Tuesday, January 28, 2025

1:40 PM – 2:00 PM

Modernizing Defensive Cyber Operations – the AI Imperative

Zachary Vaughn

Director, Federal Security Engineering

Vectra AI

Abstract:

Cyber defenders and incident responders have largely been detecting and reacting to human-driven attack efforts – even large-scale offensive cyber attacks are being launched and managed by human operators. Offensive use of artificial intelligence is expanding and with it the speed and scale at which attackers can operate necessitates defensive security tools capable of responding in kind.

Sophisticated attacks prey upon rigid architectural and political boundaries separating infrastructure, identity, software and platform resources and exploit the deficit of human responders relative to vast amounts of data produced requiring inspection and correlation.

Defenders need tools that 'think' like attackers.

A true security-led AI platform must act as an all-seeing, dispassionate and tireless observer of all interactions across multiple networks to drastically reduce the mean-time-to-detection and mean-time-to-response for defensive cyber operators, incident responders and analysts, providing them immediate context and narrative around the types of indicators and how they play a part of potentially larger attack campaigns.

Vectra is able to operate at scale, drastically reducing the previously manual and reactive tasks of attributing seemingly disaggregated signals and attributing them back to the participating or impacted systems, identities and services.

- Smoke and Mirrors: Not all AI and ML are equal when it comes to security
- Focusing on 'right-of-boom' is a losing proposition. Real-time analysis and correlation across multiple domains empowers defenders to mitigate threats as they occur
- Perimeter defenses alone are not enough; NGFW, EDR and similar technologies continue to be bypassed
- Specific use cases and scenarios where AI/ML is best suited to realize meaningful results
- Supporting existing DCO efforts without additional complexity and friction