Authors: Susana González Zarzosa, Cybersecurity Engineer at Atos Research & Innovation, Spain. Can be reached at susana.gzarzosa@atos.net.
Jesus Villalobos Nieto, Cybersecurity Engineer at Atos Research & Innovation, Spain. Can be reached at jesus.villalobosnieto@atos.net.

SOCCRATES - Automation and Orchestration of Security Operations

SOCCRATES (SOC & CSIRT Response to Attacks & Threats) is an European innovation project, co-funded by the Horizon2020 programme and led by TNO. It brings together some of the best European expertise in the field to develop, implement and evaluate an automated security platform to support SOC analysts. This fourth article on the project will focus on the SOCCRATES Orchestrator and Integration Engine which is at the core of the SOCCRATES platform providing automation and orchestration of security operations to response.

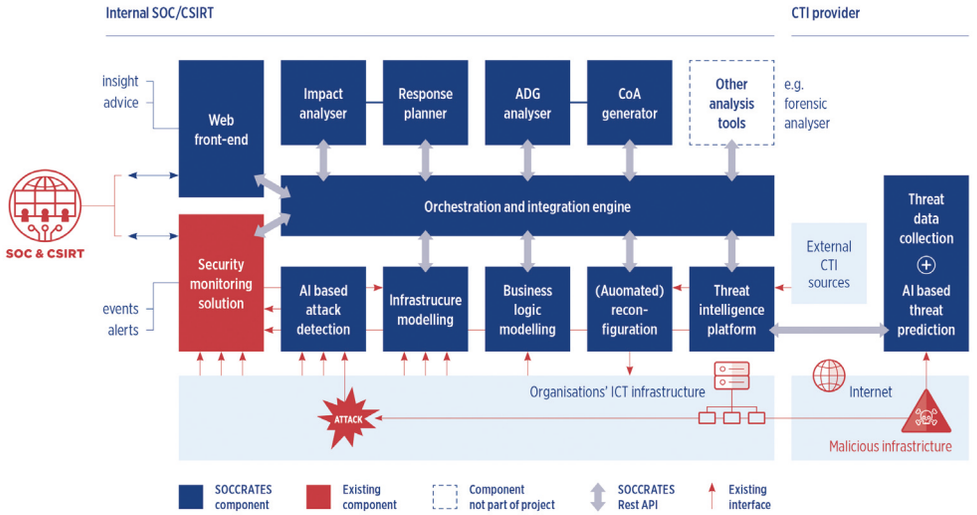

Figure 1: The SOCCRATES Platform.

The SOCCRATES project was introduced in three previous articles (IB4-, IB5.2021, and IB5.2022). The first article gave an overview of the challenges that Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) face, and how the SOCCRATES project addresses these challenges by developing a security automation and decision support platform, 'the SOCCRATES platform'. The second (winning) article described in more detail how the SOCCRATES platform is providing security automation for SOC and CSIRT processes. How it provides situational awareness and option awareness to the SOC analyst and enables (semi) automated response execution. This fourth article goes into more details on the SOCCRATES Orchestrator and Integration Engine which is at the core of the SOCCRATES platform.

As described in the first articles, there are many challenges that SOCs, CSIRTs and Managed Security Service Providers (MSSPs) face to offer an efficient and quick answer to the increasing, evolving and more and more complex number of cyber attacks that organisations are confronted with.

One of these challenges is to provide support to the security analysts in the automation and orchestration of the different tasks they need to perform to give response to specific common situations, such as the ones included in the SOCCRATES Use Cases:

- ***Use Case 1: Response on Detected Ongoing Attack***
  Detect ongoing attacks and automatically analyse the attack, automatically determine the best response, and initiate deployment of the selected response.
- ***Use Case 2: Response on Newly Received Cyber Threat Intelligence***
  Continuously collect new threat information, automatically analyse the potential business impact and determine best options for proactive mitigation.
- ***Use Case 3: Response on Newly Discovered Vulnerable Assets***
  Automatically detect vulnerabilities on assets in the ICT infrastructure, assess if they enable new attack paths, determine and initiate mitigation actions.
- ***Use Case 4: Response on Discovered System Configuration Change***
  Automatically detect configuration changes on assets in the ICT infrastructure, assess if they enable new attack paths and determine if action is needed.
- ***Use Case 5: Response on Deployment of New Systems in Infrastructure***
  Automatically detect introduction of new systems to the ICT infrastructure. Automatically assess the new situation and determine if (additional) security measures are needed.

The SOCCRATES Orchestrator and Integration Engine is at the core of the SOCCRATES platform (see figure 1) and was developed from existing technologies to cover the requirements about automation and orchestration established in the project.

After analysing the current state of the art in security orchestration and automation solutions, two different open-source solutions (Activiti (1) and Cortex(2)) were chosen as starting point to provide on the one hand workflow execution capabilities and on the other hand support to interconnect and invoke external tools. Consequently, the component was divided in two main sub-

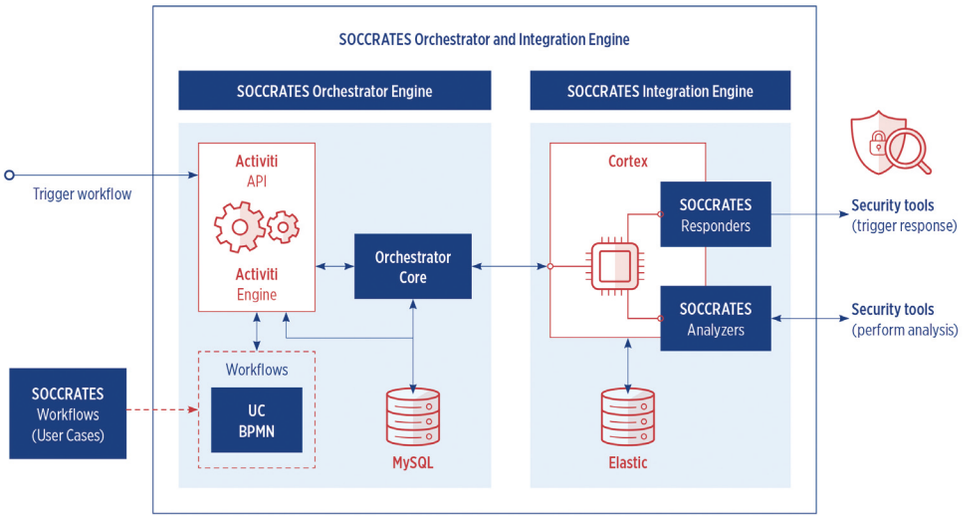

Figure 2: SOCCRATES Orchestrator and Integration Engine Architecture.

components (see figure 2), each of them focused on one of those main functionalities and built on top of different technologies:

- the SOCCRATES Orchestrator Engine, and
- the SOCCRATES Integration Engine.

The SOCCRATES Orchestrator Engine

This component integrates the lightweight open-source BPMN (Business Process Model and Notation) workflow engine Activiti to support the management and execution of the security automation and decision processes included in the five use cases defined in the project. The different workflows associated to the use cases have been modelled using the standard BPMN and they are loaded to the Activiti Engine.

The workflows can be triggered by different external tools invoking the Activiti REST API. In particular, the Use Case 1 is triggered by a *SIEM (Security Information and Event Management)* when there is an alarm for an ongoing attack, Use Case 2 is triggered by the *Threat Intelligence Platform* when it is reported a new exploit code discovered for a vulnerability or a new technique associated with a threat actor, and the other Use Cases (3-5) are triggered by the *Infrastructure Modelling* component in different situations. Each of these triggering messages starts a new process definition in the Activiti Engine.

The Orchestrator Core manages the communication between Activiti and the SOCCRATES Integration Engine, retrieving from the triggering messages the relevant information, preparing the request data necessary for the invocation of the different security components in charge of each task included in the workflows and processing the responses received.

The SOCCRATES Integration Engine

This component is composed by the open-source solution Cortex created by The Hive Project (3) and a set of SOCCRATES Responders and Analysers, most of them developed in the project by the tool partners and associated to each of the components in the SOCCRATES Platform.

Analysers and responders are connectors that allow interaction between Cortex and external tools. The main difference between them is that Responders just trigger some action in an external tool (e.g. send an email or update a business model) without the need of receiving any response from the component, whereas the Analysers request some analysis or action providing some data in the request and obtain a response with the report of the analysis performed. These Cortex Analysers and Responders are invoked by the SOCCRATES Orchestrator Engine throughout the different workflow stages. The following components of the SOCCRATES Platform are integrated through Cortex analysers or responders:

- **Attack Defence Graph (ADG) Analyzer**, to analyse and generate a next step analysis or determine the potential attack path.
- **Course of Action (CoA) Generator**, to suggest potential defences (Course of Actions) included in the model to the SOC analysts that could be activated to isolate or mitigate the risks.
- **Business Impact Analyzer (BIA) & Business Logic Modelling**, to evaluate the affected or potentially affected assets and for containment.
- **AI based Attack Detection (AAD)**, to perform a new attack detection based on multiple data sources when a new vulnerability or asset has been found in the infrastructure.
- **Infrastructure Modelling Component (IMC)**, to get information of

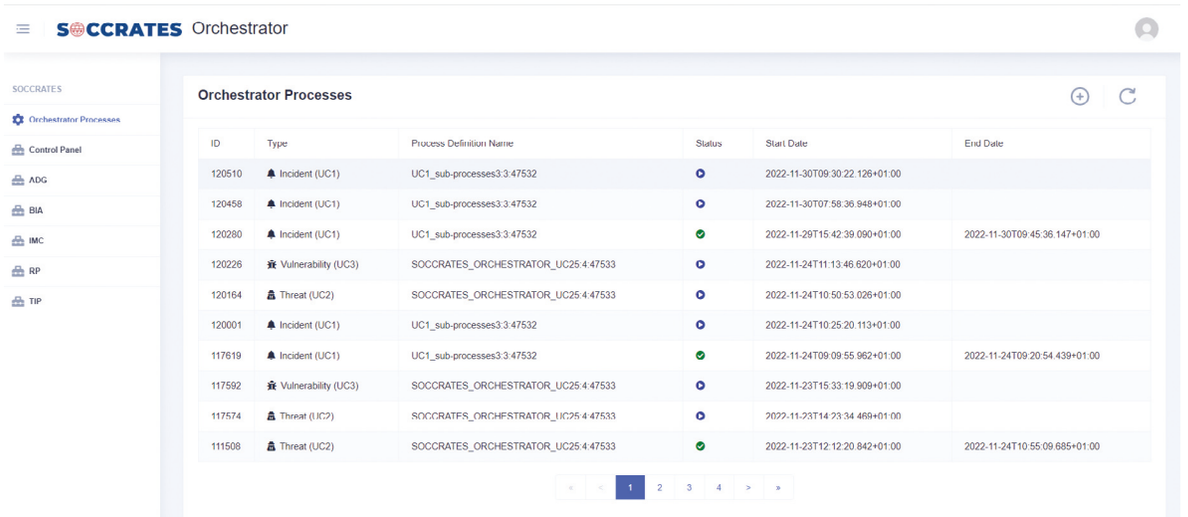

Figure 3 – SOCCRATES Web Front End.

the monitored infrastructure, mainly to translate from IPs and hostnames to internal identifiers.

- **Automated Reconfiguration (AR)**, to interact with the IT support or IT infrastructures to perform some mitigation action (e.g. send an email, send a webhook notification to an endpoint or execute a CACAO playbook) depending on the selection of Course of Actions done by the SOC analyst.
- **Response Planner (RP)**, to calculate the Return on Response Investment (RORI) associated to the Course of Actions identified.

The SOCCRATES Orchestrator and Integration Engine also includes a Web Front End (see figure 3) which provides a graphical user interface that allows the SOC/CSIRT analysts to visualize and interact with the different workflows (Use Cases) running in the Orchestrator and access to the graphical user interfaces provided by the different SOCCRATES components (Business Impact Analyzer, Response Planner, Infrastructure Modelling Component and Threat Intelligence Platform).

Future research lines

As it has been presented, current functionality of the SOCCRATES Orchestrator and Integration Engine is based on the capabilities provided by two open-source solutions, Activiti and Cortex, and it provides automation and orchestration for the workflows defined by the use cases considered in the project. These workflows should be reviewed and updated to support different target SOC/CSIRT infrastructure models (such as hybrid, cloud based, virtualized) and add the possibility to be tuned for specific environments. It is also necessary to perform more research and new developments to improve the visualisation capabilities of the component and allow its integration with other open-source tools that could be also used in SOC/CSIRT environment. Related to interoperability, investigate the feasibility of normalizing the data formats used in the communication between the different components integrated through the SOCCRATES Orchestrator and Integration Engine is another potential research topic. The usage of some standardized format (such as STIX or OpenDXL) in this communication could help to extend and generalize the workflows and facilitate the integration of the SOCCRATES platform with other security products or tools used by SOC/CSIRTs analysts.

It would be also interesting to investigate how to improve the capabilities of the SOCCRATES Orchestrator and Integration Engine to support the simultaneous triggering of events related to a same security incident and do some additional research to integrate Artificial Intelligence (AI) in the component, for example to add the possibility of learning from the decision-making process done by the SOC/CSIRT analysts in order to make suggestions for future handling of security events based on previous choices. Finally, also related to an effective security decision-making process, human-machine interaction in SOC/CSIRT operations is also an important topic for future research and many open questions are still to be answered in this area.

References

(1) https://www.activiti.org/

(2) https://github.com/TheHive-Project/Cortex

(3) https://thehive-project.org/

(4) SOCCRATES Vision, Roadmap & Guidance for SOC. Available at https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES-Vision-Paper.pdf

(5) D6.1 Initial version of the SOCCRATES Platform Orchestration, Reconfiguration and Front-end. Available at https://www.soccrates.eu/results/

(6) D6.2 Initial version of the SOCCRATES platform. Available at https://www.soccrates.eu/results/