DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

2026 FIELD GUIDE

Inside OT, ICS & IoT VAPT

What CISOs Need to Test, Scope, and Defend

2026 FIELD GUIDE

Table of Contents

A CISO's guide to scoping, testing and defending operational technology — from the connected industrial environment to a practical readiness model.

One field guide for the OT / ICS / IoT security decision

EXECUTIVE PERSPECTIVE

The OT Attack Surface No Longer Ends At The Plant Floor

Operational technology has become part of a much broader digital ecosystem. Enterprise IT, engineering workstations, remote maintenance platforms, vendors, cloud services, and connected devices increasingly interact with the systems that monitor and control physical processes.

That connectivity brings efficiency. It also creates pathways an attacker can use to move closer to the operation. For a CISO, the VAPT question is therefore changing. It is no longer enough to ask: What can be compromised?

> **The question is how far a compromise can travel before it reaches something that matters physically.**

That is where OT VAPT begins.
Scope the environment, understand the path, and test the consequences.

THE EVOLUTION OF THE INDUSTRIAL ENVIRONMENT

From Isolated Control Systems to Connected Operations

Industrial control environments were historically designed around a simple priority: keep the process running. Systems often operated within tightly controlled environments with limited external connectivity. Controllers communicated with supervisory systems, operators worked from dedicated stations, and many industrial networks remained physically or logically separated from enterprise infrastructure. That model gave industrial operators a degree of isolation. Connectivity has steadily changed it.

Modern facilities increasingly connect operational environments with enterprise IT, engineering systems, remote maintenance platforms, cloud services, analytics, vendor infrastructure, and connected devices. These connections support remote operations, centralized visibility, predictive maintenance, production optimization, and data-driven decision-making. They also create relationships that did not exist in the original control architecture.

THE NEW PERIMETER

The modern industrial security boundary can extend across:

Plant Networks → **Enterprise IT** → **Engineering Workstations** → **Remote Access** → **Third Parties** → **IoT / IoT Infrastructure** → **Cloud Services**

The result is a broader attack surface with more dependencies and more opportunities for unintended trust. For VAPT, that means the perimeter cannot be defined by an IP range alone. It has to be understood as a connected system of assets, access paths, and trust relationships.

WHAT CHANGED FOR THE CISO?

The result is the CISO has expanded from protecting individual systems to understanding how the systems interact. A secure PLC can still sit behind an insecure remote access pathway. A well-configured OT network can still depend on a compromised enterprise identity. A protected production environment can still inherit risk from a third-party connection.

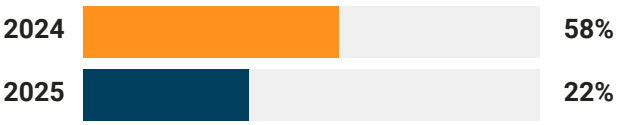
THE EVOLUTION OF THE INDUSTRIAL ENVIRONMENT

Five Numbers That Matter to the CISO

The industrial security conversation often focuses on vulnerable controllers, legacy devices, and patching constraints. The bigger picture sits one level above the device. Where an incident begins, how an attacker enters, how vulnerabilities are distributed, and how industrial environments connect to external systems all influence what a CISO should put inside the testing scope. Five numbers from the 2025-2026 landscape illustrate that shift.

02

ICS VULNERABILITIES RECEIVING A PUBLISHED CISA ADVISORY



Coverage declined sharply, reinforcing the need for broader vulnerability intelligence.

Source: Sapiorid 2026 field-report source set

03

2025 ICS CVE SEVERITY

Medium-severity disclosures exceeded high-severity disclosures in 2025.

Source: Sapiorid 2026 field-report source set

01

96%

OF OT SECURITY INCIDENTS TRACE BACK TO AN IT LEVEL COMPROMISE

The starting point for many OT incidents sits outside the control environment itself. Enterprise infrastructure, identities, endpoints, and connected systems can become the first stage of an attack before an adversary reaches operational technology.

What it changes:
An OT VAPT scope that stops at the OT network can miss the path that leads there.

04

26

OF OT-DEDICATED THREAT GROUPS TRACKED BY DRAGOS

Dragos tracks 26 threat groups dedicated to OT environments, including three groups that emerged in 2025. The growing specialization of threat activity reinforces the need to evaluate industrial environments as operational targets, not simply extensions of enterprise IT.

What it changes:
VAPT should test realistic pathways and defensive controls against the possibility of an attacker who understands the industrial environment.

05

50%

OF ICS / OT INCIDENTS IN 2025 BEGIN WITH UNAUTHORIZED EXTERNAL ACCESS

Third-party remote maintenance represents a particularly important pathway into industrial environments. Remote support infrastructures, vendor accounts, VPNs, and older externally accessible services can create trusted routes toward sensitive systems.

What it changes:
Third-party remote access belongs in the attack surface map and should receive explicit testing attention.

THE EVOLUTION OF THE INDUSTRIAL ENVIRONMENT

IT, ICS, and IoT: The Critical Differences

OT, ICS, and IoT increasingly operate alongside one another. That convergence can make the three terms sound interchangeable, but their roles are different, and those differences matter when a security team decides what to test.

- **Operational Technology (OT)** is the broadest category. It covers hardware and software used to monitor or control physical processes, including industrial control and safety systems.
- **Industrial Control Systems (ICS)** form a subset of OT. They include technologies such as SCADA, distributed control systems, programmable logic controllers, remote terminal units, and human-machine interfaces.
- **Internet of Things (IoT)** refers to connected devices that collect, process, or transmit data. In industrial environments, IoT can connect sensors, gateways, and edge systems with operational networks, enterprise platforms, and cloud services.

The distinction matters because a compromise can produce very different consequences depending on what the technology does, what it connects to, and how close it sits to the physical process.

WHY THE DISTINCTION MATTERS

OT	ICS	IOT / IOT
Purpose Monitor and control physical operations. **Typical risk** Safety, availability, process integrity. **Testing priority** Consequence-aware assessment.	**Purpose** Execute and supervise industrial control. **Typical risk** Loss of control, process disruption. **Testing priority** Controlled system and protocol testing.	**Purpose** Sense, transmit, and exchange data. **Typical risk** Unauthorized access, data integrity, lateral movement. **Testing priority** Device, firmware, API, network, and connectivity assessment.

OT IS NOW A CISO-LEVEL CONCERN

Fortinet's 2025 global OT security survey found that:

Organizations with CISO or CSG responsibility for OT security

+36
percentage points since 2022

OT security ownership has moved sharply toward executive responsibility.
Source: Fortinet, 2025 State of Operational Technology and Cybersecurity Report | Global survey of 550+ OT professionals

THE EVOLUTION OF THE INDUSTRIAL ENVIRONMENT

The Connection Between Plant Floor and Enterprise

The systems closest to the process are not always the systems closest to the attacker.

The industrial environment has become a chain of connected technologies. At one end are field devices that measure and influence the physical process. At the other are enterprise systems, cloud platforms, vendors, and remote users that may never enter the plant but can still interact with systems inside it.

Between those points sits a layered operational environment: controllers, supervisory systems, engineering workstations, historians, application servers, gateways, and network boundaries. Each layer performs a different role. Each connection creates a different security consideration.

For the CISO, the important question is not where the plant ends. It is where trust begins and where it can travel.

> The distinction matters because a compromise can produce very different consequences depending on what the technology does, what it connects to, and how close it sits to the physical process.

OT IS NOW A CISO-LEVEL CONCERN

Before testing begins, the environment should be understood through more than IP addresses:

Assets	Connections	Trust	Privileges	Boundaries	Consequence
What exists?	What communicates with what?	Which systems, identities, or vendors are trusted?	What can they do?	Where does access change from one zone to another?	What happens when a compromised system moves deeper into the environment?

THE REALITY OF OPERATIONAL CYBER RISK

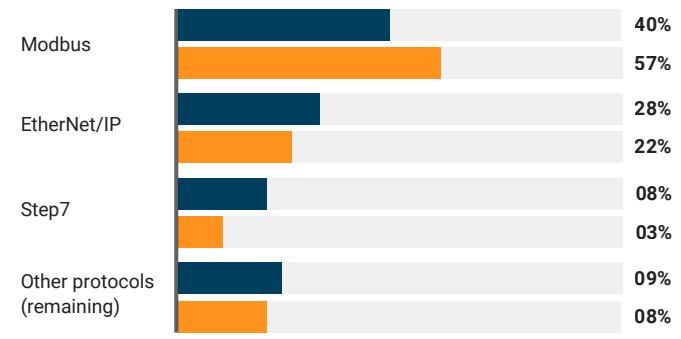
The Communications Behind the Industrial Process

Every industrial environment depends on communication between field devices, controllers, supervisory systems, engineering workstations, gateways, and applications. Those communications determine how systems report conditions, exchange control information, and, in some cases, issue commands.

For VAPT, that makes the communication layer more than a technical detail. The protocols present in an environment influence what can be observed, what can be controlled, where trust exists, and how safely a tester can interact with the system.

The first question is therefore simple: What protocols are actually running in the environment?

OT-PROTOCOL ATTACK ACTIVITY 2024 → 2025



+84%

overall increase in attacks using OT protocols in 2025.

BACnet accounted for 8% of observed OT-protocol attacks in 2025 and was the third-most targeted protocol.

odbus remained the dominant target, while attackers continued to concentrate on widely deployed industrial protocols.

THE PROTOCOLS A TESTER SHOULD RECOGNIZE

MODBUS
Widely used in industrial automation and PLC environments.
VAPT focus: command exposure and segmentation.

DNP3
Common in utilities and distributed infrastructure.
VAPT focus: authentication, command authorization, and remote communications.

BACnet
Used in building automation and can connect HVAC, energy management, and other building systems.
VAPT focus: device exposure and unauthorized control.

PROFINET
Supports real-time industrial communications.
VAPT focus: map communication relationships and control the rate and type of active testing.

OPC UA
Provides defined security capabilities and is widely used to connect industrial systems and applications.
VAPT focus: certificates, authentication, encryption and trusted connections.

MQTT
Common in IoT and IIoT deployments, where brokers distribute messages among devices and applications.
VAPT focus: broker exposure, authentication, topic permissions, encryption and device identity.

CoAP
Designed for constrained connected devices and commonly operates over UDP.
VAPT focus: exposed endpoints, device authentication, transport protection and gateway relationships.

WHAT PROTOCOL KNOWLEDGE CHANGES

What command exists	Where authentication occurs	Where encryption is available	Which system can communicate	What active testing environment can handle

That makes protocol identification an early scoping activity, not something discovered halfway through the engagement.

THE REALITY OF OPERATIONAL CYBER RISK

The Expanding OT Attack Surface

The attack surface of an industrial environment is no longer a list of controllers. It is the full set of ways an adversary can reach, influence, or observe the systems that run the process. Every new connection built for efficiency — remote support, cloud analytics, a vendor tunnel — adds another way in.

For scoping, the useful question is not “how many devices do we have?” but “how many paths lead to the ones that matter?” The surfaces below rarely appear on a single asset inventory, yet each is a recurring entry point in real incidents.

WHERE THE SURFACE ACTUALLY EXPANDS

Remote access
VPNs, RDP and vendor tunnels that reach operational zones from outside the plant.

Third-party & vendor
Integrator and OEM accounts with standing access and shared credentials.

Cloud & IIoT telemetry
Gateways and brokers pushing operational data to external platforms.

Engineering workstations
Programming software and project files that can rewrite controller logic.

Wireless & field networks
Industrial Wi-Fi, cellular gateways and radio links at the edge.

Firmware & supply chain
Unsigned firmware, embedded components and update mechanisms.

50%

OF ICS / OT INCIDENTS IN 2025 BEGAN WITH UNAUTHORIZED EXTERNAL ACCESS
Remote and third-party pathways are now the leading route into operational networks — not the field devices themselves.

CISO FIELD NOTE

Map the paths, not just the devices. A useful OT scope traces remote, vendor, cloud, engineering, wireless and supply-chain connections to the operational zones they can reach. Prioritise the paths that cross trust boundaries toward process-critical assets.

THE REALITY OF OPERATIONAL CYBER RISK

The Limits of Conventional IT VAPT

Conventional IT penetration testing is built for resilient, redundant systems where a crashed service can be restarted and confidentiality is the primary concern. Operational technology inverts those assumptions. Availability and safety come first, many devices are fragile by design, and a single malformed packet can halt a process.

The techniques that make IT testing effective — aggressive scanning, exploitation, credential brute-forcing — are precisely the ones that can cause harm in an OT environment. The method has to change before the scope does.

IT VAPT VS OT VAPT — WHAT ACTUALLY DIFFERS

Dimension	Conventional IT VAPT	OT / ICS VAPT
Priority order	Confidentiality → Integrity → Availability	Safety → Availability → Integrity → Confidentiality
Primary risk	Data breach, account takeover	Process disruption, physical consequence, safety
Techniques	Active scanning, exploitation, brute force, DoS testing	Passive discovery, controlled and consequence-aware testing
Disruption tolerance	High — systems restart and scale	Very low — downtime and trips carry real cost
Patch cadence	Frequent, routine maintenance windows	Rare, tightly scheduled, often vendor-gated
Measure of success	Systems compromised	Consequences proven without causing them

CISO FIELD NOTE

OT VAPT changes the definition of a successful test. The objective is to validate exposure and demonstrate realistic attack paths while preserving safety and availability. Test intensity should follow the consequence of failure, not the capabilities of the tool.

THE REALITY OF OPERATIONAL CYBER RISK

Scanning Within Operational Environments

Discovery is the foundation of any assessment, but in operational environments the act of looking can itself be disruptive. Legacy controllers may exhaust their limited resources responding to a scan, mishandle unexpected packets, or fault when probed with traffic they were never designed to receive.

Passive first

Observe traffic without transmitting to devices. Safe for production and often the richest source of truth.

- SPAN / mirror-port capture and network taps
- Protocol and asset identification from live flows
- Communication mapping — who talks to whom
- Baseline of normal operational behaviour

Active with caution

Only where justified, rate-limited, and agreed — never as a default across the plant.

- Targeted, single-host queries — not broad sweeps
- Strict rate control and timing windows
- Engineering staff present, rollback ready
- Excluded: safety systems and fragile legacy devices

A SAFE-SCANNING LADDER

Passive capture **Preferred** → Vendor / config review → Targeted active query **(agreed)** → Broad active scan **Lab only**

SAFE DISCOVERY PRINCIPLE

Begin with passive visibility wherever possible: mirrored traffic, network taps, configuration review and communication baselines can reveal assets and relationships without touching fragile devices. Move to targeted active queries only when the target, timing and rollback plan are agreed.

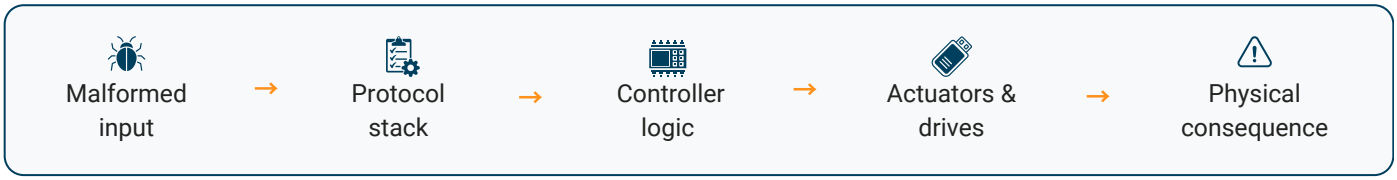
THE REALITY OF OPERATIONAL CYBER RISK

Fuzzing and the Potential for Physical

Fuzzing — sending malformed or unexpected input to find flaws — is a powerful way to uncover protocol and firmware weaknesses. In OT it is also one of the most consequential techniques available, because the software under test sits directly above equipment that moves, heats, pressurises, or energises the physical world.

A crash in an IT service is an outage. A crash in a controller can be a stopped line, a tripped safety function, or an uncontrolled physical state. The risk is not theoretical; it follows the signal path.

HOW A MALFORMED INPUT REACHES THE PHYSICAL WORLD



Where fuzzing belongs

- Offline test benches and lab replicas
- Spare or decommissioned identical hardware
- Digital twins and vendor test rigs
- Pre-deployment acceptance testing

Where it does not

- Live production controllers
- Anything interlocked with a safety function
- Single points of failure with no redundancy
- Environments without rollback or engineering cover

LAB-FIRST VALIDATION

Fuzzing is most valuable when it can be separated from production risk. Use representative hardware, replicas, digital twins or vendor test rigs to explore malformed inputs, then carry validated lessons back into the live assessment as controlled, evidence-based findings.

THE REALITY OF OPERATIONAL CYBER RISK

Safety, Availability, and the Limits of Testing

Every industrial assessment operates inside a boundary that IT testing rarely encounters: the obligation to preserve safety and availability while the process is live. That boundary is not a limitation on rigour — it is the definition of doing the work correctly.

The most important system in many plants is the one a tester must treat with the greatest care. Safety instrumented systems (SIS) exist to bring a process to a safe state; interfering with them can remove the last line of defence against physical harm.

THE TESTING CONTRACT

A live-environment assessment must never:

- Interrupt or degrade a running physical process
- Alter, bypass, or test a safety instrumented function
- Modify controller logic or setpoints without authorisation
- Introduce traffic a device cannot safely handle
- Continue after an abort condition is reached

THE PRIORITY THAT GOVERNS SCOPE

1 Safety

No action may increase risk to people or the process.

2 Availability

Production continuity is protected throughout.

3 Integrity

Control and data remain trustworthy and unaltered.

4 Confidentiality

Sensitive information is protected, but never first.

> The goal of OT VAPT is to prove what an attacker could do — without doing it. Risk is demonstrated, not triggered.

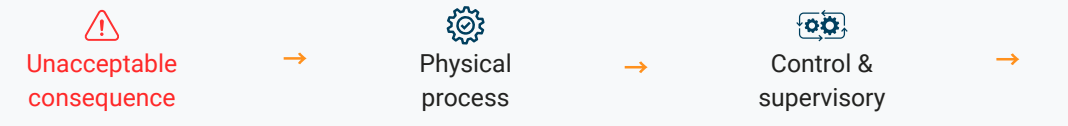
THE OPERATING BOUNDARY

THE FRAMEWORK FOR INDUSTRIAL SECURITY TESTING

Consequence-Based Testing Scopes

A scope defined by IP ranges answers the wrong question. It tells you what exists, not what matters. Consequence-based scoping starts at the other end — with the physical and business outcomes the organisation cannot accept — and works backward to the systems and access paths that could cause them.

WORK BACKWARD FROM THE OUTCOME



Scope becomes the set of systems and pathways on the route to a consequence that matters.

WORK BACKWARD FROM THE OUTCOME

Tier	Example outcome	Testing focus
Critical	Safety event, environmental release, loss of life	Consequence-aware, passive-first, SIS excluded from active tests
High	Unplanned shutdown, equipment damage, major outage	Attack-path analysis to critical control; controlled validation
Moderate	Quality loss, degraded throughput, data integrity	Configuration, segmentation and access-control review
Low	Localised, recoverable, no process impact	Standard hardening and monitoring checks

SCOPING PRINCIPLE

Consequence-based scoping keeps attention on what the organisation cannot afford to lose. Start with the unacceptable outcome, trace the control and supervisory systems behind it, then identify the access paths an adversary would need to reach them.

THE FRAMEWORK FOR INDUSTRIAL SECURITY TESTING

Industrial Architecture and Testing Boundaries

Testing boundaries follow architecture. The Purdue model — and the zones-and-conduits approach of IEC 62443 — give a shared language for where systems sit, how they should be separated, and how much testing pressure each level can safely absorb.

TESTING POSTURE BY ARCHITECTURAL LEVEL

5	**Enterprise (IT)** ERP, business systems, corporate network	Full IT VAPT
4	**Site business / DMZ** Historians, patch & remote-access services	Active, controlled
3	**Operations & supervisory** SCADA, HMIs, engineering workstations	Careful active
2	**Control** PLCs, RTUs, DCS controllers	Passive-first
1	**Field devices** Sensors, actuators, drives, valves	Passive only
0	**Physical process** The process itself	Off-limits

ARCHITECTURE DRIVES TESTING

Testing pressure should decrease as systems move closer to the physical process. Enterprise and DMZ layers may support controlled active testing, while controllers and field devices generally require passive-first or passive-only approaches. The architecture sets the boundary for safe validation.

THE FRAMEWORK FOR INDUSTRIAL SECURITY TESTING

Critical Assets and Protected Systems

Not every asset can be treated the same way. Some are the target of the assessment; others are so critical, or so fragile, that they are protected — observed and reasoned about, but never actively tested. Deciding which is which is a core scoping activity, agreed before any tool is run.

ASSET CLASSIFICATION AND TEST POSTURE

Asset	Role	Posture
Safety instrumented system (SIS)	Brings the process to a safe state	**Excluded**
Process-critical PLC / DCS	Directly controls hazardous or high-value process	**Passive**
HMI / operator stations	Human control and visibility of the process	**Careful active**
Engineering workstation	Programs controllers; can rewrite logic	**Active, controlled**
Historian / data server	Bridges OT and enterprise data	**Active, controlled**
Jump host / remote gateway	Entry point from outside the OT zone	**Full test**
OT domain controller / identity	Authenticates access across the environment	**Full test**

PROTECT THE CROWN JEWELS

Critical assets should be explicitly classified before any tool is run. Exclusion does not mean ignoring them: protected systems still belong in architecture review, attack-path analysis and consequence reasoning. The goal is to understand how they could be reached without placing them under unnecessary test pressure.

THE FRAMEWORK FOR INDUSTRIAL SECURITY TESTING

Rules of Engagement in a Live Environment

In a live industrial environment, the rules of engagement are as important as the testing itself. They convert intent into a controlled, reversible, well-communicated activity — and they give everyone a shared understanding of what happens when something looks wrong.

RULES OF ENGAGEMENT ESSENTIALS

- **Written authorisation** and a defined scope, in and out
- **Named contacts** and a live communications channel
- **Testing windows** agreed with operations
- **Approved techniques** — and explicitly excluded ones
- **Abort criteria** and a shared stop condition
- **On-site engineering** presence and rollback plan
- **Evidence handling** and data protection rules

THE ABORT PATH

Anomaly observed

↓

Pause activity immediately

↓

Notify operations & test lead

↓

Verify safe state & roll back

↓

Record, review, resume only on approval

MAKE THE ABORT PATH REAL

Rules of engagement are effective only when everyone knows what happens after an anomaly. Define named contacts, stop conditions, testing windows, engineering coverage, rollback steps and evidence-handling rules in advance. A clear abort path turns uncertainty into a controlled response.

THE FRAMEWORK FOR INDUSTRIAL SECURITY TESTING

Testing Approaches for Industrial Systems

There is no single way to test an industrial environment. The right approach depends on criticality, redundancy, and how much the organisation already understands about its own architecture. Most programmes combine several, moving from low-risk methods toward higher-fidelity ones as confidence grows.

THE APPROACH SPECTRUM — LOWER TO HIGHER FIDELITY

Passive assessment → Architecture & config review → Controlled active testing → Lab / replica testing → Red / purple team

Lowest process risk — **Highest fidelity — most control required**

MATCHING APPROACH TO ENVIRONMENT

Approach	What it delivers	Best when
Passive assessment	Asset & comms visibility with no device impact	Always — the safe baseline
Architecture review	Segmentation, trust and boundary weaknesses	Early maturity, live plants
Controlled active	Validated exposure on agreed, non-critical targets	Redundancy & windows exist
Lab / replica	Deep exploitation & fuzzing, safely	Critical or fragile systems
Red / purple team	End-to-end attack paths & detection testing	Mature programmes

MATCH FIDELITY TO MATURITY

A mature OT testing programme does not start with the most aggressive technique. It builds confidence from passive assessment and architecture review toward controlled validation, lab testing and eventually red or purple team activity. Higher fidelity requires stronger safeguards and clearer operational readiness.

THE ANATOMY OF AN INDUSTRIAL ATTACK PATH

The Components of a Complete OT VAPT Assessment

A complete OT assessment is a sequence, not a single test. Each phase builds the context the next one needs — and the early phases are what make later, higher-risk activity safe and meaningful.

THE SEVEN PHASES OF AN OT VAPT ENGAGEMENT

1 **Scoping & consequence definition**
Agree crown-jewel outcomes, boundaries and rules of engagement.

2 **Asset & architecture discovery**
Passive mapping of assets, protocols and communication paths.

3 **Threat modelling**
Identify realistic adversaries, entry points and attack paths.

4 **Vulnerability assessment**
Correlate exposures across devices, services and configuration.

5 **Controlled validation**
Prove exploitability on agreed targets — safely and reversibly.

6 **Attack-path analysis**
Chain findings into end-to-end routes toward consequence.

7 **Reporting & remediation**
Prioritised, consequence-ranked findings and a defensive roadmap.

Typical deliverables

- Asset & communication map
- Attack-path and risk narrative
- Consequence-ranked findings
- Prioritised remediation roadmap

ASSESSMENT AS A SEQUENCE

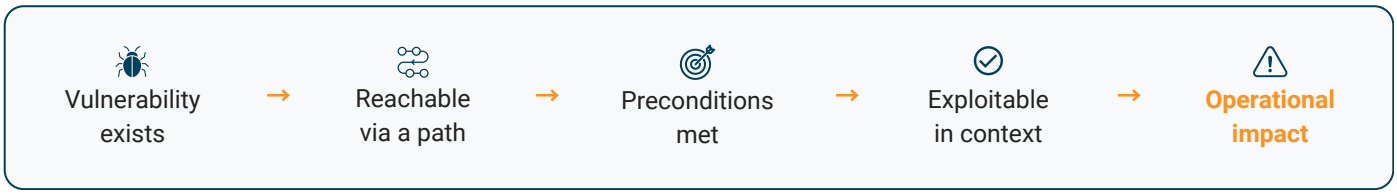
Each VAPT phase creates the context required by the next. Scoping defines the consequence, discovery reveals the environment, threat modelling identifies plausible routes, and validation proves only what can be tested safely. Reporting then converts those results into consequence-ranked decisions and remediation priorities.

THE ANATOMY OF AN INDUSTRIAL ATTACK PATH

The Components of a Complete OT VAPT Assessment

A vulnerability is a possibility; an attack path is a route. Not every weakness can be reached, and not every reachable weakness leads anywhere that matters. The work of OT VAPT is to separate the exposures that are truly exploitable — in this environment, along a real path — from the long list that is not.

FROM EXPOSURE TO IMPACT — THE PRECONDITION CHAIN



MAPPED TO MITRE ATT&CK FOR ICS

Attack paths are described using a shared adversary language — from first access to physical effect:

Initial Access → **Execution** → **Persistence** → **Discovery**
↓
Lateral Movement → **Inhibit Response** → **Impair Process Control** → **Impact**

FROM CVE TO ATTACK PATH

A vulnerability becomes operationally meaningful when it is reachable, its preconditions can be met, and exploitation can produce an effect that matters. Attack-path analysis therefore adds the missing context between a device-level weakness and a consequence at the process or business level.

THE ANATOMY OF AN INDUSTRIAL ATTACK PATH

Identity, Remote Access, and Third-Party Trust

In connected industrial environments, identity has become the perimeter. Most modern intrusions do not begin by breaking a protocol — they begin by using legitimate access: a vendor account, a remote-support tunnel, a shared credential, a jump host that trusts too much.

A TRUSTED PATH INTO OT

HOW ACCESS TRAVELS INWARD

Third-party / vendor

↓

Remote access / VPN

↓

Jump host / OT DMZ

↓

Operational systems

CONTROLS TO TEST

- **MFA** on every path into OT, without exception
- **Named, individual** accounts — no shared logins
- **Just-in-time vendor** access, disabled by default
- **Brokered remote** access through a controlled gateway
- **Least privilege and network** segmentation at the jump host
- **Full session logging** and revocation on demand

#1

REMOTE & THIRD-PARTY ACCESS IS THE LEADING INITIAL-ACCESS VECTOR INTO OT

Standing vendor accounts and externally reachable remote services repeatedly appear at the start of industrial intrusions. Identity and access belong in the testing scope explicitly — not as an afterthought.

IDENTITY IS PART OF THE OT PERIMETER

Remote access controls should be assessed as an end-to-end path: vendor or third party, VPN or remote service, jump host or OT DMZ, and finally the operational system. MFA, individual accounts, just-in-time access, least privilege, logging and revocation all determine how far trust can travel.

THE ANATOMY OF AN INDUSTRIAL ATTACK PATH

Recent Incidents and Their OT Security Lessons

The clearest case for OT VAPT is written in the record of real incidents. Each one exposed a different assumption — about isolation, about safety systems, about trusted access — and each maps to something an assessment can find in advance.

2010 — Stuxnet	**Air-gaps are not absolute** Malware crossed an isolated network via removable media and altered controller logic — proving physical isolation is a control, not a guarantee.
2015–16 — Ukraine grid	**IT compromise, OT impact** Attackers entered through enterprise systems and remote access, then operated HMIs to cut power — the path ran IT → OT.
2017 — TRITON / TRISIS	**Safety systems are targets** Malware reached a safety instrumented system directly — the first known attack aimed at the last line of physical defence.
2021 — Colonial Pipeline	**IT outage stops OT** An enterprise ransomware event halted operations for safety and billing reasons — OT need not be touched to be shut down.
2021 — Water utility (FL)	**Remote HMI, real setpoint** An operator interface was reached over remote access and a chemical setpoint changed — exposed remote control of a live process.
2023–24 — Pre-positioning	**Access held, not used** State-linked activity quietly established persistence in critical-infrastructure networks — access itself is the objective.

INCIDENTS TURN ASSUMPTIONS INTO TESTS

The incidents highlighted here point to recurring assessment questions: Can removable media bypass isolation? Can an enterprise compromise reach OT? Can safety systems be reached? Can an IT outage stop operations? Can remote access change a live process? Each question can become a concrete scoping or control-validation check.

THE ANATOMY OF AN INDUSTRIAL ATTACK PATH

The Gaps Beyond the Vulnerability List

A vulnerability list is a useful artefact and an incomplete picture. It catalogues known weaknesses in individual devices, but the risks that matter most in OT often live in the spaces between systems — in architecture, trust, visibility, and the ability to respond.

WHAT A CVE LIST DOES NOT SHOW

Architecture & trust
Flat networks and implicit trust that let a single foothold spread.

Detection & monitoring
Little or no visibility of OT traffic, so intrusions go unseen.

Response & recovery
Untested playbooks and unclear ownership when OT is affected.

Third-party exposure
Vendor access and dependencies outside the asset inventory.

Safety interplay
How a security event could interact with safety functions.

People & process
Change control, credentials and operational practice.

A vulnerability list says
"These devices have these known weaknesses."

A risk model says
"Here is how an attacker reaches something that matters — and what stops them."

LOOK BETWEEN THE ASSETS

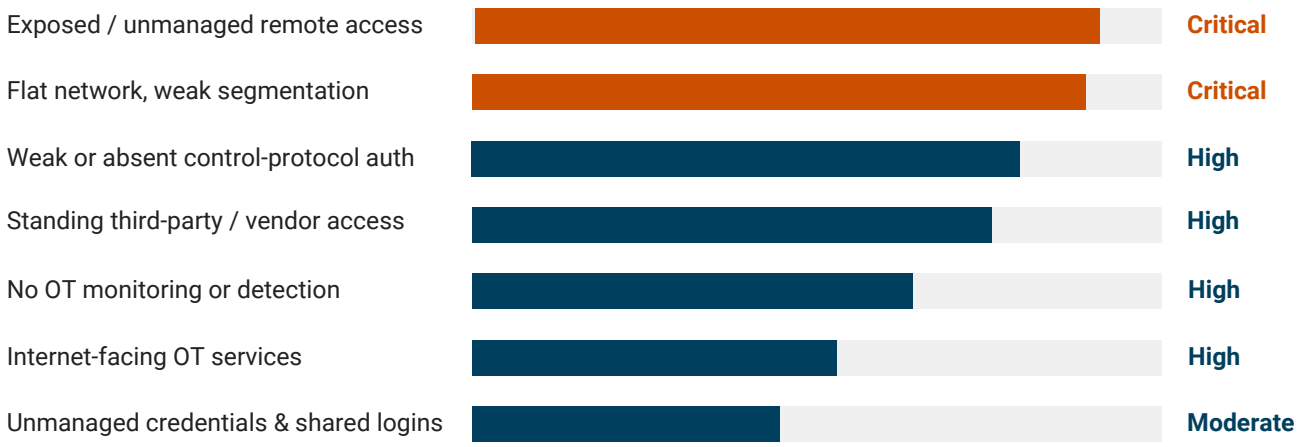
A vulnerability list describes weaknesses on individual devices, but operational risk often sits between them. Architecture, trust, monitoring, recovery, third-party access, safety interplay and people/process controls determine whether a weakness becomes an attack path — and whether the organisation can stop it.

THE PATH FROM EXPOSURE TO RESILIENCE

Findings With the Greatest Operational Impact

Across industrial assessments, the same findings recur — and a small number account for most of the real operational risk. Ranking them by consequence, not by raw count, is what turns a report into a decision the CISO can act on.

RECURRING FINDINGS BY OPERATIONAL IMPACT



Bar length reflects typical operational impact when the finding is present, based on recurring assessment patterns.

RANK BY CONSEQUENCE

The highest-value findings are not necessarily the ones with the largest CVE count. Exposed remote access, flat networks, weak control-protocol authentication, standing vendor access, missing OT monitoring and internet-facing services should be prioritised according to the operational consequence they enable.

THE PATH FROM EXPOSURE TO RESILIENCE

Patching, Exposure, and Operational Continuity

In IT, patching is routine. In OT it is a scheduled, vendor-gated event that may require certification, a shutdown window, and acceptance testing — and some systems cannot be patched at all. Exposure therefore has to be managed, not simply eliminated.

WHEN YOU CANNOT PATCH IMMEDIATELY

The decision path

Can it be patched in a window?

↓ *if not*

Isolate & segment the asset

↓

Restrict & broker all access

↓

Monitor closely for abuse

Compensating controls

- **Virtual patching** at the network layer
- **Zone isolation** and strict conduit rules
- **Application allow-listing** on workstations
- **Least-privilege** and brokered remote access
- **Enhanced monitoring** around the exposed asset
- **Risk-based windows** for eventual patching

WHEN PATCHING MUST WAIT

Unpatched OT exposure needs a compensating-control strategy. Segment the asset, restrict and broker access, monitor for abuse, and use network or application controls where appropriate. Keep a risk-based path toward eventual patching so temporary controls do not quietly become permanent exposure.

THE PATH FROM EXPOSURE TO RESILIENCE

VAPT Findings and Defensive Action

A report only creates value when it becomes a plan. The strongest OT assessments translate findings into sequenced, defensible action — quick containment first, structural change next — and map each step to a recognised framework so progress can be measured.

WHEN YOU CANNOT PATCH IMMEDIATELY

0–30 days

- Close exposed remote access
- Enforce MFA on all OT entry
- Disable dormant vendor accounts
- Isolate internet-facing OT services

30–90 days

- Segment critical zones
- Broker & log remote access
- Deploy OT network monitoring
- Harden engineering workstations

90–180+ days

- Mature detection & response for OT
- Formalise IR & recovery playbooks
- Align to IEC 62443 zones
- Establish continuous assessment

FINDINGS MAP TO CONTROLS AND FRAMEWORKS

Finding theme	Defensive control	Framework anchor
Exposed remote access	Brokered access, MFA, just-in-time vendor accounts	IEC 62443 / NIST 800-82
Flat network	Zones & conduits, OT DMZ, segmentation	IEC 62443-3-3
No monitoring	Passive OT detection, logging, baselining	NIST CSF — Detect
Weak recovery	Backups, tested IR & recovery playbooks	NIST CSF — Respond / Recover

TURN FINDINGS INTO A ROADMAP

Remediation is strongest when actions are sequenced. Close the most exposed access paths first, then strengthen segmentation and monitoring, and finally mature detection, response, recovery and continuous assessment. Mapping findings to IEC 62443 and NIST guidance helps turn technical work into measurable programme progress.

THE PATH FROM EXPOSURE TO RESILIENCE

The CISO's OT Security Readiness

OT security readiness is not a single score — it is a profile across the domains a CISO must be able to answer for. The scorecard below turns the themes of this guide into a self-assessment: where the programme is strong, where it is exposed, and where an assessment should look first.

OT SECURITY READINESS SCORECARD

Domain	Maturity	The question to answer
Asset visibility	●●○○	Do we know every asset and connection into OT?
Network segmentation	●●○○	Are critical zones separated with controlled conduits?
Identity & access	●○○○	Is every path into OT authenticated and least-privilege?
Secure remote access	●○○○	Is vendor and remote access brokered, logged, revocable?
Monitoring & detection	●○○○	Would we see an intrusion in the OT network?
Vulnerability management	●●○○	Do we manage exposure where patching is impossible?
Incident response	●●○○	Are OT playbooks defined, owned and tested?
Safety alignment	●●●○	Are security and safety governed together?

Illustrative baseline — complete against your own environment. Four dots denote a mature, tested capability.

READINESS IS A PROFILE

Use the scorecard as a conversation starter rather than a single security number. The useful question for each domain is whether the capability is known, owned, tested and repeatable — from asset visibility and segmentation to identity, monitoring, vulnerability management, incident response and safety alignment.

REFERENCE

OT, ICS & IoT Glossary

A shared vocabulary for the systems, standards and techniques referenced throughout this guide.

USING THE GLOSSARY

OT — Operational Technology Hardware and software that monitors or controls physical processes and equipment.	**NIST SP 800-82** U.S. guidance for securing operational technology and control systems.
ICS — Industrial Control System The control systems — SCADA, DCS, PLCs — that operate an industrial process. A subset of OT.	**Zones & Conduits** IEC 62443 grouping of assets (zones) and the controlled connections between them (conduits).
IIoT Industrial Internet of Things: connected sensors, gateways and devices linking OT with analytics and cloud.	OT DMZ A demilitarised zone separating enterprise IT from the operational network.
SCADA Supervisory Control and Data Acquisition — centralised visibility and control of distributed operations.	**Jump Host** A hardened intermediary system used to reach OT from outside its zone.
DCS Distributed Control System — process control distributed across controllers within a facility.	**Modbus** A widely used, historically unauthenticated industrial protocol.
PLC Programmable Logic Controller — a rugged industrial computer executing control logic.	**DNP3** A protocol common in utilities and distributed infrastructure.
RTU Remote Terminal Unit — a field device for telemetry and control over wide areas.	**OPC UA** A modern industrial protocol with built-in security capabilities.
HMI Human-Machine Interface — the screen operators use to monitor and control the process.	**MQTT** A lightweight publish/subscribe protocol common in IoT and IIoT.
SIS Safety Instrumented System — independent system that brings a process to a safe state.	**PROFINET / EtherNet/IP** Real-time Ethernet-based industrial automation protocols.
Historian A database recording time-series process data; a common OT/IT bridge.	**ATT&CK for ICS** MITRE's knowledge base of adversary tactics and techniques against industrial systems.
Purdue Model A reference architecture placing systems in levels 0–5 from field to enterprise.	**Passive scanning** Discovery by observing traffic without transmitting to devices.
IEC 62443 The international standard for industrial automation and control system security.	**Consequence-based testing** Scoping an assessment from unacceptable outcomes back to systems and paths.

REFERENCE

References, Authors & Contributors

SELECTED SOURCES & FURTHER READING

- **CISA** — ICS Advisories and Industrial Control Systems guidance
- **Dragos** — OT/ICS Cybersecurity Year in Review; tracked threat groups
- **Fortinet** — State of Operational Technology and Cybersecurity Report
- **IEC 62443** — Security for industrial automation and control systems
- **NIST SP 800-82** — Guide to Operational Technology Security
- **MITRE ATT&CK for ICS** — Adversary tactics and techniques

METHODOLOGY NOTE

Figures cited in this guide are drawn from the public reporting above and from recurring patterns observed across industrial security assessments. Where a single indicative value is shown, it is used to illustrate a trend rather than to represent any single organisation.

AUTHORS & CONTRIBUTORS

DivIHN OT Security Practice
Research, authoring and technical review by DivIHN's operational-technology and offensive-security specialists.

Editorial & Design
DivIHN Marketing & Content team.

DISCLAIMER

This guide is provided for general information and executive awareness. It does not constitute specific security advice. OT security testing must be planned and authorised for each environment, with appropriate safety controls. DivIHN accepts no liability for actions taken solely on the basis of this document.

FIELD GUIDE TAKEAWAY

The guide is intended to connect executive decisions with practical testing boundaries. Use the selected standards and public reporting as reference points, then adapt the assessment to the specific architecture, safety requirements, operating windows and authorisations of the environment being tested.

REFERENCE

About DivIHN

DivIHN helps organisations secure the systems that keep operations running. Our operational-technology security practice brings IT and OT expertise together — assessing industrial environments the way an adversary would, while protecting the safety and availability the business depends on.

HOW WE HELP CISOS

OT / ICS / IoT VAPT
Consequence-based assessment across the full industrial attack surface.

Architecture & segmentation
Zones, conduits and secure remote access aligned to IEC 62443.

Monitoring & detection
Visibility and detection engineering for operational networks.

Response & resilience
IR playbooks, tabletop exercises and recovery readiness for OT.

Ready to test what matters — safely?

Talk to DivIHN about scoping an OT VAPT assessment around the consequences your organisation cannot accept — from the connected industrial environment to a practical readiness model.

- www.divihn.com
- OT Security Practice

DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

A PRACTICAL NEXT STEP

Start with the consequences the organisation cannot accept. From there, map the systems and access paths that could lead to them, decide which layers can be tested safely, and define the evidence needed to prove exposure without triggering the risk you are trying to measure.

Inside OT, ICS & IoT VAPT
WHAT CISOs NEED TO TEST, SCOPE, AND DEFEND · 2026 FIELD GUIDE