A comprehensive initiative to enhance the security posture of open-source software

Marica Antonacci (INFN Bari)

ISGC 2024, Taipei
26 March 2024

Information security

Safeguarding information assets has emerged as a paramount concern for organisations across all sectors

Significance for organizations

Inadequate security measures can have severe consequences including financial losses, reputational damage, regulatory non-compliance, legal repercussions

Research and academia

the integrity and confidentiality of data are not merely operational considerations but fundamental principles that safeguard the integrity of the scientific process, uphold ethical standards, foster innovation, and maintain public trust in the pursuit of knowledge.

INFN's Commitment to Security

As a prominent player in the research domain, INFN recognizes the critical importance of protecting sensitive data, given its extensive involvement in distributed computing infrastructures and numerous research projects dealing with health and other confidential data.

INFN DataCloud

The Datacloud project represents a **strategic initiative** aimed at developing a **comprehensive portfolio** of Infrastructure-as-a-Service (**IaaS**) and Platform-as-a-Service (**PaaS**) cloud services.

These services facilitate the deployment of innovative solutions by providing **seamless access to geographically distributed computing and storage resources**.

Key objectives

- Enable researchers to leverage cutting-edge technologies and resources for their projects.
- Foster collaboration and knowledge exchange within the research community by offering a platform for shared infrastructure and tools.

Distinct features

- The middleware developed as part of the Datacloud project caters specifically to the needs of research communities.
- It offers tailored solutions and cloud-native applications designed to support the unique requirements of research projects.

Co-design

- Datacloud project adopts co-design, fostering collaboration between researchers and developers to tailor solutions for users' needs.
- Users' domain expertise shapes the development process, making their needs and concerns central to solution design.

Our strategic security initiative

For some of the middleware components, the emphasis on swiftly delivering new features and functionalities has, at times, resulted in the unintentional neglect of robust security practices.

INFN is now embarking on a strategic security initiative to comprehensively assess and enhance the security posture of the open-source components within the Datacloud production middleware.

Objectives

- Aligning with industry best practices and standards to fortify the security foundation of Datacloud middleware.
- Correcting past oversights by prioritizing security as a fundamental aspect throughout the development lifecycle.

Approach

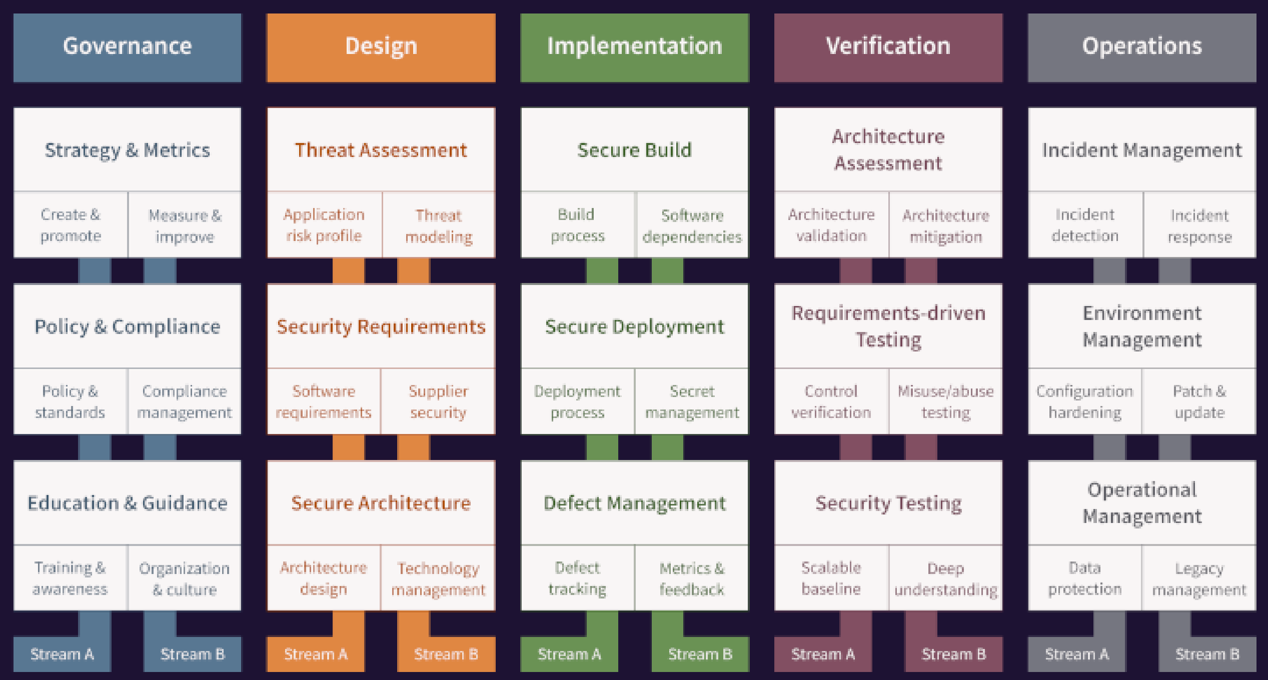
- Collaborative effort involving development leads, "security champions" and key stakeholders to establish robust governance frameworks and virtuous processes.
- Implementation of tasks focusing on defining security standards, policies, roles, security training, and awareness to foster a culture of security within the organisation.

Frameworks for security ehnancement

OWASP SAMM

(Software Assurance Maturity Model)

Provides a structured approach for organizations to assess, improve, and benchmark their software security practices.



Governance		Design		Implementation		Verification		Operations	
Strategy & Metrics		Threat Assessment		Secure Build		Architecture Assessment		Incident Management	
Create & promote	Measure & improve	Application risk profile	Threat modeling	Build process	Software dependencies	Architecture validation	Architecture mitigation	Incident detection	Incident response
Policy & Compliance		Security Requirements		Secure Deployment		Requirements-driven Testing		Environment Management	
Policy & standards	Compliance management	Software requirements	Supplier security	Deployment process	Secret management	Control verification	Misuse/abuse testing	Configuration hardening	Patch & update
Education & Guidance		Secure Architecture		Defect Management		Security Testing		Operational Management	
Training & awareness	Organization & culture	Architecture design	Technology management	Defect tracking	Metrics & feedback	Scalable baseline	Deep understanding	Data protection	Legacy management
Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B

ISO/IEC 27000 family International standard

ISO/IEC 27001 outlines the requirements for an Information Security Management (ISM) whereas ISO/IEC 27002 offers best practices and control objectives.

ISO 27001
Information Security
Management

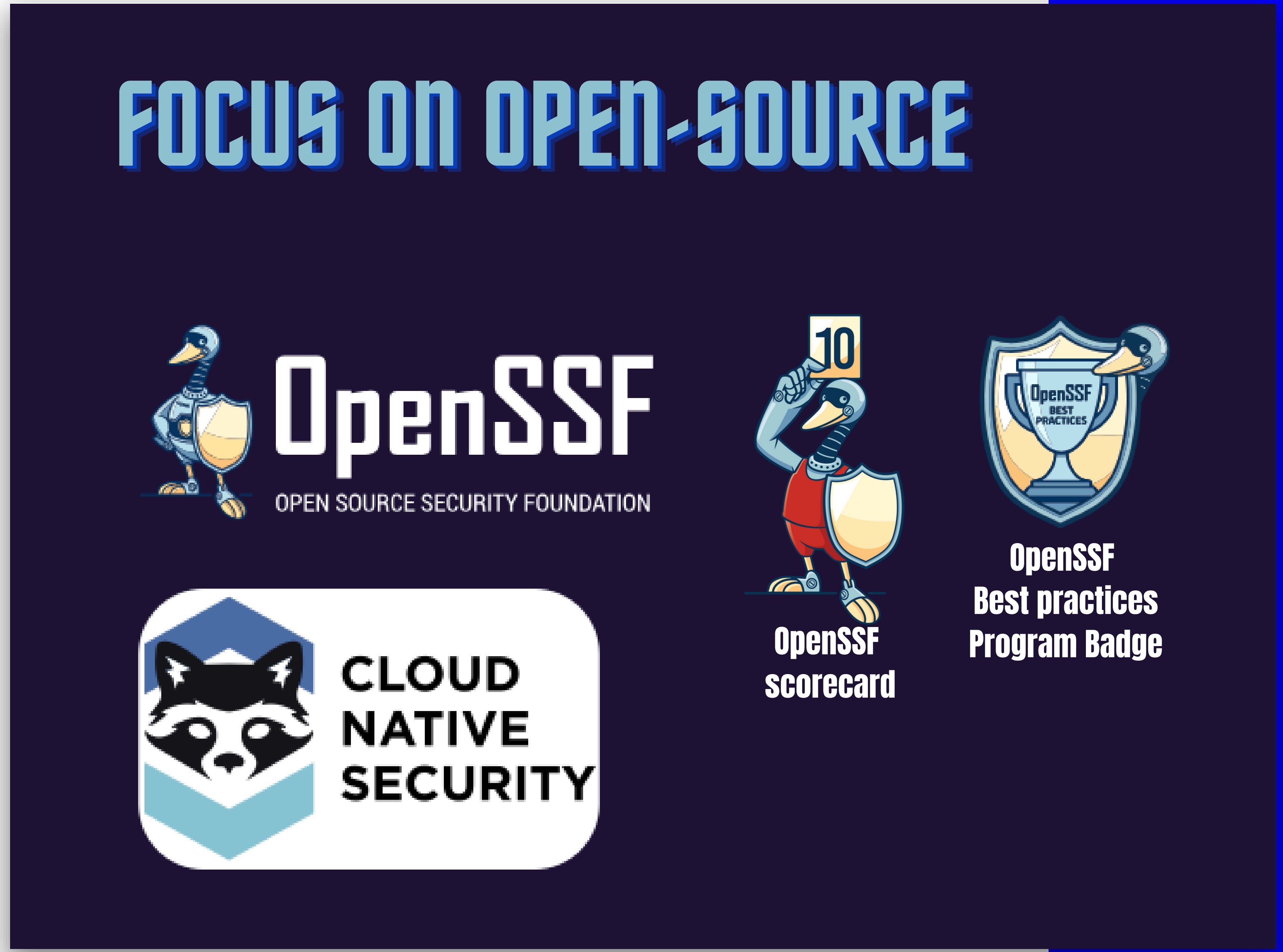
ISO 27002
Information Security
Controls

Integrating SAMM and ISO/IEC 27002

Towards a robust Security posture

Our strategy involves integrating the strengths of both frameworks:

by aligning software security practices with SAMM's principles and embracing the comprehensive information security controls of ISO/IEC 27002, our goal is to establish a robust and cohesive security posture.



WP1: Governance and compliance

- Define, review, and communicate security policies and standards, aligning them with the ISO/IEC 27002 framework.
- Develop a comprehensive security training program for team members.

WP2: Security Self-assessment

- Identify the risks, assess adherence to security policies, and promote continuous improvement in our security posture
- Supply chain analysis (SBOM)
- Prioritise the identified issues and remediate

Work plan objectives:

1. Establish formal processes to develop secure code, prioritizing risk management to ensure a robust foundation for future development endeavors
2. align existing software: bridging the gap between current software practices and the newly established secure development strategy

WP3: Continous Monitoring

- Establish and maintain ongoing processes to enhance software quality, update dependencies promptly, and respond swiftly to emerging vulnerabilities
- Systematically collect metrics and feedbacks.

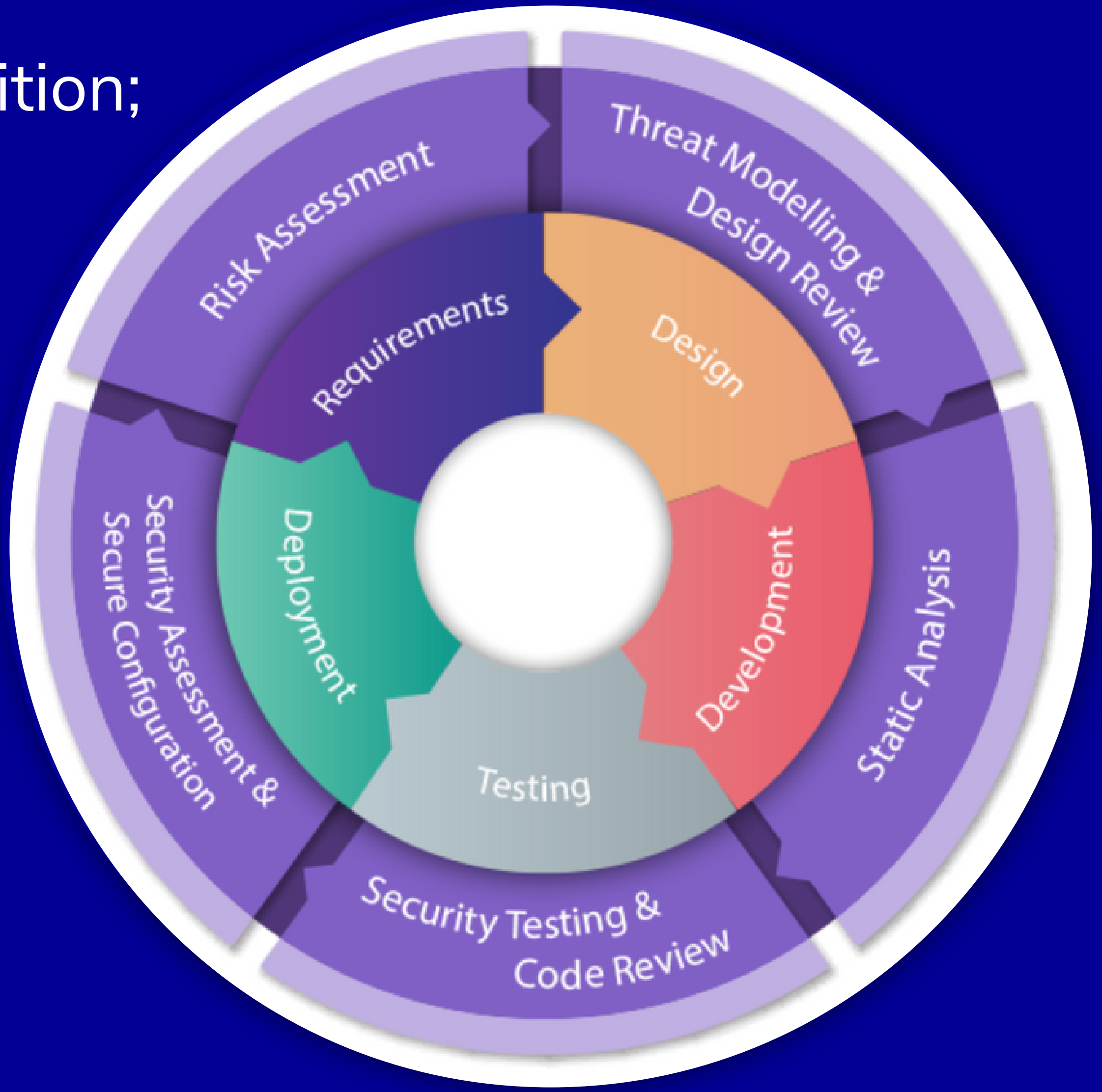
"security is a process not a product... there's no such thing as perfect security. Interestingly enough, that's not necessarily a problem. ... Security does not have to be perfect, but the risks have to be manageable...".

Bruce Schneier - The process of security (2000)

Secure Software Development Cycle

It is critical that security is embedded in all stages of the SDLC:

- Requirements definition;
- Design;
- Development;
- Testing;
- Deployment


Risk Assessment
Threat Modelling & Design Review
Static Analysis
Security Testing & Code Review
Security Assessment & Secure Configuration
Requirements
Design
Development
Testing
Deployment

> “The cost of removing an application security vulnerability during the design phase ranges from 30-60 times less than if removed during production”

NIST, IBM, and Gartner Group

Security requirements

What are the key security risks within the application?

- Type of information application is processing
- Legal and regulatory security requirements
- Use case modelling

Security design

Building security into the design of the application

- Thread modeling
- Planning the security testing phase

Development

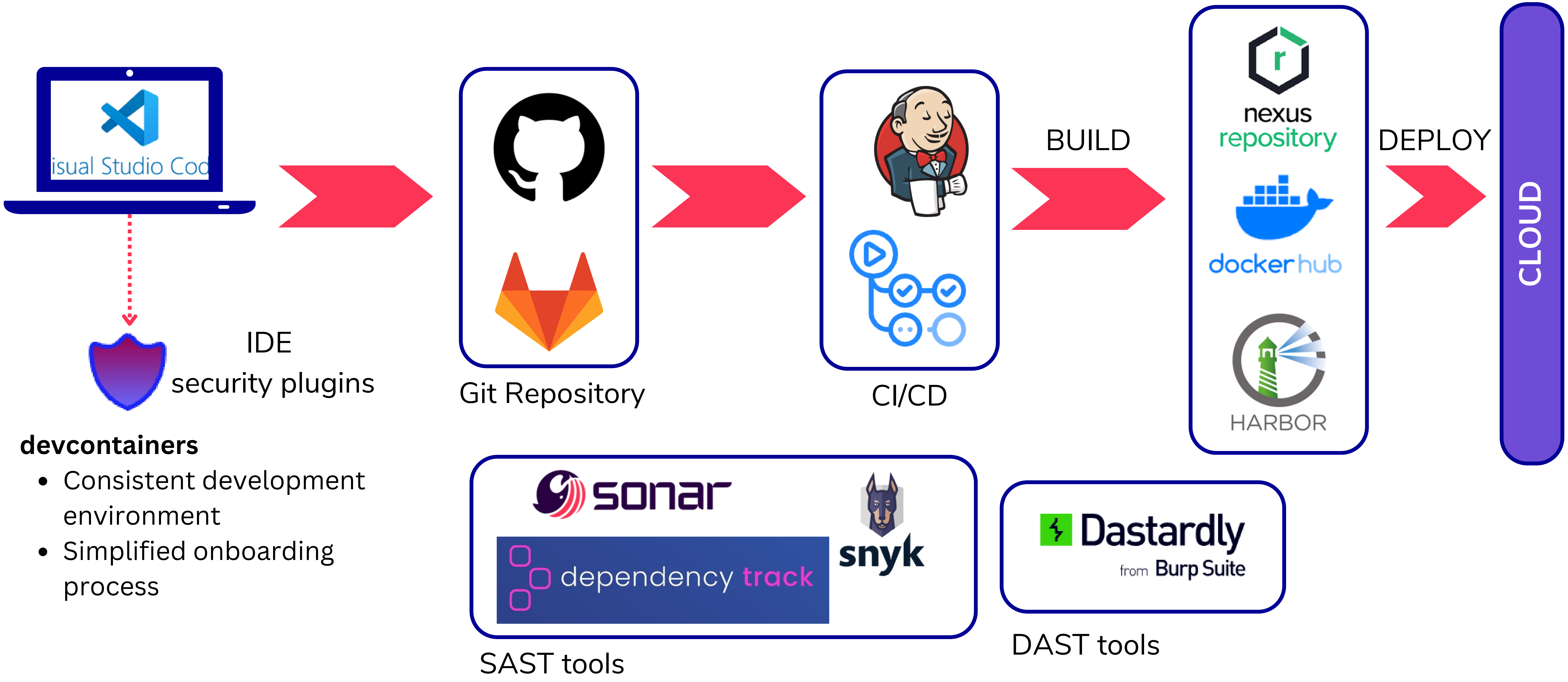
Ensuring that code is developed securely and implementing the security controls identified during the design phase

Testing

Ensure the application meets the security standards

From DevOps to DevSecOps

- thinking about application and infrastructure security from the start
- selecting the right tools to continuously integrate security



IDE
security plugins

Git Repository

CI/CD

BUILD

DEPLOY

CLOUD

SAST tools

DAST tools

devcontainers

- Consistent development environment
- Simplified onboarding process

Security culture

Security champions play a vital role in ensuring security is inclusive and universally understood within the organization, contributing to a more robust security posture.

Security as a shared responsibility.

An overarching awareness of information security can foster buy-in from technical operators and developers as they recognize security is not someone's else problem, but everyone's.

Enhance the effectiveness of DevSecOps programs.

Security champions help cross-functional DevOps teams focus on the advantages of application security and security operations.

Conclusions

We are committed to **enhance the security posture of the software** developed in the DataCloud project.
By strategically **integrating OWASP SAMM and ISO/IEC 27002**, we aim to fortify our security practices.

While we have begun automating security tests within our pipelines, we understand that **fostering a security culture is equally important.**
Together, we recognize security as a shared responsibility and a precious organizational value, ensuring the integrity of our systems and data.

The success of this initiative depends on a **collaborative effort from numerous stakeholders** within our organization, each playing an important role in achieving our shared goal of a robust and harmonized security posture.

Thank you!

Marica Antonacci (INFN BARI)
Barbara Martelli (INFN CNAF)
Giacinto Donvito (INFN BARI)
Vincenzo Ciaschini (INFN CNAF)

Contacts:

marica.antonacci@ba.infn.it