYPES OF ATTACKS ON AI

There are three major types of attacks on AI:

- **Adversarial Machine Learning Attacks**
- **Generative AI System Attacks**
- **Supply Chain Attacks**

GET THE FULL REPORT ➔

FEATURED IN VentureBeat DARK READING tech.co