SOCCRATES

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

D8.6

Exploitation plan

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

Responsible organisation:	MNM
Editor:	Reinder Wolthuis
Revision:	1.0

Abstract	This deliverable describes the SOCCRATES exploitation plan. The plan lists for each of the foreseen results the exploitation by the SOCCRATES consortium partners, as well as uptake by organisations outside the consortium.
Keywords:	Exploitation, innovation, market, security automation

Management summary

This SOCCRATES exploitation plan lists the plans for Exploitation of results after the SOCCRATES project has ended.

We have made a high level market analysis and we have listed all exploitable SOCCRATES results. Each partner describes which results the partner is intended to Exploit and how they intend to exploit them.
Besides partner exploitation plans we also ensured continuous project exploitation:

- Many of our produced knowledge base will remain available on or via our project website after the projects has ended: deliverables, Open Source software, articles, vision paper, webinar recordings etc.
- We have decided to make available the SOCCRATES platform as a whole on our website, but not to further exploit the platform as a whole. The exploitation of technical results focusses specifically on the platform components and these components will be part of (commercial) products and services or published as Open Source and also will be further built-on in follow-up projects.

Although the dissemination enabling exploitation outside the consortium has been hampered by COVID-19, we sufficiently have reached our envisaged target groups during the project. We think that with the exploitation plans we will achieve high impact, that adequately addresses the expected impact from the call. We also think that with the plans laid down in this report, we ensure the continuous use and further development of the SOCCRATES results, contributing to a society that is more robust against cyber-attacks.

Contributor(s)	All General Assembly members

Reviewer(s)	Richard Kerkdijk (Content) Aljosa Pasic (Security)

Security Assessment	See deliverables table for security assessment requirements
Approval Date	27/10/2022
Remarks	None

Table of Contents

MANAGEMENT SUMMARY 2

1 INTRODUCTION 6

1.1 The SOCCRATES project 6
1.2 Introduction to the exploitation plan 7
1.3 Purpose & objectives 7
1.4 Methodology 7
1.5 Structure of this deliverable 7
1.6 Deviations from original Description of Work (DoW) 8
1.6.1 Project extension 8
1.6.2 Pilot 8
1.7 Other information 9

2 EXPLOITATION STRATEGY 9

2.1 (High level) market analysis 9
2.1.1 Assess commercially available security products, Open Source products and state of standardization 9
2.1.2 Assess maturity of end-users 9
2.1.3 Discussions with the Advisory Board (SOCAB) 10
2.1.4 Joint standardization 10
2.1.5 Discussions with the stakeholder group 11
2.1.6 Horizon Results Booster 12
2.1.7 Conclusion 12
2.2 Exploitable results 12
2.2.1 SOCCRATES platform 12
2.2.2 SOCCRATES demonstrator 13
2.2.3 ADG Analyser 15
2.2.4 DGA detective 16
2.2.5 AAD 16
2.2.6 ACT SOCCRATES improvements 17
2.2.7 Infrastructure Modelling Component(IMC) 17
2.2.8 Adversary Emulation Planner (AEP) 18
2.2.9 Contributions to MITRE ATT&CK 18
2.2.10 Pilot results 18
2.2.11 Platform for hunting malicious domains in sandbox environment 19
2.2.12 Shadowserver SOCCRATES API 19
2.2.13 SOCCRATES orchestrator 20
2.2.14 Webhook Notification Cortex Responder 20
2.2.15 CACAO playbook Cortex responder 21
2.2.16 L-ADS 21
2.2.17 SOCCRATES website (after the project) 22
2.2.18 Organising exercises and education (for analyst staff) with the SOCCRATES knowledge ... 22
2.2.19 CoA generator 22
2.2.20 BIA 23
2.2.21 Response planner 24

2.3 Other results 24
2.3.1 Experience with complex software development 24
2.3.2 Follow-up proposal in Horizon Europe 27
2.4 Modes of Exploitation 27
2.4.1 Publication of Open Source Software 27
2.4.2 Standardization 28
2.4.3 New and enhanced products and services 28
2.4.4 Knowledge development & further innovation 29
2.4.5 Education and training 30
2.4.6 Events and publications 31
3 JOINT PROJECT EXPLOITATION 31
3.1 Exploit SOCCRATES platform (all partners) 31
3.2 Spread the vision of SOCCRATES with SOCCRATES demonstrator (WithSecure, TNO) 32
3.3 Exploit SecuriCAD functionality improvements (foreseeti and KTH) 34
3.4 Exploit DGA detective (SHS and TNO) 34
4 INDIVIDUAL PARTNER EXPLOITATION PLANS 34
4.1 SOCCRATES End users 34
4.1.1 Mnemonic 34
4.1.2 Vattenfall 36
4.2 SOCCRATES vendors and service providers 36
4.2.1 Shadowserver 36
4.2.2 WithSecure 37
4.2.3 Foreseeti 39
4.2.4 ATOS 39
4.3 SOCCRATES RTOs 41
4.3.1 TNO 41
4.3.2 AIT 41
4.4 SOCCRATES universities 42
4.4.1 IMT 42
4.4.2 KTH 42
5 RELATED LEGAL AND REGULATORY ASPECTS 43
6 CLOSING REMARKS 44
7 ABBREVIATIONS 46

1 Introduction

This section introduces the SOCCRATES project and defines the goals of this deliverable.

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.

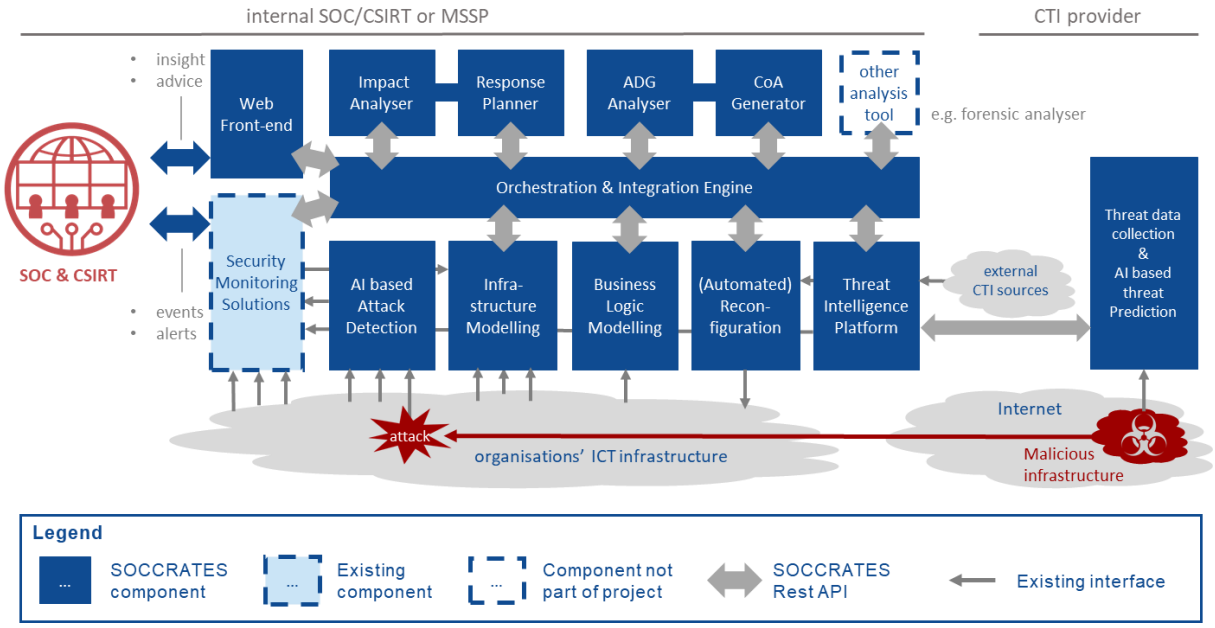


Figure 1.1: The SOCCRATES platform

The SOCCRATES platform (see **Figure 1.1**) 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 visit www.SOCCRATES.eu for more information on the SOCCRATES project.

1.2 Introduction to the exploitation plan

The exploitation plan lists for each of the foreseen results the exploitation by the SOCCRATES consortium partners as well as any uptake by organisations outside of the consortium. It is based on a high level market analysis. We also assess the (already achieved and planned) impact of SOCCRATES results.

Of course, successful exploitation also requires visibility of the achieved results. That is why this exploitation plan also depends on successful dissemination. To this end we refer to SOCCRATES deliverable D8.5: *Final report on dissemination and standardization activities.*

1.3 Purpose & objectives

This deliverable provides an overview of the plans for exploitation of the SOCCRATES results in the two years after the project has ended. Its aim is to ensure that project results are actually used and furthers built upon, so that the project results will actually have the impact that was envisaged in the project proposal.

1.4 Methodology

The method used to compile this exploitation plan is:

- Perform a high level market analysis, targeting those markets that are applicable for the SOCCRATES results;
- Create a list of all achieved results;
- Present joint exploitation efforts, in which partners collaboratively exploit one or more project results;
- Present individual partner exploitation plans; all partners will list foreseen (individual) exploitation of the achieved results
- Assess related legal and regulatory aspects.

1.5 Structure of this deliverable

Chapter 2 presents the Exploitation strategy. It includes a high level market analysis, a list of exploitable and other results and lists the modes of Exploitation that we use for the SOCCRATES results. Chapter 3 identifies and presents joint exploitation plans, in which partners collaboratively exploit one or more project results. Chapter 4 contains the individual partner exploitation plans, going into

further detail about how exploitation is being set up at each partner. Chapter 5 assesses related legal and regulatory aspects, chapter 6 draws some conclusions.

1.6 Deviations from original Description of Work (DoW)

We were mostly able to follow the original plans as they were set out in the DoW. There were some deviations:

1.6.1 Project extension

The project requested and was granted a two month extension, which was needed because of several factors that were delaying the project:

- The organization of the final workshop to present all SOCCRATES results. In the original planning this would have to be planned in the summer holiday period and that is not a good timing to attract sufficient audience
- The software implementation of the SOCCRATES platform, pilot deployment and pilot execution were delayed because of COVID travel restrictions. In some cases, such as implementation and deployment of complex software systems, physical presence is a condition for success. The extension provided us with the possibility to execute and learn from the pilot even if it is delayed for this reason.

So the post-project exploitation starts two months later than originally planned.

1.6.2 Pilot

The SOCCRATES platform is a large and complex software implementation. Because of a large number of unforeseen and hard to control technical issues in the pilot deployment, we could not fully deploy the platform on the mnemonic and Vattenfall pilot sites, which are TRL 7-9[1] environments. However, the ambition for the SOCCRATES platform was to achieve TRL 6[2]. For the project, getting the TRL 6 demonstrator environment running in full meant that the target of the original project proposal was achieved. To maximize the exposure of actual SOC analysts to the platform and its automation capabilities, the project sought ways to also evaluate it in higher TRL environments. To this end, a hybrid setup was established that went well beyond the original ambitions:

- At the mnenomic pilot site, the project was able to get the workflow for use case 1 (specifically the "initial access" scenario) running on actual operational infrastructure. For a limited period of time, this allowed actual analysts to conduct evaluations with the SOCCRATES platform on actual alerts that had been triaged in the mnenomic SOC. Effectively this means that selected platform capabilities were operated and trialled at TRL 7.
- The demonstrator environment (see section 2.2.2) was used to let analyst teams at both Vattenfall and mnemonic become acquainted with the platform in its entirety. For all of the project's use cases (1-5), therefore, both pilot teams evaluated the SOCCRATES platform in its full TLR 6 manifestation.

This slightly adapted pilot has no direct influence on most of the SOCCRATES exploitation plans, which are about further exploiting the technology, which was developed as planned.

[1] Technology Readiness Level (TRL) 7: System prototype demonstration in operation environment

[2] TRL 6: Technology demonstrated in relevant environment

1.7 Other information

During the project term, Foreseeti was acquired by Google Cloud EMEA Ltd, a limited liability company established in Ireland. This development further advances SOCCRATES' project goals by increasing the potential of exploitation and dissemination of Foreseeti's securiCAD functionality through the planned integration with Google Cloud's security portfolio, which will ultimately bring greater cybersecurity protections and options to customers.

2 Exploitation strategy

2.1 (High level) market analysis

To explore the market, we have initiated several activities. These are explained in the following sections.

2.1.1 Assess commercially available security products, Open Source products and state of standardization

During SOCCRATES, we have not seen products emerging on the market (or offered as Open Source) that offer functionality that the SOCCRATES platform offers. Of course more and more SOAR tools are available on the market (e.g. Splunk SOAR, Google Siemplify, IBM QRadar SOAR, ServiceNow) and there were developments in the SOAR tooling e.g. many tool providers claim that they integrated AI and Machine Learning techniques in their products. As the 2020 Market Guide for Security Orchestration, Automation and Response Solutions of Gartner[3] puts it: "As a pure-play technology, SOAR continues to mature but remains a relatively niche market. It is being consumed into other markets such as SIEM, XDR and MDR."

But the way the SOCCRATES platform applies security reasoning to integrally increase situational and option awareness both from a technical and business perspective, applying technologies such as Attack Defense Graphs and automatic CoA generation, is certainly not available in the market today. So the SOCCRATES results still have an innovative contribution to existing products, Open Source and standardization.

2.1.2 Assess maturity of end-users

The maturity of end-users has increased during the SOCCRATES project lifetime. As we have seen during the stakeholder meetings (see also below) and webinars, the audience was knowledgeable and the interaction showed interest and a need to improve. Also, the scarcity of security expertise was confirmed in these interactions, which actually was one of the key pillars to start SOCCRATES and increase security automation in SOC and CSIRT environments. Overall, the (mature) end users seem eager to use technology developed by SOCCRATES. Of course, it is rather challenging to get automation concepts such as SOCCRATES adopted in an actual organization. And also, SOC and CSIRT teams typically don't have the mandate at present to execute changes in the operational infrastructure. To get automated reconfiguration adopted, many organizations will need to reconsider their

[3] https://www.gartner.com/en/documents/3990720

existing maintenance and change procedures and the mandate of their security teams. It requires something of a culture change and that is inherently hard.

2.1.3 Discussions with the Advisory Board (SOCAB)

We had many interesting discussions with our Advisory Board on the SOCCRATES project and results. We want to mention some points that came out of the discussion that are relevant for Exploitation.

No greenfield

The SOCCRATES platform incorporates many (automation) functions. It also includes collecting security event data through the Anomaly Based Detection Module. But a SOC that is already in operation, will also have a SIEM (and other security monitoring solutions) that also contains security events from the infrastructure that is monitored. And also, a SOC will have tooling that they use which might cover part of the functionality of the SOCCRATES platform. We can therefore not assume that the SOCCRATES platform *as a whole* will be easily deployed in an operational environment. The evaluation we did with the platform at our pilot sites confirms this conclusion. We have therefore concluded that the SOCCRATES platform as a whole will not be a valid exploitation result as a commercial product. We will provide the opportunity to build the whole platform (https://www.SOCCRATES.eu/platform-software/) and we will demonstrate the platform by using the demonstrator with a small demo infrastructure. But the exploitation focus lies on the *individual functional modules* that we have developed as part of the platform.

Multiple attackers simultaneously

We discussed whether the platform could handle multiple attacks at the same time, e.g. multiple attackers on one host. We think in this case we need to group attacks, which might be difficult and capacity may be insufficient to handle multiple attacks simultaneously. This is not in scope of the current SOCCRATES project, but definitely something to include in future projects.

Infrastructure Modelling

Our Advisory board, and also interaction during the presentations and events we have organized, confirmed that Infrastructure Modelling is one of the biggest opportunities for the modern SOC environments. A good Infrastructure Modelling implementation can steer SOC teams and their broader organizations away from recurring asset inventory projects that rarely lead to a structural and actual insight into the assets that are in an organization's infrastructure. The Advisory Board stressed the need to use existing standards for Infrastructure Modelling, which we indeed did in the SOCCRATES project.

Attack Defense Graphs

Our advisory board particularly liked this concept and considered it to be very innovative and suitable for future SOC operations.

2.1.4 Joint standardization

We 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.

2.1.5 Discussions with the stakeholder group

We had several meetings with our stakeholder group (https://www.SOCCRATES.eu/project/stakeholder-group/). In the first meetings, we presented our work and had some interactive discussions, but one meeting was dedicated specifically to exploitation. There were some interesting results coming out of this.

As can be seen in the picture below, the stakeholder group thinks that Open Source outcomes provide most value for them.

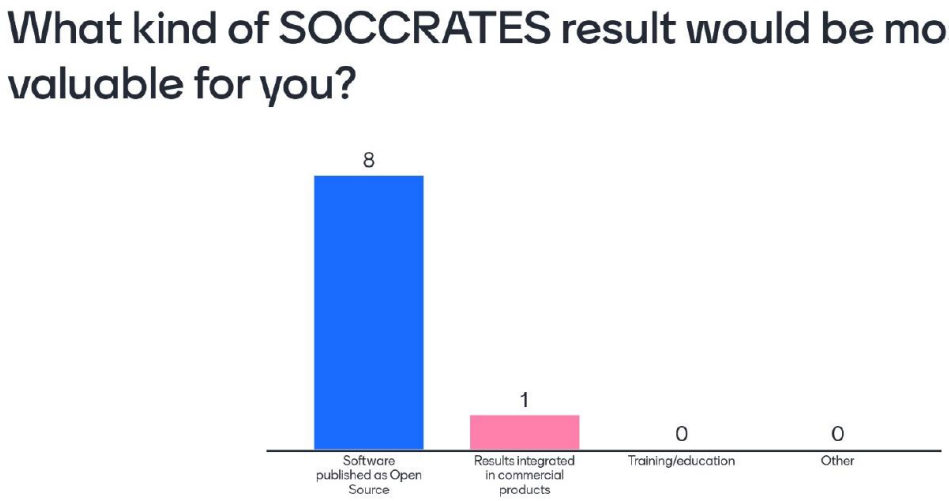


Figure 2.1: Results of question to stakeholder group on value of SOCCRATES results

We also asked them which specific SOCCRATES functionality they liked and would like to see integrated into future products. The following topics were mentioned:

- AI based attack detection
- CTI platform
- Infrastructure modelling
- ADG analyser
- Impact analyser

The stakeholder group also stressed the need for suitable training material in able to use the Open Source products.

And finally, we asked them which aspects they missed in the SOCCRATES project. The following topics were mentioned:

- Response automation (partly covered in SOCCRATES with the Automated Reconfiguration)
- Better triaging functions
- Logs coverage in the context of detection.

All in all, this discussion with the stakeholder group confirmed that we address the right topics and have the right exploitation focus with SOCCRATES but also identifies future topics to develop.

2.1.6 Horizon Results Booster

Supported by the European Commission's Horizon Results Booster program (HRB), SOCCRATES, SAPPAN and CYBERSANE have formed a Project Group (PG) based on commonalities between their work in this research field.

HRB supports effective transfer of research and innovation project results to policy makers, industry and society by offering various services as dissemination, exploitation strategy and business plan development to projects supported under the 7th Framework Programme (FP7) or Horizon 2020 funding schemes.

This has resulted in a document, D1.1 Portfolio of Research and Innovation Project Results of SOCCRATES PG, that pools together the collective results of the PG to be disseminated, defines their characteristics and the target stakeholders that can benefit from these results and are ultimately the target audience for the PG dissemination activities. This was helpful and we have assessed whether we could also make use of follow-up modules that provide more actual support in dissemination activities such as the organization of events and also exploitation. We have decided not to take this step because the conclusion was that the advantages of these activities did not weigh up to the effort required to put in by the project members.

2.1.7 Conclusion

The SOCCRATES platform fills an evident gap in automation of SOC and CSIRT operations. The market is ready to adopt these kind of technologies and end-users require them.

2.2 Exploitable results

SOCCRATES has produced an elaborate set of exploitable results. We list the results in this paragraph; exploitation of the results by each partner will be further elaborated in chapters 3 and 0.

2.2.1 SOCCRATES platform

The SOCCRATES Platform, see Figure 1.1, consists of multiple components. Each component provides a particular service within the security automation and decision support platform. The SOCCRATES Platform has been designed to handle five security operations use cases:

- Use Case 1: Response on Detected Ongoing Attack
- Use Case 2: Response on Newly Received Cyber Threat Intelligence
- Use Case 3: Response on Newly Discovered Vulnerable Assets
- Use Case 4: Response on Discovered System Configuration Change
- Use Case 5: Response on Deployment of New Systems in Infrastructure

All the SOCCRATES Platform components and the interfaces have been specified in deliverable D2.3[4]. This deliverable also specifies for each of the five use cases how the SOCCRATES platform provides both situational awareness and option awareness for security decision support. The software for each of the components of the SOCCRATES Platform is presented on the SOCCRATES website[5]. Much

[4] https://www.soccrates.eu/wp-content/uploads/2021/09/SOCCRATES_D2.3_20210830_FINAL.pdf

[5] https://www.SOCCRATES.eu/platform-software/

of the software is made available as open source. For the commercial products, and the software that is available under commercial license, contact information is provided.

2.2.2 SOCCRATES demonstrator

To show that the SOCCRATES platform can improve SOC and CSIRT operations a demonstration environments has been developed. The SOCCRATES demonstration environment consists of two parts (see Figure 2.2): a) a deployment of the SOCCRATES Platform and b) an Infrastructure Under Control. For the Infrastructure Under Control it was not only necessary to define and implement the IT assets, but also define a business logic model for the Business Impact Assessment. For the later we adopted the ArchiMate models of a fictitious insurance company ArchiSurance[6], which was defined by the Open Group as an example for the ArchiMate enterprise modeling language[7].

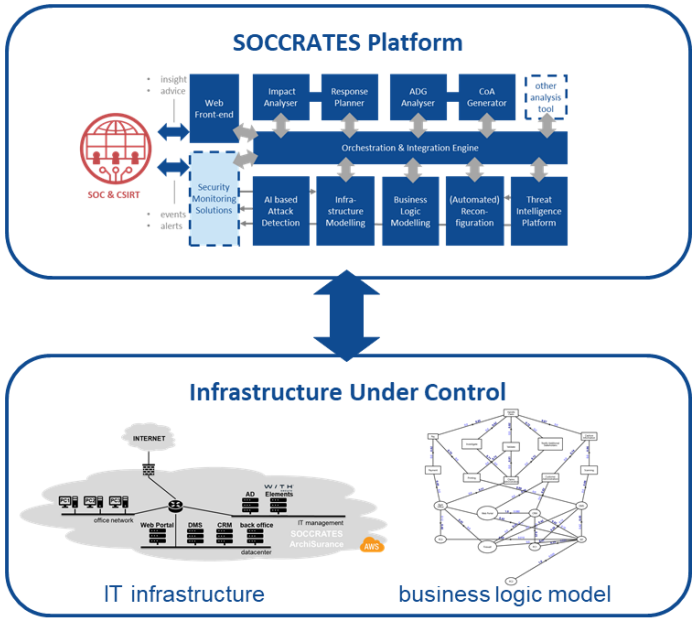


Figure 2.2: SOCCRATES demonstration environment

The Infrastructure Under Control is hosted by WithSecure on AWS and contains several workstations, servers, a firewall, Active Directory and WithSecure products (i.e. WithSecure Elements Vulnerability Scanner, WithSecure Elements Endpoint Protection and WithSecure Elements Endpoint Detection And Response (EDR). The SOCCRATES Platform has been deployed to operate on the Infrastructure Under Control It consists of the following deployments:

- *ADG Analyser* deployed in AWS hosted by foreseeti,
- *TIP* and *IMC* deployed in AWS hosted by mnemonic,
- Threat Data collection & AI based threat prediction deployed at Shadowserver, and
- rest of *SOCCRATES Platform* deployed in Azure hosted by TNO.

In Figure 2.3 the deployment concept of the SOCCRATES Demonstration Environment has been depicted.

[6] https://github.com/archimate-models/archisurance

[7] https://www.archimatetool.com/

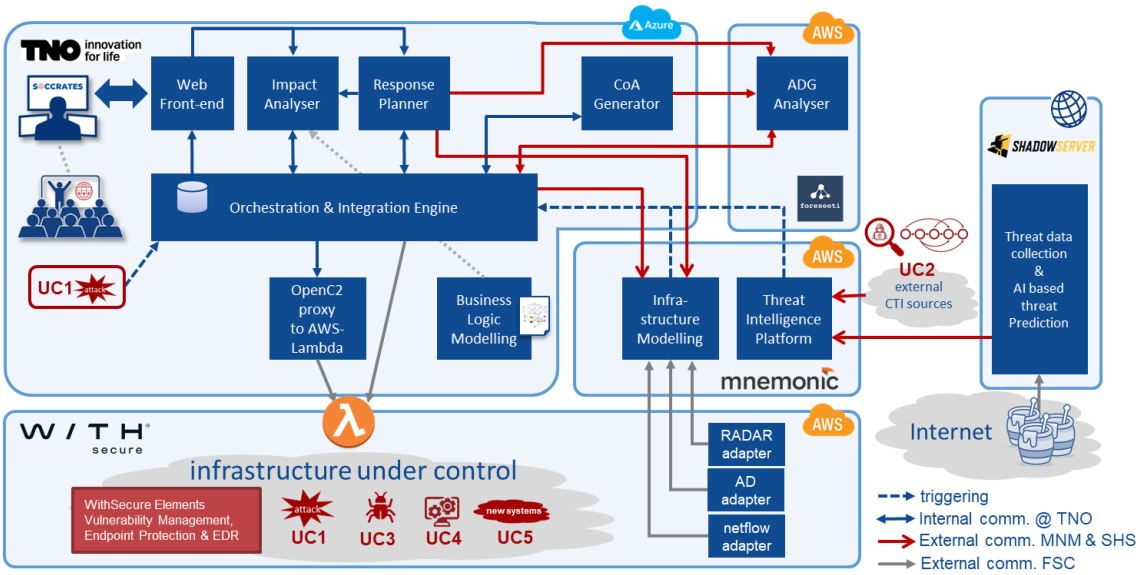


Figure 2.3 : Overview of the SOCCRATES Demonstration environment.

The SOCCRATES Platform Demonstration environment has be setup to demonstrate SOCCRATES use cases 1 (three scenario's), 2 and 3 (see Figure 2.4). The SOCCRATES Front End has been extended to easily trigger these use cases. A screen shot of this page is given in Figure 2.5.

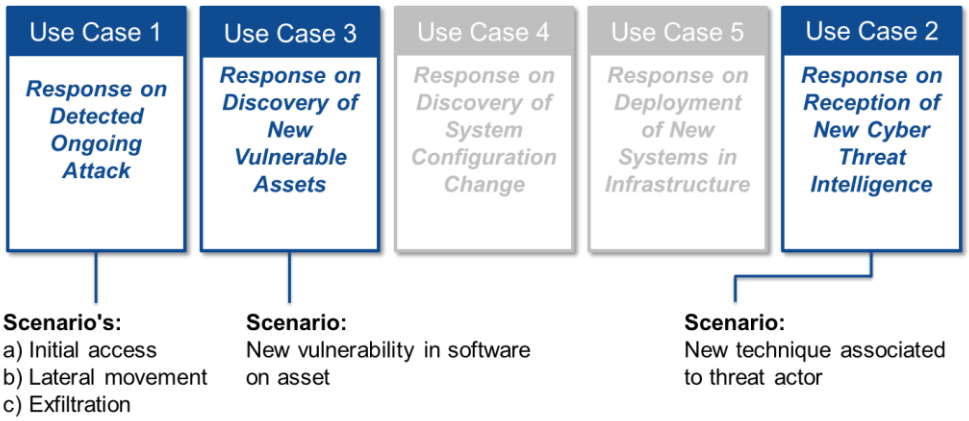


Figure 2.4: SOCCRATES Platform Demonstration use cases.

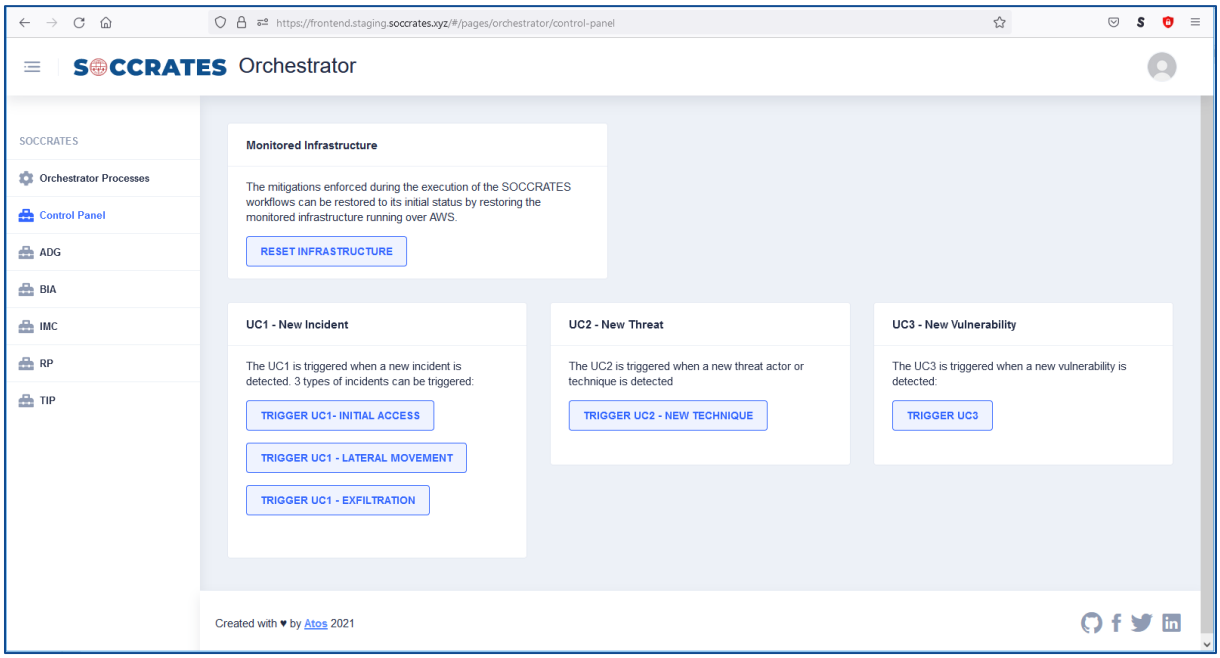


Figure 2.5: Screen shot of the SOCCRATES Front End for triggering the demonstration use cases.

2.2.3 ADG Analyser

The Attack Defence Graph Analyser consists of three parts:

- The Domain Specific Language that specifies the Attack Defence Evaluation logic
- The Attack Defence Graph Cortex Analyzer.
- A SOCCRATES version of securiCAD Enterprise

The Domain Specific Language that specifies the Attack Defence Evaluation logic

The Domain Specific Language is the part of the Attack Defence Graph Component that specifies the Attack Defence Evaluation Logic. I.e.

- How the Attack Defence Graph Model is constructed
- The capabilities of the attacker in the Attack Defence Graph Analysis
- The capabilities/impacts of defences of the objects and defences in the model

The Domain Specific Language CoreLang, that has been further developed within the SOCCRATES project to conduct better analyses and to accommodate for better interaction within the SOCCRATES Platform and other SOCCRATES Components, has been open sourced under the Apache License, Version 2.0[8].

The Attack Defence Graph Cortex Analyzer

The Attack Defence Graph Cortex Analyzer enables the Attack Defence Graph Component to interact with the SOCCRATES Platform and other SOCCRATES Components.

A SOCCRATES version of securiCAD Enterprise

The Attack Defence Graph Evaluations, as specified by the Domain Specific Language, are practically run on a SOCCRATES version of securiCAD Enterprise. securiCAD is Background IP to the SOCCRATES project, as specified in the Consortium Agreement.

[8] https://mal-lang.org/coreLang/

2.2.4 DGA detective

DGA Detective is a stand-alone tool developed by TNO and SHS to classify DGA domains at scale. The tool has been published as open-source by TNO under the Apache 2.0 license at https://github.com/COSSAS/dgad.

The tool implements functionality to perform training and classification of DGA domains. It comes with a default model trained with SHS data, allowing a user that is lacking a training set to quickly be able to classify domains. It uses a Temporal Convolutional Network (TCN) to obtain it's results.

It can classify domains from the command line, in a batch mode from a file or over a network with an API.

It was scaled up a number of domains to be able to operate on large sets of domains in an operational environment, specifically the SHS sandbox.
The detected domains and associated malware information have been made available to SOCCRATES project partners for the SOCCRATES platform pilots. But also to external trusted Internet Defender parties, such as National CSIRTs. They can now query a newly developed set of API methods (see also 2.2.12) to obtain results on the latest DNS domain classifications. The newly detected domains can then be used as enrichment in Threat Intelligence Platforms (TIPs) or added to filter/block lists to protect users.
The successful SOCCRATES outputs have delivered real world operational results at scale and have already improved situational awareness of global cyber security threats.

For more details on the inner workings of the developed framework and DGA Detective as well as examples of real world results, please read D4.3 Threat Identification and Threat Trend Prediction - Final Prototype[9].

2.2.5 AAD

Approaches to detecting cyber-attacks using machine learning techniques is being widely explored in the research community and there are several commercial solutions on the market. Many of these solutions aim to detect anomalies that could indicate the presence of a cyber-attack using different data sources that are collected from computer systems and networks. In the SOCCRATES project, partners introduced their anomaly detection solutions to be integrated into an *Advanced* Anomaly Detection (AAD) system. The goal was to address two main challenges that are associated with Anomaly Detection (AD) systems – i) the number of false alarms they can generate; and ii) bridging the gap between an anomaly being detected and determining a suitable Course of Action (CoA).

[9] https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES_D4.3-Threat-Identification-and-Threat-Trend-prediction-%E2%80%93-Final-Prototype-Final.pdf

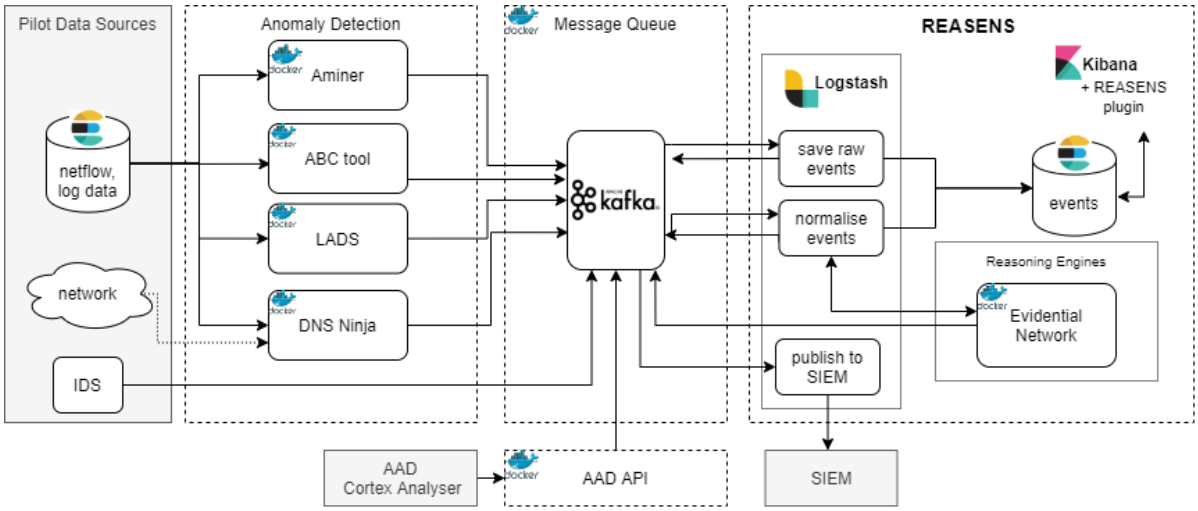


Figure 2.6: An overview of the SOCCRATES AAD

The AAD is a set of loosely coupled anomaly detection systems (e.g. AMiner, ABC tool, LADS and DNS Ninja, as shown in Figure 2.6) that are integrated using the Elastic Stack with a system, which can be used to aggregate and infer the root cause of anomalies, called REASENS. At the centre of REASENS is an inference engine that is based on Evidential Networks (ENs). In addition to the integration of anomaly detection tools, a bespoke EN has been developed that can be used to infer the nature of an attack that is "described" by the anomaly detection systems. The EN provides inferences about whether the observed anomalies pertain to *initial access, lateral movement,* or *data exfiltration*. There are corresponding incident response playbooks (CoAs) that can be triggered with the insights provided by the AAD. Inferences are accompanied by a likelihood, which is derived from expert knowledge and a so-called Positive Predictive Value (PPV), which is derived from the performance of the detectors (i.e. False Positive and False Negative Rates). In this way, the AAD can support SOC analysts in both managing the false positives associated with AD systems and moving more directly to an appropriate CoA.

2.2.6 ACT SOCCRATES improvements

The ACT platform[10] was taken into SOCCRATES as an existing tool for collecting and processing cyber threat information. The ACT platform has been further developed in the scope of SOCCRATES with new object types, better user guidance and an improved deployment process. Furthermore, the ACT platform now supports the Shadowserver Threat Data Collection & Threat Prediction component as an enrichment source.

2.2.7 Infrastructure Modelling Component(IMC)

An infrastructure modelling tool[11] has been developed with the ability to represent nodes in an infrastructure as a graph. The tool uses the graph database from the ACT platform. The tool consumes connections and relationships between infrastructure components, represents this in a graph, and provides the opportunity to query the graph with the query language Gremlin[12].

[10] https://github.com/mnemonic-no/act-platform

[11] https://github.com/mnemonic-no/act-types-imc

[12] https://tinkerpop.apache.org/gremlin.html

2.2.8 Adversary Emulation Planner (AEP)

A need for Adversary Emulation Plans emerged in the project, and the operational flow of such plans were in need of being identified and represented in a structured manner. Mnemonic created the Adversary Emulation Planner (AEP)[13] to take a set of Mitre ATT&CK techniques and create useful and possible sequences of them to emulate actual adversary behaviour. An example of the output from the tool, with the input from the SolarWinds incident[14], is shown in Figure 2.7. A detailed description of the AEP can be found in D4.4 Tactical Threat Intelligence for Attack Defence Graphs[15] .

stage	techniques	new promises @end-of-stage	tactics
Attack stage 1	Develop Capabilities (Resource Development) Develop Capabilities:Malware (Resource Development) Domain Trust Discovery (Discovery) Obtain Capabilities (Resource Development) Obtain Capabilities:Code Signing Certificates (Resource Development) Supply Chain Compromise (Initial Access) Supply Chain Compromise:Compromise Software Supply Chain (Initial Access)	exploit_available info_domain_trust infrastructure_certificate privileges_user_local tool_available tool_delivery	Discovery Initial Access Resource Development
Attack stage 2	Command and Scripting Interpreter (Execution) Command and Scripting Interpreter:PowerShell (Execution) Command and Scripting Interpreter:Windows Command Shell (Execution) Scheduled Task/Job (Execution,Persistence,Privilege Escalation)	defense_evasion execute_code file_transfer persistence	Execution Persistence Privilege Escalation
Attack stage 3	Application Layer Protocol (Command and Control) Application Layer Protocol:Web Protocols (Command and Control)	access_filesystem access_host access_network command_and_control	Command and Control
Attack stage 4	Account Discovery: Local Account (Discovery) Dynamic Resolution (Command and Control) [*] Dynamic Resolution:Domain Generation Algorithms (Command and Control) [*] Event Triggered Execution (Persistence,Privilege Escalation) [*] Ingress Tool Transfer (Command and Control) [*] Permission Groups Discovery (Discovery) Permission Groups Discovery:Domain Groups (Discovery) Process Discovery (Discovery) Unsecured Credentials (Credential Access) Unsecured Credentials:Private Keys (Credential Access)	credentials_user_domain credentials_user_local credentials_user_thirdparty info_groupname info_process_info info_target_employee info_username	Command and Control Credential Access Discovery Persistence Privilege Escalation
Attack stage 5	Account Manipulation:Additional Cloud Credentials (Persistence) [*] Cloud Service Discovery (Discovery) Email Collection:Remote Email Collection (Collection)	info_cloud_services privileges_user_domain target_information	Collection Discovery Persistence
Attack stage 6	Archive Collected Data (Collection) Archive Collected Data:Archive via Utility (Collection) Data Staged (Collection) Data Staged:Remote Data Staging (Collection) Exfiltration Over Web Service (Exfiltration)	objective_exfiltration staged_data	Collection Exfiltration

Figure 2.7: Output from the Adversary Emulation Planner with inputs from the SolarWinds incident.

2.2.9 Contributions to MITRE ATT&CK

Through the work with the Adversary Emulation Planner (AEP, see previous paragraph), mnemonic did extensive work with the MITRE ATT&CK knowledgebase. As a results, improvement suggestions were submitted and approved and are now part of the published version of the well-known (and widely used) MITRE ATT&CK framework:

- https://attack.mitre.org/techniques/T1588/002/

2.2.10 Pilot results

First and foremost, deployment of all components in the mnemonic pilot environment has led to extensive increase in tooling available for automation in (especially mnemonic and Vattenfall) SOC processes, which has increased the service level for SOC operations and the ability to further develop in new research and collaboration projects due to identified gaps in our own tooling.

[13] https://github.com/mnemonic-no/aep

[14] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[15] https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES_D4.4_final.pdf

Mnemonic learned from coordinating the pilots and being pilot site for both first and second pilot. The main learnings from this are:

1. Increased understanding of automation in the SOC processes
2. Increased knowledge and experience with use of technologies such as Gitlab, Docker Containers and Docker Swarm.

Experience with project management in research projects with a significant amount of project partners.

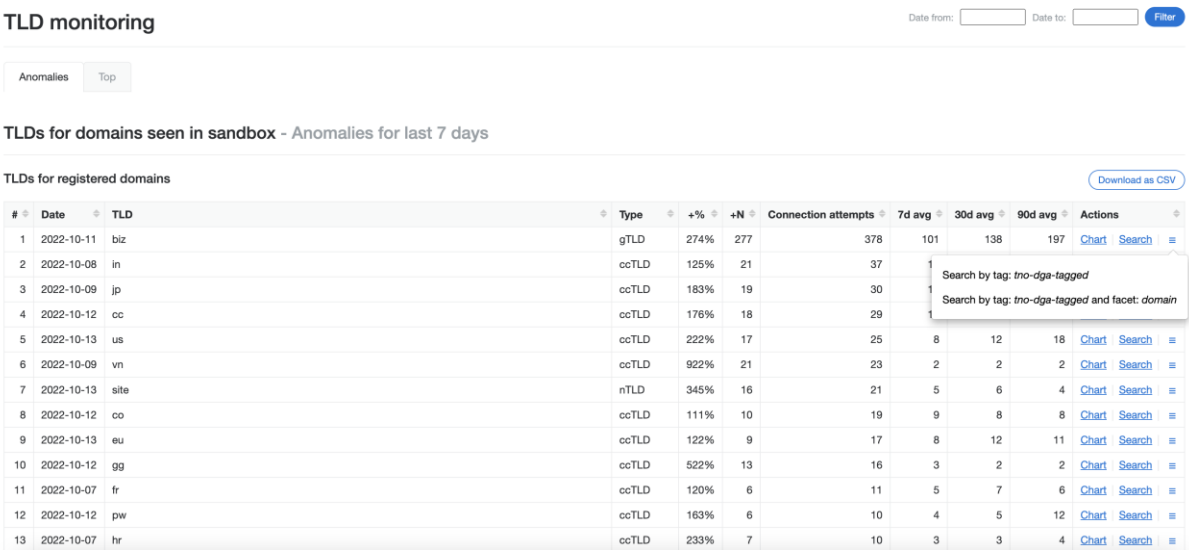
2.2.11 Platform for hunting malicious domains in sandbox environment

SHS built an internal dashboard and a number of support mechanisms to better explore anomalies and trends in their sandbox data, with a focus on malicious domains and DGAs. These include the results supplied by DGA Detective running in an operational environment. The goal was to have a set of tools supported by machine learning to enable effective threat alerting and hunting, which can also be used for future post-project exploitation of results.

The internal dashboard signals anomalies and trends in the following DNS related sandbox activity, and facilitates their exploration:

- TLD monitoring (see Figure 2.8)
- DoH/DoT usage monitoring
- Registrar usage monitoring

The dashboard is supported by daily e-mail reports of unregistered domains (including blockchain based domains) to analysts.



#	Date	TLD	Type	+%	+N	Connection attempts	7d avg	30d avg	90d avg	Actions
1	2022-10-11	biz	gTLD	274%	277	378	101	138	197	Chart Search
2	2022-10-08	in	ccTLD	125%	21	37	1			
3	2022-10-09	jp	ccTLD	183%	19	30	1			
4	2022-10-12	cc	ccTLD	176%	18	29	1			
5	2022-10-13	us	ccTLD	222%	17	25	8	12	18	Chart Search
6	2022-10-09	vn	ccTLD	922%	21	23	2	2	2	Chart Search
7	2022-10-13	site	nTLD	345%	16	21	5	6	4	Chart Search
8	2022-10-12	co	ccTLD	111%	10	19	9	8	8	Chart Search
9	2022-10-13	eu	ccTLD	122%	9	17	8	12	11	Chart Search
10	2022-10-12	gg	ccTLD	522%	13	16	3	2	2	Chart Search
11	2022-10-07	fr	ccTLD	120%	6	11	5	7	6	Chart Search
12	2022-10-12	pw	ccTLD	163%	6	10	4	5	12	Chart Search
13	2022-10-07	hr	ccTLD	233%	7	10	3	3	4	Chart Search

Figure 2.8: : Dashboard showing anomalies in recent TLD abuse

2.2.12 Shadowserver SOCCRATES API

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 SOCCRATES deliverables D2.3[16] and D4.3[17].

2.2.13 SOCCRATES orchestrator

The SOCCRATES Orchestrator and Integration Engine is an asset developed by Atos in the project to manage and orchestrate the interoperation among the SOCCRATES components throughout different workflows associated to common incident response situations. It has been designed making use of different existing open-source solutions, in particular the BPMN (Business Process Model and Notation) workflow engine Activiti[18] and Cortex[19], a tool developed in TheHive project to orchestrate the execution of analyzers.

Two BPMN files have been created with the workflows that cover five Use Cases considered in SOCCRATES, one to be followed after the detection of an ongoing attack (Use Case1) and other that covers the Use Cases 2 to 5 (reception of a new Cyber Threat Intelligence information, detection of a new vulnerability in an asset, detection of changes in the system configuration and detection of the deployment of new system in the infrastructure). These BPMN files are published on the SOCCRATES website.

The SOCCRATES Orchestrator and Integration Engine receives the triggering messages to start in Activiti some of these Use Cases workflows. Through the execution of the different SOCCRATES Cortex analyzers and responders associated to each component of the SOCCRATES platform, the invocation is performed of the required functions included in the security incident response workflows. More details about this asset can be found in SOCCRATES deliverables D6.1[20] and D6.2[21].

The interaction with the workflows executing in the SOCCRATES orchestrator by the SOC/CSIRT analysts is done using the SOCCRATES Web Front-end. This is a web portal that provides access to the analysts not only to the status of the different workflows and the results of the different analysis performed by the platform but also to the user interfaces of the different SOCCRATES components (ADG, BIA, RP, IMC, TIP). Atos has developed this asset purpose-built reaching a TRL 5 by the end of the project. More details about the SOCCRATES Web Frontend can be found in SOCCRATES deliverable D6.4.

2.2.14 Webhook Notification Cortex Responder

The Webhook Notification Cortex Responder is part of the Automated Reconfiguration (AR) component and it provides the SOCCRATES platform with the capability of sending information about the Course of Actions selected by the SOC/CSIRT analysts and relevant information about the workflow running in the SOCCRATES Orchestrator to any external webhook endpoint using a predefined JSON format. In this way, it can be integrated with any SOC/CSIRT tool to receive these webhook

[16] https://www.soccrates.eu/wp-content/uploads/2021/09/SOCCRATES_D2.3_20210830_FINAL.pdf

[17] https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES_D4.3-Threat-Identification-and-Threat-Trend-prediction-%E2%80%93-Final-Prototype-Final.pdf

[18] https://www.activiti.org

[19] https://github.com/TheHive-Project/Cortex

[20] https://www.soccrates.eu/wp-content/uploads/2020/12/SOCCRATES_D6.1-Initial-version-of-the-SOCCRATES-Platform-final.pdf

[21] https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES_D6.2_v1.0-FINAL.pdf

notifications and act in consequence. For example, the notification could be just logged for auditing purposes or it could be opening a ticket or executing some action in an external third-party SOAR. More details about this responder can be found in SOCCRATES deliverable D2.3[22]. A great achievement is that this responder will be included in TheHive project Cortex responders repository[23].

2.2.15 CACAO playbook Cortex responder

At the end of its execution run, the Response Planner (Section 2.2.21) will produce a playbook, setting out all the steps that should be taken to mitigate the security event. These steps can be either manual steps that for instance require a SOC analyst to execute a certain task, or an automated task. The playbook produced by the Response Planner is written using the OASIS Collaborative Automated Course of Action Operations (CACAO) standard, an open standard to implement the course of action playbook model for cybersecurity operations, developed and maintained by OASIS Open.

The CACAO playbook is sent to the CACAO playbook Cortex responder, which parses it, iterates over the steps prescribed within the playbook, and extracts the automated tasks. These automated tasks are defined as commands in the OpenC2 language, another open standard of OASIS Open, a standardized language for the command and control of cyber defence technologies using JSON as a data-interchange format. The OpenC2 commands are then sent to the OpenC2 proxy, which on its turn parses them, and translates them to AWS Lambda calls in the Infrastructure under Control (demonstrated by Figure 2.9). Available actions in the current Infrastructure under Control are:

1. to contain an asset through the Endpoint Protection tool running on the asset, or
2. to drop traffic (by addition of firewall rules) to the asset.

These actions can be extended, both in the CACAO playbook as well as in the OpenC2 language, and may serve as contributions to these open standards.

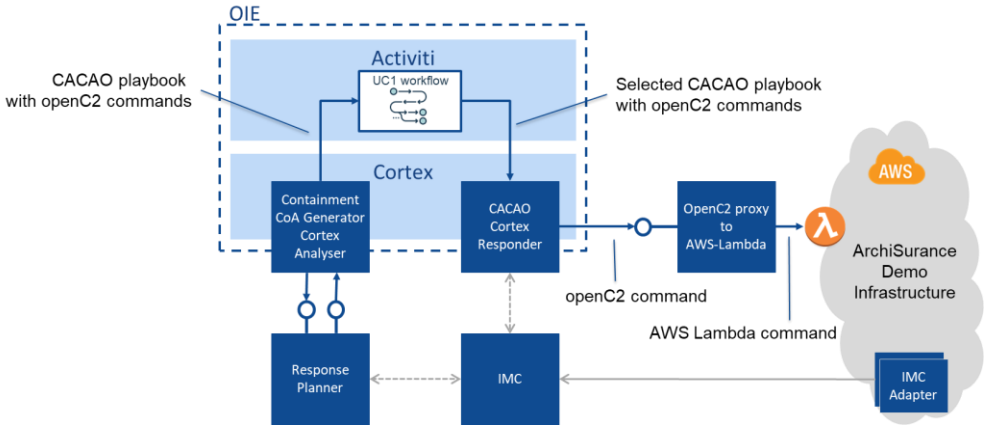


Figure 2.9: CACAO Cortex Responder

2.2.16 L-ADS

The L-ADS (Live Anomaly Detection System) is a tool based on a Deep Learning algorithm that aims to identify possible anomalies in a given internal network. It learns from the legit traffic used to train the algorithm and evaluates the new incoming traffic. If the difference is significant, this new incoming traffic can be classified as an anomaly. For more details, please consult SOCCRATES deliverable D4.1[24].

[22] https://www.soccrates.eu/wp-content/uploads/2021/09/SOCCRATES_D2.3_20210830_FINAL.pdf

[23] https://github.com/TheHive-Project/Cortex-Analyzers

[24] https://www.soccrates.eu/wp-content/uploads/2020/12/SOCCRATES_D4.1_FINAL_Version2.pdf

Initially the asset was able to capture traffic through the Softflowd tool, which is an implementation of Netflow. However, for SOCCRATES, the asset has been modified to work in the same manner as the rest of the AAD components. For this, the Netflow traffic coming from the ElasticSearch is used as input instead of the Softflowd tool.

In terms of the progress made for SOCCRATES, two different versions have been implemented in the L-ADS. One of them without filters on the IPs and the other one allows the generation of a Deep Learning model for specific IPs. This second version facilitates a specific model with less noise in the data for a specific IP or range of IPs.

In addition, the L-ADS asset has been adapted to be deployed by the Docker Swarm tool. This is a necessary step to complete the integration with the rest of the components. Atos has developed this asset to reach a TRL 5.

2.2.17 SOCCRATES website (after the project)

TNO will keep the SOCCRATES website on-line for at least 5 years after the project ends. It will not be updated anymore, but it will offer access to all SOCCRATES results that were achieved. This includes the project's deliverables but also an overview of the SOCCRATES platform software and videos of the 10 webinars that the project ran throughout its course.

2.2.18 Organising exercises and education (for analyst staff) with the SOCCRATES knowledge

It is well-understood that there is a cyber security skills shortage in Europe and further afield. In the context of a multi-faceted approach to addressing this issue, suitable training materials and exercises are required. The Security Operations Centre (SOC) is central to many organization's approach to managing the cyber security problem. Consequently, suitable training and exercise materials that can be used to educate professionals on this topic is important. To this end, the AIT has developed training courses that focus on SOCs, building on the experiences and knowledge that has been created in the SOCCRATES project. For example, a one-week long course has been created that includes topics such as SOC technologies (IDS, SIEM and SOAR solutions), SOC organizational structures, security playbooks, etc. The training course makes use of AIT's Cyber Range to provide hands-on exercises, concluding with a half-day incident response exercise[25].

2.2.19 CoA generator

The Course of Action (CoA) generator component operates on a model developed in in a domain specific language compatible with the ADG component. In this project the domain specific language has been CoreLang (described just above). The CoA generator component searches for "inactive defences" in the model and suggests to activate a set of them that have been identified as the most effective. The set of defences is restricted by an assumed overall budget and assumed costs for activating each of the different defences. In SOCCRATES this is used to suggest defences to improve the security of ICT infrastructure to an SOC analyst. In order to do this the CoA generator forms a feedback

[25] https://www.ait.ac.at/en/research-topics/cyber-security/ait-cyber-range-training

loop with the ADG analyser. To drive the optimization process, the CoA generator uses the attack graph from the ADG component to compute a partial response to the analysed threat, runs the ADG analyser to obtain the expected behaviour of the attacker under this partial response, and then repeats the procedure on the newly obtained attack path. When the available budget is spent, the overall result with one or more defence actions are suggested to the SOC analyst who then can choose to implement the suggested defences (or not). The CoA generator can take any number of cost types (e.g. CAPEX, OPEX, implementation time) into account simultaneously. It can also implement schemes of increasing or decreasing cost depending on how many times a certain type of defence is activated. In the project demonstration only the basic capability of static costs in a single dimension has been used.

2.2.20 BIA

The main objective of the Business Impact Analyser (BIA) was to generate metrics that allow the SOC analyst to evaluate the operational impact and the level of emergency of an external event, such as an attack or a mitigation deployment, on one or several infrastructure assets. The BIA that was developed during the SOCCRATES project fulfilled this objective, through the production of the following metrics:

- Impact probability on the business functions, processes, and on the company as a whole
- Downtime tolerance before the impact propagates to the various business functions and processes
- Criticality value of each asset

To do so, the BIA first needs to build a model, based on a manually designed model of the business functions and processes of the company on one hand, and on the traffic volume between assets on the other hand. After each business impact analysis request, the BIA displays the model and the computed metrics on an interactive graphical interface, that gives an overview of the impact of the event on the whole business functions and processes, allowing a SOC analyst to immediately pinpoint the entities on which the impact is the most critical. Moreover, the analyst can manually edit values and nodes on the graphical interface and observe the consequences on the impacts, in order to further investigate an issue. The graphical interface of the BIA is shown on Figure 2.9.

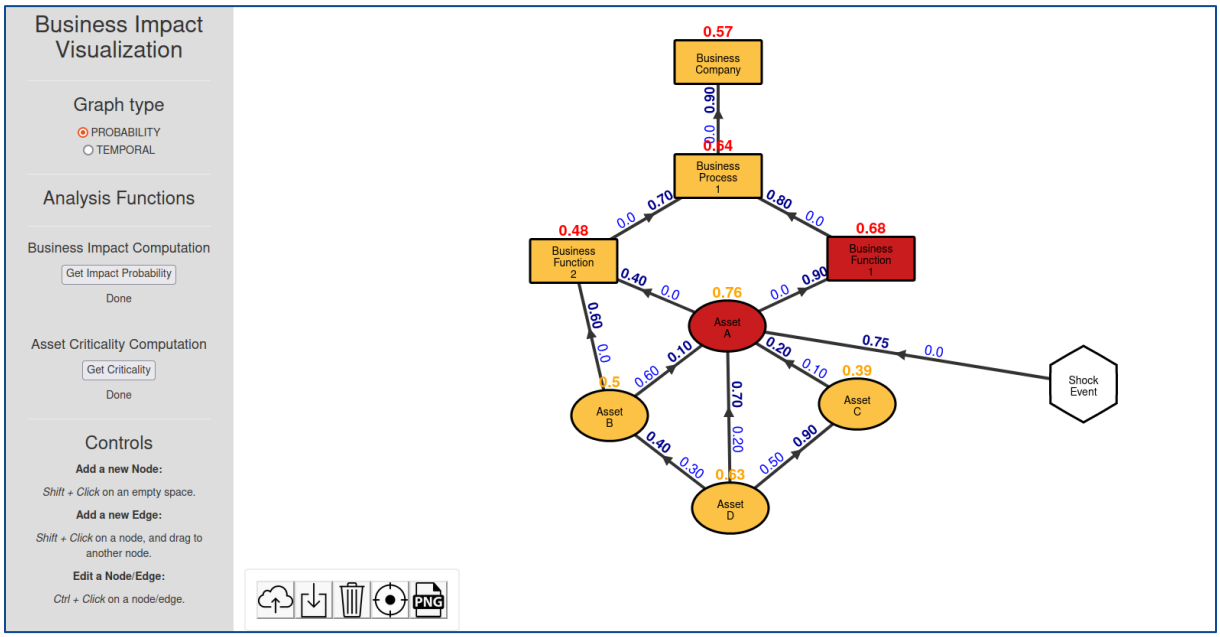


Figure 2.9: : Business impact computation on the BIA

2.2.21 Response planner

The Response Planner (RP) is a component that fulfils two objectives:

- Evaluation of the financial impact of a CoA with the Return On Response Investment (RORI) metric;
- Generation of containment CoAs that can be deployed in an automated way.

The RORI metric aims to allow an operator to rank CoAs according to the long term, financial impact on the company. A negative value indicates that it is not viable deploying the CoA (for example if the attack does not represent a major threat, while the CoA is very costly), whereas a positive value indicates that it is financially beneficial for the company to deploy the CoA – the higher the RORI value, the more beneficial it is.

In the case of real time attack detection, the RP will also generate containment CoAs, which are specific CoAs meant to stop the progression of the attack with immediate effect. Since these CoAs have to be deployed as quickly as possible, the RP generates OpenC2 commands inside a CACAO playbook, so that the deployment of these CoAs can be fully automated, hence providing an immediate emergency response to an ongoing attack.

2.3 Other results

2.3.1 Experience with complex software development

It is worthwhile to discuss the many challenges and lessons learned in developing the software behind the SOCCRATES platform. The KISS principle[26] remains a pearl of wisdom. However, it is not trivial to apply it to complex, heterogeneous software systems. The reality is that some complexity must exist when multiple units of software have to interact with each other. The challenge then becomes where to move the complexity and how to deal with it. This should be dealt with when designing the platform architecture. In SOCCRATES, we designed a system based on the idea that work packages could work on modular components.

[26] https://en.wikipedia.org/wiki/KISS_principle

However, in hindsight we fell short on two topics :

1. The abstraction layer did not capture underlying complexity of the software well enough and
2. The software architecture (a mesh of microservices calling each other) did not allow for true asynchronous and independent work of the work packages. This required continuous alignment and synchronization of the inevitable changes (no battle plan survives impact with the enemy).

These topics, combined with the fact that the SOCCRATEs platform turned out to be even more complex than anticipated, and the COVID pandemic that prevented developers to meet in F2F implementing sessions, led to delays and the need to find alternative ways to gather pilot experiences pilot the platform appropriately.

Collaborative software development is not trivial. It is a well-known fact that source code should be stored in central repositories and versioned automatically through version control systems such as git. However, it is not necessarily obvious to understand what should and should not go together in a same repositories. Should artifacts go in a same repository because the team of people that works on it is the same (the so called monorepo approach), or should artifacts always be in different repositories (the so called polyrepo approach)? Early on, SOCCRATES software architecture and work package management intuitively led to the work packages setting up their own monorepo repositories. We discovered that there are at least two reasons why this was a bad choice:

1. Monorepos make it harder to track and revert changes to individual sub-components
2. Continuous Integration and Continuous Deployment (CI/CD) pipelines rebuild all sub-components, even if changes are made only to one, leading to longer than necessary pipeline durations
3. CI/CD pipelines redeploy all components, even if changes are made only to one, leading to higher resources usage (and thus costs).

The AAD (Advanced Anomaly Detection) component started as a monorepo but was split in smaller polyrepos. The OIE (Orchestration and Integration Engine) was also started as a monorepo, and due to its complexity it has been kept as a monorepo. The development team of the AAD benefited greatly from the split, whereas the development team of the OIE has suffered the pains described above until the end of the project. The important takeaway here is that splitting labour in work packages is a required but not sufficient activity. It has to be coupled with an integrated technical implementation process, to avoid work packages operating in silos. Silos mentality creates other kinds of inefficient labour. For example, 3 separate components rely and deploy Elasticsearch (a popular noSql database technology) deployments: 1 in the OIE, 1 in the IMC&TIP and 1 in the AAD. Elasticsearch is not trivial to setup and configure, especially when deployed to be highly available and performant. Three teams roughly ended up doing the same thing. It would have been much better if a central Elasticsearch cluster was set up for all components to use. But each silo made the decision to use Elasticsearch individually. The lesson learned here is that a complex software project should have a dedicated central work package involving all developers that is orthogonal and complementary to more research/budget oriented work packages.
When the architecture allows for it, components of a larger system can be implemented by different teams. Teams skills and culture, when working in silos, can be very different. In SOCCRATES we have experienced that it is not obvious that the developers of a system are their owners. Clear ownership

(and agreement on its implication) of each component is a *'conditio sine qua non'* to a successful and smooth integration of components delivered by different teams. Alignment on the cultural and practical meaning of ownership are therefore mandatory and should be ironed out as early as possible in such a project. A mentality of "but it works on my machine" is not a helpful one. The goal should be to adopt the following devops approach to ownership: "you build it, you deploy it, you monitor it". In other words, it is not sufficient for developers to provide source code and call it a day. Developers must provide: source code, its unit tests, its reproduceable deployment as code. The lesson we have learned here is that such a culture must be established and agreed explicitly as early as possible. Technology exists to facilitate enforcement, however it is not fruitful on its own. Establishing this culture and expectation should be a key activity of an aforementioned "orthogonal" software development work package. Whereas implementation choices are sole responsibility of the developers, operational choices need to be collective. The operational tech stack should thus be chosen and communicated appropriately as early as possible, so that there is sufficient time to fill any knowledge gaps. Software quality should be enforced by making unit tests and an appropriate level of code coverage strict requirements.

Continuous Integration and Continuous Deployment are critical to bridge the aforementioned natural gap between development (writing features in source code) and operations (deploy and monitor that source code) and to enforce requirements established from culture. Continuous integration should be used to run unit tests whenever the source code is altered. In SOCCRATES there was no requirement on delivering unit tests, which lead to most bugs being discovered during or after deployment at the pilot sites. The earliest a developer becomes aware of a bug, the earliest he can fix it. Bug discovery should happen not only as temporally close as possible to the developer, but also spatially (virtually) close to him. A bug discovered at a pilot site can be hard to reproduce and describe, especially if, like in SOCCRATES, developers are not allowed to access that environment directly. A bug discovered through a unit test performed in continuous integration, instead, is trivial to reproduce. If we did not make the most out of Continuous Integration, we ended up benefiting substantially from Continuous Deployment. Unfortunately, this was introduced too late, just a few months before the pilots. It took time to perfect it and it reached a satisfactory state only by the end of the project. Our continuous deployment setup allows developers with no understanding of containerized software operations to test and deploy their changes automatically into a staging environment. The setup includes a container management solution that allows developers to monitor, among other things, logs and performance. Every project like SOCCRATES should rely on a similar continuous deployment solution. For all its benefits, continuous deployment requires an infrastructure to happen. Setup and maintenance of such an infrastructure on premise can be expensive, especially in terms of time.

Finally, last but not least, we have learned the importance of tools such as Gitlab to asynchronously collaborate on large software projects with a large group of developers, operators and testers. These tools can be double edged swords. They are powerful in that they allow to organize and monitor multi stage activities, to define dependencies, assign tasks with deadlines and automate all kinds of testing. The downside of such power is that it is not trivial to make the most out of it, and they can have a pretty steep learning curve. Furthermore, there can be different personal and cultural expectations in communication etiquette. In SOCCRATES we used Gitlab to collaborate on more than

software, leading to an even larger and heterogeneous user group. A solution to this downside is to train the entire project team formally (through workshops by a third party for instance) early on.

2.3.2 Follow-up proposal in Horizon Europe

Six of the SOCCRATES partners are involved in a drafting a project proposal for the call HORIZON-CL3-2022-CS-01-01 - *Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures*. The proposal builds on the SOCCRATES results, but with additional partners we will also build on results of other EU funded projects and we will extend the scope of innovation to include the OT domain. The required TRL level of this proposal is TRL 7, this perfectly aligns with the results of SOCCRATES (which were required to be TRL 6).

2.4 Modes of Exploitation

2.4.1 Publication of Open Source Software

Parts of the SOCCRATES innovations are implemented in software and made available as Open Source software. We have made use of the COSSAS platform (a TNO initiative) and more general Open Source platforms to publish these results.

2.4.1.1 Open Source Platform (COSSAS)

COSSAS[27] is an open source community initiative specifically oriented at automation solutions for cyber security operations. Its constituency is comprised of SOC, CERT and CTI professionals, which corresponds exactly to the prime target audience of the SOCCRATES project. COSSAS features an ever expanding base of novel software solutions for cyber security automation that are subjected to strict quality evaluations before they are released. The initiative was launched by TNO and is actively supported by parties such as dcypher (a Dutch collaboration platform for cyber security innovation) and CIRCL (the national incident response centre in Luxemburg).

COSSAS features two software components that were developed in the SOCCRATES project:

- The **DGA Detective** software, developed by TNO and Shadowserver, was directly incorporated in the COSSAS software portfolio and is maintained in the native COSSAS GitHub space.
  see: https://cossas-project.org/portfolio/dgad/
- The **Adversary Emulation Planner** software was developed and released as open source by mnemonic. The software is maintained in mnemonic's own GitHub repository and showcased by COSSAS as a "partner product".
  see: https://cossas-project.org/partner-software/

By employing COSSAS as its open source channel, the project managed to bring these software components to the direct attention of their intended end user base. COSSAS will also ensure continued attention for the maintenance, enhancement and adoption of these component after the project has been finalized.

[27] Community for Open Source Security Automation Software

2.4.1.2 General Open Source channels

Several partners have setup Open Source channels on general Internet hosting services for open source software development projects, such as github.com and gitlab.com. In the table below an overview is given of the open source channels used for the SOCCRATES project.

Table 2.1 Open Source channels used for the SOCCRATES project

Partner	Open Source channel
AIT	https://github.com/ait-aecid/
IMT	https://gitlab.com/tsp-SOCCRATES-components/
KTH & FRS	https://github.com/mal-lang/
MNM	https://github.com/mnemonic/
TNO	https://github.com/COSSAS/ https://gitlab.com/cossas/ https://github.com/TNO/
WithSecure	https://github.com/withsecurelabs/

2.4.2 Standardization

At least three initiatives have led to (industry) standardization results:

- TNO became member of OASIS Open - TC openC2 and TC CACAO[28] and shared information from the SOCCRATES project to the group.
- The project coordinator was appointed as a member of the Enisa ad-hoc working group on SOC/CSIRT[29] 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.[30]

2.4.3 New and enhanced products and services

Some SOCCRATES innovations have led to enhancement of existing (commercial) products and services (e.g. ADG Analyser)

The ADG Analyser consists of three parts as described under section 2.2.3

- The Domain Specific Language that specifies the Attack Defence Evaluation logic.
- The Attack Defence Graph Cortex Analyzer
- A SOCCRATES version of securiCAD Enterprise

The ADG Analyzer includes both project results and background IP.

- The Domain Specific Language CoreLang, has been further developed within the SOCCRATES project. Developed by both KTH and Foreseeti. CoreLang has been open sourced under the Apache License, Version 2.0.

[28] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao

[29] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/ad-hoc-working-group-on-socs

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

- The Attack Defence Graph Cortex Analyzer has been fully developed within SOCCRATES project. Developed by Foreseeti.
- The SOCCRATES version of securiCAD Enterprise is a specific version of securiCAD Enterprise. The existing background product - securiCAD - is Background IP, owned by Foreseeti. The developments are done by Foreseeti.

Foreseeti support project exploitation in line with project and consortium agreements. This includes both Attack Defence Graph Cortex Analyzer and the SOCCRATES version of securiCAD Enterprise as of end of project. During the project term, Foreseeti was acquired by Google Cloud EMEA Ltd, a limited liability company established in Ireland. This development further advances Soccrates' project goals by increasing the potential of exploitation and dissemination of Foreseeti's securiCAD functionality through the planned integration with Google Cloud's security portfolio, which will ultimately bring greater cybersecurity protections and options to customers.

Other SOCCRATES innovations have led to the introduction of completely new tools and products, in use by SOCCRATES partners, e.g. the DGA detective (see 2.2.4) and the Orchestrator and Integration Engine with the SOCCRATES Web Frontend (see 2.2.13).

2.4.4 Knowledge development & further innovation

The innovations and knowledge developed in SOCCRATES are and will be used in future innovation projects to elaborate and expand.

AIT will exploit the results from the SOCCRATES project to develop further research and innovation (R&I) projects. For example, in the current version of the REASENS Framework the inference engine is based on an expert knowledge-based formalism, called an Evidential Network. In future projects, we will seek to explore data-driven approaches to inferring the root causes of outputs from sensors, such as AD systems. Moreover, more advanced forms of inference (e.g. using models to answer "what if?" questions) could be investigated in future R&I projects. The use of digital twins for this purpose appears promising. In the SOCCRATES project, a study on the potential risks associated with adversarial machine learning (adversarial examples, specifically) was conducted. The study highlighted that this issue could be significant in the medium-term and that more applied research, e.g. using testbeds that realize potential threat scenarios, would be beneficial. We will seek to acquire research funding that moves this topic forward, thus helping AIT to fulfil its mission to inform its key stakeholders about emerging and future risks.

TNO applies the SOCCRATES knowledge on anomaly detection and DGA detection. It will build on the DGA detector, that is published as Open Source. Also the security reasoning knowledge will be further elaborated on in future research projects, both EU funded and national (e.g. for Ministry of Defense and Dutch Tax services). Among other things, a number of SOCCRATES partners is involved in a new Horizon proposal, coordinated by TNO (call topic HORIZON-CL3-2022-CS-01-01), that focusses on synergy between IT and OT SOCs and the SOCCRATES results will be a major starting point for this project proposal. Also the knowledge and lessons learned on the CI/CD pipeline and DevOps environment will serve as a good foundation for future projects in which innovative development is needed.

KTH have recently started a project together with The Swedish Armed Forces, Swedish Defence Research Agency, and Swedish Defence Materiel Administration with the goal of demonstrating Machine Learning-based defence actors acting from a SOC. In this project the ML agent will be trained

on CoreLang-based attack graphs. At the time of writing, no other project has been granted but several project ideas that exploits the SOCCRATES results are under development.

IMT has plans to further develop the innovations of the SOCCRATES project in upcoming research and innovation projects. In particular, the theoretical model used in the Business Impact Analyser can be further improved with a finer granularity design that would generate more realistic representations of the infrastructure, accounting for redundant assets, traffic differentiation, and more generally the specificities of the various assets. On the business level, more detailed guidelines in the evaluation of the dependencies would greatly improve the applicability of the model. This could be done through the design of a new language taking over BPMN. Currently, IMT is already involved in national cybersecurity projects such as the SuperviZ project, which addresses security supervision and orchestration, or the Beyond 5G project, in which IMT is involved in cybersecurity quantification in 5G slices, thus extending the impact quantification innovations from the SOCCRATES project.

2.4.5 Education and training

To support in fighting the shortage of skilled staff, SOCCRATES results are exploited in the education and training area. This does not only mean that we support the security experts in their work with the SOCCRATES platform but also by contributing towards the training and development of graduates and operational personnel in cyber security. Educational material will be generated and brought to relevant audiences as part of the SOCCRATES communication strategy.

In this regard, the **AIT** has already begun to develop training material for professionals that builds on the knowledge that has been created in the SOCCRATES project. This material has been delivered by AIT staff to professionals from different sectors, such as electrical energy distribution system operators. In the future, these courses will be extended to includes aspects that are related to Operational Technology (OT) SOC activities and how IT/OT SOCs can be implemented. Moreover, AIT has an initiative to implement cyber security exercises using their cyber range to national and international stakeholders – the case studies, threat scenarios, and knowledge about SOC activities that have been developed in SOCCRATES will inform the design of these exercises.

KTH has no current plans to exploit SOCCRATES results in education. However, most likely they will be used in several Master thesis projects in the coming years.

IMT has been developing concrete use cases for the students to illustrate cybersecurity concepts and approaches from the SOCCRATES project. In particular, students are introduced to the automation of mitigation deployment through the OpenC2 language, as well as the use of machine learning for anomaly based intrusion detection. On top of teaching activities, IMT is active in several projects related to education and training: the ERASMUS+ funded project REWIRE, that aims at building a concrete European Cybersecurity skills strategy, and the Horizon Europe project CyberSecPro, that aims at promoting a new conceptual approach to training solutions. IMT is also part of the national project proposal TCE (Training Cyber Experts) that has been submitted.

2.4.6 Events and publications

Knowledge transfer is an important aspect of Exploitation. The knowledge we have built-up in SOCCRATES supports others in making their work more effective, their innovations more targeted and their strategic directions more clear. We have had many events, public and communications as can be read in the SOCCRATES deliverable D8.5: *Final report on dissemination and standardization activities.* One important deliverable in this context is the SOCCRATES vision paper[31].

Figure 2.10: : SOCCRATES vision paper

3 Joint project exploitation

Some of the SOCCRATES results will be jointly exploited. The joint exploitation plans are explained in this chapter.

3.1 Exploit SOCCRATES platform (all partners)

There are no plans to make an integrated version of the SOCCRATES Platform available for installation, since (as explained in paragraph 2.1.3) any deployment of the SOCCRATES Platform will require large amount of integration with existing security tools and adaption to data formats used in the specific environment. On the SOCCRATES website, however, a specific page[32] has been setup that provides links and information on how to retrieve the software of each of the SOCCRATES Platform components. Not all software is available as open source. For the licensed or commercial software contact information has been provide. Furthermore, not all integration components or IMC adapters have been made available, as they were very specific for demonstration or for the pilot environment.

The platform software page on the SOCCRATES website will enable organizations to collect software components to build their own security automation and decision support platform in line with the concepts and vision of the SOCCRATES Platform. The SOCRRATES deliverable D2.3 Architecture and

[31] https://www.soccrates.eu/wp-content/uploads/2022/05/soccrates_vision_paper_downloadable.pdf

[32] https://www.SOCCRATES.eu/platform-software/

interface specifications[33] will enable organizations to add and/ integrate their own components where they see fit, and the swim lane diagrams (and BPMN workflows) for the SOCCRATS use cases can inspire them to define their own workflows for generating situational awareness and option awareness in a more generic manner.

3.2 Spread the vision of SOCCRATES with SOCCRATES demonstrator (WithSecure, TNO)

The SOCCRATES demonstrator was established to support the dissemination of the SOCCRATES Platform, in particular the SOCCRATES vision and concepts. The SOCCRATES demonstrator will be available for two months after the SOCCRATES project has ended to enable partners to demonstrate the capabilities both internally and externally. It is possible to demonstrate a partner's individual SOCCRATES Platform component within the platform as a whole, but also to demonstrate how the SOCCRATES Platform provides situational awareness and option awareness for use cases 1, 2 and 3 to support security decision making by SOC and CISRT teams.

The Demonstrator includes an easy to use control panel allowing use cases to be triggered easily and it consolidates the User Interfaces (UIs) of different SOCCRATES platform component UIs together in a single portal. See figures below.

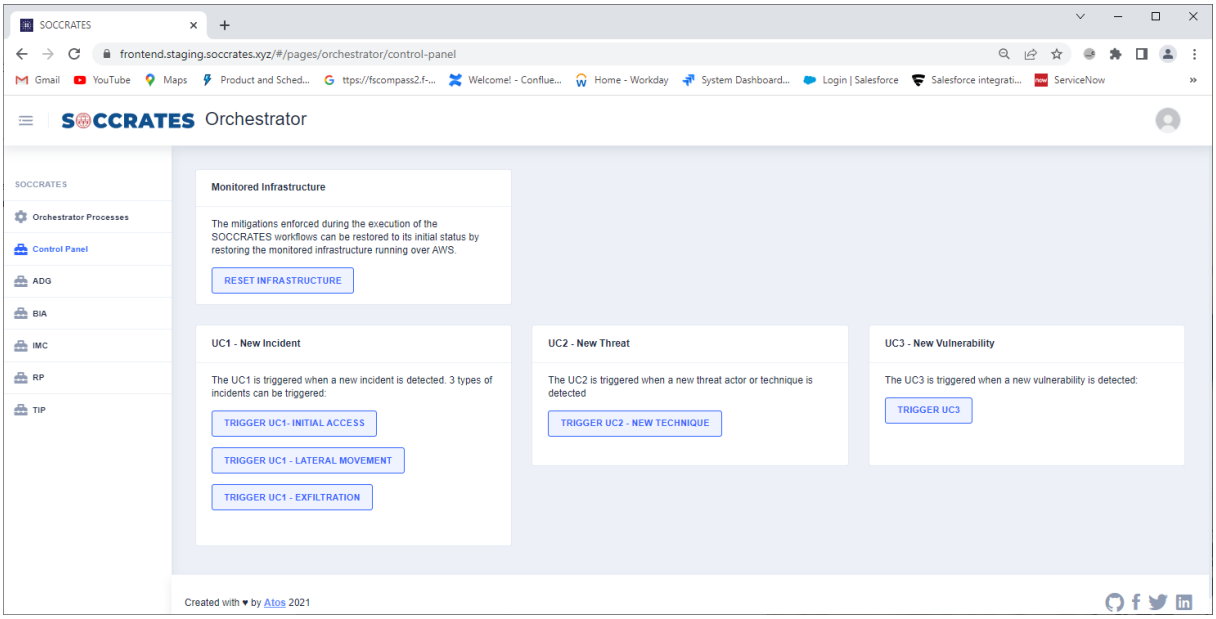


Figure 3.1: : Business impact computation on the BIA Demonstrator control panel

[33] https://www.soccrates.eu/wp-content/uploads/2021/09/SOCCRATES_D2.3_20210830_FINAL.pdf

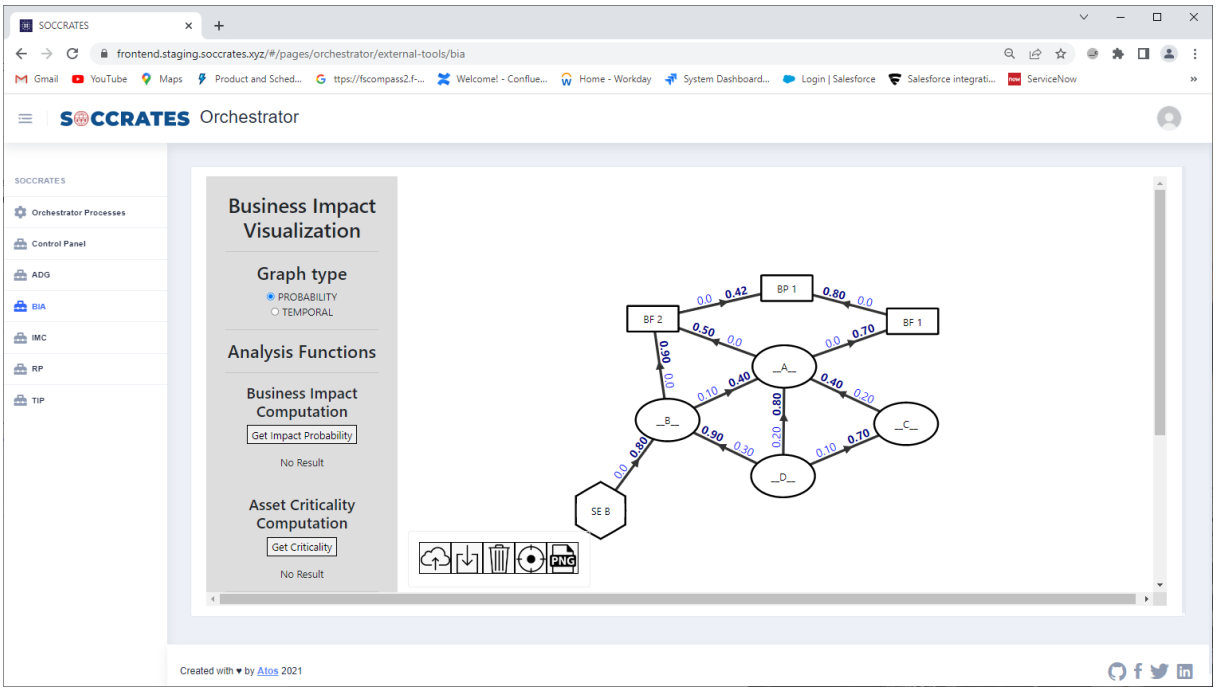


Figure 3.2: Individual component UIs consolidated into common UI

Planned demonstration of the SOCCRATES Platform are presented in the table below.

Table 3.1 Planned demonstration of the SOCCRATES Platform

Date	Event	Partner
18-10-2022	ONE Conference 2022	TNO
19-10-2022	SOCCRATES Final Event at the Cybersecurity Week Luxembourg (CSWL)	all
To be decided	Webinar for the European Telco ISAC (ETIS Information Security Working Group (ISWG) and ETIS CERT-SOC Working Group)[34]	TNO

[34] https://www.etis.org

3.3 Exploit SecuriCAD functionality improvements (foreseeti and KTH)

The ADG Analyser will be part of exploiting the SOCCRATES platform. See section 3.1 above for details.

Some additional notes:

- Foreseeti and KTH have made “Meta Attack Language” as well as the domain specific language “CoreLang” open source as part of the exploitation and dissemination, creating the best value, fostering standardization and contributing the learning and development for society.
- Foreseeti support ADG Analyser exploitation in line with project and consortium agreements for Attack Defence Graph Cortex Analyzer and the SOCCRATES version of securiCAD Enterprise as of end of project. During the project term, Foreseeti was acquired by Google Cloud EMEA Ltd, a limited liability company established in Ireland. This development further advances SOCCRATES’ project goals by increasing the potential of exploitation and dissemination of Foreseeti's securiCAD functionality through the planned integration with Google Cloud's security portfolio, which will ultimately bring greater cybersecurity protections and options to customers.

3.4 Exploit DGA detective (SHS and TNO)

SHS has integrated DGA Detective in its daily operations. Past the project duration, it will continue to collaborate with TNO to provide feedback and/or suggest improvements and install any software in its operational environment. SHS and TNO will continue promoting the tool in the operational security community, a.o. through the COSSAS community under which it was open sourced (see section 2.4.1.1).

4 Individual partner exploitation plans

This chapter lists the individual exploitation plans, structured to the type of organization.

4.1 SOCCRATES End users

4.1.1 Mnemonic

The following mnemonic target groups are identified and will benefit/be approached with the results from SOCCRATES:

1. All Managed Detection and Response (MDR) customers of mnemonic, existing and new: International medium to large corporations in both public and private sector.
    - The MDR services of mnemonic are delivered through the proprietary platform Argus. The Argus platform is modular and rely and allow for integration with a range of external tools and data sources.
    - The results from SOCCRATES will integrate in the service and will to little extent be sold as standalone service additions. The exact value is therefore difficult to

estimate, but will rather serve as obvious differentiation points used for marketing our services.

2. Internal operations and analyst teams
    - The operations and various analyst teams in mnemonic are relying on tooling and automation to perform their tasks. The SOCCRATES results that are not integrated directly into our Argus platform, will be integrated in our services by means of relevant personnel applying those results.
    - The value from exploiting the results in such a way is effectiveness and efficiency in our service delivery.
3. Security community, including academic institutions: Security Analytics, Incident response, Threat Intelligence, Security Automation
    - The security community as a whole is seen by mnemonic as a great source of learning, collaboration and networking. To extract value from such, we need to contribute as much as we consume. The SOCCRATES results will be actively used for such activity.
    - The value for mnemonic from security community contributions are branding, access to data and talent, employee satisfaction and adhering to our code of conduct where we state that we aspire to provide community contributions for the greater good of society.

The exploitable results, Market, market approach, timeline and investments are listed in the table below.

Table 2: Overview of Exploitation approach of mnemonic

Exploitable result	Market	Market Approach	Timeline and need for investments
Infrastructure Modelling Component(IMC)	All Managed Detection and Response (MDR) customers of mnemonic Security community	Integration in proprietary MDR platform Argus. Used as input to new innovation projects.	IMC is already implemented as a proof of concept internally and will follow the development process for integration in Argus. IMC is part of the proposal described in 2.3.2.
ACT SOCCRATES improvements	All MDR customers of mnemonic	Integration in proprietary MDR platform Argus.	The ACT platform is planned published as part of our Argus service in Q4 2022. The GUI and backbone are now integrated as part of our internal development and maintenance processes.

Adversary Emulation Planner (AEP)	Security Community Internal operations and analyst teams	Open Source code. Dissemination to community: presentations and workshops. Integration of tool in internal systems and procedures.	AEP is already available on GitHub and presented externally as described in the dissemination overview. AEP is further developed in the project CyberHunt[35]. AEP is installed and used by the mnemonic Threat Intelligence team since creation.
Contributions to MITRE ATT&CK	Security Community	Submission to MITRE ATT&CK knowledgebase.	Already published in MITRE ATT&CK knowledgebase.
Using the DGA Detective	All MDR customers of mnemonic	Integration in proprietary MDR platform Argus.	Part of Q1 2023 roadmap.
Pilot results	Internal operations and analyst teams	The results are expected to be part of future development and research projects, for future roadmap of the proprietary MDR platform Argus.	Unknown.

4.1.2 Vattenfall

There are components of SOCCRATES platform related to DGA research such as DGA Detective, which are evaluated further for potential future use. Besides that, the core SOCCRATES idea of heavy integration of business view in Security Operations is appreciated by internal stakeholders and the learning points of development, deployment and evaluation will be taken into account in future plans.

Some elements of pilot implementation may be potentially reused for future projects. For example:

- Data collection architecture
- Custom adapter scripts

No specific plans exist regarding actual use of the SOCCRATES platform, since the platform as a whole will be too complicated to deploy.

4.2 SOCCRATES vendors and service providers

4.2.1 Shadowserver

SHS has integrated the DGA Detector (DGA Detective) in its daily operations. The tool provides a DGA assessment of all domains seen in the SHS sandbox (potentially hundreds of thousands daily). Together with other trend anomaly tools and dashboard it allows for analysts to daily monitor domains and identify candidates of interest and further investigation. Results are also shared via an API, which

[35] hhttps://www.mn.uio.no/ifi/english/research/projects/cyberhunt/

can also be accessed by external trusted users in a secure manner with an API key. The Tools are mature enough to function at TRL9 already.

The tools will therefore serve both for internal and external use (in this case, results will be accessible through an API). In the case of external use, the service is provided for free to trusted parties, such as National CSIRTs and LEA.

SHS aims to expand the amount of users who can access the tool results via the API by spreading the word about the service in its presentations to the Internet defender community. This is a continuous task that will be carried out as part of standard SHS activities.

As of the time or writing of this deliverable, SHS already has 22 CERTs (Albania, Australia, Brazil, Czechia, Denmark, Fiji, India, Italy, Latvia, Luxembourg, Malawi, Netherlands, Paraguay, Philippines, Poland, Slovakia, Slovenia, Taiwan, Thailand, Togo, Tunisia, Vietnam) signed up to using the API for access to the above results. Ten of them have been observed actually using the SOCCRATES methods. It is expected that this number and usage will steadily increase over time post-project, as the API methods are now part of the Shadowserver offering to vetted partners.

As mentioned in section 2.2.12 and D4.3, the developed service has already provided impact in the real world by sink holing threats, sharing with CSIRTs and network owners, as well as identifying new DGAs. This work will continue post-project and is expected to result in similar successes in the future.

4.2.2 WithSecure

WithSecure Corporation, formerly known as F-Secure Corporation, was leading the WP3 with focus on Infrastructure Modelling Component (IMC). IMC provides unified view to the ICT infrastructure for the rest of the SOCCRATES platform by normalizing raw data coming from various data sources.

WithSecure has a portfolio of integrated cyber security products, known as WithSecure Elements, targeted to corporate customers. Elements gathers extensive raw data of the protected customer ICT infrastructure through network vulnerability scans, integrated endpoint protection and detection agent and with integrations to customer Active Directory. In addition, WithSecure has been gathering threat intelligence for decades.

Visibility to ICT infrastructure assets is a key enabler for efficient cyber security operations, i.e. you cannot protect or manage what you cannot see. Furthermore, ICT infrastructure asset information is key enabler for automating cyber security operations. Currently the industry lacks for how to combine information related to ICT infrastructure data coming from different types of tools in different formats.

Gartner has identified a new emerging technology called cyber asset attack surface management (CAASM), focusing on solving the asset visibility problem for security teams. Based on Gartner, CAASM “expands beyond the limited scope of products that focus on a subset of assets” and “replaces manual and time-consuming processes to collect and reconcile asset information”[36].

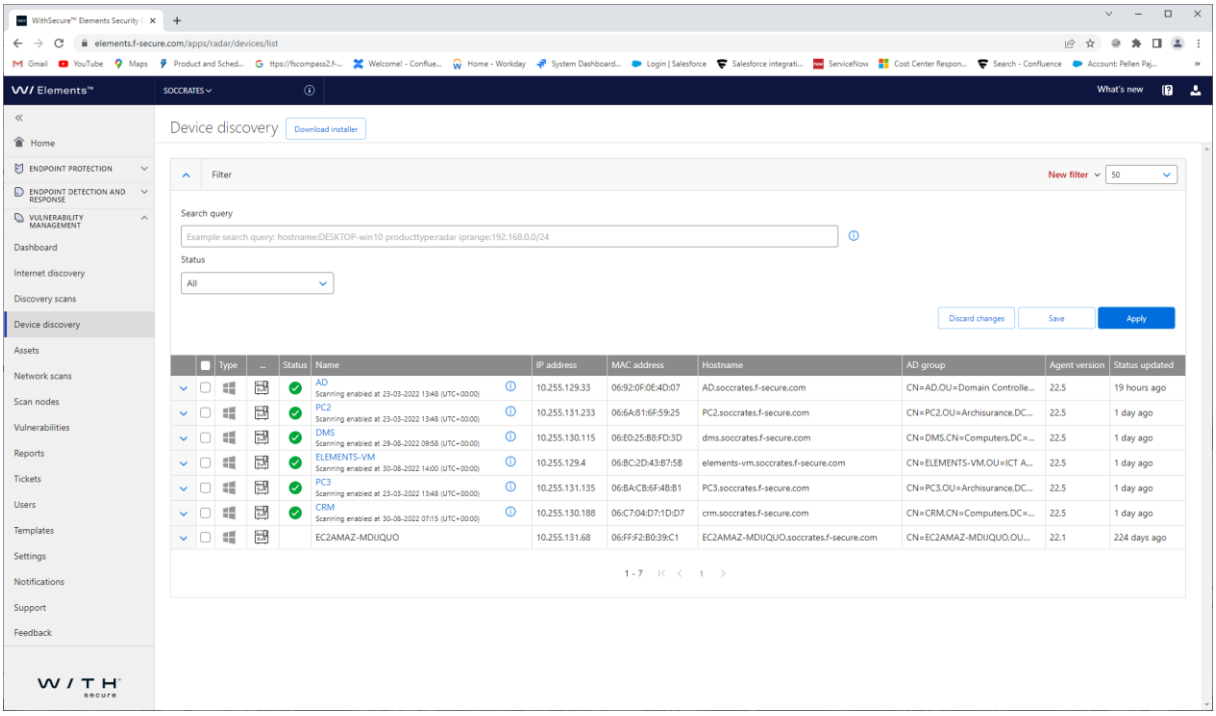
[36] Gartner Hype Cycle for Security Operations, 2021

Processing vast amounts of asset data and linking that with dynamic threat intel require novel approaches as traditional relational databases do not scale. Graph database technology was applied in SOCCRATES IMC to enabling asset and threat intel data to be updated independently. Several CAASM solutions depend on graph database technology as well.

Conceptual, graph-based, infrastructure data model developed within SOCCRATES project enables WithSecure to further integrate WithSecure Elements together and build CAASM features into the Elements product itself. This way WithSecure can provide holistic view to the customer ICT infrastructure and its security posture for its partners and customers, and further automate the security operations by extending the machine learning capabilities already existing in Elements endpoint detection and response solution.

Concretely WithSecure has developed initial version of IMC into Elements within the SOCCRATES project. This initial version of IMC enables Elements to combine information coming from millions of Elements endpoint agents with the network discovery scan results. First use case for this is to enable WithSecure Elements VM customers to use integrated Elements endpoint agent to scan their endpoints for vulnerabilities and provide unified asset view combining data from agents and network scans[37].

Endpoint-oriented vulnerability scanning works also outside company networks, enabling mobile and remote workers laptops to be better protected. Figure 4.1 below illustrates the device discovery in Elements VM.



[37] https://community.f-secure.com/vulnerability-management-fi/kb/articles/8997-f-secure-radar-endpoint-agent-available-for-windows

Figure 4.1: : Elements VM with Device discovery of integrated EPP/EDR/VM endpoint agent

Second feature utilizing data integration within Elements is Elements VM asset risk score. Asset risk score is a rating that indicates what is the size of potential loss or damage if an identified threat materializes in a specific asset. Risk score calculation uses data both from the network scanner and the endpoint agent. Figure 4.2 below illustrates the asset risk score feature in Elements VM[38].

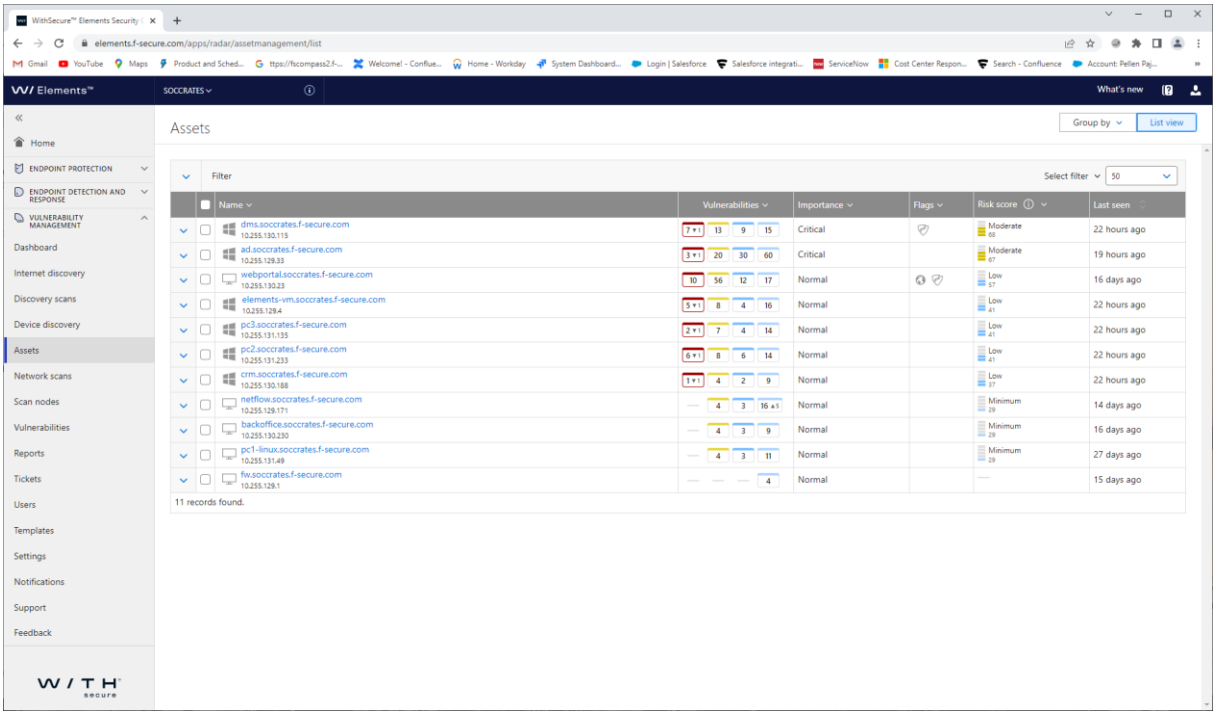


Figure 4.2: Elements VM asset risk score

WithSecure will continue to develop similar CAASM features into Elements utilizing the conceptual IMC data model developed in the SOCCRATES project.

4.2.3 Foreseeti

Foreseeti will support project and ADG Analyser exploitation with background and results in line with project and consortium agreements.

Foreseeti and KTH have made “Meta Attack Language” as well as the domain specific language “CoreLang” open source as part of the exploitation and dissemination, creating the best value, fostering standardisation and contributing the learning and development for society.

4.2.4 ATOS

Atos is a global leader in digital transformation with 112.000 employees in 72 countries. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry.

[38] https://community.withsecure.com/kb/articles/29311-whats-new-in-withsecure-elements-june-july-2022

The task of translating the research results and outcomes of the SOCCRATES project to Atos global portfolio and service lines is performed by a technology transfer and business development team which is part of Atos Research & Innovation (ARI), the node of R&D at Atos in Spain.

The main assets provided by Atos to this project are:

- **SOCCRATES orchestrator**

The SOCCRATES Orchestrator and Integration Engine is an asset developed by Atos in the project to manage and orchestrate the interoperation among the SOCCRATES components throughout different workflows associated to common incident response situations. Although the technology was available, Atos has developed this asset from scratch reaching a TRL 6 by the end of the project. It has been designed making use of different existing open-source solutions, in particular the BPMN (Business Process Model and Notation) workflow engine Activiti and Cortex, a tool developed in TheHive project to orchestrate the execution of analysers.

- **L-ADS (Live Anomaly Detection System)**

The L-ADS (Live Anomaly Detection System) is a tool based on a Deep Learning algorithm that aims to identify possible anomalies in a given internal network. It learns from the legit traffic used to train the algorithm and evaluates the new incoming traffic. If the difference is significant, it is considered that this new incoming traffic can be classified as an anomaly. Atos has developed this asset till a TRL 5.

Initially the asset was able to capture traffic through the Softflowd tool, which is an implementation of Netflow. However, for this project, the asset has been modified to work in the same manner as the rest of the AAD components.

All components are Atos proprietary under different licensing, and the development's investment also relies in Atos financials. EU project budget supports the enhancements of the backgrounds provided by Atos and will also support achieving a higher maturity level.

Atos R&D developments are evaluated under the perspective of the suitability for the Atos business lines commercial portfolio offering. Once presented to the specific Atos business lines, they decide whether the development can or cannot be included into the commercial offering to the customer portfolio of the CyberSecurity unit, extending in that way the offer or increasing the value proposition of the current offering. Currently there is an ongoing discussion to add L-ADS in the ATOS portfolio.

Based on the maturity level of the different assets (from TRL 2 to TRL 6) the timeline expected to become part of the commercial offering is no less than 3 years.

Atos R&D will continue its developments and will use the current developments as background for new projects (e.g. L-ADS has been also included already in 3 new projects (e.g. SDN-microSENSE, CyberMAR and ELECTRON).

Atos business unit BDS has expressed his interest in detection in OT environments, as this is one of the enhancements they need to include in their commercial offering since currently they depend on the usage of third parties' solutions.

Additionally to all this, both assets (L-ADS and the orchestrator) are going to be included in some proposals for the HORIZON-CL3-2022-CS-01-01 call such as a follow-up of SOCCRATES project where these assets will be extended for SOC/CSIRTs in combined IT/OT domains. See also paragraph 2.3.2.

4.3 SOCCRATES RTOs

4.3.1 TNO

TNO foresees exploiting several results from the SOCCRATES project, in particularly:

- DGA Detective and Middleman
- SOCCRATES Platform vision, concepts, and several (open source) tools
- Automated Response software tools for processing CACAO playbooks and OpenC2 commands. Although the AR software components for SOCCRATES contain specific functions for the project (e.g. query IP addresses in the IMC based on a timestamp and UUID), the SOCCRATES project aims to contribute to
    - Test and development for the OASIS Open standards. As a member of both the CACAO and OpenC2 technical committees, TNO aims to contribute in test and development of the software provided by OASIS and used within SOCCRATES (e.g. Yuuki[39]).
    - Furhermore, in the future TNO aims to contribute to the extension of both standards, for instance by extending OpenC2 actuator profiles[40] and by adopting the standard in other projects.
- CI/CD pipeline and DevOps environment

The work at TNO on SOCCRATES Platform vision, concepts, and several (open source) tools will continue in new projects and the following projects that recently started:

- ASOP project with VMWare, KPN and BizzDesign.
- HORIZON EU project eFORT
- EDP project AInception

4.3.2 AIT

There are several ways that the AIT foresees exploiting the results from the SOCCRATES project. For several years, the AIT has undertaken an initiative to developed a cyber range-based training and exercises capability[41]. The knowledge from the project will inform training courses and exercises that will be delivered by the AIT as a commercial offering. The customers of these courses tend to be professionals from critical infrastructure operators, both within Austria and further afield (e.g. the Middle East). Furthermore, the AIT supports training and awareness activities with the International Atomic Energy Agency (IAEA) – knowledge from the SOCCRATES will support the development of training material and demonstrations in the context of this initiative.

[39] GitHub - oasis-open/openc2-yuuki: OASIS TC Open Repository: Yuuki is a python package for building an OpenC2 proxy

[40] OpenC2 Actuator Profile Subcommittee | OASIS (oasis-open.org)

[41] The AIT Cyber Range : https://cyberrange.at/

The AIT has a group that performs penetration tests for commercial entities. This activity largely focuses on application, web-application, cloud, infrastructure and network penetration tests. As examined in the SOCCRATES project, there is the potential for machine learning algorithms to be subverted by an adversary. This presents a potential risk to systems that use this technology – a future offering for the AIT penetration testing group could relate to testing the robustness of machine learning models to adversarial behaviour (such as adversarial examples). This could help to ensure the robustness of the tested models and promote their implementation and deployment in a robust fashion. We do not foresee this market being available immediately at the end of the project, but there could be a potential future market that targets developers, integrators and operators of cyber security solutions that use machine learning-based models.

Finally, as a research centre, the AIT will look to exploit the results from projects in further research projects that aim to elevate the TRL of the prototypes that have been developed in the project and to explore some of the open problems that have been identified during evaluation activities. The software that has been developed in the project by AIT will be made available in an open-source manner – the intention is this could lead to use of the software by a community of users and potential future partnerships.

4.4 SOCCRATES universities

4.4.1 IMT

IMT has three main directions to exploit the results from the SOCCRATES projects. First, IMT is actively involved in numerous research and innovations projects that provide opportunities to further develop the Business Impact Analyser and Response Planner and raise the TRL of these components. Regarding the BIA, the business logic modelling can be further refined with more realistic considerations with respect to the representation of the infrastructure and the business entities. Regarding the RP, substantial effort was made in the context of the SOCCRATES project in order to adapt the parameters of the RORI metric to the values that were made available by our partners. Such effort can be carried on along with industrial partners in order to further update the RORI metric definition based on inputs that could be evaluated in a real time context.

IMT also has several training programs in cybersecurity, in which the approaches and scenarios defined in the SOCCRATES project can be added to the courses and projects. In particular, automation of mitigation deployment and anomaly based intrusion detection have already become a focus within these programs. By building on the SOCCRATES results, IMT will be able to train cybersecurity experts that will further contribute to SOC development in industrial context.

Finally, IMT is actively supporting the French economy deployment, particularly through transfer to industry. Since IMT is hosting the IMT Starter incubator, which welcomes 10 to 15 startups every year, transfer to one or several of the incubated companies can be considered.

4.4.2 KTH

KTH will continue developing, maturing, and using results from SOCCRATES in multiple ways. For CoreLang first of all additional validation projects have been initiated where attack graph predictions will be compared with actual attacker behavior in terms of student data from a cyber range Capture

The Flag (CTF) that is the fundament in KTH's ethical hacking course as well as expert assessments of this environment. Moreover, CoreLang is also used as the fundament in a threat modeling language particularly designed for the domain of power substation automation systems. Finally, CoreLang will also serve as a fundament in a project, similar in structure and mission to SOCCRATES, that will demonstrate Machine Learning based defence actors in a cyber range hosted by the Swedish Defence Research Agency. Here the ML agent will be trained on CoreLang-based attack graphs. As for the CoA it will be further developed to include not only defence actions encoded as "defence steps" in the attack graph but also how structural changes in the system architecture can be formalised into courses of actions in a defence strategy. This work has been initiated already during SOCCRATES, but will be further developed and finalized after. The CoA generator will also serve as baseline for automated response in the aforementioned demonstration project with the Swedish Defence Research Agency.

5 Related legal and regulatory aspects

The major potential legal considerations for the project regard compliance with EU and national regulations, particularly the EU NIS Directive, and in particular with respect to critical infrastructure operators. The NIS Directive was adopted in 2016 and transposed into national law by 2018 by Member States and is open to interpretation with respect to the details of its implementation. Although there are differences between Member State in the implementation of the Directive, key tenets of the Directive should be realized consistently. This should be supported by the NIS Platform whose aim is to harmonize the Directive's implementation across Europe and promote the application of best practices. The 2020 evaluation[42] of the NIS Directive revealed a number of issues following the transposition into national law, such as : insufficiently clear NIS Directive expectations ; insufficient support from national authorities ; insufficient investments in information security. To counter the fragmented implementation of the NIS Directive, and to respond to new challenges of digital security, the European Commission submitted the NIS2 proposal in 2022. This is an updated version of the NIS Directive aiming to increase cybersecurity in the EU, imposing more obligation on organizations and sectors (security requirements, security of supply chains, reporting obligations, stricter and more harmonized supervisory and enforcement requirements across the EU).[43]

Through the SOCCRATES advisory Board, the Stakeholder Group and the project's partners that have a European footprint, the project has been tracking these developments to ensure implementation details do not lead to a reduced impact.

The other main EU legislation we have taken into consideration is the General Data Protection Regulation (GDPR); this regulation is especially relevant to the AI-based detection techniques that were developed in the project. SOCCRATES focuses on the development of integrated approaches to support SOC and CSIRT operations and will not generate (personal) data, a privacy impact assessment was not needed and the project also opted out of the Open Data pilot. As a consequence, a Data Management Plan (DMP) was not required. However, the project chose to provide such a DMP on a voluntary basis.

[42] https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist

[43] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

SOCCRATES generated quite some foreground results. We have published results as Open Source in many cases, in other cases the foreground served as enhancements of existing commercial products. In any case all foreground was treated in accordance with the SOCCRATES consortium agreement.

6 Closing remarks

A range of exploitable results has been produced as planned. We believe that SOCCRATES has realized considerable impact with these results during the project, although we were restricted by the COVID pandemic for an extensive period of time. We were very successful in reaching the relevant target groups to explain the benefits of our results, a.o. by exposing our stakeholder group to the project's vision and outcome, organizing events and workshops, conducting webinars and demonstration, publishing a vision paper and further (more specific) articles and other dissemination activities as described in our final dissemination report (D8.5).

The expected impact required in the call[44] was:

Short/medium term

- Enhanced protection against novel advanced threats;
- Advanced technologies and services to manage complex cyber-attacks and to reduce the impact of breaches;
- The technological and operational enablers of cooperation in response and recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive.

Long term

- Robust, transversal and scalable ICT infrastructures resilient to cyber-attacks that can underpin relevant domain specific ICT systems (e.g. for energy) providing them with sustainable cybersecurity, digital privacy and accountability.

With the exploitation initiatives explained in this document we will raise further material effects after the project has ended and we think we have adequately addressed the required impact of the call:

- "Enhanced protection against novel advanced threats"
    - *We have built a platform with innovative cyber security technology that will provide better protection against advanced cyber-attacks. The platform will remain available on our website for anyone to re-build and the demonstrator will be used in demos for some time after the project. Much of our developed knowledge base will remain available on or via our project website after the projects has ended: deliverables, Open Source software, articles, the vision paper, webinar recordings. All project partners will keep on using SOCCRATES results after the project, be it built in commercial products, included in trainings, input for new projects to further build on etc.*
- "Advanced technologies and services to manage complex cyber-attacks and to reduce the impact of breaches"

[44] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-01-2018

    - *The SOCCRATES platform with all its individual components includes many advanced technologies that were specifically developed to manage advanced cyber-attacks and reduce the impact of breaches. The exploitation focusses specifically on the platform components and these components will be part of (commercial) products and services, published as Open Source and further built up-on in follow-up projects.*
- "The technological and operational enablers of co-operation in response and recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive."
    - *The SOCCRATES project has contributed considerably to the knowledge base of the CSIRT community. As D8.5 reveals, we have been in contact with at least 26 MSSPs and 6 national CERTs in the course of our work. Through our partner Shadowserver we reached out to National CSIRTs from over 135 countries about SOCCRATES. 21 CERTs have asked to sign up to the Shadowserver SOCCRATES API methods. Our stakeholder group encompassed 8 SOC/CSIRT operators, 9 MSSPs and 4 national CERTS. These stakeholders have all been made aware of the opportunities that SOCCRATES automation technologies offer and they all confirmed that the SOCCRATES results are and will remain relevant for them.*
- "Robust, transversal and scalable ICT infrastructures resilient to cyber-attacks that can underpin relevant domain specific ICT systems (e.g. for energy) providing them with sustainable cybersecurity, digital privacy and accountability."
    - *The SOCCRATES project has evaluated the platform with analysts of actual end user organizations, including a SOC facility in the energy infrastructure (Vattenfall). This has resulted in tangible indications that the concepts incorporated in the SOCCRATES platform can indeed make ICT infrastructures more robust against cyber-attacks.*

With the plans described in this report, we ensure the continuous use and further development of the SOCCRATES results, contributing to a society that is more robust against cyber-attacks.

7 Abbreviations

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

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

MDR	Managed Detection and Response
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