Cloud Native Security

Digital Technology Service

Agenda

- Who are we

- Overview
  - A raised concern
  - Cloud native vs traditional

- Sorint's Tailored Journey
  - The make it model
  - Instantiated from
  - Experts Involved

- Success Stories

- Bonus slide - Related by Sorintains

- Going Forward

17 Offices
3 Continents

EUROPE
Milan, Rome, Bergamo, Turin, Padova, London, Madrid, Frankfurt, Paris, Wroclaw, Brasov, Bologna, Lecce
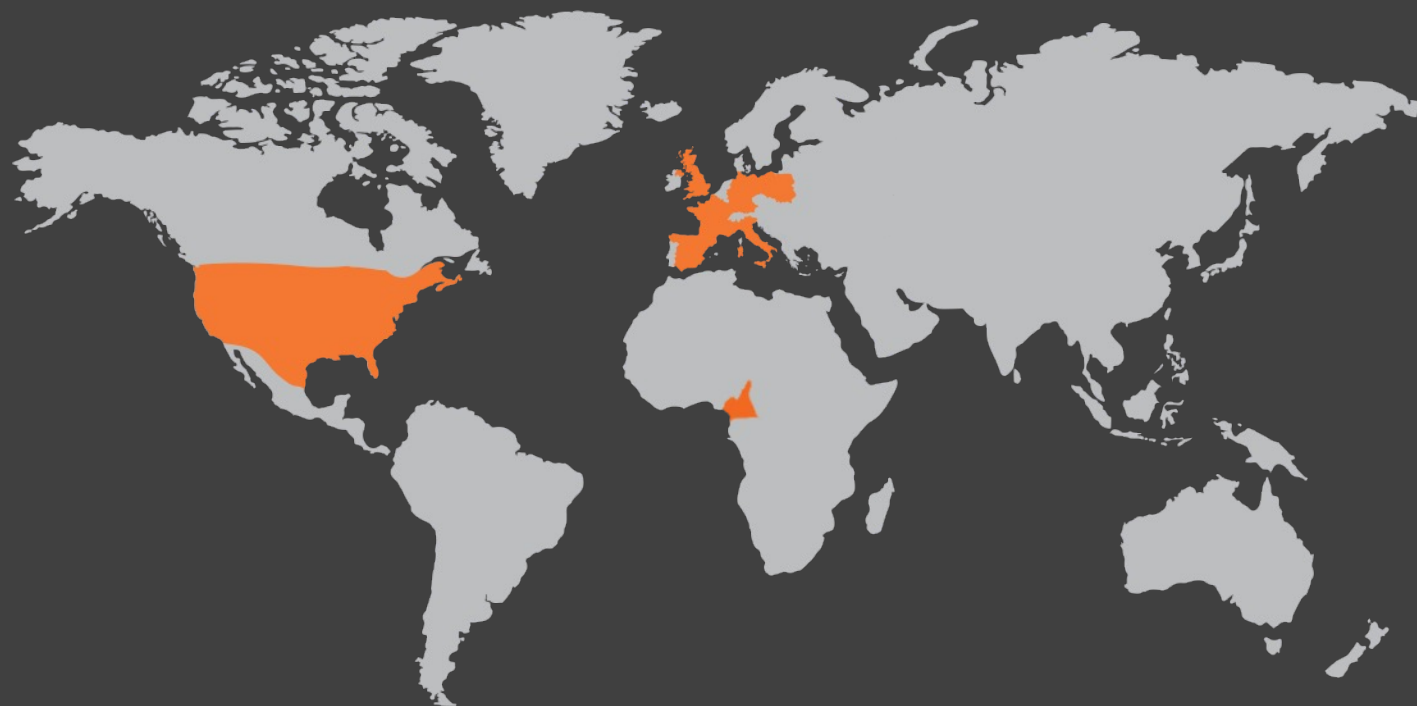
USA
San Diego

AFRICA
Douala

Other Business Units

SORINT.sec   SORINT.tek   experim
a cloud of skills

SORINT.lab

Overview Facts

900+

Tech-Savvy

Cloud Engineers
SREs
DevOps Engineers
Full Stack Developers

+40000

Training
hours
per year

50+

Technical
Sircles

Methodology

ISO 27001
ISO 20000
ISO 9001
ISO 14001

PM Methodology

Prince2
PMI
Agile
SCRUM/UX

35+

Years of
experience
with a
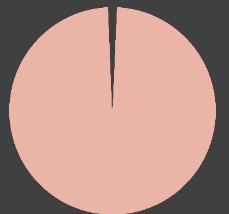Startup mindset

250+

Large Enterprise
Customers

Market

Finance & Insurance,
Utility & Telco,
Industry & Services,
Transport,
Public Administration

98%

Customer
Retention
Rate

INTESA SANPAOLO
BANCA 5
Deutsche Bank
ING
BANCO BPM
widiba
CRÉDIT AGRICOLE
illimity
IBL Banca
BPER: Banca
Creval
UniCredit
BBVA
Santander

BORSA ITALIANA
nexi
sia
cdp
cassa depositi e prestiti
Vittoria Assicurazioni
REALE MUTUA
Allianz
engie
2i Rete Gas
Terna
a2a smart city
iren

SKY
vodafone
TIM
FASTWEB
un passo avanti
Visura
TINEXTA GROUP
InfoCert
TINEXTA GROUP
allitude
IRIDEOS
LIS Holding
IGT
EUROBET
Sisal

CAREL
DANIELI
intercos GROUP
ICA
Q8
MBE MAIL BOXES ETC.
MENARINI
AIFA
AGENZIA ITALIANA DEL FARMACO
AER Agenzia Entrate Riscossione
Ministero della Difesa
De Cecco dal 1886
ESSELUNGA
EVOCA GROUP
MARELLI
ITALDESIGN
LAMBORGHINI
brembo
SEA Milan Airports
Orio al Serio international airport
S.A.C.B.O. S.p.A.
DIESEL
Ermenegildo Zegna
UNITED COLORS OF BENETTON.
INDITEX

Clients

Technology Partners

Cloud Native Security

Digital Technology Service

- Containerization is the practice of deploying and managing applications and all the dependencies within an isolated environments.

- Strategies, practices, & tools to safeguard the containerized applications and the underlying environment from potential cybersecurity threats and vulnerabilities. Plus, continuous monitoring.

- Resulting in a solid supply chain security architecture across all layers. E.g.

  - Infrastructure layer
  - O.S
  - Runtime/Platform layer
  - Network layer

  - Storage
  - Application layer

- On private and public cloud environments.

70%

In 2022, year-over-year inquires on CNAPP(Cloud Native Application Protection Platforms) increased 70%.

*Gartner March 2023

A Raised Concern

The need of container security

Container environment are rapidly moving to production

In 2021, less than 40% of global organization ran containerized applications in production.

90% by 2027

The attack surface is increasing

Attackers are targeting the misconfiguration of cloud infrastructure (network, storage, identities and permissions), APIs and the software supply chain itself. Gartner 2023

Knowledge & Awareness

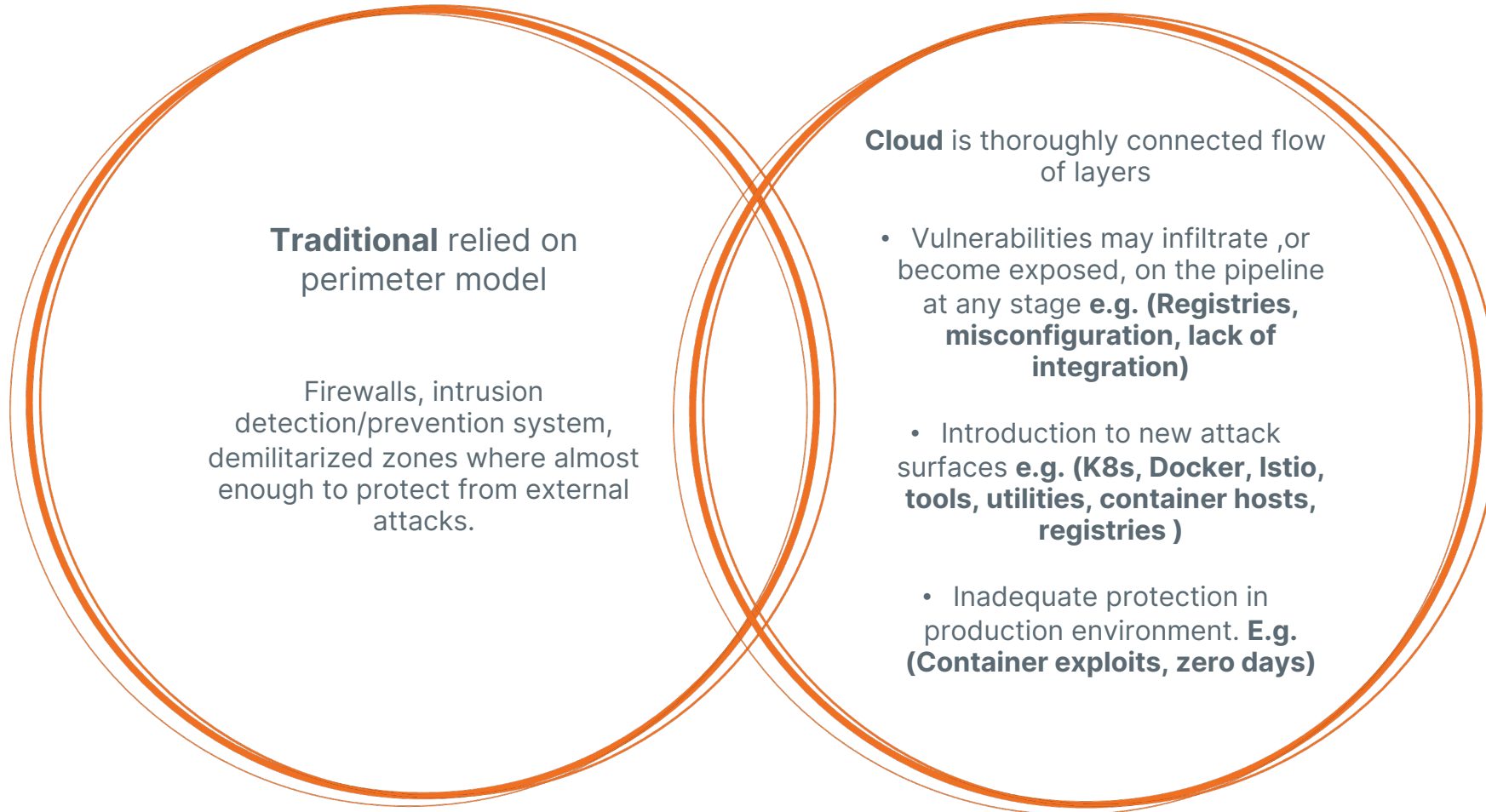K8s abstracts container networking, trading off the network security.

Tools

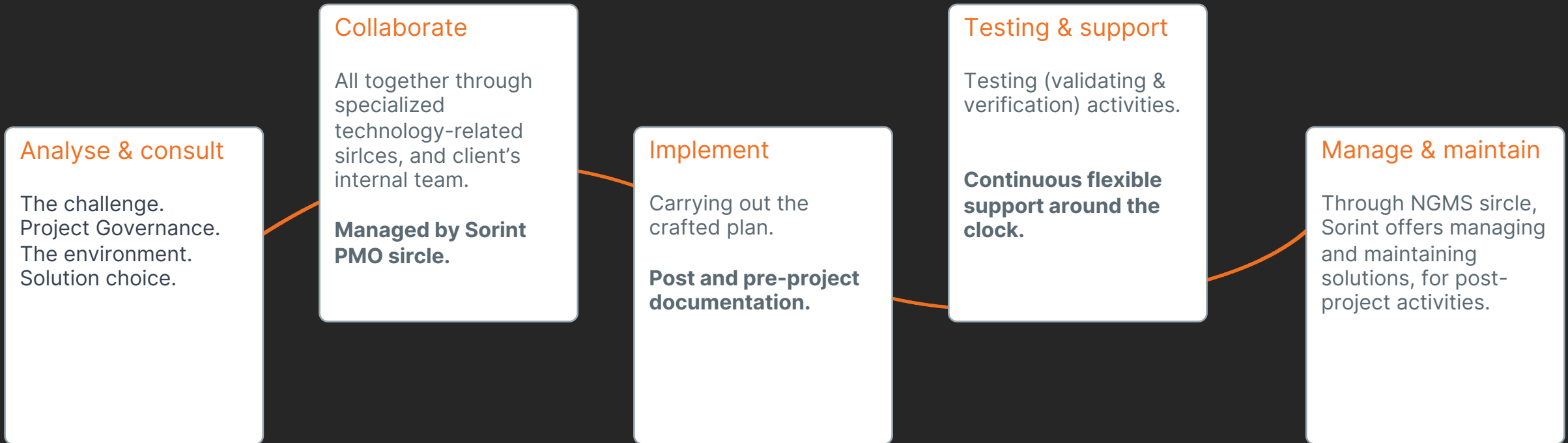Traditional tools do not work with containerized environment. New tools and practices emerge every day.

Cloud native Vs traditional

Cost of dynamic approach

Traditional relied on perimeter model

Firewalls, intrusion detection/prevention system, demilitarized zones where almost enough to protect from external attacks.

Cloud is thoroughly connected flow of layers

• Vulnerabilities may infiltrate ,or become exposed, on the pipeline at any stage **e.g. (Registries, misconfiguration, lack of integration)**

• Introduction to new attack surfaces **e.g. (K8s, Docker, Istio, tools, utilities, container hosts, registries)**

• Inadequate protection in production environment. **E.g. (Container exploits, zero days)**

Sorint's Tailored Journey

The make it model

Collaborate

All together through specialized technology-related sirlces, and client's internal team.

Managed by Sorint PMO sircle.

Testing & support

Testing (validating & verification) activities.

Continuous flexible support around the clock.

Analyse & consult

The challenge.
Project Governance.
The environment.
Solution choice.

Implement

Carrying out the crafted plan.

Post and pre-project documentation.

Manage & maintain

Through NGMS sircle, Sorint offers managing and maintaining solutions, for post-project activities.

Striving for nothing short of a perfect solution and a well-defined roadmap

Sorint's Tailored Journey
Instantiated from

Every journey is a unique challenge, but our know-how:

Executed countless projects in the field to prominent entities in Europe, US, and Africa.

For various industries
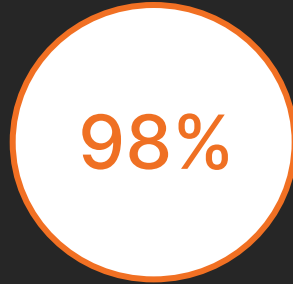
98%
Customer retention rate
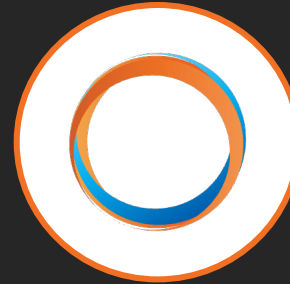
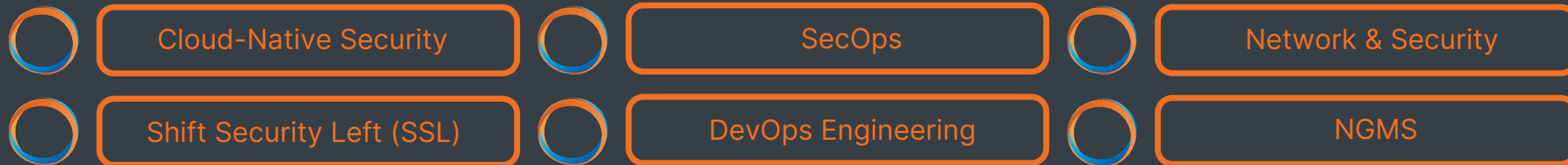Dedicated sircles specialized in given fields and technologies

Highest certification in various fields and "Training Partner" to some vendors

Expert PM with technical background ensuring project's objectives are met

Day x —— Continues support —— Continues support —— Continues support —— Day y

Experts Involved

Cloud-Native Security

SecOps

Network & Security

Shift Security Left (SSL)
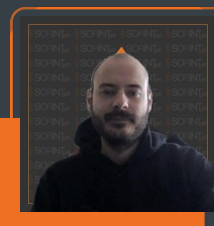
DevOps Engineering

NGMS

Senior masterminds

Maurizio Pagani

Head of Cloud-Native Security | System Architect

+10 years of experience in IT security, expert in SELinux

Manual Salvi

Security Consultant | Software Architect

+10 years of experience in both application and infrastructure design

Cesare Pizzi

Reverse Engineer | Incident Responder | Opensource Developer and Contributor

CTF player, trainer, regular speaker at DEFCON, Insomni'hack, Nullcon

Some prestigious certifications

Closer Look

Areas and field of focus

Project-based

Analysis, architect, consultant, and implement.

Tailored proposals. Based on project and client's needs.

Consultancy

Where our security experts advise and hand-on workshops, training, knowledge, solutions, assess the security posture and much more.

Staff Augmentation

Offer experts in given fields or technologies.

Success stories

Delivered by: Sorintians

A Global known Transportation and Aviation Entity

Introducing a new tool and integration

Challenge
Client faced several challenges with the current endpoint container security solution. Both on functionality and administrational levels.
- Pre-defined infrastructure.
- Running two OS. Linux and Windows.

Going forward
Analysing and understanding the infrastructure

Accepting the challenge - Solution and Implementation
For its centralized administration console and it's powerful integration with vSphere virtualization systems. It was decided to integrate the infrastructure with Carbon Black Workload Protection.
The solution's has various pros. E.g.
- Solid compatibility integration with vSphere.
- Enables security operators to handle potential threats and security notification from a centralized console.

Result & delivery
- Installed and integrated the new solution.
- Secured and centralized the monitoring of 500 systems with Carbon Black.
- Carried out test through injecting both OS with malware. All successfully identified.
- Alignment workshop with client's team.
- Single product with no extensions was a major success to client's needs.

Floatingpoint.sorint.com

Bonus Slide

Related Solutions and Tools by Sorintians

Modern Infrastructure
Center of Excellence

From traditional infrastructure to a modern approach. Entails aligning with the latest industry standards, best practices, and business needs. Activities vary from server creation , consolidation, patching services, migration, automation and much more.

Inquire

NGMS
Core IT Service

Remotely manages IT infrastructures ensuring the correct functionality, support for vendor and Open-source products. Reducing response times to new problems. Speed, flexibility, method and technical preparation are part of our DNA.

Inquire

DevOps Engineering
Technology Consultant Service

Advanced set of practices, tools, and technologies that power automation throughout the development, testing, and deployment phases.

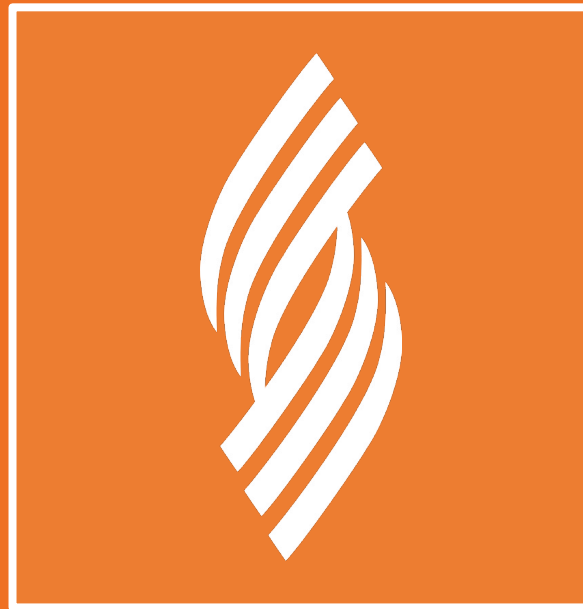inquire

Going Forward

How we can move forward from here

One hour workshop

Read more on /sorintlab

Alternative approach

BUILDING GREAT
TECHNOLOGY

SORINT.lab

IT | ES | UK | DE | US | FR | PL | CMR | RO