# Confidential Computing for Sensitive Data Analysis: The EOSC-SIESTA Approach

Alvaro Lopez, Andres Heredia, Viet Tran
viet.tran@savba.sk

Funded by the European Union

ISCG 2026
15-20 March 2026

# SIESTA in a nutshell

- HORIZON-INFRA-2023-EOSC-01-06 call
- Duration: 1st Jan 2024 – 31st Dec 2026
- 12 partners (ES, IT, FR, SK, DK, SE, NL)
  - Academic and Research: CSIC, IISAS, INSERM, ISI, CNRS, ULE, SRU, NRU
  - Law: Javier de la Cueva
  - SMEs & Industry: Cendio, interWAY, Predictia
  - Statistical offices: INE

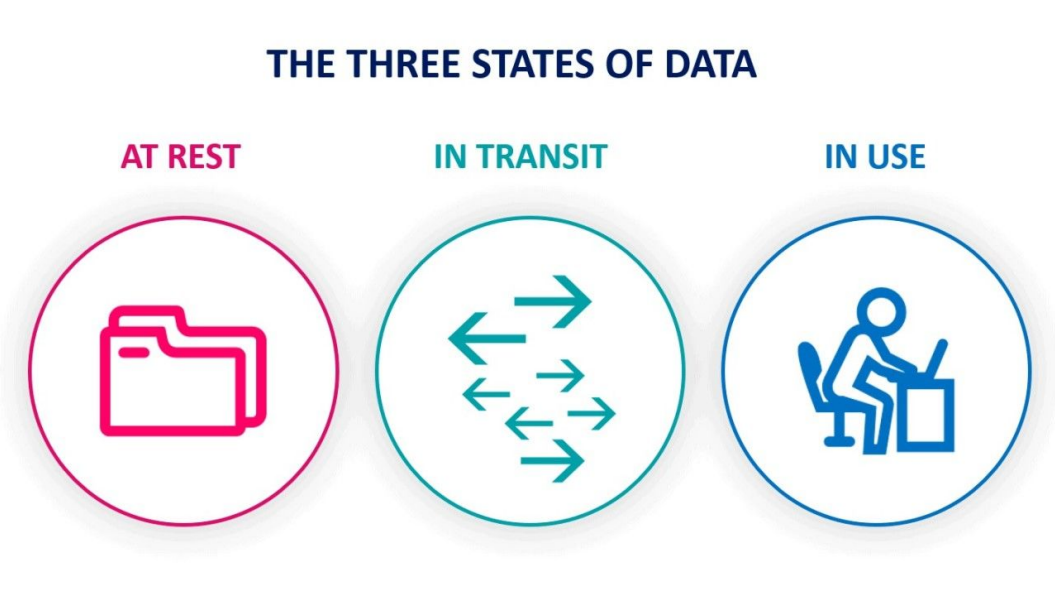
https://cordis.europa.eu/project/id/101131957

Funded by the European Union

ISCG 2026
15-20 March 2026

# Where we started: motivation

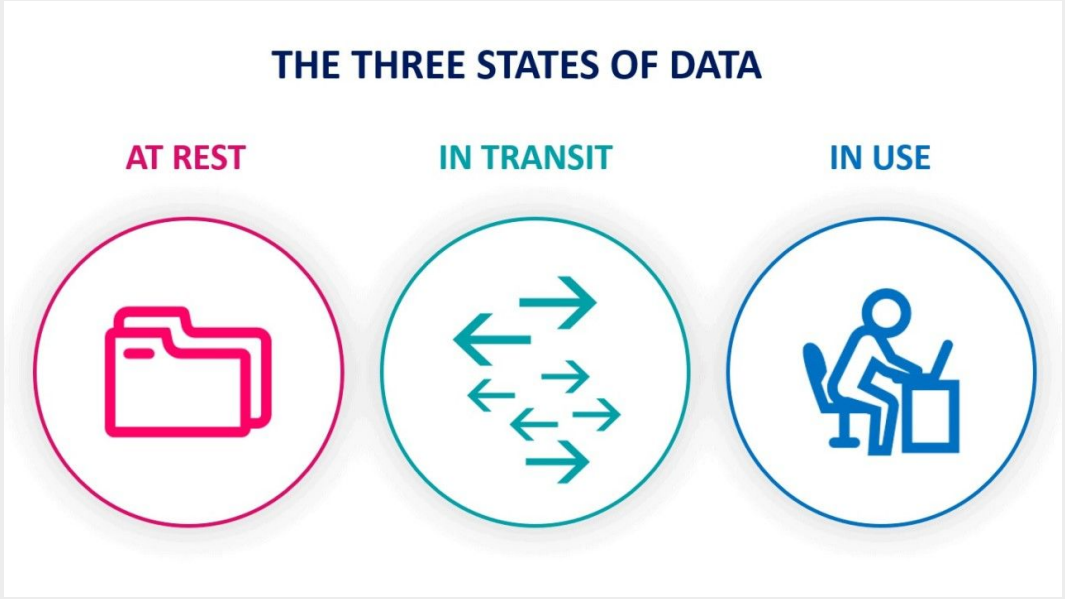
- To create a platform that enables researchers the creation of **secure** and **confidential** environments where to perform **sensitive** data analytics.
- To secure data across all states:
  - At rest: Encryption of stored databases and archives.
  - In motion: Protecting data as it traverses public or private networks
  - In use: Ensuring security while data is actively being accessed or modified.




Funded by the European Union

# Where we started: motivation

- Data **in use** at risk!
- Traditional security is not enough in the cloud
  - Memory dump attack
  - Memory replay
  - DMA Attack
  - Side channel
  - Cold boot attack




Funded by the European Union

# Confidential computing backbone: TEEs

- A trusted execution environment (TEE) is a secure area of a processor.
- Hardware-based memory encryption that isolates application code and data while in use.
- Every manufacturer implements this in their own way:
  - **AMD:** Secure Encrypted Virtualization (SEV), Secure Nested Paging extension (SNP)
  - **ARM:** TrustZone
  - **IBM:** Secure Service Container, formerly zACI
  - **Intel:** Trusted Execution Technology (TXT), Software Guard Extensions (SGX)
  - **RISC-V:** MultiZone Security Trusted Execution Environment


Funded by the European Union

# AMD SEV-SNP

- Ram memory is encrypted using dedicated, specialized hardware located inside the SOC memory controllers.
- AES **128 bits** engine.
- Keys are managed by an AMD Secure Processor (ARM Cortex-A5)
- Each key is generated using dedicated hardware that follows the NIST SP 800-90 recommendations at each reset cycle.

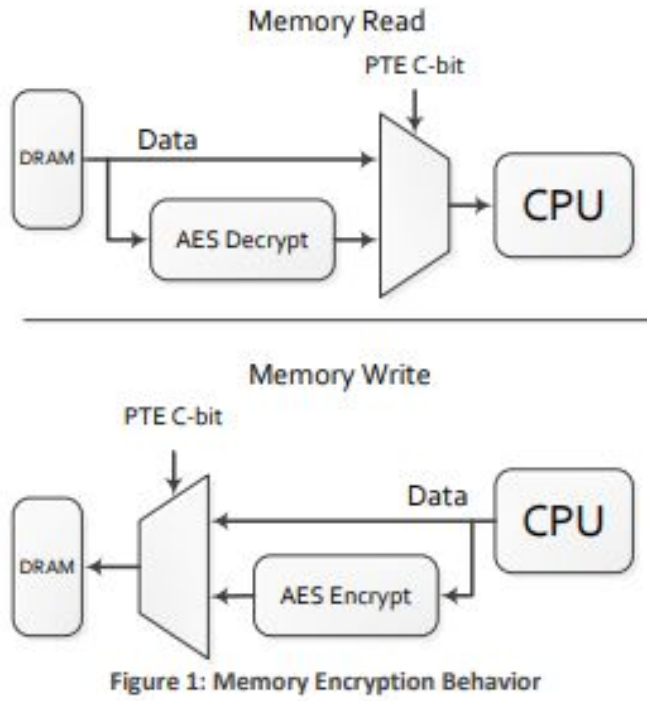



**Figure 1: Memory Encryption Behavior**

Source: Kaplan, David, Jeremy Powell, and Tom Woller. "AMD memory encryption." *White paper* 13 (2016): 12.

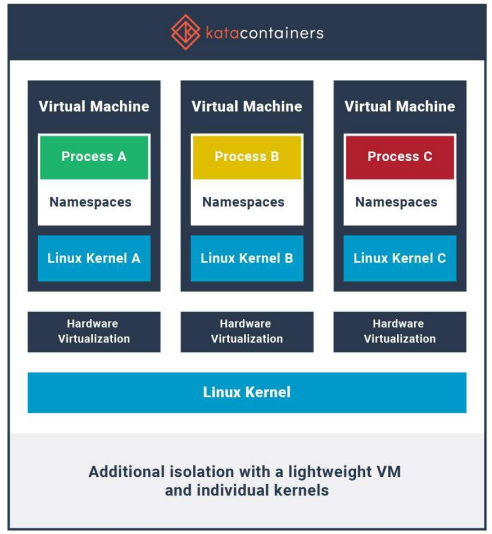
**Funded by the European Union**

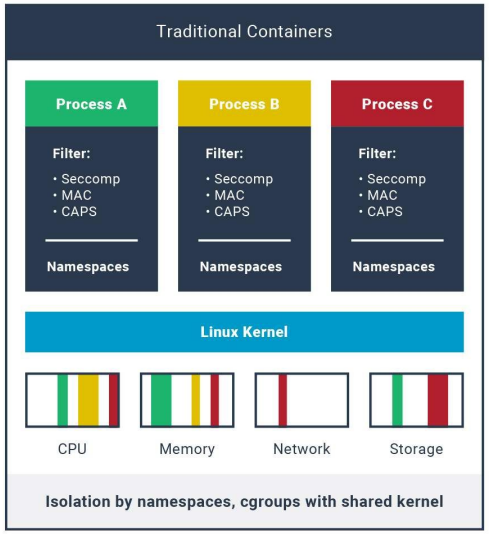
eosc | SIESTA

# CONFIDENTIAL CONTAINERS

Kata containers

"Confidential Containers is an open source community working to enable cloud native confidential computing by leveraging Trusted Execution Environments to protect containers and data" [confidentialcontainers.org]



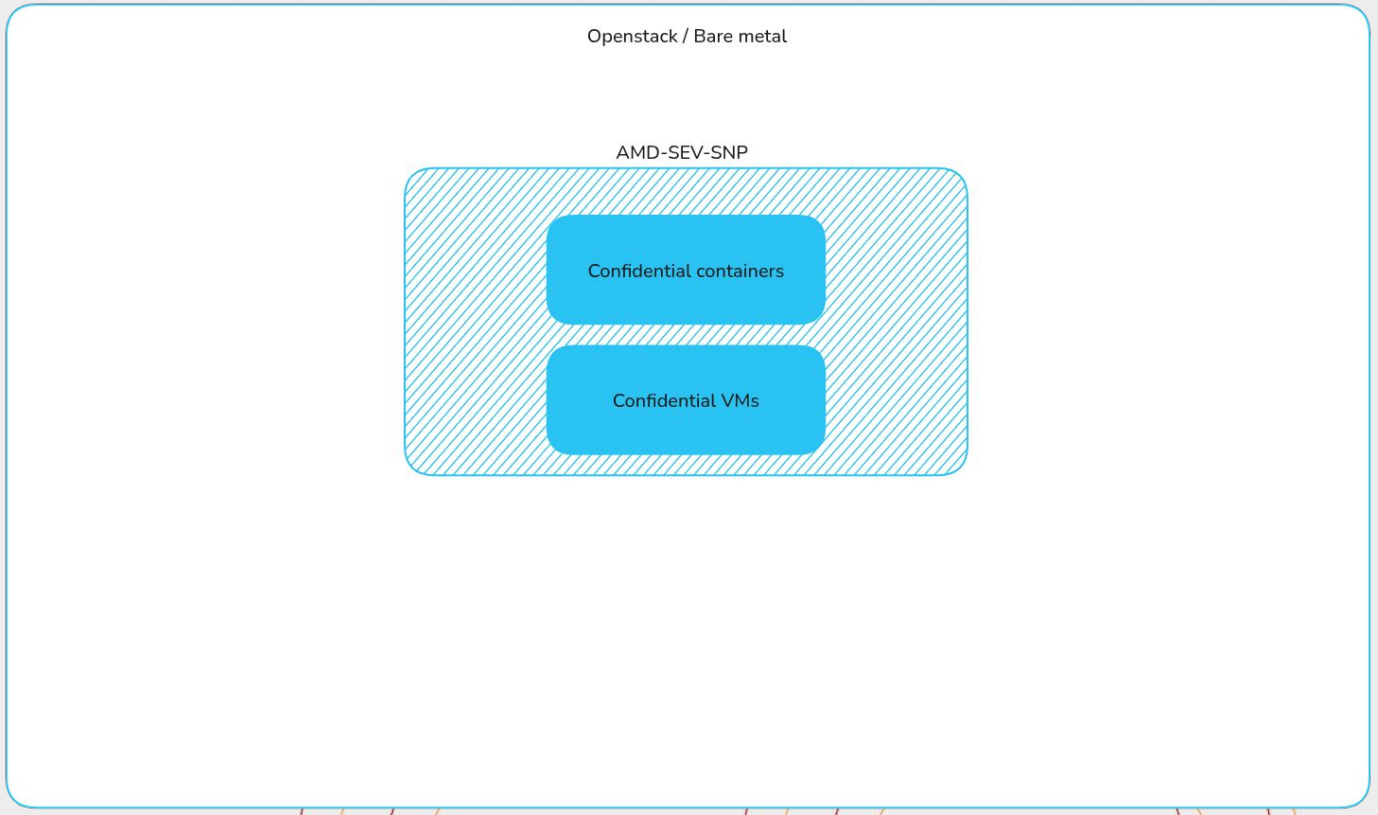

Funded by the European Union

ISCG 2026
15-20 March 2026

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - How do I know if the platform has not been tampered?
  - Is the code running in the platform safe to run?
  - Is my data secure?
  - How can I control who access or runs what, and where?
  - Is it scalable?
  - Is it replicable?
  - etc.

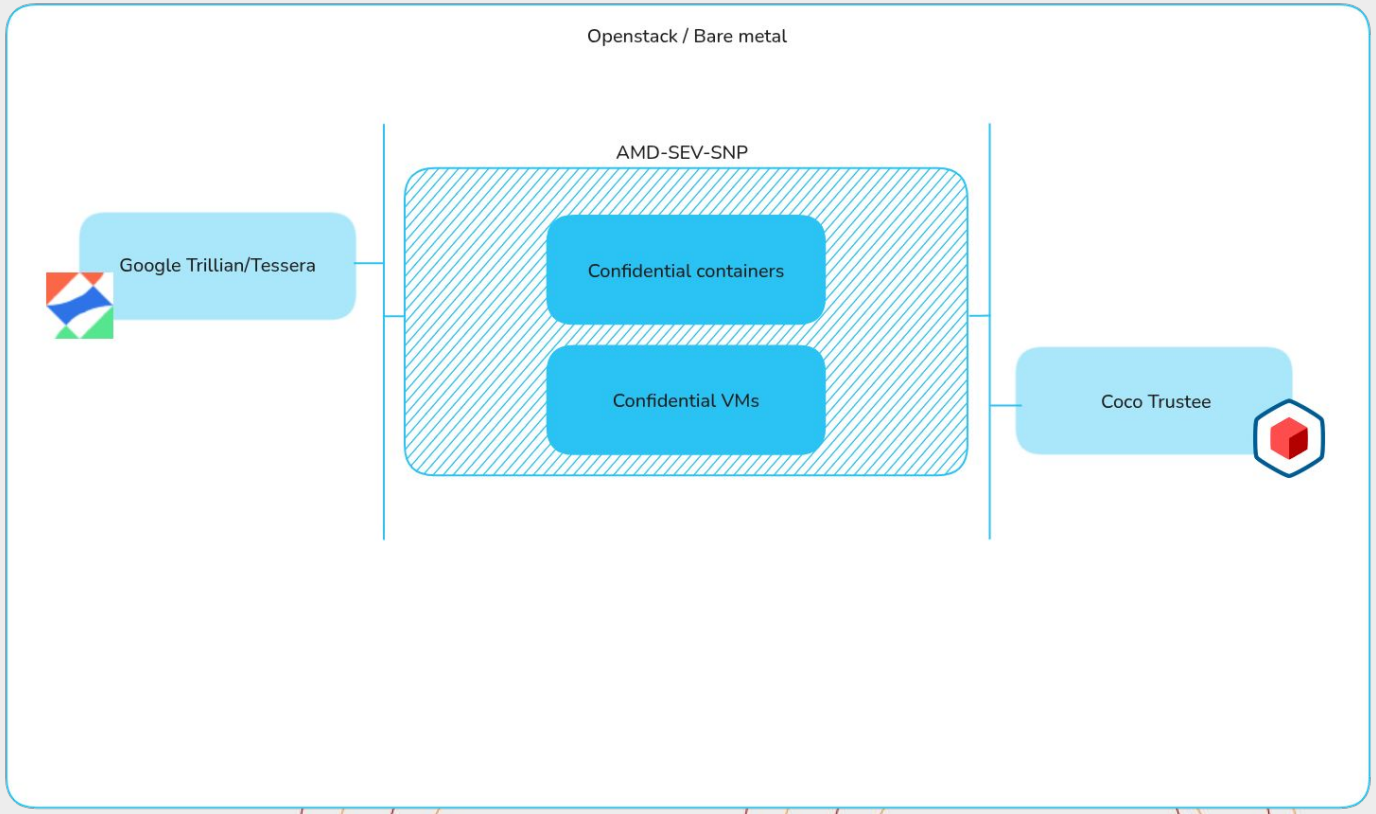



Funded by the European Union

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - **How do I know if the platform has not been tampered?**
  - Is the code running in the platform safe to run?
  - Is my data secure?
  - How can I control who access or runs what, and where?
  - Is it scalable?
  - Is it replicable?
  - etc.

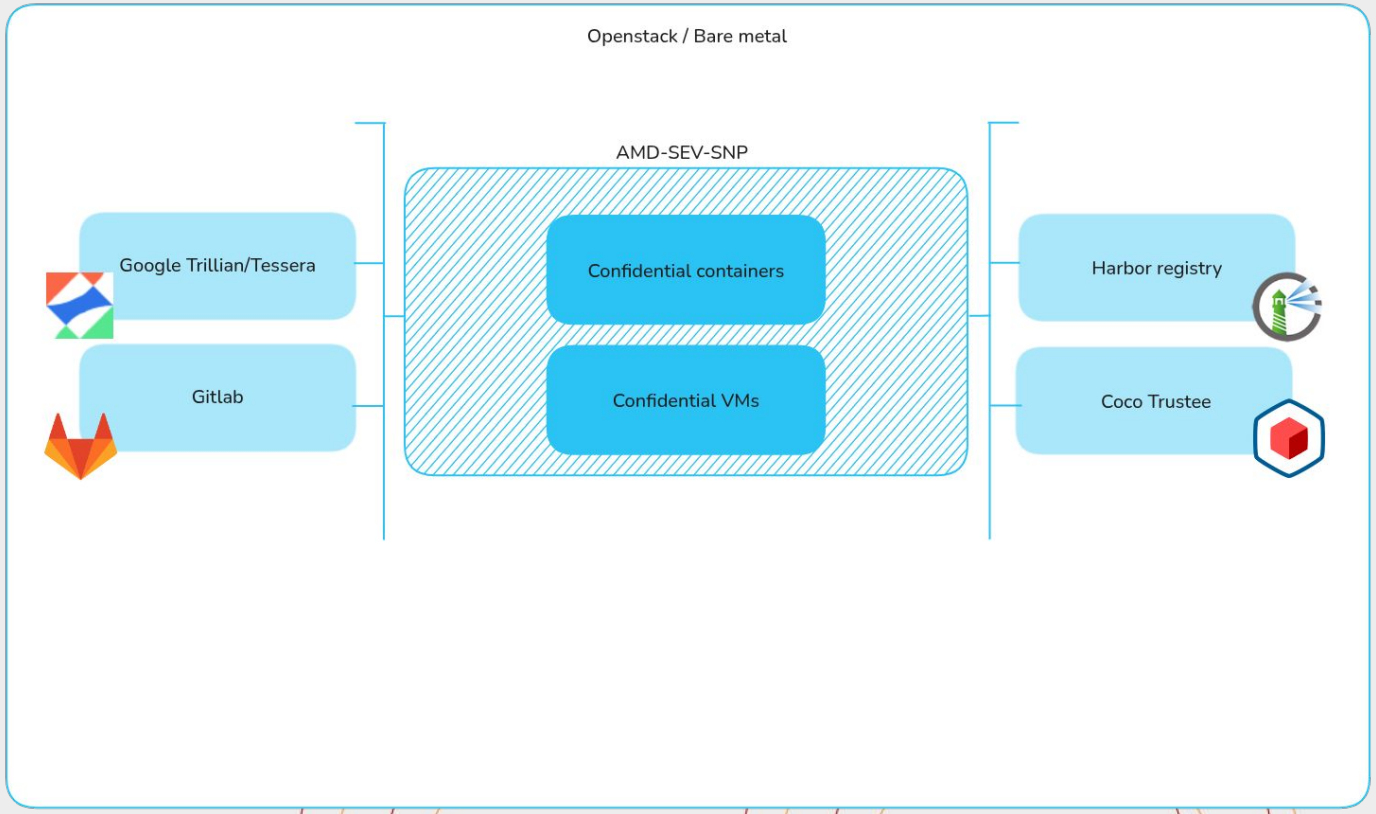



Funded by the European Union

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - How do I know if the platform has not been tampered?
  - **Is the code running in the platform safe to run?**
  - Is my data secure?
  - How can I control who access or runs what, and where?
  - Is it scalable?
  - Is it replicable?
  - etc.

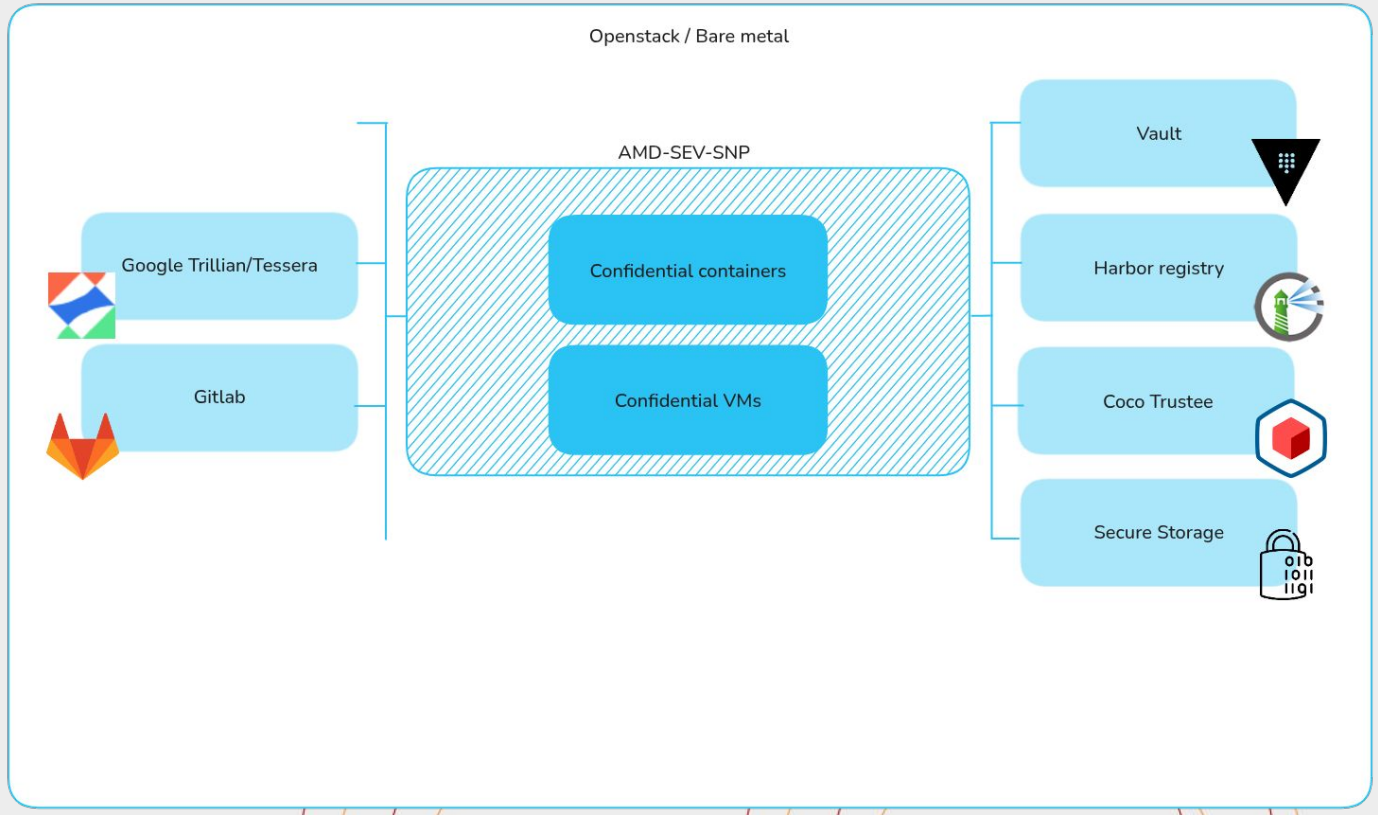



Funded by the European Union

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - How do I know if the platform has not been tampered?
  - Is the code running in the platform safe to run?
  - **Is my data secure?**
  - How can I control who access or runs what, and where?
  - Is it scalable?
  - Is it replicable?
  - etc.

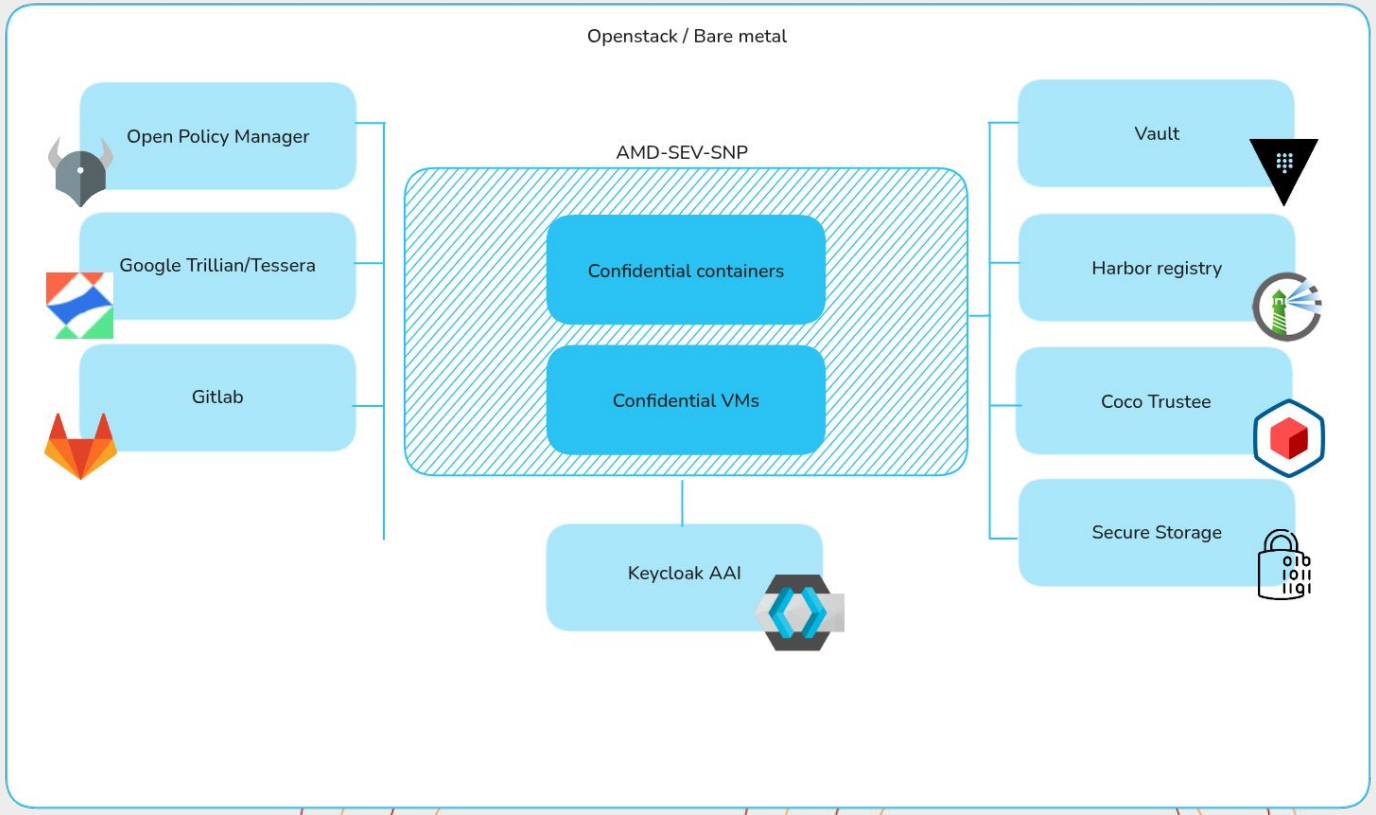



Funded by the European Union

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - How do I know if the platform has not been tampered?
  - Is the code running in the platform safe to run?
  - Is my data secure?
  - **How can I control who access or runs what, and where?**
  - Is it scalable?
  - Is it replicable?
  - etc.

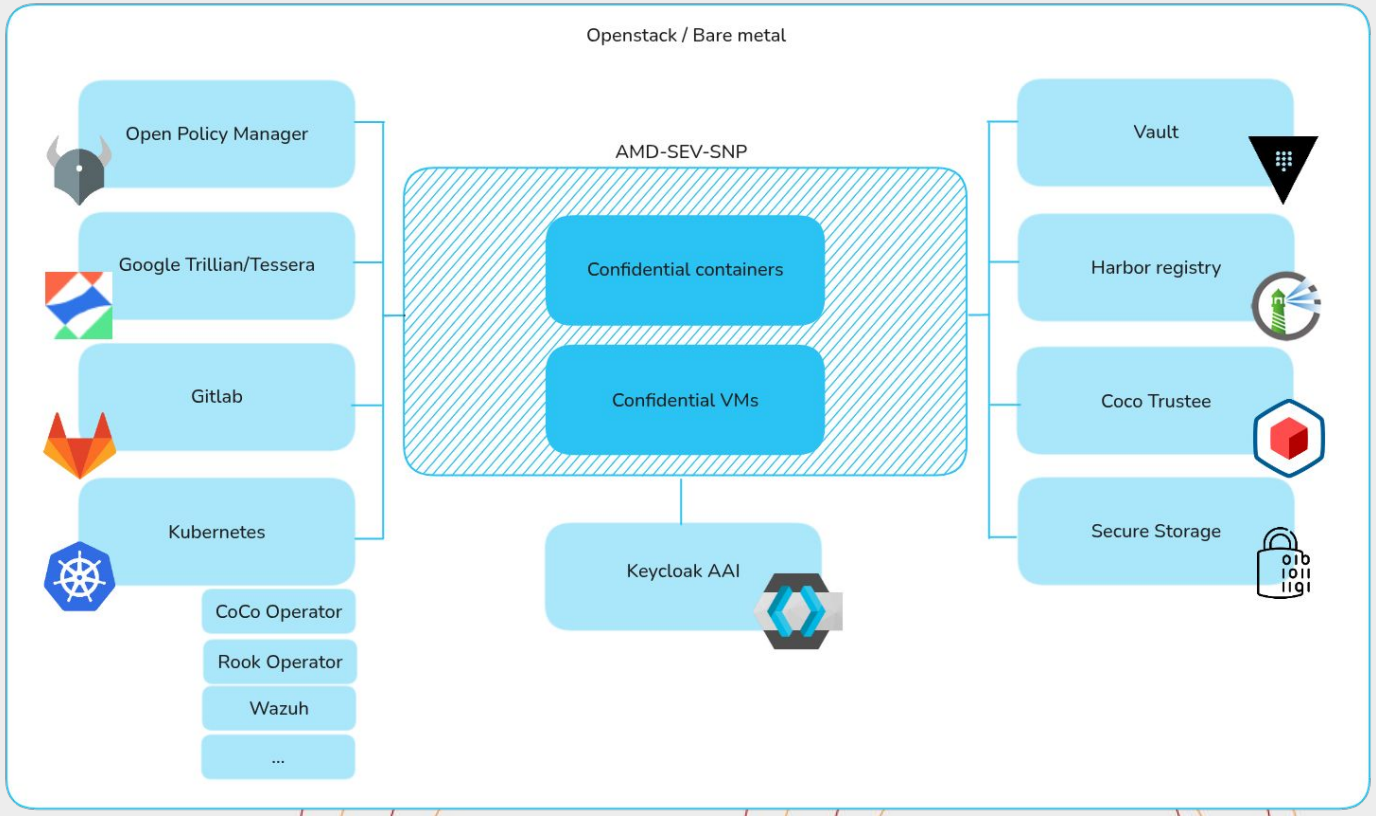



Funded by the European Union

# Our approach

## More Than TEEs: Critical Platform Components

- **TEES** by themselves are **not enough**
- Questions a user may ask
  - How do I know if the platform has not been tampered?
  - Is the code running in the platform safe to run?
  - Is my data secure?
  - How can I control who access or runs what, and where?
  - **Is it scalable?**
  - **Is it replicable?**
  - etc.

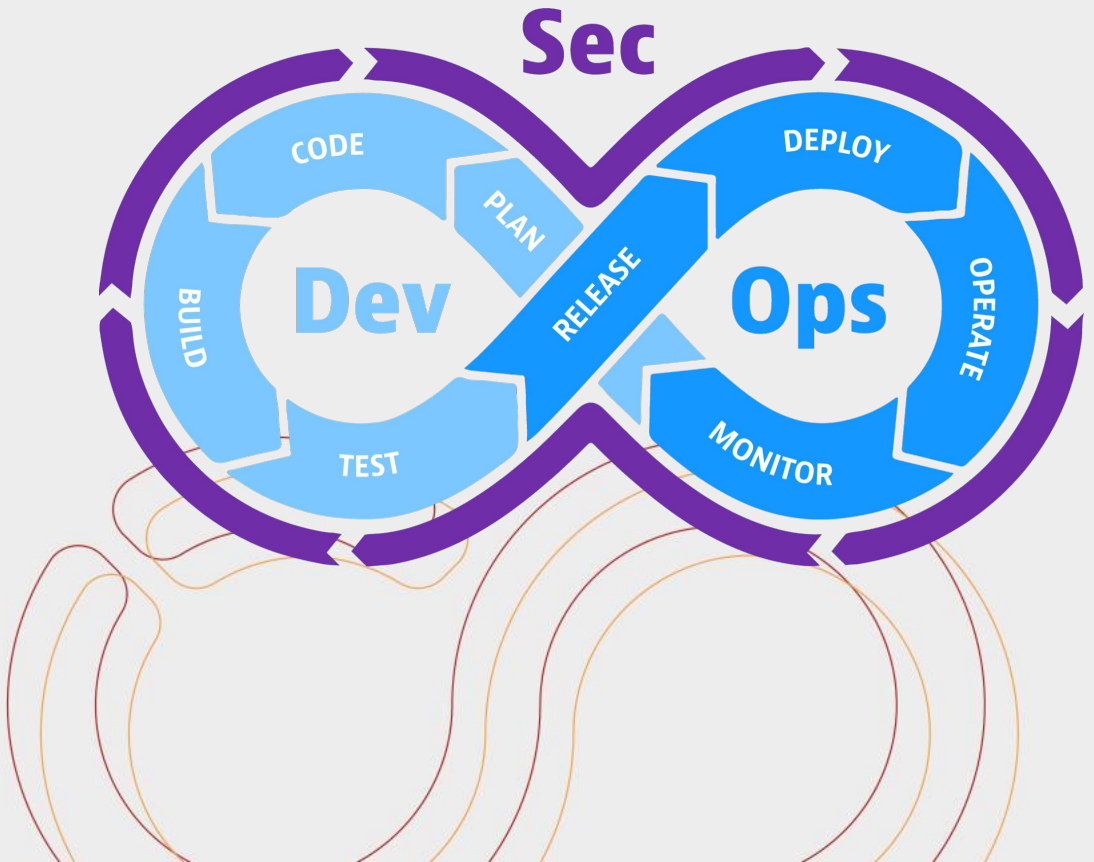



Funded by the European Union

# Our approach

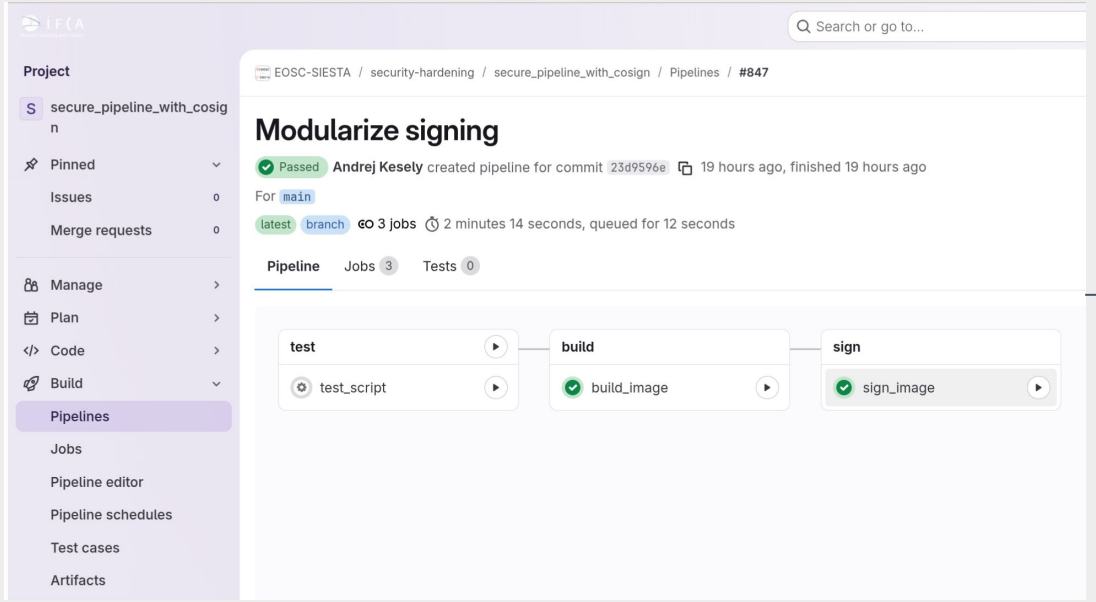
## The cherry on top: DevSecOps methodologies

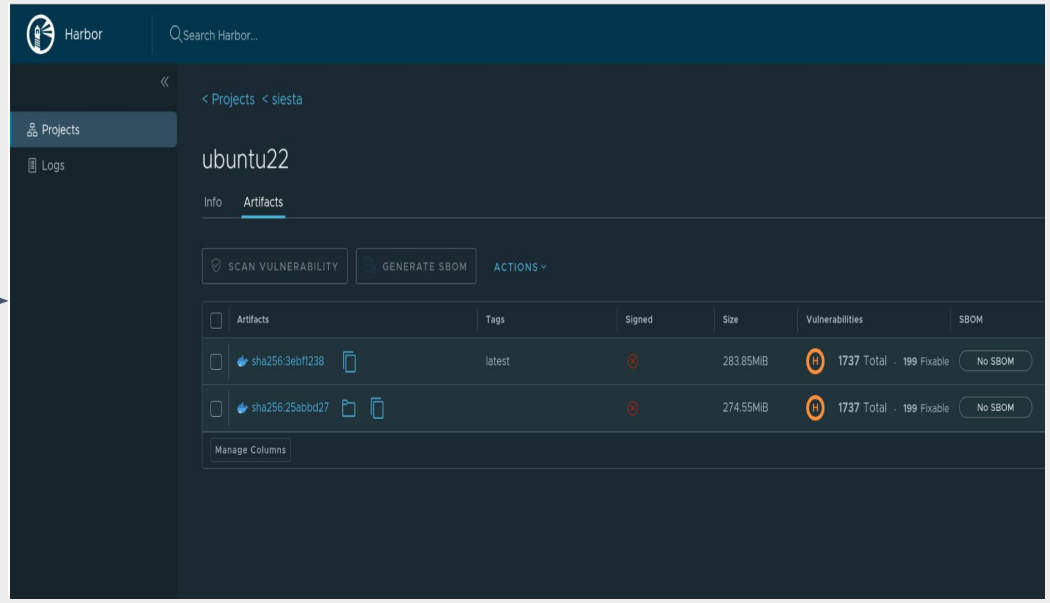
- K8s cluster is deployed using Terraform + Ansible (IaC + Configuration Management)
- K8s components are deployed following a GitOps workflow with FluxCD.
- Integration with Gitlab Pipelines: automation from the start.
- Secure storage procedures using ansible playbooks
- Security hardening




Funded by the European Union

eosc | SIESTA

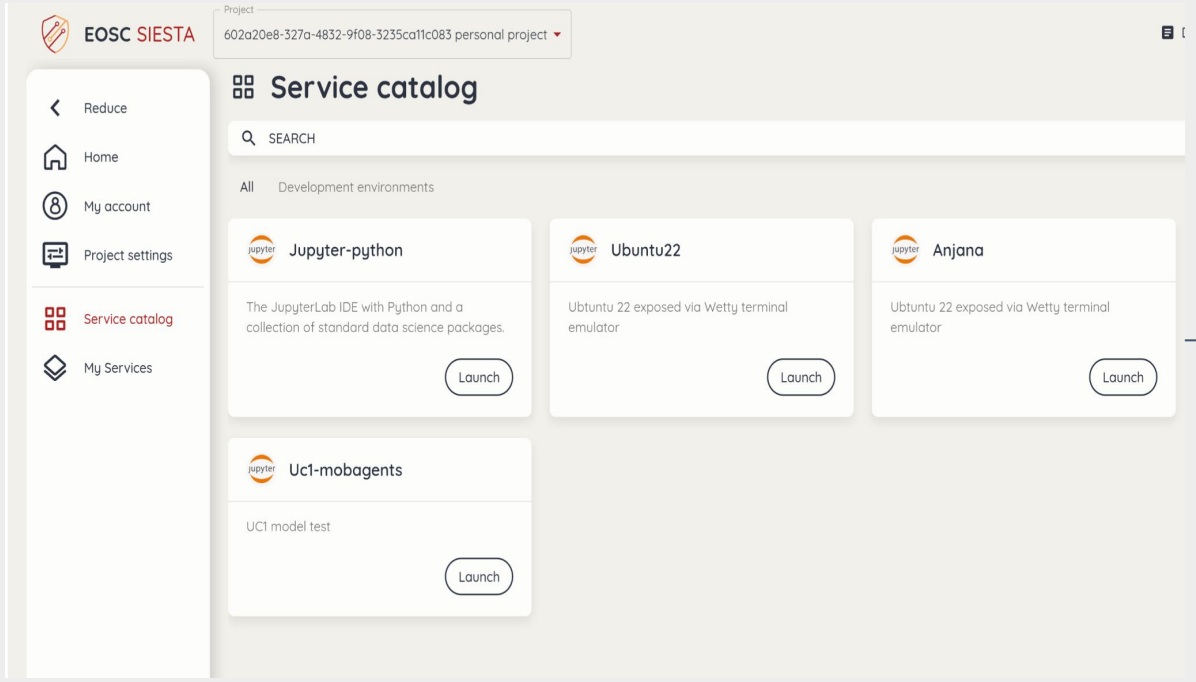


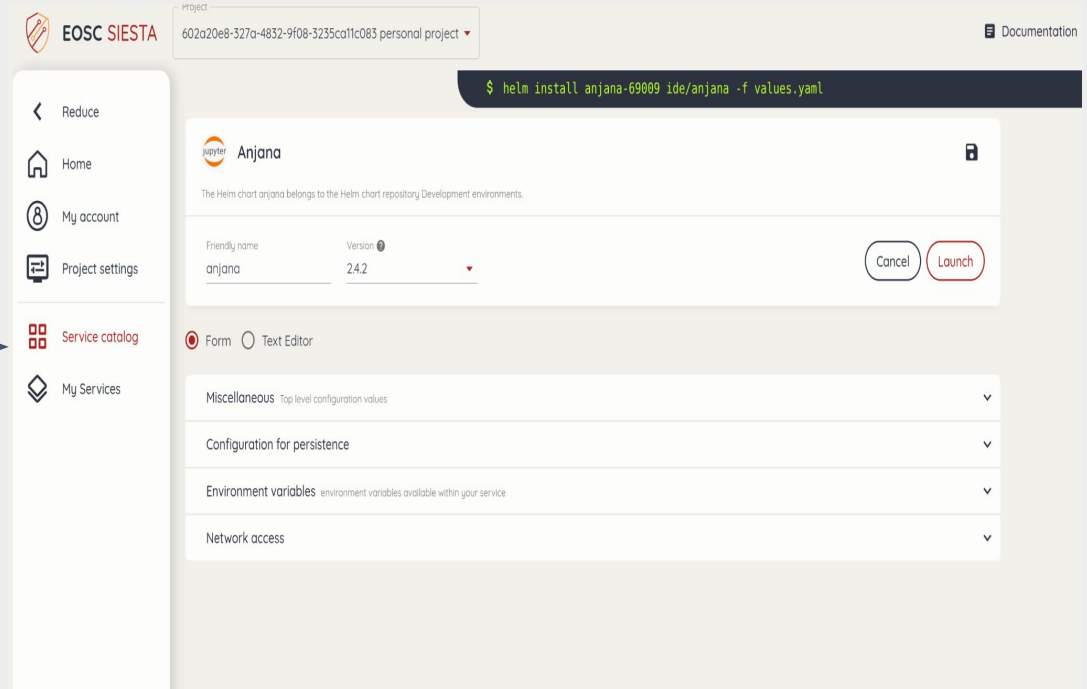




Funded by the European Union

ISCG 2026
15-20 March 2026

eosc | SIESTA




Funded by the European Union

ISCG 2026
15-20 March 2026

# Summary

EOSC-SIESTA: Confidential Computing for Sensitive Data Analysis

- Provides a trusted, hardware-protected environment for analyzing sensitive & confidential data without exposure
- Built on Confidential Containers technology
  → Leverages Trusted Execution Environments (TEEs) for end-to-end confidentiality
- Extended with a powerful set of enabling services for secure data sharing & reproducible workflows
- Adopts full DevSecOps automation
  → CI/CD pipelines, infrastructure-as-code, policy-as-code
- Hides complexity from developers & researchers
  → They focus on science & analysis — not on security plumbing

Funded by the European Union

# Thanks

Viet Tran
viet.tran@savba.sk

Funded by
the European Union

ISCG 2026
15-20 March 2026