SORINTlab

BUILDING GREAT TECHNOLOGY

SecOps

Digital Technology Service

October 2023

All rights reserved Sorintlab©

Agenda

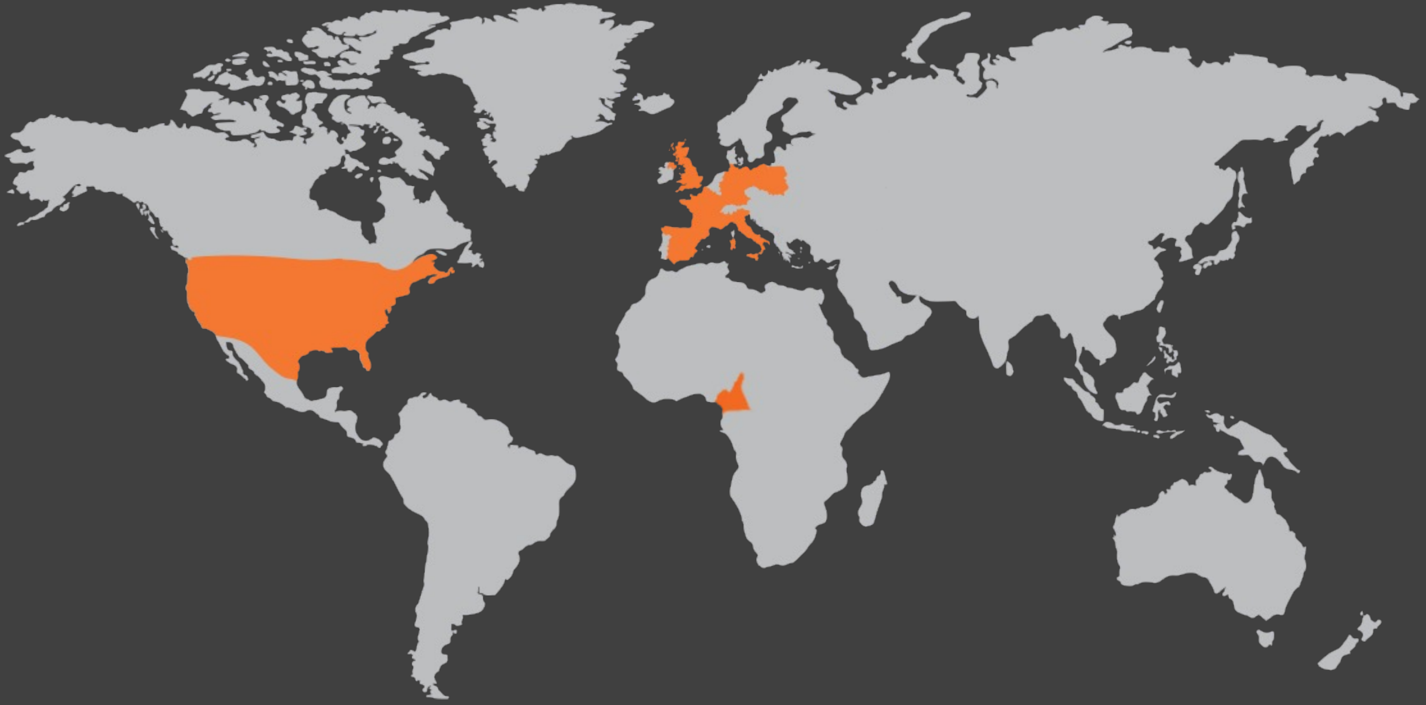
- Who are we
- Overview
  - Cybersecurity in number
- Sorint’s Tailored Journey
  - SecOps
  - The Process
  - Detecting & monitoring
  - Penetration
  - Sorint4Security
  - Experts Involved
  - Certifications
- Success Stories
- Bonus slide - Related by Sorintains
- Going Forward

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

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

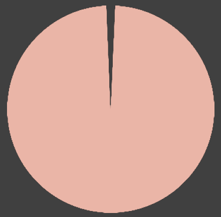
Finance & Insurance,
Utility & Telco,
Industry & Services,
Transport,
Public Administration

98%

Customer

Retention

Rate



Clients

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

- aws partner network Advanced Consulting Partner
- Microsoft Azure
- CANONICAL
- Check Point SOFTWARE TECHNOLOGIES LTD
- CISCO
- CiTRiX Partner Silver Solution Advisor
- cloudera connect BRONZE PARTNER
- COMMVAULT
- confluent
- Couchbase
- DARKTRACE
- DATADOG
- DELL Technologies
- dynatrace
- elastic
- entando A digital world without boundaries
- exabeam
- Extreme Customer-Driven Networking
- FIREEYE
- ForeScout
- FORTINET
- Google Cloud Partner
- HashiCorp
- hazelcast
- HITACHI Inspire the Next
- Hewlett Packard Enterprise
- HUAWEI
- IBM Business Partner
- imperva
- Inuvika
- MariaDB
- Silver Microsoft Partner
- mongoDB
- NetApp
- netskope
- ORACLE
- paloalto NETWORKS
- PICUS
- proofpoint
- Qualys
- Red Hat Premier Business Partner
- rubrik
- SentinelOne
- SIREN DATA INTELLIGENCE
- splunk>
- sysdig
- SUSE Platinum Partner
- TRILIO
- veeAM Accredited Service Partner
- VERITAS
- vmware

Technology Partners

SecOps

Digital Technology Service

- SecOps framework involves integrating security practices, principles, and tools to ensure a more proactive and comprehensive approach towards cybersecurity.
- Aiming to enhance an organization's capability to identify, address, and alleviate security incidents and vulnerabilities.
- Some of the key components and activities might include
  - Security information and event management (SIEM)
  - Network security monitoring (NSM)
  - Endpoint security
  - Vulnerability management
  - Incident response (IR)
  - Threat intelligence
  - Access control
  - Security awareness and training

10.5
Trillion

Is the inflicted damage by cybersecurity by 2025. From 6 trillion in 2021. 15% yearly growth.

*Cybersecurity Ventures Magazine

A raised concern

Cybersecurity attacks in numbers

45% small businesses

Organizations of all sizes are target.

Phishing 36% of breach

The technique emphases the need of internal staff training.

$20 billion in 2021

Cost of ransomware could lead to financial distress or bankruptcy in some cases.

$265 billion **by 2031**

Healthcare 45% increase

Highlights the importance of customer's data.

30% increase on remote workers

Covid 19's work from home initiative opened doors for more security vulnerabilities.

Average cost increased 42%

Over the last 3 years. The average cost of cyberattacks increased 42%.

25 billion connect device

By 2025

Indicated more security vulnerabilities and measures.

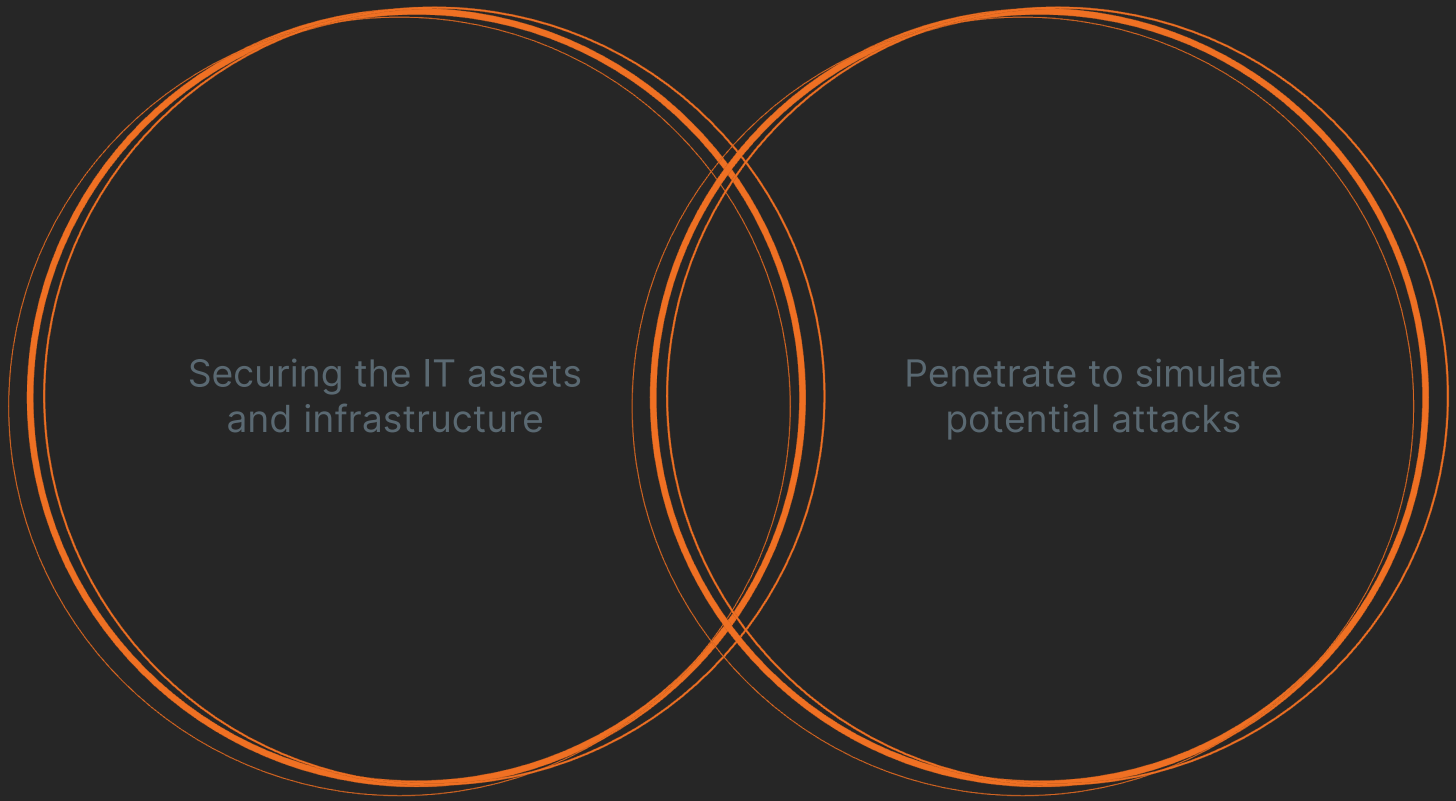
CEOs 86% responsible

Due to the severe impacts that could emerge.

Respondents of a study held 86% responsible to c-level management.

SecOps

Relationship lies in their shared goals

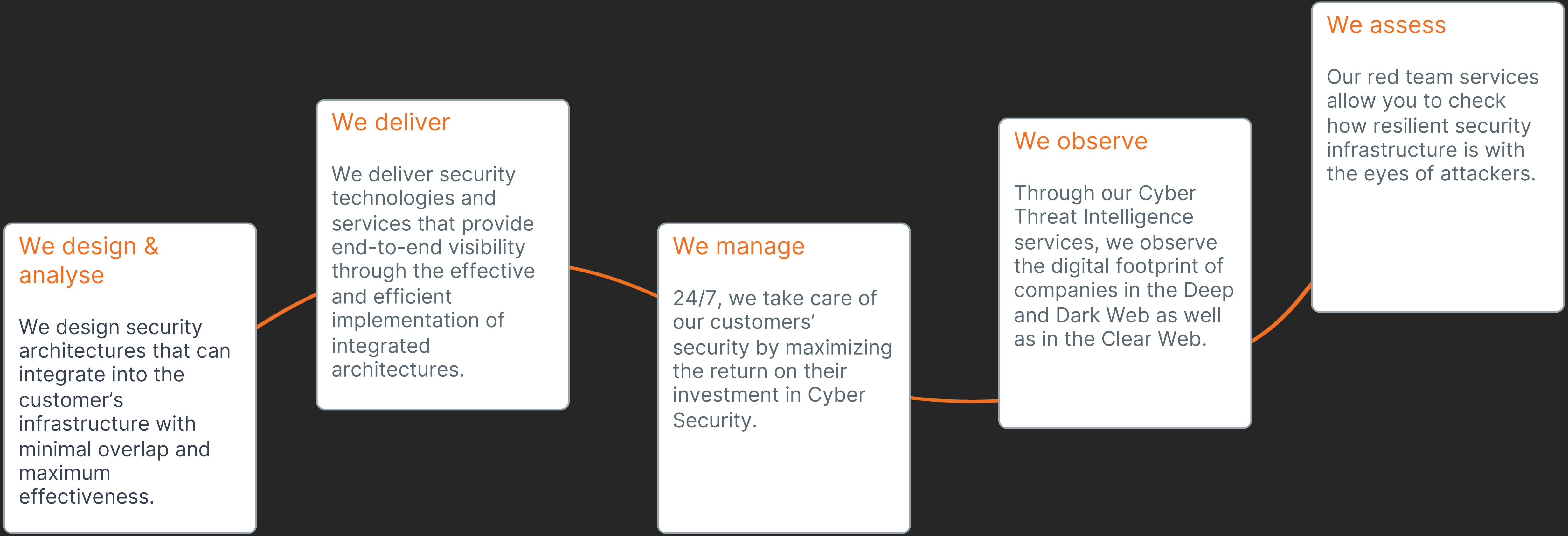

Securing the IT assets and infrastructure
Penetrate to simulate potential attacks

Also known as team blue & team red

Readiness & 360° view of security posture

Sorint’s Tailored Journey

High-level overview



We design & analyse

We design security architectures that can integrate into the customer’s infrastructure with minimal overlap and maximum effectiveness.

We deliver

We deliver security technologies and services that provide end-to-end visibility through the effective and efficient implementation of integrated architectures.

We manage

24/7, we take care of our customers’ security by maximizing the return on their investment in Cyber Security.

We observe

Through our Cyber Threat Intelligence services, we observe the digital footprint of companies in the Deep and Dark Web as well as in the Clear Web.

We assess

Our red team services allow you to check how resilient security infrastructure is with the eyes of attackers.

Sorint’s Tailored Journey

Monitoring and detecting - The make it model

Risk assessment

Identifying, evaluating, and understanding potential threats on infrastructure, systems, network, data, and running apps.

Threat analysis

Deeper understanding of the potential risks, domain, and characteristic.

Threat Intelligence (CTI) platforms
Malware analysis tools

Prevention measures

All proactive activities to mitigate potential risks and solidifying the security posture.

EDR, firewalls, multi-factor authentication systems, data encryption systems

Monitoring

Regular monitoring of IT infrastructure

Intrusion Detection Systems (IDS)
Intrusion Prevention Systems (IPS)
Security Event Management Systems (SIEM)
Application Firewalls (WAF)
Cloud and Containers Security

Collaboration

Smooth flow of communication between all stakeholders

Security case management platforms (Ticketing tools),
Document management systems.

Incident response

Protocols designed to effectively manage and reduce the impact of /prevent security incidents as they happen.

Incident response systems
Incident orchestration platforms (SOAR).

Reporting

Reporting tools and documentation practices.

Consulting and support

Continues support in all security related matter.

Ensure stakeholders are aware of the fundamentals/protocols.

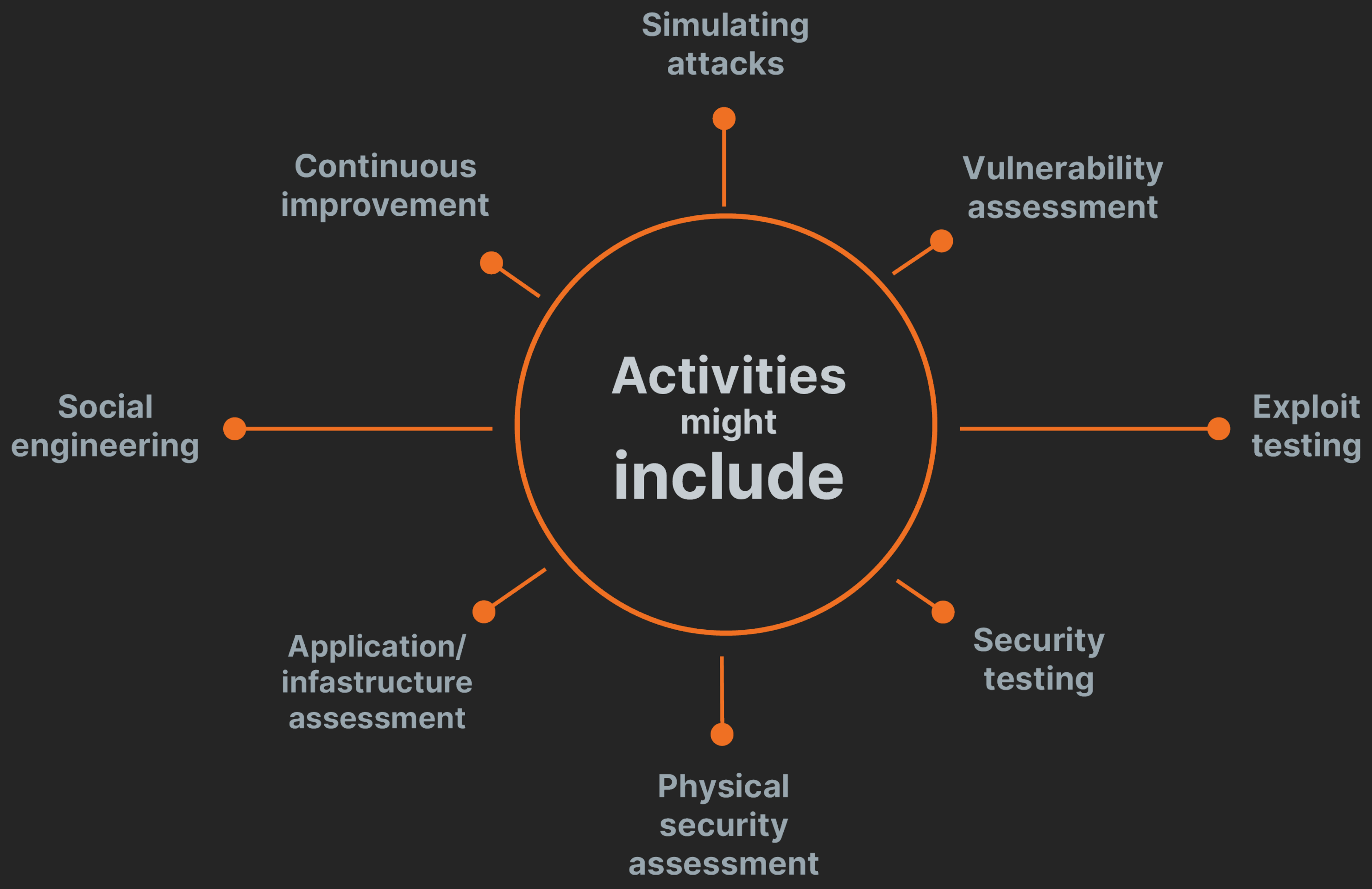
Knowledge management systems
Online training tools

Supporting the IT operations team to ensure that security processes are properly integrated into daily operations

Sorint’s Tailored Journey

Penetration - The make it model

Staying ahead of emerging threats and outpacing intrusion attempts



Activities might include

Simulating attacks

Vulnerability assessment

Exploit testing

Security testing

Physical security assessment

Application/ infastructure assessment

Social engineering

Continuous improvement

Sorint4Security

Mastering cybersecurity since mid-1990s

Dedicated sircles targeting various areas of security

Legend team in the field

Training hours

Fully handling security activities of prominent entities, in various industries, in Europe, US, and Africa.

Community support & developed various open-source security related tools

24x7x365 days support

Highest field accreditation

Hands-on tools experience and accreditation

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

Experts Involved

- SecOps
- Network & Security
- Shift Security Left(SSL)
- Cloud-Native Security
- NGMS

Senior masterminds

Davide Chinnì

Cyber Security Analysts | Incident Responder | SecOps Specialist

+10 years of experience in network & cyber security. Cyber security enthusiast

Cesare Pizzi

Reverse Engineer | Incident Responder | Opensource Developer and Contributor

CTF player, trainer, 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

OFFENSIVE security
OSED
GIAC REVERSE ENGINEERING MALWARE
GREM
CHECK POINT
CCSA
Certified Security Administrator
CERTIFICATION
CISCO CERTIFIED
CCNA
ROUTING & SWITCHING
CompTIA
Security+
CyberDefenders
FIREEYE
SOPHOS
splunk>
EC-Council
E|HA
ETHICAL HACKING ASSOCIATE
AXELOS
ITIL
FOUNDATION

Some Prestigious Certificates

From technology/vendor, skill levels, IT domains/specialization, to vender-neutral certifications

3CX
6sigma
Aerohive
Aerohive Networks
Alison
ALTARO
Amazon
AMPG International
APMG
Apple
Aruba
AXELOS
Barracuda
BIT
Blue Team
BMC
Brocade
Business Objects
CEPIS
CertProf
Check Point
Cisco
Citrix
Cloud Champion
Cloudera
Cobit

COMMVAULT
Company Tutor
Compaq
CompTIA
CROSSNOVA
CSSC
Cyberark
D-LINK
Databricks Academy
DataCore
DELL EMC
Devops Institute
Dynatrace
Ec-Council
ECDL
Edx
eipass
Elastic
eLearnSecurity
EMC
EnterpriseDB
enVision
EUCIP
EXIN
Extreme Networks
F5

FacilityLive
FinOps Foundation
FireEye
ForeScout
FORTINET
GIAC
GitLAB
Google
Google Cloud
Google Play Academy
HashiCorp
Hazelcast
Hitachi
HP
Huawei
IBM
Infoblox
INIM Eletronics
Istituto Italiano di Project Management
ISTQB
Juniper
Konnex
Lacework
LibraEsva
Linux Foundation
Linux Professional Institute

MariaDB
Meru
MIA-PLATFORM
Microsoft
MikroTik
MongoDB
Neo4j
NetApp
Netscreen
Netskope
Netwitness
NETWRIX
Novell
NUTANIX
ObserveIT
Offensive Security
OpenSecurityTraining2
ORACLE
Palo Alto
People Cert
PMI
Qualys
Rancher Academy
Red Hat
Reevo Cloud Academy
Reuters

SCP
Scrum Alliance
Scrum.org
ScrumStudy
SonicWall
SOPHOS
Splunk
Stormagic
Sun
SUSE
Symantec
TERADATA
Toshiba
Trend Micro
Triton
Veeam
Vendor
Veritas
VMware
WatchGuard
WatchGuardONE
WEBROOT University
ZERTO
ZyXEL

ISO 27001
ISO 20000-1
ISO 9001
ITIL

Closer Look

Areas and field of focus

Monitoring & Detecting	Penetration	Consultancy	All journey
360 view around the clock SOC activities	Executing, reporting, and consultation Might include handling reported issues	In-depth analysis of project posture, team awareness, and a customized going forward strategy Processes, methodologies, tools, & workshops	Cybersecurity governance

Success stories

Delivered by: Sorintians

Confidential

Technology Industry

EDR Solution, Design, & Implementation for All Endpoints

Challenge

Find, configure, and deploy an EDR (Endpoint Detection & Response) tool. Thousands of endpoints.

- Windows environment (CrowdStrike)
- Linux environment (SentinelOne)

Going forward

Investigation phase focused deeply on analysing client's infrastructure & evaluating possible relevant tools. Resulting in a group of POCs and tests. Along with a clear deployment proposal.

Result & delivery

- Successful deployment.
- Documentation & reporting activities.
- Testing activities not only to validate, but also to prototype to the client.
- SecOps sircle has been granted long-term support, maintenance, and monitoring to the solution.

Accepting the challenge - Solution and Implementation

After the tool selection phase. The deployment phase included activities such as:

- Automation system to convert detections into a streamlined ticketing process.
- Developed customized scripts to accelerate forensic collection & forensic analysis of the endpoint.
- Configuring the EDR in compliance to client's standards/policies.

Activities aiming to provide real-time visibility of the detected threats and isolating them from the network. Providing accurate analysis.

- Introduced a streamline process on how threats are handled through automation. Elements including identification, scanning, where and how to operate on the threat(isolated-manner, or on the network), malicious pattern against YARA rules, incident timeline, recovery resetting/rebuilding, etc..

Success stories

Delivered by: Sorintians

Confidential

Technology Industry

Implementation and Management of a SIEM Solution

Challenge

A SIEM tool able to:

- Handle huge number of logs arriving from client's endpoints.
- Automate tasks to support client's SOC and NOC workflows.

Going forward

Evaluating client's SOC and NOC workflow during the tool selection phase. Closely aligning with client's internal team.

Accepting the challenge - Solution and Implementation

Following the evaluation process and the agreement on the proposal submitted. SIEM Elastic was the go-to-choice due to the capability of being a modular/unified, scalable, and on top, being an open-source solution. Importantly, allowing SOC analysts to conduct swiftly analytical security events. Furthermore, the implementation phase carried out activities like:

- Identifying the data source.
- Implementation of data ingestion.
- Monitoring volume alerts during staging phase.
- Built-in detection rules and the addition of IoC through integration of one or more threat intelligent feed.

Result & delivery

Within the agreed timeframes, a high-quality software product that fully complied to all pre-planned requirements. E.g.

- Multi-functional user role system.
- Monitoring thousands of end-points.
- Improved user interface.
- Optimized performance.
- Quality code due to a solid code reviews strategy.

Success stories

Delivered by: Sorintians

Confidential

Reporting Major XSS Bug Vulnerability To UpdraftPlus

Black-box Penetration Testing – WP extension

Challenge

While carrying out penetration test activities to a client's web solution. Our security team were able to detect a critical XSS bug for the extension WP-Optimize (+1 million active installation). Developed by Team UpdraftPlus. A well-known WordPress plugin.

Going forward

The bug was documented & reported to the providers.

Result & delivery

- Bug was documented and reported to the providers immediately after Sorint's internal security review process.
- Vendor immediately responded to handling the bug and included it in the next release.
- The provider issued a CVE ID (2023-1119) as a gesture of appreciation to the effort and the finding.

Accepting the challenge - Solution and Implementation

As a summary, the challenge was complicated to proof. It required tools/extensions (WPScan, WordFence Security, and others) several attempts, injecting payloads, probing the search function using Burp Intruder as an attack type, plus refining the tactics of the attacks. After few attempts, we were able to get the XSS-reflected payload.
The team was able to analyse how the WebP-Conversion option causes a flow during the process of converting HTML entities to the reserved HTML characters. Clearly an issue. Attackers can inject malicious input encoded using HTML entities and str_get_html function. The function will convert it back to actual HTML tags, where the browser will be able to render it. Bypassing Wordfence filtering, which happens before the str_get_html function.

Bonous Slide

Related Solutions and Tools by Sorintians

SORINT SEC

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

SSL - Shift Security Left
Technology Consulting Service

SSL promotes security as a common responsibility shared by all teams involved in software development. The service follows DevSecOps as a methodology.

Inquire

NGMS
Core IT Services

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

☆ Star 260

SYNwall
Open-source software product

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

☆ Star 127

REW SPLOIT

REW - sploit
Open-source software product

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

github.com/REWsploit

DOCK12

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

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