USCYBERCOM Capability Summary: PacketViper Full-Stack AMTD

Non-proprietary. Response to USCYBERCOM Command Challenge Problems (Edition 3). ≤2 pages.

1. Company Name: Viper Network Systems, LLC d.b.a. PacketViper, LLC **2. Company Website:** https://packetviper.com **3. Company POC Name:** Francesco Trama, Founder & CEO **4. Company POC Email:** frank.trama@packetviper.us **5. Company POC Phone:** 412-368-2077 **6. Company Overview:** PacketViper is a U.S.-based (Pittsburgh, PA) cybersecurity company and originator of Automated Moving Target Defense (AMTD), with foundational IP dating to 2011. Its platform, the Secure Control Layer, delivers preemptive, inline defense for IT and OT in a single agentless appliance, running a closed control loop (Observe → Understand → Decide → Enforce → Prove). Operating thesis: control beats detection, the decisive action happens inline, before an action completes.

7. Capability Name: PacketViper Full-Stack AMTD (network + endpoint)

8. Capability Overview: Full-Stack AMTD continuously shifts the network/endpoint attack surface so adversary reconnaissance goes stale, and distributes rotating Deceptive Responders (decoys) with no legitimate business purpose, making any contact a high-confidence detection. On contact, enforcement is deterministic and policy-driven: inline block, redirect-to-deception, rate-limit, contain, or escalate, surgically scoped to the offending source, never the subnet. A detection at one node propagates fleet-wide ("detection anywhere = containment everywhere"). No human in the loop is required; AI is decision support, not decision-making.

9. Capability / Technology Area Keywords: Automated Moving Target Defense (AMTD); cyber deception; deceptive responders; autonomous containment / self-healing; inline enforcement; proactive cyber defense; Defensive Cyberspace Operations response actions (DCO-RA); self-adaptive architecture; distributed/federated defense; contested-environment operation.

10. Capability Availability: Available now (0 months; fielded, generally available). Orderable government-wide via Carahsoft on Army CHESS **ITES-SW2 (W52P1J-20-D-0042, current participation through ~March 2027)** and via GSA Schedule (durable path). Hardware-agnostic and software-defined, deploys as a PacketViper ruggedized DIN-rail fanless edge appliance or rack appliance (TPM 2.0 hardware root of trust, measured boot, UL/IEC 61010 safety), as a virtual/cloud instance (Azure/AWS/VMware/Hyper-V), or on customer-provided hardware.

11. Technical Readiness Level: TRL 9 for network AMTD (proven in operational use on production IT/OT networks); TRL 7-8 for the endpoint AMTD Agent (2026 release).

12. Applicable CYBERCOM Command Challenge Problems (CCP): - CCP 1.4, Proactive Cyber Defense *(primary; verbatim match):* USCYBERCOM seeks "decoy technology, moving target defense techniques, and refined approaches to Defensive Cyberspace Operations -

Response Actions." Full-Stack AMTD *is* this, rotating decoys + continuous attack-surface movement + deterministic inline response actions in one platform. - **CCP 2.3, Automated Network Healing:** A detection at any node autonomously propagates containment fleet-wide and isolates the affected source without human intervention. - **CCP 3.4, Defending Against Adversary Use of AI:** AMTD is an AI-resistant, self-adaptive architecture. In a March 2026 controlled test run several different ways, a self-replicating autonomous AI attack agent (AutoGen + GPT-4o) was contained at the first sensor across patient, stealthy, and multi-agent configurations, no internal host reached, no data exfiltrated, using standard production settings and no AI-specific detection logic. (Scope: network-layer traversal containment.) - **CCP 5.1, C2 in Contested Environments:** Federation is distributed, not centralized, every node keeps enforcing if the WAN/hub link drops, replays events on reconnect, and hardens under Spoke Lockdown; a multi-tier Sub-Federation hierarchy mirrors a military command tree. - **CCP 1.3, Insider Threat:** Internal contact with a deceptive responder is high-confidence intent; east-west sensors and trust-relationship modeling flag unauthorized lateral activity.

13. What similar technologies exist today? Deception/honeypot tools (legacy Illusive/TrapX-class), EDR/XDR, NDR, SOAR, and OT monitoring (Claroty, Dragos, Nozomi). These are predominantly detect-and-alert or post-compromise, and depend on a human analyst, a SIEM/SOAR layer, or endpoint agents to act.

14. Differentiator / what is innovative: PacketViper blocks the threat itself, inline, at wire speed, with no human in the loop and no SOAR or agent dependency. AMTD makes the attacker's map unstable; deception makes validating that map dangerous ("deceptive contact is probabilistic across probes; enforcement after contact is deterministic"). It is agentless (critical for OT), consolidates roughly five tools into one box, survives network partition for contested operations, and is validated against an autonomous AI adversary. AMTD is patented IP dating to 2011, not a point feature.

15. Compliance: a. **NIST SP 800-53 Rev 5 / 800-171 Rev 2:** Maps to / provides evidence across 800-53 families AC, AU, CA, CM, CP, IA, IR, PE, PM, RA, SA, SC, SI, including **SC-26 (Decoys)** and **SC-30 (Concealment & Misdirection)**, CA-7, SI-4, IR-4, AC-3; and 800-171 families 3.1, 3.3, 3.4, 3.5, 3.6, 3.7, 3.10, 3.11, 3.12, 3.13, 3.14. Compliance evidence is generated as a byproduct of enforcement (SHA-256 hash-chained audit trail). b. **CMMC:** PacketViper's built-in Compliance module maps **control-by-control to CMMC 2.0 Levels 1, 2, and 3**, generating live evidence (one framework within a 665-control / 29-framework mapping engine). Viper Network Systems meets CMMC control requirements and will pursue formal certification if required, for example in support of an Authorizing Official (ATO) process. c. **NIAP / NIST-FIPS:** PacketViper embeds FIPS 140-2 cryptography and operates in FIPS mode (self-contained, no external crypto dependency), using a FIPS 140-2 validated cryptographic module (validated OpenSSL + kernel crypto API; FIPS-mode toggle blocks non-validated algorithms). No separate product-level CMVP certificate; NIAP: not currently held. d. **CSfC:** Not applicable. PacketViper is an inline defense / AMTD / deception platform, not a commercial encryption or VPN component (the categories CSfC covers). Not listed on the NSA CSfC Components List. e. **FedRAMP:** Not applicable. PacketViper is an on-premises, customer-controlled appliance (air-gap capable), not a cloud service offering. f. **DoD Impact Level:** Not separately authorized. DoD Impact Levels (IL2-IL6) apply to

cloud service offerings under the DoD Cloud Computing SRG; PacketViper deploys on-premises inside the customer's own authorization boundary and operates at the impact level of the environment in which it is accredited. g. **Foreign ownership / export control:** Viper Network Systems, LLC is 100% U.S.-owned and staffed by U.S. citizens, no foreign ownership, control, or influence (FOCI). Commercial cybersecurity product; export governed under EAR (not ITAR/USML).

16. Currently in use by U.S. Government (examples): Available to Army, DoD, and Federal agencies via Carahsoft on Army CHESS **ITES-SW2 (W52P1J-20-D-0042)**. Deployed in production across commercial critical-infrastructure and enterprise environments.