FIELD GUIDE

Listen first

A practical guide to starting OT security discovery

Most OT security programmes stall on one question: what is actually on the plant network, and what is it saying? This guide covers the first weeks of finding out, without putting the process at risk.

Quantum Clave Ltd Accurate as of October 2026 10 sections · ~16 min read

SIX STEPS TO A FIRST INVENTORY — SECTIONS 01 TO 06, IN ORDER

01 Get permission and agree the scope	02 Do no harm: listen before you probe	03 Where to listen
04 What to look for	05 Turn findings into an inventory	06 Keep the inventory current

Why discovery comes first

AT A GLANCE

- Listen to the traffic already on the plant network before sending anything, because probing can upset older controllers.
- With written approval, listen first where the office network meets the plant and in the control room; leave safety systems out.
- Turn what you hear into a record of devices, connections and the encryption each uses, if any, and keep it current.

Every later OT security control depends on knowing what is there. Firewall rules need a list of the connections the process requires. Vulnerability management needs a list of devices and firmware. A post-quantum migration plan needs to know where cryptography is used at all, and where it is missing.

Official guidance now agrees on the starting point. In 2025 CISA, the UK NCSC and partner agencies published joint guidance on OT asset inventories and on keeping a definitive view of OT architecture. The NCSC's post-quantum migration timeline sets 2028 as the milestone by which organisations should "carry out a full discovery exercise", and ISA/IEC 62443 supplies the zones-and-conduits vocabulary for organising what you find.

This guide is for the engineer who has been asked to start. It assumes Ethernet-connected control systems and some separation, however imperfect, between the business network and the plant. While foundational principles can be validated on a testbench using open-source tools, ClaveQ's position is that enterprise-scale, continuous discovery necessitates automated, schema-validated tooling.

01 Get permission and agree the scope

Discovery on a live plant is a change to that plant, even when the method is passive.

Inserting a TAP (test access point: a small device fitted into a cable that copies the traffic) means breaking a cable. Enabling a mirror (SPAN) session, where the switch copies chosen ports' traffic to a spare port, changes a production switch's configuration. A laptop on the wrong port is a new device on the process network. Put the work through the site's change process, which NIST SP 800-82r3 lists among the activities that maintain the integrity of OT systems.

01 **Get written sign-off from the process owner.**

This is usually the operations or production manager, not the IT security lead. CISA's guide makes governance its first step: identify the authority that requires the inventory and the roles responsible for it.

02 **Bring operations and process safety in early.**

They know which systems cannot tolerate an interruption, when maintenance windows fall, and which equipment sits under an integrator's or OEM's support contract that limits third-party connections. Ask those vendors what they will support before you plug anything in. Treat any safety instrumented system (SIS) network as out of bounds: nothing connects to it, even passively, without the safety engineer's written approval. NIST SP 800-82r3 (section 2.3.7) describes the SIS as often independent of the basic process control system and designed in accordance with IEC 61511, so any change there falls under the site's safety case.

03 **Scope by zone, and start small.**

Write down which zones and systems are in scope, and what counts as an asset. One site and one control system is a sensible first scope.

04 **Agree how captures will be handled.**

Plant captures contain process values, device configuration, personal data such as usernames and, on cleartext protocols, sometimes credentials. Decide where they are stored, who may see them, how long they are kept and whether they may leave site. NCSC treats the architecture record itself as sensitive information.

05 **Tell the people who watch the network.**

A new sensor on a mirror port, or a burst of unfamiliar traffic, should not trigger an incident. NCSC asks organisations to give their Security Operations Centre the timing and scope of any active scanning; give the same notice for passive work.

06 **Agree who works in the cabinet and how the sensor is connected.**

Fitting a TAP means opening a live control cabinet, which typically carries 24 V DC and often 230 V AC. That needs a permit to work and a competent person, often the integrator, plus a tested rollback; removing the TAP later needs a second outage. The sensor's own management and output connection is a new path into the zone, and a sensor fed from several zones can bridge them. Put it on the plan and route it through the zone's firewall or out of band.

The output is a one-page plan signed by the owner. It sets out where and when you will listen, who does the physical work, and how to roll back.

---

02 *Do no harm: listen before you probe*

There are two ways to learn what is on a network. Active discovery sends packets and studies the replies. Passive discovery copies traffic that is already flowing and analyses the copy.

On an office network the difference is mostly one of speed. On a plant it decides whether the process keeps running. NIST is direct about it:

> "OT network owners should exercise extreme caution when permitting active scanning on an operational network due to device sensitivity on the target network. Active scans may cause device instability or interfere with the device process state, potentially impacting safety and integrity."
>
> NIST SP 800-82r3, Appendix E.2.3 (September 2023)

The NCSC gives the same warning: active scanning "has the potential to overwhelm legacy devices that may have limited processing power, leading to performance degradation, freezing or crashing."

What passive capture cannot do

Passive discovery has limits. NIST notes that it "cannot identify devices that are not actively communicating, nor can it inspect encrypted traffic (without special provisioning)", and it "will often take days to complete due to its dependence on existing network traffic." A spare controller powered only during a changeover, or a modem that connects once a month, will not appear in a one-day capture. Anything not on Ethernet, such as serial links, PROFIBUS or 4–20 mA loops, is invisible to it. Ethernet device networks behind a controller's second port, such as PROFINET or EtherNet/IP links to remote I/O and drives, are visible only if you listen on them.

Where active techniques fit

Active querying still has a place later, used with care. NIST describes a "safe active scanning" pattern that "first learns about connected equipment through passive means and then uses device-specific

communication” to collect more detail; several of the commercial platforms in section 07 offer it. NCSC advises using native ICS/OT protocols and tools, with methods “tested and validated by the original equipment manufacturer (OEM) of each asset”, and NIST adds that automated tools should be tested on offline systems before they reach production.

> **The order that works:** passive capture first, to build a baseline inventory. Targeted active queries second, inside planned maintenance windows, against device types the OEM has approved. Manual checks of cabinets and project files to fill the gaps neither method reaches.

---

03 *Where to listen*

A passive sensor only sees traffic that passes the point where it is connected. Placement is the most consequential decision in the project.

NIST’s guidance is that “typical installations locate the network sensors between the control network and corporate network, but other locations can include network perimeters, key network segments (e.g., DMZ), and critical OT devices.” The figure shows those choices on a simplified water-treatment site, drawn on Purdue-model levels.

The order to add listening points

A **The OT side of the IT/OT boundary.**

Every conduit between business and plant crosses here, including anything that was never documented. Listening on the plant side of the firewall shows what the rule set actually allows through, which is often more than its documentation says.

B **The control-room core switch.**

SCADA servers and engineering workstations converge here with the HMIs, along with their polling traffic to the controllers. A single sensor here sees most of that supervisory traffic.

C **Telemetry and remote-access head-ends.**

Outstations reached over private cellular networks or radio come in here, and so do many vendor connections. The head-end is not the only way in, though. In the December 2025 attack on a Polish combined heat and power plant, the attacker entered a wind farm through its internet-facing VPN, used the wind farm’s cellular router to reach the distribution operator’s private APN (a closed mobile data network), found a controller at the plant whose web interface was exposed on that APN with default credentials, and tunnelled from it into the plant’s OT network. CERT

Polska reported this as, to the best of its knowledge, the first observed use of a private APN to reach an OT network in a real attack, and recommends monitoring traffic between the OT network and the private APN. So list every controller or outstation with its own cellular interface, because its traffic may never pass the head-end, and listen on the OT side of each one too.

D

Selected area or cell switches.

Traffic between an HMI and a PLC on the same switch, or between peer controllers, never reaches the core. Add these points for the highest-consequence process cells once the first two are stable. Leave any safety-system network out, as section 01 explains.

Capture for long enough to cover the plant's own cycles: shift changes, weekly backups, scheduled vendor maintenance. As a starting point, and as our own judgement since NIST says only that passive discovery takes "days", we suggest at least one full week at points A and B. Treat anything that runs on a longer cycle, such as a monthly modem, a seasonal pump or an annual maintenance connection, as unconfirmed until records or a longer capture cover it. Size storage for the week before you start: full packet capture at a core switch can run to hundreds of gigabytes.

TAP or mirror port?

NIST notes that network traffic is usually accessed through TAPs or SPAN ports, "though performance impacts to the OT system may result from their use, especially with SPAN ports."

	MIRROR (SPAN) PORT	NETWORK TAP
Installation	Configuration change on an existing managed switch; no cable is broken	Inserted into the cable, so the link is down while it goes in; needs an outage window. On a ring link, expect a ring reconfiguration and agree it with the integrator
What you see	Whatever the switch chooses to copy. If the mirrored ports carry more than the destination port can, the excess is dropped and the sensor is not told	Both directions of the tapped link. A TAP with one monitor port per direction delivers a full copy; one that merges both directions onto a single monitor port can drop frames when their combined rate exceeds that port's speed
Can the sensor transmit?	Depends on switch configuration; check it	A good TAP blocks transmission from its monitor ports. Verify this on your unit
Not possible when	The switch is unmanaged, or lacks spare ports or mirror sessions	No outage can be agreed, or the cabinet has no suitable power

> **A receive-only TAP can still take the link down.** Some TAPs lose the link when they lose power, so test the power-loss behaviour of a unit before you rely on it.

TAP vendors explain why. At gigabit speeds a copper TAP needs active electronics, and one TAP maker states that "without failsafe protection, a powered TAP could take down the link between the two network devices during a power loss to the TAP." For a plant, that suggests four rules:

- On fibre, prefer an optical TAP that splits the light and needs no power. Check the split ratio against the link's optical budget first, because the split adds loss on the live path.
- On copper, choose an industrial unit with fail-safe (power-loss) protection that keeps the link up if the TAP loses power, then test the power-loss behaviour yourself. Ask the vendor how long the link takes to come back after the TAP loses power and switches over.
- Power the TAP from the cabinet's own protected supply, never from the sensor, so that the live link does not depend on your monitoring hardware.
- Keep office-grade units on the bench.

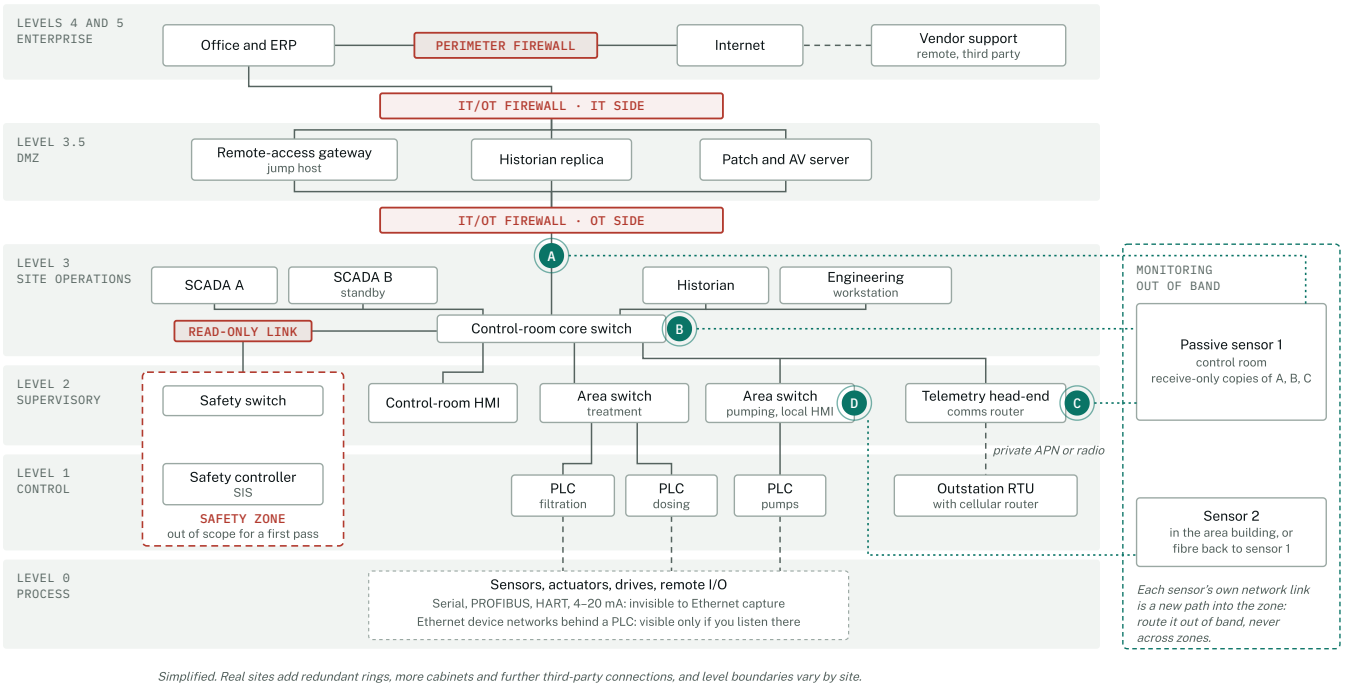

Figure 1. Recommended listening points, in the order to add them. Each point copies traffic through a TAP or a mirror (SPAN) port to a receive-only sensor that sits outside the plant levels (dotted lines). Distant points need their own sensor or a dedicated fibre run; remote mirroring (RSPAN/ERSPAN) carries the copies over the production network and adds load to it. Firewalls are shown in red.

- **A** **First.** OT side of the IT/OT boundary.
- **B** **First.** Control-room core switch.
- **C** **Second.** Telemetry and remote-access head-end.
- **D** **Later.** Selected area switches.

Safety zone. The safety instrumented system has its own network and is not a listening point. Leave it out of a first pass; nothing connects to it, even passively, without the safety engineer's written approval.

04 *What to look for*

The first capture will produce more data than anyone can read. Four questions keep the analysis focused.

Devices and connections nobody listed

Compare what the sensor sees with the drawings and the asset register. Expect differences: a laptop that never left after commissioning, a historian talking directly to a PLC across a zone boundary, a managed switch with its web interface open. Where monitoring and documented designs disagree, NCSC says you "must validate if the changes were planned" and document them if they were. The unplanned ones are findings.

Cleartext control protocols

Modbus/TCP, S7comm, DNP3, EtherNet/IP and IEC 60870-5-104 were designed for closed networks and, in their base forms, carry no encryption and little or no authentication. A passive sensor can read register writes and program downloads as they happen, and so can anyone else on the path. Record whether each connection uses a secured variant where one exists, such as DNP3 Secure Authentication, OPC UA security modes or CIP Security; a capability the device supports but nobody enabled is a common finding. NCSC asks for a central record of the protocols and ports each asset needs, regular audits of those protocols, and, where legacy protocols cannot be replaced, compensating controls such as a VPN.

Remote-access paths

List every route by which someone outside the site can reach a control device: vendor VPNs, remote-desktop sessions through the DMZ, remote-support software installed on engineering workstations, and cellular routers at outstations. NCSC asks for particular attention to third-party connections that can change device configuration. Flows that cross the boundary but appear in no firewall rule documentation deserve the first look.

Weak and quantum-vulnerable cryptography

Where traffic is encrypted, the handshake is still visible. TLS, SSH and IKE (the IPsec key exchange) reveal the cipher suite and key-exchange method; older TLS versions also send the server certificate in the clear, whereas TLS 1.3 encrypts it, so it is hidden from a passive observer. Look for obsolete protocol versions, expired certificates, and self-signed certificates on interfaces that should chain to a site certificate authority. On management interfaces, look for Telnet, FTP and SNMP v1 or v2c community strings.

Then look for key exchange and signatures that a future quantum computer could break. NCSC names RSA, finite-field Diffie-Hellman, ECDH, DSA, ECDSA and EdDSA as vulnerable to such a computer. For key exchange, NCSC warns of “an attacker collecting and storing data today and decrypting it at some point in the future”, which matters for data that must stay confidential for years. Signatures face a different risk: once such a computer exists, NCSC notes, an adversary “could forge signatures to impersonate the legitimate private key owner”, which would undermine trust in signed firmware. NIST published the replacement standards, ML-KEM, ML-DSA and SLH-DSA, in August 2024. Passive capture records only what was negotiated on the wire. Keys stored on devices and firmware-signing chains need other methods.

FINDING	TYPICAL FIRST ACTION
Undocumented device or connection	Identify owner; confirm whether planned; update record or remove
Cleartext write or program-download traffic	Restrict which hosts may send them; enable secured variant where supported
Remote path not in firewall documentation	Confirm business need; route through managed remote access or close
Obsolete TLS, SNMP v1/v2c, Telnet	Upgrade configuration; schedule firmware where needed
RSA or elliptic-curve key exchange or signatures	Record in the cryptographic inventory; plan migration by priority

05 *Turn findings into an inventory*

The capture shows what talked to what while you were listening. The inventory turns that into a record that operations, security and auditors can act on.

The asset list

CISA's guide sets out a five-step process, from defining scope to managing assets over their life cycle, and names fourteen high-priority attributes to collect, including active and supported communication protocols, asset criticality, IP and MAC addresses, manufacturer, model, operating system, physical location, ports and services, and user accounts. A passive sensor fills several of these directly; criticality and ownership have to come from the people who run the plant.

Organise the list by zone and conduit, as CISA's example taxonomies do using the ISA/IEC 62443 model, and map the communication pathways between zones using data-flow analysis, protocol identification and layer 2 and layer 3 network details. The figure in section 03 is a starting template.

The cryptographic bill of materials

Alongside the asset list, record the cryptography each connection uses, or the fact that it uses none, in a machine-readable form. CycloneDX, an OWASP project standardised by Ecma International as ECMA-424 (the second edition, December 2025, defines CycloneDX 1.7), supports a cryptography bill of materials (CBOM) that represents cryptographic assets such as algorithms and certificates, and how they relate to

components. A standard format can be imported into a governance tool, handed to an auditor without re-keying, and compared between scans.

Prioritise the findings

NCSC suggests prioritising systems by their impact on the business function or the potential for national impact; by third-party connections, particularly where these can change the configuration of system components; and by their overall exposure, such as how many connections they have to other systems. In practice that puts boundary-crossing remote access, cleartext control paths to high-consequence processes and long-lived cryptography at the top of the list.

---

06 *Keep the inventory current*

Suppose an integrator comes in to swap a drive the day after the first inventory is signed off. The record has already started to drift.

NCSC calls the definitive record “continually updated” and points out that passive monitoring tools “can also aid in spotting undocumented changes to the OT system”.

The practical route is to leave the sensors in place once the first inventory is accepted. Then:

- compare each new capture against the accepted baseline and treat new devices or connections and changed cryptography as change requests to be explained;
- link the inventory to the site’s change process, so a planned change updates the record before the sensor sees it;
- repeat any active queries on a fixed schedule, inside maintenance windows;
- review the prioritised list with operations at least once a year, and after any major project;
- use the cryptographic inventory to track progress against the NCSC milestones of 2028 for discovery and planning, 2031 for the highest-priority migrations and 2035 for completion.

NIST’s guidance on continuous monitoring adds one caution: OT cybersecurity staff “must be part of the diagnostic process of interpreting the alerts provided by network monitoring tools.” A sensor that raises alerts nobody on the plant side understands is soon ignored, then switched off.

---

07 *Tools to start with*

The method does not depend on any one product. These are the common starting points.

TOOL	TYPE	WHAT IT OFFERS
Zeek with CISA's ICSNPP parsers	Open source	Passive network monitor producing structured logs; ICSNPP adds parsers for industrial protocols such as BACnet, EtherNet/IP and S7comm
Malcolm	Open source (CISA)	Packaged traffic-analysis suite for packet captures, Zeek logs and Suricata alerts
Wireshark	Open source	Packet-level inspection for checking individual conversations
Nozomi Networks Guardian	Commercial	Passive OT and IoT monitoring sensor; optional Smart Polling for active queries
Claroty xDome	Commercial	Asset discovery through passive monitoring, Safe Queries, Claroty Edge and project-file analysis
Dragos Platform	Commercial	Passive network monitoring with controlled active collection

The open-source route costs engineering time and needs someone who can read Zeek output. In our view, owners of open-source tools configure and maintain them by hand, and translate logs into compliance artefacts manually. ClaveQ Scan automates the step from capture to a schema-validated CycloneDX 1.7 CBOM on every scan.

Platforms such as Dragos, Claroty and Nozomi focus mainly on asset inventory, operational visibility and threat detection. ClaveQ Scan focuses on cryptographic inventory, which we treat as a separate task that feeds into post-quantum planning.

The permission and placement steps apply to all of them.

ClaveQ Scan covers one part of this work: the cryptography question. It connects to a TAP or mirror port. It is designed never to transmit on the monitored network, and on a TAP whose monitor ports block transmission it physically cannot. It decodes IT and OT protocols and rates each connection whose protocol or handshake it can read as unencrypted, quantum-vulnerable or quantum-safe, and it reports the connections it cannot read as a coverage gap. It writes the result as a CycloneDX 1.7 CBOM whose format is validated against the official schema in testing. It is designed to complement an asset and threat-monitoring platform, not to replace one. Its limits are worth stating. It sees Ethernet and IP traffic only; serial protocols such as Modbus RTU and DNP3 serial are decoded only when tunnelled over TCP, and it does not decode MIL-STD-1553, CAN or other non-IP buses. It does not classify DTLS sessions, such as CIP Security over UDP, and it does not detect IEC 62351-6 signatures on IEC 61850 GOOSE messages. Like any passive tool, it misses devices that stay silent and certificates hidden by TLS 1.3.

08 Glossary

CBOM

Cryptography bill of materials: a machine-readable list of the cryptography each system or connection uses.

Cleartext

Data sent without encryption, so anyone who can see the traffic can read it.

DMZ

A separate network between the office and the plant that holds servers both sides need.

HMI

Human-machine interface: the screen operators use to watch and control part of the process.

IT/OT boundary

The firewalled point where the office and business network meets the plant network.

OT

Operational technology: the computers, controllers and networks that run physical processes such as water treatment.

Permit to work

A written site authorisation stating who may do hazardous work, where, when and with what precautions.

PLC

Programmable logic controller: a rugged industrial computer that directly runs one part of the process.

Post-quantum cryptography

Encryption and signing methods designed to stay secure against a future quantum computer.

Purdue model

A reference model that stacks plant systems in numbered levels, from field devices up to business systems.

SCADA

Supervisory control and data acquisition: control-room software that monitors and commands the site's controllers.

SPAN (mirror) port

A switch port that receives a copy of the traffic on other chosen ports.

TAP

Test access point: a small device fitted into a cable that copies its traffic to a monitor.

Zones and conduits

Grouping systems into zones with shared security needs, and controlling the connections (conduits) between them.

09 Sources

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
1	CISA, EPA, NSA, FBI and partners	Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators ↗ (https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf)	13 Aug 2025	01 inventory as foundation; 02 governance first; 06 five-step process, fourteen attributes, zones and conduits
2	NCSC, CISA, FBI and partners	Creating and maintaining a definitive view of your OT architecture ↗ (https://www.ncsc.gov.uk/collection/operational-technology/definitive-architecture-view)	29 Sep 2025	01 joint guidance; 02 record as sensitive, SOC notice; 03 active-scanning risk, OEM validation; 05 validating differences, protocol record; 06 prioritisation; 07 continually updated record
3	NCSC	Timelines for migration to post-quantum cryptography ↗ (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines)	20 Mar 2025	01 and 07: 2028, 2031 and 2035 milestones
4	ISA	ISA/IEC 62443 series of standards ↗ (https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards)	Series	01 and 06: zones-and-conduits vocabulary
5	NIST	SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security ↗ (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf)	Sep 2023	02 change management, safety systems (2.3.7); 03 active and passive scanning (E.2.2, E.2.3), offline tool testing (6.1.1); 04 sensor placement, TAP and SPAN (6.3.2.1); 07 OT staff in alert diagnosis
6	CERT Polska	Follow-up analysis of the 29 December 2025 energy sector incident ↗ (https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/)	Aug 2026	04 private APN attack path and monitoring recommendation (point C)

#	PUBLISHER	DOCUMENT	DATE	SUPPORTS
7	Garland Technology	Passive and Failsafe Copper TAPs ↗ (https://www.garlandtechnology.com/blog/passive-and-failsafe-copper-taps-which-option-is-best-for-your-network)	30 Jul 2026	04 powered TAP behaviour on power loss
8	IETF	RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3 ↗ (https://www.rfc-editor.org/rfc/rfc8446)	Aug 2018	05 TLS 1.3 hides the certificate
9	NCSC	Next steps in preparing for post-quantum cryptography ↗ (https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography)	14 Aug 2024	05 vulnerable algorithms; recorded traffic versus signature forgery
10	NIST	NIST releases first 3 finalized post-quantum encryption standards ↗ (https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)	13 Aug 2024	05 ML-KEM, ML-DSA and SLH-DSA
11	Ecma International	ECMA-424, CycloneDX Bill of Materials Specification, 2nd edition ↗ (https://ecma-international.org/publications-and-standards/standards/ecma-424/)	Dec 2025	06 CycloneDX 1.7 standard
12	CycloneDX (OWASP)	Cryptography Bill of Materials ↗ (https://cyclonedx.org/capabilities/cbom/)	Undated web page	06 what a CBOM represents

Find the cryptography on your OT network

To talk through a first discovery exercise, or to see a sample CBOM, get in touch.

More guides and contact details at claveq.com →

COPYRIGHT AND TERMS OF USE

Copyright	© 2026 Quantum Clave Ltd, trading as ClaveQ. Company no. 17340121. All rights reserved, except as below.
Sharing	You may copy and share this paper in full and unmodified, with this notice intact. Please do not edit it, remove our name, or sell it.
Quotations and sources	Quotations from published sources are reproduced with attribution for the purposes of review and comment. Named products and organisations belong to their owners; mention does not imply endorsement.
Trade mark	ClaveQ® is a registered trade mark of Quantum Clave Ltd in the United Kingdom.
Disclaimer	This paper is general information, accurate as of October 2026. It is not legal, regulatory or compliance advice. Check current guidance before acting on it.

© 2026 Quantum Clave Ltd, trading as ClaveQ · Company no. 17340121

Accurate as of October 2026 · claveq.com