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 - Real-time threat, impact analysis and response automation for SOC/CSIRT operations

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 second article on the project will zoom in on the security automation process and the role of each of the SOCCRATES platform components. The article concludes with some discussion and challenges we encountered.

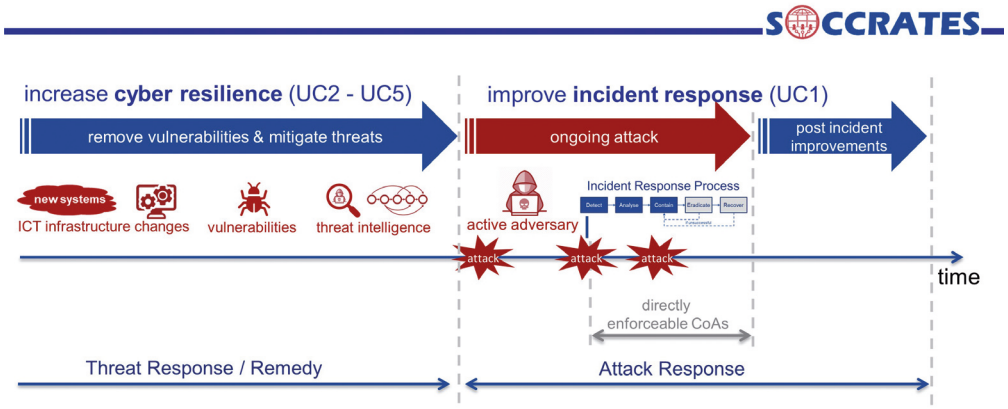

Figure 1 - The SOCCRATES use cases along an incident response time line.

The SOCCRATES project was introduced in the previous article. It gave an overview of the challenges that SOCs and CSIRTs currently face when defending their organisation's complex and continuously evolving ICT infrastructures against complex cyber-attacks and emerging threats, while at the same time there is a shortage of qualified cybersecurity talent. We described how the project addresses these challenges by developing a security automation and decision support platform, 'the SOCCRATES platform'. We will now look in a little more detail to the SOCCRATES platform and its role in the SOC and CSIRT process.

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 can potentially cause lots of harm. An organisation must be very careful when responding to the attack, as this can tip off the attacker. For use case 1 we thus follow the incident response steps: detection, analysis, containment, eradication, and recovery, as described in NIST SP800 61 (1) and the ISO/IEC 27035 series (2). Within SOCCRATES we decided to focus the automation, that is provided by the SOCCRATES platform, on the first three steps of incident response (detection, analysis and containment).

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 1.

General flow

When analysing the automation of these use cases, four common phases can be distinguished that are inspired by the MAPE-K (Monitor, Analyse, Plan, Execute and Knowledge) reference model used in autonomic computing (3) and self-adaptive systems. The four phases are (see figure 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, so called courses of action (CoAs), to mitigate threats or contain the ongoing attacks. The CoAs are assessed on effectiveness and business trade-off (i.e. costs, operational impact). 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 has selected a CoA and the SOCCRATES platform prepares and initiates the (semi)automated execution of this CoA.

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, and the Cortex framework from the Hive project for easy integration of security tools. In the following sections the role of the SOCCRATES components are described in each of these four phases.

Monitor phase

Based on the five use cases we can easily identify the security events for which we require monitoring capability.

For automating response on detected ongoing attacks (use case 1) it is necessary to detect attacks with high certainty and provide information on the attack stage (e.g. initial compromise, lateral movement, or exfiltration). For this purpose, the SOCCRATES project developed a concept to use an AI based reasoning tool on the events generated by different attack detection tools. The AI based Attack Detection (AAD) component will reduce the false positive rate, improves understanding of the situation, and identifies sequential patterns.
For collecting and triggering the SOCCRATES platform based on new threat Intelligence (use case 2) we use an open source Threat Intelligence Platform (TIP), called ACT. Since we also wanted to trigger new evaluations on threat actor profiles, the platform is extended with tools for creating adversary emulation plans.

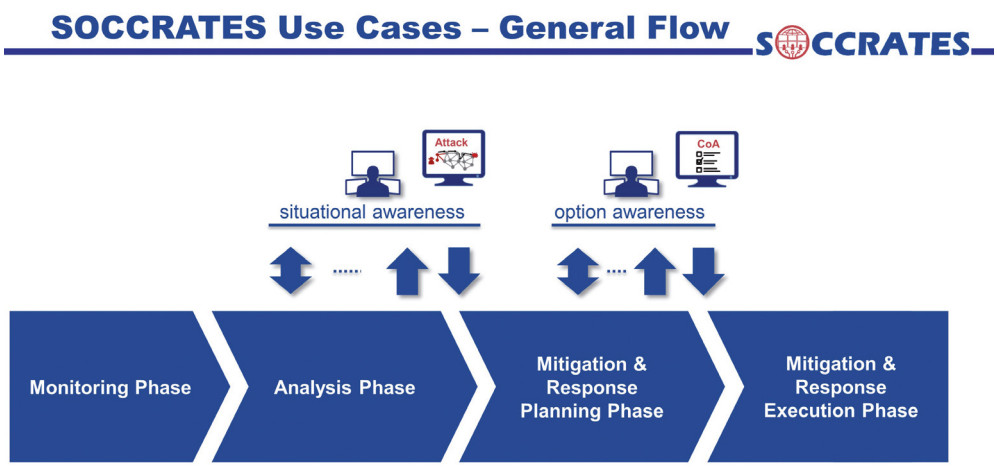

Figure 2 - General flow for the SOCCRATES Use Cases.

After collecting additional data, the SOCCRATES platform performs a threat analysis.

For discovering new vulnerabilities, configuration changes and new systems (use cases 3, 4 and 5) we rely on existing vulnerability scanning, network scanning and asset discovering tools. These scanning tools can also be used to automatically 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 an up to date understanding of the environment they defend. The models can also be used for innovative analysis tools such as automated threat modeling and attack simulation.

Analysis phase

After collecting additional data, the SOCCRATES platform performs a threat analysis. For the threat analysis we use an Attack Defence Graph (ADG) based analysis to predict how attacks propagate over a model of the ICT infrastructure (provided by the IMC). This can for instance 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 be useful during an ongoing attack to determine if and how other systems can be compromised, 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. APT group) may compromise the infrastructure. The ADG is based on research from SOCCRATES partner KTH (Swedish university) (4) (5), that has been transformed in a commercial product securiCAD by the spin-off company foreseeti.

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.

Mitigation & response planning phase

For use case 1, the main focus of mitigation & response planning is on containing the attack. These attack response actions must be directly enforceable and typically only active during incident response. In a PhD-thesis (6) a term Tactical Response was introduced for the most efficient countermeasure to halt the ongoing attack. Strategic Response aims not only to end the ongoing attack, but also to prevent the occurrence of this attack in the future. Containment CoAs (CCoAs) are typically Tactical Responses. Next to these CCoAs, SOCCRATES platform also can generate attack responses 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). The latter two may be strategic responses.

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 deploying software patches. Since deploying such changes takes more time, we refer to them as planned responses. A combination of directly enforceable and planned response is also possible. A software patch is typically deployed after testing and during planned

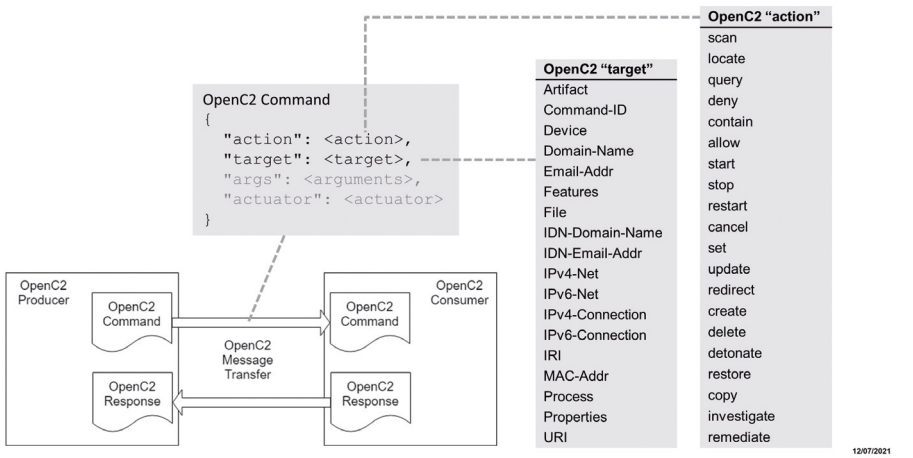

Figure 3 - OpenC2 command structure.

system downtime. An organisation can choose to first block certain traffic to the vulnerable system until the 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. The first, 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 improvement. An algorithm is developed to automatically figure out which defences can best be turned on within a given total cost factor (each defence can be assigned a financial cost and/or deployment time). The second component that produce CoAs is the Response Planner. This component focusses on identification of directly enforceable response actions for e.g. containment of 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.

Mitigation & response execution phase

After the analyst has selected 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 potential scary concept. An attacker may misuse such mechanisms to perform for instance a denial of service attack. 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 IT support tickets or email with the recommended CoAs. This enables the integration of a human in the loop for authorisation of the CoA execution, and to include manual reconfiguration. To further automate the execution of the CoAs, SOCCRATES has adopted two machine readable languages that are being specified by OASIS Open:

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

OpenC2 is used to formulate response actions, such as filter

The SOCCRATES platform has been designed as an open extendable framework.

traffic or contain hosts, in a machine-readable language. CACAO is used to combine multiple response actions (defined with OpenC2) into a playbook and add meta data. An OpenC2 command must contain the 'action' and 'target', and optionally contains the 'actuator' and 'arguments', see figure 3. The actuator executes the command specified with the action and target. Since not many security systems support OpenC2, it is necessary to develop OpenC2 proxies that translate the OpenC2 commands to the proprietary commands of a security systems.

Example OpenC2 command to contain host:

```
{
 "action": "contain",
 "target": {
  "device": {
   "name": "hostname"
   "IPv4-Addr": "1.2.3.4"
  }
 }
}
```

During the SOCCRATES pilots (at MSSP mnemonic and the SOC of Vattenfall), automated execution of CoAs will not or only under specific conditions be allowed. The SOCCRATES platform will have the capability to initiate automatic reconfiguration, but in most cases this will be limited to sending IT support tickets.

Discussion & challenges

The SOCCRATES platform has been designed as an open extendable framework, enabling different security tools to be integrated in an automated platform. In particularly, we expect that in the future more security analysis and reasoning tools will emerge that can provide additional security information for faster and better decision making by the SOC / CSIRT. During the project we identified that some tasks are difficult to fully automate. A typical example of this is assessing the full extent of an incident. This is usually done by a SOC / CSIRT analyst by iteratively searching for evidence in multiple data sources to identify all compromised hosts in an ongoing attack. If security tools do not provide standardised and/or easy to integrate open APIs, further automation of security operations will be difficult. This is why we believe that security automation will not entirely replace human analysts, but automation will support the analysts in making their task more effective and efficient. We do believe that the task of the analyst will change; instead of analysing the details of each individual incident him/herself, the automation platform will take over a lot of the standard analysis steps. The analyst will be provided with option awareness and select CoA's presented by the automated security platforms; the analyst therefore will act on a higher abstraction level and this will require education and training.

Furthermore, the adoption of fully automated reconfiguration or execution of CoAs will take time. Within some domains, however, such as cloud environments, we anticipate that the concept of security automation will be adopted very fast.

This is part two. Part one SOCCRATES – Security automation in SOC & CSIRT environments was published in iB-Magazine 4.

References

(1) Paul Cichonski. Tom Millar, TimGrance, and Karen Scarfone, 'Computer Security Incident Handling Guide', NIST Special Publication 800-61 Revision 2, August 2012.

(2) ISO/IEC 27035-1:2016, Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management.

(3) An architectural blueprint for autonomic computing, IBM whitepaper, June 2005 http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf

(4) Pontus Johnson, Robert Lagerström, Mathias Ekstedt, 'A Meta Language for Threat Modeling and Attack Simulations', ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security, August 2018 Article No.: 38, Pages 1–8 https://dl.acm.org/doi/abs/10.1145/3230833.3232799

(5) Sotirios Katsikeas, Simon Hacks, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Joar Jacobsson, Max Wällstedt, Per Eliasson, 'An Attack Simulation Language for the IT domain', International Workshop on Graphical Models for Security, GraMSec 2020: Graphical Models for Security pp 67-86, https://link.springer.com/chapter/10.1007/978-3-030-62230-5_4

(6) Wael Kanoun, 'Intelligent Risk-Aware System for Activating and Deactivating Policy-Based Response', PhD thesis, 2011

(7) https://www.oasis-open.org/committees/openc2

(8) https://www.oasis-open.org/committees/cacao