**Authors:** Reinder Wolthuis, senior consultant/project manager cybersecurity at TNO. Can be reached at reinder.wolthuis@tno.nl.
Frank Fransen, senior scientist cybersecurity at TNO. Can be reached at frank.fransen@tno.nl.

# SOCCRATES - Security automation in SOC & CSIRT environments

SOCCRATES (SOC & CSIRT Response to Attacks & Threats, based on attack defence graphs Evaluation Systems) is a European innovation project, co-funded by the Horizon2020 program 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 first article provides an introduction to SOCCRATES, in two follow-up articles we will highlight the underlying concepts.

Over the past years, the cyber threat landscape has greatly evolved. Advanced cyber-attacks are now conducted by professional threat actors that have substantial resources and (technical) capabilities. Such attacks are often targeted in nature and may involve a great degree of automation, persistence and (technical) sophistication. Meanwhile, the dependency on Information and Communication Technology (ICT) and thus the potential impact of any cyber-attack is ever increasing. Combined with the continuously evolving ICT infrastructures with diverse and emerging technologies (e.g. Internet of Things (IoT)), organisations are faced with a challenging task.

To deal with these challenges, many organisations have increased their effort in security monitoring and incident response. Many organisations have setup internal Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) to perform these tasks, others outsourced these tasks to a Managed Security Service Provider (MSSP). In recent years, these security operation activities have been extended with collection and processing of Cyber Threat Intelligence (CTI), to anticipate upcoming threats and take appropriate precautions. Although security operations have gotten more attention over the years, these SOCs and CSIRTs (both internal and MSSP) are faced with complex challenges:

*Improve and extend detection capability.* Threat agents (attackers) continuously evolve and improve their Tactics, Techniques and Procedures (TTPs), including stealth techniques. The SOCs consequently need to improve the detection capability and coverage with more advanced techniques that assist the analyst in discovering indicators in a massive amount of data while reducing the number of false positives.
Automate the CTI process. As the amount of available CTI is increasing and the value of a large portion of that CTI is limited to a short time span, it is becoming more important to automatically assess and apply mitigation strategies to these threats.

*Understand the ICT infrastructure.* Simply put; you cannot defend what you don't know. As SOC analysts need to interpret and understand the detected security events, insight in the continuously evolving ICT networks and systems is essential. The SOC analyst also needs to understand the critical attack surfaces, attack vectors that may lead to a compromise of critical business assets as well as defence mechanisms deployed to counter attacks.
Assess business impact of an incident. In addition to understanding the ICT infrastructure, the SOC analyst needs to be able to assess the potential impact on the business of an ongoing attack or emerging threat. Business processes thus need to be mapped on the ICT infrastructure components, and insight in the consequences of a breach of confidentiality, integrity and/or availability of system resources or information assets needs to be (near real-time) available.

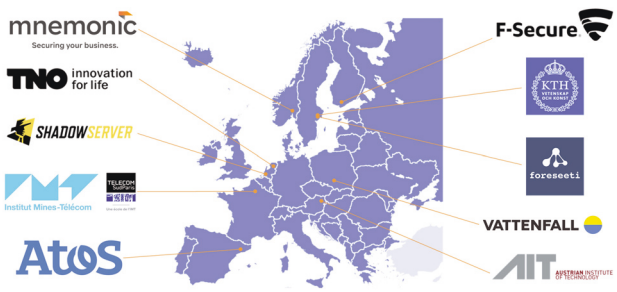


*Figure 1 – The SOCCRATES partners.*

*Recommend Course of Actions (CoAs).* When faced with an attack or emerging threat, the SOC analyst needs to identify possible responses and determine which response is the best given the ICT infrastructure, available (on demand) reconfigurable security functions, and the effect on the business.

## How SOCCRATES addresses these challenges

### The Project

The SOCCRATES consortium is a collaboration of 10 partners across Europe (see figure 1), each with a different perspective (university, knowledge institute, end user, Managed Security Service Provider (MSSP), vendor) and providing unique contributions.

The main SOCCRATES objective is: 'Develop and implement a Security Decision Support framework that enhances the effectiveness of SOC and CSIRT operations.' The results specifically targeted at end user's inhouse SOC and Managed Security Service Providers (MSSP) that provide SOC services. The project has a total budget of 5.9 Million Euro for three years.

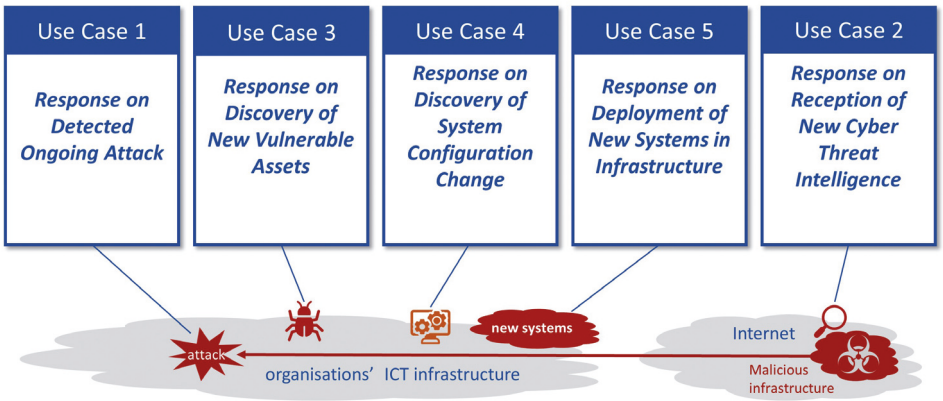


*Figure 2 – The SOCCRATES use case.*

**The Use cases**

The work in SOCCRATES is based on five different use cases, see figure 2:

- **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 use cases are used to derive requirements for the platform and to define KPI's for the evaluation of the platform.

**The Platform**

The integrated Security Decision Support framework will consist of a platform with a modular set of components with standardized interfaces and a central orchestration function, see figure 3:

The SOCCRATES platform will have the following capabilities:

1. **Automated discovery and modelling** of an organisation's technical assets to provide an accurate, machine-readable description of the ICT infrastructure;
2. **Detection of (sophisticated) cyber-attacks**, even in the case of encrypted network traffic, by applying advanced data analytics techniques (including AI and deep learning) on large amounts of network and log data;
3. **Attack simulation** by means of Attack Defence Graph (ADG) based analysis on a model of the ICT infrastructure (both before and during an attack), and determination of the best response to these threats and attacks;
4. **Quantification of the (potential) business impact of emerging threats and ongoing attacks** by means of business impact modelling and appraisal of business trade-offs in possible mitigations;
5. **Cyber Threat Intelligence (CTI) utilization** in incident detection, analysis and response, including Adversary Emulation Plans to enable threat actor specific attack simulation with Attack Defence Graphs;
6. **Identification, classification, and prediction of malicious activities and trends** through automated analysis on large amounts of malicious infrastructure and malware forensic data.
7. **Plan and enable automatic execution of Courses of Action (CoAs)**, while including humans in the loop for authorization or manual reconfiguration, by supporting open standards for security automation (i.e. OpenC2 (1) and CACAO (2)).

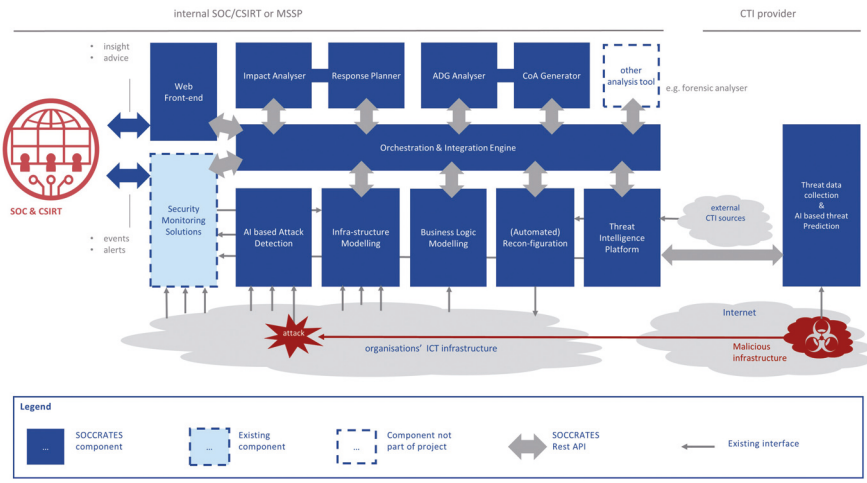


*Figure 3 – The SOCCRATES platform.*

The platform is a mix of technical innovations; both completely new innovations and innovations on already existing products. The platform is being built in three iterations between 2019 and 2022.

It has several components. The central component is the Orchestration and Integration Engine that facilitates communication and exchange of information between components and orchestrates the actions undertaken by the SOCCRATES platform when it is triggered.

Underneath the Orchestration and Integration Engine all components are presented that directly interact with the ICT infrastructure of an organisation or collect (threat) intelligence from external sources (e.g. the Infrastructure Modelling Component and Threat Intelligence Platform). Above the Orchestration and Integration Engine the analysis components are shown (i.e. Impact Analyser & Response Planner, ADG Analyser & CoA Generator, and other analysis components). The SOC and CSIRT teams that are envisaged as primary users of the platform are shown to the left of the Orchestration and Integration Engine, as are the organisation's existing Security Monitoring Solutions. Although these Security Monitoring Solutions are not part of the SOCCRATES platform, they are able to trigger and interact with it.

The Threat Data Collection & Threat Prediction component (see figure 2, shown on the right) resides at an organisation that specialises in analysing malicious infrastructures. This component is thus outside the scope of the SOCCRATES platform itself, which is typically operated by a corporate SOC or MSSP. It does, however, interact closely with the SOCCRATES platform via the Threat Intelligence Platform (TIP), one of the native SOCCRATES platform components.

**The Evaluation**

The SOCCRATES platform will be evaluated in three pilots. The SOCCRATES platform will be implemented at managed security service provider mnemonic and at the corporate ICT SOC of Vattenfall. In addition, Shadowserver (CTI collection, processing & analysis) will provide the pilots with CTI. We have defined specific KPI's that will be assessed during the pilots.

The first two pilots will be closed because they will handle confidential customer data. The third (demo) pilot specifically is targeted at demonstrating the usefulness of the SOCCRATES platform to a wider audience. The site for the demo pilot is yet to be determined, and the decision will be based on experiences from the previous pilots.

**The Results**

The main target groups for SOCCRATES results are:

- Managed Security Service Providers (MSSPs);
- Security Operations Centres (SOCs);
- Cyber Security Incident Response Teams (CSIRTs);
- National Certs;
- Security Product Vendors;
- Regulatory bodies;
- Policy makers;
- Standardisation bodies.

Considering the wide variety of the target group, we utilize different communication channels, such as webinars, conference presentations, workshops, demonstrations, the SOCCRATES website, social media, video. One of the goals here is to raise awareness among the target groups on how to improve SOC/CSIRT operations with SOCCRATES results and disseminate project results to relevant target groups and

potential users of the SOCCRATES Platform and components. Concrete examples are the SOCCRATES introduction video (3) and accepted presentations on the 2021 One conference and the prestigious FIRST (Forum of Incident Response and Security Teams) annual conference.

Another objective is to ensure active exploitation of SOCCRATES results. SOCCRATES is a so called 'Innovation action' and is expected to deliver results on Technology Readiness Level (TRL) up to 6 (System Adequacy Validated in Simulated Environment), but we anticipate that some results will even be on higher level. The integrated SOCCRATES platform will consist of a mix of commercially available components and Open Source components. We do not foresee actual commercial exploitation of the entire platform. Commercial exploitation will most probably only be done by individual partners on a module basis. The platform should be seen as an example for automation in security operations and inspire SOCs, CSIRTs and security product vendors. With the SOCCRATES innovation results, individual partners will be able to enhance their existing products and consequently improve commercial exploitation of those products.

SOCCRATES has adopted an active Open Source approach, in which we utilize the existing open source channels of all partners to publish the results that are available as Open Source. The Adversary Emulation Planner is already available (https://github.com/mnemonic-no/aep).
Finally, in the end phase of the project we will define more concrete exploitation activities for after SOCCRATES has ended which will include (besides the commercial exploitation and Open Source results) also activities such as education and further research. For the last item we will prepare a vision paper.

**The Involvement**

In order to have a project sounding board and interaction with the real experts in the field we have arranged two different bodies to support us in this:

- SOCCRATES Advisory board - The SOCCRATES Advisory Board (SOCAB) forms an independent review group of external (non-funded) experts within relevant areas. SOCAB members provide external reflection on the operational and strategic direction of the project and are invited to visit project events, will contribute to the requirements, and review project results. We have 4 experts in the field from different areas as member in the Advisory Board.
- Stakeholder group - The SOCCRATES Stakeholder Group is a group of people working at SOCs, CSIRTS, National CERTs, MSSPs, end-users and vendors that have indicated to be interested in the results of the project. They will be informed about progress, encouraged to provide input and be invited for SOCCRATES events. The Stakeholder Group also is important for the exploitation of project results, where we expect some of the members to become early users of SOCCRATES results. We currently have 26 members of 24 different organisations and are still expanding our group. If you want to become a member, it's free! Please contact us.

## Current status

At this moment, we are already more than halfway of the project. The first half of the project mainly focussed on innovation, design and implementation. The second half of the project will be more focussed on evaluation and exploitation of results. We are well on track with delivering the results we promised in our original planning. The main evaluation pilot will start at the beginning of 2022.

## Lookout to next articles

In the coming articles (next editions of the PvIB magazine) we will zoom in on some of the SOCCRATES platform underlying technology and innovations and the challenges we encountered.
More info at www.soccrates.eu

*SOCCRATES has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No. 833481.*

References

(1) https://openc2.org/ and https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2
(2) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao
(3) https://vimeo.com/442734821