Transforming Cyber Threat Intelligence via 25D

A pivotal role

Sgt. 1st Class Trestan Savoy
U.S. Army Network Enterprise Technology Command

In an increasingly complex cyber domain, the U.S. Army must remain agile and innovative to maintain its advantage. This imperative is at the forefront of the chief of staff of the Army's (CSA) strategic focus, which prioritizes modernizing our forces and enhancing our ability to compete and win against peer and near-peer adversaries.

The Intelligence Support Element (ISE), with its forward-thinking approach to cyber defense, has found a unique force multiplier in the technical expertise of the cyber network defender (25D). By bridging the gap between traditional intelligence analysis and highly specialized cyber investigations, the 25D is transforming the Army's approach to threat intelligence.

Since its inception in September 2022, the ISE has conducted more than 100 successful investigations that have resulted in the development of new detection rules and improved defenses for the Department of War Information Network-Army (DOWIN-A). This success is directly attributable to the seamless integration of traditional intelligence investigations, led by the all source intelligence technician (350F) and intelligence analyst (35F), with the technical depth of the 25D. These collaborative efforts have spurred actionable changes across multiple theaters and refined the tactics, techniques, and procedures (TTP) of our cyber security service provider-defensive (CSSP-D) teams, cyber mission forces, and network engineers.

The ISE routinely conducts in-depth investigations into incidents and alerts on DOWIN-A devices, providing direct, actionable findings to regional cyber center (RCC) directors. The 25D plays a pivotal role in this process as the subject matter expert in cybersecurity, network architecture, and threat actor methodologies. Their extensive training and hands-on experience allow them to use powerful tools like Microsoft Defender for Endpoint, Elastic/Unified-Security Information and Event Management (SIEM), and the Gabriel Nimbus suite to effectively break down cyber incidents. At the same time, the 35F focuses on the "who" and "why" of an attack, while the 25D provides the "how." This includes detailed technical insights essential for understanding while ensuring that every piece of a digital puzzle – from a suspicious log entry to an obscure vulnerability – is properly analyzed.

Concerns from senior 25Ds about defenders working in an intelligence directorate have been addressed by defining a unique role for the 25D within the ISE. This role focuses strictly on cybersecurity investigations, without bleeding into traditional intelligence functions.

Defenders use a specific toolset, including Microsoft Defender for Endpoint, to improve their skills in a cloud environment and develop advanced Kusto Query Language queries. They also hone their SIEM analysis skills by creating dashboards based on alerts, crafting queries to investigate events of interest, and identifying network anomalies specific to their theater of operations. This focused process leverages tools like the Gabriel Nimbus suite, which is used by cybersecurity personnel at the RCCs to respond to, investigate, and report incidents on the DOWIN-A.

The ISE continues to drive innovation by defining a process that develops a defender's skills in the cybersecurity realm. Beyond their role as technical experts, 25Ds within the ISE have significant opportunities for project leadership. As subject matter experts, they are empowered to identify and develop innovative tools and processes that enhance the entire investigation workflow.

If a 25D has an idea for a new capability, they are encouraged to dedicate time to research, develop a use case, and integrate it into the unit's standard operating procedures. This proactive approach to innovation allows defenders to lead from the front, continuously improving the enterprise's defensive posture. A recent use case highlights this value.

A suspected security device compromise on a government network was identified, but there wasn't enough evidence to confirm or deny the breach. The device was taken offline as a precaution. Without the 25D's specialized technical insight, the intelligence investigation would have stalled with an unconfirmed alert, and the device would have remained offline indefinitely. Instead, a 25D with the ISE researched the device model and application version, quickly identifying related vulnerabilities and potential

exploit chains. This clarity provided the precise starting point for a focused investigation: Was that specific vulnerability exploited, what indicators can be linked to the action, and how far can we trace the threat actors' path? This technical clarity informed the intelligence investigation, which in turn yielded a more complete picture.

Results included new indicators for creating detection rules, information on similar malicious actions in other theaters, and an assessment of the overall severity of the incident.

The 25D is more than merely a network defender; they are a key force multiplier in today's cyber environment. By offering technical expertise and practical perspectives, they enable the ISE to move beyond simple alert responses and deliver truly actionable intelligence that safeguards our networks. This unique integration of technical "how" and intelligence "who/why" gives our commanders a critical edge.

As the Army continues to modernize and face increasingly sophisticated threats, leveraging the 25D's unique skills will be crucial for maintaining our readiness to compete and succeed in an ever-changing battlefield. To sustain and grow this vital capability, the RCC ISEs need to expand its ranks.

We call out to the 25D community to preference U.S. Army Network Enterprise Technology Command G2 in their enlisted marketplace to join the ISE team.

Author

Sgt. 1st Class Trestan Savoy is a Washington D.C. native and graduate of the Cyber Network Defender Course (Class 009-22). He currently serves as the senior cyber network defense analyst for the Regional Cyber Center-Pacific Intelligence Support Element. Savoy holds a Bachelor of Science in computer networks and cybersecurity along with a Master of Science in cyber operations.