SORINT.lab

BUILDING GREAT TECHNOLOGY

# SecOps

## IT Operations 24x7

## Agenda

- SecOps by Definition
- Monitoring, Detecting, & Penetrating
- 24x7 Operations
- Why SORINT.lab?
- Service’s Delivery Models

SORINT lab

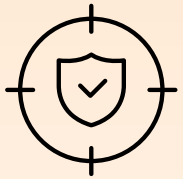
# SecOps

Integrating security practices, principles, and tools to ensure a more comprehensive proactive approach towards your organization's cybersecurity.

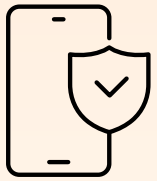
Identify, address, and alleviate security incidents and vulnerabilities.

Key activities might include

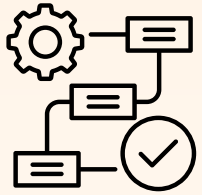
Security information and event management (SIEM)



Network security monitoring (NSM)



Endpoint security

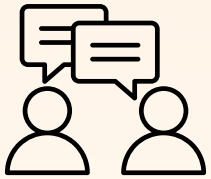


Vulnerability management

Incident response (IR)

Threat intelligence

Access control



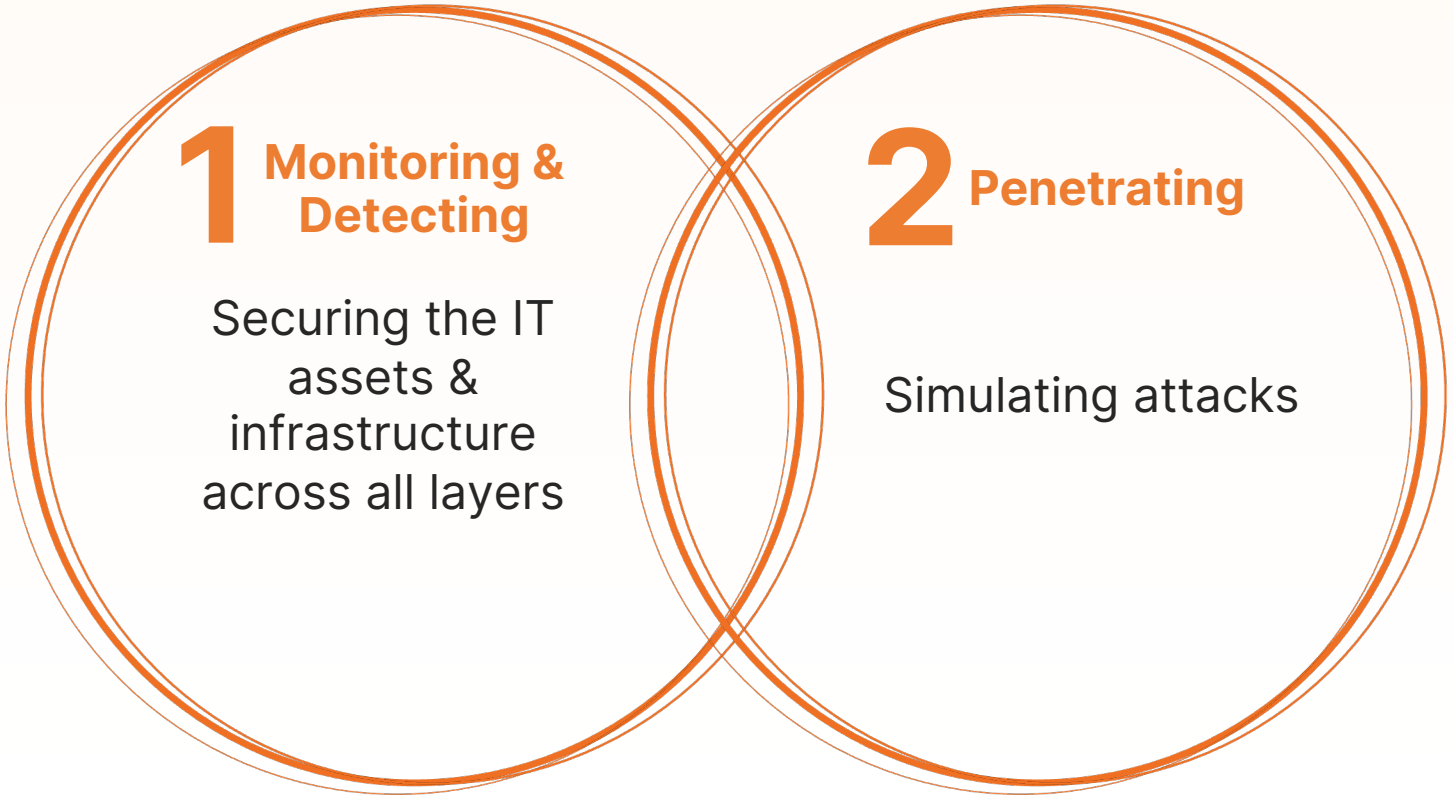
Security awareness & training

SORINT.lab

# SecOps Fundamentals

Readiness & 360 visibility on security posture

## A relationship that lies on one shared goal



SORINT.lab

# Monitoring & Detecting

## Risk assessment 1

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

## Threat analysis 2

Deeper understanding of potential risks, domain, and characteristic.

Cyber Threat Intelligence (CTI) Platforms & malware analysis tools.

## Prevention measures 3

Ongoing proactive activities to mitigate potential risks and solidifying security posture.

EDR, firewalls, multi-factor authentication systems, data encryption systems, for instance.

## Regular monitoring 4

**(IDS)** Intrusion Detection Systems
**(IPS)** Intrusion Prevention Systems
**(SIEM)** Security Event Management Systems
**(WAF)** Web Application Firewalls
**(CNAPP)** Cloud & Containers Security

## Collaboration 5

Smooth means of communication between all stakeholders.

Security case management platforms (ticketing tools).

Document management systems & procedures.

## Incident response 6

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

Incident Response Systems
Incident Orchestration Platforms (SOAR).

## Reporting 7

Reporting mechanism, tools and documentation practices. Reference to needs and SLA defined.

## Consulting & support 8

Continuous support to maintain security health and stakeholder awareness of all critical protocols, driven by accessible knowledge management and online training.
Business & technical.

SORINT lab

## Penetrating

# Staying ahead of emerging threats & outpacing intrusion attempts

# 24x7 – Global Coverage

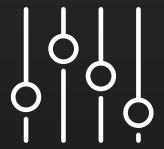
## Services

Incident and Request Management

3rd Party Supplier Management

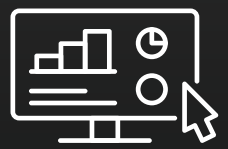
Release Management

Problem Management

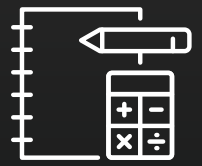


Capacity Management

SecDevOps Support



Monitoring/ Observability event management



Cost Optimization

Provisioning & Configuration

Performance Health Check

## Domains

Service Desk

Multi-cloud Infrastructure Support

Application Support

DevOps

SecOps

3rd vendor Support

# The Make IT Model

## Overview on the journey

**We design & analyze**
A tailored solution, model & roadmap that can integrate into client's tech and business ecosystem with minimal disruption. Check marking overall objectives incompliance regulations

**Deliver & implement**
Technologies , procedures, and other related services inline with the agreed governance approach.

**Manage**
By integrating the tailored operational model and enabling the end-to-end visibility needed, this phase deliver maximum cybersecurity ROI for your organization.

Dynamic SLA. Up to 24/7. Globally.

**Observe**
Through our Cyber Threat Intelligence services, we observe the digital footprint of companies. Reaching as far as Deep and Dark Web, and Clear Web.

Iteratively proactively!

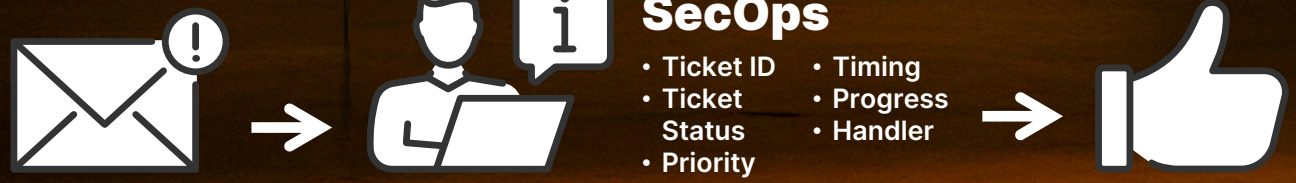
**Assess**
In parallel, dedicated red team, & services, brings findings on resiliency from within the attacker's perspectives.

Iteratively proactively!

Day x — Continues support — **Multi-disciplinary approach** — Continues support — **Shoulder-to-shoulder with client's team** — Continues support — **Quality assurance team & SLA compliance** — Day y

# 99% SLA compliance maintained

SORINT offers this service to +100 prominent entities in Europe, US, & Africa



**SecOps**

- Ticket ID
- Ticket Status
- Priority
- Timing
- Progress
- Handler

**Your IT Will Change, Your Business Will Change too!**

# A multidisciplinary approach to a wide range of IT fields & domains

- Network Administration
- System Administration
- Database Management
- Cloud Computing
- IT Support
- IT Consulting
- Big Data
- Software Development
- Cybersecurity
- Advanced Analytics & Business Intelligence
- IT Project Management
- Enterprise Resource Planning
- Virtualization and Cloud Infrastructure
- Data Science
- Governance & Compliance
- Artificial Intelligence & Machine Learning

Certification & Training

# +130 major & various

## Training Partner to some IT vendors

3CX
COMMVAULT
FacilityLive
MariaDB
SCP
6sigma
Company Tutor
FinOps Foundation
Meru
Scrum Alliance
Aerohive
Compaq
FireEye
MIA-PLATFORM
Scrum.org
Aerohive Networks
CompTIA
ForeScout
Microsoft
ScrumStudy
Alison
CROSSNOVA
FORTINET r
MikroTik
SonicWall
ALTARO
CSSC

GIAC
MongoDB
Amazon
Cyberark
GitLAB
Neo4j
SOPHOS
AMPG International
D-LINK
Google
NetApp
Splunk
APMG
Databricks Academy
Google Cloud
Netscreen
Stormagic
Apple
DataCore
Google Play Academy
Netskope
Sun
Aruba
DELL EMC
HashiCorp
Hazelcast

Netwitness
SUSE
AXELOS
Devops Institute
NETWRIX
Symantec
Barracuda
Dynatrace
Hitachi
HP
Novell
TERADATA
BIT
Ec-Council
Huawei
NUTANIX
Toshiba
Blue Team
ECDL
IBM
ObservelT
Trend Micro
BMC
Edx
Infoblox
Offensive Security
Triton
Brocade

eipass
INIM Eletronics
OpenSecurityTraining2
Veeam
Business Objects
Elastic
Istituto Italiano di Project
ORACLE
Vendor
CEPIS
eLearnSecurity
Management
Palo Alto
Veritas
CertProf
EMC
ISTQB
People Cert
Check Point
EnterpriseDB
Juniper
PMI
VMware
Cisco
enVision
Konnex
Qualys

WatchGuard
Citrix
EUCIP
Lacework
Rancher Academy
WatchGuardONE
Cloud Champion
EXIN
LibraEsva
Red Hat
WEBROOT University
Cloudera
Extreme Networks
Linux Foundation
Reevo Cloud Academy
ZERTO
Cobit
F5
Linux Professional Institute
Reuters
ZyXEL

# Technology Landscape

**Cloud Infrastructure & Platform Services**

aws, Microsoft, Google Cloud, HashiCorp, ORACLE, vmware by Broadcom

**Enterprise Backup & Recovery Software Solutions**

DELL Technologies, rubrik, COMMVAULT, VERITAS, veeam, TRILIO

**DevOps Platforms**

mia Platform, aws, Microsoft, Google Cloud, Red Hat, GitLab, vmware by Broadcom

**Distributed File & Object Storage**

DELL Technologies, HUAWEI, NetApp, SUSE, Hitachi Vantara

**Primary Storage**

HUAWEI, DELL Technologies, Hewlett Packard Enterprise, NetApp, Hitachi Vantara

**Container Management**

aws, ORACLE, CANONICAL, nethopper, Google Cloud, Microsoft, Red Hat, CLASTIX, SUSE, vmware by Broadcom

**Application Performance Monitoring**

Microsoft, dynatrace, splunk>, DATADOG, CISCO, elastic

**Cybersecurity**

CISCO, FORTINET, KnowBe4, SUSE, elastic, splunk>, aqua, LACEWORK, sysdig

**Database Management Systems**

Microsoft, EDB, Cockroach Labs, CLOUDERA, mongoDB., ORACLE, Couchbase, Redis, HAZELCAST, MariaDB, MySQL, aws

**Data Streaming**

Red Hat, CONFLUENT, CLOUDERA, HAZELCAST

**Internal Development Platform**

mia Platform, Red Hat, nethopper, GitLab

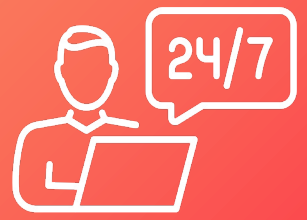
# Tackling Challenges with SORINT.lab

## sircles

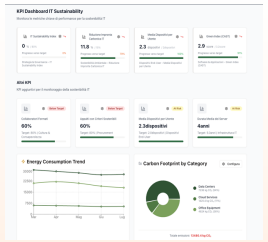
A framework which allows effective collaboration across specializations, maximizing value by involving experts from every field. Smoothly!

## Managing & Operating

IT and cybersecurity of prominent organizations in Europe, US, and Africa




Assessment portals & templates
to better demonstrate the unique needs & project governance attribute!



## End-to-end Technology Support

Holistic IT & governance capabilities, rather than a point solution

## 100% Vendor Independent – Purpose

Believe in technology that fosters innovation and human wellness. Our commitment towards every company, institution or community is to help them run their business and solve their problems through a choice of the best technology.

**98%** Customer Retention Rate

# Offering's Delivery Models

**Consultation**
Assessment phase includes evaluation and consultation on current posture. Delivering a business & technical proposal submission.

**Project scoped**
Client's defined deliverables, such as, vulnerability assessment, threat modeling, tool choice, deployment, targeted educational upskilling.

**24x7 SecOps**
Full, or partially, managing & operation.

Managed Detection and Response (MDR), along Managed Security Services, in accordance with SLA.

# Request Case Studies

**We are all ears!**
A discovery call with a technical engineer, or a business representative.
welisten@sorint.com
www.sorint.com/contact

**Read more – Our 3 blogs**
A formal business blog, SORINTian's vibrant space with a transparent and unique writing style, or dedicated cybersecurity publications
www.sorint.com/blogs

**Follow us**

# BUILDING GREAT TECHNOLOGY

SORINT lab

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

www.sorint.com