# Dossier: HIDDENLAYER INC

## SBIR Award Details

**Award Title:** N/A

**Amount:** $1,249,913.00

**Award Date:** 2023-09-22

**Branch:** USAF

## AI-Generated Intelligence Summary

**Company Overview:**

HiddenLayer, Inc. is a cybersecurity company focused on protecting artificial intelligence (AI) models from adversarial attacks. Its primary business is providing a security platform that detects and prevents threats targeting AI models at runtime, without requiring access to the underlying model code, training data, or algorithms. Their core mission is to empower organizations to safely deploy and utilize AI by ensuring the integrity and reliability of AI-driven systems. The company addresses the growing vulnerability of AI models to adversarial attacks, which can compromise critical decision-making processes across various sectors, including defense, finance, and healthcare. HiddenLayer's unique value proposition is its agentless security approach, enabling organizations to secure their AI models without impacting performance or requiring modifications to existing AI infrastructure.

**Technology Focus:**

* AI Model Security Platform:\*\* Provides runtime monitoring and protection against adversarial attacks targeting AI models. The platform utilizes machine learning to detect anomalies and identify malicious inputs attempting to manipulate AI model behavior.
* Agentless Architecture:\*\* Deploys without requiring access to the underlying AI models, training data, or code, minimizing integration complexity and preserving intellectual property.

**Recent Developments & Traction:**

* Series A Funding (October 2023):\*\* Raised $50 million in a Series A funding round led by M Ventures and Moore Strategic Ventures. Other investors include Booz Allen Ventures, Lockheed Martin Ventures, and Capital Factory.
* Partnership with Booz Allen Hamilton (2023):\*\* Strategic partnership to deliver AI model security solutions to government and commercial clients, leveraging HiddenLayer's technology to protect AI systems in critical infrastructure and national security applications.
* Product Expansion:\*\* Continued expansion of supported model types, including large language models, computer vision, and time series models, to address a broader range of AI security needs.

**Leadership & Team:**

* Chris Sestito (CEO):\*\* Previously held leadership positions at Claroty, founding team member and VP of Sales at Cylance, and Mandiant. Has extensive experience in cybersecurity sales and go-to-market strategy.
* James Worrall (CTO):\*\* Prior experience with AI model security vulnerabilities and deep background in cloud security.

**Competitive Landscape:**

* CalypsoAI:\*\* Offers an AI security platform focused on governance, risk, and compliance for AI systems.
* Robust Intelligence:\*\* Provides a platform to validate and monitor the robustness of AI models.

HiddenLayer's differentiator is its agentless architecture and singular focus on runtime protection against adversarial attacks, setting it apart from competitors with broader, more general AI security offerings.

**Sources:**

* [https://hiddenlayer.com/](https://hiddenlayer.com/)
* [https://www.securityweek.com/hiddenlayer-raises-50m-series-a-funding-to-secure-ai-models/](https://www.securityweek.com/hiddenlayer-raises-50m-series-a-funding-to-secure-ai-models/)
* [https://www.boozallen.com/s/news/press-release/2023/booz-allen-hamilton-and-hiddenlayer-partner-to-deliver-ai-model-security-solutions.html](https://www.boozallen.com/s/news/press-release/2023/booz-allen-hamilton-and-hiddenlayer-partner-to-deliver-ai-model-security-solutions.html)
* [https://www.m-ventures.com/news/m-ventures-leads-50m-series-a-investment-in-hiddenlayer](https://www.m-ventures.com/news/m-ventures-leads-50m-series-a-investment-in-hiddenlayer)