USCYBERCOM Capability Summary: PacketViper Analytics, Compliance & Situational Awareness

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, IP since 2011). Its single agentless platform pairs inline enforcement with on-device analytics, situational awareness, and continuous compliance evidence, for IT and OT, including air-gapped and bandwidth-constrained environments.

7. Capability Name: PacketViper Analytics, Compliance & Situational Awareness (AlertBox, Threat Reach, Proactive Advisory, Embedded Compliance & Audit Suite)

8. Capability Overview: PacketViper curates raw traffic into a small set of classified, contextualized signals, profiling normal behavior and classifying every deviation as misconfiguration, unknown device, or threat, rather than flooding analysts with alerts. AlertBox delivers context-enriched telemetry as a lightweight SIEM alternative (10-15 MB/day/unit, works over cellular/satellite/air-gap). Threat Reach reconstructs an indicator's observed reach across the federation for rapid, explainable incident scoping. A local, on-device AI assistant (Proactive Advisory) answers natural-language questions over live traffic with no external AI calls, as decision support. Compliance evidence, mapped to 25 frameworks, is generated automatically as a byproduct of enforcement.

9. Capability / Technology Area Keywords: Cyber situational awareness; SIEM alternative / big-data analytics; AI-assisted threat hunting; false-positive reduction; behavioral analytics; compliance automation; audit evidence; continuous monitoring (cATO/RMF); network topology; DNS/domain/application control; threat intelligence.

10. Capability Availability: Available now (0 months; fielded). Orderable via Carahsoft **ITES-SW2 (W52P1J-20-D-0042, through ~March 2027)** and GSA Schedule. Hardware-agnostic and software-defined, deploys as a PacketViper ruggedized edge or rack appliance, as a virtual/cloud instance (Azure/AWS/VMware/Hyper-V), or on customer-provided hardware.

11. Technical Readiness Level: TRL 9, proven in operational use on customer production networks.

12. Applicable CYBERCOM Command Challenge Problems (CCP): - CCP 3.1, AI-assisted Cyber Threat Hunting: Proactive Advisory answers natural-language questions over live traffic on-device; context enrichment drives ~70% faster triage with drill-down and sharp false-positive reduction (contact with a deceptive responder is a high-confidence, low-

noise signal), including defense of CIKR. - **CCP 3.2, Employ AI for DCO / continuous monitoring:** Inline discovery, quarantine, monitoring, and blocking of vulnerabilities, illegitimate data flows, and suspicious behaviors; AI presents options, the human decides. - **CCP 5.2, SIEM Integration with Big Data:** AlertBox is a SIEM alternative/augment; the on-device analytics engine sustains **501,496 connections/sec and 503,427 events/sec with zero packet drops**, holds **2,000,000 concurrent sessions**, and queries **2.9 billion rows in 0.07 seconds**, big-data analytics at operational speed, on-prem/air-gap capable. - **CCP 5.5, Express Cyber Mission Risk Across Echelons:** Per-device Unified Asset Risk Scores (0-100, composite of CVE, coverage, anomaly, compliance, criticality) roll up across the federation for per-node and multi-node posture at different echelons. - **CCP 2.4, MRT-C Resilience / Situational Awareness:** Living Topology, cross-unit Threat Reach forensics, unified OT+IT asset inventory, and TLS-SNI/DNS visibility map data pathways and establish cyber situational awareness across distributed networks. - **CCP 6.3, Big Data Analytics:** On-device analytics engine identifies and correlates events at scale; ACE adaptive sampling protects the enforcement path under load.

13. What similar technologies exist today? SIEM/SOAR platforms (Splunk, QRadar, Sentinel), NDR, and GRC/compliance tools. These typically require heavy log ingestion, cloud connectivity, separate agents, and human orchestration; most cannot operate on air-gapped OT and treat compliance as a separate workflow.

14. Differentiator / what is innovative: Analytics, situational awareness, and compliance are **byproducts of inline enforcement on one box**, not bolt-on products. It reduces noise at the source (30-70% inbound-traffic reduction; up to ~$300K/site/yr in SIEM cost avoidance; ~70% faster triage), runs a **local AI assistant with no external calls** (data sovereignty), and produces **tamper-evident, SHA-256 hash-chained audit evidence** mapped to 29 frameworks, usable where cloud GRC cannot reach. 93% of proof-of-concepts convert to production.

15. Compliance: a. **NIST 800-53 Rev 5 / 800-171 Rev 2:** Embedded Compliance & Audit Suite maps **~665 controls across ~29 frameworks** with **39 live continuously-validated posture checks**. 800-53 families AC, AU, CA, CM, CP, IA, IR, PE, PM, RA, SA, SC, SI (incl. CA-7 continuous monitoring, SI-4, AU family, SC-26/SC-30); 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. Also IEC 62443, NERC CIP (incl. CIP-015-1 INSM), NIST CSF 2.0, CIS v8, ISO 27001, PCI DSS, HIPAA, CISA ZTA. Evidence supports SCA / Authorizing Official review and cATO. 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.