SOCCRATES

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

D8.5

Final Dissemination report

Deliverable type:	Report
Contributing work packages:	WP8 Dissemination
Due date of deliverable:	31/10/2022
Submission date:	31/10/2022
Dissemination level:	PU

Responsible organisation:	TNO
Editors:	Marije Berding, Reinder Wolthuis, Lenny Zilverberg
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) Lenny Zilverberg (TNO) Marije Berding (TNO) Paul Smith (AIT) Frank Fransen (TNO) Piotr Kijewski (SHS) Mathias Ekstedt (KTH) Siri Bromander (MNM) Susana Gonzalez Zarzosa (ATOS) Christophe Kiennert (IMT) Maciej Kosz (VTF) Malgorzata Gren (VTF) Erik Ringdahl (FRS) Ville Alkkiomäki (WSC)

Reviewer(s)	Martin Eian (mnemonic, content) Aljosa Pasic (Atos, Security review)

Security Assessment	
Approval Date	October 28th 2022
Remarks	-

TABLE OF CONTENTS

1 INTRODUCTION 4
1.1 The SOCCRATES project 4
1.2 This deliverable 5
1.3 Structure of this deliverable 5
2 OVERALL DISSEMINATION RESULTS 6
2.1 Progress on dissemination objectives 6
2.2 Clustering of results for dissemination and communication purposes 7
2.3 Influence of the Pandemic on dissemination 7
2.4 Target groups that were reached 8
2.5 Sensitive information 8
3 DISSEMINATION ACTIVITIES AND RESULTS 9
3.1 SOCCRATES Advisory Board (SOCAB) 9
3.2 SOCCRATES stakeholder group 10
3.3 Other stakeholders 11
3.3.1 MSSPs, National CERTs, Vendors, End users 11
3.3.2 Participation at industry bodies' events 12
3.3.3 Security research community: 12
3.3.4 Vision Paper 13
3.3.5 Presentations 13
3.4 Cooperation with other projects 14
3.4.1 EU H2020 projects 14
3.4.2 Other projects 15
3.5 European Commission's Innovation Radar 15
3.6 SOCCRATES workshops 16
3.7 SOCCRATES website 20
3.8 Social media 21
3.9 SOCCRATES webinars 22
3.10 Promotional give-aways 23
3.11 SOCCRATES Video 24
3.12 SOCCRATES pilots 24
3.13 SOCCRATES demonstrations 24
3.14 Conferences 25
3.15 Journals and magazines 26
3.16 SOCCRATES final event 27
3.17 Standardization 28
4 CONCLUSION 29
ABBREVIATIONS 30
REFERENCES 32
ANNEX: OVERVIEW OF CURRENT KPI SCORES 33

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.

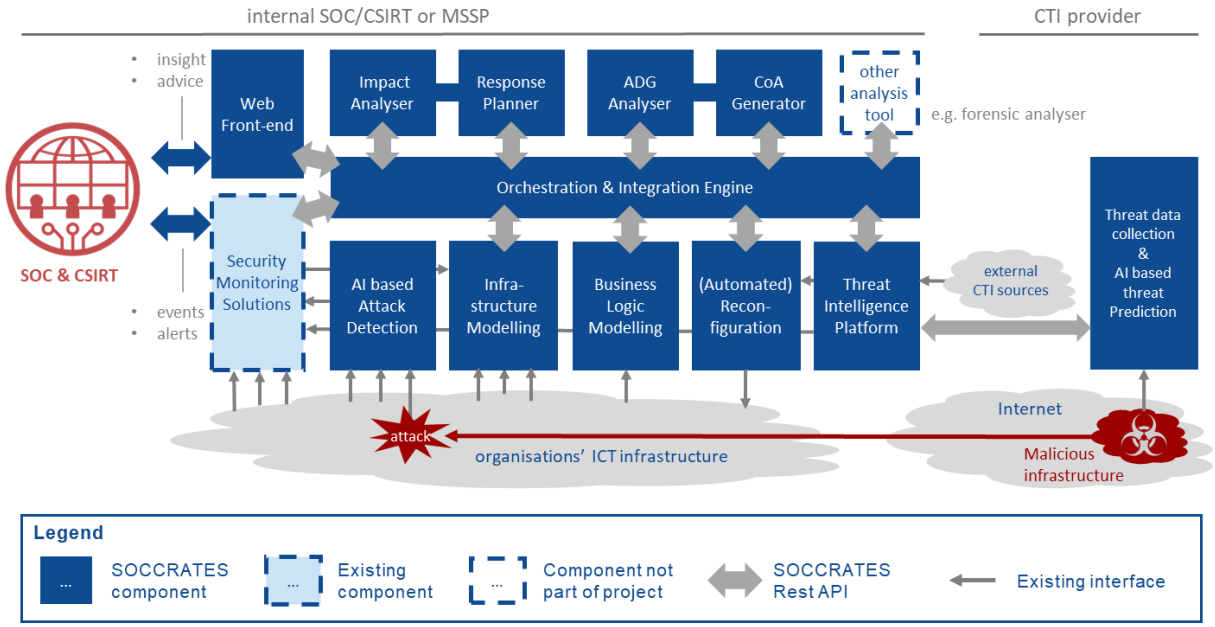


Figure 1 – The SOCCRATES platform

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 final report on dissemination activities. It includes all dissemination results, including the results that were reported in the First Dissemination Report [D8.3]. We report on the dissemination KPI's as defined in the SOCCRATES Dissemination Plan [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. Finally, the annex provides an overview of KPI levels that were achieved and some details on how we achieved these levels.

2 Overall dissemination results

2.1 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. We also had some discussions to policy makers and regulatory bodies, but it has been rather limited.
- *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 contains the SOCCRATES (high level) results and experiences in an easy accessible way, suitable for policy makers and higher management of stakeholders. It will be available on-line. It is more or less a management summary of D2.4 (Vision paper) and D7.2 (pilot evaluation) complemented with some high level experiences from D7.3 (best practices guide). Main target audience: policy makers and (higher) management of organizations that have an operational SOC or intend to build a SOC.
- *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 and podcasts See chapter 3.
- *To identify and execute opportunities for contributions to standards based on SOCCRATES results.* At least three initiatives have led to (industry) standardization results:
  - TNO became member of OASIS Open - TC openC2 and TC CACAO and shared information from the SOCCRATES project to the group.
  - The project coordinator was appointed as a member of the Enisa adhoc working group on SOC/CSIRT and also as a rapporteur for the task force CTI sharing taxonomies. This input to this working group is based for a large part on results of the SOCCRATES project.
  - SOCCRATES results on the Adversary Emulation Planner are adopted by MITRE and included in the ATT&CK framework. SOCCCRATES is listed as a contributor.[1]

  We also organized a joint workshop with a number of EU projects (CyberSane, Guard, SAPPAN, SIMARGL, C4IIoT, CARAMEL) in February 2022 with the focus of looking for opportunities to provide input to standardization bodies collaboratively. Although the workshop itself was very useful in exchanging knowledge, identifying potential standardization groups to target and getting to know each other, it did not lead to concrete ideas for collaborative input to standardization bodies.
- *To develop and implement an interactive and user-friendly website 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 have kept it up-to-date with all our results and deliverables and also added new pages where relevant (e.g. the platform software). It was very well visited. We maintain the website up to 5 years after 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.* In our First dissemination report

[1] https://attack.mitre.org/techniques/T1588/002/ and https://attack.mitre.org/resources/contribute/

we've explored ideas on exploitation. During the project we have expanded these ideas, which resulted in an Exploitation Plan (D8.6, SOCCRATES Exploitation plan).

2.2 Clustering of results for dissemination and communication purposes

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*;
  - The first technical pilot was limited to evaluating a number of SOCCRATES modules, and ran between January and April 2021.
  - The second pilot was intended to run between February and May 2022. We suffered delays here and in the end the pilot was only partially successful.
  - To gather more results, we have organized an evaluation session with analysts from VTF and MNM, using the SOCCRATES demonstrator.
  - For more details, see paragraph 3.12 and D7.2: Pilot application and evaluations

- *Guidance on the use of these technologies by SOCs and CSIRTs, highlighting their potential benefits;* We have presented the technologies that SOCCRATES has developed and its benefits in many events, papers, articles and webinars (in which also many SOC and CSIRT representatives participated) as described in this final report. We also had intense discussions about this with our SOCAB and stakeholders. One important deliverable in this respect is the vision paper, that we turned into a nice and easy to read document that we also published in a printed version.
- *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, the final event, conferences we presented, our webinar series, podcasts, social media updates, blog posts, and 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.* The SHS SOCCRATES API is a set of methods that enable fetching of the results of the work of the DGA Detective and the malicious domain hunting platform on SHS sandbox data. These methods are accessible to SOCCRATES project partners and external trusted users (such as National CSIRTs). API results can be used for domain reputation, detection of malicious domains and for TIP enrichment. The API is described in detail in D2.3 and D4.3.

2.3 Influence of the Pandemic on dissemination

The COVID-19 pandemic 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 actually 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. This package did not meet our needs, so we successfully implemented WebinarGeek later in the project;

- 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.
After the pandemic, when it was once again possible to meet face to face, we held live activities whenever possible, for example;

- A workshop at the ARES conference 2022 in Vienna
- A presentation at the FIRST conference 2022 in Dublin
- A presentation at the FIC 2022 in Lille
- A 'deep dive' during the One Conference 2022 in The Hague
- The SOCCRATES final event in Luxembourg

In addition to these live activities, we made full use of all digital dissemination and communication opportunities, for example;

- Maintaining social media channels with a growing number of followers (October 2022, 260 followers on LinkedIn).
- Organising online webinars
- Organising online workshops, in collaboration with other (H2020) projects
- Releasing podcasts
- Publishing blog posts
- Maintaining the SOCCRATES website
- Maintaining the cyberwatching.eu website (SOCCRATES pages)

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.
We have had contact with Mitre ATT&CK, OASIS and ENISA and also contributed to these (see above). Overall, the contacts with regulatory bodies and policy makers 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 during the project. There were a few exceptions:

- The SOCCRATES white paper was planned to be published on February 28th 2022, but is published at the end of the project because we wanted to include the pilot experiences. On top of that we decided to give additional attention to deliverable D2.4, the SOCCRATES vision paper. We published the SOCCRATES vision paper as an attractive printed (and online) booklet. We distributed 500 copies of the booklet. The vision paper was very well received. It was downloaded from the website about 70 times.
- There was no reason to publish a SOCCRATES press release

We have defined several Dissemination KPIs. 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 is:

- Andy de Petter, Head of Global SOC, Exclusive Networks, (former) Head of cyber security intelligence & incident response, Proximus (BE)
- Frode Hommedal, CEO Amplio Group AS (NO)
- Dr. Judith E.Y. Rossebo, specialist cyber security & infrastructure - ABB (NO)
- Martin Pekarek, Cybersecurity advisor Dutch National Cyber Security Center (NL)

During the project we have organised 7 SOCAB meetings, three in 2020 (May 26th, September 15th, December 15th 2020). In 2021 two meetings (May 26th 2021, September 14th 2021,) and in 2022 also two meetings (January 25th 2022 and May 23rd 2022). During every meeting at least two SOCAB 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 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.
Judith Rossebo attended the final event in Luxembourg. Andy de Petter was unable to attend at the last minute.

Measurable outcome:

KPI	Target level	Current score
Number of SOCAB meetings	3	7
SOCAB Attendance on SOCCRATES organized workshops	1	1

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 is also 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.

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	Noorderpoort College	NL
Jan Willem Spee	CISO	RDW	NL
John Post	Program director	Topsector energie	NL
Ulrich Seldeslachts	CEO	LSEC	BE
Wim Stoffelen	*Manager*	*LSEC*	*NL*
Dr.-Ing. Peter Amthor	Postdoctoral Researcher	Technische Universität Ilmenau	DE
Vesna Lucassi	Chief Information security officer SLL	Stockholm County Council (SLL)	SE
Tale Sundlisæter	Security Analyst	Telenor	NO
Simen Linderud	Security Analyst	Telenor	NO
Lieven de Smaele and Rajendra Mekhale	Senior Manager IT Security	Proximus	BE
Ronald Pool	Cyber Security Specialist	Crowdstrike	NL
Wim Stoffelen	Director partnerships and alliances	SECO-Institute	NL
Erik Post	Senior Consultant Cyber Security	Cyber Security Challeges	NL
Jacob Henricson	CISO	Skanska Sweden	SE
Bijay Limbu Senihang	Chief Technology Officer	Vairav Technology	NP
Dr. Vilius Benetis	Director	NRD Cyber Security	IT
Olivier BETTAN	Head of Cybersecurity Lab	Thales SIX GTS FRANCE	FR
Johan von Konow	Cparta Cyber Defense	CTO	SE
Lars Erik Smevold	Security Analyst	Nowegian Enegy Sector and Control System CERT	NO
Alexandre Dulaunoy	Security Researcher	Response Center Lux(CIRCL)	LU
Pawel Pawlinski	Security Analyst	CERT PL -Pollish National CERT	PL
Markus Riegler	Head of Managed Defense	IKARUS	AT
Armins Palms	Cyber Security Incident Handler	CERT LV- Lavian National Cert	LV
Tim Ruhl	CTO	Sightlabs	NL
Aaron Kaplan	Security Analyst		
Ondrej Nekovar and Jan Pohl	CISO/Sec. Analyst	SPCSS Czech Republic	CZ
David Olgart	Coordinator for Cyber Defense	Swedish Amred Forces HQ	SE
Chris Few	Strategic Risk Specialist	National Grid	UK
Roger Cato Bergheim Johnson	Security Analyst	Defendable	NO

At the end of the period we have 36 members of 30 different organisations. There have been 4 stakeholder meetings, namely September 28th 2020 (15 stakeholders present) and February 16th 2021 (15 stakeholders present), September 21th 2021 (30 stakeholders present) and March 15th 2022 (25 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 Planner and reserved one hour for interactive discussion that was guided by questions we prepared. In the third meeting we demonstrated the Business Impact Analyser and presented the pilot set-up and evaluation plans. In the fourth meeting we presented the initial pilot evaluation results and discussed the demonstrator. An important topic was also to discuss the expectations on SOCCRATES Exploitation. Using a mentimeter questionnaire, we were able to gather valuable insights on this topic.

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). We are especially satisfied with the number of national CERTs, which we could reach through the excellent network of our partner Shadowserver.
In some cases 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).
During the period, we continued our efforts to expand the stakeholder group to include the various organisational profiles, which led to a continuing expansion of the group. To this end, we approached contacts with personal invitations and produced an informative leaflet with information for prospective members.
Ten stakeholder group members joined the final event in Luxembourg.

KPI	Target level	Current score
Number SOC/CSIRT operators in stakeholder group	>10	8
Number of MSSP's in stakeholder group	>10	9
Number of National CERTs in stakeholder group	>2	4
Number of end users in stakeholder group	>10	8
Number of vendors in stakeholder group	>5	4
Stakeholder group members attendance on SOCCRATES organized workshops	>6	14

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	25
Number of national CERTs contacted about SOCCRATES	>5	6
Number of vendors contacted about SOCCRATES	>10	10
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. Details can be found in the annex.

KPI	Target level	Current score
Participation at industry bodies 'events	6	7

3.3.3 Security research community:

We have defined three KPIs to measure the interest in the security research community, see the table below. During the project, we have successfully submitted 5 papers, which increased the number of citations. 3 more papers will be submitted in the coming period. Therefore the total number of citations will probably increase. We had several invited talks.

KPI	Target level	Current score
Publication downloads	100	*
Citations during project	50+	35**
Invited talks by consortium members	7	4

* *Please note that the number of downloads of our scientific publications is unfortunately untraceable. The number of downloads of SOCCRATES deliverables on the website was over 500.*

**

Paper	Number of citations
Subverting Network Intrusion Detection: Crafting Adversarial Examples Accounting for Domain-Specific Constraints *M Teuffenbach, E Piatkowska, P Smith*	5
Mapping Cyber Threat Intelligence to Probabilistic Attack Graphs *A Gylling, M Ekstedt, Z Afzal, P Eliasson*	3
An attack simulation language for the IT domain *S Katsikeas, S Hacks, P Johnson, M Ekstedt, R Lagerström, J Jacobsson, M. Wällstedt, P. Eliasson.*	27
Security Countermeasures Selection Using the Meta Attack Language and Probabilistic Attack Graphs	0 (This paper has just recently been published in 2022)

WOJCIECH WIDEŁ , PREETAM MUKHERJEE , AND MATHIAS EKSTEDT AI-based Detection of DNS Misuse for Network Security *I Chiscop, F. Soro, P Smith*	0 (This paper has just recently been accepted)

3.3.4 Vision Paper

On top of the SOCCRATES white paper we decided to give additional attention to deliverable D2.4, the SOCCRATES vision paper. We published the SOCCRATES vision paper as an attractive printed (and online) booklet in May 2022. We distributed 500 copies of the booklet. The vision paper was very well received. It was downloaded from the website about 70 times.

The SOCCRATES Vision Paper provides a vision and concrete next steps on innovative security automation and answers questions such as 'Why should we invest in automated security and how do you start?', 'What does the Next Generation SOC looks like?' and 'How can we integrate automation into our way of working?'.
You can download the Vision Paper here

Cover of the SOCCRATES vision paper

3.3.5 Presentations

Several presentations that addressed SOCCRATES were provided at several events, for example:

- 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.

- Mnemonic (Martin Eian) presented SOCCRATES at the ONE Conference 2021.
- TNO provided a 'Deep dive' into SOCCRATES at the ONE Conference 2022.
- TNO gave a pitch at the FIC exhibition 2022 in Lille at the EU area. We also presented the SOCCRATES vision paper at this event, which was very well received.
- mnemonic (Martin Eian) presented a SOCCRATES related topics at the FIRST Conferences '21 and '22.
- Erik Ringdahl (foreseeti) and Frank Fransen (TNO) presented a session at the FIRST Conference '21: 'Attack Defense Graph Analysis for Supporting SOC and CSIRT Operations'.
- The SOCCRATES final event took place on 19 October 2022 in Luxembourg.

3.4 Cooperation with other projects

3.4.1 EU H2020 projects

On initiative of the CyberSANE project, we co-organized two online workshops (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 and on February 8th 2022.

All projects were present:

- 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

It is very good to have close collaboration with these projects.

We have made a liaison with SAPPAN already in the beginning of the project. We have co-organized three workshops with them (ARES '20, '21 and '22). On September 28th 2021 SAPPAN and SOCCRATES held a joint theme session on detecting DGA (Domain Generation Algorithm) related threats.

We have made a liaison with CyberSEAS (Cyber Securing Energy dAta Services) for our 4th International Workshop on Next Generation Security Operations Centers (NG-SOC 2022) at the ARES 2022.

Together with CyberSane and SAPPAN, we have made use of the Horizon Results Booster (SERVICE 1 "Portfolio Dissemination and Exploitation Strategy (PDES)). We implemented some elements from

the advice, such as paid LinkedIn campaigns. The remaining advice was mostly already included in our own dissemination plan. Therefore, we chose not to enroll in other modules.

KPI	Target level	Current score
Liaisons with other EU projects	>2	3

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.
- TNO has exchanged insights from SOCCRATES with other TNO projects, such as ASOP.
- Francesca Soro (AIT) provided a lecture 'Domain generation algorithms (DGA) detection using machine learning' during the ARTISAN Summer School 2022 (Role and effects of ARTificial Intelligence in Secure ApplicatioNs), 4-7 Jul 2022 Valence (France).

This is really interesting for SOCCRATES and the other projects and strengthens the SOCCRATES relation network.

KPI	Target level	Current score
Exchange of information with other projects (including EU projects)	3	13
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 four EU project workshops that are co-located with the ARES conference[2]. The workshop series, called NG-SOC[3], 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 following workshops were co-organized with members of the SAPPAN consortium. The workshop in 2022 was co-organized with SAPPAN and CyberSEAS.

Picture of the ARES workshop 2022

The workshop continued to mature and gain visibility within the community. 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 (Shadows-erver)
- 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)

Co-hosted workshop:

August 17, 2021: 3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021), in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021), video conference.

Agenda:

Time		Talk	Duration [min]
13:45	14:00	Welcome and Workshop Overview *Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)*	15
Session 1 *Session Chair: Irina Chiscop (TNO, Netherlands)*			60
14:00	14:20	System for Continuous Collection of Contextual Information for Network Security Management and Incident Handling *Martin Husák (Masaryk University, Czechia),* *Martin Laštovička (Masaryk University, Czechia), and* *Daniel Tovarňák (Masaryk University, Czechia)*	20
14:20	14:40	On the Evaluation of Sequential Machine Learning for Network Intrusion Detection *Andrea Corsini (University of Modena and Reggio Emilia, Italy),* *Shanchieh Jay Yang (Rochester Institute of Technology, USA) and* *Giovanni Apruzzese (University of Liechtenstein, Liechtenstein*)	20
14:40	15:00	A Recommender System for Tracking Vulnerabilities *Philip Huff (University of Arkansas, USA),* *Kylie McClanahan (University of Arkansas, USA),* *Thao Le (Bastazo, Inc., USA), and* *Qinghua Li (University of Arkansas, USA)*	20
15:00	15:30	*Coffee break*	30
Session 2 *Session Chair: Tomáš Jirsík (Masaryk University, Czechia)*			80
15:30	16:10	**Keynote: Title (TBD)** Frode Hommedal, *Chief Technology Officer and head of Cyber Threat Operations (Defendable, Norway)*	30 +10 Q&A
16:10	16:30	Combining anomaly detection models for more reliable attack detection *Dmitriy Komashinskiy (F-Secure, Finland)*	20
16:30	16:50	Quantitative Impact Analysis *Christophe Kiennert (Télécom SudParis, France)*	20
16:50	17:15	*Coffee break*	25
Session 3 *Session Chair: Avikarsha Mandal (Fraunhofer FIT, Germany)*			80

17:15	17:35	Adversary Emulation Planner: Generating MITRE ATT&CK Technique Sequences *Martin Eian (mnemonic, Norway)*	20
17:35	17:55	Graph-based Network Traffic Analysis for Incident Investigation *Milan Cermak (Masaryk University, Czechia)*	20
17:55	18:15	Automated Infrastructure Modelling – Foundation for Security Operations *Ville Alkkiomäki (F-Secure, Finland)*	20
18:15	18:35	Taking a look at the *.ch zone with a DGA detector *Mischa Obrecht (DreamLab Technologies AG, Switzerland)*	20
18:35	18:45	Wrap Up *Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)*	10

Co-hosted workshop:
August 23, 2022: 4th International Workshop on Next Generation Security Operations Centers (NG-SOC 2022) in conjunction with the 17th International Conference on Availability, Reliability and Security (ARES 2022), Vienna.

Session 1: 10:45-12:15 Session Chair: Irina Chiscop (TNO, The Netherlands)	**Presentations**	**Format**
10.45-11:15	Attack graphs as digital twins for managing breach prevention, detection, and reaction by Giuseppe Nebbione and Mathias Ekstedt *(KTH Royal Institute of Technology, Sweden)*	online
11:15-11:45	Methodological improvement of the Cyber Security of Energy Data Services: the CyberSEAS way *by Luigi Cappolino (University of Naples "Parthenope", Italy)*	online
11:45-12:15	A joint approach to cybersecurity for Energy operators: the CyberEPES cluster *by Paolo Roccetti (Engineering R&D Labs, Italy)*	online
Session 2: 14:00-15:15 Session Chair: Francesca Soro (AIT, Austria)	**Presentations**	**Format**
14:00-14:30	Toward Automated Playbook Generation through Natural Language Processing by *Zsolt - Levente Kucsván*	In person

	(University of Twente, The Netherlands)	
14:30-14:50	Algorithms for detecting automatically generated domain names by *Irina Chiscop (TNO, the Netherlands) and Francesca Soro (AIT, Austria)*	In person
14:50-15:15	Analysis of anomalies detected on endpoints by *Dmitriy Komashinskiy (F-secure, Finland)*	online

Webinars

During the project, we have organized 9 webinars, which attracted 30 to 60 participants per session. One webinar is planned to be held after the end of the project. The replay videos were published on the SOCCRATES website and promoted via social media.

Measurable outcome:

KPI	Target level	Current score
Number of workshops	>2	4
Number of workshop attendees	20-30	35
Co-hosted workshops	2	3
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 front page of the website is shown 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 is continuously refreshed with new information.

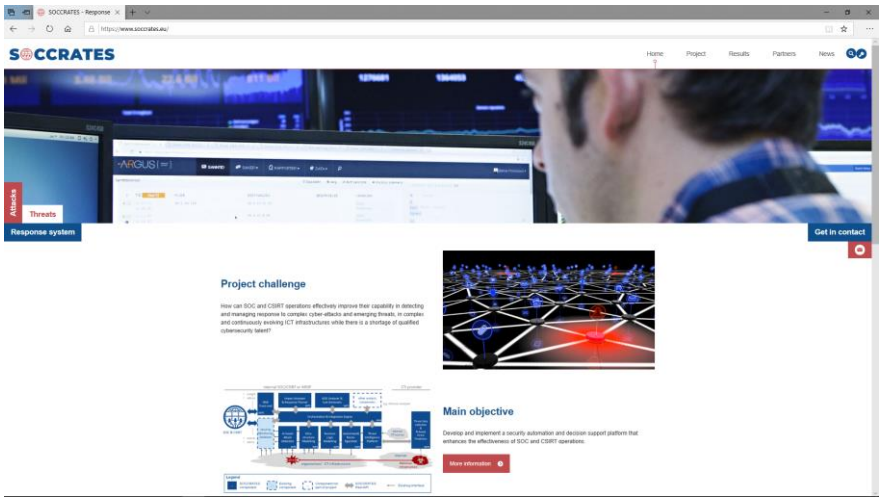


Figure 2 – front page of the SOCCRATES website

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. During the project period we've updated the website with news, deliverables, podcasts and blog posts.

KPI	Target level	Current score
Blog posts (news)	15	32
Yearly visits to the closed part of the website	>100	n/a
Views/accesses of the website during the project lifetime	>3000	14.000
Unique visitors to SOCCRATES website per month in the last year of the project	>100	January: 156 February: 509 March: 569 April: 211 May: 227 June: 215 July: 197 August: 222 September: 374 October: (until 5-10) 91

Please note that we have published three blog posts, besides from the news articles on the website:

- From Anomalies to Actions: Reasoning About the Root Cause of Anomalies to Determine Actionable Insights for Cyber-Attack Mitigation
- Automating the hunt for new DGAs and other malicious domains
- Future needs of next generation SOCs and CSIRTs

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). 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 use it to promote project events, like workshops, webinars, attendance at exhibitions and public fora and similar, downloads and deliverables, podcasts and blog posts, leveraging social media links to other related ongoing EU- and nationally-funded projects. In the last period we added a 'Platform Software' page:

The SOCCRATES Platform consists of multiple components. Each component provides a particular service within the security automation and decision support platform. On this webpage the software is listed for each component, including information on where to get the software and instructions for

installation. The SOCCRATES Platform can be deployed as a whole, or individual SOCCRATES components can be integrated within your own security infrastructure.

We significantly expanded the reach of our LinkedIn group, with 290 followers by October 2022. We set up paid LinkedIn campaigns to increase the number of followers, and to promote the vision paper.

KPI	Target level	Current score
Posts made by SOCCRATES project members	>100	93*
Membership of SOCCRATES target groups	>30	52
Active participation of members (e.g. posts, comments, likes)	>100	1750 clicks on socials posts in the last year of the LinkedIn page.

**Please note that there were 93 posts by SOCCRATES on the SOCCRATES social media channels. It is not possible to measure how many times these posts were liked and shared by project members.*

3.9 SOCCRATES webinars

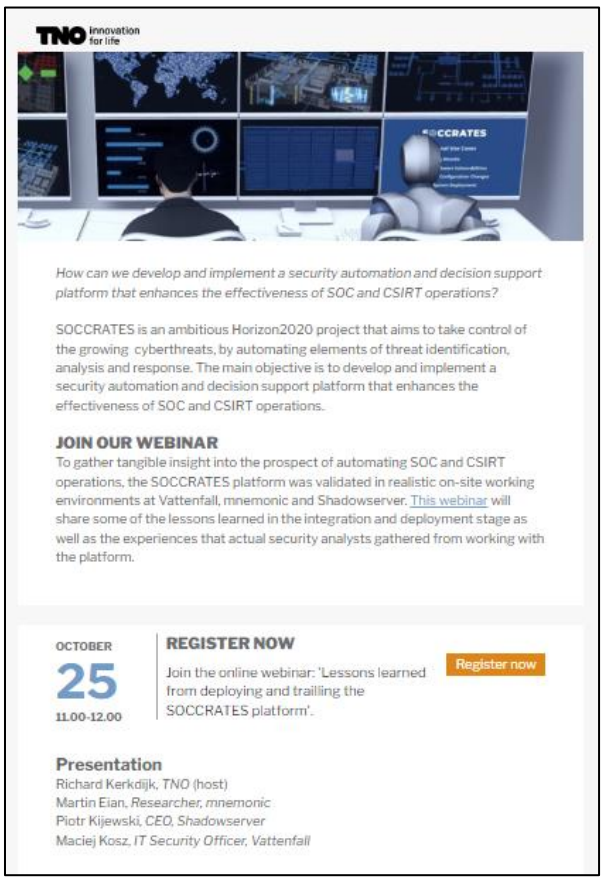
SOCCRATES has organized nine webinars, featuring different innovation topics and all combining presentations and demonstrations. Participants can register on the SOCCRATES website and the webinars are also advertised on several partner websites, newsletters and social media channels.

The webinars are well visited, although we noted that on average, only one third of the registered people actually attended the webinars. 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 especially 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. This package did not meet our needs, so we successfully implemented WebinarGeek later in the project.

Measurable outcome:

KPI	Target level	Current score
Number of webinars held	>5	9
Number of participants per webinar	>15	29



Example of a newsletter promoting a SOCCRATES webinar.

Example of a social media update promoting a SOCCRATES webinar.

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 released 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'), social media and also here: https://vimeo.com/423498497. There is a version with subtitles (https://vimeo.com/442734821). For promoting the final event, we've made a promotional video, which can be seen here. Finally, all webinars have been posted as recordings on the website.

Measurable outcome:

KPI	Target level	Current score
Informative and educational videos	3-6	12
Number of video views	>50	290 (introduction video)

3.12 SOCCRATES pilots

We have run several pilots that we also used to disseminate results:

- The first technical pilot was limited to evaluating a number of SOCCRATES modules, and ran between January and April 2021. Three modules were tested on location of SOCCRATES partner mnemonic: AI-based Attack Detection (AAD), Infrastructure Modelling Component (IMC), Threat Intelligence Platform (TIP). The SOCCRATES modules that were tested seemed to work in practice.
- The second pilot was intended to run between February and May 2022. We suffered delays here and in the end the pilot was only partial successful. The second pilot mnemonic pilot site was run with analysts from for two weeks in September 2022. The second pilot Vattenfall pilot site was never run with analysts. Pilot site Shadowserver ran for the duration of 2022.
- To gather more results, we have organized an evaluation session with analysts from VTF and MNM, using the SOCCRATES demonstrator (full functionality except the AAD) to get feedback. This led to interesting results that we also shared on events and in webinars.
- For more details, see D7.2: Pilot application and evaluations

3.13 SOCCRATES demonstrations

We have provided many demonstrations. Demonstrations consisted of individual modules and we provided them in webinars, to our advisory board, to our stakeholder group and in external

presentations. The complete SOCCRATES platform was presented at the SOCCRATES final event, the ONE Conference 2022 and in our webinar. After the project we will keep the demonstrator online for several months and we already have several demonstrations planned for after the project end.

Measurable outcome:

KPI	Target level	Current score
Demonstrate SOCCRATES platform at cyber security related events	>5	3

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.
  Please note, the CD-MAKE paper has been downloaded 506 times, according to Springer

2021 IEEE International Conference on Cyber Security and Resilience (IEEE CSR)

- A. Gylling, M. Ekstedt, Z. Afzal, and P. Eliasson: 'Mapping cyber threat intelligence to probabilistic attack graphs', 2021
-

NativeNI 2022

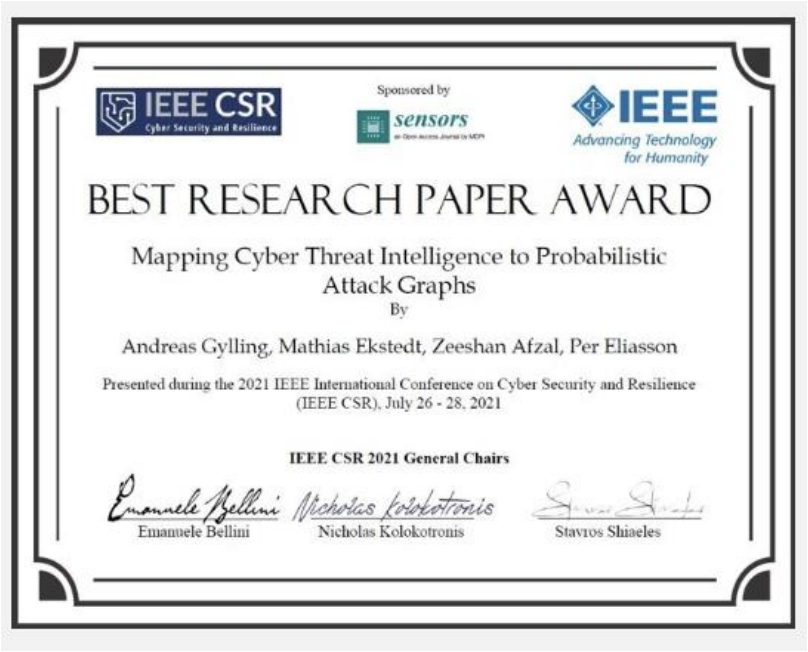
- I. Chiscop, F. Soro and P. Smith, 'AI-based Detection of DNS Misuse for Network Security', 2022

The number of submitted papers was less than we planned, because a large focus was on the development and implementation of the platform. There are still a few scientific papers in the pipeline that might lead to acceptance, but we cannot tell at this moment in time.

Measurable outcome:

KPI	Target level	Current score
Number of scientific publications: conference papers accepted	10-20	4

Please note that 'Mapping cyber threat intelligence to probabilistic attack graphs' (2021) has won the Best Research Paper Award, presented during the 2021 IEEE International Conference.



3.15 Journals and magazines

Successfully submitted:

- SOCCRATES - Security automation in SOC & CSIRT environments, Reinder Wolthuis, Frank Fransen, IB magazine, 2021 (TNO)
- SOCCRATES - Real-time threat, impact analysis and response automation for SOC/CSIRT operations, Reinder Wolthuis, Frank Fransen, IB magazine 2021 (TNO)
- SOCCRATES - Vision & Roadmap for SOC & CSIRTs, Reinder Wolthuis, Frank Fransen, IB magazine 2022 (TNO)
- SOCCRATES – Automation and Orchestration of Security Operations, Susana Gonzalez Zarzosa, Jesus Villalobos Nieto, IB magazine 2023 (ATOS)

Measurable outcome:

KPI	Target level	Current score
Number of (scientific) publications: journals	3	4

Please note that our paper SOCCRATES - Security automation in SOC & CSIRT environments by Reinder Wolthuis, Frank Fransen in IB magazine (2021) has won the 'Article of the year award', an initiative from IB magazine.

3.16 SOCCRATES final event

The SOCCRATES final event 'Innovation for Next Generation SOC' was organised in collaboration with the Cybersecurity Week Luxembourg 2022. The event took place 19 October 2022 in Kirchberg, Luxembourg. The event was well attended. We received over 70 registrations. We promoted the event through our website, social media, and direct mail to our stakeholders. We made a promotional video, which can be seen here. We also spread an attractive invitation. We were proud to present keynote speaker Christine Bejerasco, CTO of WithSecure.

Programme highlights

- Keynote speech by Christine Bejerasco, CTO WithSecure: 'Threat Landscape & A New Security Mindset'
- SOCCRATES vision & results
- Use case demos: SOCCRATES use cases and infrastructure, infrastructure modelling, the SOCCRATES platform
- Pilot learnings
- SOCCRATES results in commercial and Open Source products
- Presentation of the SOCCRATES vision paper

Invitation to the SOCCRATES final event

Reinder Wolthuis opening the SOCCRATES final event

3.17 Standardization

There were several successes on standardization, both contributions and relationships:

- TNO became member of OASIS Open - TC openC2 and TC CACAO and shared information from the SOCCRATES project to the group.
- The project coordinator was appointed as a member of the Enisa adhoc working group on SOC/CSIRT and also as a rapporteur for the task force CTI sharing taxonomies. This input to this working group is based for a large part on results of the SOCCRATES project.
- SOCCRATES results on the Adversary Emulation Planner are adopted by MITRE and included in the ATT&CK framework. SOCCCRATES is listed as a contributor.[4]

KPI	Target level	Current score
Contributions to policy and standards, e.g. citations of SOCCRATES results	2	3
New relationships with appropriate bodies	2	3 (OASIS Open, MITRE and Enisa)
References to results in policy	2	0
Position papers (e.g. to ECSO WG6 (research) or WG5 (education)	3	1 (vision paper)

[4] https://attack.mitre.org/techniques/T1588/002/ and https://attack.mitre.org/resources/contribute/

4 Conclusion

SOCCRATES has planned and executed very many communication and dissemination activities. The KPIs we have formulated have not all been met, but most of them we have met and many we have exceeded. Also we have initiated many dissemination activities that were not planned. Overall this has led to high visibility and interaction with relevant target groups and greatly supported in achieving a high impact.

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)

[D8.3] SOCRATES first Dissemination report, version 1.0, February 28th 2021, Reinder Wolthuis (editor)

Annex: Overview of current KPI scores

KPI	Target level	Current score	Details
Number of SOCAB meetings	3	7	• May 26th 2020 • September 15th 2020 • December 15th 2020 • May 26th 2021 • September 14th 2021 • January 25th 2022 • May 23rd 2022
SOCAB Attendance on SOCCRATES organized workshops	1	1	• Judith Rossebo attended the final event in Luxembourg. Andy de Petter was unable to attend at the last minute.
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	9	• KPN, • Amadeus, • Telenor, • Proximus, • Ordina, • Thales, • NRD, • Defendable • Sightlabs
Number of National CERTs in stakeholder group	>2	4	• Latvian National CERT, • Polish National Cert, • Norwegian Energy Sector Cert • SPCSS Czech Republic
Number of end users in stakeholder group	>10	8	• CZ • ONVZ • RDW • Europol • Stockholm count Council • Skanska • Telenor • KPN
Number of vendors in stakeholder group	>5	4	• Amadeus IT Group, • Thales, • Vairav technology, • Crowdstrike
Stakeholder group members attendance on SOCCRATES organized workshops	>6	7	• SECO 2020 • ARES 2020 • ARES 2021 • ARES2022

			• Final event
Number of MSSPs contacted about SOCCRATES	>25	25	Among others: • 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	10	Among others: • 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	7	• 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 (2020 and 2022) • SOC Automation 1.1, SOCCRATES presented (Frank Fransen, Erik Ringdahl), August 26th 2020 • Connect2Trust Presented SOCCRATES, September 3rd 2020 (Reinder Wolthuis) • SCADA, 8-9 November (Mathias Ekstedt) • FIC 2022, June 7-9th, Reinder Wolthuis provided a pitch

Publication downloads	100	-	the number of downloads of our scientific publications is unfortunately untraceable. The number of downloads of SOCCRATES deliverables on the website was over 500.
Citations during project	50+	35	• Subverting Network Intrusion Detection: Crafting Adversarial Examples Accounting for Domain-Specific Constraints, M Teuffenbach, E Piatkowska, P Smith: 5 • Mapping Cyber Threat Intelligence to Probabilistic Attack Graphs, A Gylling, M Ekstedt, Z Afzal, P Eliasson: 3 • An attack simulation language for the IT domain, S Katsikeas, S Hacks, P Johnson, M Ekstedt, R Lagerström, J Jacobsson: 27
Invited talks by consortium members	7	4	Among others: • 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	3	• SAPPAN • CyberSEAS • CyberSane
Exchange of information with other projects	10	13	Among others: • 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	4	• ARES '19 • ARES '20 • ARES '21 • ARES '22
Number of workshop attendees	20-30	35	
Co-hosted workshops	2	4	• ARES '20

			• ARES '21 • ARES '22
Attendees at co-hosted workshops	30-50	35	
Blog posts	15	32	
Yearly visits to the closed part of the website	>100	n/a	
Views/accesses of the website during the project lifetime	>3000	14.000	
Unique visitors to SOCCRATES website per month in the last year of the project	>100		January: 156 February: 509 March: 569 April: 211 May: 227 June: 215 July: 197 August: 222 September: 374 October: (until 5-10) 91
Posts made by SOCCRATES project members	>100	93	Please note that there were 93 posts by SOCCRATES on the SOCCRATES social media channels. It is not possible to measure how many times these posts were liked and shared by project members.
Membership of SOCCRATES target groups	>30	52	
Active participation of members (e.g. posts, comments)	>100	1750	1750 clicks on socials posts in the last year of the LinkedIn page.
Number of webinars held	>5	9 (1 planned after project end)	SOCCRATES Webinars - Soccrates
Number of participants per webinar	>15	29	
Informative and educational videos	3-6	12	9 webinar replays (one planned after project end) 1 informative video 1 promotional video
Number of video views	>50	290	290 (introduction video)
Demonstrate SOCCRATES platform at cyber security related events	>5	3	One conference, Final event, webinar. Several demonstrations planned for after the project end
Number of scientific publications: conference papers accepted	10-20	4	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. *Please note, the CD-MAKE paper has been downloaded 506 times, according to Springer* 2021 IEEE International Conference on Cyber Security and Resilience (IEEE CSR) - A. Gylling, M. Ekstedt, Z. Afzal, and P. Eliasson: 'Mapping cyber threat intelligence to probabilistic attack graphs', 2021 - NativeNI 2022 - I. Chiscop, F. Soro and P. Smith, 'AI-based Detection of DNS Misuse for Network Security', 2022
Number of scientific publications: journals	3	4	- SOCCRATES - Security automation in SOC & CSIRT environments, Reinder Wolthuis, Frank Fransen, IB magazine, 2021 (TNO) - SOCCRATES - Real-time threat, impact analysis and response automation for SOC/CSIRT operations, Reinder Wolthuis, Frank Fransen, IB magazine 2021 (TNO) - SOCCRATES - Vision & Roadmap for SOC & CSIRTs, Reinder Wolthuis, Frank Fransen, IB magazine 2022 (TNO) - SOCCRATES – Automation and Orchestration of Security Operations, Susana Gonzalez Zarzosa, Jesus Villalobos Nieto, IB magazine 2023 (ATOS)
Contributions to policy and standards, e.g. citations of SOCCRATES results	2	3	OASIS Open, MITRE and Enisa
New relationships with appropriate bodies	2	3	OASIS Open, MITRE and Enisa
References to results in policy	2	0	
Position papers (e.g. to ECSO WG6 (research) or WG5 (education)	3	1	Vision paper