Swiss Post Cybersecurity

Detect and Adapt: Building Resilience Through Cloud Detection

Swiss Cyber Storm, 28.10.2025

01
Presentation & Agenda

Swiss Post Cybersecurity

Arthur VUAGNIAUX

Security Engineer – Detection Team Leader

Former Cloud Team Leader

arthur.vuagniaux@swisspost-cybersecurity.ch

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED SECURITY OPERATIONS ANALYST ASSOCIATE

Microsoft CERTIFIED IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

splunk> CERTIFIED Splunk Core Certified User

aws certified Cloud Practitioner FOUNDATIONAL

Agenda

1. Presentation & Agenda

2. Short Reminder(s)

3. Let’s build our solution
   1. Solution Scope
   2. Solution Architecture
   3. Solution Cost

4. Conclusion

02
Short Reminder(s)

Short Reminder(s) – What do we call ‘Resilience’ in cybersecurity

Cyber resilience refers to an organization's ability to **anticipate, withstand, recover from, and adapt to** adverse cyber events such as attacks, breaches, or system failures.

Key Points to retain:

- **Anticipation**: Understanding potential threats and preparing for them.
- **Withstanding**: Maintaining core operations during an attack.
- **Recovery**: Restoring systems and data quickly and effectively.
- **Adaptation**: Learning from incidents to improve future defenses.

Short Reminder(s) – Current Context

28% more

cyber incident between 2023 and 2024

70% of

Swiss companies have increased their cybersecurity budgets.

21.5%

growth rate

$400

million investment to strengthen Switzerland's digital future

70% of

Swiss companies have increased their cybersecurity budgets.

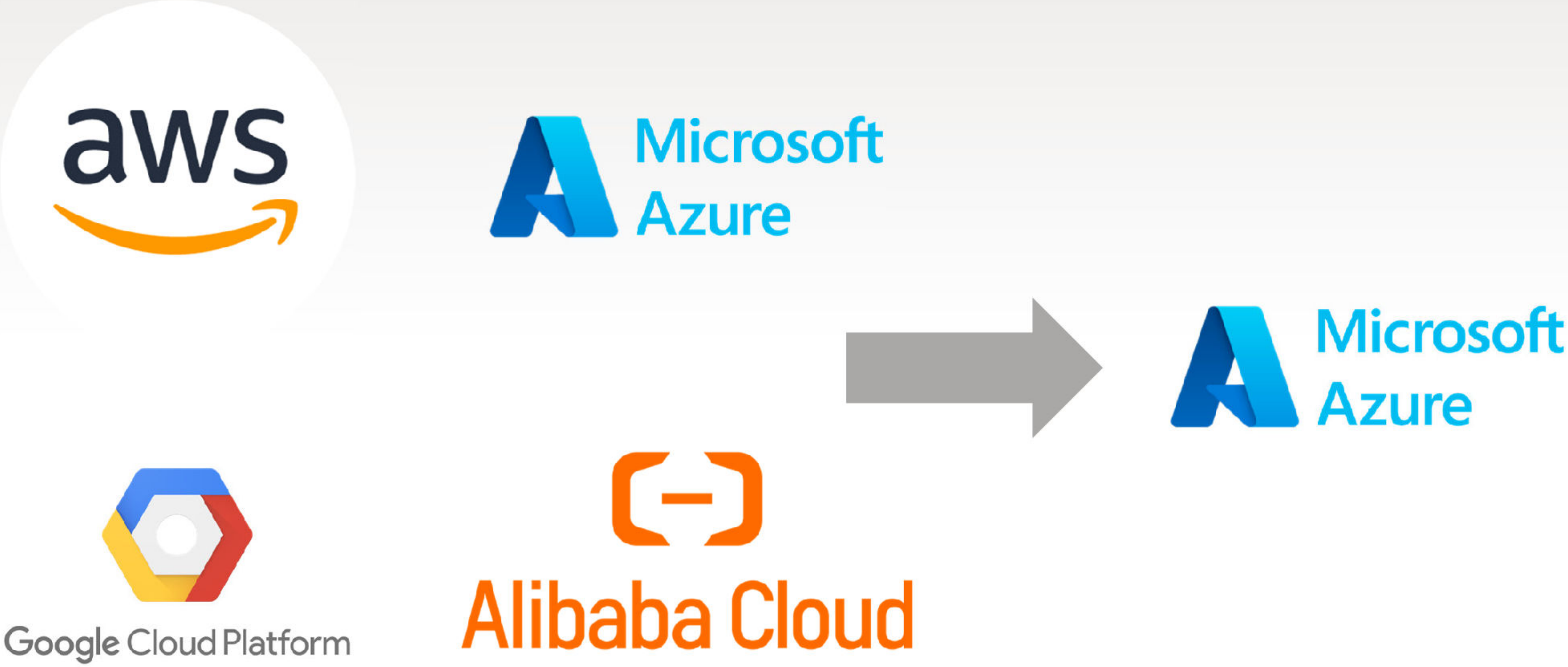
03

Let’s Build our solution

03-1

Solution Scope

Solution Scope: Cloud Provider



Solution Scope: Why Azure and not AWS ?

- Two **good cloud providers** but (*in my honest opinion*):
  - **More products to do this exercise on Azure** (not spoiling the presentation now).
  - One **major tools specifics** tools exist on Azure without equivalent on AWS.
    - Automatic correlation of alerts across components.
    - Unified visibility into incidents through a centralized portal.

- Doing it from Azure, allow also to have a way of protecting our other Cloud Assets.

- Azure is used more than AWS.

- Final argument: that’s my presentation :)

Solution Scope: Microsoft Cloud Stack Overview

Microsoft Sentinel

Microsoft Entra ID & Protection

Microsoft Defender for Cloud

Microsoft Intune

Microsoft 365 (ex Office 365)

Microsoft Purview

Microsoft Defender for Identity

Microsoft Defender for IoT

Microsoft Defender for Cloud Apps

Microsoft Defender for Office 365

Microsoft Defender for Endpoint

03-2

Solution Architecture

Solution Architecture – Microsoft Purview

- **Data Loss Prevention (DLP)**: Deploy policies to monitor and block sensitive data transfers (including third-party apps).

- **Classification and Labeling**: Use Purview Information Protection for automatic sensitive data classification.

Goal: Prevent data loss and maintain regulatory compliance.

- **Insider Risk Management**: Detect risky behaviors (data exfiltration, misuse of AI tools).

- **Adaptive Protection**: Dynamically restrict access for high-risk users.

Goal: Prevent data loss and maintain regulatory compliance.

Solution Architecture – Microsoft Entra ID & Entra ID Protection

- **MFA and Conditional Access**: Enforce Multi-Factor Authentication and dynamic policies to reduce unauthorized access risks.
- **Privileged Identity Management (PIM)**: Apply least privilege with just-in-time access for admin roles.
- **Identity Protection**: Detect risky sign-ins and anomalies (e.g., impossible travel, anonymized IPs, password spray attacks).
- **Resilient Architecture**: Use Active-Active and cell-based architecture to avoid single points of failure.
- **Recovery Plan**: Backup critical configurations (RBAC, Conditional Access) for quick restoration.
- **Zero Trust Principles**: Explicit verification, privilege segmentation, and strong authentication for all

Goal: Ensure identity security and availability during crises.

Solution Architecture – Microsoft Defender(s)

Microsoft Defender for Cloud

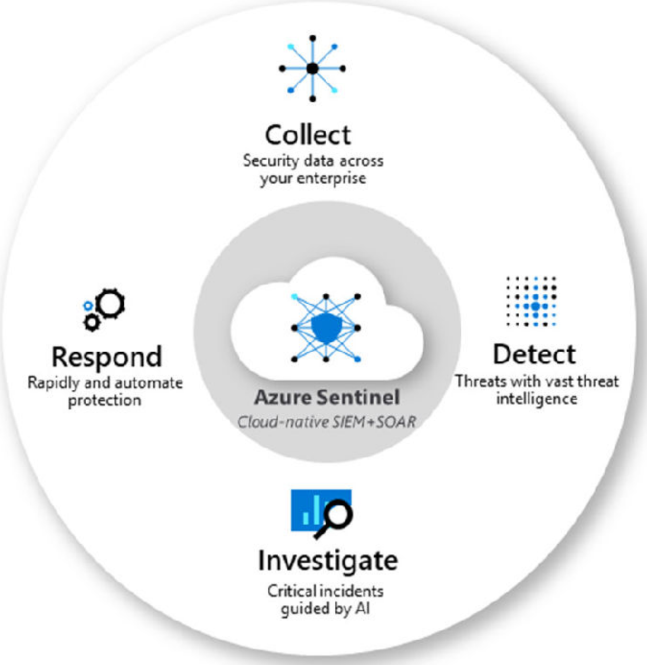
Microsoft Defender for Identity

Microsoft Defender for Office 365

Microsoft Defender for Endpoint

Goal: Detect, contain, and remediate threats quickly.

Solution Architecture – Microsoft Sentinel


Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

Collect:

- Content Hub
- Data Connectors

Detect:

- Analytics Rules (Scheduled, NRT or Fusion)
- Watchlist

Investigate:

- Workbooks
- Hunting Queries
- Notebooks
- Entity Behavior
- Threat Intelligence

Respond:

- Automation Rules
- Playbooks (Logic Apps)

Goal: Build a resilient detection and response backbone that minimizes impact and accelerates recovery.

Solution Architecture – Microsoft XDR

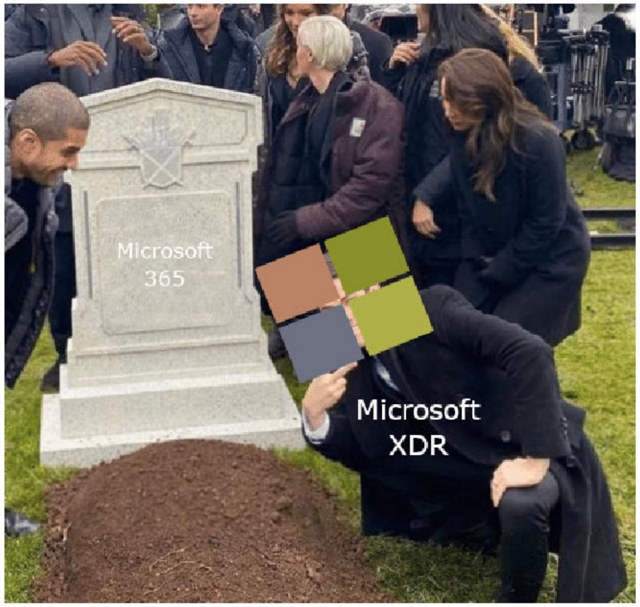
A brand new product → **New name** for Microsoft 365

Release 19th April 2024

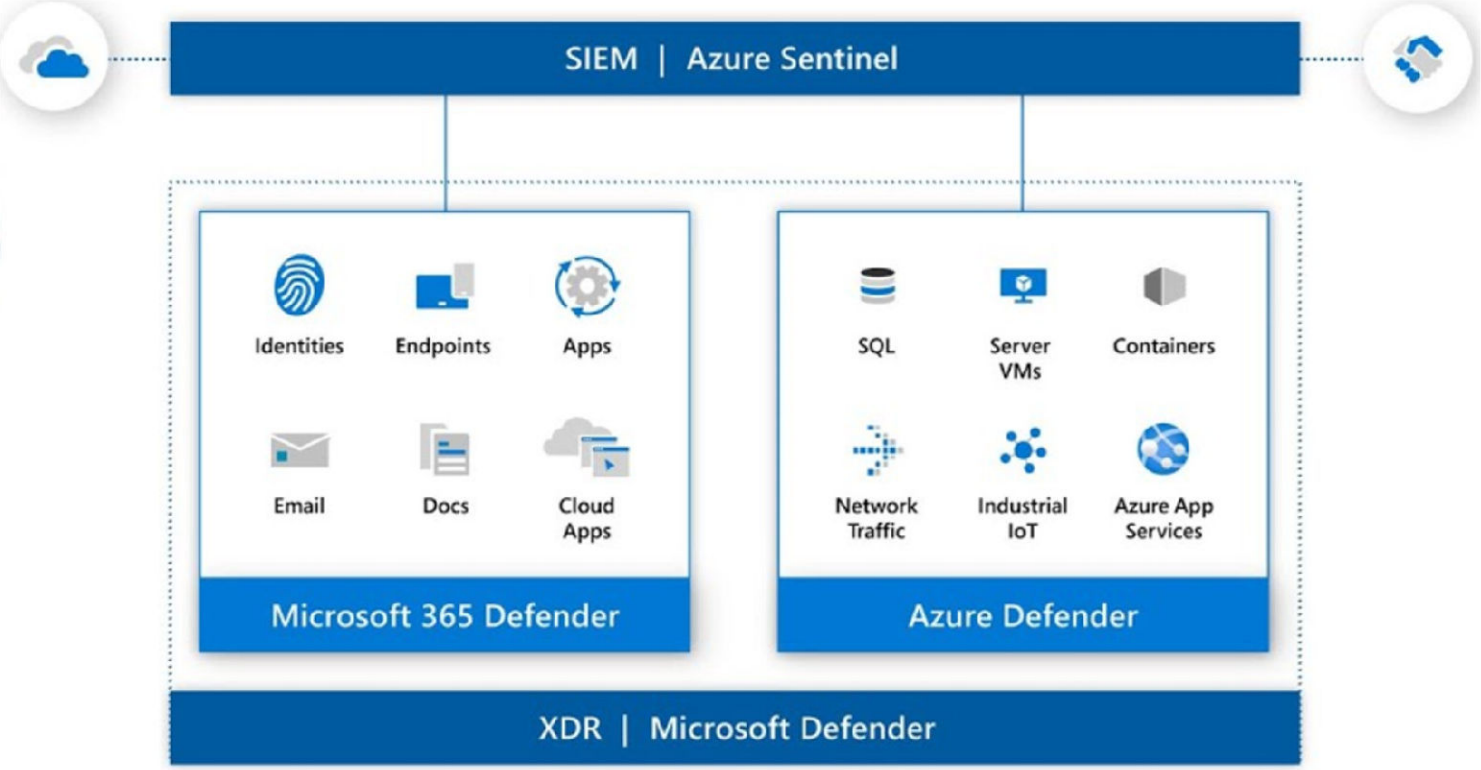
One **Unified** Console for (almost) all products:

- **Cross-product single pane of glass** in the Microsoft Defender portal
- **Combined incidents queue**
- **Cross-product threat hunting**
- **Self-healing** for compromised devices, user identities, and mailboxes (a little bit of IA)

To simplify for us: Sentinel and Defender into a single console



Solution Architecture – Our perfect solution



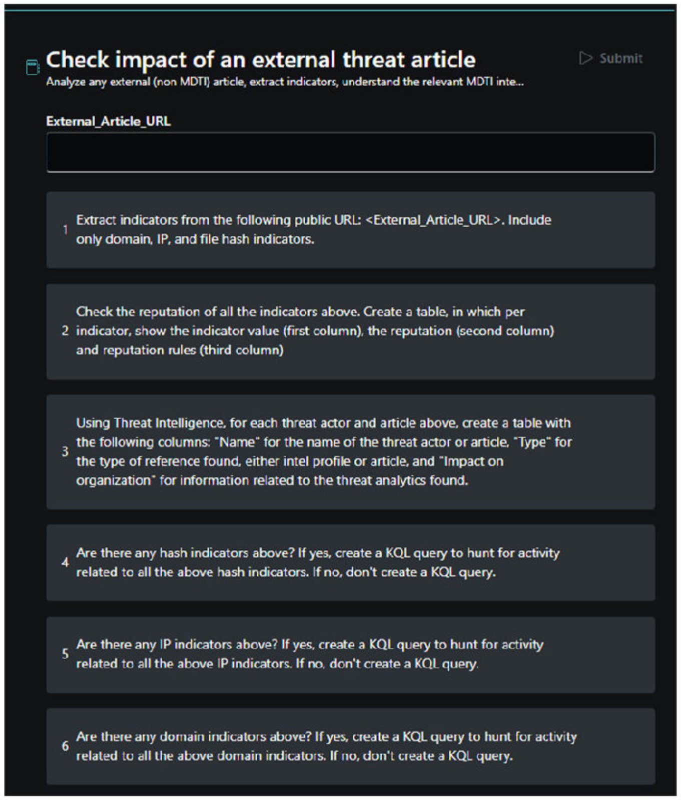
Solution Architecture – Microsoft Copilot for Security

- **Generative AI-powered security solution** that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale.

- **Standalone experience** and seamlessly integrates with others Microsoft products

- Automation:
  - **Triage and investigation**: SOC analysts can reverse engineer scripts, generate KQL queries, and investigate incidents faster using natural language.
  - Generates clear, actionable summaries and step-by-step remediation guidance, reducing recovery time.

- **Copilot for Security =/= Copilot for Microsoft 365 =/= Copilot**



Check impact of an external threat article

Analyze any external (non MDTI) article, extract indicators, understand the relevant MDTI inte...

External_Article_URL

1 Extract indicators from the following public URL: <External_Article_URL>. Include only domain, IP, and file hash indicators.

2 Check the reputation of all the indicators above. Create a table, in which per indicator, show the indicator value (first column), the reputation (second column) and reputation rules (third column)

3 Using Threat Intelligence, for each threat actor and article above, create a table with the following columns: "Name" for the name of the threat actor or article, "Type" for the type of reference found, either intel profile or article, and "Impact on organization" for information related to the threat analytics found.

4 Are there any hash indicators above? If yes, create a KQL query to hunt for activity related to all the above hash indicators. If no, don't create a KQL query.

5 Are there any IP indicators above? If yes, create a KQL query to hunt for activity related to all the above IP indicators. If no, don't create a KQL query.

6 Are there any domain indicators above? If yes, create a KQL query to hunt for activity related to all the above domain indicators. If no, don't create a KQL query.

Goal: Accelerate human decision-making and automate complex recovery steps during and after incidents.

Solution Architecture – Solution and Resilience

If we are taking back our points:

Anticipation:

- Defender XDR, Sentinel and Copilot for Security.

Withstanding:

- Entra ID, PIM and Identity Protection.

Recovery:

- Backup and Purview.

Adaptation:

- Defender, Copilot for Security.

03-3

Solution in real life

Solution Architecture - Cost

Pillar	Microsoft Product	Pricing (CHF)
Anticipation	*Microsoft Defender for Cloud*	Free for 30 days, then billed per protected resource (CSPM, workloads, etc.)
	Microsoft Sentinel	~0.14 CHF per GB of ingested data
	Microsoft Copilot for Security	Included in some E5 plans or usage-based via SCU (approx. 4 CHF/hour provisioned, 6 CHF/hour overage)
Withstanding	*Microsoft Defender XDR Suite*	~10.92 CHF per user/month
	Microsoft Entra Suite	~10.70 CHF per user/month
Recovery	*Azure Backup*	Billed based on volume and frequency (calculated via Azure Pricing Calculator)
	Microsoft Purview Suite	~10.70 CHF per user/month
Adaptation	*Microsoft Copilot for Security*	Included or usage-based via SCU (same as above)
	Microsoft Learn / Training	Free or included in Microsoft 365 subscriptions

Solution Architecture - Solution

Start by ask yourself:

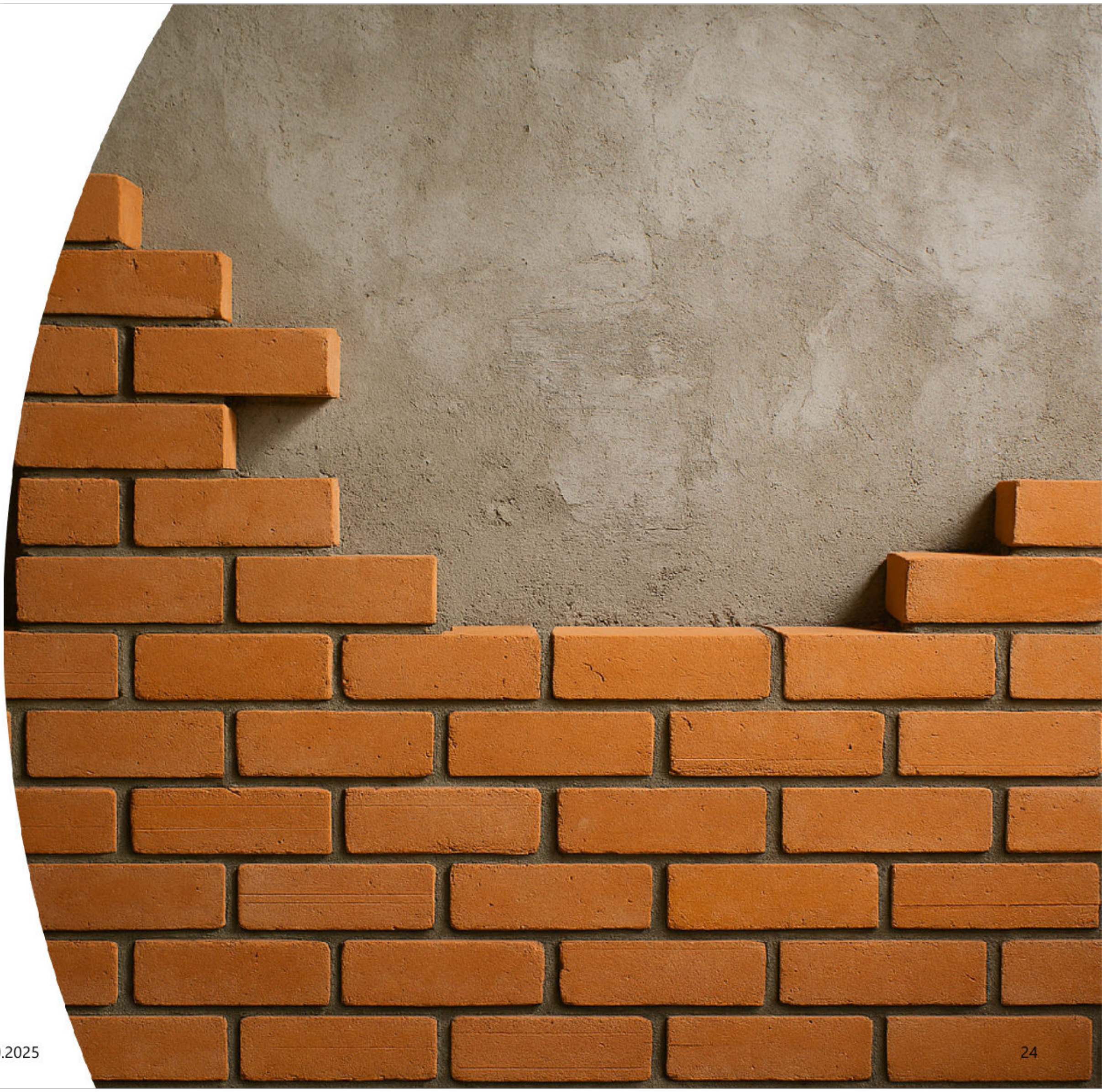
- *Do I really need that product ?*
- *Would it cost me less to take some global specific license ?*
- *Do I need everything to make it work for me ?*

Then:

Scope what you want to cover.

Scope your needs

Finally: **Start little, this is also a marathon.**
Build bricks by bricks



04

Conclusion

Conclusion: Con points

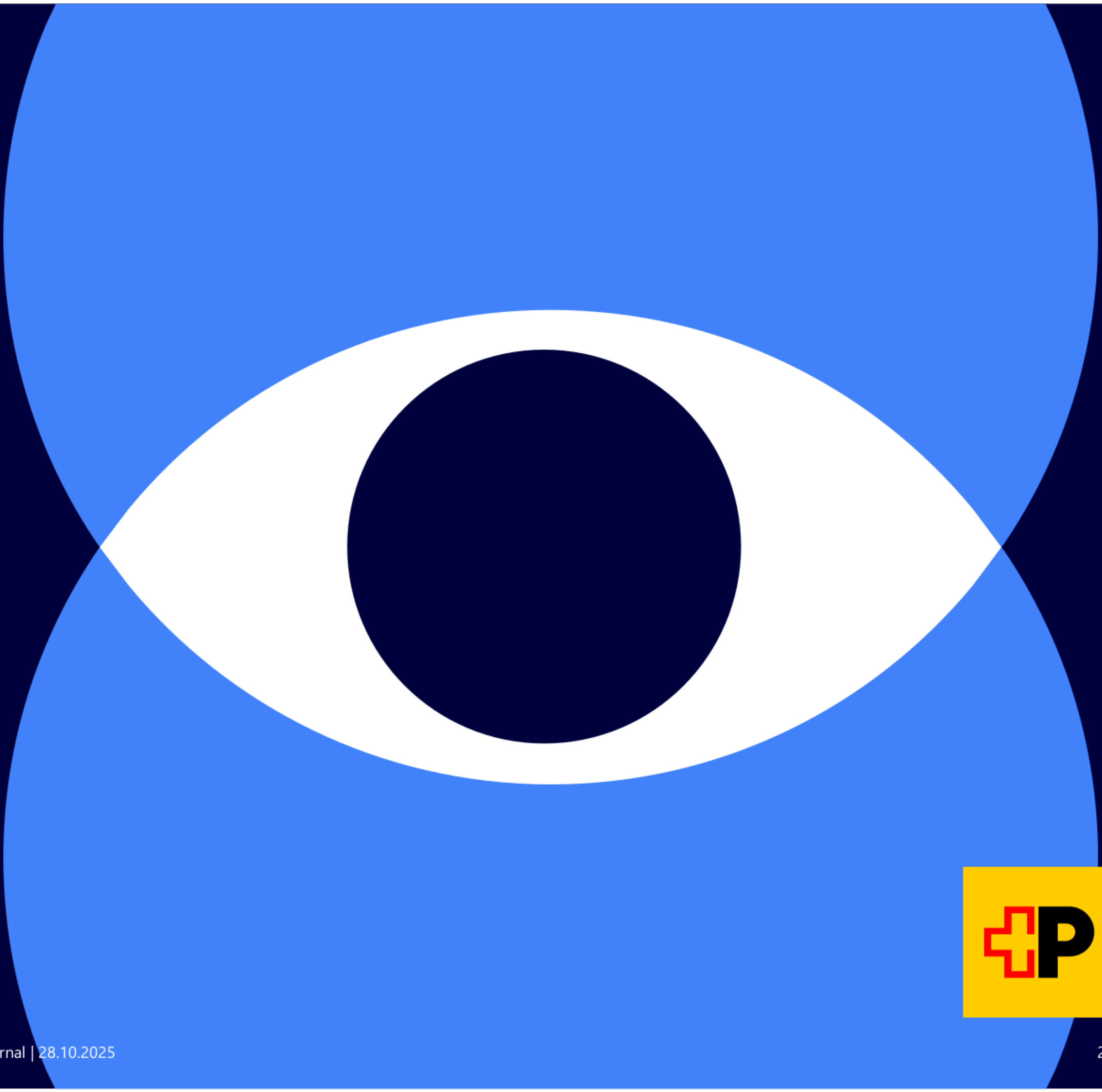
Resilience is an **Ouroboros**:

- Continuous Cycle of Defense and Adaptation.
- Self-Healing after Incidents.
- Balance between Chaos and Order.
- Holistic and Systemic Thinking.

Build your own Resilience (hopefully with Cloud) and adapt every day

Swiss Post Cybersecurity

Thank you
Danke
Merci
Grazie



Appendix

Sources

- **NIST** - https://csrc.nist.gov/glossary/term/cyber_resiliency
- **IBM (What is cyber resilience)** - https://www.ibm.com/think/topics/cyber-resilience
- **Rapport PWC 2023** - https://www.pwc.ch/fr/centre-de-presse/la-nouvelle-etude-pwc-cloud-business-survey-2023.html
- **RTS - Investissement dans le cloud** -https://www.rts.ch/info/economie/2025/article/microsoft-investit-400-millions-en-suisse-pour-booster-le-cloud-et-l-ia-28901924.html
- **CIO online** - https://www.cio-online.com/actualites/lire-21-de-croissance-pour-le-cloud-public-en-2025-selon-gartner-15999.html
- **Loyco** - https://www.loyco.ch/actualites/tendances-2025-en-cybersecurite-en-suisse/
- **OFCS - Rapport annuel 2024** – Office fédéral de la cybersécurité (OFCS) - www.ncsc.admin.ch
- **Princing Calculator** - https://azure.microsoft.com/en-us/pricing/calculator/?service=azure-sentinel
- **Security Copilot** - https://learn.microsoft.com/en-us/copilot/security/developer/cost-considerations / https://www.microsoft.com/en-us/security/pricing/microsoft-security-copilot/
- **Defender for Cloud** - https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
- **Entreprise Security Suite** - https://www.microsoft.com/en-us/security/pricing/enterprise/security-suites
- **Entra id** - https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing
- **Microsoft Learn** - https://learn.microsoft.com/en-us/training/support/plans
- **Prompt - Security Copilot** - https://learn.microsoft.com/en-us/copilot/security/using-promptbooks