SOCCRATES

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

D8.3
First Dissemination report

Deliverable type:	Report
Contributing work packages:	WP8 Dissemination
Due date of deliverable:	28/02/2021
Submission date:	28/02/2021
Dissemination level:	PU

Responsible organisation:	TNO
Editor:	Reinder Wolthuis
Revision:	1.0

Abstract	This document reports the dissemination activities and results that were conducted and achieved during the first half of the of the SOCCRATES project.
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

Author(s)	Reinder Wolthuis (TNO) Paul Smith (AIT) Ewa Piatkowski (AIT) Frank Fransen (TNO) Lenny Zilverberg (TNO) Piotr Kijewski (SHS) Mathias Ekstedt (KTH) Martin Eian (mnemonic) Ruben Trapero (ATOS) Christophe Kiennert (IMT) Rafal Kondracki (VTF) Per Eliasson (FRS) Marko Komssi (FSC)

Reviewer(s)	Gabriela Bodea (TNO)

Security Assessment	
Approval Date	24/02/2021
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.

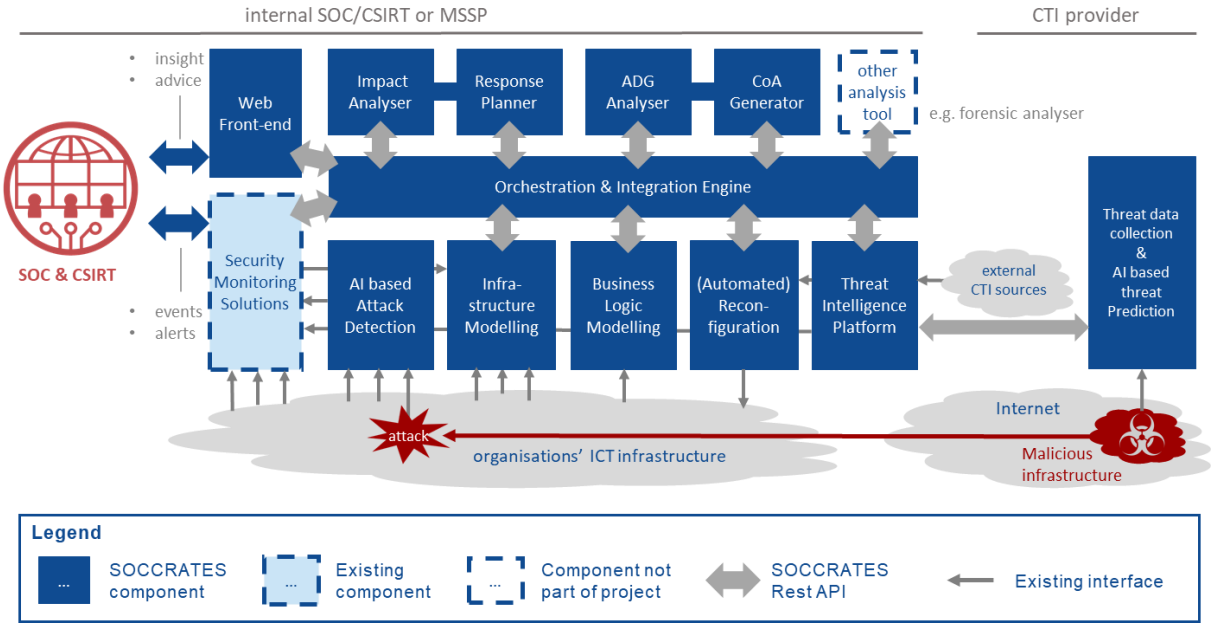

Figure 1 – The SOCCRATES platform

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 intermediate report on dissemination activities and contains the progress of dissemination activities and standardization activities in the first half of the SOCCRATES project. We also have included the first ideas for exploitation of results during and after the project. Additionally, we report on the progress on the dissemination KPI's as defined in the SOCCRATES Dissemination Pan [D8.2].

1.3 Structure of this deliverable

Section two reports the overall progress on dissemination, with respect to project results, dissemination objectives that were defined and issues that have arisen. Section three lists all dissemination and activities that were conducted and the KPI levels that were achieved in the first half of the project. Section four provides initial ideas on exploitation of SOCCRATES results during and after the project and section five looks ahead to the second half of the project and provides a high level planning of dissemination and exploitation activities to be conducted. Finally, the annex provides an overview of KPI levels that were achieved and some details how we achieved these levels.

2 Overall dissemination progress

2.1 Project results

In the dissemination plan, we had defined four main categories of project results that SOCCRATES intends to disseminate to stakeholders. We shortly describe the achievements thus for each of these categories :

- *Prototype technologies that have been validated in the project's piloting activities*; We started the first technical pilot, that is limited to evaluating a number of SOCCRATES modules, on January 1st 2021, so we are in an early stage of validation. Three modules are tested on location of SOCCRATES partner mnemonic:
  - AI-based Attack Detection (AAD)
  - Infrastructure Modelling Component (IMC)
  - Threat Intelligence Platform (TIP)

  First early results are promising and show that, although there are some issues to overcome (mainly on integration of technologies and embedding SOCCRATES innovations in existing environments), the SOCCRATES modules that were tested seem to work in practice.
- *Guidance on the use of these technologies by SOCs and CSIRTs, highlighting their potential benefits;* As mentioned above, we have not come to a stage in which we can provide guidance on implemented solutions to our target groups on potential benefits yet. But we did provide much information on the concepts and design of some of the technologies to our SOCAB and stakeholders and in a series of webinars, in which also SOC and CSIRT representatives participated.
- *Materials, such as published articles, that highlight the technological innovations from the project that can be built upon by the community*; we have conducted several dissemination activities for this. Examples are our deliverables (published on our website), several workshops we organized and presented, conferences we presented, our webinar series and a first list of articles. Please see section three for more details. We will publish much of the developed software as Open Source.
- *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.* We are in the process of developing these API's and datasets. They are not available to the SOC and CSIRT community yet, but we will be able to make them available in the second half of the project.

2.2 Influence of the Pandemic on dissemination

Since March 2020, due to the COVID-19 pandemic, the world was closed for travel; internationally, but most countries also had heavy restrictions on national travel and limits on the number of people that can gather. This influenced our dissemination plans quite heavily. We had to organize most events we planned as virtual meetings. It proved to be difficult to interest people to virtual events and we noticed that only about one third of people that registered for virtual events actual did attend. Also talking to interested parties became much harder. We took some measures to improve the effect and impact of our virtual dissemination activities:

- We purchased 15 professional quality (USB) microphones; one for each partner and a few additional ones for people that often present in webinars. This definitely improved the sound quality and consequently the overall quality and attractiveness of virtual events;
- We purchased a CISCO webex events license, to be able to organize virtual events in a professional manner;
- We updated our website to facilitate webinar registration and made sure that all our webinars are recorded and recordings are put on the website;

We could do all this within the agreed budget, because the number of travels and thus the travel cost was heavily reduced due to COVID-19.

2.3 Progress on dissemination objectives

SOCCRATES adopted a number of dissemination objectives that support the SOCCRATES objectives (see paragraph 1.1). See below a short description of the progress in reaching these objectives (in italic the objective, in regular character the progress)

- *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;* we reached many service providers, end users and vendors through our webinars and stakeholder group (see section 3). We noticed through the heavy interaction and compliments that we succeeded in raising their awareness. The number of policy makers and regulatory bodies we reached was limited. We are in the process of combining forces with other H2020 projects from SU-ICT-01-2018 to be more effective in approaching these policy makers and regulatory bodies.
- *To develop the SOCCRATES SOC/CSIRT white paper composed of project results specifically targeted to raise awareness among higher management of stakeholders;* The white paper is scheduled to be produced in the second half of the project, so we can include learnings from the pilot evaluations.
- *To disseminate project results to relevant target groups and potential users of the SOCCRATES Platform and components;* We have undertaken many activities in this area: presentations, papers, webinars, workshops. We will continue to do so in the second half of the project.
- *To identify and execute opportunities for contributions to standards based on SOCCRATES results.* Also here, progress was limited thus far. We hope to profit of the cooperation with other H2020 projects from SU-ICT-01-2018 and will increase our efforts in this area in the second half of the project.
- *To develop and implement an interactive and user-friendly web site to inform the public and relevant stakeholders about the project;* The website has been up-and running from month 3 after the project start. We keep it up-to-date and it seems to work quite well.
- *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.* We have put the initial ideas on exploitation in chapter four. We will continue to expand these ideas and this will result in an Exploitation Plan at the end of the project.

2.4 Target groups that were reached

As explained in the previous paragraphs, with our activities we have reached most of the target groups that we aimed for: MSSPs, SOCs, CSIRTs, National Certs, Vendors, End Users. We had intense contacts with them at events, workshops, webinars and in our stakeholder group. The contacts with regulatory bodies, policy makers and standardisation bodies were not as many as we had hoped for.

2.5 Sensitive information

All deliverables and material that became public has been assessed by our Security Advisory Board and our ethics advisor. For most deliverables and material this did not lead to any issues, only for one specific deliverable (D7.1, pilot plan) this led to an advice to change the classification level from 'Public' to 'Confidential, only for members of the consortium (including the commission services)'.

3 Dissemination activities and results

Almost all dissemination instruments as described in the dissemination plan have been utilized as effectively as possible in the dissemination activities of the first period. There were a few exceptions:

- The SOCCRATES white paper is planned to be published in the second period,
- There was no reason to publish a SOCCRATES press release

We have defined several Dissemination KPI's. In the paragraphs below we have summarized the KPI score per dissemination activity or result. More detailed information can be found the Annex at the end of this report.

3.1 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 visit 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, Head of Cyber Threat Operations, Defendable (NO)
- Dr. Judith E.Y. Rossebo, specialist cyber security & infrastructure - ABB (NO)
- Martin Pekarek, Cybersecurity advisor Dutch National Cyber Security Center (NL)

So far there have been 3 SOCAB meetings, namely May 26th 2020, September 15th 2020 and December 15th 2020. At the first and third meeting, all 4 members were attending. The second SOCAB meeting, 3 members were present. The SOCAB meetings proved to be very useful. We presented results and provided demonstrations (specifically requested by the SOCAB members) and there was intense interest from and interaction with the SOCAB members. We even had to schedule a second part of the May meeting on June 9th, again with all members present, because we did not get through the agenda. We had many good suggestions that helped us to improve the project results. Also there was individual follow-up with several SOCAB members to support us in dissemination opportunities. The members were, so far, not able to attend our SOCCRATES workshops.

Measurable outcome:

KPI	Target level	Current score
Number of SOCAB meetings	3	3
SOCAB Attendance on SOCCRATES organized workshops	1	0

3.2 SOCCRATES stakeholder group

The SOCCRATES Stakeholder Group is a group of SOCs, CSIRTS, National certs, MSSPs, end-users 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 listed in the table below.

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	Security Advisor / Cyber Defense Specialist	CZ health insurance	NL
Wil van Gemert	Deputy Executive Director Operations	Europol	NL
Paul Samwel	CISO	ONVZ	NL
Erik Rutkens	Practor safe hard- and software / board member Zerocopter	Noorderpoort	NL
Jan Willem Spee	CISO	RDW	NL
Tijs Wilbrink	Business innovaton manager	Topsector energie	NL
John Post	Program director	Topsector energie	NL
Ulrich Seldeslachts	CEO	LSEC	BE
Peter Amthor	Postdoctoral Researcher	Technische Universität Ilmenau	DE
Vesna Lucassi	CISO SLL/ Head of Information Security Department	Stockholm County Council (SLL)	SE
Tale Sundlisaeter and Simen Linderud	Security analyst	Telenor	NO
Ronny Vaningh	Expert cyber security intelligence & incident response	Proximus	BE
Ronald Pool	Cyber Security Specialist	Crowdstrike	NL
Wim Stoffelen	Director partnerships and alliances	SECO-Institute	NL
Erik Post	Senior consultant informatietechnologie	Ordina	NL
Olivier Bettan	Head of Cyber Security Lab	Thales Six GTS France	FR
Jacob Henricson	CISO	Skanska Sweden	SE
Bijay Limbu Senihang	Chief Technology Officer	Vairav Technology	NP
Dr. Vilius Benetis	Director	NRD Cyber Security	LT
Armins Palms	Security analyst	CERT.LV	LV
Lars Erik Smevold	Security analyst R&D	Norwegian Energy Sector and Control System CERT	NO
Pawel Pawlinski	Principal security apcialist	CERT.PL	PL
Roger Cato Bergheim Johnson	Security analyst	Defendable	NO

We currently have 26 members of 24 different organisations and are still expanding our group.
So far there have been 2 stakeholder meetings, namely September 28th 2020 (15 stakeholders present) and February 16th 2021 (15 stakeholders present). We used the first meeting as an introduction, where we introduced the project and provided several demonstrations. In the second meeting, we presented the project progress, provided a demonstration of the Adversary Emulation Plan and reserved one hour for interactive discussion that was guided by questions we prepared. The meetings were very well received and many remarks were made on the ambitious SOCCRATES goals and without exception our stakeholders think the topics that SOCCRATES addresses are very interesting

and relevant. Also we received valuable feedback and suggestions that we can use to improve the project.
Please see in the table below the stakeholder members per organisation profile. Please note that some organisations have more than one profile, e.g. KPN both has an own internal SOC but also is a provider of security services (MSSP). As the table shows, we are well on our way to reach the desired target levels and in one case we already have reached the target level. We are especially satisfied with the number of national CERTs, which we could reach through the excellent network of our partner Shadowserver.
In some case contact persons have changed organisation. In a few cases this meant that we lost the organisation as stakeholder member (e.g. TDC, de Volksbank), in other cases the organisation assigned other staff to become member of the stakeholder group (e.g. Telenor). Also in some cases the contact person made sure that their new organisation also became a member of the stakeholder group (e.g. CZ).
We will continue our efforts to expand the stakeholder group with the different organisation profiles.

KPI	Target level	Current score
Number SOC/CSIRT operators in stakeholder group	>10	8
Number of MSSP's in stakeholder group	>10	8
Number of National CERTs in stakeholder group	>2	3
Number of end users in stakeholder group	>10	6
Number of vendors in stakeholder group	>5	4
Stakeholder group members attendance on SOCCRATES organized workshops	>6	2

3.3 Other stakeholders

3.3.1 MSSPs, National CERTs, Vendors, End users

Please see in the table below the number of organisations contacted, per organisation profile. Please note that some organisations have more than one profile, e.g. Thales is both a vendor and an MSSP. Please also note that we also included members that have become member of the stakeholder group after initial contact in this table. Information about the SOCCRATES project has also been shared by Vattenfall with about 40 users from different business units (internally).
The details of the table below can be found in the Annex.

KPI	Target level	Current score
Number of MSSPs contacted about SOCCRATES	>25	10
Number of national CERTs contacted about SOCCRATES	>5	6
Number of vendors contacted about SOCCRATES	>10	4
Number of end users contacted about SOCCRATES	>25	14

3.3.2 Participation at industry bodies' events

SOCCRATES presented on several industry bodies events, see table below. We are well on the way to reach the targeted number of these participations and expect to exceed this target at the end of the project. Details can be found in the annex.

KPI	Target level	Current score
Participation at industry bodies 'events	6	5

3.3.3 Security research community:

We have defined three KPI's to measure the interest in the security research community, see the table below. We did not produce many papers yet, and also our white paper is scheduled for the second half of the project, that is why the number of downloads and citations still is quite low. We expect to reach the target for downloads, but we estimate the target for the number of citations is too optimistic; we will most probably not reach this target. We already had a few invited talks.
Please note that we did not take into include the number of downloads of SOCCRATES deliverables, which was 387.

KPI	Target level	Current score
Publication downloads	100	0 (see remark above)
Citations during project	50+	1
Invited talks by consortium members	7	3

3.3.4 Presentations

Several presentations that addressed SOCRATES were provided at several events:

- Presentation MSS Managers, MSS department and employees (internal) by Martin Eian
- March 11th 2020 Presentation by Mnemonic to one of the vendors
- Mnemonic presented SOCCRATES to the Norwegian Defence Research Establishment
- Information about SOCCRATES was included in different internal presentation for security related audience as part of Vattenfall IT Security activities (10+)
- Shadowserver Updates and Highlights from Recent Activities, Piotr Kijewski, January 2020, included SOCCRATES overview from Shadowserver perspective
    - https://www.first.org/events/symposium/malaga2020/program#pThe-Shadowserver-Foundation-Updates-and-Highlights-From-Recent-Activities
- Foreseeti 2020-04-29 Tech Meetup Webinar - Including promotions in organic LinkedIn posts leading up to the webinar.
- Foreseeti 2020-03-13 Tech Meetup Webinar - Including promotions in organic LinkedIn posts leading up to the webinar.

3.4 Cooperation with other projects

3.4.1 EU H2020 projects

On initiative of the CyberSANE project, we co-organized a workshop (Joint Standardisation Workshop of Dynamic countering of cyber-attacks projects) with all 7 projects that are funded in the SU-ICT-01-2018 call on January 22nd 2021.

All projects were present and presented themselves in short presentations during the morning:

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

In the afternoon we discussed potential cooperation on disseminating results of the projects into standardisation bodies. This resulted in several ideas, that will be elaborated in the next months. It is very good to have close collaboration with these projects

We have made a liaison with SAPAN already in the beginning of the project. We have co-organized two workshops with them (ARES 2019 and ARES 2020) and planning for ARES 2021. Also we plan to organize joint webinars.

KPI	Target level	Current score
Liaisons with other EU projects	>2	1

3.4.2 Other projects

We have exchanged information with several other non -EU funded projects:

- KTH, H2020 Energy Shield
- KTH, National: Center for Cyber Defense and Information Security

- AIT, National funded project; MALORI
- TNO presented SOCCRATES at a COST Recodis meeting
- ATOS has introduced the SOCCRATES Security orchestrator to the Cybersec4eu project, which is also developing a orchestrator and shares with SOCCRATES similar approaches for the technologies selected.

This is really interesting for SOCCRATES and the other projects and strengthens the SOCCRATES relation network.
We currently do not have established a liaison with another non-EU project yet.

KPI	Target level	Current score
Exchange of information with other projects (including EU projects)	3	11
Liaison with other (non-EU) projects	>2	0

3.5 European Commission's Innovation Radar

Two of the SOCCRATES partners were informed that their SOCCRATES innovations had been analysed by the European Commission's Innovation Radar and will be published on the European Commission's Innovation Radar's platform Innovation Radar.

SOCCRATES partner Shadowserver:

- Innovation Title: Cyber Threat Identification by Automated Detection of Botnet Domain Names;
- Market Maturity of the Innovation: 'Exploring';
- Market Creation Potential of the innovation: addresses the needs of existing markets/existing customers;

SOCCRATES partner F-Secure:

- Innovation Title: A Platform to aid SOC & CSIRT Response to Attacks & Threats based on Attack Defence Graphs Evaluation Systems;
- Market Maturity of the Innovation: 'Exploring';
- Market Creation Potential of the innovation: addresses the needs of existing markets/existing customers;

This is a very honour full result.

3.6 SOCCRATES workshops

The project has successfully (co)organized two EU project workshops that are co-located with the ARES conference[1]. The workshop series, called NG-SOC[2], aims to bring together practitioners and researchers in the domain of SOC operations to discuss major challenges and research-driven solutions. The first workshop was organized by SOCCRATES. The second workshop was co-organized with members of the SAPPAN consortium. Now in its third year, the NG-SOC workshop will be held again alongside the ARES conference in August 2021 and co-organized with SAPPAN. In contrast to previous years, we plan to have a Call for Papers for the workshop and solicit contributions for peer review. We plan to form a Technical Programme Committee from experts in the projects that were funded

under the same call as SOCCRATES. The workshop continues to mature and gain visibility within the community; soliciting peer-reviewed publications is a step towards establishing the workshop as a respected forum for research contributions on SOC operations.
Previously, the NG-SOC workshops were attended by approximately 35 participants (excluding SOCCRATES and SAPPAN staff).

SOCCRATES workshop:

- August 26th 2019 - International Workshop on Next Generation Security Operations Centers (NG-SOC 2019) in conjunction with 14th International Conference on Availability, Reliability and Security (ARES 2019), University of Kent, Canterbury, UK

Agenda:

Session I *(Session Chair: Ewa Piatkowska)*	
The SOCCRATES Project: Motivation and Aims	*Reinder Wolthuis (TNO)*
ACT: Cyber Threat Intelligence Platform	*Siri Bromander (Mnemonic)*
Threat modelling and attack simulations with MAL and securiCAD	*Erik Ringdahl (Foreseeti)*
Automated Response based on securiCAD recommendations	*Frank Fransen (TNO)*
Session II *(Session Chair: Reinder Wolthuis)*	
Anomaly Detection (DNS Ninja & ABC tool)	*Irina Chiscop (TNO)*
Adversarial Machine Learning	*Ewa Piatkowska (AIT)*
Open Discussion: Future Challenges for SOCs	*Moderator: Paul Smith (AIT)*
Conclusions and Wrap Up	*Reinder Wolthuis (TNO)*

Co-hosted workshop:

- August 25th 2020, International Workshop on Next Generation Security Operations Centers (NG-SOC 2020) in conjunction with 15th International Conference on Availability, Reliability and Security (ARES 2019), video conference

Agenda:
Session 1 (Ewa Piatkowska)

- Welcome Ewa Piatkowska
- The SOCCRATES Project: Overview and Objectives Frank Fransen (TNO)
- The SAPPAN Project: Overview and Objectives Avikarsha Mandal (Fraunhofer FIT)
- Keynote: Semi-Automated Cyber Threat Intelligence (ACT) Martin Eian (Mnemonic)

Session 2 (Tomas Jirsik)

- Monitoring Malicious Infrastructures to Produce Threat Intelligence Piotr Kijewski (Shadowserver)
- Pipeline development for Automatically Generated Domain detection Irina Chiscop (TNO)
- Leveraging Machine Learning for DGA Detection Arthur Drichel (RWTH Aachen University)
- Knowledge Management and Anonymization Techniques in Cyber-Threat Intelligence Lasse Nitz, Mehdi Akbari Gurabi (Fraunhofer FIT)

- Reputation Management Techniques for IP addresses, domains, and mail Mischa Obrecht (DreamLab)

Session 3 (Avikarsha Mandal)

- Host and Application Behaviour Modelling Tomas Jirsik (Masaryk University) and Sebastian Schaefer (RWTH Aachen University)
- L-ADS: Live Anomaly Detection System Alejandro Garcia Bedoya (ATOS)
- Adversarial Examples against Intrusion Detection Systems Ewa Piatkowska (AIT)
- Fast and Scalable Cybersecurity Data Processing Josef Niedermeier, Gabriela Aumayr (HPE)

Session 4 (Irina Chiscop)

- Attack Analysis with Attack Defence Graphs Erik Ringdahl (Foreseeti)
- Attack Graph-based Courses of Action for Defense Wojciech Widel (KTH)
- Visual Analytics for Cyber Security Data Christoph Müller and Franziska Becker (University of Stuttgart)
- Endpoint Protection Paolo Palumbo (FSecure)

Panel Session

- Discussion on Future Challenges for SOC Speakers: Pavel Kacha (CESNET) Sarka Pekarova (DreamLab) Paul Smith (AIT) Panel chair: Tomas Jirsik (Masaryk University)

Wrap up Ewa Piatkowska (AIT)

We have organized quite a number of webinars and we are hoping to organize on or two face-to-face workshops in the second half of the project, which will be focused on presenting results and discussing exploitation potential.

Measurable outcome:

KPI	Target level	Current score
Number of workshops	>2	1
Number of workshop attendees	20-30	25
Co-hosted workshops	2	1
Attendees at co-hosted workshops	30-50	35

3.7 SOCCRATES website

The SOCCRATES website (www.SOCCRATES.eu) is the general communication channel for SOCCRATES. the frontpage of the website is sown in Figure 2. 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 continuously is refreshed with actual information.

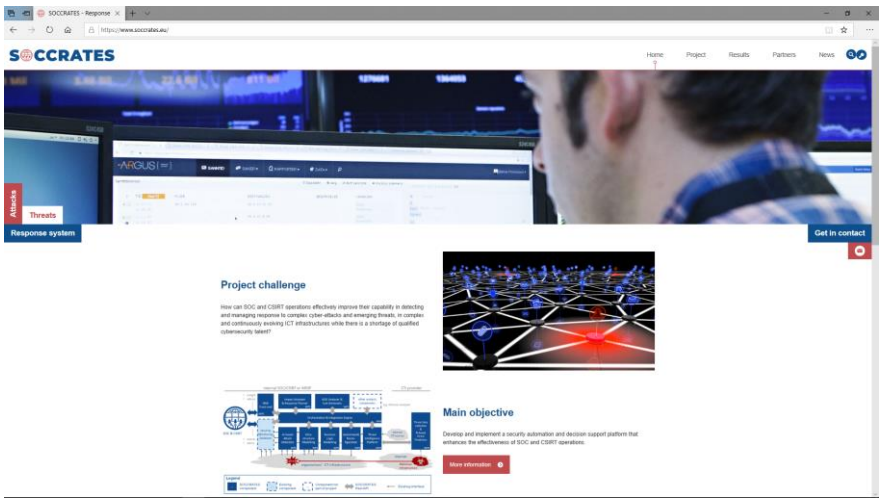

Figure 2 – front page of the SOCCRATES website

We also implemented a closed website part that is only accessible for members of the SOCAB and the stakeholder group and was intended to share specific information with them and discuss with them. But this closed part did not seem to fulfil a need, because most of the SOCCRATES information already is public and we have many other ways to interact with our Advisory Board and Stakeholder group (meetings, LinkedIn, Twitter). So we decided not to use the closed part of the website.

KPI	Target level	Current score
Blog posts (news)	15	13
Yearly visits to the closed part of the website	>100	100
Views/accesses of the website during the project lifetime	>3000	14648
Unique visitors to SOCCRATES website per month in the last year of the project	>100	N/A

This last KPI concerns the last year of the project. During the period January 1st 2020 – February 23rd 2021 we measured 3674 unique visits to the SOCCRATES website, which is an average of 262 per month.

3.8 Social media

Although the original SOCCRATES plan was to focus our social media efforts on LinkedIn, we have decided also to use a Twitter account.

The twitter account (@soccrates_eu) was set up in January 2021 (https://twitter.com/soccrates_eu). Project related tweets are planned to start in February. The decision to establish a Twitter presence was made as it is a popular medium in the cybersecurity area, with a lot of other EU funded projects also active in this space.

SOCCRATES has implemented a LinkedIn group (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.
We did not frequently use the LinkedIn group yet, but intend to do so in the second half of the project.

SOCCRATES partner Shadowserver had 3 social media announcements in the First Reporting Period (through its own Twitter and LinkedIn accounts):

- https://www.linkedin.com/posts/piotrkijewski_soccrates-improving-detection-and-response-activity-6647890737352495104-b-vb
  https://twitter.com/Shadowserver/status/1242024668745338881
- https://www.linkedin.com/feed/update/urn:li:activity:6647802905724272640/

Also SOCCRATES partner foreseeti had several posts on LinkeIn, mostly addressing the webinars

- 2020-12-01 LinkedIn post https://www.linkedin.com/feed/update/urn:li:activity:6739445193575018496
- 2020-11-27 LinkedIn post https://www.linkedin.com/feed/update/urn:li:activity:6738042015818252289

KPI	Target level	Current score
Posts made by SOCCRATES project members	>100	8
Membership of SOCCRATES target groups	>30	38
Active participation of members (e.g. posts, comments)	>100	0

3.9 SOCCRATES webinars

SOCCRATES has organized three webinars, featuring different innovation topics and all combining presentations and demonstrations. We still have two webinars planned in the first series. After that, we will organize a new series of webinars that will focus more on results and pilot evaluation. Participants can register on the SOCCRATES website (see also picture below) and the webinars are also advertised on several partner websites and channels, e.g. foreseeti:

- 2020-11-25 – 2020-12-01 InMail to 10300 people on LinkedIn.
- 2020-11-25 Promotion pop-up on the foreseeti web
- Sign-up and landing page on the foreseeti home page: https://foreseeti.com/webinar-december-2020/
- 2020-11-24 email campaign to 2967 foreseeti contacts

The webinars are well visited, although we noted that on average, only one third of the registered people actually attends the webinar. This is also why we record the webinar and put the recordings on the SOCCRATES website.
As mentioned in chapter 2, webinars are an important means to reach out to our stakeholders in times of restrictions due to the pandemic. This is why we purchased 15 professional quality (USB)

microphones that improved the sound quality and consequently the overall quality and attractiveness of virtual events. Also we have purchased a CISCO webex events license, to be able to organize virtual events in a professional manner.

Measurable outcome:

KPI	Target level	Current score
Number of webinars held	>5	3
Number of participants per webinar	>15	29

3.10 Promotional give-aways

The SOCCRATES Project has been running since September 2019 and has in many respects been effected by its visibility through Covid-19. We would like to be in contact with interested parties and in the same time create visibility. Therefore we decided to make facemasks. In times like these we all need to wear a facemask and with these facemasks, the project becomes visible.

3.11 SOCCRATES Video

To be able to provide interested parties a short introduction to the SOCCRATES project, we have released of our first animated video at the end of May 2020. This video provides an introduction of SOCCRATES and can be seen on our website (see 'news' and 'results') and also here: https://vimeo.com/423498497

There are is a version with subtitles (https://vimeo.com/442734821).

The coming year we plan to release another video, which will more be focused on SOCCRATES results.

Measurable outcome:

KPI	Target level	Current score
Informative and educational videos	3-6	1
Number of video views	>50	270

3.12 SOCCRATES pilots

The first pilot has started, but this is a technical pilot. We will refer to it in dissemination activities, provide demonstrations of this intermediate result, and evaluate and learn from this first pilot. However, the real dissemination power will come from the second pilot and its evaluation and the demo pilot that is planned at the end of the project.

3.13 SOCCRATES demonstrations

We have provided many demonstrations until now, but not of the complete SOCCRATES platform. Demonstrations consisted of individual modules and we provided them in webinars, to our advisory board, to our stakeholder group and in external presentations. So the KPI as shown in the table below still is scored at zero, we expect we can easily reach the targets value once the complete SOCCRATEs solution is ready.

Measurable outcome:

KPI	Target level	Current score
Demonstrate SOCCRATES platform at cyber security related events	>5	0

3.14 Conferences

We have submitted papers to several conferences

Workshop paper GraMSec 2020

- KTH: An Attack simulation language for the IT domain; S. Katsikeas, S. Hacks, P. Johnson, M. Ekstedt, R. Lagerström, J Jacobsson, International Workshop on Graphical Models for Security, 67 -86, June 2020

International IFIP Cross Domain (CD) Conference for Machine Learning & Knowledge Extraction (MAKE) 2020

- Martin Teuffenbach, Ewa Piatkowska, Paul Smith: "Subverting Network Intrusion Detection: Crafting Adversarial Examples Accounting for Domain-Specific Constraints," International IFIP Cross Domain (CD) Conference for Machine Learning & Knowledge Extraction (MAKE) 2020, Online Event, pp. 301-320, 2020.
  CD-MAKE paper has been downloaded 506 times, according to Springer

Measurable outcome:

KPI	Target level	Current score
Number of scientific publications: conference papers accepted	10-20	2

3.15 Journals and magazines

KTH has submitted two papers to journals, but they are still under review. We expect to submit more papers to journals in the second half of the project.

Measurable outcome:

KPI	Target level	Current score
Number of scientific publications: journals	3	0 (2 submitted)

3.16 Standardization

Discussion with standardization bodies has been limited until now. As previously mentioned, we try to join forces on this subject with a number of other H2020 projects; we had a joint workshop featuring exactly this subject and we have follow-up actions form this workshop. Also we have discussions with a few members of our advisory board that potentially could support us in this area. We expect to have more success in the second half of the project.

KPI	Target level	Current score
Contributions to policy and standards, e.g. citations of SOCCRATES results	2	0
New relationships with appropriate bodies	2	0
References to results in policy	2	0
Position papers (e.g. to ECSO WG6 (research) or WG5 (education)	3	0

4 First exploitation ideas

4.1 Overall perspective

Overall, SOCCRATES is very well on its way to successful exploitation of results. Not only do we have the different target groups for exploitation in our consortium (End users, a threat intel provider, vendors, research companies, universities) but we also have built a strong community around SOCCRATES, with our advisory board, stakeholder group and visitors of events that will make successful exploitation much easier.

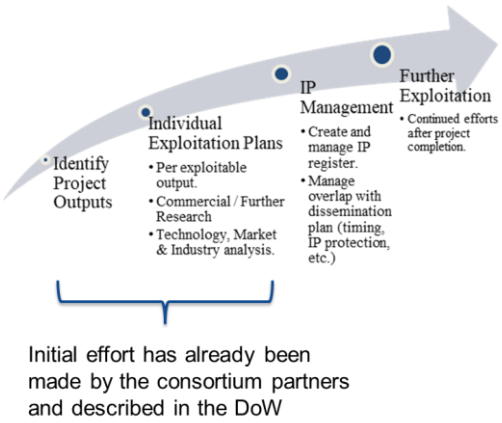

Figure 3 Phases for development of SOCCRATES exploitation pathways

As already mentioned in the DoW, we do not anticipate the full platform to be exploited as a single commercial product. We rather focus exploitation efforts on individual modules, knowledge, training and bringing results towards standardization bodies. We will briefly go through the initial ideas in several of these areas. More detailed plans will be developed in the second half of the project and result in exploitation plans for each partner.

Next steps:

- Organize dedicated meeting(s) on exploitation activities, considering joint output from the project (e.g. community contributions);
- Partners will start to refine their own individual exploitation plans as defined in the DoW. These will be discussed and elaborated in the exploitation meetings;
- We will explore exploitation potential with our SOCAB and Stakeholder Group (already subject of discussion in the second stakeholder group meeting) and involve them in setting the direction for exploitation. At the time of writing, we have had initial discussions with the Stakeholder Group, who provided useful feedback and suggestions to the consortium. In many ways they confirmed our strategy, e.g. regarding exploitation of modules rather than the complete platform.

4.2 Commercial exploitation

Commercial exploitation will most probably only be done by individual partners on a module basis. With the SOCCRATES innovation results, individual partners will be able to enhance their existing products and consequently improve commercial exploitation of those products. An interesting point that was raised by the Stakeholder Group members related to the modularity of the SOCCRATES components, which has a bearing on their commercial exploitation. It was noted by participants that SOAR tools are rarely deployed in a “green field” setting but rather solutions are integrated into

existing “legacy” solutions. With this in mind, we will investigate the most appropriate solutions to conduct this form of integration. To this end, we will continue to pay close attention and attempt to align with initiatives such as The Hive Project. For example, we use Cortex to support automation, in a similar manner to the approach proposed by Hive.

4.3 Open Source strategy

We are in the process of assessing whether individual modules are suitable to publish as open source. We already have a list of all modules and adaptors that will be developed in SOCCRATES and discuss with the responsible partners the open source potential. In some cases, the basis on which we do innovation already is open source (ACT from mnemonic), in other cases this still needs to be discussed.

We currently think we will not start a SOCCRATES open source community. If modules are put open source, this will be included in already existing open source communities of partners. We will refer to these from the SOCCRATEs website.

4.4 Education and training

We still plan to stick to the original ideas on training and education as stated in the DoW. We will explore these ideas in more detail in the Exploitation Plan.

4.5 Standardization

As noted above, our efforts towards submitting results to standardization efforts are at an early stage. To build on our initial efforts, we have joined forces with other H2020 projects and we anticipate that this will strengthen the visibility towards standardisation bodies. Furthermore, as suggested by out Stakeholder Group, we will reach out to communities associated with the MITRE ATT&CK Framework and FIRST[3]. We have good connections to these communities within the consortium. Moreover, we will investigate alignment of SOCCRATES with existing standardisation activities for SOC operations.

[3] https://www.first.org/

5 Plans for coming period

This section describes (on a high level) SOCCRATES dissemination activities in the second half of the project. These activities can be divided in two 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)

5.1 Ongoing dissemination activities

A number of dissemination activities are ongoing activities and are listed in

Table 1 below.

Table 1 - 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
Schedule regular stakeholder group meetings and Advisory Board meetings	TNO
Maintaining the LinkedIn account	TNO
Maintaining the Twitter account	SHS + all partners
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

5.2 Planned dissemination activities

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

Table 2 – planned dissemination activities

Dissemination activity	Planned date	Responsible partners
Organize workshop at ARES event (submitted papers)	August 2021	AIT + TNO in cooperation with SAPPAN
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
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
Submit papers for: • IEEE Symposium on Security and Privacy • IEEE/IFIP International Conference on Dependable Systems and Networks	Q4, 2021	All partners
Short video to highlight the results of SOCCRATES	Q2, 2021	TNO
SOCCRATES workshop/event	Q3, 2021	TNO
SOCCRATES workshop/event	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
Short video to highlight final results	Q2, 2022	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, 2022	All partners
Publication of SOCCRATES White paper (D8.4)	Q2, 2022	TNO
SOCCRATES final workshop	Q2, 2022	TNO
Organize workshop at ARES event 2022	Q3, 2022	AIT

Organize workshop at ARES event 2022	Q3, 2022	AIT, TNO
Publishing SOCCRATES exploitation plans	Q3 2022	All partners

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 3 – 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

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

References

[D8.2] SOCCRATES Dissemination Plan, version 1.0, December 3rd 2019, Reinder Wolthuis (editor)

Annex: Overview of current KPI scores

KPI	Target level	Current score	Details
Number of SOCAB meetings	3	3	• May 26th 2020 • September 15th 2020 • December 15th 2020
SOCAB Attendance on SOCCRATES organized workshops	1	0	
Number SOC/CSIRT operators in stakeholder group	>10	8	• Amadeus, • KPN, • CZ, • RDW, • Telenor, • Proximus, • NRD, • Defendable
Number of MSSP's in stakeholder group	>10	8	• KPN, • Amadeus, • Telenor, • Proximus, • Ordina, • Thales, • NRD, • Defendable
Number of National CERTs in stakeholder group	>2	3	• Latvian National CERT, • Polish National Cert, • Norwegian Energy Sector Cert
Number of end users in stakeholder group	>10	6	• CZ • ONVZ • RDW • Europol • Stockholm count council • Skanska
Number of vendors in stakeholder group	>5	4	• Amadeus IT Group, • Thales, • Vairav technology, • Crowdstrike
Stakeholder group members attendance on SOCCRATES organized workshops	>6	2	
Number of MSSPs contacted about SOCCRATES	>25	10	• Cparta Cyber Defense (KTH) • Telenor (TNO) • Proximus (TNO) • Swisscom (TNO) • KPN (TNO) • Amadeus IT group (IMT) • Ordina (TNO) • Thales (IMT)

			• NRD ((SECO) • Defendable (TNO)
Number of national CERTs contacted about SOCCRATES	>5	6	• NCSC (NL) (TNO) • CERT Polska (PL) (SHS) • CERT.LV (LV) (SHS) • GOVCERT.LU (LU) (SHS) • CIRCL (LU) (SHS) • EC DIGIT CSIRC (CSIRT for EC) (SHS)
Number of vendors contacted about SOCCRATES	>10	4	• Crowdstrike (TNO) • Amadeus IT Group (IMT) • Thales (IMT) • Vairav technology (TNO)
Number of end users contacted about SOCCRATES	>25	14	• Swedbank (KTH) • Swedish defense (KTH) • Uniper (energy company) (KTH) • Stockholm public transport (KTH) • Stockholm County Council (KTH) • Klarna (bank) (FRS) • Swedavia (airports) (FRS) • ONVZ (health insurance) (TNO) • RDW (Vehicle admission) (TNO) • ING (bank) (TNO) • Rabobank (bank) (TNO) • ABN AMRO (bank) (TNO) • Achmea (insurance company (TNO) • Volksbank (bank) (TNO)
Participation at industry bodies 'events	6	5	• Ericsson, Internal Network Security, Seminar, SOCCRATES presented by Shadow server, September 22nd • ATOS has introduced the SOCCRATES project to the ATOS DigitalShow, an event organized every year within the ATOS community, where the main advancements on research are presented to the different ATOS worldwide offices • TNO Cyber Security Marktdag; SOCCRATES presented by Frank Fransen • SOC Automation 1.1, SOCCRATES presented (Frank Fransen, Erik Ringdahl), August 26th 2020 • Connect2Trust Presented SOCCRATES, September 3rd 2020 (Reinder Wolthuis)
Publication downloads	100	0	We did not include the number of downloads of deliverables, which was 387.
Citations during project	50+	1	
Invited talks by consortium members	7	3	• Invited talk to Graduate School of TU Delft in December 2020 Paul Smith and Frank Fransen, "Machine learning and Critical Infrastructure Security and Resilience: is data always king? • Mathias Ekstedt was invited to give a talk to Prof. Heiko Mantel's Research Group at TU Darmstadt. • Shadowserver presented SOCCRATES at the FIRST TC Malaga 2020, https://www.first.org/events/symposium/malaga2020/program#pThe-Shadowserver-

			Foundation-Updates-and-Highlights-From-Recent-Activities.
Liaisons with other EU projects	>2	1	• SAPPAN
Exchange of information with other projects	3	11	• GUARD (TNO, AIT) • CyberSANE (TNO, AIT) • C4IioT (TNO, AIT) • SAPPAN (TNO, AIT) • SIMARGL (TNO, AIT) • nIoVe (TNO, AIT) • H2020 Energy Shield (KTH) • National: Center for Cyber Defense and Information Security (KTH) • National funded project; MALORI (AIT) • COST Recodis (TNO) • Cybersec4eu project (ATOS)
Liaison with other (non-EU) projects	>2	0	
Number of workshops	>2	1	• August 26th 2019 - International Workshop on Next Generation Security Operations Centers (NG-SOC 2019) in conjunction with 14th International Conference on Availability, Reliability and Security (ARES 2019), University of Kent, Canterbury, UK
Number of workshop attendees	20-30	25	
Co-hosted workshops	2	1	• August 25th 2020, International Workshop on Next Generation Security Operations Centers (NG-SOC 2020) in conjunction with 15th International Conference on Availability, Reliability and Security (ARES 2020), video conference
Attendees at co-hosted workshops	30-50	35	
Blog posts	15	13	
Yearly visits to the closed part of the website	>100	100	
Views/accesses of the website during the project lifetime	>3000	14648	
Unique visitors to SOCCRATES website per month in the last year of the project	>100	N/A	This KPI concerns the last year of the project. During the period January 1st 2020 – February 23rd 2021 we measured 3674 unique visits to the SOCCRATES website, which is an average of 262 per month.
Posts made by SOCCRATES project members	>100	8	
Membership of SOCCRATES target groups	>30	38	
Active participation of members (e.g. posts, comments)	>100	0	

Number of webinars held	>5	3	
Number of participants per webinar	>15	29	
Informative and educational videos	3-6	1	https://vimeo.com/423498497 (without subtitles) https://vimeo.com/442734821 (with subtitles
Number of video views	>50	270	
Demonstrate SOCCRATES platform at cyber security related events	>5	0	
Number of scientific publications: conference papers accepted	10-20	2	
Number of scientific publications: journals	3	0	2 submitted
Contributions to policy and standards, e.g. citations of SOCCRATES results	2	0	
New relationships with appropriate bodies	2	0	
References to results in policy	2	0	
Position papers (e.g. to ECSO WG6 (research) or WG5 (education)	3	0	