Wednesday, May 7, 2025

8:30 am – 8:50 am

*ARx: Active Cyber Defense & Deception Platform*

**W. Eric Singleton**

Vice President of Operations, Cyber

Cycurion

Abstract:

The Defense Information Systems Agency (DISA) needs advanced cyber defense platforms which actively protect networks while engaging and deceiving adversaries who have become more evasive and persistent.

The active cyber defense platform – ARx creates operational expenses for attackers through its combination of intelligent deception and dynamic traffic analysis and real-time behavioral intelligence.

The platform functions as an intelligent Web Application Firewall (WAF) and reverse proxy which examines and controls incoming traffic across various security checkpoints. Core features include:

- Enforcement and behavioral profiling to detect adversaries and hunt bots.
- Machine learning to score anomalies in real-time.
- Deception technology through simulated targets and agent-based responses to engage attackers and capture their intentions.
- Complete traffic visibility which includes headers and body and origin and geo data for forensic analysis.
- Adaptive rule sets which enable users to customize WAF operations and perform geo-blocking and rate limiting functions.

ARx supports both MITRE ATT&CK and Cyber Kill Chain models to produce threat intelligence data which can be directly integrated into DoD SOC workflows. The deception mechanisms implemented by this platform create expenses for attackers which enable defenders to acquire essential information and time for their response.

The cloud-native platform supports hybrid and on-premises environments which enables DISA cyber defenders to use agile tools for domain maneuvering.