SOCCRATES

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

D8.2
Dissemination plan

Deliverable type:	Report
Contributing work packages:	WP8 Dissemination
Due date of deliverable:	30/11/2019
Submission date:	03/12/2019
Dissemination level:	PU

Responsible organisation:	TNO
Editor:	Reinder Wolthuis
Revision:	1.0

Abstract	This document contains the approach, activities target groups, channels and high level planning for the dissemination of the SOCCRATES results to relevant stakeholders.
Keywords:	Dissemination, security, automation, exploitation.

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

Classification level: Public

Author(s)	Reinder Wolthuis (TNO) Paul Smith (AIT) Frank Fransen (TNO) Hervé Debar (IMT) Siri Bromander (MNM) Mathias Ekstedt (KTH)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	30/11/2019
Remarks	None

TABLE OF CONTENTS

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 has 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 cybersecurity talent?***

The main objective of SOCCRATES is to develop and implement a security automation and decision support platform (‘**the SOCCRATES platform’)** that will significantly improve an organisation’s capability (usually implemented by a SOC and/or CSIRT) to quickly and effectively detect and respond to new cyber threats and ongoing attacks.

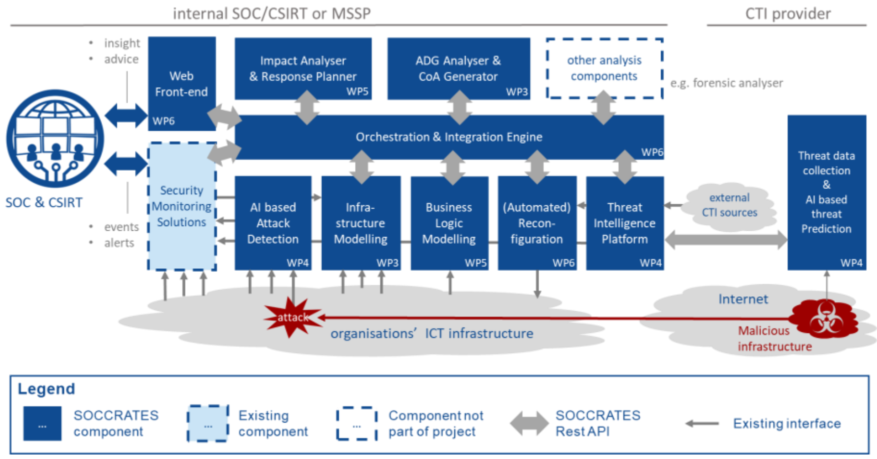

internal SOC/CSIRT or MSSP
CTI provider
insight
advice
Web Front-end
WP6
Impact Analyser & Response Planner
WP5
ADG Analyser & CoA Generator
WP3
other analysis components
e.g. forensic analyser
Orchestration & Integration Engine
WP6
SOC & CSIRT
Security Monitoring Solutions
events
alerts
AI based Attack Detection
WP4
Infra-structure Modelling
WP3
Business Logic Modelling
WP5
(Automated) Recon-figuration
WP6
Threat Intelligence Platform
WP4
external CTI sources
Threat data collection & AI based threat Prediction
WP4
Internet
attack
organisations’ ICT infrastructure
Malicious infrastructure
Legend
SOCCRATES component
Existing component
Component not part of project
SOCCRATES Rest API
Existing interface

Figure 1 – The SOCCRATES platform

The SOCCRATES platform (see Figure 1) 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.

SOCCRATES has the following concrete project objectives:

1. Deliver the SOCCRATES 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.

Please see www.SOCCRATES.eu for more information on the SOCCRATES project.

1.2 This deliverable

This document is the dissemination plan for the SOCCRATES project (deliverable D8.2). The Dissemination Plan (DP) describes the approach of SOCCRATES regarding dissemination objectives, plans, activities target audience and results.

1.3 Structure of this deliverable

Section 2 describes the dissemination strategy and measurable dissemination objectives, while section 3 identifies the SOCCRATES stakeholders and the target audience for the dissemination activities, considering their specific information needs.

Section 4 provides details on the organization of the dissemination activities and the specific scope of the activities. Section 5 lists the channels and media that SOCCRATES intends to utilize in the dissemination activities, including a detailed list of messages and hints tailored according to the category of the audiences and stakeholder groups, in terms of content, format, style and support. Also, in section 5 are the projects, organizations and standardization activities that SOCCRATES aims to liaise with. Chapter 6 briefly summarizes the exploitation approach, which will be laid down in a separate exploitation plan (D8.6). Finally, in chapter 7, the work plan is laid down, describing the planning for all dissemination activities and their intended results.

2 Dissemination strategy and objectives

2.1 Dissemination strategy

Given the importance of security across all industrial sectors and, indeed, to the public, dissemination and communication activities will be critical for ensuring that the best practice guidelines and new technologies developed by the consortium reach a wide audience.

To achieve our ambitious objectives, we implement a three-strand approach to manage the dissemination of results internally and externally.

- The internal strand comprises an ongoing proactive review process for project deliverables, and other significant milestones, whereby such results are allocated specific dissemination objectives and indicators of success. The aim is to ensure that project deliverables and results do not fade into the background after completion, but instead continue to be live assets to the project which are actively pursued to provide impact. The WP8 leader will ensure that a dissemination session will be held at each face-to-face plenary meeting, to agree dissemination objectives, and to review previous efforts.
- The second strand of the dissemination plan is a set of dissemination objectives and schedule of events to engage directly with stakeholders, to achieve a high visibility of the SOCCRATES platform and encourage and enable adoption of SOCCRATES results. Organizations that maintain a SOC, CSIRTs and MSSPs are a major focus of this dissemination strand. In line with the expected impacts of the project, the project will target the European CSIRT Network. Our dissemination activities therefore focus on engaging with these stakeholders.
- The third strand for disseminating and validating the quality of the project results will be active engagement with academic and industrial peers through publications at conferences, organisation of special sessions and research workshops, and publication in high impact scientific journals. These events will provide a direct dissemination opportunity and promote the visibility of SOCCRATES at an international level.

The following points represent the main categories of project results that SOCCRATES intends to disseminate to stakeholders:

1. Prototype technologies that have been validated in the project's piloting activities;
2. Guidance on the use of these technologies by SOCs and CSIRTs, highlighting their potential benefits;
3. Materials, such as published articles, that highlight the technological innovations from the project that can be built upon by the community; and
4. APIs and public data sets, e.g., from SHS, that can be used to support enhanced SOC and CSIRT operations and enable the wider community to develop novel cyber security solutions.

2.2 The SOCCRATES dissemination objectives

SOCCRATES adopted the following dissemination objectives that support the SOCCRATES objectives (see paragraph 1.1):

- To raise awareness among all relevant stakeholders (e.g. policy makers, regulatory bodies, service providers, end users and vendors) on how to improve SOC/CSIRT operations with SOCCRATES results;
- To develop the SOCCRATES SOC/CSIRT white paper composed of project results specifically targeted to raise awareness among higher management of stakeholders;
- To disseminate project results to relevant target groups and potential users of the SOCCRATES Platform and components;
- To identify and execute opportunities for contributions to standards based on SOCCRATES results.
- To develop and implement an interactive and user-friendly web site to inform the public and relevant stakeholders about the project;
- To produce an exploitation plan which will include a list of opportunities that arise from the project's achievements and a detailed analysis of benefit and impact.

2.3 Sensitive information

Where relevant, dissemination information (such as papers, demonstrations, presentations) will be assessed by the SOCCRATES Security Advisory Board (SAB) to make sure that no security or privacy sensitive information is published. The SOCCRATES SAB has drawn up procedures to this end.

3 Target audience and stakeholders

We anticipate that SOCCRATES results will be applicable across a range of stakeholders. Although we welcome engagement with all interested stakeholders, we will focus on building strong relationships with SOC and CSIRT teams in Europe. The strong involvement of security solution providers in the consortium (MNM, FRS, SHS, and FSC) and end-user VTF provides us with an exceptional insight into the key needs of the industry, end users, and potential commercial customers, and enables us to shape our message in the most effective way to reach and exert influence on external stakeholders, such as those in the Stakeholder Group. SOCCRATES has identified a comprehensive set of target groups that will be elaborated in the following paragraphs.

3.1 MSSPs offering SOC and CSIRT services

This group of Managed Security Service Providers (MSSPs) is highly relevant for SOCCRATES and offers SOC and CSIRT services to end users that do not have the capacity, size or ambition to have their own SOC and CSIRT organization.

We aim to reach this group by including as many as possible of these operators in our stakeholder group, invite them to demonstrations, workshops and webinars and communicate to them by the

SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Number of MSSPs in stakeholder group [>10]
- Number of MSSPs contacted about SOCCRATES [>25]

3.2 End users operating their own SOC/CSIRT

End users are specific SMEs or large companies identified as potential end-users of SOCCRATES technology. Of course, they are also highly relevant for SOCCRATES both for delivering input to the development and receivers of the exploitation activities of the project.

We aim to reach this group by including as many as possible of these end users in our stakeholder group, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Number of end users in stakeholder group [>10]
- Number of end users contacted about SOCCRATES [>25]

3.3 National CERTs

National CERTs also are a highly relevant target group for SOCCRATES, because they could be a user of SOCCRATES developed technology, but they also need to understand the potential of automated security and the impact it will have on their cooperation with SOCs and CSIRTs end users and MSSPs.

We aim to reach this group by including some national CERTs in our stakeholder group, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Number of National CERTs in stakeholder group [>2]
- Number of national CERTs contacted about SOCCRATES [>5]

3.4 Vendors

Vendors of products that relate to the SOCCRATES platform can benefit of the knowledge gained by the project and are therefore a relevant target group.

We aim to reach this group by including interested vendors in our stakeholder group, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Number of vendors in stakeholder group [>5]
- Number of vendors contacted about SOCCRATES [>10]

3.5 Industry platforms & standardization bodies

Industry Platforms and Associations, Standardisation Bodies (e.g., cPPP on cyber security, appropriate ECSO working groups) are a relevant target group to use the knowledge that is developed in SOCCRATES as input for their work.

We aim to reach this group by engaging with them, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Participation at industry bodies' events [6]
- Contributions to policy and standards, e.g. citations of SOCCRATES results [2]
- New relationships with appropriate bodies [2]

3.6 Policy professionals

Policy Professionals (e.g., Europol EC3, national stakeholder (ministries), ENISA, …) are a relevant group for SOCCRATES because they need to know the impact of security automation and use the output of SOCCRATES to update policies where necessary.

We aim to reach this group by engaging with them, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- References to results in policy [2]
- Position papers (e.g. to ECSO WG6 (research) or WG5 (education)) [3]

3.7 Security research community

The international security research community (academic and industry) is an important target group both to provide input to SOCCRATES but also discuss the (scientific) SOCCRATES results.

We aim to reach this group by attending and presenting at (scientific) conferences and seminars, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Publication downloads [100+]
- Citations during project [50+]
- Invited talks by consortium members [7].

3.8 (EU) security automation innovation projects

It is important to liaise with other innovation projects that deal with security and security automation. Knowledge can be shared and dissemination activities can be organized more effectively and efficiently.

We aim to reach this group by sharing knowledge and liaise with other projects, co-organize events, invite them to demonstrations, workshops and webinars and communicate to them by the SOCCRATES video, blogposts on our website and through social media. We will also distribute the white paper to this group.

Measurable outcome:

- Exchange of information with other projects [>10]
- Liaison with other projects [>2]
- Co-hosted workshops [2].

3.9 General public

The public is not a direct target group for SOCCRATES, as the results are meant for end users and MSSPs. We will however make sure that SOCCCRATES also brings forward the general goal of the project and the benefit for society to the public.

We aim to reach this group by making sure that our website contains some clear information that is understandable for the public.

4 Dissemination organisation and scope

TNO is the coordinator of the dissemination activities, which are managed in WP8, and all partners are involved. The activities are distributed among the SOCCRATES project partners, but each partner will have a specific focus. E.g. the focus of the KTH, IMT and TNO will be more towards the scientific community, while the focus of mnemonic and Vattenfall will be more towards MSSPs and the end-user community.

The other work packages of SOCCRATES provide input for the dissemination activities, see Figure 2.

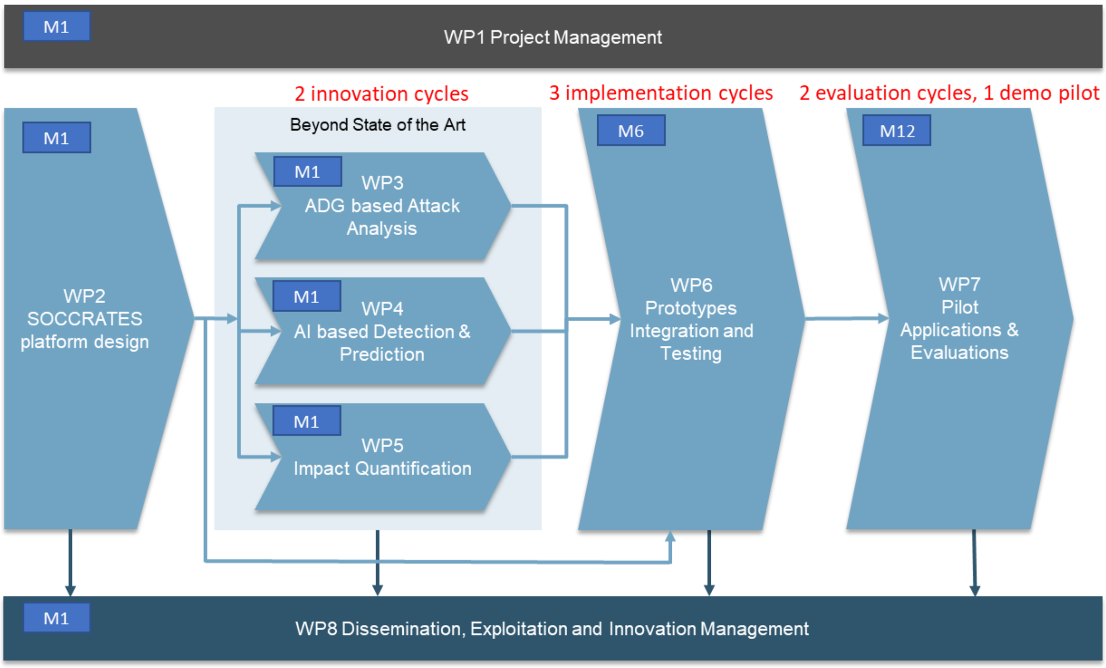

M1
WP1 Project Management
2 innovation cycles
3 implementation cycles
2 evaluation cycles, 1 demo pilot
M1
WP2 SOCCRATES platform design
Beyond State of the Art
M1
WP3 ADG based Attack Analysis
M1
WP4 AI based Detection & Prediction
M1
WP5 Impact Quantification
M6
WP6 Prototypes Integration and Testing
M12
WP7 Pilot Applications & Evaluations
M1
WP8 Dissemination, Exploitation and Innovation Management

Figure 2 - Overview of WPs and dependencies

Work package 8 is organized according to the following tasks:

- T8.1 Develop and maintenance of the SOCCRATES web site
- T8.2 Develop the SOCCRATES white paper
- T8.3 Targeted dissemination and standardisation activities
- T8.4 Preparation and realisation of SOCCRATES workshops
- T8.5 Exploitation

And will deliver the following results:

Table 1 - WP8 results

Deliverable number	Deliverable title	Dissemination level	Delivery date
D8.1	**SOCCRATES public website** The project website (easily accessible) that contains actual information regarding the project and its events and where deliverables can be downloaded.	PU	M03
D8.2	**Dissemination plan** Contains all plans of SOCCRATES for dissemination at events and to stakeholders.	PU	M03
D8.3	**Intermediate report on dissemination and standardization activities** Contains the progress of dissemination activities and standardization activities.	PU	M18
D8.4	**SOCCRATES white paper** High quality and attractive deliverable containing the SOCCRATES results and experiences in an easily accessible way, suitable for policy makers and higher management of stakeholders. It will be available on-line and in printed version.	PU	M30
D8.5	**Final report on dissemination and standardization activities** Contains the overview and results of all dissemination activities and standardization activities that have been undertaken in the SOCCRATES project.	PU	M36
D8.6	**SOCCRATES Exploitation plan** Contains the plans for exploitation of the expected project results.	PU	M36

5 Communication Channels, liaison, means and media

SOCCRATES utilizes several channels and media to reach the ambitious dissemination goals. This chapter highlights these channels and media.

5.1 SOCCRATES Advisory Board (SOCAB)

The SOCCRATES Advisory Board (SOCAB) forms an independent review group of external (non-funded) experts within the areas of CSIRT organizations, academia, industry and regulations. SOCAB members provide external reflection on the operational and strategic direction of the project and are invited to project events, will contribute to the requirements, and should review project results, which will include both software and written deliverables. The SOCAB does not have a direct governing role in the project but may be consulted by any of the other project roles or governing bodies. The composition of the SOCAB at the time of delivery of this document is:

- Andy de Petter, Head of cyber security intelligence & incident response, Proximus (BE),
- Frode Hommedal, subject matter lead CERT and SOC, PwC (NO)
- Dr. Judith E.Y. Rossebo, specialist cyber security & infrastructure - ABB (NO)
- Martin Pekarek, Cybersecurity advisor Dutch National Cyber Security Center (NL)

The SOCAB will meet with the project at least once a year.

Measurable outcome:

- Number of SOCAB meetings [3]
- SOCAB member attendance on SOCAB meetings [>2]
- SOCAB attendance on SOCCRATES organized workshops [>1].

5.2 SOCCRATES stakeholder group

The SOCCRATES Stakeholder Group is a group of service providers, end-users, regulators and vendors that have indicated to be interested in the results of the project. They will be informed about progress, encouraged to provide input and be invited for SOCCRATES events. The Stakeholder Group also is important for the exploitation of project results, where we expect some of the members to become early users of SOCCRATES results. Current members are:

Name	Role	Organization	Country
Olivier Thonnard	Senior Expert, Tech Lead Application SOC	Amadeus IT group	FR
Etienne Kuijkhoven	manager SOC	KPN	NL
Rob van Os	Product owner cyber defense center	Volksbank	NL
Wil van Gemert	Deputy Executive Director Operations	Europol	NL
Paul Samwel	CISO	ONVZ	NL
Tone Thingbo	Security officer	TDC	DK
Erik Rutkens	Owner and director Qbit	Qbit	NL
Jan Willem Spee	CISO	RDW	NL
Tijs Wilbrink	Business innovation manager	Topsector energie	NL
John Post	Program director	Topsector energie	NL
Jelle Groenendaal	Global Resilience Manager	ING	NL
Ulrich Seldeslachts	CEO	LSEC	BE
Peter Amthor	Postdoctoral Researcher	Technische Universität Ilmenau	DE

We will expand the group during the project.

Measurable outcome:

- Number of SOC/CSIRT operators in stakeholder group [>10]
- Stakeholder group member attendance on SOCCRATES organized workshops [>6]

5.3 SOCCRATES logo

The SOCCRATES logo will be used consistently throughout all communications of the SOCCRATES project. See below in Figure 3 for the logo and its different appearances.

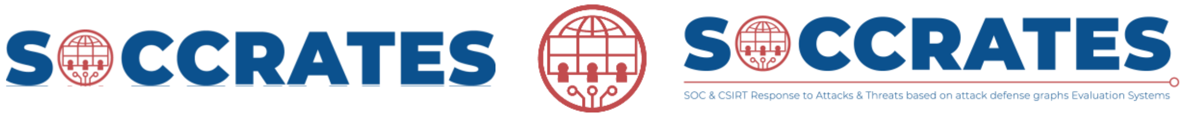
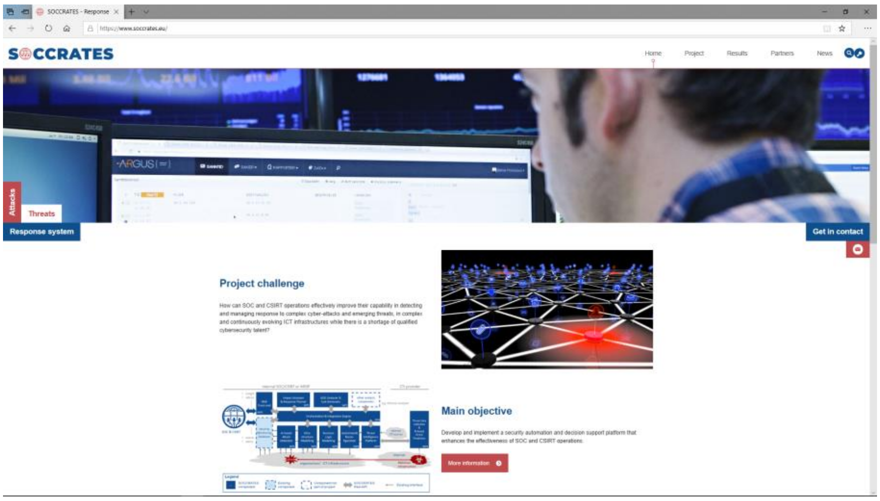

SOCCRATES
SOCCRATES
SOC & CSIRT Response to Attacks & Threats based on attack defense graphs Evaluation Systems

Figure 3 – SOCCRATES logos

5.4 SOCCRATES website

The SOCCRATES website (www.SOCCRATES.eu) is the general communication channel for SOCCRATES. the frontpage of the website is sown in Figure 4. The website shows general information of the SOCCRATES project, the project approach and its partners. Also, it offers the possibility to download public deliverables and the opportunity to contact the project. The website will be refreshed with actual information as often as possible.



Project challenge

How can SOC and CSIRT operators 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 cybersecurity talent?

Main objective

Develop and implement a security automation and decision support platform that enhances the effectiveness of SOC and CSIRT operations.

Figure 4 – front page of the SOCCRATES website

The website also has a closed part that is only accessible for members of the SOCAB and the stakeholder group and is used to share specific information with them and discuss with them.

Measurable outcome:

- Blog posts [15]
- Yearly visits to the closed part of the website [>100]
- Views/accesses of the website during the project lifetime [>3.000]
- Unique visitors to SOCCRATES website per month in the last year of the project [>100]

5.5 Social media

The social media presence of SOCCRATES will be focussed around LinkedIn. We consider this a more professional and therefore suitable platform than media such as Twitter and Facebook. SOCCRATES has implemented a LinkedIn account (https://www.linkedin.com/groups/13786643/) to provide the LinkedIn community with results of SOCCRATES and to discuss the approach of the project and usability of the results. This allows SOCCRATES to quickly reach a wide audience with news of important breakthroughs, both those arising from within the project, because of our efforts, and those stemming from external sources, such as new threats being discovered, and/or relevant technologies being developed in parallel with the project. We will also use it to promote project events, like workshops, attendance at exhibitions and public fora and similar, leveraging social media links to other related ongoing EU- and nationally-funded projects.

Measurable outcome:

- Posts made by SOCCRATES project members [>100]
- Membership of SOCCRATES target groups [>30]
- Active participation of members (e.g. posts, comments) [>100]

5.6 SOCCRATES webinars

SOCCRATES will organize several webinars, to present and discuss SOCCRATES results. The invitation to attend a webinar will be spread widely to all SOCCRATES stakeholders (see chapter 3). The webinars focus on specific subjects and therefore complement the other SOCCRATES events, such as the workshops.

Measurable outcome:

- Number of webinars held [>5]
- Number of participants per webinar [>15]

5.7 Give-aways

If budget allows and suitable items are found, SOCCRATES will order some simple give-aways with the SOCCRATES logo, to distribute at conferences and events and increase the visibility of the project.

5.8 SOCCRATES white paper

SOCCRATES will edit and publish a high quality and attractive deliverable containing the SOCCRATES results and experiences in an easily accessible way, suitable for policy makers and higher management of stakeholders. It will be available on-line and in printed version. The white paper is a high-quality deliverable (D8.4) and will be referred to as the SOCCRATES SOC/CSIRT security white paper.

Measurable outcome:

- Number of white paper downloads [>250]
- Number of printed copies given to interested people [>100]

5.9 SOCCRATES Video

SOCCRATES will produce several short (animated) videos with a simple explanation of the SOCCRATES approach and results, to present the SOCCRATES results to a broader public. They can be viewed and will be downloadable from the SOCCRATES website.

Measurable outcome:

- Informative and educational videos [3-6]
- Number of video views [>50]

5.10 SOCCRATES pilots

The SOCCRATES platform will be deployed and validated at two pilot sites (i.e. Vattenfall and mnemonic). In addition, a third pilot site (i.e. SHS) at which a large amount of threat data is collected by monitoring malicious infrastructures is used for testing and validation of the SOCCARTES threat prediction technology.
These pilots are an excellent opportunity to show that the SOCCRATES platform adds value to operational environments. We will use the opportunity for dissemination through video, webinars etc.

5.11 SOCCRATES demonstrations

There will be three iterations of the SOCCRATES platform. We will use each iteration to illustrate SOCCRATES results by demonstrating the functionality of the SOCCRATES platform at events and workshops.

Measurable outcome:

- Demonstrate SOCCRATES platform at cyber security related events. [>5]

5.12 SOCCRATES workshops

Several public dissemination workshops will be organised, possibly in collaboration with other conferences. At least one workshop will take place just before the first project review, so the consortium still has the possibility to adjust specific system aspects, methods or tools based on the feedback. Also at least one workshop will be organized at the end of the project so that we can inform end users, service providers and vendors about the project's results and gather feedback. These events will be public and advertised in a timely manner to convey a large audience.

Measurable outcome:

- Number of workshops [>2]
- Number of workshop attendees [20-30]

5.13 Conferences

SOCCRATES will take a flexible approach towards conferences. When it is in the interest of SOCCRATES, the project will strive to attend or if possible present at relevant conferences. Although a complete and comprehensive list cannot be given for the whole project lifetime, at least the following list of conferences is important for SOCCRATES and active presence will be sought at these conferences.

Table 2 - Conferences relevant for SOCCRATES

Academic Conference	**Deadline**
International Conference on Cyber Situation Awareness, Data Analytics and Assessment	Feb
International Conference on Computer Safety, Reliability, and Security	Feb
IEEE Conference on Communications and Network Security	April
International Conference on Critical Information Infrastructures Security	June
IEEE Symposium on Security and Privacy	Nov
IEEE/IFIP International Conference on Dependable Systems and Networks	Dec
ACM Conference on Computer and Communications Security	May
Tradeshow and Practitioner Events	**Date**
FIC (Forum International de la Cybersécurité), Lille, France	Jan

e-Crime & Cyber Security	March
FIRST Conference	June
MITRE ATT&CK workshops	Ongoing
BlackHat Conference	August

SOCCRATES will also strive to participate in the annual conferences as shown in Table 3 below.

Table 3 Overview of annual conferences

Conferences	About	Target audiences
ARES	http://www.ares-conference.eu/conference/	Research community
RAID - International Symposium on Research in Attacks, Intrusions and Defenses	http://www.raid-symposium.org/	Research community
DIMVA - SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment	https://www.dimva.org/	Research community
GraMSec	https://gramsec.uni.lu/	Research community
ESORICS - European Symposium on Research in Computer Security	www.esorics.org	Research community
Euro S&P - European Symposium on Security and Privacy	https://www.ieee-security.org/TC/EuroSP2020/	Research community
FSE (Fast Software Encryption)	http://light-sec.org/fse2015/index.php/event/program	Research community

Measurable outcome:

- Number of scientific publications [10-20 conference papers accepted].

5.14 Journals and magazines

Journals and magazines are a very suitable channel to publish SOCCRATES results. SOCCRATES has identified the following list of journals and magazines as relevant for the project dissemination objectives and will strive to publish SOCCRATES results in those magazines. This does not exclude any other opportunity that might arise to publish SOCCRATES results in other magazines or journals. Journals/magazines where SOCCRATES has published or plans to publish are:

Journals and Magazines	Impact Factor
IEEE Access	3.24
IEEE Security & Privacy Magazine	1.38
Proceedings of IEEE	9.24
ACM Transactions on Privacy and Security	NA
Elsevier Computers & Security	2.85

Elsevier Journal of Information Security and Applications (JISA)	1.357
Computers and Security (COSE)	3,06
International Journal of Information Security (IJIS)	1,82

Measurable outcome:

- Number of scientific publications [3 journals].

5.15 Press releases

SOCCRATES does not foresee the publication of press releases. But if necessary, this channel will be utilized if relevant, after consultation of the PO.

5.16 Liaison with other projects

5.16.1 EU projects

SOCCRATES aims to liaise with a limited number) of projects that have comparable objectives as SOCCRATES. We already identified the following projects, funded in the same call as SOCCRATES:

- GUARD - A cybersecurity framework to GUArantee Reliability and trust for Digital service chains
- CyberSANE – Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
- C4IioT - Cyber security 4.0: protecting the Industrial Internet Of Things
- SAPPAN – Sharing and Automation for Privacy Preserving Attack Neutralization
- SIMARGL - Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware
- nIoVe - A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles

But we also look at projects outside the same call but with the comparable objectives as SOCCCRATES :

- Energy Shield – Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical energy Infrastructures (both Foreseeti and KTH participate in this project)
- Concordia – A cybersecurity competence Network with leading research, technology, industrial and public competences
- Cyberwatching.eu - the Cyberwatching.eu project uses a number of underpinning information sources to visualise the state of the art of projects in more than 25 calls which ware in the domain of cybersecurity and privacy, as a means to maintain oversight of the larger European Cybersecurity research landscape.

Measurable outcome:

- Liaison with other EU projects [>2]
- Co-hosted workshops [2]
- Attendees at co-hosted workshops [30-50]

5.17 Standardization

SOCCRATES will follow the work of relevant standardization bodies. Where possible and relevant, SOCCRATES will discuss with those bodies, deliver input or set up liaisons. One reason is the dissemination of SOCCRATES results into standardization bodies, another reason is the improved availability of standards for the SOCCRATES project.

The following is a list of potentially relevant standards & standardization bodies.

Cyber Threat Intelligence & SOC/CSIRT operations	
OASIS CTI TC	OASIS Cyber Threat Intelligence (CTI) TC is chartered with developments and maintenance related to specifications: • STIX (Structured Threat Information Expression), • TAXII (Trusted Automated Exchange of Indicator Information) These are the well-known standards for automated cyber threat intelligence sharing. https://www.oasis-open.org/committees/cti *Relevant for SOCCRATES:* CTI exchange
OASIS OpenC2	OASIS Open Command and Control (OpenC2) TC is chartered to create standardized language for the command and control of technologies that provide or support cyber defenses. OpenC2 typically uses a request-response paradigm where a Command is encoded by a Producer (managing application) and transferred to a Consumer (managed device or virtualized function) using a secure transfer protocol, and the Consumer can respond with status and any requested information. First standards have versions of the OpenC2 specification have been published. https://www.oasis-open.org/committees/openc2 See also OpenC2 Forum https://openc2.org/ *Relevant for SOCCRATES:* CoA execution
OASIS CACAO	OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC members are developing a standard to implement the course of action playbook model for cybersecurity operations. CACAO was launched in September 2019. https://www.oasis-open.org/committees/cacao *Relevant for SOCCRATES:* CoA execution
OASIS TAC	TAC TC seeks to resolve ambiguity across different sources and solutions in order to support organizing what is known and to share information about threat actors and the STIX Domain Objects (SDOs) related to them such as Intrusion Sets, Campaigns and Indicators. The TC will establish a common knowledge framework that enables semantic interoperability of threat actor contextual information. https://www.oasis-open.org/committees/tac Relevant for SOCCRATES: CTI exchange, Threat Intelligence Platform
IETF MILE	Managed Incident Lightweight Exchange (MILE) working group develops standards to support computer and network security incident management. Among others: • RFC 7970 - Incident Object Description Exchange Format (IODEF) • RFC 6545 - Real-time Inter-network Defense (RID) • RFC 8322 - Resource-oriented lightweight information exchange (ROLIE)

	https://datatracker.ietf.org/wg/mile/about/ *Relevant for SOCCRATES:* CTI exchange, Infrastructure Modelling
FIRST CTI SIG	FIRST CTI SIG The Cyber Threat Intelligence (CTI) Special Interest Group (SIG) focusses on the application of threat intelligence capability. Incl. best practice in the context of supporting effective digital forensics and incident response (DFIR) operations. The group also discusses CTI standards. https://www.first.org/global/sigs/cti/ *Relevant for SOCCRATES:* CTI exchange
FIRST Standards Groups	FIRST also enables members to initiate Special Interest Groups to develop standards that increase interoperability between security and incident response teams. Most relevant for SOCCRATES are: • Common Vulnerability Scoring System (CVSS) • Information Exchange Policy • Traffic Light Protocol (TLP) https://www.first.org/standards/ *Relevant for SOCCRATES:* CTI exchange
ICT Infrastructure modelling	
NIST SCAP Incl. CPE, OVAL, XCCDF	The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications. SCAP is a standardized form for expression and reporting of security content. The specifications were initially setup towards vulnerability management application. Nowadays it is viewed broader and include: compliance, remediation, and network monitoring. • CPE - CPE is a structured naming scheme for information technology systems, software, and packages. MITRE developed the Common Platform Enumeration (CPE). NIST holds operational responsibility. • OVAL - Open Vulnerability and Assessment Language (OVAL) includes representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. • XCCDF - The Extensible Configuration Checklist Description Format (SCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. NIST is currently working on SCAP 2.0. The work is related to IETF SACM. https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol https://csrc.nist.gov/publications/detail/white-paper/2018/09/10/transitioning-to-scap-version-2/final *Relevant for SOCCRATES:* Infrastructure Modelling
SWID ISO/IEC 19770-2	ISO/IEC 19770 is a family of standards for IT asset management and addresses both the processes and technology for managing software assets and related IT assets. Software Identification (SWID) Tags are defined in ISO/IEC 19770-2:2015 and provide authoritative identifying information for installed software. NIST has selected SWID for SCAP 2.0 instead of CPE. https://www.iso.org/standard/65666.html https://tagvault.org/ Relevant for SOCCRATES: Infrastructure Modelling

IETF SACM	Security Automation and Continuous Monitoring (sacm) working group develops standards for protocols and models aiding collection and evaluation of endpoint elements enable (security) automation. (Security) Posture assessment entails the following five steps: 1. Identify and characterize target endpoints 2. Determine specific endpoint elements to assess 3. Collect and make available specified elements' actual values 4. Compare actual element values to policy compliant element values 5. Make results available Among others: - RFC 7632 - Endpoint Security Posture Assessment: Enterprise Use Cases - RFC 8248 - Security Automation and Continuous Monitoring (SACM) Requirements - RFC 8412 - Software Inventory Message and Attributes (SWIMA) for PA-TNC - SACM Information Model, IETF Internet-Draft, draft-inacio-sacm-info-model-00, July 2019 The work is related to NIST SCAP 2.0. https://datatracker.ietf.org/wg/sacm/ *Relevant for SOCCRATES:* Infrastructure Modelling
DTMF Common Information Model (CIM)	DMTF (formerly known as the Distributed Management Task Force) creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. The Common Information Model (CIM) provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. https://www.dmtf.org/standards/cim *Relevant for SOCCRATES:* Infrastructure Modelling
IETF OSM	Open Source MANO (OSM) is a collaborative open source project hosted by ETSI to develop an NFV Management and Orchestration stack aligned with ETSI NFV Information Models and APIs. OSM Information Model is aligned with ETSI NFV release 2 Information model. https://osm.etsi.org/wikipub/index.php/OSM_Information_Model *Relevant for SOCCRATES:* Infrastructure Modelling (Comment FF: A colleague pointed to this standard. He is responsible for our research cloud. I cannot yet assess if this is a relevant standard for SOCCRATES)
General ICT / cyber security standardisation bodies	
ETSI TC Cyber	ETSI TC Cyber is ETSI centre of expertise in the area of Cyber Security. It develops standards on divers set of security topics. Most relevant for SOCCRATES is that TC Cyber is since 2019 responsible for maintenance of the ISG Information security indicators (ISI) specifications. ISI provide the basis to switch from a qualitative to a quantitative culture in IT Security Scope of measurements: External and internal threats (attempt and success), user's deviant behaviours, nonconformities and/or vulnerabilities (software, configuration, behavioural, general security framework). Include standards for SOC and SIEM. https://en.wikipedia.org/wiki/Information_security_indicators

ISO JTC1 SC27	ISO JTC1 SC27 is the committee that develops standards for the protection of information and ICT. The focus is on Information security, cybersecurity and privacy protection. SC27 has the following working groups: • WG1 – Information security management systems • WG2 – Cryptography and security mechanisms • WG3 – Security evaluation, testing and specification • WG4 – Security controls and services • WG5 – Identity management and privacy technologies https://www.iso.org/committee/45306.html
CEN JTC13	New European standardisation group that develops standards for data protection, information protection and security techniques.
ITU-T SG17	Study Group 17 of ITU-T is tasked with Cyber Security standardisation.

6 Exploitation

The SOCCRATES partners all will strive to maximally exploit the SOCCRATES results. These results will be exploited by all individual partners, after the project. The way of exploitation will be addressed in the exploitation plan (D8.6), that will be made in the last phase of the project. The exploitation plan will identify and capture the commercial exploitation of SOCCRATES results by each of the consortium partners and by others. It identifies the scientific and technical knowledge, products and services (deliverables) of the project susceptible to be exploited, classification of these according to their commercial potential, while foreseeing potential barriers for the exploitation. It includes high level assessment, of the expected impact of the knowledge and technology generated and the factors that would influence their exploitation (such as standardisation, regulatory aspects, etc.). It includes an IPR protection strategy according to the interest of partners and stated in the Consortium Agreement, assessment of future feasibility of the project results in the respective marketplaces and a technology implementation plan developed for the future commercial deployment of the results.

7 Dissemination Work Plan

This section provides a comprehensive plan for the SOCCRATES dissemination activities. These activities can be divided in three categories:

- Ongoing activities – these are activities that will be ongoing during project lifetime, such as maintaining the website

- Planned activities – these are activities that can be planned beforehand, either at a specific date or in a timeframe (e.g. Q4 of 2016)

- To-be planned activities these are activities that cannot be planned at this moment. They will be listed and where possible, the activities are planned at specific dates during the project, but not every activity can be planned beforehand.

After each year, a concise report of the SOCCRATES dissemination activities will be made.

7.1 Ongoing dissemination activities

A number of dissemination activities are ongoing and are listed in

Table 4 below.

Table 4 - Ongoing dissemination activities

Dissemination activity	Responsible partners
Maintaining the SOCCRATES website : post news, update information, publish deliverables etc	TNO
Actively inform the Advisory Board and Stakeholder group on project progress, by bulletins, email etc.	TNO
Maintaining the LinkedIn account	TNO
Webinars	All partners
Demonstrate SOCCRATES platform at cyber security related events	All partners
Responding to questions of interested people (through website or Linked-in)	All partners
Set up liaisons with other projects and standardization bodies	All partners

7.2 Planned dissemination activities

The table below shows the planned dissemination activities for the SOCCRATES project.

Table 5 – planned dissemination activities

Dissemination activity	Planned date		Responsible partners
Organize workshop at ARES event	2019	August 2019	AIT
Launch SOCCRATES website		Q4 2019	TNO
Submit papers for: • International Conference on Cyber Situation Awareness, Data Analytics and Assessment • International Conference on Computer Safety, Reliability, and Security	2020	Q1, 2020	All partners
First SOCAB meeting		Q2, 2020	TNO
Submit papers for: • IEEE Conference on Communications and Network Security • International Conference on Critical Information Infrastructures Security • ACM Conference on Computer and Communications Security		Q2, 2020	All partners
Submit papers for: • IEEE Symposium on Security and Privacy		Q4, 2020	All partners

• IEEE/IFIP International Conference on Dependable Systems and Networks			
Short video to introduce the concepts of SOCCRATES		Q2, 2020	TNO
SOCCRATES workshop/event		Q2, 2020	TNO
Organize workshop at ARES event		Q3, 2020	AIT
SOCCRATES workshop/event	2021	Q1, 2021	TNO
Second SOCAB meeting		Q1, 2021	TNO
Submit papers for: • International Conference on Cyber Situation Awareness, Data Analytics and Assessment • International Conference on Computer Safety, Reliability, and Security		Q1, 2021	All partners
Short video to highlight intermediate results		Q2, 2021	TNO
Submit papers for: • IEEE Conference on Communications and Network Security • International Conference on Critical Information Infrastructures Security • ACM Conference on Computer and Communications Security		Q2, 2021	All partners
Organize workshop at ARES event		Q3, 2021	AIT
Submit papers for: • IEEE Symposium on Security and Privacy • IEEE/IFIP International Conference on Dependable Systems and Networks		Q4, 2021	
Publication of SOCCRATES White paper (D8.4)	2022	Q1, 2022	TNO
Submit papers for: • International Conference on Cyber Situation Awareness, Data Analytics and Assessment • International Conference on Computer Safety, Reliability, and Security		Q1, 2022	All partners
Final SOCAB meeting		Q2, 2022	TNO
Short video to highlight SOCCRATES results and exploitation		Q2, 2022	TNO
Submit papers for: • IEEE Conference on Communications and Network Security • International Conference on Critical Information Infrastructures Security		Q2, 2022	All partners

• ACM Conference on Computer and Communications Security		
Publishing SOCCRATES exploitation plans	Q3 2022	All partners
SOCCRATES final workshop	Q2, 2022	TNO

7.3 To-be-planned dissemination activities

The following table contains an overview of dissemination activities that cannot be planned at this moment. This also includes annual conferences that are organized outside of Europe. SOCCRATES budget does not include travel outside of Europe, unless the SOCCRATES PO gives permission. So SOCCRATES can only be disseminated at these conferences after permission of the PO.

Table 6 – To-be-planned dissemination activities

Dissemination activity	Responsible partners
Dissemination towards standardization bodies (2019-2022)	All partners
Publishing papers in the context of conference presentations or in magazines and journals (2019-2022)	All partners
Informing policy and decision makers (2019-2022, EU and national level)	All partners
Demonstrations of running pilots for interested parties	MNM. VTF, SHS
Publishing press release(s) if relevant and needed	TNO
Submitting articles to these magazines :	
IEEE Access	All partners
IEEE Security & Privacy Magazine	All partners
Proceedings of IEEE	All partners
ACM Transactions on Privacy and Security	All partners
Elsevier Computers & Security	All partners
Elsevier Journal of Information Security and Applications (JISA)	All partners
Computers and Security (COSE)	All partners
International Journal of Information Security (IJIS)	All partners
Attending and/or contributing to these conferences if feasible:	
RAID - International Symposium on Research in Attacks, Intrusions and Defenses	All partners
DIMVA - SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment	All partners
GraMSec	All partners
ESORICS - European Symposium on Research in Computer Security	All partners
Euro S&P - European Symposium on Security and Privacy	All partners
FSE (Fast Software Encryption)	All partners
FIC (Forum International de la Cybersécurité), Lille, France	All partners
e-Crime & Cyber Security	All partners
FIRST Conference	All partners

MITRE ATT&CK workshops	All partners
BlackHat Conference	All partners

8 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
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
OS	Operating System
RORI	Return on Response Investment
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
VLAN	Virtual LAN
VM	Virtual Machine
VTF	Vattenfall