Tuesday, May 6, 2025
3:50 pm – 4:10 pm
Unlock the Threat: Apply Storyboarding to the Cyber Arena

Aaron Boteler
Chief Technology Officer & Principal Engineer
CloudCurrent LLC

Abstract:

VStrike provides a critical solution for DISA's imperative to modernize its static networks and implement robust deception strategies. At its core, VStrike delivers continuous, real-time analysis of network traffic and sensor data, a fundamental capability for identifying malicious actors and bots exploiting static network vulnerabilities. Operators can now establish baseline network behaviors and detect subtle deviations that reveal anomalies and sophisticated threats that attempt to blend into normal operations.

This foundational real-time visibility seamlessly transitions into VStrike's advanced 3D mapping and detailed data capture, further enhanced by its storyboarding capabilities. These features are pivotal in streamlining the deployment of deception technologies. With centralized management across cloud, DevSecOps, IT, and OT infrastructure, VStrike provides the actionable intelligence necessary to create realistic false targets and decoys. These strategically placed decoys effectively redirect adversaries, disrupt their operations, deplete their resources, and grant stakeholders valuable time to strengthen their defenses.

The efficacy of this integrated approach was vividly demonstrated during the NNSA/DOE Imperial Catfish Cyber Exercise. VStrike distinguished itself as the only solution capable of accurately identifying and animating the Red Team's maneuvers as they gained network control. This unique capability stemmed from its ability to synthesize actionable threat intelligence visuals by consolidating data feeds from multiple vendors—including traffic and hardware alerts—and overlaying them onto a dynamic 3D physical map. This real-world success underscores VStrike’s ability to translate complex data into clear, actionable situational awareness.

Ultimately, VStrike’s storyboarding feature acts as the culmination of its capabilities, transforming raw data into actionable insights. This empowers DISA to deploy defensive countermeasures rapidly, significantly hindering adversarial efforts and providing operators with the necessary time to reinforce network defenses. By facilitating a shift from a static security posture to one that is adaptive, agile, and centered on deception and proactive threat detection, VStrike significantly enhances DISA’s ability to counter evolving cyber threats and ensure a secure, resilient network. In essence, VStrike provides a comprehensive, end-to-end solution for modern cyber defense.