SOCCRATES

SOC & CSIRT Response to Attacks & Threats
based on attack defense graphs Evaluation Systems

D1.4
Data Management Plan

Deliverable type:	Report
Contributing work packages:	WP1 Project Management
Due date of deliverable:	29/02/2020
Submission date:	28/02/2020
Dissemination level:	PU

Responsible organisation:	TNO
Editor:	Gabriela Bodea
Revision:	1.0

Abstract	This document describes the data management plan for various categories of data to be processed by the project.
Keywords:	Data, privacy, security, ethics.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 833481
Call H2020-SU-ICT-2018 • Innovation Action • Start date: September 1st, 2019

Author(s)	Gabriela Bodea (TNO) Piotr Kijewski (SHS) Martin Eian (MNM) Rafal Kondracki (VTF)

Review	Hervé Debar (IMT) David Watson (SHS) Wojciech Widel (KTH)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	05/02/2020 – H. Debar
Remarks	The document highlights the need for compliance to partners' privacy, data protection and security practices during experiments on the use cases provided by partners. This should probably be monitored at regular intervals.

TABLE OF CONTENTS

1. INTRODUCTION 4
1.1. The SOCCRATES project 4
1.2. Voluntary Data Management Plan 5
1.3. Structure of the document 5
2. DATA SUMMARY 6
2.1. The purpose of the data processing and its relation to the objectives of the project 6
2.2. Categories and uses of data processed by the project 7
2.3. Data utility 8
3. FAIR PRINCIPLES FOR FINDABLE, ACCESSIBLE, INTEROPERABLE AND REUSABLE DATA 9
3.1. Open data 9
3.2. Limited-access data 9
3.3. Restricted or confidential data 10
4. PROTECTION OF INTELLECTUAL PROPERTY 11
5. DATA SECURITY 14
5.1. TNO Data Center 14
5.2. TNO File Servers 14
5.3. Shadowserver 14
5.4. Vattenfall Group 15
5.5. mnemonic 15
5.6. Gitlab 16
6. DATA PROTECTION AND ETHICAL ISSUES 17
6.1. Informed consent and information sheets 18
6.2. Additional ethical provisions 18
7. DATA MANAGEMENT AND THE PROJECT GOVERNANCE STRUCTURE 19
7.1. Allocation of resources 19
8. RECOMMENDATIONS 20
9. ABBREVIATIONS 21
10. ANNEX A: TEMPLATE FOR INFORMATION SHEET 23
11. ANNEX B: CONSENT FORM 25

1. Introduction

1.1. The SOCCRATES project

SOCCRATES (SOC & CSIRT Response to Attacks & Threats based on attack defence graphs Evaluation Systems) is an EU funded project under the Horizon2020 programme that addresses the following main challenge:

> ***How can SOC and CSIRT operations effectively improve their capability in detecting and managing response to complex cyber-attacks and emerging threats, in complex and continuously evolving ICT infrastructures while there is a shortage of qualified cyber security talent?***

The main objective of SOCCRATES is to develop and implement a **security automation and decision support platform** that enhances the effectiveness of SOC and CSIRT operations. The integrated Security Decision Support platform ('the SOCCRATES platform', see **Figure 1**) will consist of a modular set of components with standardized interfaces and a central orchestration function.

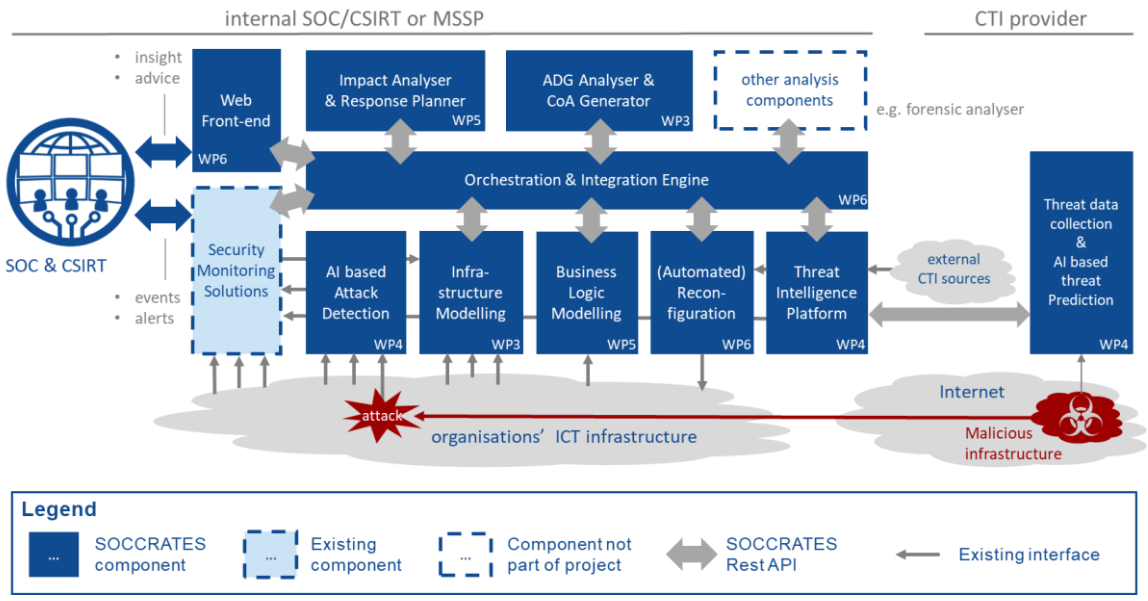

Figure 1 – The SOCCRATES platform

The main challenge that is addressed in the SOCCRATES project is determining what to do when an attack occurs, such that an ICT infrastructure and an organisation's operations can return to normal operation with minimal impact. This includes reducing exposure of private data that are used by an organization for its operations (i.e., ensuring privacy and data protection). In other words, the challenge to be addressed is to develop new techniques to improve resilience of ICT systems, such that they are resistant to cyber-attack and can rapidly return to normal operation. Such techniques should result in less operational impact when cyber-attacks do occur, enable more efficient use of ICT technology, and increase overall trust from its users. This challenge is addressed in several ways in the project, with specific innovations in key technological areas, culminating in the overall SOCCRATES platform.

SOCCRATES has the following concrete project objectives:

1. Deliver an integrated security decision support platform consisting of an orchestration function and a unique integration of innovative background solutions that seamlessly work together.
2. Show that the SOCCRATES platform can improve SOC operations by evaluating the SOCCRATES platform in two diverse real-life pilot environments.
3. Examine and illustrate the benefits of automation for selected SOC activities to help manage the cyber security skills gap in organizations.
4. Prepare for successful exploitation by the SOCCRATES partners of the individual innovated components and the integrated SOCCRATES platform in commercial products that are offered to the market and are available for the European (business) community.

1.2. Voluntary Data Management Plan

SOCCRATES focuses on the development of integrated approaches to support SOC and CSIRT operations and will not generate (personal) data. For this reason, the project has opted out of the Open Data pilot. As a consequence, a Data Management Plan was not required. However, the project chose to provide such a DMP on a voluntary basis.

1.3. Structure of the document

This document details the Voluntary DMP (VDMP) of the SOCCRATES project (deliverable D1.4) describing the chosen approach with regard to the management of the various categories of data processed by the project.

Section 2 presents an overview of data processing activities, such as the types and sources of data to be processed, the purpose of the processing of these data and the utility of the processing.
Section 3 will address the FAIR (findability, accessibility, interoperability, reusability) data principles, insofar as relevant to and consistent with the project.
Sections 5, 6 and 7 address the security, ethics and privacy aspects of the VDMP and section 8 presents the way in which this is embedded in the governance structure of the project.

The VDMP will be updated only if significant changes should arise during the course of the project, such as the processing of different or new categories of data than those described in the DOA, or changes in the composition of the consortium, likely to have an impact on data processing. [1]

[1] "The DMP should be updated as a minimum in time with the periodic evaluation/assessment of the project. If there are no other periodic reviews foreseen within the grant agreement, then such an update needs to be made in time for the final review at the latest." https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

2. Data Summary

(Personal) data processing will occur during research activities carried out in several tasks. This will observe privacy, confidentiality and security requirements, whilst taking into account recent changes in the relevant legislation, such as :

- The General Data Protection Regulation (EU) 2016/679 (GDPR) with regard to the processing of personal data;
- Directive (EU) 2016/680, if the project should process data provided by authorities responsible for preventing, investigating, detecting or prosecuting criminal offences;
- The Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications, otherwise known as the ePrivacy Directive (currently under revision), if the project should process personal data generated or processed by electronic networks;
- The 2016 Directive on security of network and information systems otherwise known as the NIS Directive, with respect to critical infrastructure operators, as transposed by EU Member States relevant for this project and
- Additional national legal requirements, if and where applicable.

2.1. The purpose of the data processing and its relation to the objectives of the project

In order to achieve its main objective, the project will undertake two main categories of data processing activities, namely:

- Research activities (including piloting at two project sites) and
- Dissemination, training, communication and other outreach activities. (see deliverable D8.2).

In the first category of data processing activities fall, for example:

- Threat Data Collection & Threat Prediction - in order to identify main characteristics of search patterns to identify trends in malicious behaviour;
- Threat Intelligence & Threat Actor profiling – in order to identify attacker tactics, techniques and procedures (TTPs) and enable the automated generation of adversary emulation plans (AEPs). Activities are aimed at describing specific procedures and observations from incident response in order to derive a general procedure definition from the specific observations and descriptions and
- Piloting activities deployed at two project sites and involving employees of the two partners.

In the second category of data processing activities fall, for example :

- Communication internal to the project, between project partners;
- Engagement with external stakeholders, to increase the visibility of the SOCCRATES platform and encourage and enable adoption of SOCCRATES results. These include organizations that maintain a SOC, CSIRTs and MSSPs and
- Engagement with academic and industrial peers through publications at conferences, the organisation of special sessions and research workshops, and the publication of research results in scientific journals.

Activities involving the processing of (personal) data are aimed at :

- Creating more robust, transversal and scalable ICT infrastructures that are used by Digital Service Providers (DSPs) and Operators of Essential Services (OESs), as defined in the NIS Directive, providing them with sustainable cyber security, digital privacy and accountability;
- Developing solutions providing enhanced protection against novel advanced threats;
- Developing and integrating advanced technologies and services to manage complex cyber-attacks and to mitigate the impact of breaches and
- Automating related tasks so as to mitigate the shortage of skills and cyber security and maximize the return on cyber security investments of organizations.

Conducting scientific research is the purpose of all data processing carried out by the project.

2.2. Categories and uses of data processed by the project

Certain tasks will involve the processing of (personal) data, for example :

- The collection and analysis of system and network data (log files, network traces, packet captures if required). Data will be collected in sandbox runs and used to identify new compromises in the network and develop deep-learning algorithms to classify malware;
- The processing of open security data (including indicators of compromise, security bulletins, forum entries, IDS rules, threat ratings, incident reports, vulnerability reports, CVE dumps, security best practices) for testing the operation and performance of the systems and prototypes developed in SOCCRATES;
- Other large data sets owned by project members and consisting of constantly updated malicious behaviours to identify new key threats and
- Personal data obtained on the basis of consent from research participants.

The platform for threat identification and trend analysis developed by SOCCRATES leverages the large datasets that are available from SHS. SHS collects malware on an industrial scale (732,000 new unique malware samples per day) and has at its disposal a dataset of 1.2 billion unique malware samples.

SOCCRATES will investigate the use of big data and AI to more effectively detect anomalies that are indicative of cyber-attacks and to support the development of actionable threat intelligence and trends. This will be realized in the context of a SOC from an Operator of an Essential Service (OES) – in SOCCRATES (namely partner VTF), a Managed Security Service Provider (MSSP) (namely partner MNM) and an organization that provides threat intelligence to its constituents (namely partner SHS). The application of AI techniques to the data sets obtained from the very large-scale sandboxing and analysis of malware samples will constitute one of the innovations of SOCCRATES.
The combined data and learnings from these new capabilities will be aggregated over many malware sample sandbox executions during the pilot phase, with the results being used to predict trends in malicious activities.

To limit data (re)use, many of the AI-based detection techniques that are being integrated into the SOCCRATES platform depend on “classical” machine learning (ML) approaches, which have a reduced need for large quantities of training data. SOCCRATES depends on the use of advanced models to support many of the innovative and impactful outcomes from the project.

Additional personal data will be obtained on the basis of consent from research participants during the two pilots as well as various communication, training, dissemination and other outreach activities.

2.3. Data utility

Enhancing the cyber security of essential services is in the interest of the entire society. In the SOCCRATES project, a strong focus will be placed on improving the cyber security of the ICT infrastructures of operators of essential services. For example, one of the pilot sites in the project is the SOC of VTF – a major energy utility, whose compromise could have significant societal and economic impact.

Enabling SOCs/CSIRTs fast and easy access to this knowledge allows them to identify and mitigate threats in their network more effectively and improve their security posture to combat future threats.

SOCCRATES will develop a Threat Intelligence API for sharing reports on malware sandbox runs with vetted CSIRTs/researchers.

In SOCCRATES, a Situation Visualization API will be developed by FSC. This public API will be provided to CSIRT teams, researchers and third-party data systems, and will provide capabilities to visualize complex cyber-attacks in a target organization's network and business context. Illustrating complex cyber-attacks in a setup that an organization is familiar with will result in faster and more precise response actions.

Other open data will be provided in the form of blogs aimed at pre-existing communities of academics, subject matter experts and decisionmakers. This will ensure that the innovations of SOCCRATES will reach and potentially be exploited by a large, influential audience across all the target sectors.

SOCCRATES will contribute in providing cyber defence mechanisms for organizations that do not have cyber security capabilities (such as SMEs). By utilizing the benefit of automation to improve scale, the overall cost involved by defence will be significantly lower. Automating certain tasks that do not require highly skilled personnel or supporting skilled personnel with carefully chosen automated tools, decreases the burden on staff and enables more clients to be serviced.

Insights from data processing for automatic threat detection will be used to train graduates and researchers for the cyber security sector. Educational material will be generated and brought to relevant audiences as part of the SOCCRATES communication strategy.

3. FAIR principles for findable, accessible, interoperable and reusable data

It is not a primary objective of the project to produce data sets that would be usable outside the context of the project. However, subject to the agreement of the SOCCRATES consortium, the project will seek to make data sets publicly available by identifying suitable national or international repositories where the data may be placed. Appropriate anonymization of the data will be applied.

3.1. Open data

Insofar as possible, SOCCRATES data will be made findable and openly accessible depending on whether data are considered to be :

- Commercially non-sensitive;
- Not lead to violations of personal privacy;
- Not violate any ethics approvals obtained for experimentation, especially where human participants are involved and
- Of scientific interest to verify or disseminate project results (deliverables, journal articles, etc.).

APIs and public data sets (e.g. from SHS) will be made available and can be used to support enhanced SOC and CSIRT operations and enable the wider community to develop novel cyber security solutions. Interest has already been expressed by the French military research in hosting a secure testbed for data, providing access to researchers. An update will be provided in the next version of the DMP.

Additional initiatives to contribute to the open data and knowledge initiative include the organization of webinars, the drafting of newsletters and distribution of online materials and will be aimed at the broader research community.

3.2. Limited-access data

SOCCRATES will also expand the benefits of more restricted information-sharing schemes, to vetted organisations, via the CSIRT Network.

SHS cooperates closely with the European and worldwide CSIRT community, delivering daily free victim remediation reports to over 107 National CSIRTs worldwide (including all EU MS National CSIRTs) and 4,600+ network owners worldwide[2]. SHS also shares undetected malware samples each day with leading anti-virus vendors, to improve detection.
Innovation that enables better understanding of malware behaviour and malware trends on such large datasets, provided as a new free SHS service to the vetted organizations, will have a potential large impact on the security posture of organizations in Europe and around the world.

Third-party access to data sets will be made available to trusted security research organizations and detailed in D4.3.

[2] https://www.shadowserver.org/news/celebrating-milestones-european-cert-csirt-report-coverage/

Machine-readable format for describing detailed cyber-attack procedures integrated into the ACT platform will be made available as part of D4.4.

Technical solutions, APIs and documentation for the use of AI-based threat identification and trend analysis will be made available to representatives of the Cyber security- industry and SMEs.

Additional educational material generated by the project will be made available to the relevant audiences, such as security professionals in training.

3.3. Restricted or confidential data

Some of the data generated in the context of the use cases could be directly or indirectly related to identified or identifiable natural persons thus constituting personal data as defined in Article 4 of the EU General Data Protection Regulation. Their publication would therefore possibly infringe upon natural persons' privacy rights and be a violation of European data protection legislation.

Additionally, as the project builds software tools, applied during pilots at commercial partners' sites (who have high privacy requirements), publication of the data will be incompatible with their confidentiality requirements.

4. Protection of intellectual property

The IPR strategy has been defined to protect the innovations and knowledge developed within the time-frame of the project and help in maximising the returns on the human, capital and intellectual investments. Full details are included in the Grant Agreement defining the rules for participation and in the Consortium Agreement between the SOCCRATES partners.

The management of knowledge and intellectual property and other aspects of innovation in this project are allocated to specific activities within work packages and include :

- IPR applications for new systems and solutions that will be prepared by participants and
- Information that will be disseminated within the project and to external bodies through publications, presentations and regulatory and standards bodies, but only after the necessary steps for ensuring the protection of IPR have been considered. This ensures that intellectual property will be secured in the interest of project partners.

These activities are part of WP1 (Project Management) and WP8 (Dissemination).

Additionally, all partners have a joint non-exclusive right to exploit commercially all Intellectual Property produced by any participant in the project as a part of its work. The contractors should be granted a cost-free license to use other partners' pre-existing intellectual property for the purposes of the project while the project is running; thereafter they should not be unreasonably denied a license to use the property, although a commercial rate may be negotiated.

This approach to knowledge management and IPR is regulated in the Consortium Agreement, setting the basis for a specific Exploitation Agreement. Some of the major aspects covered are indicated below briefly.

- Confidentiality: Each partner will treat information from others as confidential and not disclose it to third parties unless it is obvious that the information is already publicly available, or disclosure is required by law;
- Ownership of Knowledge: Knowledge is owned by the partners who carried out the work generating the knowledge, or on whose behalf such work was carried out. If a partner wishes to assign any knowledge to a third party, they should inform the other partners and request their consent, which should not unreasonably be withheld;
- Patents: Partners who own patentable knowledge may (and are encouraged to) at their own expense make applications for a patent or similar form of protection and will supply details of each such application to the other partners;
- Access Rights: Partners grant to each of the other partners royalty-free access right to knowledge generated in the project to the extent needed to successfully perform the project. Access rights to knowledge generated in the project and to pre-existing knowledge for use outside the project are, when needed to make use of the project result, given between partners in different WPs on preferential conditions. Access rights to knowledge generated in a WP, when needed to make use of the project result, is given royalty free to the other partners participating in the same WP. Access rights to a partner of pre-existing knowledge for use outside the project is, when needed and only to the extent necessary to make use of the project result, given on preferential conditions to the other partners in the same WP;

- Rights Usage: As part of the ongoing IPR work the project partners will evaluate the benefits of existing models for marketing intellectual property and knowledge and look for creating new ones if necessary to maximize return on their efforts while ensuring social and ethical aspects of the importance of threat intelligence. To ensure best solutions, the efforts on the IPR and the preparation of business models shall be amalgamated to crystalize beneficial and marketable solutions, considering all possible licensing and service models – sell single software tool, sell toolkits or market entire toolchains, sell models and ideas with or without implementation, sell a service or bundles of services and software, create an open members-only service provider or consortium. The different pricing models will also be evaluated – one-off fee, recurring charges, differentiated pricelist for clients contributing vs. clients consuming threat intelligence, etc.

In addition to the Consortium Agreement regulating the IPR management in more detail, a specific exploitation plan will be set up and be reviewed regularly. The consortium will pay specific attention to IPR (management, early detection, protection).

Complementing the EC contract, partners agreed on pre-existing intellectual property rights excluded from SOCCRATES and user licenses in the consortium agreement. The basic rule is that each partner retains the ownership of its background knowledge. The agreement details rights to exploit project results for commercial purposes; each partner will, however, maintain the right to use the project outcome for internal use. During the lifetime of SOCCRATES, the implementation of these IPR principles will comprise the following main tasks:

- Updating of background knowledge: collect, update and maintain the list of major background knowledge (known as “pre-existing know-how”) required for implementing SOCCRATES. This includes the list of background excluded from SOCCRATES before the contract signature, as set up in the Consortium Agreement, and of other background identified throughout the project lifetime;
- Management of the SOCCRATES knowledge portfolio: collect information on the knowledge gained and agree with the owners of the knowledge the standard access conditions within the project. The SOCCRATES knowledge portfolio will also be the key tool for dissemination and exploitation of project results;
- Knowledge protection: propose a general policy regarding co-ownership of knowledge and moderate solutions in case of co-ownership between different beneficiaries and provide advice about knowledge project when required (patents, copyrights, etc.);
- Consortium Agreement maintenance and evolution: Prepare and maintain the Consortium Agreement (based on the DESCA model) and prepare corresponding decisions to be taken by the Steering Committee related to modifications of the pre-existing know-how, termination of participation and entrance of new partners and
- Preparation for marketing of the IPR. Evaluate the marketability of the knowledge and solutions created within SOCCRATES with a view to the interests pertaining to existing knowhow and setting up appropriate structures and processes for allocation of the proceeds and benefits from the SOCCRATES project among partners, including through setting up one or more legal entities or appointing a copyrights management partner or otherwise.

The implementation of these IPR principles and exploitation preparation fall under the responsibility of the Coordinator, who will report on a regular basis and whenever requested to the Project

Steering Committee (PSC). In case of major conflicts that cannot be solved by the Coordinator, the PSC will be called on for resolution.

5. Data security

This section provides additional details on data security measures put in place by TNO as the coordinator of the SOCCRATES project as well as individual consortium partners involved in the processing of data.

5.1. TNO Data Center

Data related to project management tasks are stored in the SharePoint service of TNO. The data is located in one of the two data centres contracted by TNO in the Netherlands. The equipment installed in these data centres is owned by TNO and is managed exclusively by TNO. Access to the information is possible worldwide based on a TNO account from the TNO network, or via TNO telecommuting facilities based on Multi Factor Authentication. TNO offers standard facilities to safeguard the confidentiality, integrity and availability of the information, including at least daily backup of the information to the data centre other than where the service itself is active.

5.2. TNO File Servers

Additionally, data related to the project are stored on the TNO file servers. The data is located in one of the two data centres contracted by TNO in the Netherlands. The equipment installed in these data centres is owned by TNO and is managed exclusively by TNO. Access to the information is possible worldwide based on a TNO account from the TNO network, or via TNO telecommuting facilities based on Multi Factor Authentication. TNO offers standard facilities to safeguard the confidentiality, integrity and availability of the information, including at least daily back-up of the information to the data center other than where the service itself is active.

5.3. Shadowserver

SHS is at its core a threat data collection project on a massive scale, which enables the organization to function as a global observatory of threats propagating on the Internet. This knowledge can be used to augment the capabilities of SOCS/CSIRTS, who can apply this knowledge to supplement internal threat detection and response systems available to them.

Over the past 10 years, SHS has built its own, unique, internal sandbox system that only has been available to SHS's staff and volunteers. This proprietary sandbox system has not been made available to the wider security researcher community or the public.

SHS collects malware through various sources: the sandbox itself (stage 2 malware etc.), exchange partnerships with the AV and Threat Intel industry, security researchers and communities, honeyclients, sensor networks of spampots and honeypots, etc.).

As a result, SHS possesses a unique malware repository, containing over 1.2 billion malware samples, which is increasing in size at around 732,000 unique (by hash) samples per day. The malware samples ingested by SHS are analysed using their sandboxes on a daily basis. SHS has 2000 virtual sandboxes and nearly 300 bare metal sandboxes at its disposal. Each malware sample that is run in a sandbox generates an analysis report. Analysis reports from these sandbox runs include recorded network traffic from a live Internet connection, host level changes (registry, filesystem, process, etc.) and AV classification. Any associated snort rulesets or yara rules being triggered are also reported.

The SHS sandbox report dataset that is being shared in the SOCCRATES project as part of the Pilot #3 work in WP4 AI-based Threat Detection and Prediction is self-generated by SHS. The dataset contains a subset of information collected in analysis reports during the execution of the malware in the SHS sandbox. To ensure adequate security and privacy, access to the main malware repository (physically located in the US) and sandbox analysis results is secured through various state of the art security mechanisms according to current best practice on a strict "need-to-know" basis. In the SOCCRATES context, data is shared for research purposes only. WP4 partners collaborating on sandbox analysis result dataset have access to a test/training VM that contains a limited time-window of the self-generated SHS data under similar best practice principles. The VM with the test data can easily be placed in any environment, either in the EU or US if necessary. Partners that have their algorithms executed on the main SHS repository (after the VM testing/training phase) do not have direct access to it: the algorithms/tools are run by SHS staff and only aggregated results shared. The future API (Pilot #3 Deployment of Threat Prediction at SHS) that will be used to share results with the SOCCRATES platform and trusted (vetted) external CSIRTs and investigators will also be accessible only on a need-to-know basis and in accordance with current best security practices. To ensure compliance with GDPR principles, SHS has developed a GDPR based privacy policy on data management available at https://www.shadowserver.eu/privacy.en.html.

5.4. Vattenfall Group

SOCCRATES partner Vattenfall, because of its significant importance for national security in Sweden and in other countries, is required to have in place protective security measures. These are regulated by the Protective Security Act (2018:585) and Protective Security Ordinance (2018:658) according to the Swedish law. Also, other requirements for data protection, data privacy and data processing apply, for instance applicable law in relation to other countries or the EU General Data Protection Regulation[3]. Vattenfall Group operates an Information Security Management System (in accordance with ISO/IEC 27001) within its IT Function in order to provide secure IT services for critical IT infrastructure.

5.5. mnemonic

SOCCRATES partner mnemonic has implemented appropriate technical and organizational measures to protect the data and the information systems on which the data is stored. mnemonic has been ISO/IEC 27001 certified since 2005.
mnemonic might process (personal) data during pilots. Data might include log files and security alerts in order to detect and respond to security incidents. These data, similar to mnemonic customer data are stored in data centers in Norway[4].

Although Norway is not a member of the EU, the EU recognises the adequate level of data protection in Norway[5] and does not require any additional safeguards than those similar to the GDPR requirements.

[3] More GDPR-related information can be found at https://group.vattenfall.com/uk/site-assets/privacy-policy-general

[4] https://www.mnemonic.no/about/privacy-notice/

[5] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?cookies=disabled

5.6. Gitlab

In addition to the information provided above, it should be noted that project members also make use of Gitlab as a shared communication and work platform. The platform indicates that it is GDPR compliant and adheres to the Privacy Shield Framework, certified January 26, 2017[6].
Gitlab encrypts all data in transit to ensure protection of login information and credentials. Gitlab stores a one-way hash of all user passwords using bcrypt. Account login is protected from brute force attack with rate limiting.[7]

[6] https://help.github.com/articles/github-privacy-statement/
[7] https://github.com/security/trust

6. Data protection and ethical issues

As mentioned previously, SOCCRATES might process personal data :

- Indirectly, as part of research activities (i.e. personal data are not necessary for substantive tasks of SOCCRATES research, but might be processed incidentally) and
- Directly, as part of piloting, dissemination, training, communication and other outreach activities.

All activities involving the processing of personal data will observe the key GDPR principles of:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Additional criteria of confidentiality and security will be applied to both personal and non-personal data.

Insofar as relevant, and in addition to GDPR compliance, the processing of personal data in SOCCRATES will take into account specific national requirements regarding data processing.

A declaration on compliance or authorisation for collecting and processing personal data as carried out during the SOCCRATES project is not required under the Dutch national law, the applicable law of the SOCCRAATES project coordinator TNO. All personal data processed by TNO will be done according to the GDPR requirements and additional relevant national legislation. The research project has been approved by an internal TNO ethics review committee.

For the purpose of all data processing within SOCCRATES, the partners share all responsibilities equally as co-controllers.

TNO, as coordinator of SOCCRATES, provides partners with advice regarding data processing and privacy matters relevant to research activities. Gabriela Bodea, (TNO) is the appointed Privacy and Ethics Advisor and Rafal Kondracki (VTF) is the SOCCRATES Security Officer.
In addition, TNO provides research participants with information on their privacy and data protection rights under GDPR through the informed consent. For subsequent inquiries regarding the exercise of their privacy rights (e.g. the right of access and correction to their personal data), research participants can send in a request by using a digital form on the TNO website: https://www.tno.nl/en/about-tno/contact/corporate-legal/privacy-statement/ or contact the TNO data protection and privacy officer directly:

Mr Remy van den Boom LL.M.
Data Protection Officer Privacy, TNO
Legal Department
PO Box 96800
2509 JE The Hague, The Netherlands

6.1. Informed consent and information sheets

All participants to major events and pilots that are organized by SOCCRATES ('research participants') will be provided with an information sheets about the project and will be required to sign a consent form before taking part in project activities.
Templates for the information sheet and the consent form, in a language and formulation easy to understand by all potential research participants, can be found in Annex A and B to this document.

Research participants retain all rights with regard to their personal data shared with the project. Research participants have the right to withdraw from the project at all times.

Research participants are expected to be involved primarily in the context of :

- Two planned piloting activities of the SOCCRATES platform that will take place at VTF and MNM, the teams operating the SOC / CISRT. The participants in the pilot are the team members of the organisation's SOC / CSIRT themselves. SOCCRATES will make sure that selecting participants for the pilot reflect the organisation's gender distribution within these teams, and strive to reflect a gender-neutral distribution as much as possible. The Privacy and Ethics Advisor will provide the necessary advice to support the overall handling of gender and social/cultural factors in in the project, and in particular in the pilots and
- Dissemination, training, communication and other outreach activities.

6.2. Additional ethical provisions

Partner KTH provides a course on ethical hacking aimed at both university students and industry, as part of lifelong learning projects. PhD students and Master's students who will be involved in the project will attend this course.

7. Data management and the project governance structure

SOCCRATES has adopted a number of measures to anchor data management in the governance structure of the project (see also Fig.2 below):

- SOCCRATES has appointed a Privacy & Ethics Advisor (PEA) tasked with identifying and advising on relevant issues related to privacy, data protection and ethics. She provides advice (on request and pro-actively) to the consortium and in answer to requests from the EC Project Officer;
- SOCCRATES has appointed a Security Officer, tasked with identifying and advising on relevant issues related to security. He provides advice (on request and pro-actively) to the consortium and in answer to requests from the EC Project Officer;
- Both the PEA and the Security Officer are included in the Project management Team (PMT);
- The Project Coordinator (PC) takes responsibility for the overall project management. This includes management of the overall ethical and gender issues;
- The SOCCRATES advisory Board, the Stakeholder Group and the project's partners are enlisted to actively follow the implementation of the NIS Directive in their respective countries and signal to the rest of the project differences likely to impact their activities.

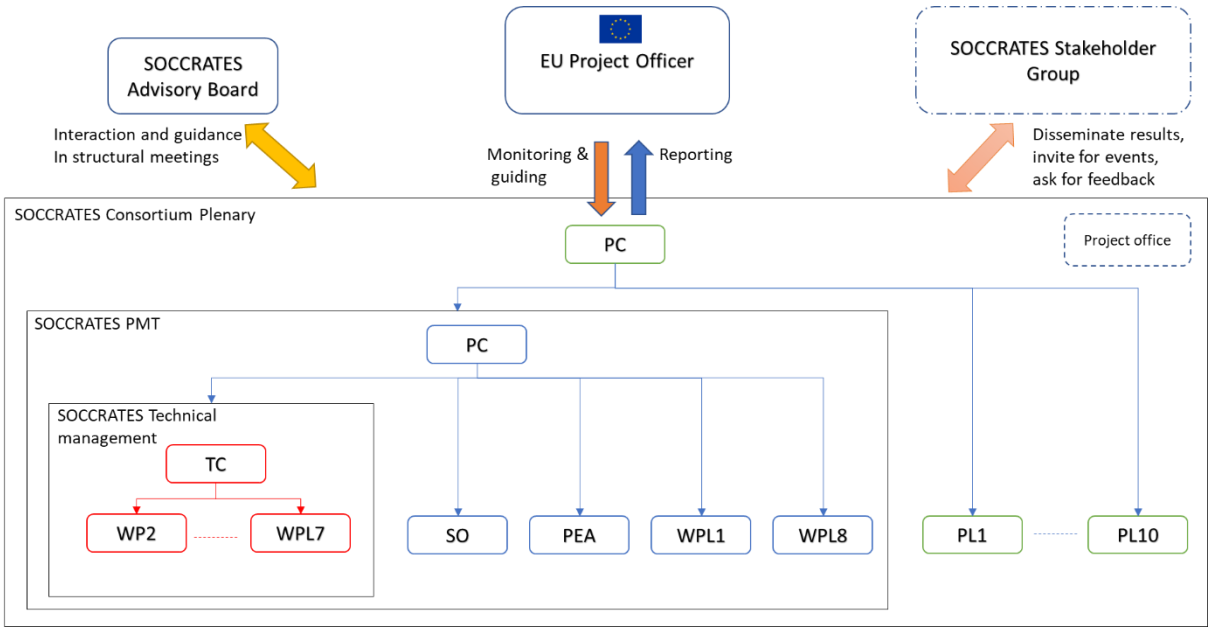

Figure 2 – SOCRATES project governance structure

7.1. Allocation of resources

Costs related to data management activities have been included in the overall project plan and specific categories have been included in the dissemination plan. Each individual partner will be responsible for bearing the costs related to their activities within the project.

The project coordinator bears the overall responsibility for the data management of SOCCRATES.

8. Recommendations

SOCCRATES will continue to monitor security and privacy/data protection/ethics matters throughout the course of the project: Gabriela Bodea (TNO), as the appointed Privacy and Ethics Advisor, and Rafal Kondracki (VTF), as the SOCCRATES Security Officer.
If necessary, the VDMP will be updated to reflect new activities involving data processing (e.g. the project pilots).

9. Abbreviations

This glossary serves as inventory of abbreviations used in the document.
This is a standard glossary, used for all SOCCRATES report deliverables; it will be expanded when necessary

Acronym	Description
ACT	semi-Automated Cyber Threat intelligence
ADG	Attack Defence Graph
AEF	Argus Event Format
AI	Artificial Intelligence
AIT	AIT Austrian Institute of technology
API	Application Programming Interface
APT	Advance Persistent Threat
ATOS	ATOS Spain
AV	AntiVirus
BPMN	Business Process Model and Notation
CC	Command and Control
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
CSIRT	Computer Security Incident Response Team
CoA	Course of Action
CTI	Cyber Threat Intelligence
DC	DataCentre
DGA	Domain Generated Algorithm
DMP	Data Management Plan
DNS	Domain Name System
EDR	Endpoint Detection and Response
ELK	Elasticsearch/Logstash/Kibana
FRS	Foreseeti
FSC	F-secure
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMC	Infrastructure Modelling Component
IMT	Institut Mines-Télécom - Télécom SudParis
INTF	Interface
IoC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IRM	Incident Response and Management
ITIL	Information Technology Infrastructure Library
KTH	Kungliga Tekniska högskolan - Royal Institute of Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M_n	Infrastructure Model (at time *n*)
MNM	Mnemonic
MSSP	Managed Security Service Provider
MTTD	Mean Time To Detection
NOC	Network Operations Centre
OT	Operational Technology
SDN	Software Defined Network

SHS	Shadowserver
SIEM	Security information and event management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Centre
SOCCRATES	SOC & CSIRT Response to Attacks & Threats based on attack defence graph Evaluation Systems
SSL	Secure Sockets Layer
TAP	Test Access Point
TIP	Threat Intelligence platform
TLS	Transport Layer Security
TNO	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek
TTC	Time To Compromise
UC	Use Case
VTF	Vattenfall
VDMP	Voluntary data management plan

10. Annex A: Template for information sheet

SOC & CSIRT Response to Attacks & Threats
based on attack defense graphs Evaluation Systems

Information sheet

SOCCRATES is an international research project co-funded by the European Commission under Grant agreement ID: 833481.

SOCCRATES is part of the Programme H2020-EU.2.1.1. - INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT).

The project started on the 1st of September 2019 and will end on the 31st of August 2022.

SOCCRATES aims

ICT infrastructures used by organisations in the EU make them highly vulnerable to cyber-threats and cyber-attacks. The lack of attack detection methods and of cyber security specialists underscore the need for advanced tools that make the infrastructures resistant and capable of responding to cyber threats in a timely and effective manner.

The SOCCRATES project intends to develop and demonstrate a security platform for Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs).

The SOCCRATES Platform consists of an orchestrating function and a set of innovative components for automated infrastructure modelling, attack detection, cyber threat intelligence utilization, threat trend prediction, and automated analysis using attack defence graphs and business impact modelling to aid human analysis and decision making on response actions, and enable the execution of defensive actions at machine-speed.

The SOCCRATES platform will be implemented and deployed at two pilot environments with highly complex and diverse ICT environments and typical application scenarios: an organisation's internal SOC, and a Managed Security Service Provider. The threat trend prediction component will be deployed at a third pilot environment at which large amount of malicious infrastructure data is collected and analysed.

The SOCCRATES platform and innovative components will enable organisations to improve the resilience of their infrastructures and increase productivity and efficiency at the SOC. SOCCRATES's

outcome contributes to a more secure cyberspace and strengthens competitiveness in the EU digital single market.

The aim is to exploit the SOCCRATES platform and its components in commercial products.

SOCCRATES consortium partners

The project participants include: MNEMONIC AS (Norway), AIT Austrian Institute Of Technology GMBH (Austria), Kungliga Tekniska Hoegskolan (Sweden), FORESEETI AB (Sweden), Institut Mines-Telecom (France), Stichting The Shadowserver Foundation Europe (The Netherlands), F-SECURE OYJ (Finland), ATOS Spain SA (Spain), VATTENFALL IT Services (Poland).

SOCCRATES coordination

The project is coordinated by TNO, the Netherlands Organization for Applied Scientific Research.

For more information about the project, please go to https://www.soccrates.eu/ or contact the project coordinator:

Mr Reinder Wolthuis
reinder.wolthuis [at] tno.nl
Anna Van Buerenplein 1
2595 DA The Hague, The Netherlands

11. Annex B: Consent Form

Consent form

Thank you for accepting to take part in the survey/workshop/conference organized by the H2020 project SOCCRATES.

Before signing this form, please read it carefully as well as the information sheet that has been provided to you.

Your participation in the SOCCRATES survey/workshop/conference is entirely voluntary.

You are free to withdraw from the SOCCRATES survey/workshop/conference at any time.

You can require to have your contact details changed or deleted from the project's contact list at any time by sending a request to the e-mail address provided below.

The project will collect only information that is relevant to its activities. Information, including personal data you provide to the SOCCRATES survey/workshop/conference will be anonymized and used for the writing of deliverables/articles/etc. The project will not share or transfer your personal data to third parties. These data will be deleted within five years after the end of the project, conform the EC rules.

Your signed consent form will be stored in a separate file in a secure manner (including password protection where required). Only designated members of the research team will be able to access these data.

For any further information, you can contact:

the SOCCRATES project coordinator

Mr Reinder Wolthuis
reinder.wolthuis [at] tno.nl

the SOCCRATES Privacy and ethics advisor

Ms Gabriela Bodea
gabriela.bodea[at]tno.nl

the SOCCRATES Security Officer

Mr Rafal Kondracki
rafal.kondracki[at]vattenfall.com

I understand and agree to sign this consent form.

Name:

Signature

Date: ___/___/_____