Wednesday, August 20, 2025

1:10 PM – 1:30 PM

Future of Threat Hunting

Tim Singletary

Director, Emerging Technologies and Solutions

Peraton

Abstract:

Large, resourceful nations have dominated warfare throughout history, whether kinetic-based and large armies were involved or covertly and cyber-related. These large nations had the resources both intellectually and economically to sustain the advantage in warfare (and cyber warfare). In today's cyber landscape, just like the guerilla warfare from past conflicts, small dedicated groups can inflict significant damage on larger countries with a press of a keystroke. With the growing interconnected world, the cascading effect a single attack can wreak havoc on societies and economies around the world.

At the core of the problem is the lack of visibility and understanding of the millions of data streams that move into and around organization's networks every day. Current security systems can only process a fraction of these streams in real-time. Other security systems rely on IOC's (Indicators of Compromise) to trigger an alert, which could require hours of human review to determine. The majority of these IOC's are either signature or behavioral-based. If one indicator of the attack is dropped during the analysis phase, the IOC may be missed altogether. Compounding this is that most adversaries are aware of the measures most organizations use to detect threats. Attackers can simply avoid these by varying the attack not to trigger the pattern that causes and IOC to cause an alert. A simple technique is to "stage" the attack from multiple sources or multiple destinations, never creating a single session to execute an attack. Even newer detection methods using state of the art AI has already been proven not to be reliable. Attackers simply send unassociated attack data with the actual attack data to "train" the AI to look for a different signature, pattern, or behavior.

Solution:
As cyber threats grow more frequent, sophisticated, and damaging, organizations need more than just passive monitoring—they need real-time intelligence, rapid response, and proactive defense.

Designed for agility and precision, Peraton’s threat hunting capability, ThreatBoard is a game changer in cyber threat intelligence (CTI), detection, and mitigation. Its state-of-the-art artificial intelligence (AI) and machine learning (ML) capabilities analyze vast amounts of diverse threat data, helping organizations uncover stealthy, persistent, and fast-evolving attacks—all from a single, unified dashboard.

ThreatBoard automates the ingestion and synthesis of cyber threat data, transforming fragmented information into a cohesive, real-time operational picture. By mapping relationships among indicators of compromise (IoCs), threat actors, malware, and attack campaigns, analysts can spot patterns faster,

predict adversary moves, and disrupt attacks before they escalate. The result? Reduced detection and response time, lower analyst fatigue, and a more resilient cybersecurity posture.