SecOps
Digital Technology Service
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

USA
San Diego

AFRICA
Douala

Other Business Units
### Overview Facts

<table>
<thead>
<tr>
<th>Tech-Savvy</th>
<th>Methodology</th>
<th>PM Methodology</th>
<th>Market</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>900+</td>
<td>ISO 27001</td>
<td>Prince2</td>
<td>Finance &amp; Insurance, Utility &amp; Telco, Industry &amp; Services, Transport, Public Administration</td>
<td>35+ Years of experience with a Startup mindset</td>
</tr>
<tr>
<td>Cloud Engineers</td>
<td>ISO 20000</td>
<td>PMI</td>
<td>98% Customer Retention Rate</td>
<td></td>
</tr>
<tr>
<td>SREs</td>
<td>ISO 9001</td>
<td>Agile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DevOps Engineers</td>
<td>ISO 14001</td>
<td>SCRUM/UX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Stack Developers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+40000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training hours per year</td>
<td>ISO Certified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50+</td>
<td>Technical Sircles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Enterprise Customers</td>
<td>Methodology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 40000 Training hours per year
- 35+ Years of experience with a Startup mindset
- 98% Customer Retention Rate
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

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 emphasizes the need of internal staff training.

$20 billion in 2021
Cost of ransomware could lead to financial distress or bankruptcy in some cases.

Healthcare 45% increase
Highlights the importance of customer’s data.

$265 billion by 2031

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/infrastructure assessment
- Continuous improvement
- Social engineering
Sorint4Security
Mastering cybersecurity since mid-1990s

- Dedicated circles 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

- Davide Chinni
  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.

Senior masterminds

Some prestigious certifications
### Some Prestigious Certificates

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

<table>
<thead>
<tr>
<th>3CX</th>
<th>6sigma</th>
<th>Aerohive</th>
<th>Aerohive Networks</th>
<th>Alison</th>
<th>ALTARO</th>
<th>Amazon</th>
<th>AMPG International</th>
<th>Apple</th>
<th>Aruba</th>
<th>AXELOS</th>
<th>Barracuda</th>
<th>BIT</th>
<th>Blue Team</th>
<th>BMC</th>
<th>Brocade</th>
<th>Business Objects</th>
<th>CEPI</th>
<th>CertProf</th>
<th>Check Point</th>
<th>Cisco</th>
<th>Citrix</th>
<th>Cloud Champion</th>
<th>Cloudera</th>
<th>Cobit</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAVAULT</td>
<td>Company Tutor</td>
<td>Compaq</td>
<td>CompTIA</td>
<td>CROSSNOVA</td>
<td>CSSC</td>
<td>Cyberark</td>
<td>D-LINK</td>
<td>Databricks Academy</td>
<td>DataCore</td>
<td>DELL EMC</td>
<td>Devops Institute</td>
<td>Dynatrace</td>
<td>Ec-Council</td>
<td>ECDL</td>
<td>Edx</td>
<td>eipass</td>
<td>Elastic</td>
<td>eLearnSecurity</td>
<td>EMC</td>
<td>EnterpriseDB</td>
<td>enVision</td>
<td>EUCIP</td>
<td>EXIN</td>
<td>Extreme Networks</td>
</tr>
<tr>
<td>FacilityLive</td>
<td>FinOps Foundation</td>
<td>FireEye</td>
<td>ForeScout</td>
<td>FORTINET</td>
<td>GIAC</td>
<td>GitLAB</td>
<td>Google</td>
<td>Google Cloud</td>
<td>Google Play Academy</td>
<td>HashiCorp</td>
<td>Hazelcast</td>
<td>Hitachi</td>
<td>HP</td>
<td>Huawei</td>
<td>IBM</td>
<td>Infoblox</td>
<td>INIM Eletronics</td>
<td>Istituto Italiano di Project Management</td>
<td>ISTQB</td>
<td>Juniper</td>
<td>Konnex</td>
<td>Lacework</td>
<td>LibraEsva</td>
<td>Linux Foundation</td>
</tr>
<tr>
<td>MariaDB</td>
<td>Meru</td>
<td>MIA-PLATFORM</td>
<td>Microsoft</td>
<td>MikroTik</td>
<td>MongoDB</td>
<td>Neo4j</td>
<td>NetApp</td>
<td>Netscreen</td>
<td>Netskope</td>
<td>Netwitness</td>
<td>NETWRIX</td>
<td>Novell</td>
<td>NUTANIX</td>
<td>ObserveIT</td>
<td>Offensive Security</td>
<td>OpenSecurityTraining2</td>
<td>ORACLE</td>
<td>Palo Alto</td>
<td>People Cert</td>
<td>PMI</td>
<td>Qualys</td>
<td>Rancher Academy</td>
<td>Red Hat</td>
<td>Reevo Cloud Academy</td>
</tr>
<tr>
<td>SCP</td>
<td>Scrum Alliance</td>
<td>Scrum.org</td>
<td>ScrumStudy</td>
<td>SonicWall</td>
<td>SOPHOS</td>
<td>Splunk</td>
<td>Stormagic</td>
<td>Sun</td>
<td>SUSE</td>
<td>Symantec</td>
<td>TERADATA</td>
<td>Toshiba</td>
<td>Trend Micro</td>
<td>Triton</td>
<td>Veeam</td>
<td>Vendor</td>
<td>Veritas</td>
<td>VMWare</td>
<td>WatchGuard</td>
<td>WatchGuardONE</td>
<td>WEBROOT University</td>
<td>ZERTO</td>
<td>ZyXEL</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>Monitoring &amp; Detecting</td>
<td>Penetration</td>
<td>Consultancy</td>
<td>All journey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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

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.

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..

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

Floatingpoint.sorint.com
Success stories

Delivered by: Sorintians

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

**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.

**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.

**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.

Dock12.sorint.com
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.

**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.

**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.

**REW - sploits**
Open-source software product
Emulate and Dissect MSF and *other* attacks. Rew-splloits helps you analyse Windows shellcode or attacks coming from Metasploit Framework, Cobalt Strike, or other malicious or obfuscated code.

**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.

**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.
Going Forward
How we can move forward from here

One hour workshop

Read more on /sorintlab

Alternative approach