Combatting Insiders and Novel, Unknown Attacks with AI: A Real U.S. Government Case Study

Giuseppe "J.R." Crisafulli
Systems Architect
GDIT

Zachary Vaughn
Director, Federal Security Engineering
Vectra AI

With the proliferation of generative AI models adversaries have gained yet another tool with which to probe, infiltrate and exploit systems supporting and protecting our national security. Methods of compromise and toolsets will more rapidly change and evolve. Vectra AI's unique, security-led approach to apply specific AI/ML algorithms mapped to tactics, techniques and procedures employed by cyber criminals has allowed Vectra to successfully surface unique and novel Insider Threat activities that evade current tooling and superficial, math-led approaches.

Learn how Vectra detects Insider Threats without the need to install agents or break and inspect traffic while operating in completely air-gapped environments and direct analyst focus to the signals that matter without flooding them with noise.

During the session, the attendees will gain a better understanding of a real-world attack simulation completed within the Federal Government. The team will discuss the approach that the malicious insider actor used to circumvent traditional detection and ML-enhanced cyber tools with a TRUE low-and-slow approach where the malicious users lived off the land, and ultimately staged the exfiltrated of multiple gigabytes of data – all of which was detected by Vectra. AI-assisted correlation and scoring of the threat and certainty of the successive attacker behaviors versus simple anomalies and signatures was able to catch the actors before they had the opportunity to inflict damage.