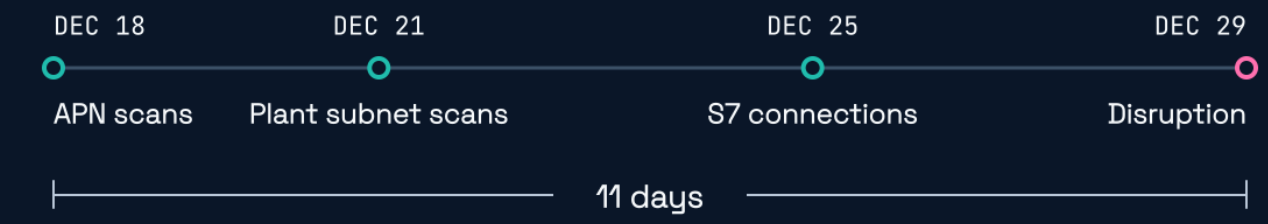
EARLIER WARNING. RECOVERABLE EVIDENCE.

The evidence that survives

Put a deliberate detection opportunity beside the access paths that matter. Preserve the record beyond the device.

OBSERVED ACTIVITY / DECEMBER 2025

A window for earlier warning



Recorded reconnaissance preceded disruption by eleven days.

Maintenance was underway, so the plant initially suspected contractor error. CERT Polska's investigation established a cyberattack.

Eleven days separated the first recorded private-APN reconnaissance from disruption at the Polish combined heat and power plant. That is a window in which a reachable, monitored decoy could have exposed unexpected discovery before destructive action.

Our goal is to give the responder less guesswork: a distinct interaction, enough context to investigate, and a record they can still retrieve during recovery. The pilot tests reachability, capture, and response on the selected site architecture.

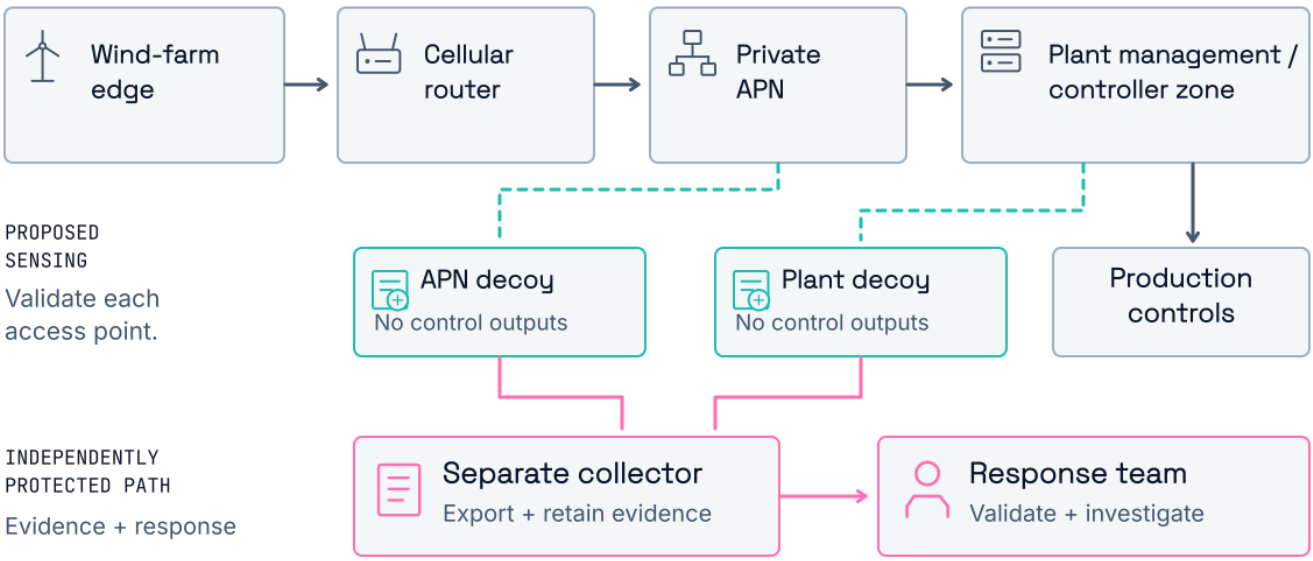
Nick Carroll, Co-Founder & CTO
Deception Check, Inc. | deceptioncheck.ai

Private connectivity is not isolation.

The reported route crossed sites. Detection should follow reachable services, not the reassuring labels on a network diagram.

CONCEPTUAL DESIGN / PROPOSED PLACEMENTS

Place sensing. Protect the evidence.



Verify reachability, protocol fit, separation, export, and response before deployment.

CERT Polska reconstructed a route from wind-farm perimeter infrastructure through a cellular router and a distribution operator's private APN to a WAGO controller at the plant. Its reachable management interface used default credentials. From there, the intruder reached the operational network.

Remote-access edge	Represent a non-production management service that discovery from the approved remote-maintenance zone can reach.
Plant boundary	Use a qualified industrial persona on a controlled branch. Keep it out of protection, interlock, and real I/O functions.
Engineering workflow	Place synthetic recovery or configuration material where unexpected access has meaning; keep real secrets out of the lure.

Sources: CERT Polska follow-up, August 2026; CISA, Using Cyber Decoys to Strengthen Detection and Response.

Show the behavior, not just a count.

Three bounded examples from Deception Check research and controlled testing show what an investigation can receive.

RESEARCH OBSERVATION / NATIVE S7 / SEPTEMBER 20, 2026

RECORDED OFFSET	SELECTED FIVE-EVENT EXCHANGE
+0 ms	COTP connection recorded
+104 ms	S7 communication setup
+203 / +313 ms	Read SZL 0x0011; two identification requests
+413 ms	Read SZL 0x001C; identification request

The selected exchange returned three deterministic identification responses. It demonstrates visibility into native S7 discovery, not a process-control attack. The 413 ms is the span of this recorded exchange, not an alert-delivery or response-time measure.

Controlled DNP3 check: before reboot -> after reboot

A September 8 controlled test rebooted the host running a pipeline-oriented research block-valve RTU persona. Checks before and after verified DNP3 Group 110 content, addressing, reconstruction, and wire CRCs, confirming protocol recovery. Off-host evidence preservation under sensor loss is the next acceptance test.

Beyond the login: retained SSH submissions

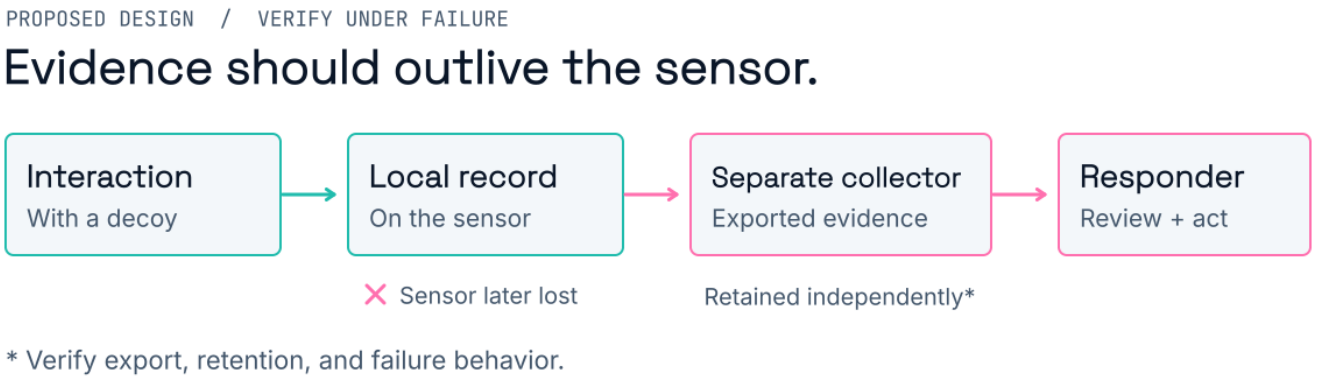
A bounded August comparison retained 24 sessions with the same ordered 16 submitted fragments across several emulated management interfaces. These sessions were received by simulated services and document attempted behavior, not execution or attribution.

Research observations inform what to instrument. Site commissioning establishes whether the selected profile, placement, and alert route answer the owner's detection question.

Evidence: retained Deception Check records listed on page 5. Related reading: After the Login.

Evidence beyond the sensor.

A separately protected collector keeps exported records available during recovery.



WAGO controller	The attacker damaged its partition table. Specialist examination could not recover the data.
Router and firewall	The FortiGate reset erased its logs. Teltonika's event database survived because RutOS before 7.07 retained it through factory reset.
Siemens controllers	Recovery factory resets removed local logs. Coordinate restoration and evidence preservation.

The report is not a story of every record being erased. Network records and surviving router events mattered. The design lesson is to avoid making the attacked device the only custodian of the evidence.

COMMISSION THE FAILURE PATH

1. Capture and deliver. Perform an approved interaction and confirm the receiving collector stores the expected record.
2. Interrupt and recover. In the lab, interrupt transport, observe the health condition, restore it, and reconcile buffered records.
3. Remove and retrieve. Take the test sensor offline after receipt. Retrieve the retained evidence and verify that an independent health check detects the missing sensor.
4. Reach a person. Record the alert, acknowledgement, investigation context, and escalation owner.

Set retention, delivery-time targets, outage limits, and response ownership before testing. Local collection supports disconnected operation; external notification still needs an approved path. The combined failure sequence above is a proposed pilot acceptance test.

Sources: CERT Polska follow-up, August 2026.

Commission one useful warning.

A small, well-specified pilot is a practical first step toward a repeatable power-sector detection service.

Design	Choose one access path and one detection question. Record reachable services, routine scanners, approved maintenance, and a named responder.
Qualify	Check the selected persona against the actual client interaction. Verify separation from production outputs, egress policy, resource limits, and removal procedure.
Prove	Run the agreed interaction, transport-failure, retention, and health tests. Capture event and receipt timestamps, evidence fields, and responder acknowledgement.
Operate	Observe routine activity for an agreed period. Tune documented exceptions, review analyst effort, and hand over the operating and escalation instructions.

WHAT THE OWNER TAKES AWAY

An as-built placement map; a permitted-traffic matrix; a profile and version record; the test results and retained evidence; a response runbook; and an expansion decision grounded in observed value.

Let’s build the first detection path together.

Deception Check contributes the decoy, interaction telemetry, and integration support. Your engineering and operations teams define the site constraints and response authority. Start with a focused architecture workshop, then a bounded lab or approved site pilot.

Nick Carroll, Co-Founder & CTO
nick@deceptioncheck.ai | deceptioncheck.ai

EVIDENCE AND READING

Sources: CERT Polska follow-up, August 2026; CISA, Using Cyber Decoys to Strengthen Detection and Response; Deception Check, After the Login.

First-party basis: September 20 S7 five-event extract; August 14-19 retained SSH comparison; September 8 controlled DNP3 reboot check. Records reviewed for this brief are bounded observations and tests. Customer deployment acceptance is performed on the selected build and architecture. Prepared October 3, 2026.