exeon

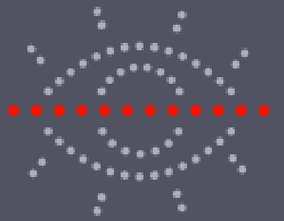
OT SECURITY EVALUATION GUIDE

OT Visibility Without More Operational Overhead

What to look for when extending visibility, validating segmentation, and making existing OT security investments more useful

A practical guide for OT security, SOC, and operational resilience leaders

THE MISSING LAYER IN MANY OT SECURITY ARCHITECTURES



Industrial organizations rarely begin an OT security evaluation with a blank sheet of paper. They already have firewalls, switches, remote-access controls, and monitoring technologies in place. Some operate specialized OT intrusion detection or deep packet inspection tools; many also route selected events into a central SIEM or an external SOC.

Yet basic questions remain surprisingly difficult to answer. Which assets are actually communicating? Which paths connect network zones? Has a temporary maintenance connection quietly become permanent? Can a SOC analyst understand an OT alert without asking an engineer to reconstruct the surrounding activity by hand?

These are not necessarily signs that the existing tools have failed. More often, each tool sees a useful part of the environment while the operational picture remains fragmented across technologies, sites, and teams. Extending OT security therefore does not always mean replacing what is already there. A complementary visibility and analytics layer can connect existing telemetry, expose the gaps between controls, and help security operations use OT information more effectively.

THE RIGHT STARTING POINT

Evaluate the gaps in the current architecture before comparing product feature lists.
The relevant question is not simply which platform sees the most.
It is which approach adds the missing visibility and context with acceptable cost, complexity, and operational risk.

A PRACTICAL EVALUATION SEQUENCE

A useful evaluation follows the way OT security value develops in practice. First, the organization needs to see assets and communications. It can then validate whether intended controls match observed activity. Once that foundation exists, OT information can be operationalized across investigations and workflows. Response remains a joint security and operational decision, supported by a shared and reliable view of what happened.

SEE

Assets, flows and dependencies

VALIDATE

Zones, policies and drift

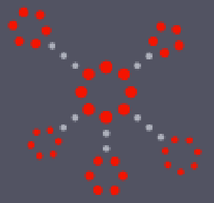
OPERATIONALIZE

Context, correlation and workflows

RESPOND

Joint decisions and evidence

1. DEFINE THE GAP BEFORE EVALUATING THE SOLUTION



An OT environment may contain sophisticated controls and still lack a dependable overview. Asset inventories become outdated, network diagrams reflect intended rather than actual connections, and information from different vendors remains difficult to combine. Distributed plants, substations, and isolated segments magnify the problem because extending the same sensor architecture everywhere may be too costly or disruptive.

Begin by documenting what the current architecture cannot show or support consistently. This keeps the evaluation focused on a real operational need and prevents the addition of another overlapping tool.

Questions to establish the scope

Which sites, segments, assets, or remote connections remain insufficiently visible?

Can teams distinguish required communication from unexpected or obsolete paths?

Does the organization know whether segmentation policies are working outside the audit window?

How much manual coordination is needed to investigate an OT event?

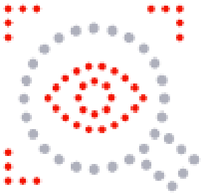
Which environments cannot accept agents, active scanning, additional sensors or cloud processing?

What data is already available from network infrastructure and existing OT security tools?

EVALUATION QUESTION

Can the proposed solution close a defined gap while preserving the investments and processes that already work?

2. SEE: GAIN VISIBILITY WITHOUT DISRUPTING PRODUCTION



Visibility is the foundation of the evaluation, but the method matters as much as the result. In production environments, every new appliance, network change and maintenance window carries operational consequences. A design that promises comprehensive coverage may still deliver little near-term value if procurement and deployment take months.

A passive, metadata-based approach offers a different starting point. Network flows, firewall logs, switch telemetry and data from existing security infrastructure can reveal which assets communicate, how systems depend on one another and where traffic crosses network boundaries. Because the analysis uses data the environment already produces, organizations can often establish useful coverage before committing to additional hardware across every site.

Evaluate the data strategy, not only the dashboard

Ask vendors to show which sources they require, what each source contributes, and where the remaining blind spots are. Useful visibility should include communicating assets, protocols, communication paths, volumes, external connections, and changes over time. It should also surface unmanaged or legacy devices that do not appear in endpoint-based inventories.

Metadata analytics and deep packet inspection answer different questions. Flow and log data can provide broad, scalable behavioral visibility, including where payload inspection is unavailable or undesirable. DPI adds protocol-level detail that may be essential in selected critical segments. A sound architecture combines them deliberately, using existing DPI investments and adding deeper inspection where the use case justifies it, rather than treating either approach as universally sufficient.

What to look for

- Passive collection without agents, active scanning, or traffic injection into production networks.
- Support for existing NetFlow, firewall, switch, network-log, DPI and OT telemetry.
- Discovery of communicating assets and dependencies across distributed and segmented environments.
- Transparent limitations, including where targeted DPI or another data source is still required.
- A path to useful initial visibility that does not depend on a full estate-wide rollout.

EVALUATION QUESTION

How much of the required visibility can we obtain from telemetry we already have, and what must be added to close the remaining gaps?

3. VALIDATE: PROVE THAT SEGMENTATION WORKS IN PRACTICE

Segmentation is central to OT security architecture, from Purdue-model designs to zones and conduits. The difficulty is that a firewall rule describes what is permitted, while a network diagram shows what was intended. Neither proves that current communication follows the design.

Real environments change. A remote-maintenance rule stays enabled after the work is complete. A connection is introduced under production pressure and never documented. A new system communicates across a boundary that nobody expected. Over time, policy and observed activity diverge. Annual or project-based reviews capture a moment; they do not reveal the drift between reviews.

Continuous validation uses observed network activity to make this gap visible. Teams can identify unexpected cross-zone communication, new protocols, undocumented paths and changes that require review. This turns segmentation from a static design exercise into a control that can be checked against everyday reality.

Validation is also a governance capability

OT operations, IT security and compliance view a network change through different lenses. Operations protects uptime and process safety. Security considers policy and attack paths. Compliance needs evidence that controls are monitored and reviewed. A common, time-based view of communication gives these teams a factual basis for deciding whether a change was expected, authorized, and acceptable.

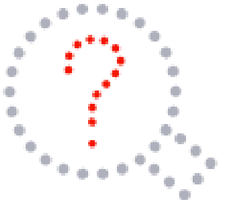
What to look for

- Visibility into actual communication across defined zones and conduits.
- Comparison of observed activity with intended policy or approved communication patterns.
- Detection of new paths, prohibited protocols, and segmentation drift over time.
- Enough history and context to review when a change first appeared and how it developed.
- Findings that OT operations and security teams can assess together.

EVALUATION QUESTION

Can the solution show where our documented segmentation differs from actual network behavior, continuously rather than only during an audit?

4. OPERATIONALIZE: CONNECT OT INSIGHT WITH SECURITY OPERATIONS



Visibility does not become operational simply because more data is available. OT security information is commonly distributed across IDS or DPI tools, firewalls, network infrastructure, remote-access systems, and IT security platforms. During an investigation, teams may have to collect fragments from several owners before they can establish a timeline.

A complementary analytics layer should normalize and correlate those signals, preserving the value of specialist OT tools while adding the network and behavioral context needed to investigate. For example, an IDS alert becomes more useful when an analyst can see the affected asset, its recent communication partners, whether the connection is new, which zone boundary it crossed and what changed before the alert.

This does not remove OT expertise from the process. It reduces the time spent gathering basic facts and helps the SOC ask better questions. The goal is a shared operational picture in which security analysts understand the activity and OT engineers can assess the consequences for production and safety.

Detection quality must be explainable

Behavioral analytics can identify deviations that signatures and known indicators miss, but an unexplained score is difficult to trust in an operational environment. Analysts should be able to see why a detection was generated, which activity contributed to it and how the behavior differs from the established baseline. Clear reasoning improves triage and gives OT specialists something concrete to confirm or challenge.

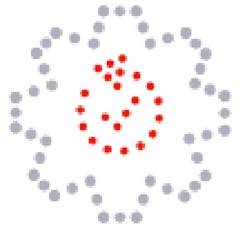
What to look for

- Vendor-independent ingestion, normalization, and enrichment of existing telemetry.
- Correlation of network behavior with alerts from specialist OT security tools.
- Behavioral baselines that reveal new or unusual communication patterns.
- Explainable detections with affected assets, activity, and timelines visible to analysts.
- Integration with the existing SIEM, SOC, MSSP, and incident-management workflow.

EVALUATION QUESTION

Can an analyst move from an OT alert to a credible account of the surrounding activity without manually assembling data from several systems?

5. RESPOND: SUPPORT JOINT DECISIONS WITH A SHARED PICTURE



OT response differs from conventional IT containment. Isolating a device may interrupt a production process, affect safety or create a larger business impact than the suspected incident. The decision to contain is therefore not a security decision alone; it requires operational knowledge and clear authority.

Technology should support this collaboration rather than promise to automate it away. A useful solution gives the SOC and OT operations the same facts, records the sequence of relevant activity, and fits the organization's agreed escalation path. The OT team can assess process dependencies and safe states, while security investigates the threat and proposes containment options.

The same information can support internal documentation, incident review, and the organization's regulatory reporting processes. It may provide evidence of monitored communications, detected changes, and investigation timelines, but it does not by itself create a compliance-ready audit report or make the organization compliant. Governance teams remain responsible for interpreting the evidence, mapping it to obligations, and producing the required submissions.

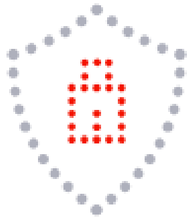
What to look for

- A consistent timeline and shared context for OT, security, and external service providers.
- Role-appropriate access to the information needed for assessment and escalation.
- Integration with established incident and case-management processes.
- Historical information that can support reviews, evidence collection, and reporting workflows.
- Clear boundaries between detection support, operational decision-making and compliance responsibility.

EVALUATION QUESTION

Does the solution strengthen our response process while keeping operational and safety decisions with the people accountable for them?

6. TEST DEPLOYMENT FIT, SOVEREIGNTY AND SCALE



OT architecture is rarely uniform. A central plant may have rich telemetry, while remote sites operate with limited bandwidth, older infrastructure, or strict isolation. The evaluation must therefore test the deployment model against the most difficult parts of the estate, not only the easiest pilot location.

Distributed collectors or gateways can parse, normalize and buffer data close to its source, forwarding only what central analytics requires. This can reduce bandwidth and simplify the connection of remote environments. Where sovereignty or isolation requirements apply, buyers should verify on-premises, self-hosted and air-gapped options, together with how updates, support and data retention work under each model.

Phased deployment is usually more defensible than a big-bang program. Starting with a critical or poorly understood segment allows the organization to test data quality, identify communication dependencies, and refine success criteria before expanding. The pilot should nevertheless demonstrate that the architecture and operating model can scale across sites without multiplying infrastructure and maintenance effort.

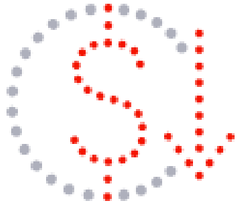
What to look for

- On-premises, self-hosted and air-gapped deployment where required.
- Distributed collection with local parsing, normalization and buffering.
- Control over which data is forwarded, processed, and retained in each location.
- A phased rollout model that minimizes network changes and production risk.
- Transparent requirements for sensors, collectors, bandwidth, compute, storage and administration.

EVALUATION QUESTION

Will this design remain secure, manageable and economically viable when it extends from the pilot to distributed and isolated environments?

7. COMPARE OPERATIONAL VALUE, NOT LICENSE COST ALONE



The true cost of an OT security approach includes more than software. Additional sensors, appliances, storage, integrations, site visits, maintenance windows and specialist administration can dominate the three-year cost. Operational delay also matters: an ambitious design creates little risk reduction while it remains in planning.

A fair comparison should account for how much existing telemetry and infrastructure can be reused, how quickly the first segment produces useful information, and how much effort is required to extend the design. It should also consider whether the solution improves the value of tools already purchased by connecting their output with broader network context and established workflows.

Claims about rapid coverage or cost reduction need a defined basis. Ask what counts as a visible asset or segment, which data sources are assumed, and which parts of the rollout remain outside the estimate. A smaller, measurable pilot provides better evidence than a generic benchmark.

What to measure during the evaluation

- Time from data access to a usable view of assets and communications.
- Previously unknown assets, paths, or segmentation exceptions identified.
- Effort required to investigate a selected OT alert or anomaly.
- New infrastructure, maintenance and specialist skills required for the pilot and rollout.
- Three-year cost, including collection, compute, storage, integration and operations.

EVALUATION QUESTION

Does the approach produce measurable operational value early enough to guide the investments that follow?

RUN AN EVALUATION THAT REFLECTS THE REAL ENVIRONMENT

A useful proof of concept should test an architecture and operating model, not stage a polished demo. Choose a scope that is limited enough to complete but representative enough to expose the real constraints.

01 Select one or two critical segments with known visibility, segmentation, or investigation challenges.

02 Inventory the telemetry, sensors and security platforms already available in that scope.

03 Agree success criteria for asset visibility, communication mapping, segmentation validation and investigation workflow.

04 Document deployment, sovereignty, bandwidth, and operational-change constraints before connecting data.

05 Compare observed assets and communications with inventories, network diagrams, and intended policy.

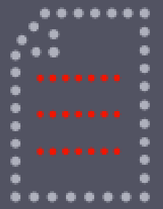
06 Test one segmentation exception and one end-to-end investigation with both OT and security participants.

07 Measure infrastructure, operational effort, and time to useful results, then model the expansion to additional sites.

A good outcome is a better investment decision

The evaluation should show where broad metadata visibility is sufficient, where targeted DPI or another control remains necessary, and how the combined architecture can be expanded without creating a new layer of operational burden.

CONDENSED OT SECURITY EVALUATION CHECKLIST



Use the checklist to compare complementary approaches during vendor discussions and proofs of concept. Record whether each criterion is fully supported, partially supported, unsupported, or still requires validation in your environment.

Architecture and visibility	
Complements existing OT IDS, DPI, firewall, and SIEM investments instead of requiring their replacement.	☐
Uses existing flow, log, network and OT telemetry through vendor-independent integrations.	☐
Monitors passively, without agents, active scanning, packet decryption or traffic injection.	☐
Identifies communicating assets, dependencies, remote paths and cross-zone activity.	☐
Explains where metadata is sufficient and where targeted DPI or another source is required.	☐

CONDENSED OT SECURITY EVALUATION CHECKLIST

Segmentation and operations	
Compares observed communication with intended zones, conduits or approved patterns.	☐
Detects new paths, prohibited protocols, and segmentation drift over time.	☐
Correlates network behavior with alerts and context from existing OT tools.	☐
Provides explainable detections and investigation timelines that OT and SOC teams can use together.	☐
Integrates with existing SIEM, SOC, MSSP, and incident workflows.	☐

Deployment and long-term value	
Supports on-premises, self-hosted, and air-gapped environments where required.	☐
Enables distributed collection, local buffering and control over forwarded data.	☐
Allows a phased rollout without extensive network changes or additional sensors at every site.	☐
Provides historical information that can support internal evidence and regulatory reporting processes.	☐
Makes infrastructure, operating effort, and three-year cost transparent.	☐

FIVE QUESTIONS TO ASK EVERY VENDOR

01 What does your solution add to our existing architecture, and which tools or controls does it still depend on?

02 How much useful visibility can we obtain from telemetry we already have?

03 Can you show where our documented segmentation differs from actual communication?

04 Can our SOC investigate an OT event without manually reconstructing the context across multiple systems?

05 What infrastructure and operating effort will be required to extend the approach across all relevant sites?

NEXT STEP: AN OT ARCHITECTURE ASSESSMENT

Map the current data sources, visibility gaps, and deployment constraints before selecting a pilot. The result should be a practical target architecture that uses existing investments where they add value and introduces new collection only where the evidence shows it is needed.

exeon

exeon.com