Wednesday, May 7, 2025
11:50 am – 12:10 pm
The Evolving Digital Battlefield: Counter State-Backed Cyber Operations in the Cloud Era

Jeff Worthington
Public Sector Executive Strategist
CrowdStrike

Abstract:
Modern cyber adversaries, including state-backed actors like China, exploit identity-based attacks, cross-domain techniques, and cloud-aware tradecraft to bypass traditional security controls. Increasingly, attackers target less protected areas such as SaaS platforms, business email infrastructure, and unmanaged assets. Cloud security threats are rising, with attackers abusing identity and access management (IAM) systems, Single Sign-On (SSO), and federated authentication to hijack sessions and escalate privileges. Business email compromise (BEC) tactics now involve email forwarding rule manipulation and OAuth abuse. Unmanaged assets, including abandoned cloud instances and orphaned accounts, provide footholds for lateral movement. Threat actors employ stealth techniques like Living-Off-the-Land (LOTL), advanced credential theft, and cloud reconnaissance. Multi-stage cyber operations increasingly evade detection, while ransomware groups refine double extortion methods. During this briefing, you will learn how adversaries—particularly China—are leveraging these tactics today. We will cover their evolving methods and discuss strategies to counter these emerging threats.