GALVANICK

carahsoft.


GALVANICK

Technical Brief

THREAT INTELLIGENCE AUGMENTATION

Problem

Industrial attacks use indicators that appear across multiple organizations and sectors. Security teams lack context about threats targeting their OT vendors, protocols, or configurations. Critical intelligence exists but remains disconnected from detection systems. Teams manually correlate external warnings with internal telemetry, missing time-sensitive indicators.

Galvanick's Unique Approach

Galvanick automatically ingests and adds third-party threat intelligence with our multi-source detection in the threat detection engine.

Our platform transforms external indicators into actionable detections specific to your environment.

Technical Differentiators

- Total enrichment: Augments behavioral detections with latest threat actor TTPs and IOCs.
- Asset-specific correlation: Maps global threats to your specific PLCs, HMIs, and protocols.
- Federated architecture: Customer-specific threat intelligence is never transmitted outside the customer deployment.

Why This Matters

When CISA issues alerts about OT attacks, organizations spend days determining exposure. When new attack variants emerge, teams cannot identify similar patterns in their environment. Galvanick instantly correlates external intelligence with your specific assets, identifying immediate risks and detecting related attack patterns.

For organizations requiring global threat awareness, Galvanick is the only platform that automatically correlates third-party intelligence with multi-source telemetry to deliver environment-specific threat detection.

SECURE INDUSTRIAL OPERATIONS 2025 GALVANICK, INC. SEATTLE & LOS ANGELES LEARN MORE AT GALVANICK.COM

# Threat Intelligence Augmentation

Thank you for downloading this Galvanick technical briefing. Carahsoft is the government solutions provider for Galvanick cybersecurity solutions available via NASA SEWP V, E & I, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Galvanick's solutions, please check out the following resources and information:

For additional resources:
carah.io/GalvanickResources

For upcoming events:
carah.io/GalvanickEvents

For additional Galvanick solutions:
carah.io/GalvanickSolutions

For additional cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Galvanick@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/GalvanickContracts

GALVANICK

# Technical Brief

## THREAT INTELLIGENCE AUGMENTATION

### Problem

Industrial attacks use indicators that appear across multiple organizations and sectors. Security teams lack context about threats targeting their OT vendors, protocols, or configurations. Critical intelligence exists but remains disconnected from detection systems. Teams manually correlate external warnings with internal telemetry, missing time-sensitive indicators.

---

### Galvanick's Unique Approach

Galvanick automatically ingests and adds third-party threat intelligence with our multi-source detection in the threat detection engine.

Our platform transforms external indicators into actionable detections specific to your environment.

### Technical Differentiators

- Total enrichment: Augments behavioral detections with latest threat actor TTPs and IOCs.
- Asset-specific correlation: Maps global threats to your specific PLCs, HMIs, and protocols.
- Federated architecture: Customer-specific threat intelligence is never transmitted outside the customer deployment.

---

### Why This Matters

When CISA issues alerts about OT attacks, organizations spend days determining exposure. When new attack variants emerge, teams cannot identify similar patterns in their environment. Galvanick instantly correlates external intelligence with your specific assets, identifying immediate risks and detecting related attack patterns.

**For organizations requiring global threat awareness, Galvanick is the only platform that automatically correlates third-party intelligence with multi-source telemetry to deliver environment-specific threat detection.**