Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/passive-first-ot-asset-discovery/

OT ASSET COVERAGE

Passive First OT Asset Discovery Across Plants

A controller on the list is a controller you can patch, monitor and include in the risk assessment the regulator will ask to see. Build the inventory from what the network actually shows and from what the cabinets actually hold, using passive capture and walkdowns alone. Call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Defend and Patch Every Industrial Controller by Knowing It Exists

Every federal and state critical infrastructure framework, from AWIA water utility mandates and NERC CIP energy standards to Coast Guard maritime cybersecurity directives, begins with the same foundational requirement: maintaining an accurate inventory of all operational technology hardware, firmware versions and network communication paths. Combining sources is what makes that inventory accurate: passive monitoring placed at lower level switches as well as the core picks up controller traffic, walkdowns reach isolated serial links, and current field records capture the years of replacements an older spreadsheet predates.

Combining Passive SPAN Telemetry With Engineering Walkdowns

Global Digital Forensics helps industrial operators and utilities build a unified, plant comparable OT asset inventory with passive methods planned around operations. Our engineers combine deep packet inspection from strategically placed switch SPAN ports and optical taps with physical cabinet walkdowns and engineering project file reviews. We document every PLC, RTU, HMI, safety instrumented system, firmware revision and active communication pair, clearly mapping sensor coverage so leadership knows what is monitored and where the next sensors or walkdowns go.

Reading the Inventory for Coverage, Confidence and Source

An inventory built from passive capture carries a confidence level for every entry, and reading it well means understanding where each entry came from. A device that announces itself through an identity response in EtherNet/IP, S7 or a similar protocol yields vendor, model and often firmware with high confidence. A device seen only by its MAC address and a Modbus conversation yields a vendor guess and a role inference. A device that appears in a PLC project file and has yet to appear on the wire during the capture window is listed as a candidate, and a walkdown is how the examiner confirms it. We record the source and the confidence for each line so that an engineer, an auditor or a regulator reading the workbook knows which entries rest on observation and which on inference.

The coverage map is as important as the entries. Serial links between a controller and a radio or a legacy device are traced by walkdown, since network capture reads what crosses the wire. Devices on VLANs outside the spanned set, on unmanaged switches with no mirror capability or behind a protocol gateway that

© 2026 Global Digital Forensics, Inc. All rights reserved.

speaks for them are reached through added capture points, gateway configuration reviews and walkdowns. Equipment powered down during the capture, such as a seasonal pump or a standby generator controller, is looked for when it runs and when the walkdown reaches its cabinet. Every workbook we deliver includes a coverage map showing which segments were instrumented and for how long, so every reader knows what the capture observed and where the walkdown filled in. That map is also the plan for the next capture cycle, and the OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/) lets an operator record coverage in the same structure from the start.

Readers in different roles use the same workbook differently. The maintenance engineer reads it by location and vendor to plan firmware updates and spare parts. The security lead reads it by zone and protocol to see which devices talk across zone boundaries and which firmware versions carry published advisories. The compliance lead reads it by categorization and owner to populate a CIP or AWIA submission and to show the auditor how each entry was established. Because the confidence and source fields travel with every line, each reader can see how much weight an entry will bear, and the plant can direct its next walkdown at the entries that matter most to the reader with the nearest deadline.

Why Every Regulator Starts With the Inventory

Regulatory frameworks begin with the asset list because every other control is evaluated against it. In the electric sector, NERC CIP-002 requires entities to identify and categorize their bulk electric system cyber systems, and every subsequent CIP standard applies to the systems that identification produces. Categorizing every controller is therefore the first compliance step, ahead of any control review. CIP-010 then requires a baseline configuration for each applicable system, including installed software and firmware, which the inventory makes possible to maintain for every listed device. Community water systems completing risk and resilience assessments under AWIA Section 2013 must assess the risks to their electronic and automated systems, which starts from knowing what those systems are.

The engineering standards say the same thing in different words. NIST SP 800-82 Revision 3 places asset management at the foundation of an OT security program, and the ISA/IEC 62443 zone and conduit model is drawn from the known assets it groups. A passive first inventory therefore does double duty: it is the first deliverable of a security program and the first exhibit in a compliance file. We format the workbook so the same data serves both, with the fields a CIP auditor or an AWIA certifier expects alongside the fields the maintenance team uses, and our water and wastewater and power and energy assessment pages describe the sector specific versions.

The Discovery Engagement in Phases

Planning comes first and determines the quality of everything after it. We review the network drawings and switch inventory with the plant's network and control engineers to identify where SPAN sessions or taps will see the most conduits, confirm that the switches can mirror traffic while keeping their own performance steady and schedule capture windows that cover each operating mode, including startup, normal production, shift change and any scheduled vendor maintenance. Where a site has unmanaged switches or serial segments, we note them now as walkdown targets so coverage is planned from the start. The plan is agreed in writing before any sensor is connected, which is the same discipline we apply to every OT engagement.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Capture and analysis follow. Traffic is parsed for industrial protocols to extract device identities, roles and communication pairs, and the resulting list is reconciled against PLC project files, HMI tag databases, purchase records and the existing spreadsheet, which the reconciliation brings up to date with replaced devices and those installed during emergencies. The walkdown then verifies the reconciled list cabinet by cabinet, photographing labels, recording serial numbers and firmware where displayed and confirming the physical location and the owner of each device. Firmware versions are matched against published vulnerability advisories so the inventory arrives with a first view of exposure. The deliverable is a plant comparable workbook with the coverage map, ready to feed a monitoring platform, a segmentation review or a compliance submission. Maritime operators preparing for a vessel or facility assessment will find the parallel process in our maritime assessment preparation guide.

Handoff is the final phase, and it is what keeps the inventory current. The workbook is delivered with the capture configurations, the parsing rules and the reconciliation notes so that the plant's own staff or a monitoring vendor can repeat the exercise, and we walk the named inventory owner through the structure so that additions, replacements and retirements are recorded the same way we recorded them. Where the plant moves to continuous passive monitoring, the workbook becomes the baseline the platform compares against, and the first alerts are often devices the walkdown confirmed outside the capture window. Where the inventory is feeding a segmentation review or a risk assessment, the coverage map shows that next engagement where to add its own capture points. An inventory handed off this way is built to stay accurate through the year that follows.

Inventory Practices and Who Prepares for the First Call

The first practice is passive collection, which keeps fragile controllers working with only the traffic they were designed to handle. The second is capturing at the lower level segments as well as the core switch and walking down the serial links, so the inventory covers the whole plant. The third is checking the integrator's as built documentation, which describes the plant at commissioning, against the plant as it stands after a decade of field replacements. The fourth is listing safety instrumented systems and protocol gateways alongside everything else, whoever is responsible for them. The fifth is naming the person who will maintain the inventory on the day it is delivered, so it is kept current from then on.

Those practices start with preparation. The control engineer gathers the PLC and HMI project files, the existing asset spreadsheet and the drawings, however dated. The network engineer identifies the switches at each zone boundary and confirms which can mirror traffic. Procurement or maintenance supplies vendor and integrator records that show what was bought and installed. The operations lead identifies the production calendar so capture windows can be set. Corporate security identifies the framework the inventory must serve and any prior audit findings about asset management. With those in hand, the scoping call can place the first sensors within days. The water and wastewater assessment manual in our planning library includes a preparation checklist, and the inventory feeds directly into the segmentation validation that usually follows.

Build Your Utility or Industrial Audit Workbook Today

Use our free interactive OT and utility workbook builder (evestigate.com/tools/ot-workbook-builder/) or call Global Digital Forensics at (800) 868-8189 to initiate a passive OT asset discovery engagement. The initial consultation is free.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Confidence and Source for Every Inventory Entry

The guide treats an OT inventory as a set of entries that each carry a confidence level and a source. This table shows how a device comes to be listed, the confidence that discovery method supports and the step that confirms it, so an engineer, an auditor or a regulator can see how much weight an entry will bear. The confirmation column sets the next walkdown targets, and a device listed in a project file moves from candidate to confirmed asset when it is seen running or found in its cabinet.

How a device enters a passive first inventory, the confidence it carries and the step that confirms it.

How the device was seen	Confidence	What confirms it
Identity response in EtherNet/IP, S7 or similar	High, with vendor, model and often firmware	Matched to a cabinet during the walkdown
MAC address and a Modbus conversation	Medium, a vendor guess and a role inference	Physical inspection of the device
Listed in a PLC project file only	Candidate, awaiting observation on the wire	Found running during a later capture or walkdown
On a VLAN outside the spanned set	Pending instrumentation of that segment	A capture point added for that segment
Behind a protocol gateway	Represented by the gateway that speaks for it	A walkdown or gateway configuration review
Powered down during capture	Pending, looked for when it next runs	Running during the next capture cycle
Serial link to a radio or legacy device	Traced by walkdown rather than capture	An engineering walkdown of the cabinet

Start the Inventory in the OT Audit Workbook Builder

Start your inventory with the OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/) rather than a blank spreadsheet. Choose the sector, add each plant or substation, and let the planning set lay out the asset classes, the communication paths and the sensor coverage boundaries you need to record. Download the workbook set and fill the coverage columns fully, including the serial links and isolated segments that call for a walkdown, so the coverage picture is clear from the first draft. Your entries stay in your browser. When the workbook lists more open entries than confirmed assets, call and the examiner will plan the passive capture and cabinet walkdowns to work through them.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Our OT Security Readiness: Inventory, Boundaries and Rules Before Testing sets out the items to secure in the order they expire. Have ready the number of sites, the drawings and asset spreadsheets as they exist, the PLC and HMI vendors in use, the switch inventory at each zone boundary, the production calendar and the framework or regulator the inventory must serve. Our OT engineer asks where traffic can be mirrored safely, which segments are serial or unmanaged, how many cabinets a walkdown would cover, what operating modes the capture must observe and who will own the inventory after delivery. You then receive a written scope naming the capture points and walkdown locations for the first site, a timing plan that spans the operating modes that matter and a proposal for the discovery, the workbook and the coverage map. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-82 Revision 3.

Authorities cited in this guide: NIST SP 800-82 Revision 3. Places asset management at the foundation of an OT security program and describes the constraints that make passive methods appropriate, in the final Revision 3 text. NERC CIP standards. Supplies the CIP-002 categorization and CIP-010 baseline configuration requirements that depend on a complete inventory, in the currently effective standards listed by NERC. EPA, AWIA Section 2013. Describes the risk and resilience assessment requirement for community water systems whose electronic and automated systems must be inventoried to be assessed, as published on the current EPA page. ISA/IEC 62443 series of standards. Supplies the zone and conduit model that requires a known asset population before zones can be defined, as described on the ISA standards page for the series.

FREQUENTLY ASKED

Passive Discovery on Legacy Controllers

Is passive discovery really safe for old PLCs and RTUs?

Yes. Passive capture mirrors traffic that is already flowing to a sensor port and sends nothing to the devices. The planning care goes into the switch configuration: a mirror session is sized to the capacity of the switch and the sensor, which is why we plan SPAN placement with your network engineer and confirm switch capacity before connecting anything. Where a switch is better left unmirrored, we use a tap or treat that segment as a walkdown target.

How long does an OT asset inventory take?

The drivers are the number of sites and network segments, how long capture must run to observe every operating mode, the number of cabinets to walk down and the state of the existing documentation. Capture often needs to span a full production cycle so that seasonal or intermittent equipment appears. Plants with good project files and recent drawings reconcile quickly. Plants that have been through acquisitions or decades of field changes take longer because more of the inventory is verified physically.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What does passive OT discovery cost?

The initial consultation is free. The proposal reflects the number of sites and segments to instrument, the duration of capture, the number of cabinets and locations for walkdowns, whether firmware vulnerability matching and compliance formatting are included and whether the inventory will be handed to a monitoring platform. Operators that use our workbook builder and planning library to prepare reduce the first phase considerably.

Will the inventory satisfy a NERC CIP or AWIA review?

The workbook is formatted with the fields those frameworks expect, including categorization, location, owner, firmware and configuration baseline information, alongside a coverage map that shows how the data was gathered. Each auditor makes that determination for each submission, so we recommend involving your compliance function in scoping so the fields and evidence match what your region or certifier has asked for in the past. The coverage map is what lets an auditor see the basis for each entry.

What happens to the inventory after you deliver it?

It is yours, in a format your team can maintain, and we name the owner and the update cadence in the report because a named keeper is what keeps an inventory current. Most operators feed it into a passive monitoring platform so changes are detected continuously, use it as the asset basis for a segmentation validation and risk assessment, and refresh the walkdown on a schedule tied to maintenance outages. We can support any of those steps, and the workbook structure is designed so the next capture cycle builds on the first.

Web Addresses for the Sources Cited

1. NERC CIP-002: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
2. AWIA Section 2013: https://www.epa.gov/waterresilience/awia-section-2013
3. NIST SP 800-82 Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final
4. ISA/IEC 62443: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.