HensonGroup

Henson Group and Cranium

Case Study

Simplify Your Cloud
Amplify Your Success

HensonGroup.com

Table of Contents

Introduction

Cranium AI, an AI security software company spun out from KPMG, has recently enhanced its security measures by partnering with Armor Defense and Henson Group to introduce an innovative Managed Detection and Response (MDR) service.

This case report outlines the strategic collaboration and the implementation of advanced security solutions to support Cranium AI's compliance and operational needs.

Challenge

Cranium AI needed to ensure that its AI models and applications, particularly the AI Card, adhered to rigorous compliance standards and were protected against increasing cybersecurity threats. The complexity of managing and securing AI applications required a sophisticated approach to security operations, one that Cranium's internal resources could not fully support due to their startup nature and budget constraints.

As AI technologies proliferate, regulatory requirements such as those from the National Institute of Standards and Technology (NIST) and the EU AI Act have become more stringent. Cranium AI sought to bolster its infrastructure security to meet these standards, particularly focusing on the FedRAMP requirements of the NIST standards.

Solution

To achieve comprehensive monitoring and enhanced security analytics, Cranium AI selected Henson Group's Intelligent MDR Security powered by Armor. This new offering integrates extended detection and response (XDR) and security operations center (SOC) capabilities to maximize the utility of Microsoft investments, complementing the existing Microsoft Defender suite.

This partnership exemplifies a seamless integration between managed security services and infrastructure management. Armor's collaboration directly with Henson Group allowed for a reduction in operational overheads and complexity for Cranium, facilitating access to advanced security expertise and resources. As Chris Savage, CTO of Henson Group, said: "We are excited about the partnership with Armor because it empowers us to deliver an in-depth security solution for those managed services customers that require the deep cyber security knowledge that Armor is now delivering for Cranium."

Solution

The primary objective of Cranium AI's initiative was to safeguard its AI systems, particularly focusing on the AI Card application, which aids organizations in assessing the trustworthiness and compliance of their AI models. This partnership Armor and Henson Group involves:

Security Infrastructure Enhancement:

1. Armor's SOC now plays a pivotal role in monitoring Cranium's infrastructure, which includes Azure and Microsoft 365 environments.
2. The service integrates 24/7 monitoring, correlating logs and telemetry data from multiple sources to enhance threat detection and reduce alert fatigue.

Compliance and Reporting:

1. A key feature of the collaboration is supporting compliance with FedRAMP and other regulatory standards.
2. Armor's custom reporting capabilities allow Cranium to maintain comprehensive oversight and deliver detailed compliance reports to stakeholders.

Proactive Threat Management:

1. Armor enhances Cranium's security posture by implementing proactive security measures including advanced threat intelligence and predictive analytics.
2. This shift aims to transition Cranium from a reactive to a more proactive approach in managing security risks.

Outcomes

The partnership has equipped Cranium AI with a robust security framework capable of addressing complex compliance requirements and enhancing its overall security posture. The integrated approach has not only streamlined operations but also provided a scalable model to support future growth and technological advancements.

Conclusion

Cranium AI's decision to partner with Armor and Henson Group represents a forward-thinking approach to cybersecurity in the AI space. This case exemplifies how integrating advanced managed security services can address complex compliance requirements and enhance overall business resilience.

This strategic initiative by Cranium AI not only addresses immediate security needs but also positions the company to confidently navigate the future landscape of AI technology deployment.

Future Outlook

As AI technologies continue to evolve, partnerships like these will be crucial in developing resilient security frameworks that can adapt to emerging threats and regulatory changes. Cranium AI's proactive approach sets a benchmark for the industry, emphasizing the importance of collaboration in achieving comprehensive cybersecurity solutions.