Bridging the security, privacy and data protection gap for smaller enterprises in Europe

This project has received funding from the European Union’s Horizon 2020 Research and Innovation program under grant agreement No 101021659.
1. SENTINEL at a glance (Project’s key facts, motivation, statement, workflow, key drivers)
2. SENTINEL Objectives
3. SENTINEL conceptual architecture
4. SENTINEL Contexts, 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

Calendar
Start: 1st June 2021
Duration: 36 months
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.

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.
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.
User onboarding;

Company data, contacts, assets profile;

Recording personal data processing activities.
SENTINEL WORKFLOW

ASSESSMENT

GDPR compliance self-assessment (GDPRCSA);
Data protection impact assessment (DPIA);
Cybersecurity assessment (MITIGATE simulation environment);
Cybersecurity simulations (CyberRange).
Creating and updating CS & PDP policy, recommending:

- Measures (OTMs);
- Educational and training material;
- Software tools and plugins;
Awareness, monitoring & compliance

Policy enforcement monitoring;
Consulting the Observatory;
Security notifications;
Incident & data breach handling;
Compliance centre.
Data Security

A wonderful serenity has taken possession of my entire soul,

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

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

Tailor-made ROPA for SMEs/MEs

Compliance to GDPR Article 30

Address gaps in PDP compliance

Assess risk across organization

SENTINEL KEY DRIVERS
SENTINEL OBJECTIVES

1. Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS)

2. 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

3. Provide novel tools and services for enabling highly-automated PDP compliance in SMEs/MEs

4. Validate SENTINEL framework in real-world settings via use cases driven by complementary industries

5. Consolidate international and European links, raise awareness and ensure the technology transfer of project’s results

6. Boost the effectiveness of the EU data economy by offering high TRL solutions (6-7)
SENTINEL CONCEPTUAL ARCHITECTURE

Contexts:
1. MySentinel
2. Self-assessment
3. Core
4. Observatory

SENTINEL Plugins:
- GDPR CSA
- DPIA
- MITIGATE
- CyberRange
- IdMS
- Security Infusion

External Plugins
- Open-source solutions (trainings, courses)
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
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.
Calculates PA risk level

SA Tools
Plugins which provide self-assessment capabilities and share the common SENTINEL data model.
Common Service
Acts as a centralized source for:
- The SENTINEL OTM classification
- Software / tools / plugins, education and training material;

Recommendation Engine
Generates a list of recommended OTMs, plugins and pieces of training based on the risk level assessment;

Policy Drafting
Generates bespoke human-readable policy drafts based on the recommendations provided by the RE;
- Implements and enforces the SENTINEL reusable policy template;

Policy Enforcement
Tracks the implementation status of policy recommendations;

Notification Aggregator
Receives notifications from registered plugin adapters:
- Provides basic filters and aggregation mechanisms
- Provides endpoint for the front end
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.

Incident Broker
Validates incidents and reports them to the Information Exchange and external bodies.
SENTINEL PLUGINS

Not part of the “core” architecture
But providing real added value to SENTINEL through Capabilities

Developed and contributed by Partners
GDPR CSA
DPIA
MITIGATE
CyberRange
IdMS
Security Infusion

Open-source solutions
Also referred to as ‘external’ plugins.
SENTINEL VALIDATION

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.
SENTINEL USE CASES

UC1
SME registration and profiling

UC2
Completing a self-assessment workflow

UC3
Acquiring policy recommendations

UC4
Receiving security notifications

UC5
Policy enforcement monitoring

UC6
Consulting the Observatory Knowledge Base

UC7
Incident reporting and sharing
SENTINEL USE CASES

**UC1**
SME registration and profiling

The SME representative (user) registers the company and fills in the related information. Based on this information, the system provides a profile of the company.

**UC2**
Completing a self-assessment workflow

The user completes a self-assessment workflow.

**UC3**
Acquiring policy recommendations

Based on the assessment of the company profile the user gets a tailor-made set of security policy recommendations.
SENTINEL USE CASES

UC4
Receiving security notifications
The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend to it.

UC5
Policy enforcement monitoring
The user can monitor the status of implementation of policies they have received as recommendations from the SENTINEL platform.

UC6
Consulting the Observatory Knowledge Base
The user browses the SENTINEL Observatory Knowledge Base and accesses information about recently identified data and privacy breaches.

UC7
Incident reporting and sharing
The User reports a security incident and shares it with appropriate response teams and/or open security data platforms.
SME Training and Education
Raise awareness and train SMEs/MEs about GDPR compliance, obligations and measures to be taken through its set of services.

Evidence-based GDPR compliance
Providing one-to-one link between privacy requirements, measures & controls, cyber assets, configurations and real time monitoring.

Cutting costs through automation
Provision of GDPR compliance check, data protection impact assessment, tailor-made recommendations for GDPR compliance and policies, as well as real-time monitoring for cybersecurity and privacy compliance.
Thank you for your attention!

Sentinel - EU Project
@SentinelH2020
www.sentinel-project.eu
Bridging the security, privacy and data protection gap for smaller enterprises in Europe

This project has received funding from the European Union’s Horizon 2020 Research and Innovation program under grant agreement No 101021659.