Post-Quantum

Cryptography Conference

Crypto Asset Discovery Tooling – an Overview of Capabilities, Characteristics and Gaps

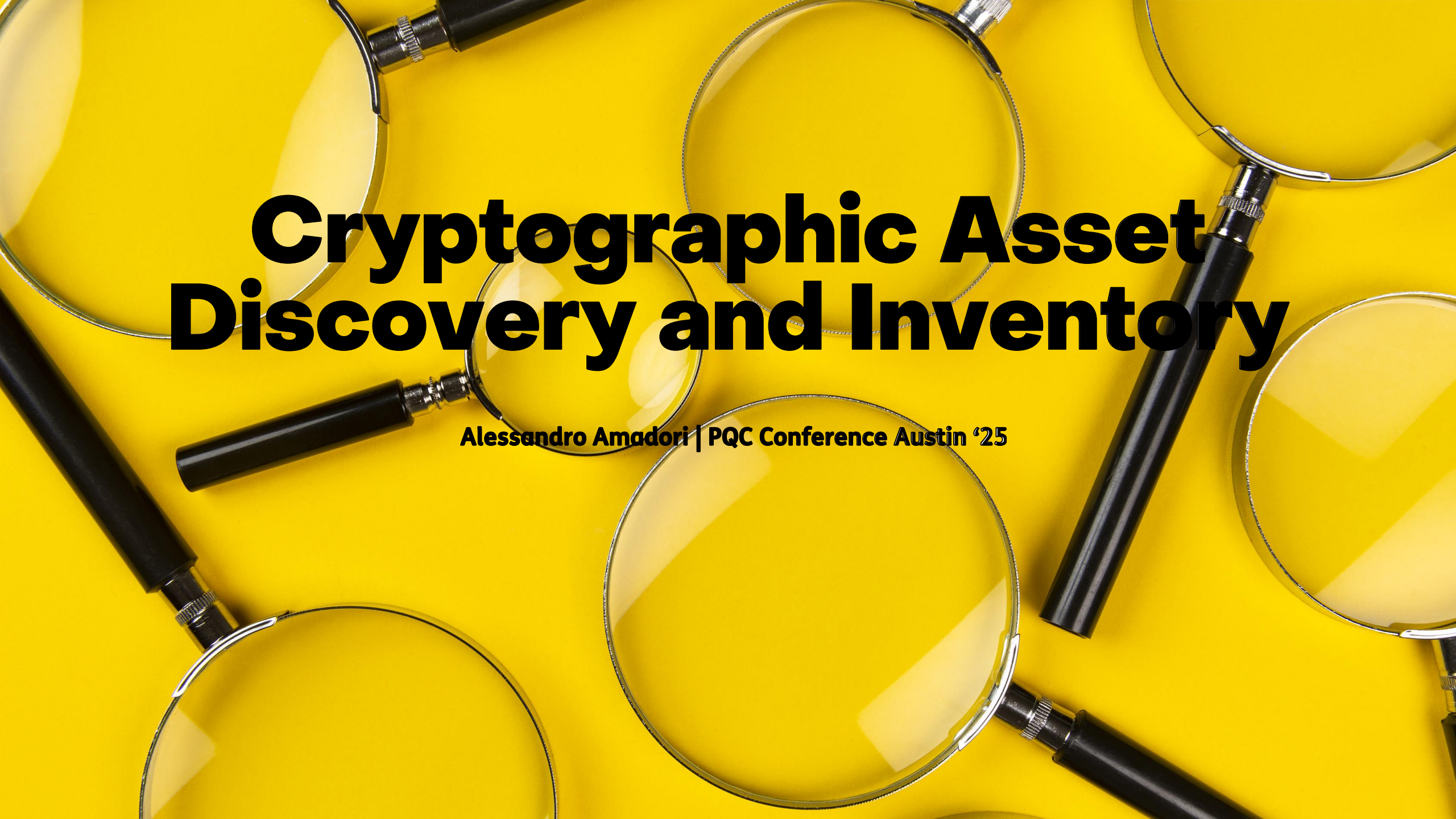
In the migration towards PQC, one of the first steps should be getting an overview of cryptographic assets in your organisation, i.e. where and why are you using which types of cryptographic algorithms, protocols, keys, etc. The result is captured in a Cryptographic Bill-Of-Materials (CBOM). Various commercial solutions exist, but how well are these addressing the problem? In 2024, as an independent research organisation, we have conducted research into crypto asset discovery tooling and their vendors, through literature research and interviews with the vendors. In this presentation, I will give an overview of the currently existing tools, the ideal setting, the gap between them and how to bridge that gap.

Alessandro Amadori

Cryptographic Researcher at Netherlands Organisation for Applied Scientific Research (TNO)

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online



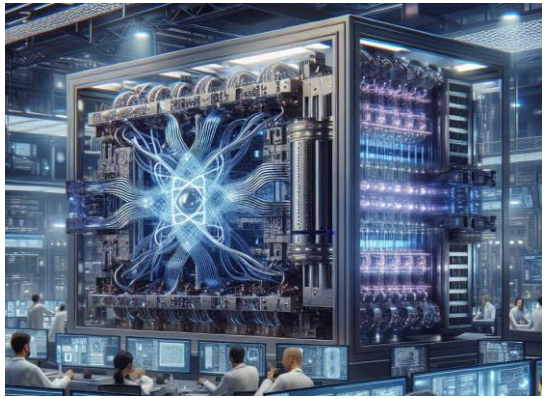
Cryptographic Asset Discovery and Inventory

Alessandro Amadori | PQC Conference Austin ‘25

Overview of Cryptographic Assets fundamental to

Prevent data leaks

Comply with regulation and legislation



Prepare for the PQC Migration

A cryptographic inventory is required for cryptographic asset and lifecycle management.

What is Crypto Asset Discovery and Inventory

- Finding all cryptographic keys, key material, primitives, protocols and their context
- Cryptography is omni-present:


Network


Filesystems


Hardware/Firmware


Apps & libraries

- In a passive/static or active/dynamic manner
- There are point-solutions and full-stack solutions
- Open source, but also proprietary

Project Goals and Overview

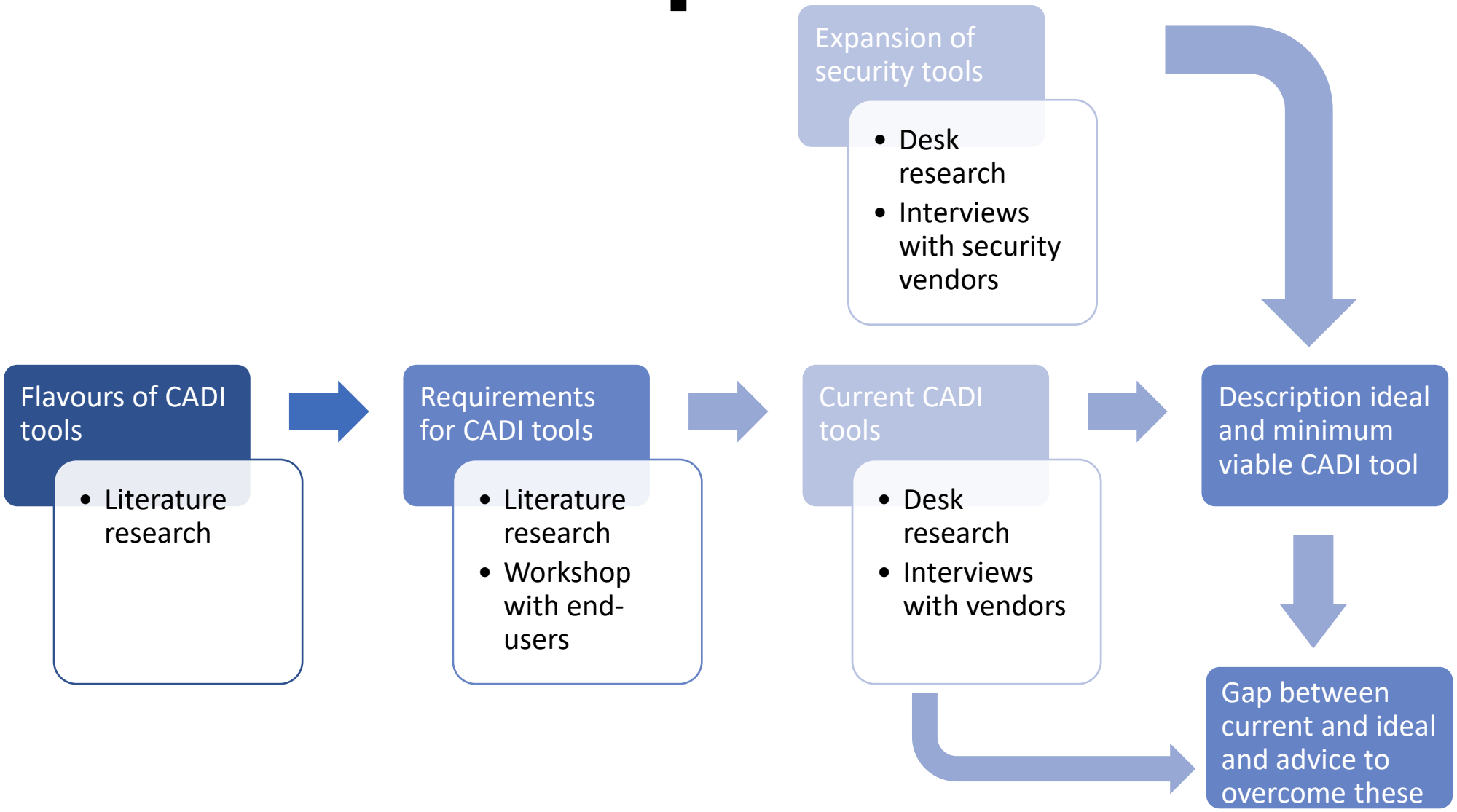
Cryptographic Asset Discovery and Inventory (CADI) project

- Started in 2024, runs until end February 2025. The research and report will be finalised then.
- As part of the Quantum Safe Cryptography Gov (QvC Rijk)
- Funded by
  - (Dutch) National Cyber Security Center (NCSC-NL),
  - Ministry of Internal Affair and Kingdom Relations (Min. BZK)
  - Ministry of Economic Affairs (Min. EZ)
- Cryptographic Asset Discovery fundamental step in PQC migration
  - No-regret move (PQC migration handbook v2)
- Main questions:

What should a Cryptographic Asset Discovery and Inventory tool look like?

What CADI are already on the market?

Research set-up

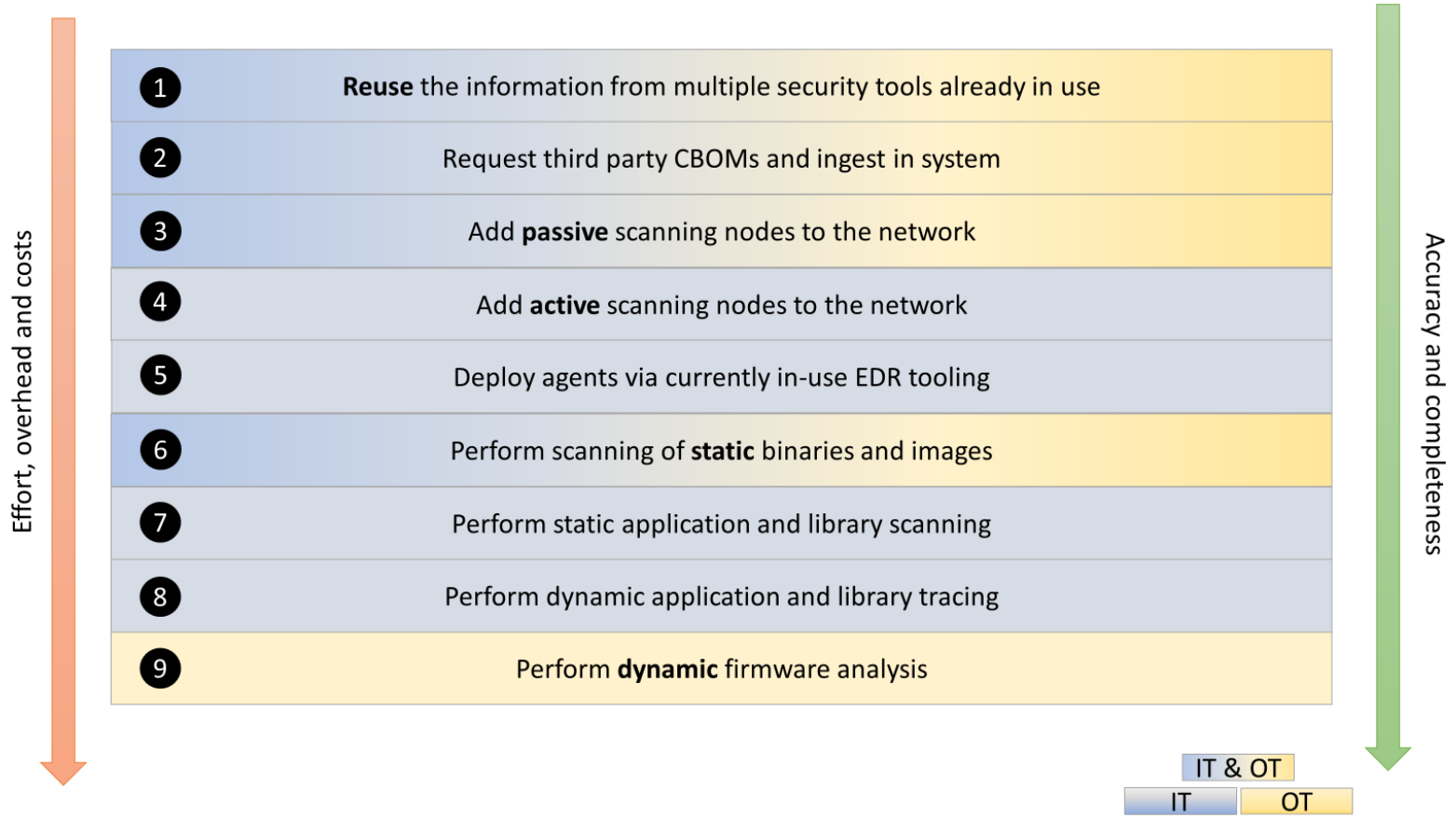


Use case dependency

- Solutions for ideal and minimal viable product MVP tool
  - Necessary distinction between IT and OT
- How to measure their performance and convenience?
  - Balance between effort, overhead & costs versus accuracy & completeness
    - Effort = implementation time for internal developers
    - Overhead = performance penalty on system because of running CADI tool
    - Costs = integration cost + price of tool and services
    - Accuracy = low false positives + quality and amount of data w.r.t. found assets
    - Completeness = low false negatives
  - Obviously the more accurate the tool the more overhead it causes

Cryptographic Asset Discovery Maturity Model

- Metric to measure maturity of the cryptographic asset discovery
- Composed of several accuracy and effort levels
  - Difference IT vs OT

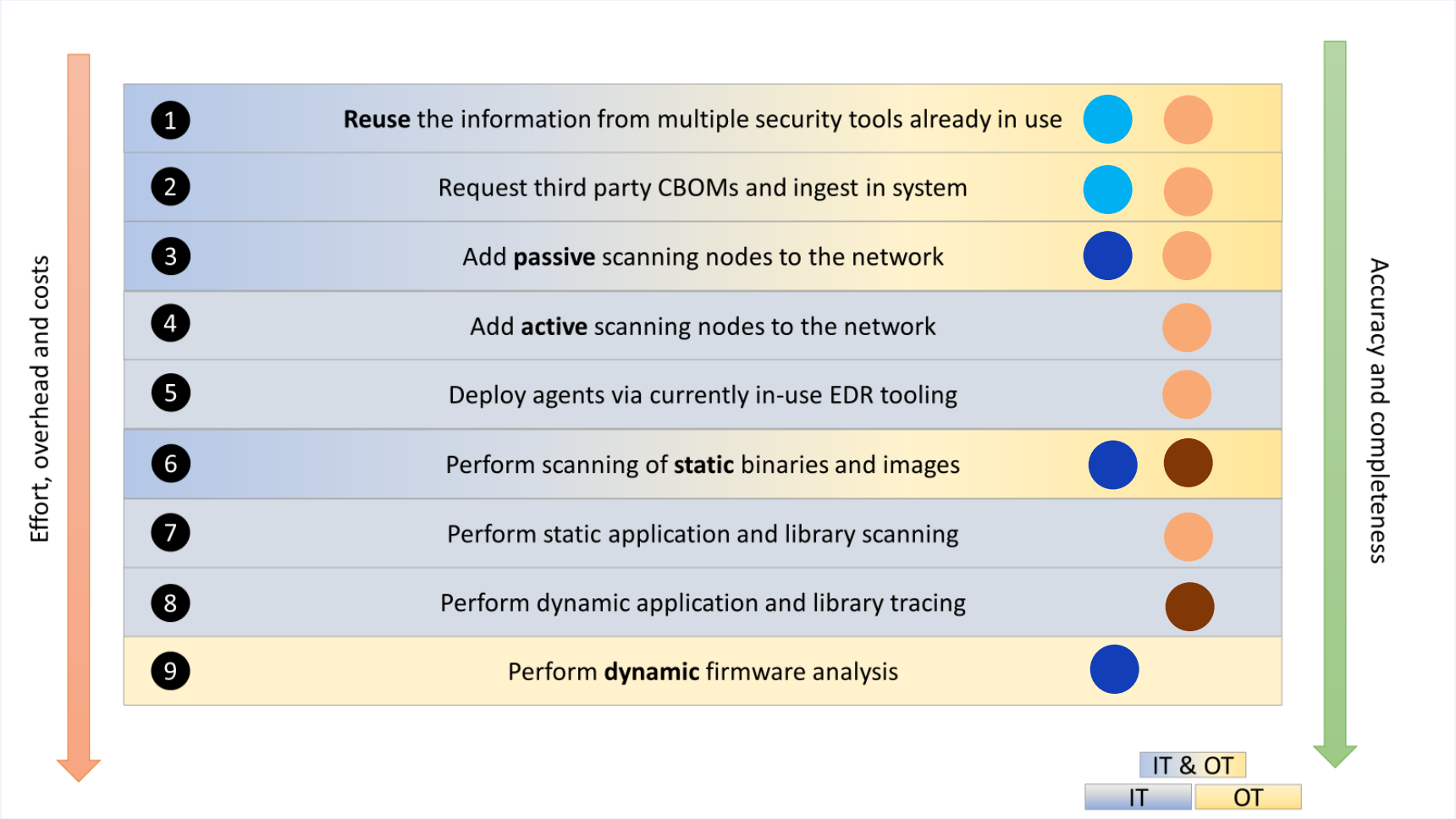


Requirements

Requirement	MVP	Ideal solution
Scan frequency	Monthly (OT), weekly (IT)	Daily (OT), real-time (IT)
Location	On-premise	On-premise
Agents	No (OT), yes (IT)	Yes*
Ingestion of CBOMs	Yes	Yes
Logs	All information surrounding the execution of scans, errors, and results	All information surrounding the execution of scans, errors, and results
Scope	Key (material), crypto primitives, crypto protocols	Idem as for MVP, but also including the discovery of PQC and placing the assets in context (owner, process)
Accuracy	30% (OT), 60% (IT)	60% (OT), 85% (IT)
Integration	No plug-and-play, but offering advice.	Plug-and-play for well-known products. Tailored solutions for other products.

MVP and ideal levels of scanning

- OT MVP
- OT ideal
- IT MVP
- IT ideal



Types of CADI tooling available

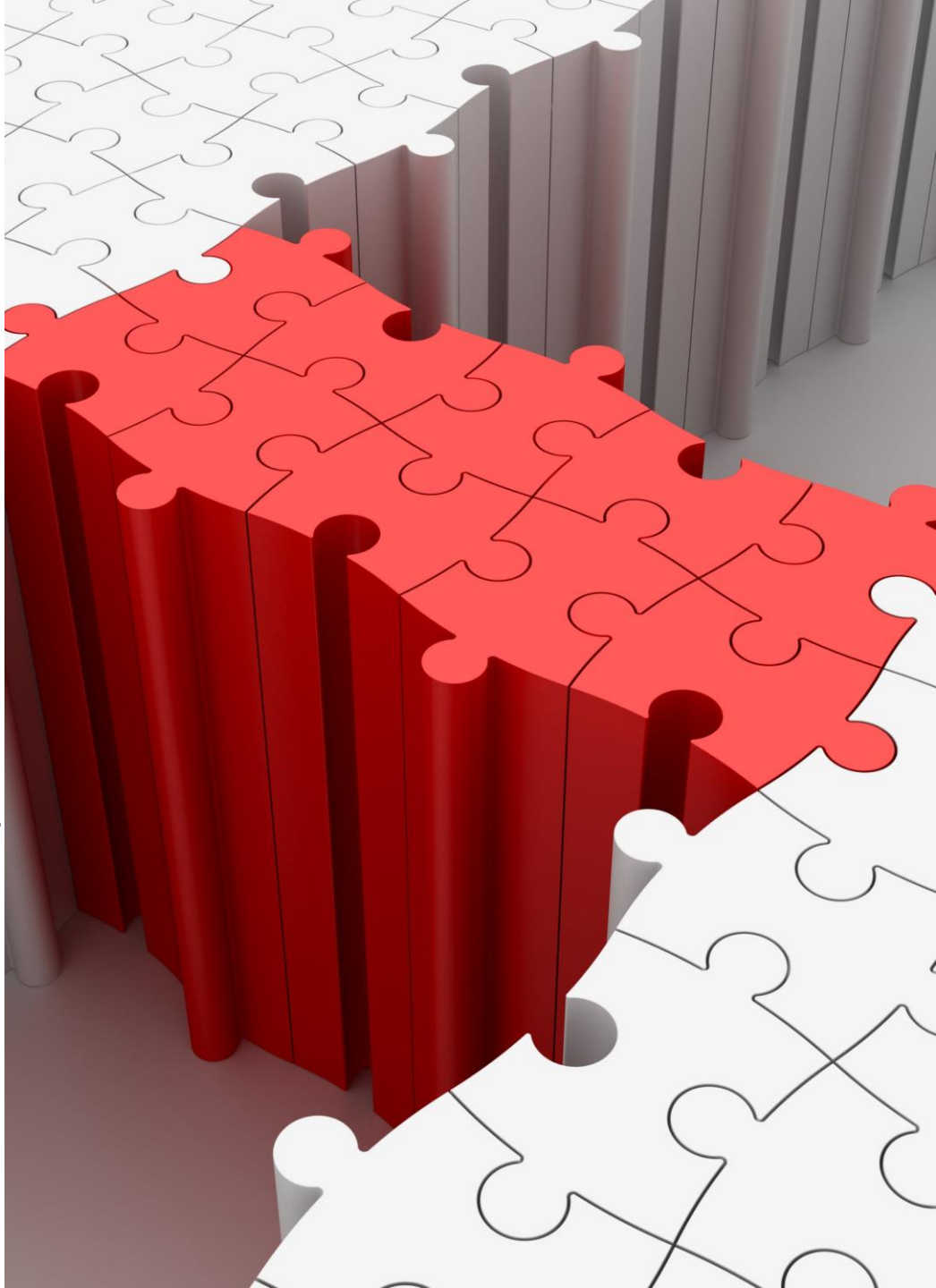
						CADI			Security*			
		MVP - IT	Ideal - IT	MVP - OT	Ideal - OT	A	B	C	I	II	III	IV
Network	Passive	X	X	X		X	X	X		X		
	Active	X	X			X	X	X	X	X		
Application and libraries	Static	X	X			X	X		X	X	X	
	Dynamic		X			X						
Firmware	Static		?		X		X		X			X
	Dynamic		?									
File system	Static	X	X		X	X	X					

* Have potential, but don't necessarily offer support for CADI at this moment

Requirements

Requirement	MVP (IT)	Ideal solution (IT)	CADI Leverancier B	CADI Leverancier A	CADI Leverancier C
Scan frequency	Weekly	Real-time	Offer full-spectrum	?	Quarterly, weekly or daily
Location	On-premise	On-premise	On-premise (or cloud)	On-premise	On-premise
Agents	Yes	Yes	Multiple options available	No	Multiple options available
Ingestion of CBOMs	Yes	Yes	Yes	No	?
Logs	All information surrounding the execution of scans, errors, and results	All information surrounding the execution of scans, errors, and results	All information surrounding the execution of scans, errors, and results	All information surrounding the execution of scans, errors, and results	All information surrounding the execution of scans, errors, and results
Scope	Key (material), crypto primitives, crypto protocols	Idem as for MVP, but also including the discovery of PQC and placing the assets in context (owner, process)	Key (material), crypto primitives, crypto protocols. Context and cross-references are being explored.	Key (material), crypto primitives, crypto protocols.	Key (material), crypto primitives, crypto protocols. Also PQC.
Accuracy	60%	85%	No clear data, as there is no clear ground truth.	Analyses network traffic and claims very high accuracy.	No clear data, as there is no clear ground truth.
Integration	No plug-and-play, but offering advice.	Plug-and-play for well-known products. Tailored solutions for other products.	Integration with many different tools.	No integrations yet, but planning on integrating with CMDB.	Integration with many different tools.

Gaps	Advice
OT environments	Stimulate vendors to include OT
No ground truth	Set-up experiment
Re-inventing the wheel and lack of integration	Sync with other asset management research and tools
Compliance-driven demand	Stronger regulation on cryptographic asset management



Wrap-up

- CADI is a no-regret move
- Any organisation should start with re-using information from security tools and request CBOMs from vendors
- CADI tools are not perfect yet, but we can already start using and integrating them
- Contact us if you want to know more!

Thank you for your attention!