



Atos Cyber Tech Radar

A pragmatic methodology for Industry & Market Trendspotting

Zeina Zakhour
VP, Global CTO Cybersecurity
24/11/2022

 ZeinaZakhour

 @ZeinaZakhour

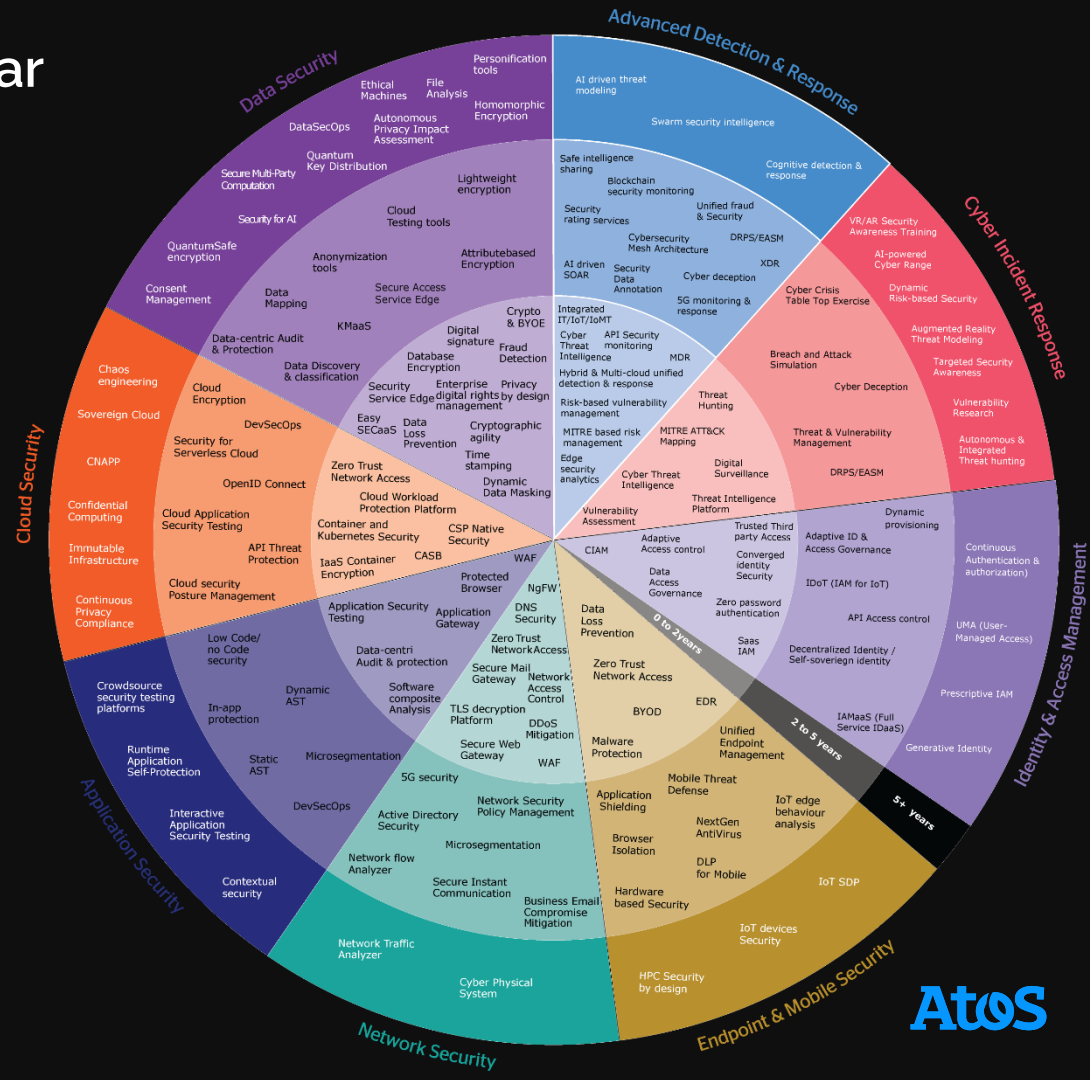


Atos Cybersecurity Tech Radar

“ A tailored tool that helps organizations track, assess and visualize major cybersecurity technology trends.”



Cybersecurity tech radar - Atos



Atos Cybersecurity Tech Radar

150

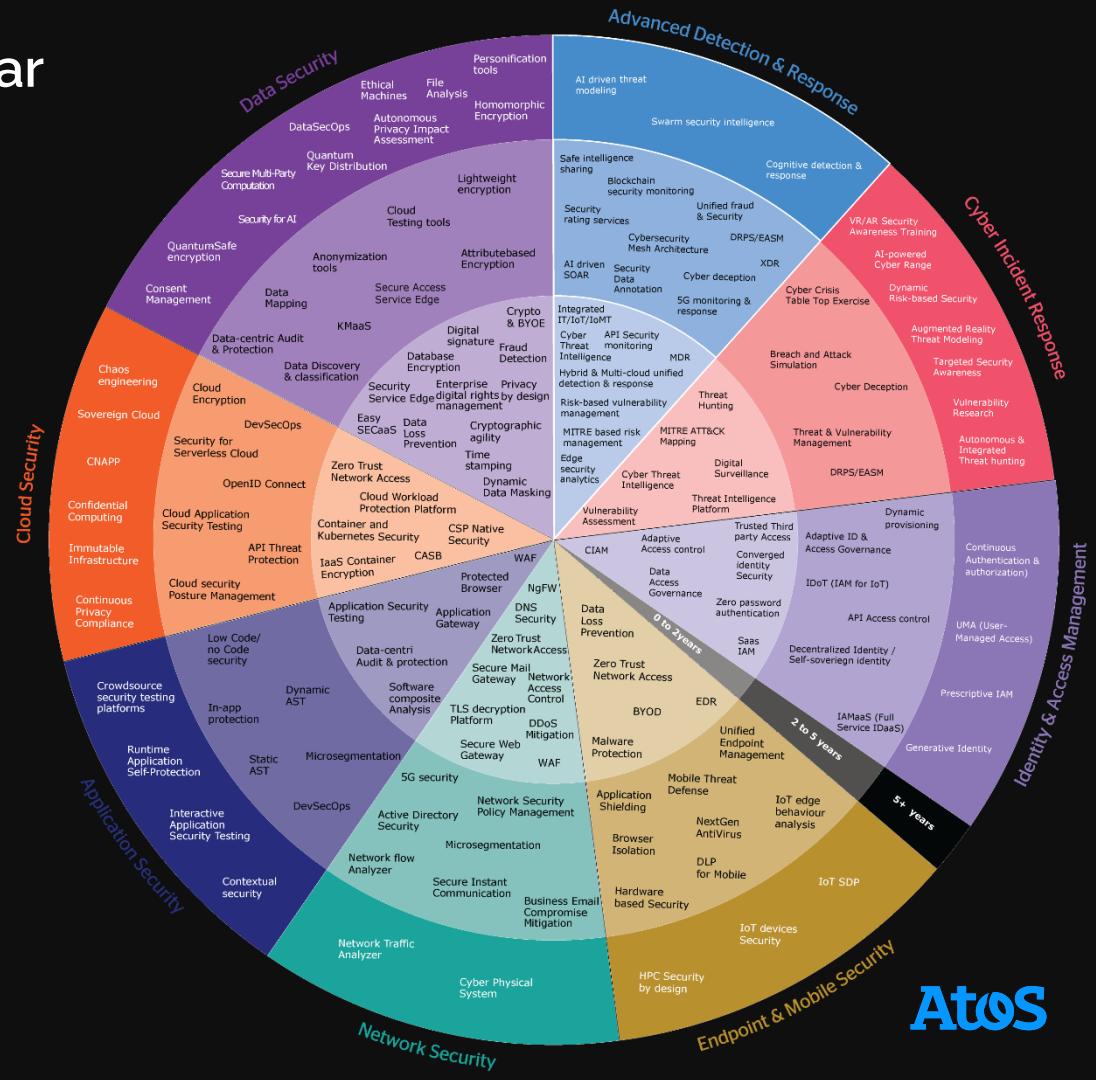
Cybersecurity
Technological Trends

8

Cybersecurity
Domains



Cybersecurity tech radar - Atos



Benefits of a Cyber Tech Radar

Identify current and future disruptions and opportunities created by technology trends

Measure maturity of own technology map and identify risks and blind spots.

Develop an R&D strategy that responds to both the incremental and disruptive innovations identified in the Tech Radar

Provide CIOs and CISOs with a tool that help prioritize cybersecurity strategy roadmap and estimate ROI

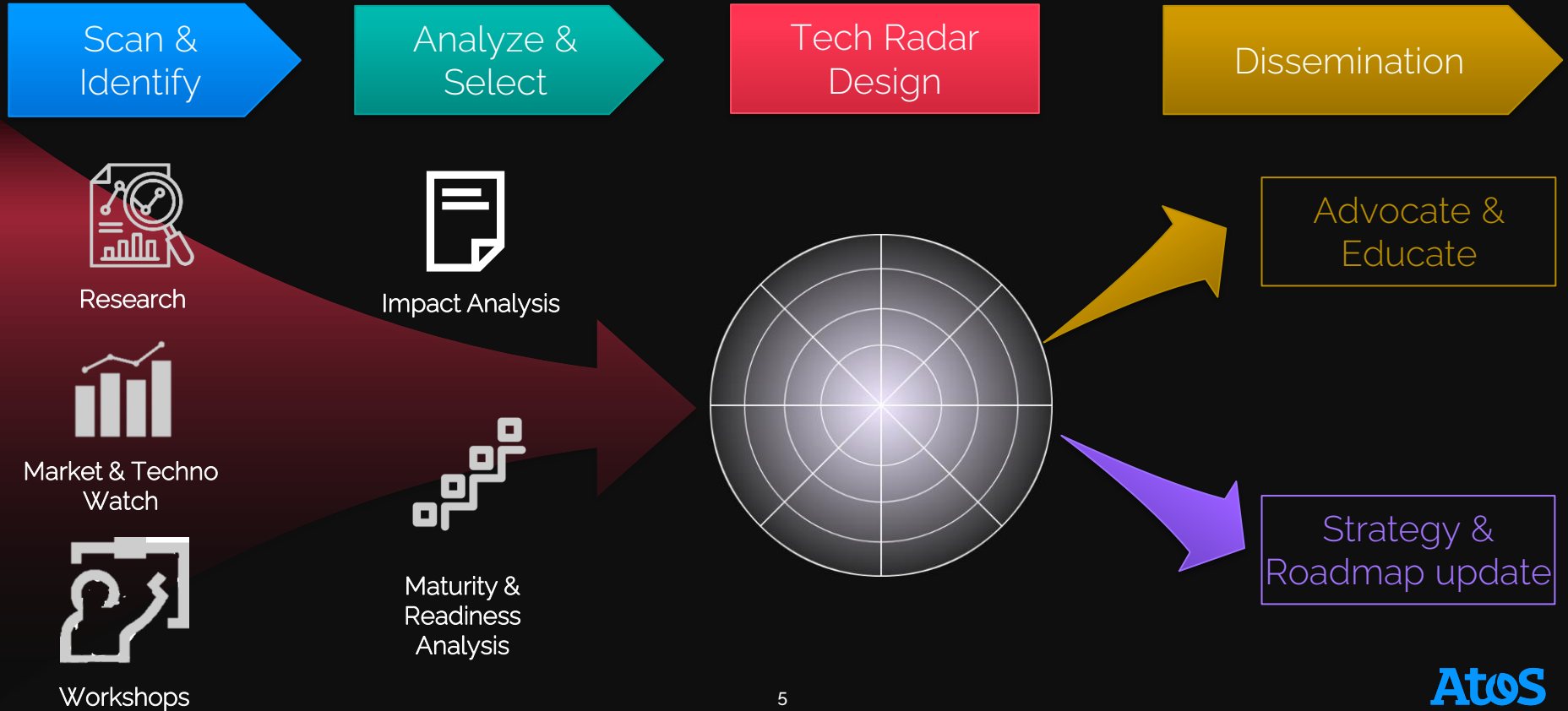
Support Policy Makers in setting priorities for Industrial and R&D Policy development

Early warning tool on evolution of cybersecurity technologies (in terms of maturity & effectiveness) as well as on emerging technologies.

Help organizations in analyzing impact of Regulatory/Legal/economical/Political on technological trends.

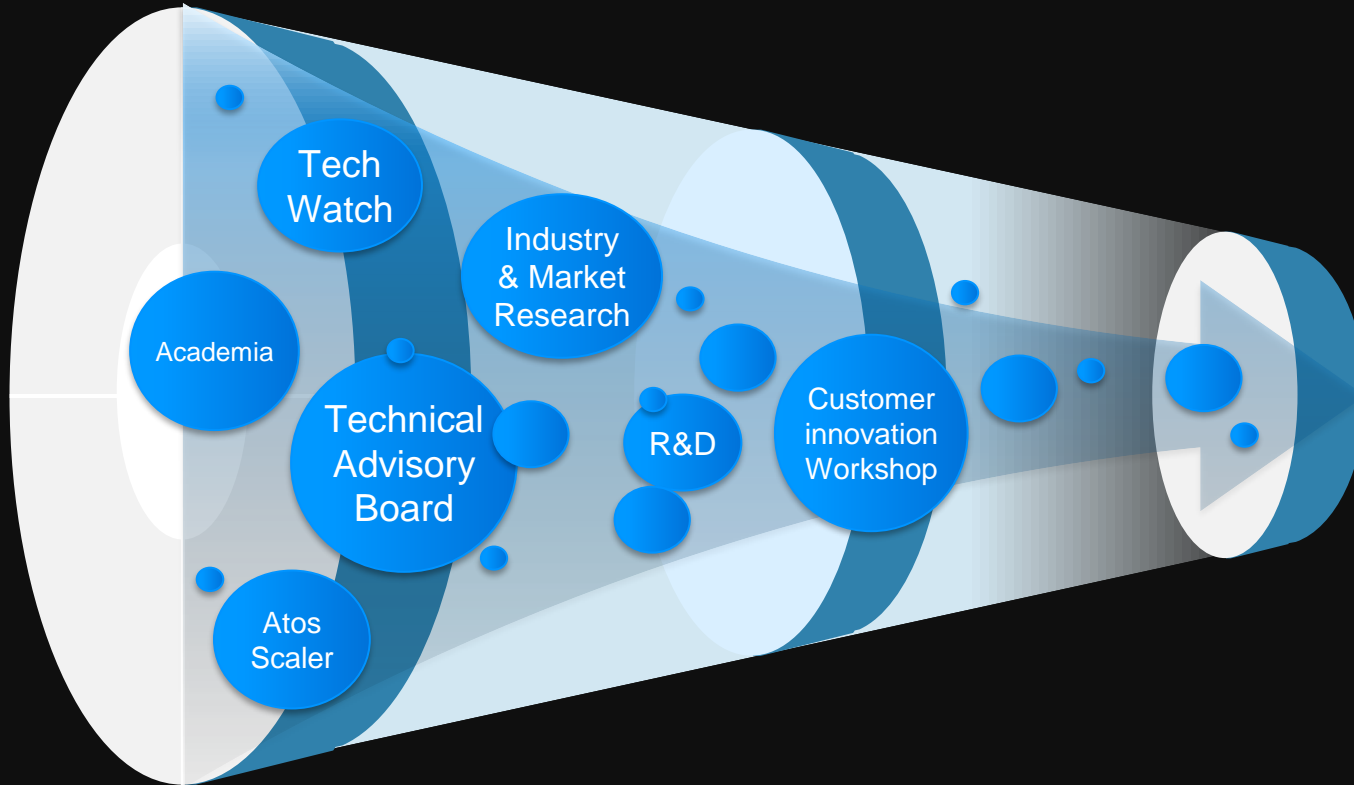
Forward thinking to spot major industry changes and their impact on regional, local, enterprise R&D strategies.

Our Methodology

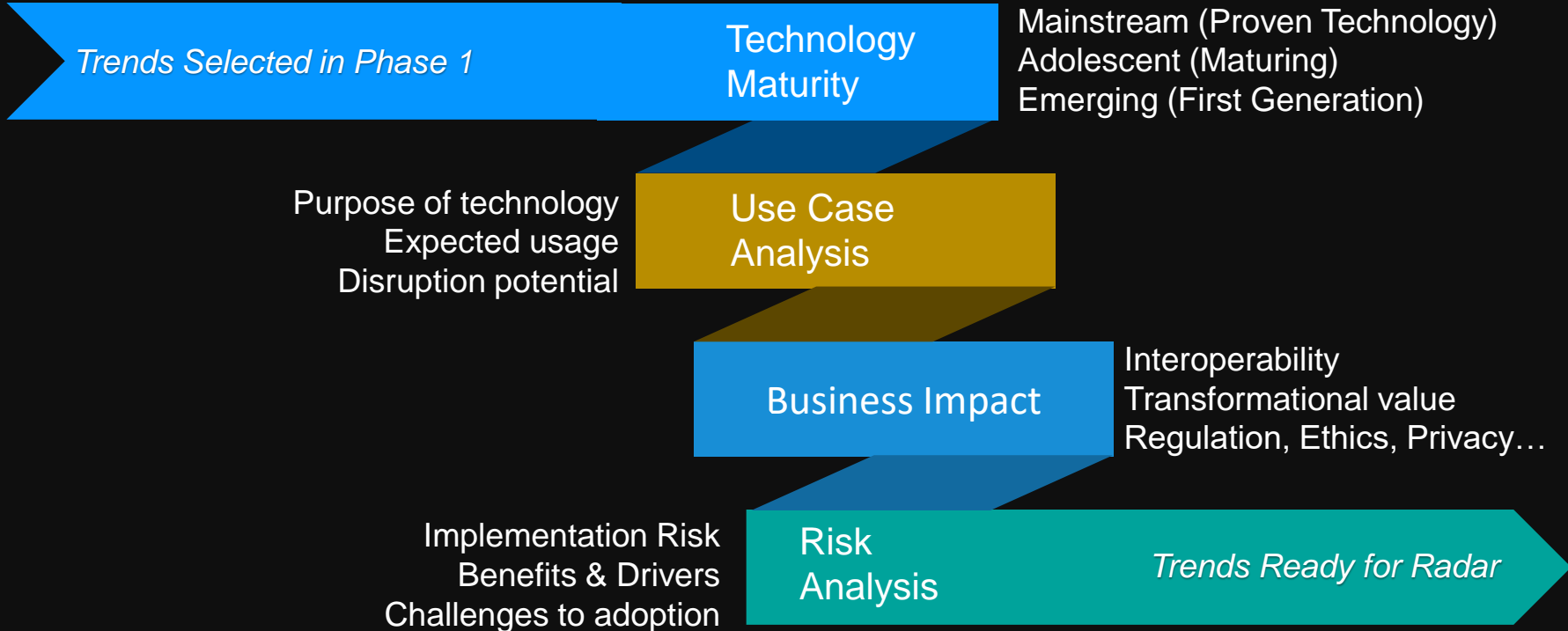


Scan & Identify: Trendspotting & Market Landscape

Key Stakeholders: Champion Experts & CTO Teams



Analyze & Select: Assess the trends and build a cybersecurity Trends repository



Tech Radar Design

8 Quadrants/Domains

Advanced Detection & Response

Cyber Incident Response

Identity & Access Management

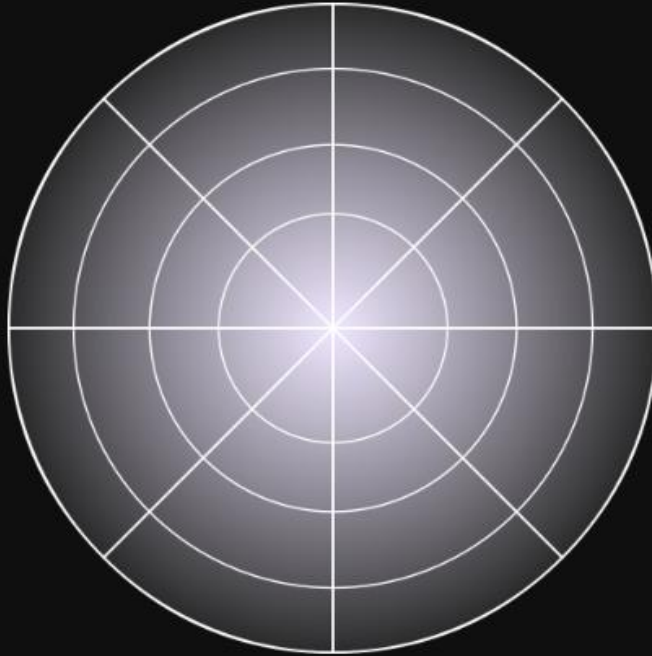
Endpoint & Mobile Security

Network Security

Application Security

Cloud Security

Data Security



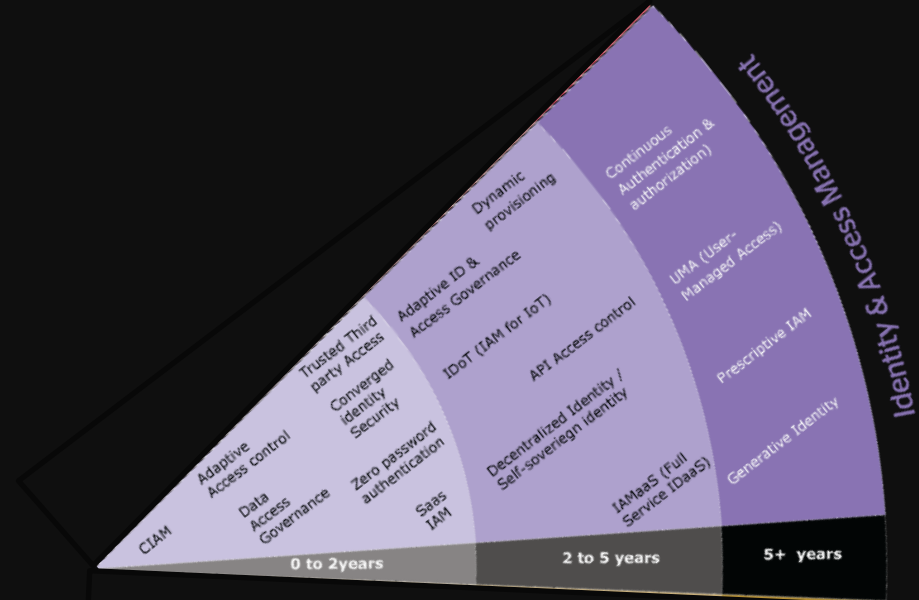
Tech Radar Design

Rings of Maturity

Zero to two years: Mature technologies are either already adopted by most organizations or will be in the next two years. In other words, these technologies have become an integral part of the security strategies of most companies.

Two to five years: Proven technologies are usually adopted in the next two to five years cycle as organizations improve in maturity.

Five years and above: emerging trends will be adopted by the mainstream after approximately five years or more. Still, organizations with a mature cybersecurity level can adopt such emerging trends earlier.



Atos Cybersecurity Tech Radar



● Quantum-Safe encryption

Description: This is Quantum Safe Cryptography (QSC – also referred to as Post-quantum cryptography) which aims to solve the threat particularly on asymmetric or Public-Key cryptography caused by the rise of quantum computing, as it relies on hard-to-solve mathematical problems that can be easily solved with a full-fledged quantum computer.

Use Case:

- Use cases of Quantum Safe Cryptography revolve mainly around replacing current standard cryptographic protocols with new quantum-safe ones that are still in a standardization process. Depending on use cases, plug-in replacement can be required for some protocols in complex cryptographic systems.
- Similarly, time when current cryptographic protocols must be replaced depends on potential short- or middle-term impact of future quantum computers on stored data.

Benefits: Replacing standard cryptographic methods with quantum-safe methods will mitigate the future threat posed by Quantum Computers and provide an opportunity to enhance communication and encryption security.

Target Verticals: Virtually any industry that relies on standard cryptographic methods will be vulnerable once full-fledged quantum computers are available. The adoption would come first on the telecom vertical and then move onwards to other sensitive industries, such as government and defense institutions, banking/finance, healthcare.

Challenges to adoption: Quantum computers are a relatively new technology and a commercially available version is not yet available. At the moment, research and development in this area is very expensive and requires a high degree of knowledge and understanding around other scientific fields, such as mathematics and physics.

Cyber Tech Radar

The Journey & The Maturity Model

Ad hoc or informal approach to trends collection

LEVEL 1

Provide mechanism to collect trends & ideas

Provide trendspotting process

LEVEL 2

Allocate Trendspotting to a dedicated Team

Apply a defined process to identify trends with business impact

Create a visualization to communicate and organize trends

LEVEL 3

Integrate trendspotting with project & EA Tools

Apply Design Thinking to develop responses to trends

Use Tech Radar to identify bling spots in roadmap and set priorities

LEVEL 4

Drive Ecosystem trend discovery and collective responses

Include Use Case and Value creation Analysis in the Trend Impact Analysis

Integrate PESTEL Analysis in Tech Radar Development

Measure business outcomes with specific and measurable results that the tech trend will provide

Leverage Automation & AI

LEVEL 5

Atos Cyber Tech Radar

An essential tool to infuse cyber innovation & improve performance

Open dialog on
strategic
technologies for
Europe's
cybersecurity
roadmap

COLLABORATION

Measure
maturity and
efficiency of
Cyber
Roadmap/
Strategy

EFFICIENCY


Help multi-
annual R&D
Program
strategically
adapt to the fast-
changing
industry

AGILITY

Questions

Thank you!

For more information please contact:
zeina.zakhour@atos.net

 ZeinaZakhour

 @ZeinaZakhour

Atos is a registered trademark of Atos SE. November 2022. © 2022 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

