# Preemptive Defense for Contested Networks

*Automated Moving Target Defense for IT and OT — agentless, inline, fielded today.*

U.S. Cyber Command — Industry Engagement Presentation

August 5, 2026 • Response to Command Challenge Problems, Edition 3

Francesco Trama, Founder & CEO

PURPOSE OF THIS SESSION

# Responding to the Command Challenge Problems

Our July capability submission mapped PacketViper to three CCP clusters. Today we show the evidence behind each mapping.

### Full-Stack AMTD

Preemptive, automated moving target defense that denies reconnaissance and contains intrusions inline.

**CCP 1.3, 1.4, 2.3, 3.4, 5.1**

### OT / Cyber-Physical Protection

Contested critical infrastructure — power, water, fuel, HVAC — protected without agents or downtime.

**CCP 1.2, 2.1, 6.4**

### Analytics, Compliance & SA

Situational awareness and tamper-evident audit evidence generated as a byproduct of enforcement.

**CCP 2.4, 3.1, 3.2, 5.2, 5.5, 6.3**

*Agenda: Problem → Platform → Evidence → Live Demonstration → CCP Mapping → Acquisition Path → Q&A*

THE OPERATIONAL GAP

# Detect-and-respond can't hold contested terrain

### The alert queue is a force-structure problem

Detection-centric defense converts every probe into analyst demand. Readiness is measured on the supply side — recruiting, training, retention — while demand grows unbounded.

### OT can't tolerate the response gap

In cyber-physical environments, dwell time between detection and response is measured in physical consequence — power, water, fuel, HVAC.

### Autonomous attackers move at machine speed

AI-driven, self-replicating attack agents act faster than human-in-the-loop response cycles. Signature and behavior detection chase a moving target.

**The premise we challenge:** defense doesn't have to start after the attacker succeeds.

THE PLATFORM

# One agentless platform, five integrated functions

*PacketViper originated Automated Moving Target Defense — IP dating to 2011. Deception is an enforcement trigger within AMTD, not the identity.*

### Automated Moving Target Defense

Continuously changes the attack surface — what attackers map is stale before they act.

### OT Protection

Purpose-built for cyber-physical and legacy environments; no downtime to deploy.

### Cyber Deception

Lightweight decoys as tripwires that trigger enforcement, not analyst tickets.

### Integrated Security Analytics

Enforcement telemetry becomes situational awareness and audit evidence automatically.

### Inline Policy Enforcement

Containment at the network layer in-line, in milliseconds — no agent, no endpoint dependency.

**Agentless. Inline. IT + OT.**
No rip-and-replace; complements existing sensors and SIEM/SOAR investments.

OPERATING CONCEPT

# Preempt → Trigger → Contain → Evidence

1

**PREEMPT**

Attack surface shifts continuously; reconnaissance yields stale, false terrain.

→

2

**TRIGGER**

Contact with decoy or policy violation is a high-confidence signal — no tuning, no baseline.

→

3

**CONTAIN**

Inline enforcement blocks at the network layer in milliseconds, before lateral movement.

→

4

**EVIDENCE**

Every enforcement action generates tamper-evident, framework-mapped audit evidence.

**No agents on endpoints or PLCs**

**No AI-specific detection logic required**

**Human-on-the-loop, not human-in-the-loop**

EVIDENCE — CCP 1.2 / 1.4

# Documented test: FOB utility segments

Representative FOB environment — power, water, fuel, HVAC — attacked in multiple configurations.

**4 / 4**

**attack runs contained**

every run, every configuration

**< 2 ms**

**inline blocking**

before lateral movement

**0**

**agents deployed**

no endpoint or PLC software

Results mapped to the DoD Zero Trust for OT framework (Nov 2025) and MITRE ATT&CK for ICS.

*Red-team engagement report and NIST 800-53 / DoD OT Zero Trust control-mapping available on request.*

EVIDENCE — CCP 3.4

# Containing an autonomous AI attack agent

March 2026 controlled test — standard production configuration, unmodified.

## Contained at first contact

- Adversary: autonomous, self-replicating AI attack agent
- No AI-specific detection logic, signatures, or model updates
- Containment triggered by the agent's own first contact with the shifting surface
- Defense held at machine speed — no analyst in the loop

### Why it matters to the Command

Preemptive defense scales against adversaries that don't yet exist. If effectiveness doesn't depend on recognizing the attacker, novel and AI-driven tradecraft loses its first-mover advantage.

# Live Demonstration

*5–8 minutes • production configuration*

Recon against a protected segment → decoy contact → inline containment → evidence trail

ALIGNMENT

# Command Challenge Problem mapping (Edition 3)

| | | |
|---|---|---|
| **Full-Stack AMTD** | Preemptive surface change, deception-triggered inline containment at machine speed | 1.3, 1.4, 2.3, 3.4, 5.1 |
| **OT / Cyber-Physical Protection** | Agentless defense of contested critical infrastructure; validated on FOB utility segments | 1.2, 2.1, 6.4 |
| **Analytics, Compliance & SA** | Enforcement telemetry as situational awareness; tamper-evident, framework-mapped evidence | 2.4, 3.1, 3.2, 5.2, 5.5, 6.3 |

*Where no predefined criterion matches, we welcome consideration through the USCC Innovation process.*

ANALYTICS, COMPLIANCE & SITUATIONAL AWARENESS

# Compliance evidence as a byproduct of enforcement

**665**

**controls mapped**

**29**

**frameworks covered**

**Frameworks include**

NIST 800-53 & 800-171 • CMMC L1–L3 • IEC 62443

NERC CIP (incl. CIP-015-1) • DoD Zero Trust for OT

### Tamper-evident audit evidence

Every enforcement action is recorded as verifiable evidence — compliance posture is produced continuously, not assembled for audits.

### Command-level situational awareness

Enforcement telemetry rolls up to a live picture of contested terrain — what probed, what was denied, what shifted.

COMPANY & PROVENANCE

# U.S.-owned, U.S.-built, fielded today

### 100% U.S.-owned

Pittsburgh, PA. Staffed by U.S. citizens. No foreign ownership, control, or influence (FOCI-free).

### Originators of AMTD

Intellectual property dating to 2011 — this is our category, not a feature bolted onto a detection product.

### Fielded & proven

In production across critical-infrastructure operators today; validated in documented red-team engagements.

### Small-team accessible

Direct access to the engineers who build the platform — no layers between the Command and answers.

ACQUISITION

# Available to DoD today — no new competition required

### Army CHESS ITES-SW2

Contract W52P1J-20-D-0042 via Carahsoft — evaluate or pilot without a new competitive action.

### GSA Schedule

Alternative path for components and services beyond ITES-SW2 scope.

### Vulcan (SOF)

PacketViper capability profile established on vulcan-sof.com per the Command's invitation.

**Bottom line:** a pilot can begin on existing vehicles — the distance from interest to evaluation is short.

PROPOSED NEXT STEPS

# Where we'd like to go from here

packetviper.com/uscybercom

1

## Technical exchange

Deep-dive with your subject-matter experts on architecture, evasion resistance, and OT deployment models.

2

## Evidence package

Red-team engagement report + NIST 800-53 / DoD OT Zero Trust control mapping — delivered this week.

3

## Capability demonstration or pilot

Reproduce the FOB scenario — or your scenario — in an environment the Command designates.

Francesco Trama, Founder & CEO • frank.trama@packetviper.us • 412-368-2077 • packetviper.com