carahsoft

CrunchAtlas
Automate. Hunt. Defend.

Agentic Threat Intelligence for IT, OT, ICS & Mission Networks

Federal Solution Brief

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, ITES-SW2, NASPO ValuePoint and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with CrunchAtlast, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/CrunchAtlasResources

Join Events & Webinars:
carah.io/CrunchAtlasEvents

Discover Technology Solutions:
carah.io/CrunchAtlas

Learn About Procurement:
carah.io/CrunchAtlasContracts

Connect With Our Team:
CrunchAtlas@carahsoft.com
(703) 871-8548



Agentic Threat Intelligence for IT, OT, ICS & Mission Networks.

IT, OT & ICS Security Technology and Services

CrunchAtlas detects, hunts and investigates threats across IT, OT, ICS and mission networks. It then correlates what it finds into campaigns, within one environment and across partner organizations.

A receive-only sensor or existing telemetry supplies the evidence. Every detection is investigated by ClemAI, an agentic investigation layer, before it reaches an analyst, who reviews an evidence-backed case rather than an alert. The same software runs hosted, portable or on premises, connected or fully air-gapped.



The Problem

State-sponsored actors move through enterprise IT and industrial control networks using valid credentials and built-in tools.[1,2] The same tradecraft works on defense and mission networks. Each step looks like routine administration, so the alert, if one fires, comes late.

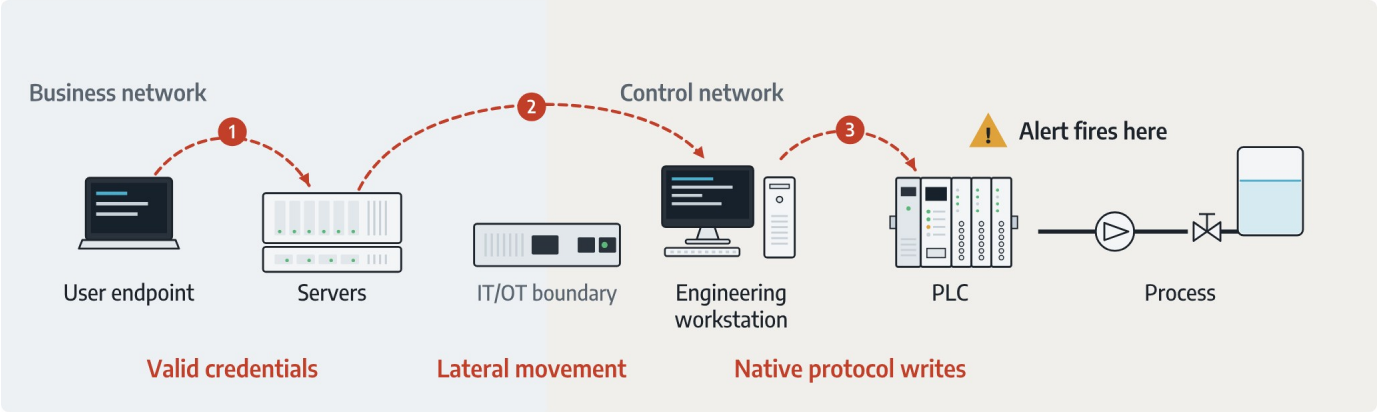


Figure 1. The alert shows the last step. The response depends on the first two.

An alert shows where an adversary surfaced, not how they got in or what else they reached.

1. CISA, NSA, FBI et al., AA24-038A, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Feb. 2024. 2. CISA et al., AA26-097A, *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure*, Apr. 2026, updated Jul. 2026.

Network Architecture & Deployment

A receive-only sensor adds visibility without scanning, host agents or changes to the network. The same software runs wherever the mission draws its boundary.

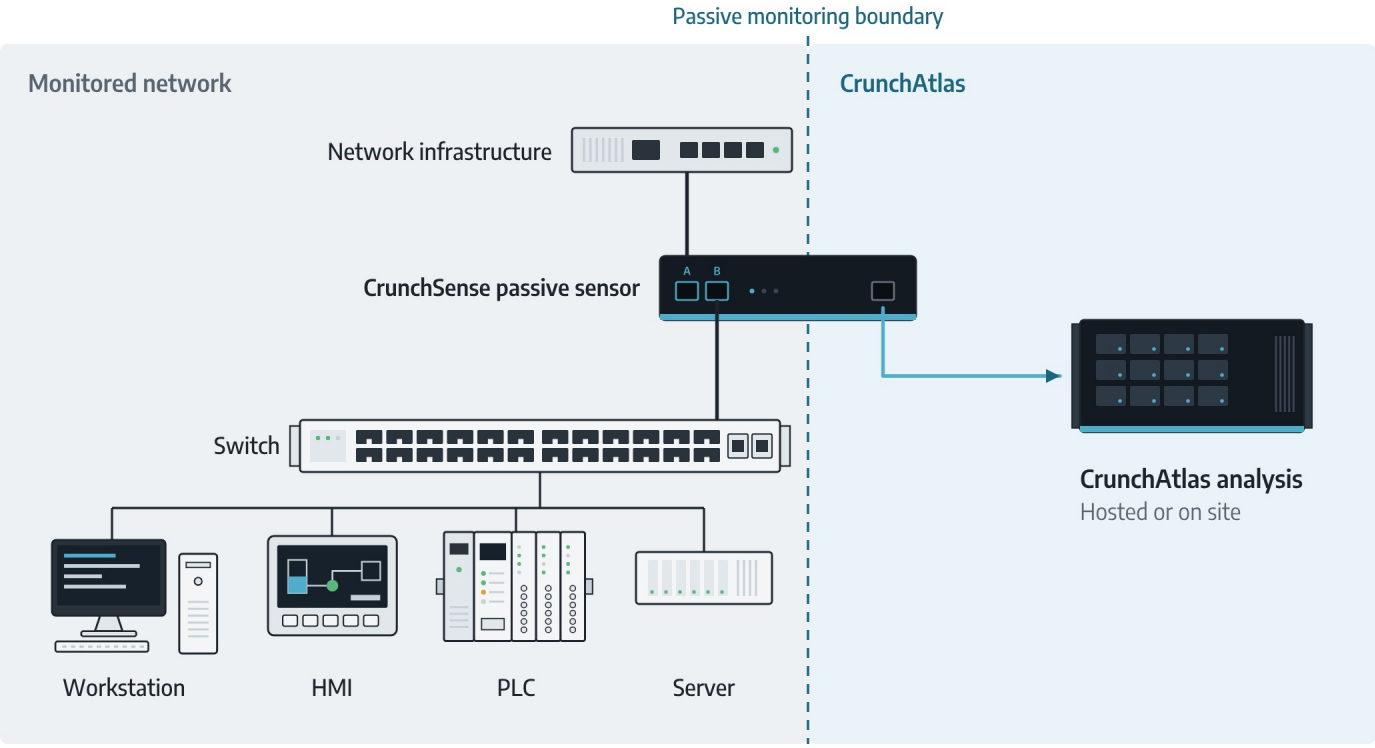


Figure 2. Integrated fail-open TAP. A SPAN port or existing telemetry can feed the same analysis.

Hosted

Sensor on site. Analysis runs in the CrunchAtlas environment over outbound-only TLS.

Portable · CrunchMini

Full analysis on one portable unit for deployable response. Connected or air-gapped.

On premises · CrunchBox

Full analysis on a 4U server for multiple analysts at installations and closed enclaves.

Air-gapped operation disables hosted analytics, remote administration, internet updates and outbound telemetry. Updates arrive by approved offline transfer and are verified before installation.

Threat Detection & Investigation

Every detection is investigated before it reaches an analyst.
The analyst reviews a case, not an alert.

Investigated case ClemAI

Key Evidence 1

- **Commands:** 48 Write Multiple Registers (FC 16), 40101–40106
- **Path:** 10.1.17.2xx to PLC 10.1.17.1xx, unit 1, TCP 502
- **Frequency:** one write about every 13 s for 11 minutes
- **PLC response:** all 48 acknowledged, 0 exception responses
- **External:** 11 outbound TLS sessions to 203.0.113.xxx:443
- **Ruled out:** HMI polling, retransmission, capture artifact

Recommendations 2

1. **Verify authorization** with Facility 1 operations for these writes
2. **Compare registers 40101–40106** to last known-good values
3. **Review workstation 10.1.17.2xx** for remote access and logons
4. **Preserve evidence**: full PCAP, PLC event log, host image
5. **Block 203.0.113.xxx** at the IT/OT boundary
6. **Investigate related activity** to and from 10.1.17.1xx
7. **Alert on further FC 16 writes** to PLC 10.1.17.1xx

MITRE ATT&CK for ICS Techniques 3

Based on the observed activity, the following MITRE ATT&CK for ICS techniques are likely involved:

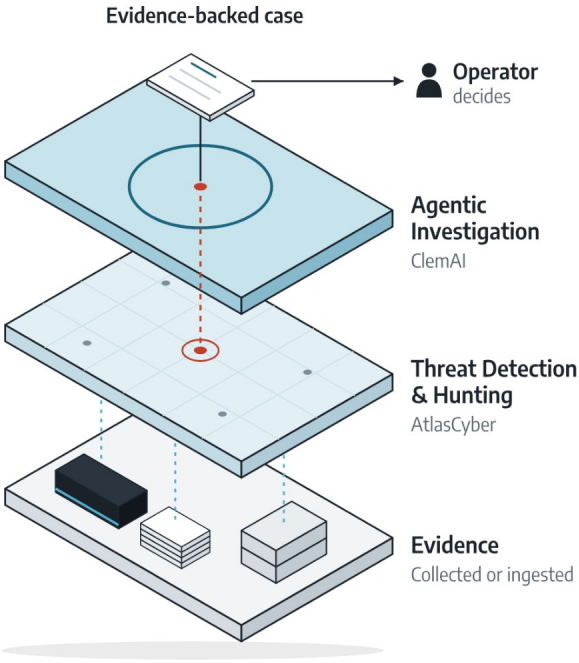
- **T0855: Unauthorized Command Message** - 48 FC 16 writes
- **T0861: Point & Tag Identification** - FC 3 reads first
- **T0869: Standard Application Layer Protocol** - TLS egress
- **T0885: Commonly Used Port** - External traffic on TCP 443
- **T0836: Modify Parameter** - Possible; depends on register use
- **T0886: Remote Services** - Possible; session origin unknown

Conclusion 4

This analysis confirms a **TRUE POSITIVE** detection of suspicious Modbus write activity. Engineering workstation 10.1.17.2xx sent 48 Write Multiple Registers (FC 16) commands to PLC 10.1.17.1xx over TCP 502, and the PLC acknowledged every one. The same workstation separately held 11 outbound sessions to 203.0.113.xxx on TCP 443. Whether the writes were authorized, and any effect on the PLC or the process, are not yet established and require operator validation.

VERDICT True Positive High Confidence 5

Production interface with demonstration data from a Modbus write alert. Addresses masked.



What the case shows

1. Key evidence and what was ruled out
2. Recommended actions, in order
3. ATT&CK for ICS techniques
4. What is not yet established
5. Verdict and confidence

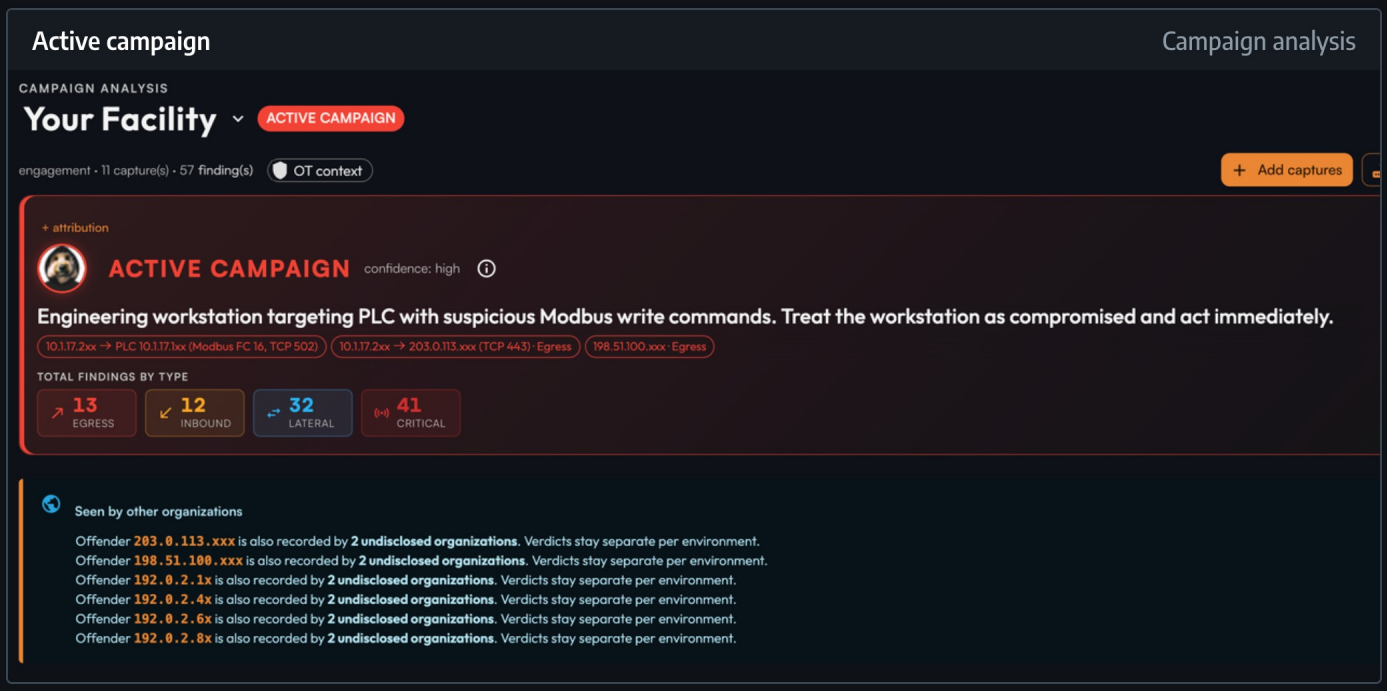
Protocol coverage

Modbus/TCP, DNP3, EtherNet/IP, BACnet/IP, S7comm and OPC UA, alongside IT traffic.

Campaign Intelligence & COP

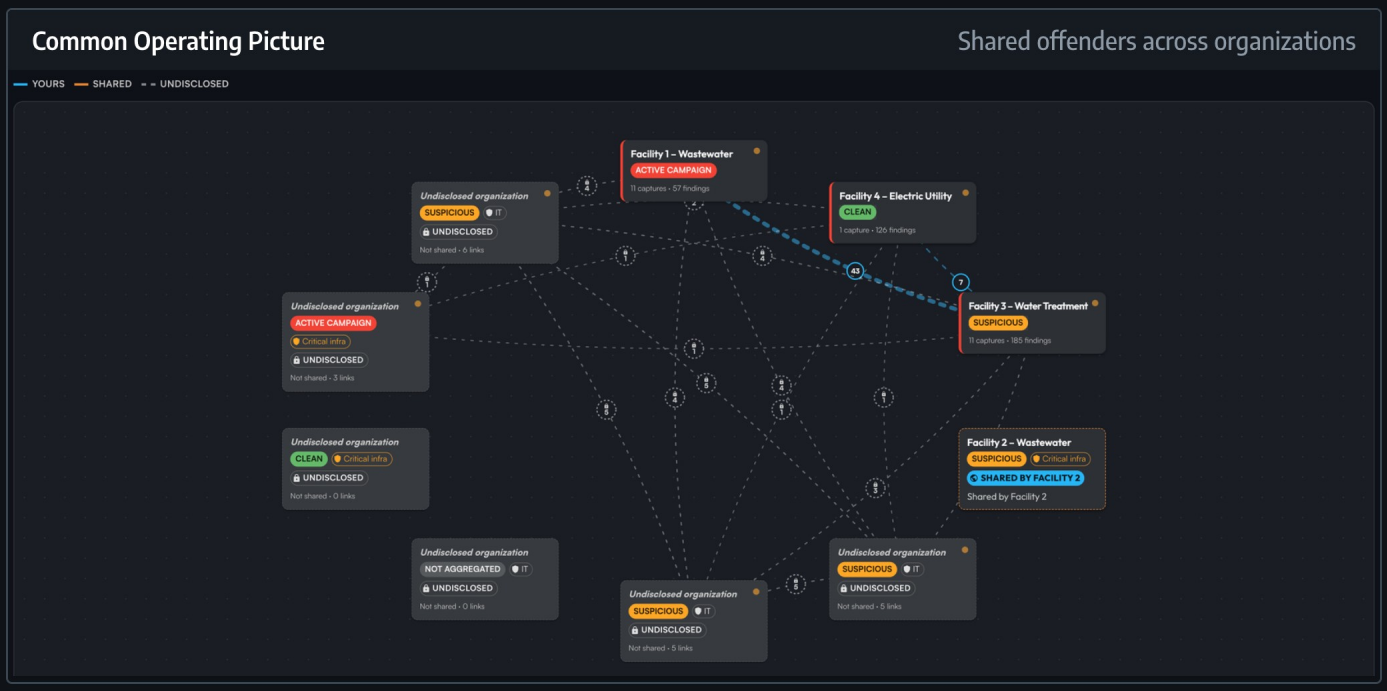
Campaign correlation Within one environment

Findings across captures become one judgment and one instruction.



Collaborative intelligence Across organizations

Partners share approved indicators. Evidence and verdicts stay local.



Production interface with demonstration data. Illustrative scenario; addresses masked, facility names anonymized.



Operational Evidence & Leadership

In use across infrastructure, defense and active response. Customer names are withheld.

Municipal and public infrastructure	Water, wastewater and municipal networks run the full platform.
Private utilities	Electric utilities monitor and investigate their OT networks.
Federal and defense	U.S. INDOPACOM pilot: operational OT deployment, fully air-gapped.
Active incident response	The same case workflow serves live incidents and persistent defense.
Regional collaborative intelligence	The New England Utility Cybersecurity Integration Collaborative operates CrunchAtlas with power and water utilities, connected and air-gapped.

45+

Years combined experience

Cyber domain experience built on 45+ years of combined military experience across U.S. Special Operations and Intelligence Community environments.

Ben Faberlle
CEO and Co-Founder

Sean McQuade
COO and Co-Founder

To arrange an evaluation: Sean McQuade, COO · sean@crunchatlas.com · 603-205-2511

CAGE 0W5Q8 · UEI SNAMPH9GTA97 · NAICS 541511 · Small business · Nontraditional defense contractor · Carahsoft · Tradewinds · ARC