Critical Infrastructure Protection Under Adversarial Awareness

by Nick Clark | Published April 25, 2026

What Critical-Infrastructure Security Currently Looks Like

The current pattern is medium-specific tooling integrated through SOCs and SIEMs. IT-network monitoring (firewalls, IDS, EDR) produces network-medium observations. OT-network monitoring (Claroty, Dragos, Nozomi) produces ICS-medium observations. Physical security (badge access, camera systems, perimeter sensors) produces physical-medium observations. Each runs in its own silo with bidirectional integration handled at SOC analysts' workstations.

The pattern works for single-vector attacks. A network intrusion that stays in the network layer produces clear within-medium signal that the IT-network tool detects. The pattern fails for cross-vector attacks: a network intrusion that drives ICS-medium effects that produce physical-medium consequences requires cross-medium attribution that the siloed tooling does not produce.

Why Multi-Vector Attacks Are the Operational Reality

Recent critical-infrastructure attacks have been multi-vector by design. Colonial Pipeline (2021): network intrusion → IT business systems impact → operational

technology shutdown. Volt Typhoon (ongoing): network intrusion → ICS reconnaissance → potential physical-effect pre-positioning. Industroyer / CrashOverride (2016): network intrusion → SCADA manipulation → physical grid impact.

The multi-vector pattern defeats single-medium analysis structurally. SOC analysts reconstruct the cross-medium narrative manually, hours-to-days after the attack progresses. The architectural gap is between the attack's tempo (minutes to seconds) and the manual cross-medium reconstruction's tempo (hours to days).

How Cross-Medium Sensing Composes With SOC Tooling

The disruption-modeling primitive consumes credentialed observations across IT, OT, and physical media simultaneously. Cross-medium correlation against credentialed multi-vector signatures (signed by CISA, ISACs, defense authorities) produces attributed multi-vector cause at machine tempo rather than analyst tempo.

The architecture composes with existing SOC tooling rather than replacing it. The IT, OT, and physical tools continue to produce their within-medium observations. The cross-medium primitive sits above them and consumes their outputs as governance-credentialed observations. The integration is additive; the value comes from cross-medium correlation that was previously the exclusive responsibility of human analysts.

What This Enables for Critical-Infrastructure Resilience

Operators gain operational tempo for multi-vector attack response. Cross-medium attribution at machine tempo lets the response logic engage before the attack progression completes. Graduated response (constrain operation, isolate affected

segments, alert peers, escalate to authorities) operates structurally rather than through manual procedure.

Cross-operator coordination becomes structural through the mesh. ISACs and CISA gain attributed multi-vector observations from operators they credential, supporting cross-operator pattern detection that single-operator analysis cannot produce. The patent positions the primitive at the layer critical-infrastructure resilience will require as multi-vector attack sophistication continues to grow.