

SSL – Shift Security Left

Technology Consulting Service

Agenda

- Who are we
- Overview
- Addressing SSL
 - Why – A Brief History
 - DevSecOps
 - SSL & DevSecOps
 - What Sorint Offers
 - Closer Look
 - Leading To
- Success Stories
- Related by Sorintains – Bonus slide
- Going Forward

17 Offices
3 Continents

EUROPE

Milan, Rome, Bergamo, Turin, Padova,
London, Madrid, Frankfurt, Paris,
Wroclaw, Brasov, Bologna, Lecce

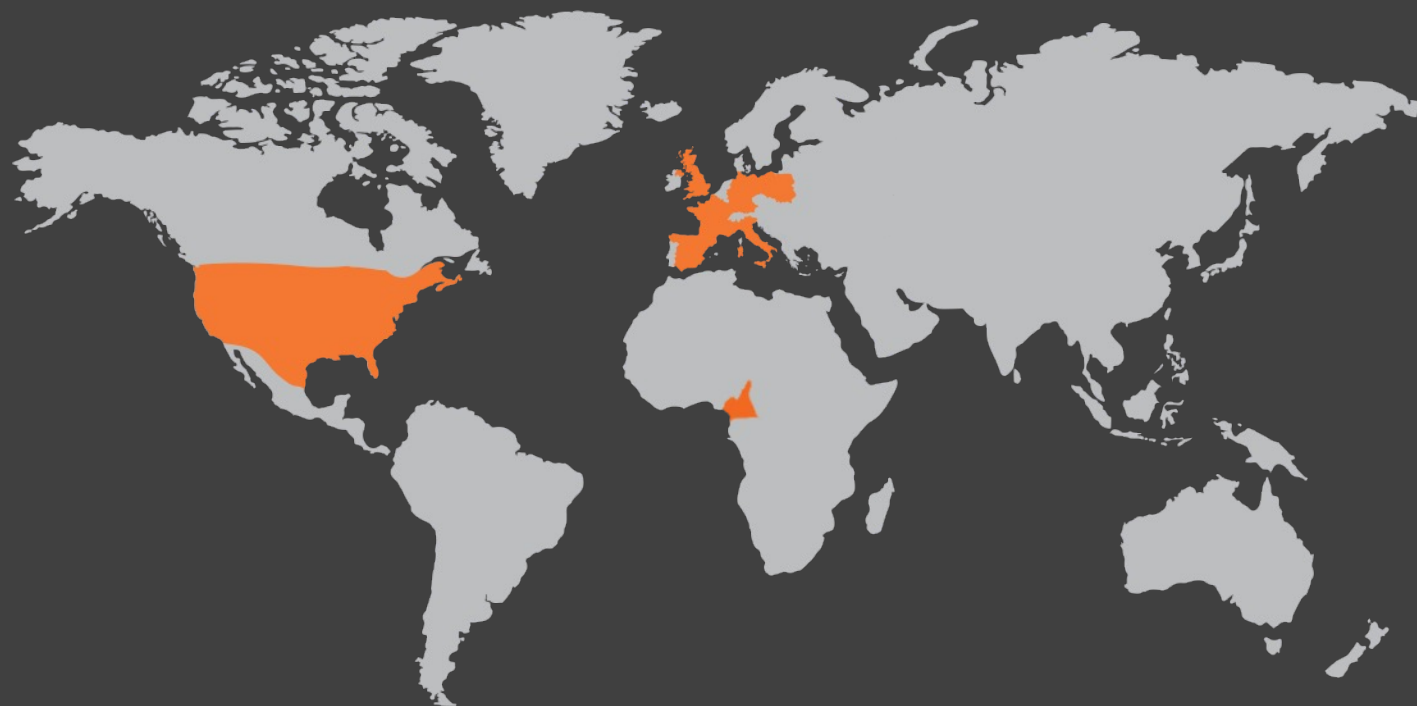
USA

San Diego

AFRICA

Douala

Other Business Units



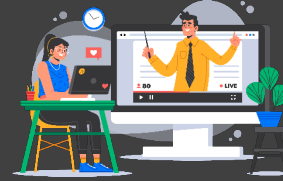
Facts on Sorintians

+900 Skilled People

Cloud Engineers
SREs
DevOps Engineers
Developers



+40K
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

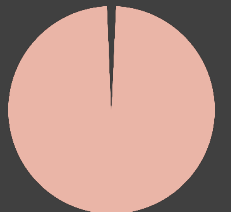


Industries

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



98%
Customer
Retention
Rate



INTESA  SANPAOLO



Clients



CANONICAL



Technology Partners

SSL – Shift Security Left



- Promotes security as a common responsibility shared by all teams involved in software development.
- Focusing on
 - Speed vs Security
 - Skill vs Mindset
 - Lack vs Positive Communication



Addressing SSL



Security activities can not be left until end of development



Insecure designing can lead to deadlocks. Impossible to fix bugs



Vulnerabilities lead to increase in cost and time



Dev and security teams need to collaborate regularly



Increased in complexity in recent software. Largely “assembled”



Lack security skills/knowledge during all stages of development



Protecting sensitive data. Mitigating insider threats and solid regulation compliance



Security activities are usually not adapted in agile methodologies

Addressing SSL – Why?

Let's take a step back

Failing to firmly prioritize software security can lead to serious consequences



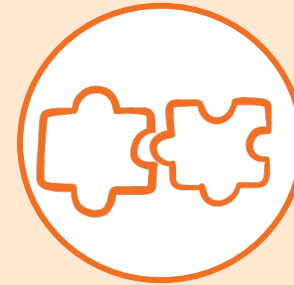
Lack of
understanding



Cost



Time constraint



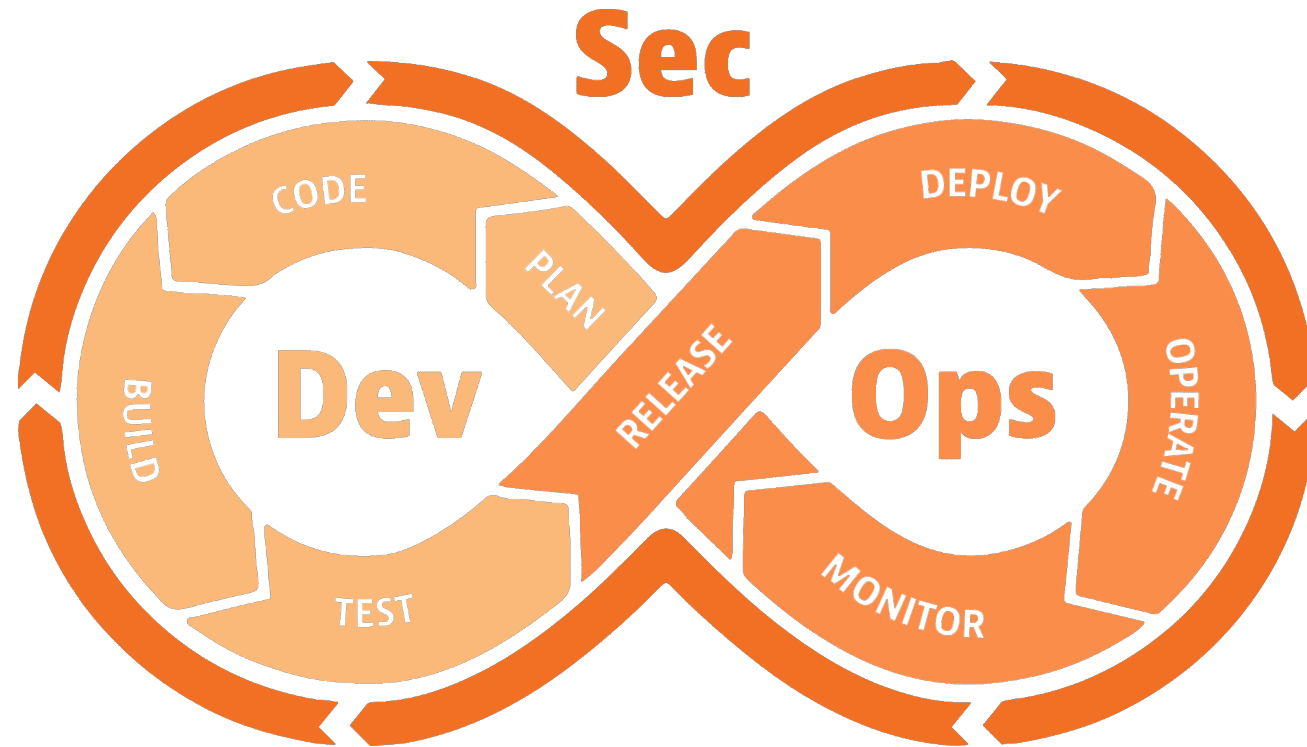
Prioritization of
features over
security



Perception of
invincibility

That's why DevSecOps methodology comes to light

DevSecOps



The "Sec" process wraps the well-known DevOps framework which is already in place for most companies that build software.

Pillars of DevSecOps



Rapid, cost-effective software delivery

In a non-DevSecOps environments security issues can easily be both time and cost consuming.



Improved, proactive security

Cybersecurity issues are address as soon as they are identified. In all SDLC/stages. Before aditional dependencies are used, placed, or coded.



Accelerated security vulnerability patching

The ability to identify and patch common vulnerabilities and exposures Common Vulnerabilities Exposures. (CVE) is diminished.



Automation compatible with modern development

Can be integrated into an automated test suite for operations teams if an organization uses a CI/CD pipeline to ship their software.

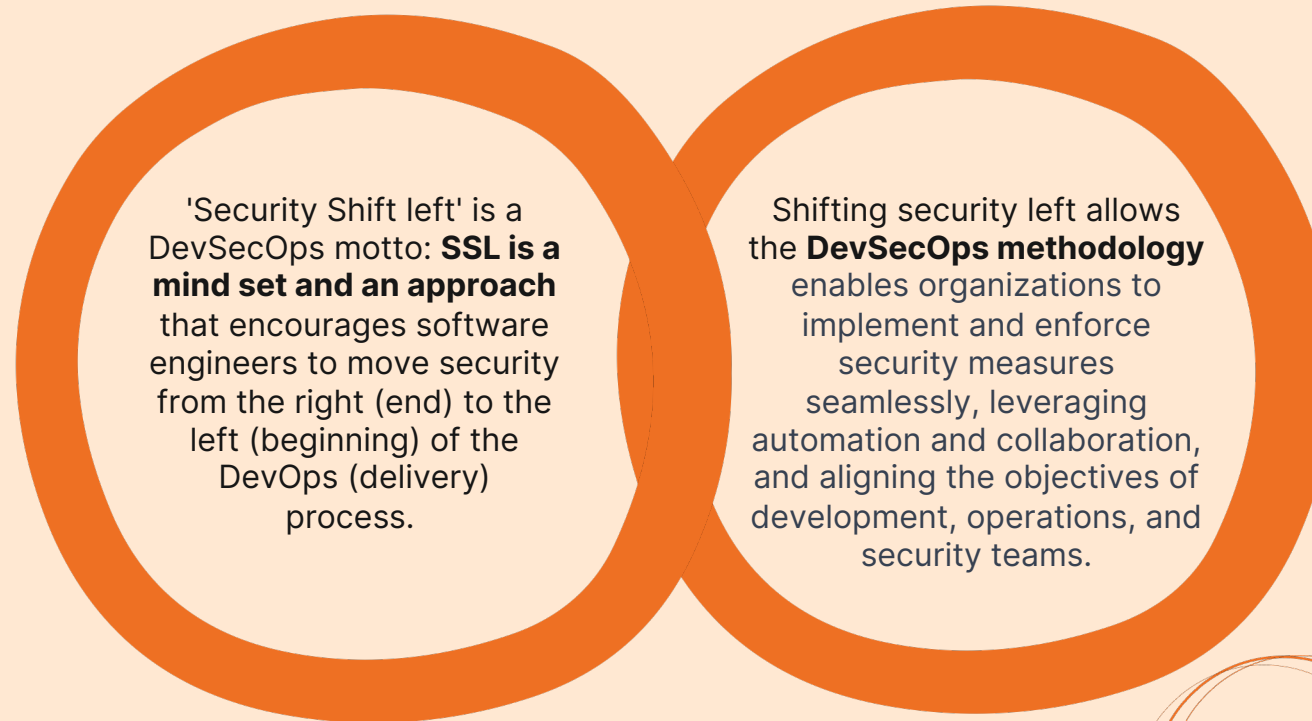


A repeatable and adaptive process

A mature implementation of DevSecOps ensures consistent security across changing environments and requirements. Resulting in a solid automation, configuration management, orchestration, containers, immutable infrastructure, and even serverless compute environments.

SSL vs DevSecOps

Relationship lies in their shared goals



● Speed vs Security

● Skill vs Mindset

● Lack vs Positive Communication

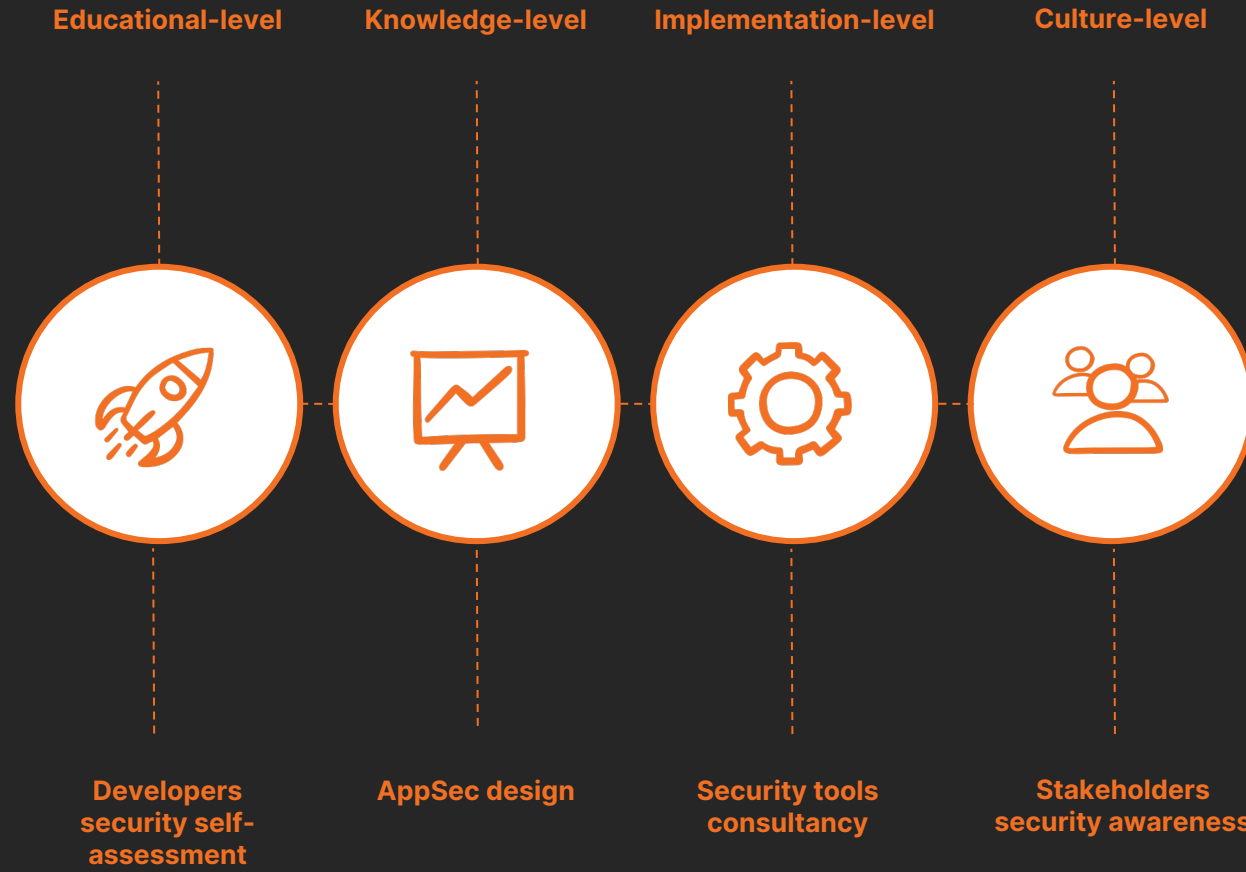
80%

Skills gap. 80% of organizations tell us they have a hard time finding and hiring security professionals and 71% say it's impacting their ability to deliver security projects

*Gartner's Security and Risk Management Summit

Sorint's Tailored Journey

How we shift security to the left



Closer Look

Areas and fields of focus



Developers security self-assessment

Measure the overall development team knowledge about security related-topics.

Identify lack of common security principles/knowledge.

Build a roadmap to plan the actual "Shift Left".

AppSec design

Evaluate/identify possible threats and how to address each of them.

Deliver a threat model that is a conceptual representation of the system and the threats that have been identified.

Security tools consultancy

Implement and configure SCA, SAST and DAST tools within the CI/CD pipeline.

Experts advise best practices to properly configure these tools, and support developers to better understand the results.

Suitable AST tools depending on projects.

Developers security awareness

Best practices for secure/defensive coding and how to avoid common mistakes.

Support developers to build their own "security mindset"

Customized trainings/workshops

Experts Involved



Shift Security Left(SSL)



DevArch



SecOps

Cesare Pizzi

Reverse Engineer, Incident Responder,
Opensource Developer and Contributor

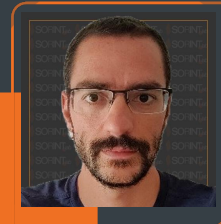
CTF player, trainer, conferences regular
speaker at DEFCON, Insomni'hack,
Nullcon



Luca Famà

Application Security Consultant

+7 years of experience in the security
field. CTF player, bug hunter and cyber
security enthusiast.



Some prestigious certifications



Leading to

Manifestation of success



Secure Design and
Culture



Threat Modelling



Secure Implementation



Secure Verification



Production Security Monitoring



Incident Management

Bonous Slide

Related Solutions and Tools by Sorintians



Sorint Sec Business Unit

Sorint.SEC is the Cybersecurity Company of Sorint.Lab Group that operates exclusively and continuously on issues related to Information Security.

sec.sorint.it



Agola – CI/CD Redefined Open source software product

☆ Star 1.3k

CI/CD system with a lot of great features like advanced and reproducible workflows (runs), containerized tasks, fully distributed, high-available and much more. Featured on Cloud Native Landscape.

www.agola.io



DevOps Engineering Technology Consultant Service

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

[inquire](#)



SYNwall Open source software product

☆ Star 260

A zero-configuration (IoT). A different way to think firewalling. Brings to you a totally new way to approach firewalling: you don't have to worry anymore about rules, IP, ports, etc

[github/SYNwall](https://github.com/SYNwall)



REW - sploit Open source software product

☆ Star 127

Emulate and Dissect MSF and *other* attacks. Rew-sploit helps you analyze Windows shellcode or attacks coming from Metasploit Framework, Cobalt Strike, or other malicious or obfuscated code.

github.com/REWsploit



Dock12 Blog

A port bar on Ceres Station in "The Expanse". This aims to be a place where people can chat (like in a bar) about topics related to security and more.

dock12.sorint.com

Success stories



Delivered by: Sorintians



Confidential

A Well Know Financial Institution Introduce Shift Security Left

Challenge

Client is developing a critical software app. Requirements included:

- Compliance with industry standards and regulations.
- Regulate and intermediate the workflow and pipelines.
- Introduce and increase security awareness and practices.
- No security measures implemented. Low security awareness .

Going forward

Intensive self-assessment sessions with security and development teams.

Accepting the challenge - Solution and Implementation

In a proposal form.

- A new workflow to remove obstacles between the teams.
- Workshop to introduce new tools and how to use/read the outputs: e.g.
 - SAST(Static Analysis Security Testing) to find vulnerability patterns in source code.
 - SCA (Software Composition Analysis) assessment done by third-party.
- Help development team choose the final pipeline tools.

Result & delivery

- Discussed all the finding with both teams. (Security Development)
- Submitted multiple reports on the security level of the application.
- Agreed on a smooth and seamlessly automated workflow embraces security.
- Guide a solid security-aware culture throughout the company. Long-lasting and will influence other software projects in the company.

Going Forward



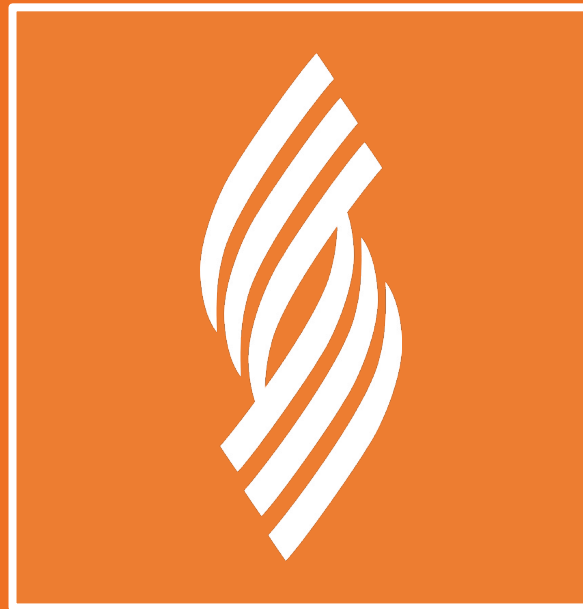
How we can move from here

One hour
workshop

Read more on:
[/sorintLab](#)



Alternative
approach



BUILDING GREAT
TECHNOLOGY



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