SOCCRATES

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

D8.4

White paper

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

Responsible organisation:	TNO
Editor:	Sebastiaan Tesink
Revision:	1.0

Abstract	This deliverable contains the SOCCRATES (high level) results and experiences in an easy accessible way, suitable for policy makers and higher management of stakeholders. It will be available on-line. It is more or less a manage-ment summary of D2.4 (Vision paper) and D7.2 (pilot evaluation) complemented with some high level experiences from D7.3 (best practices guide).
Keywords:	Security automation, SOC, CERT, CSIRT, Au-tomated Security.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 833481
Call H2020-SU-ICT-2018 • Innovation Action • Start date: September 1st, 2019

Management summary

The digital security landscape is facing multiple challenges. First of all, IT infrastructures are becoming increasingly more complex, they are continuously evolving and are becoming highly interdependent. Second, both the number and complexity of attacks are rapidly increasing. Moreover, attacks are getting more automated, while the response is still human-centred. Finally, there is a shortage of skilled cyber-security workforce.

To counter these challenges, the SOCCRATES project developed a security automation and decision support platform, 'the SOCCRATES platform', that delivers:

- A Security Automation, Orchestration and Response (SOAR) platform
- Automated security reasoning (real-time threat & impact assessment)
- Automated generation and assessment of response actions (both pro-active & reactive)
- Automated dynamic response

The SOCCRATES platform was used to automatically produce security controls for five different use cases. The first being an active ongoing attack in the IT infrastructure of an organization, the other four were pro-active in nature to increase the cyber resilience of the organization. The MAPE-K reference model, commonly used in autonomic computing and self-adaptive systems, was used to as a basis for the automation of the SOCCRATES Platform within these five use cases.

In this white paper, the results and experiences of the SOCCRATES project are summarized for different types of target audiences. The main take away for all audiences is that SOC automation is a game changing innovation, by going beyond the detection of security incidents, and by shifting the focus to security reasoning.

Contributor(s)	Reinder Wolthuis (TNO) Sebastiaan Tesink (TNO) Richard Kerkdijk (TNO)

Reviewer(s)	Frank Fransen (TNO)

TABLE OF CONTENTS

1 INTRODUCTION 5
1.1 The SOCCRATES project 5
1.2 This deliverable 6
1.3 Structure of this deliverable 6
2 POSITIONING SOCS AND CSIRTS 7
3 TRENDS & SOCCRATES VISION 9
4 SOCCRATES PLATFORM 12
4.1 SOCCRATES Use Cases 12
4.2 General flow 13
4.2.1 Monitoring phase 14
4.2.2 Analysis phase 14
4.2.3 Mitigation & response planning phase 15
4.2.4 Mitigation & response execution phase 16
4.3 Platform Software and Demonstrator 16
5 TAKE AWAYS 18

Classification level: Public

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.

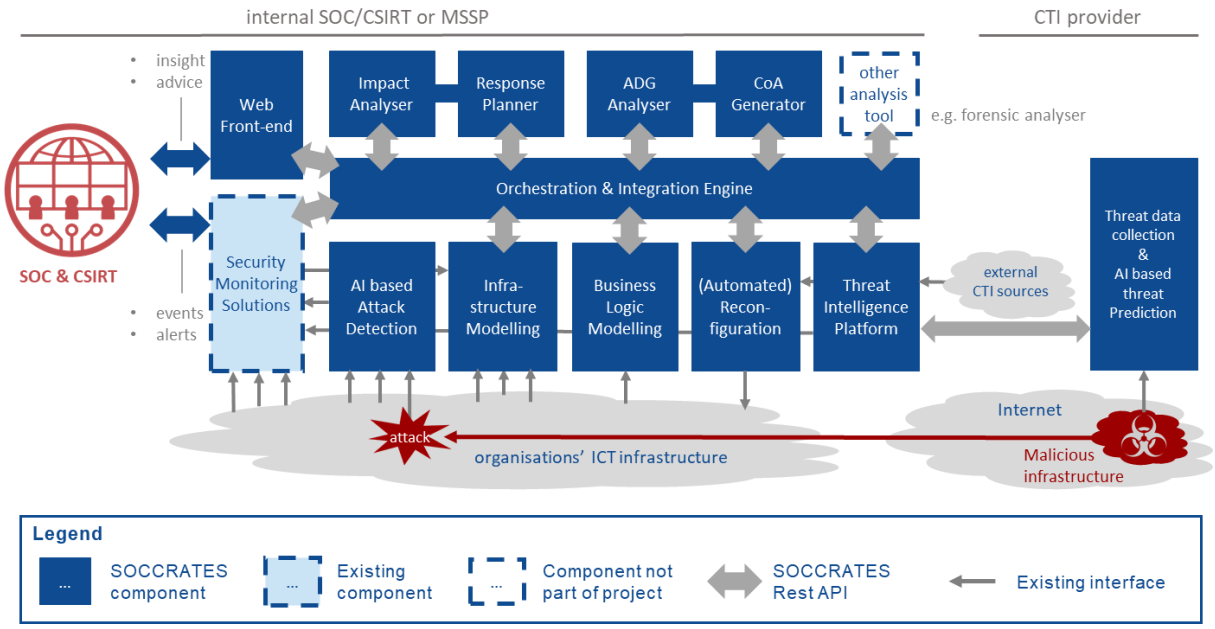


Figure 1-1: The SOCCRATES platform

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 This deliverable

With the SOCCRATES EU H2020 project drawing to a close, it is important to identify the key take-aways and lessons learned. The goal of this deliverable is to present these high level results and experiences in a structured and accessible way, providing a suitable management summary.

Whereas other SOCCRATES deliverables are more technically oriented, the aim of this paper is to provide higher management policy makers and (higher) management of organizations with a management summary on the SOCCRATES vision, results, and lessons learned of a pan-European innovation project in Security Operation Centre (SOC) and Computer Security Incident Response Team (CSIRT) automation. The intended target audience for this paper is:

- EU Cyber security competence centres (e.g. ECCC, ENISA, REA, and DG Digital).
- National cyber security centres.
- Higher management policy makers of organizations that have an operational SOC or intend to build a SOC in the near future.
- Responsible persons for SOC/CSIRTS within end-user organizations.
- Product managers at security vendors and service providers.
- R&D community (such as RTOs, and academics).

1.3 Structure of this deliverable

Since the terms SOC and CSIRT are applied in different contexts, in chapter 2 an overview is given of SOC and CSIRT applied to security teams at different levels across Europe. Next the trends and vision that insipered and motivated the work in the SOCCRATES Project are described in chapter 3. In chapter 4, the SOCCRATES Platform is described along the SOCCRATES use cases. Finally, in chapter 5 the take aways of the SOCCRATES project ar described per target audience.

2 Positioning SOCs and CSIRTs

Although the terms SOC and CSIRT are applied to security teams at different levels across Europe, they may provide different functions and services depending on their position in the SOC and CSIRT clusters and layers demonstrated in Figure 2-1.

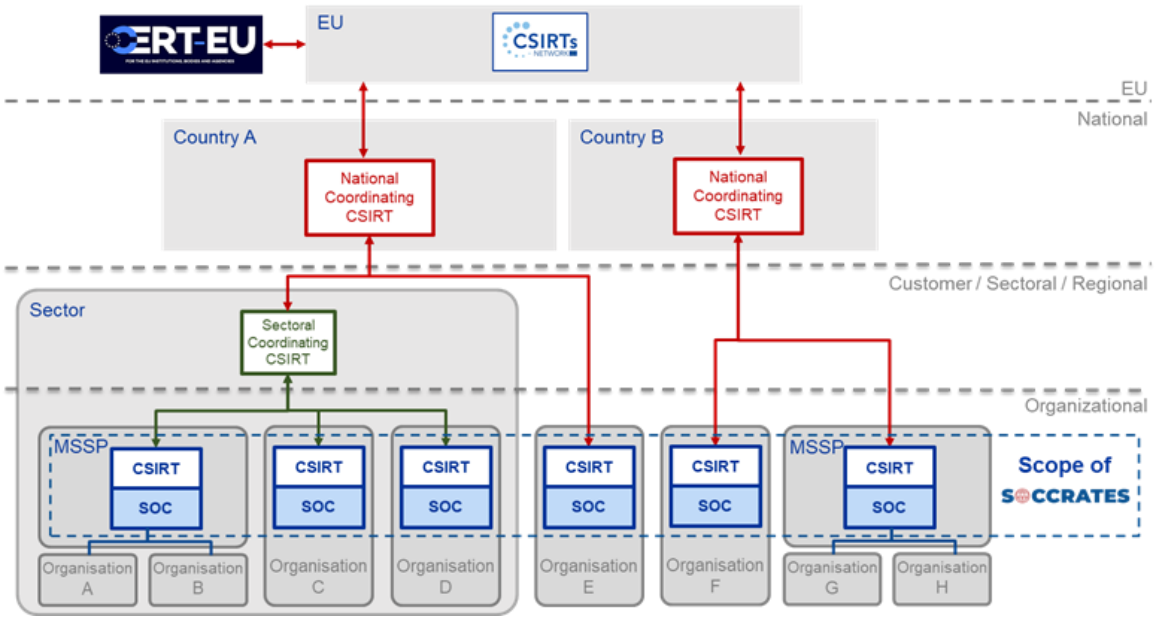


Figure 2-1. SOC and CSIRT clustering and layering

The clusters and layers are from top to bottom:

- CERT-EU[1] - This is a specific CSIRT on EU level and is the Computer Emergency Response Team for the EU Institutions, bodies and agencies. It is composed of IT security experts from the main EU Institutions. CERT-EU provides services to keep the ICT infrastructure of all EU institutions, bodies and agencies secure and cooperates with other CERTs/CSIRTs in the Member States and with specialised IT security companies in order to respond to information security incidents and cyber threats.
- CSIRT network[2] - The CSIRTs Network is a network composed of EU Member States' appointed national CSIRTs and CERT-EU ("CSIRTs Network members"). The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request. The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and coordinate response to specific incidents. The NIS Directive[3] in Article 12 establishes the CSIRTs Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation".
- National CSIRTS – These CSIRTs have the task to enhance a nation's resilience in the digital domain, prevent or limit the failure of the availability or the loss of integrity of information systems of vital operators and central government, and to handle severe computer attacks against critical infrastructure and information within the nation. Examples of such national

[1] https://cert.europa.eu/

[2] https://csirtsnetwork.eu/

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&rid=8#d1e39-1-1

CSIRTs are the Dutch National Cyber Security Centre (NCSC)[4] or the Norwegian NorCERT, hosted by the Norwegian NCSC[5].
Although the higher layers are primarily based on CSIRT capabilities and services, this does not exclude that also some monitoring and detection capabilities are executed jointly on regional or national level. This is, however, not really common considering the sensitive nature of monitoring data and specific (sensitive) knowledge required of monitored infrastructure.

- Sectoral or Regional CSIRTs – In some sectors or regions there are sector or regional CSIRTs, that collect and analyse threat intel, translate this to the specific context of the sector or region and distribute it within the sector/region organizations. Sectoral CSIRT activities may go beyond the ISAC activities, e.g. security incident coordination at sectoral level. Examples where such sector CSIRTs have been set up are healthcare, government and finance.
- Coordinating CSIRTs - National, sectoral and regional CSIRTs, the two middle layers of Figure 2-1, are coordinating CSIRTs. They provide services to a set of organizations known as their constituency (e.g. organisations in a sector, region, country, etc.). Services that these types of CSIRTs provide typically include:
    - coordination of security incidents (across organisations within the constituency),
    - acting as a single point of contact,
    - distribution of cyber threat intelligence, best practices, and training material, and
    - providing security incident analysis and forensic services.

  Note that coordinating CSIRTs sometimes operate at a same level as the Information Sharing and Analysis Centres (ISACs). ISACs are non-profit member driven organizations that facilitate gathering and sharing of information on cyber threats (relevant for the members). ISACs have been created around particular private sectors (e.g. finance, energy, health). They may facilitate two-way sharing of information between the private and the public sector, and serve as a focal point on the national level to gather information about cyber incidents and analyse it[6]. In that sense, ISACs play an important role within EU Cybersecurity Strategy.
- Organizational SOCs/CSIRTs – In the lowest layer of Figure 2-1, the SOCs/CSIRTs of an organization are represented. There are different types of organizational SOC/CSIRT set-ups:
    - Organizations that have their own CSIRT and/or SOC.
    - Organizations that make use of CSIRT and/or SOC services provided by a commercial Managed Security Service Provider (MSSP).

The primary focus within the SOCCRATES project are the SOCs/CSIRTs operating at the organizational level. Despite this focus, the different layers and sectors are of course highly interdependent, especially during severe security incidents. SOCCRATES took this intertwined relationship between SOCs/CSIRTs at different levels into account in its design of the platform and interfaces.

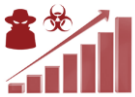
[4] https://english.ncsc.nl/

[5] https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/

[6] ENISA, *Information Sharing and Analysis Centres (ISACs) - Cooperative models*. European Union Agency For Network and Information Security. 2018

3 Trends & SOCCRATES vision

The increasing dependency of organisations and society as a whole on IT systems and networks and the increase of cyber security incidents with major impact, has led to organisations (and governments) increasing their spending on cyber security. Many organisations have established a SOC and CSIRT to protect the organisation against cyber-attacks, or contracted a MSSP to per-form these operational cyber security services for them. Despite the increased spending and new investments in cyber defences, most organizations are unable to keep up with the ongoing evo-lution of threats and attack methods. Present day SOC and CSIRT capabilities simply do not suffice to deal with the persistence and sophistication of professional threat actors. As it stands now, the gap between defenders and attackers will only increase further in the coming years. The following four challenges contribute greatly to this trend:

<table>
<tr><td>
ICT is increasingly complex, changing & interdependent</td><td>ICT is increasingly complex, changing & interdependent
The ICT infrastructure of organisations is continuously changing at an increasing pace. Introduction of new technologies, such as IoT, cloud services, and CI/CD, demand that the security teams at the organisation also adapt and learn about how to secure these technologies.</td></tr>
<tr><td colspan="2">Increasing number and complexity of attacks
The threat landscape is continuously changing and security incidents have been on the rise. The cyber-attacks are becoming more complex, targeted and automated. The security teams have to continuously learn about these new threats and attack techniques, and be able to quickly adapt so they can defend against them.</td><td> 
Increasing number and complexity of attacks</td></tr>
<tr><td>
Attacks get more automated, response is human-centred</td><td>Attacks get more automated, response is human-centred
Threat actors are increasingly using automated attack tools. The response handling in SOCs and by CSIRTs, however, is still very human-centred. This will lead to an uneven battle: machine speed versus human speed. In order to reduce the time to detect, respond and recover, security teams have to increase the level of automation in incident response.</td></tr>
<tr><td colspan="2">Shortage of skilled cybersecurity staff
The quality and effectiveness of security operations heavily depends on skilled cybersecurity experts, while at the same time there is a clear shortage of skilled cybersecurity workforce for several years. Recruiting, hiring and retaining cybersecurity staff for SOC and CSIRT is challenging.</td><td>

Shortage of skilled cybersecurity staff</td></tr>
</table>

This trend can only be stopped through a fundamental game changer. SOCCRATES vision is to increase the level of automation in SOC / CSIRT operations to increase:

- the speed and effectiveness of *detection of* and *response to ongoing attacks*, and
- the scope, effectiveness and efficiency of *proactive analysis of threats* to the ICT infrastructure to enhance its cyber resilience. Potential threat sources that are considered are changes in the infrastructure, new vulnerabilities and new cyber threat intelligence.

Nowadays, so called Security Automation, Orchestration and Response (SOAR) capabilities are available and can be considered to be a central starting point for SOC automation. The vision of SOCCRATES is to build *Automated security reasoning capabilities* on top of these SOAR solutions to to

form a better understanding of the current security posture (for instance information on the vulnerability involved, potential attack paths through the organization's ICT infrastructure, and potential business impact of an attack) as well as to deliver a higher quality of response action by automatically assessing and ranking possible response actions. In order to close the response loop and to increase the speed of responding to ongoing attacks and emerging threats, the ICT infrastructure has to be adapted, so it can support automatic instantiating and/or reconfiguring of security controls. Such *automated response capability* will in many environments include a human-in-the-loop, but in modern ICT environments (e.g. programmable infrastructure, cloud-native technology) this may even be a fully autonomous response systems.

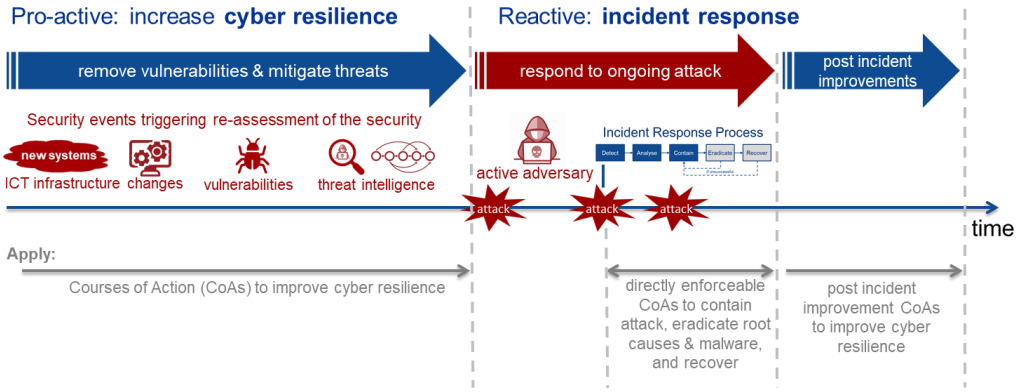


Figure 3-1. Proactive and reactive responses

In summary, during the SOCCRATES project new automation capabilities were developed on top of the already existing capabilities, see Table 3-1.

Table 3-1. New capabilities to be developed for automation

	SOC	CSIRT
Current capabilities	• Monitoring and detection • Event analysis • Information security incidents analysis (triage) • Vulnerability analysis • Awareness Building	• Information security incidents analysis (incl. CTI collection, analysis and correlation) • Artefact and forensic evidence analysis • Information security incident coordination • Vulnerability coordination • Awareness Building
	• Event detection (through alerting and/or hunting) / threat hunting • SOC tool life-cycle support (incl. operations and maintenance, tuning tools (e.g. detection sensors), engineering and deployment, and R&D)	
New capabilities	• Security Automation, Orchestration and Response (SOAR) • Automated security reasoning (real-time threat & impact assessment) • Automated generation and assessment of response actions (both pro-active & reactive) • Automated dynamic response	

The SOCCRATES project has identified and worked on the following challenges for SOC and CSIRT operations that will support the implementation of the new capabilities:

- Machine-readable model of the infrastructure; enabling the analyst to go back in time through the infrastructure model.
- Improvement of detection capability and coverage; by using AI-based Attack Detection capabilities, with the capability to determine the attack step.

- Advanced use of Cyber Threat Intelligence; using Domain Generation Algorithms detection to identify Command and Control traffic.
- Real-time Business Impact Assessment; by mapping the Enterprise Architecture with the technical Infrastructure Architecture, the platform is able to automatically determine the business impact of security events.
- Automatically generate courses of action (CoAs); dynamically rank and propose the best security playbook.
- Automation and orchestration to improve SOC response; dependent on the use case (see section 4.1) and the attack stage detected in an active attack, a different workflow is selected, resulting in a different orchestration of all the platform components.

4 SOCCRATES Platform

SOCCRATES addresses the challenges as described in the previous paragraph by developing a security automation and decision support platform, 'the SOCCRATES platform'. The SOCCRATES platform is depicted in Figure 1-1 and 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.

The development of the SOCCRATES Platform has been guided using five different use cases for security operations. These use cases will be introduced in the next section. How the SOCCRATES Platform automates these use cases is described in section 4.2. Finaly, this section elaborates on the results of the development of the SOCCRATES Platform.

4.1 SOCCRATES Use Cases

To guide the development and validate the platform's capabilities, five different use cases have been defined. The use cases have been selected to represent the most relevant situations in which an organisation needs to reassess the security state of their ICT infrastructure, and determine if and how to react in order to protect the organisation's interests. The use cases are characterized by a particular security event that triggers the SOCCRATES platform to analyse and determine the best mitigation or response strategy.

- *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.

There is a crucial difference between use case 1 and the other use cases. In use case 1 the organisation is responding to a detected ongoing attack. That means that an active adversary has access to the organisation's ICT infrastructure and poses an imminent threat to the organisation. An organisation must be very careful when responding to the attack, as this can tip off the attacker. Use case 2 to 5 are triggered by security events that allow an organisation to improve the security in order to prevent an attacker to make use of it. In other words, these use cases focus on preventing incidents and are focussed on increasing the cyber resilience of the organisation, see Figure 4-1.

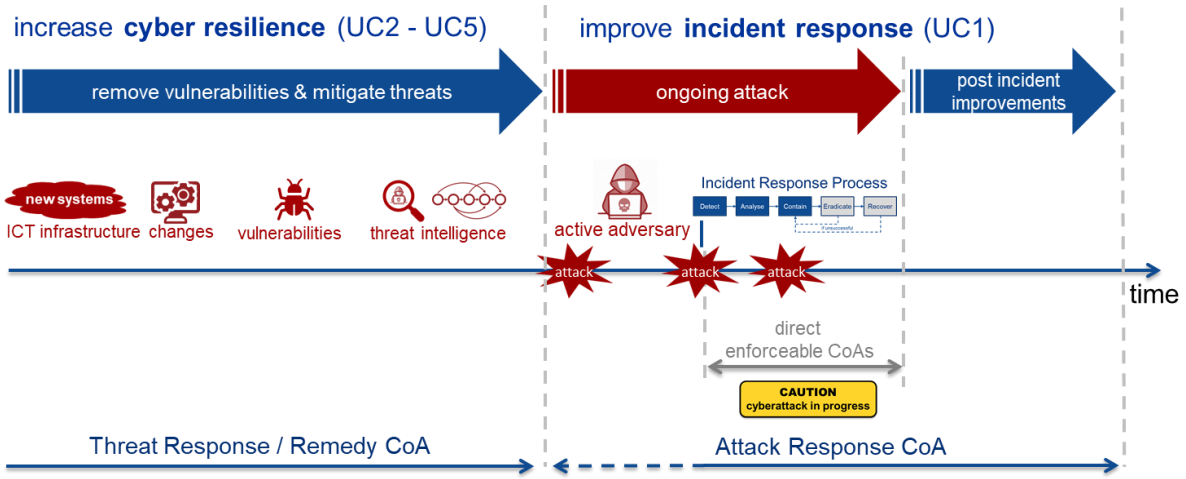


Figure 4-1: Use cases along an incident response time-line

4.2 General flow

The SOCCRATES Platform automates these use cases in a similar manner along the four phases of the MAPE-K reference model: Monitor, Analyse, Plan, Execute and Knowledge. MAPE-K commonly used in autonomic computing[7] and self-adaptive systems. The four phases are (see Figure 4-2):

1. *Monitoring phase (M)* – the system monitors for security events specific to the five use cases, and triggers the orchestration function of the SOCCRATES platform.
2. *Analysis phase (A)* – in this phase the SOCCRATES platform will automatically analyse the security event by collecting additional data, assessing the threat and determine the potential business impact. This is then presented as *situational awareness* to the SOC analyst. The SOC analyst may at this stage escalate to a CSIRT member.
3. *Mitigation & response Planning phase (P)* – in this phase the SOCCRATES platform will automatically generate possible responses, courses of action (CoAs), to mitigate threats or contain the ongoing attacks. The CoAs are assessed on effectiveness and business trade-off (i.e. operational business impact versus the costs of implementing the remediation). This is then presented as *option awareness* for the SOC analyst / CSIRT member.
4. *Mitigation & response Execution phase (E)* - in this phase the SOC analyst / CSIRT member is able to select a CoA, and the SOCCRATES platform prepares and initiates the (semi)automated execution of this CoA.

[7] An architectural blueprint for autonomic computing, IBM whitepaper, June 2005
https://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf

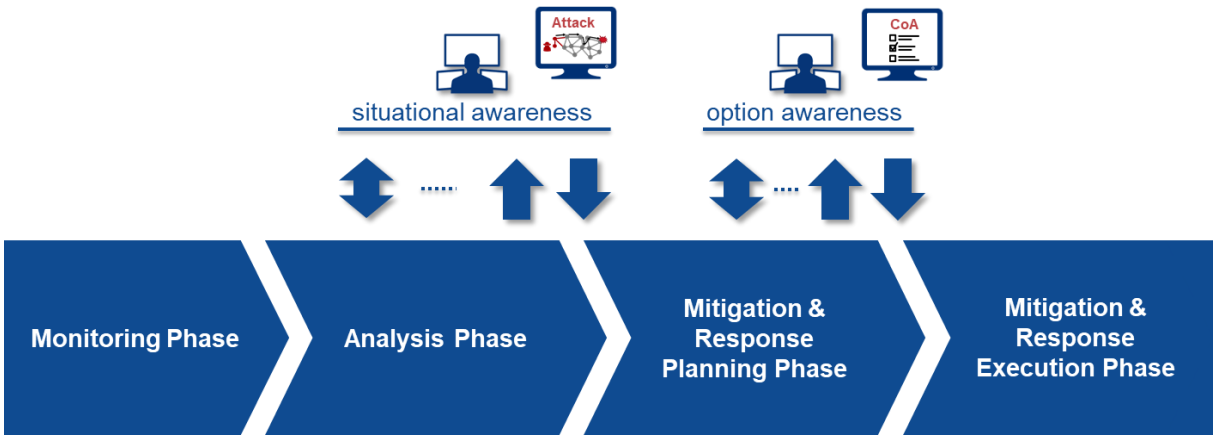


Figure 4-2: General flow for the SOCCRATES use cases

The SOCCRATES platform uses an Orchestration and Integration Engine (OIE) to integrate, manage, and orchestrate all other components through these four phases. The OIE consists of an open source workflow tool, *Activiti*[8], and the *Cortex framework*[9] from the TheHive project[10] for easy integration of security tools. In the following sections the role of the SOCCRATES components are described in each of these four phases.

4.2.1 Monitoring phase

For automating response on detected ongoing attacks (use case 1) it is necessary to detect attacks with high certainty and provide additional information on the attack stage (e.g. initial compromise, lateral movement, or exfiltration). For this purpose, the SOCCRATES project developed an AI based reasoning engine, that analyses the attack stage based on on the events generated by several attack detection tools. The AI based Attack Detection (AAD) component will reduce the false positive rate, will improve understanding of the situation, and will identify sequential patterns.

For the collection of CTI and triggering the SOCCRATES platform based on new threat Intelligence (use case 2) the SOCCRATES platform incorporates an open source Threat Intelligence Platform (TIP), called ACT developed by SOCCRATES partner mnemonic. The platform is extended with tools for creating adversary emulation plans.

For the discovery of new vulnerabilities, configuration changes and new systems (use cases 3, 4 and 5 respectively) existing vulnerability scanners, network scanners and asset discovery tools were implemented. These scanning tools can also be used to automatically collect information to generate models of the organization's ICT infrastructure. To facilitate model generation, the SOCCRATES project developed an Infrastructure Modelling Component (IMC). The IMC provides the SOC and CSIRT with a real-time visualisation and understanding of the environment they are defending. The models can also be used for innovative analysis tools such as automated threat modelling and attack simulation.

4.2.2 Analysis phase

After having collected additional data, the SOCCRATES platform performs a threat analysis. An Attack Defence Graph (ADG) analysis is performed to predict how attackers could propagate through

[8] https://www.activiti.org
[9] http://docs.thehive-project.org/cortex/
[10] https://thehive-project.org/

Classification level: Public

the ICT infrastructure. The results of this analysis can be used to determine the potential effect of a new threat, new vulnerability, or changes in a system's configuration. The ADG based analysis can also be used during an ongoing attack to determine how other systems could get compromised allowing the attacker with access to business critical systems, or to support root cause analysis. Based on the adversary emulation plan provided by the TIP, the ADG will analyse how a particular adversary (i.e. a specific APT group) could compromise the infrastructure. The ADG is based on research from the Swedish university KTH [4] [5], together with the spin-off company foreseeti, who jointly developed the commercial product securiCAD.

To estimate the operational impact of a new threat or attack on the business, the SOCCRATES project developed a Business Impact Analyser (BIA) component that uses business logic modelling to build a graph representing the dependencies between the technical assets and the business missions, functions and processes. The BIA component will quantify the (potential) impact and provide the terminology of affected business functions and processes, enabling the SOC analyst to communicate more effectively to business owners during a security incident.

The results of the analysis will be provided to the SOC Analyst. Based on this information the SOC analyst may decide that it is necessary to act, and initiate threat or attack response (e.g. contain an ongoing attack). The SOCCRATES Platform will then proceed to the mitigation & response planning phase.

4.2.3 Mitigation & response planning phase

For use case 1, the main focus of mitigation & response planning is on containing the ongoing attack. These attack response actions must be immediately enforceable and typically only active during the incident response process. Containment CoAs (CCoAs) are the most efficient countermeasure to put an end to the ongoing attack. Next to these CCoAs, the SOCCRATES platform enables the SOC analyst to stop exfiltration to prevent an adversary to regain access after recovery (root cause CoAs), and to protect critical assets during the attack (Impact Reduction CoAs).

For use cases 2 to 5, the response action could be structural changes, like the introduction of new security measures, changes in network configuration, or the deployment of software patches. Since these changes are less time sensitive, these are referred to as *planned responses*. A combination of *directly enforceable* and *planned* responses is also possible. An organisation can choose to first block certain traffic to the vulnerable system until a patch is deployed (i.e. directly enforceable response) and later deploy a software patch (i.e. planned response). Post incident response for UC1 may include structural changes based on lessons learned during the analysis and aftermath of the incident. The SOCCRATES platform has two components that can produce CoAs. First of all, the CoA Generator is based on the use of the ADG. Since the attack languages used by the ADG includes all kinds of different defences, it is possible to turn on certain defences in the model of the ICT infrastructure and analyse the potential improvement. An algorithm is developed to automatically optimise the selection of defences within a given total cost factor (each defence can be assigned a financial cost and/or deployment time).

The second component that produces CoAs is the Response Planner. This component focusses on identification of directly enforceable response actions for instance to contain compromised hosts. As part of the analysis the CoA Generator will provide information on the effectiveness of the recommended CoA. For financial assessment of the CoA, the Response Planner can calculate the Return on

Response Investment (RORI). In addition, the Business Impact Assessment component can be consulted to determine if the CoA will have negative consequences for the business functions and processes.

The SOCCRATES platform will present the list of generated CoAs with the analysis on effectiveness, RORI and business consequences to the SOC/CSIRT analyst, thereby enabling the analyst to make informed decisions on the response actions.

4.2.4 Mitigation & response execution phase

When the analyst selects the CoAs to be executed, the SOCCRATES platform will initiate the (semi-)automatic execution of the CoAs. For many organisations automated execution of security responses and reconfiguration of security controls is a new and potentially scary concept. Moreover, for MSSPs it is typically not allowed to perform reconfigurations in their customers network. Therefore, the basic response execution of the SOCCRATES platform is to automatically send either support tickets or e-mails containing the recommended CoAs to their IT department. This enables the integration of a human in the loop for authorisation of the CoA execution, and to include manual reconfiguration. For the automatic execution of the CoAs, SOCCRATES has adopted two machine readable languages that are being specified by OASIS Open:

- *Collaborative Automated Course of Action Operations (CACAO)* [8] – standard for implementing course of action playbooks for cybersecurity operations.
- *Open Command and Control (OpenC2)* [7] – language for the command and control of technologies that provide or support cyber defences.

CACAO is used to combine multiple response actions (defined with OpenC2) into a playbook and add meta data. OpenC2 is used to formulate response actions, such as filter traffic or contain hosts, in a machine-readable language.

4.3 Platform Software and Demonstrator

In the previous section, the SOCCRATES Platform components have been introduced. These components have been specified, developed, and deployed in pilot and demonstration environments. The SOCCRATES website[11] contains an overview with for each of the components a brief description, list of software componnets and information on how to get access to the software (see Figure 4.3).

Not all software is available as open source. For the licensed or commercial software contact information has been provided on this webpage. Furthermore, not all integration components or IMC adapters have been made available, as they were very specific for demonstration or for the pilot environment. Table 4-1 provides an overview of SOCCRATES Components and how the software is distributed.

Since the SOCCRATES Platform is a collection of both open source and commercial software components, it is not possible for the SOCCRATES project to distribute the SOCCRATES Platform as a whole. Furthermore, any deployment of the SOCCRATES Platform needs to be adapted to the specific environment (i.e., integration with existing security tools and data formats). The SOCCRATES project

[11] https://www.soccrates.eu/platform-software/

therefore provides the means to get access to the SOCCRATES Platform components and has setup a demonstration of the SOCCRATES Platform to inspire others of the vision, and to encourage them to develop their own solution for their environment and potentially re-using some of the SOCCRATES Platform components.

The SOCCRATES Platform demonstration has been developed to show how the platform provides situational awareness and option awareness to support decision making by the SOC analyst. Deliverable D6.4 describes the final version of the SOCCRATES Platform and a walktrough of UC1 and UC2 on the SOCCRATES Platform demonstration.

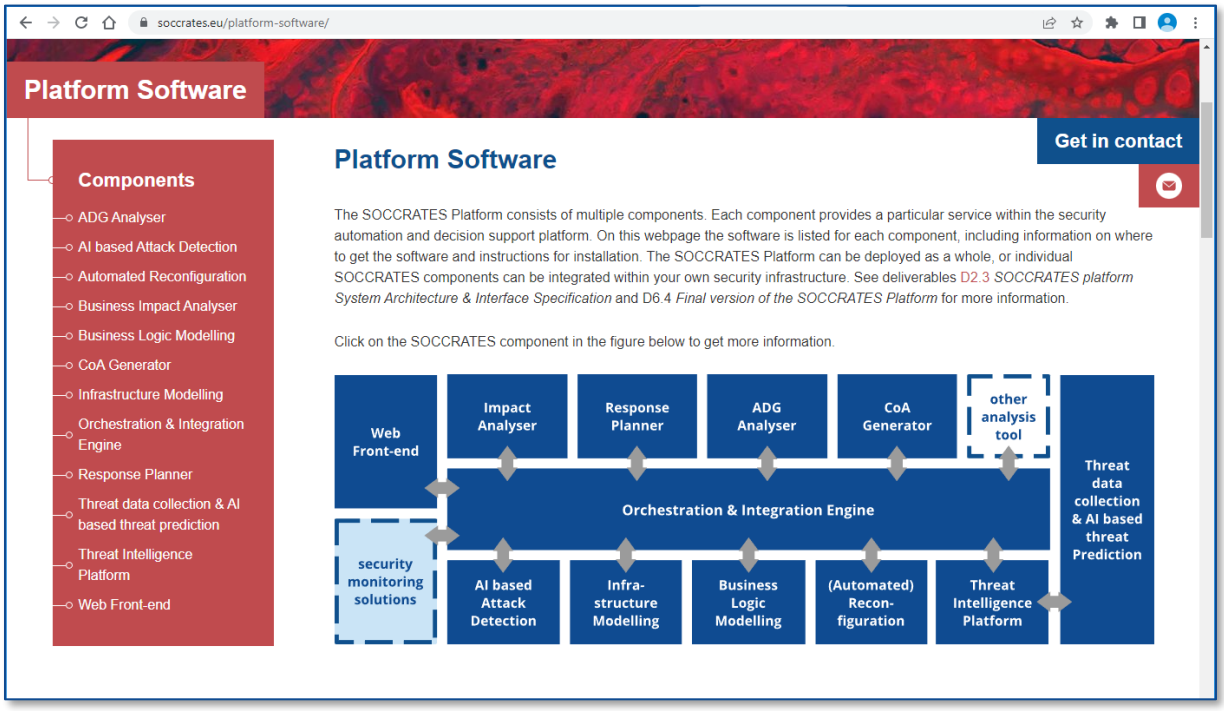


Figure 4.3: Web page on SOCCRATES website with information on the platform software

Table 4-1 : Overview of SOCCRATES Components and availability of software

SOCCRATES Component name		Availability
AAD	AI based Attack Detection	Set of commenrial and open source tools
ADG	ADG Analyser	Commercial product securiCAD
AR	Automated Reconfiguration	Open source software
BIA & BLM	Business Impact Analyser & Business Logic Modelling	Open source software
CoAG	Course of Action Generator	Open source software
IMC	Infrastructure Modelling component	Open source software
OIE	Orchestration & Integration Engine	Commercial license & open source software
RP	Response Planner	Open source software
TDC&TP	Threat Data Collection & Threat Prediction	Open source software & public service
TIP	Threat Intelligence Platform	Open source software

5 Take aways

The key take aways of the SOCCRATES project can be split per target audience group mentioned in section 1.2.

EU Cyber security competence centres

As in many other projects, during the SOCCRATES project, new potential research angles were encountered. In some cases, a first step was taken, for instance with the extension of the SOCCRATES platform with tools for creating adversary emulation plans. Nevertheless, unsolved research questions remain to fully close the loop from detection to remediation. The task at hand in the domain of autonomous security can be compared to the levels of autonomous self-driving vehicles[12]. With SOCCRATES, it was demonstrated that level 1 in autonomous security can be reached (i.e. human assisted technology). However, not all technology developed within SOCCRATES is ready to be put on the market, since several components are still at a low Technology Readiness Level (TRL)[13].

In order to improve the balance between attackers and defenders, there is a role for the EU competence centres to invest in projects that improve automation solutions and steer in the direction of autonomous security. Although several commercial products are gaining momentum, such as SOAR solutions, a lot of work still needs to be done to properly integrate these products with all levels of organizations, from strategic to operational levels. Moreover, SOCCRATES encourages this to be an open solution for integration with security vendors, with the development of an open source Automated Security Platform.

National cyber security centres

As described in section 2, cyber security centres are exchanging a lot of information with SOC/CSIRT teams at an organisational level. This information exchange could be more efficient and effective, if the national cyber security centres support the automation efforts of organisations. For instance, the exchange of CACAO playbooks to automate workflows during a specific security incident, could help to support the organisation. Defining clear interfaces and standards that can be used in case of a security incident would thus support the target group of SOCCRATES.

Higher management policy makers

At the organisational level, a generic take away is that SOC analysts and security personnel in general are scarce. Therefore it is essential to invest in automation, not to take away their job, but to make the work of a SOC analyst less repetitive, with more interesting challenges at hand, so that they remain at the organization.

Integrating and embedding the SOCCRATES platform in the pilot sites proved to be a challenging activity. The pilot sites already had different security solutions in place, as well as different processes in their SOC teams. When dealing with an existing SOC, embedding security automation is a difficult task that requires the investment a lot of resources. Management support for this is investment for the future is a key element.

In a greenfield situation, in which there is an intention to build a SOC in the near future, it is important to immediately start thinking in automating SOC processes. Embedding a security solution into your organization at a later stage will be more cumbersome and expensive.

[12] https://www.epa.gov/greenvehicles/self-driving-vehicles

[13] https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level

However, when implemented well, the SOC solution could deliver a high return, especially when the solution takes into account the business impact of security events. Investment in security controls can be made more effectively when based on potential business impact and risk management.

Responsible persons for SOC/CSIRTS within end-user organizations

For people managing a SOC/CSIRT within an end-user organization, the key take aways are to start automating. Nowadays, attackers are well-organized teams, and are a step ahead in automating attacks. Moreover, the attackers have to be able to launch one successful attack to gain access to the organizational infrastructure, whereas the defenders have to defend the entire infrastructure successfully 24/7. This is an asymmetrical fight that cannot be won without automation.

Although current SOAR solutions can provide basic functionality, it is important to take a step further while embedding automation in the organization. One example of this next step taken by SOCCRATES is the translation of what a security incident means in terms of business impact. In order to provide the organization with this, an enterprise architecture and a technical infrastructure model need to be in place. Based on the infrastructure model, attack simulations can be performed such ADG analysis.

Another improvement compared to current SOAR solutions is the ability to provide dynamic playbooks, instead of static pre-defined playbooks.

Another important take away is to integrate the efforts of the SOC/CSIRT automation with the IT department. Automating security controls may also have a big impact on their business. Furthermore, the steps towards autonomous security solutions are based on building trust in such a solution. It is important to have management support in building this trust.

Product managers at security vendors and service providers

The SOCCRATES platform consists of both open source components as well as closed source commercial products from security vendors. The entire platform was developed as a micro-service architecture. This approach uses server applications as a set of small services, providing basic services to the SOCCRATES platform. This makes the SOCCRATES very versatile and dynamic. However, the interfaces between components, the input they require and the output they can deliver, need to be well specified.

For security vendors, it is important to bring the abilities of automation to their services and products. This can be realized for instance by publishing OpenAPI[14] specifications for their products, and building security products based on a micro-service oriented architecture such as Docker[15] or Kubernetes[16].

For service providers, such as ISPs and MSSPs, there is an opportunity to deliver services tailored to their customers infrastructure, for instance by having a better understanding of business impact of security incidents in the customer's infrastructure, and by proactively determining and countering possible attack paths.

R&D community

Within the R&D community, there has been a strong focus on the detection of cyber-attacks, especially by introducing machine learning algorithms to lower the false positive rate, thus reducing alert fatigue with the SOC analysts. The key take away for this target audience is to go beyond the detection of security incidents, and shift the focus to security reasoning.

[14] https://www.openapis.org/

[15] https://www.docker.com/

[16] https://kubernetes.io/

A completely new research field is opening up, in getting situational awareness within technical infrastructures, reasoning what an attacker could do related to business impact on the organisation, and finally by gaining a view on the available options and optimisation of the quality of playbook selection.