Tuesday, May 6, 2025
2:50 pm – 3:10 pm
Pre-Emptive Threat Intelligence: Disrupting Adversary Operations Before They Strike

Noah Plotkin
Solutions Engineer
Silent Push

Abstract:
Threat actors rely on well-structured infrastructure to conduct cyber operations, including reconnaissance, malware distribution, and command-and-control (C2) activities. By understanding how adversaries build, manage, and evolve their infrastructure, defenders can shift from reactive response to proactive disruption—denying adversaries the operational environments they depend on. This talk will explore key methodologies for identifying and tracking adversary infrastructure, including fingerprinting hosting patterns, leveraging WHOIS and DNS records, and detecting behavioral signatures that expose attacker operations.

Using Sapphire Sleet—a North Korean APT group—as a case study, we will examine how adversaries strategically age domains, rotate infrastructure, and exploit hosting providers to evade detection. By analyzing their evolving tactics and operational shifts, we'll demonstrate how DoD cyber defenders can apply pattern-based intelligence to preemptively uncover new infrastructure before it becomes fully operational.

Silent Push enables this level of proactive threat hunting through its ability to track adversary infrastructure at scale, leveraging first-party DNS telemetry, real-time scanning, and behavioral fingerprinting to detect pre-weaponized attack infrastructure. By integrating these techniques, defenders can significantly reduce blind spots, identify adversary campaigns earlier, and strengthen their ability to disrupt emerging threats in alignment with DoD cyber defense objectives.

Attendees will leave with actionable methodologies for real-time infrastructure tracking, allowing them to move beyond traditional intelligence gathering toward the active disruption of adversary operations.