Wednesday, August 20, 2025

2:10 PM - 2:30 PM

Hacked from Above: Stopping Adversaries Who Launch Attacks from the Cloud

Jeff Worthington

Public Sector Executive Strategist

CrowdStrike

Abstract:

As the Army accelerates digital transformation and embraces cloud-first initiatives, adversaries are exploiting gaps across hybrid environments—leveraging the cloud plane not just as a target, but as a launchpad for broader attacks. Modern cyber actors—especially nation-states like China and Russia—are adept at exploiting misconfigurations, abusing federated identity, and establishing persistent access through cloud-native services that bypass traditional perimeter defenses.

In this session, CrowdStrike will examine how adversaries weaponize the cloud to move laterally between cloud and on-premise IT assets, using the cloud control plane as a vector to escalate privileges, execute reconnaissance, and disrupt mission-critical operations. We'll highlight real-world threat actor tradecraft, provide insight into how the DoD's attack surface has evolved, and discuss how the convergence of Zero Trust principles with cloud-native security can close critical gaps.

Attendees will gain:

· A threat-focused understanding of adversarial activity in cloud environments

· Insights into cross-domain attacks that begin in the cloud and target on-prem assets

· Best practices to harden identity, protect workloads, and operationalize threat intelligence across hybrid deployments

Cloud is not just infrastructure—it's a warfighting domain. Defending it requires continuous visibility, identity enforcement, and a proactive, threat-informed posture.