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

USA
San Diego

AFRICA
Douala

Other Business Units
# Overview Facts

## Tech-Savvy
- 900+ Tech-Savvy
- Cloud Engineers
- SREs
- DevOps Engineers
- Full Stack Developers

## Methodology
- ISO 27001
- ISO 20000
- ISO 9001
- ISO 14001

## PM Methodology
- Prince2
- PMI
- Agile
- SCRUM/UX

## Market
- Finance & Insurance, Utility & Telco, Industry & Services, Transport, Public Administration

## Large Enterprise Customers
- 250+

## Training hours per year
- +40000

## 50+ Technical Sircles

## 35+ Years of experience with a Startup mindset

## 98% Customer Retention Rate

## 900+ Tech-Savvy

- Cloud Engineers
- SREs
- DevOps Engineers
- Full Stack Developers

## ISO Certified

## Training hours per year
- +40000

## 50+ Technical Sircles

## 35+ Years of experience with a Startup mindset

## 98% Customer Retention Rate
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

70%

In 2022, year-over-year inquiries 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

**Analyze & consult**

**Collaborate**
All together through specialized technology-related silces, and client's internal team.
Managed by Sorint PMO sircle.

**Implement**
Carrying out the crafted plan.
Post and pre-project documentation.

**Testing & support**
Testing (validating & verification) activities.
Continuous flexible support around the clock.

**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

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

For various industries

Customer retention rate

Dedicated circles 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  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

- Offensive Security Certified Professional (OSCP)
- Certified Cloud Security Administrator (CCSA)
- Certified Kubernetes Administrator (CKA)
- Certified Kubernetes Security Specialist (CKSS)
- Neuvector Full Lifecycle Container Security
- Ethical Hacking Association (EHA)
- CompTIA Security+
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.
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 its powerful integration with vSphere virtualization systems, it was decided to integrate the infrastructure with Carbon Black Workload Protection. The solution 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.
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.

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.

DevOps Engineering
Technology Consultant Service
Advanced set of practices, tools, and technologies that power automation throughout the development, testing, and deployment phases.
Going Forward
How we can move forward from here

One hour workshop

Read more on /sorintlab

Alternative approach
BUILDING GREAT TECHNOLOGY

SORINTlab

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