Joint Cyber Security Webinar

19th January 2023

Siranush Akarmazyan siranush@itml.gr

This project has received funding from the European Union’s Horizon 2020 Work Programme for research and innovation 2018-2020, under grant agreement nº101021659
Outline

1. SENTINEL at a glance (Project’s key facts, motivation, statement, workflow, key drivers)
2. SENTINEL Objectives
3. SENTINEL Architecture
4. SENTINEL Modules, Plugins
5. SENTINEL Validation and Use Cases
6. SENTINEL Offerings
SENTINEL at a glance: Key Facts

PROJECT CONSORTIUM
• 13 partners

PROJECT TYPE
• Innovation Action

MAX EU CONTRIBUTION
• € 3,998,982.50

START DATE
• 1 June 2021

DURATION
• 36 months
SENTINEL Motivation

EU SMEs/MEs

Need Protection

- Violation on individuals’ privacy and rights.
- Operational downtime and/or data loss.
- Reputation damage.
- GDPR fines.

Face Challenges

- Lack of awareness about personal data protection (PDP), cybersecurity (CS) and how they interconnect.
- Lack of PDP/CS and GDPR compliance due to price, commitment of resources, complexity, etc.
- Mitigating risks, monitoring and troubleshooting their IT assets.

Violation on individuals’ privacy and rights.
Operational downtime and/or data loss.
Reputation damage.
GDPR fines.
SENTINEL provides a **complete privacy, cybersecurity and data protection suite** that enables small and medium enterprises to achieve business security and safeguard their and customers’ assets in an efficient and affordable manner.

- It **integrates security** and **privacy technologies** into a unified architecture and then applies **intelligence for compliance**.
  - It **educates SMEs on GDPR** requirements and how to achieve compliance.
    - It **automates GDPR compliance** and provision of recommendations for personal data protection and cybersecurity.
- It provides a plethora of tools for **real time monitoring** and **threat mitigation**.
SENTINEL Workflow

- User onboarding
- Company data, contacts, assets profile
- Recording personal data processing activities

- Creating and updating CS & PDP policy, recommending:
  - Measures (OTMs)
  - Educational and training material
  - Software tools and plugins

- GDPR compliance self-assessment (GDPRCSA)
- Data protection impact assessment (DPIA)
- Cybersecurity assessment (MITIGATE simulation environment)
- Cybersecurity simulations (CyberRange)

- Policy enforcement monitoring
- Consulting the Observatory
- Security notifications
- Incident & data breach handling
- Compliance centre
SENTINEL Key Drivers

GDPR Article 30 the so-called “Record of Processing Activities (ROPA)”.

- A Processing Activity is a description of how an organization handles personal data
- It is an obligation for many companies (depending on size and data types they handle)
- SENTINEL aims to help such entities keep a record of processing activities in an understandable manner

Tailor-made ROPA for SMEs/MEs
Compliance to GDPR Article 30
Address gaps in PDP compliance
Assess risk across organization
<table>
<thead>
<tr>
<th><strong>SENTINEL Objectives</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS)</td>
</tr>
<tr>
<td><strong>2.</strong> Provide scientific and technological advances in SMEs/MEs’ data protection compliance assessment, orchestrated towards the comprehensive digital Privacy and PDP compliance framework for SMEs/MEs</td>
</tr>
<tr>
<td><strong>3.</strong> Provide novel tools and services for enabling highly-automated PDP compliance in SMEs/MEs</td>
</tr>
<tr>
<td><strong>4.</strong> Validate SENTINEL framework in real-world settings via use cases driven by complementary industries</td>
</tr>
<tr>
<td><strong>5.</strong> Consolidate international and European links, raise awareness and ensure the technology transfer of project’s results</td>
</tr>
<tr>
<td><strong>6.</strong> Boost the effectiveness of the EU data economy by offering high TRL solutions (6-7)</td>
</tr>
</tbody>
</table>
SENTINEL Architecture

Main characteristics

- 4 Main modules
  1. MySentinel
  2. Self-assessment
  3. Core
  4. Observatory

- 8 Plugins (from partners & open source)
  - GDPR CSA
  - DPIA
  - MITIGATE Simulation Environment
  - CyberRange
  - IdMS
  - Security Infusion
  - Forensics Visualisation Toolkit
  - Open-source solutions Also referred to as ‘external’ plugins.
SENTINEL’s visualization/UI component and primary dashboard

Aggregates data from all front-end components and user-facing web applications

Provides visual insight into SMEs’ progress towards achieving their CS and PDP goals
Self-Assessment

- **Profile Service**
  - Provides centralised storage and retrieval services for all SME data (Core organisation data, Personal data Processing activities (PAs), Self-assessment results, Recommendations Policy drafts).

- **SA Service**
  - Performs eligibility checks and enables related workflows.

- **SA Tools**
  - Plugins which provide self-assessment capabilities and share the common SENTINEL data model.
Core

- **Common Service**
  - Acts as a centralized source for
    - The SENTINEL OTM classification
    - Software / tools / plugins
    - Awareness, education and training material

- **Recommendation Engine**
  - Generates a list of recommended OTMs, plugins and trainings
  - Based on the risk level assessment provided by the SA service

- **Policy Drafting**
  - Generates bespoke human-readable policy drafts
  - Based on the recommendations provided by the RE
  - Implements and enforces the SENTINEL reusable policy template
  - Adheres to the SENTINEL OTM classification
Observatory

- **Knowledge Base**
  - Provides storage and access to the information collected from external open data sharing platforms.

- **Information Exchange**
  - Continuously monitors and collects information from open security data sharing platforms.
  - Populates and updates the Observatory Knowledge Base.
The SENTINEL framework validation in real-world settings is facilitated by two distinct enterprises in the fields of genomics and social care.

**#1: Microenterprise test case**

The focus of this test case is to implement extra security measures for accessing genomic sequence and personal data from a bioinformatics platform software pipeline.

**#2: Small-Medium Enterprise**

The focus of this test case is to homogenize the approach to data protection and compliance across multiple portfolio business through a single platform.
<table>
<thead>
<tr>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>SME registration and profiling</td>
</tr>
<tr>
<td>Completing a self-assessment workflow</td>
</tr>
<tr>
<td>Acquiring policy recommendations</td>
</tr>
<tr>
<td>Consulting the Observatory Knowledge Base</td>
</tr>
<tr>
<td>Policy enforcement monitoring</td>
</tr>
<tr>
<td>Incident reporting and sharing</td>
</tr>
<tr>
<td>Receiving security notifications</td>
</tr>
</tbody>
</table>

Already implemented in the FFV of the SENTINEL platform
The SME representative registers the company and fills in a related questionnaire.

The system stores a profile of the company.
The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, adjusted to the SME profile.
UC3: Acquiring policy recommendations

- The SME representative fills in the company security profile and performs related self-assessment tasks indicated by the system.

- The system returns a tailor-made set of security policies.
The system detects a CS or PDP incident that affects an SME and alerts the SME representative so that they attend to it.
The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from the SENTINEL platform.
The SME browses the SENTINEL Observatory Knowledge Base and accesses information about recently identified data and privacy breaches.

The Knowledge Base is continuously updated and synchronised with external resources.
UC7: Incident reporting and sharing

- A security incident has been detected and the SME wants to report and share it with appropriate response teams and/or open security data platforms.
SENTINEL Offerings

**SME Training and Education**

- Assist SMEs to understand
  - Why individuals’ data and privacy need protection
  - How their data processing activities affect subjects’ privacy.

- Guide SMEs to understand what needs to be done to
  - Improve privacy
  - Achieve compliance

**Evidence-based GDPR compliance**

- Providing one-to-one link between
  - Privacy requirements
  - Measures/controls
  - Cyber assets
  - Configurations
  - Real-time monitoring

**Cutting costs through automation**

- Automated compliance and recommendations
  - GDPR compliance check
  - DPIA Tailor-made recommendations
  - Policies
  - Real-time monitoring
  - Cybersecurity
  - Privacy compliance
Thank you for your attention!

Would you like to trial the SENTINEL offerings?

Feel free to contact us!

sentinelh2020@gmail.com

Further Information

Sentinel - EU Project

@SentinelH2020

www.sentinel-project.eu