SOCCRATES

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

D2.1

Use cases definition & pilot sites requirements

Deliverable type:	Report
Contributing work packages:	WP2 SOCCRATES platform design
Due date of deliverable:	01/12/2019
Submission date:	02/12/2019
Dissemination level:	PU

Responsible organisation:	mnemonic
Editors:	Martin Eian
Revision:	1.0

Abstract	This deliverable describes the five use cases that represent different security operations that the SOCCRATES platform should support, as well as the pilot site requirements for the Vattenfall, mnemonic and Shadowserver pilots.
Keywords:	Security Automation, use case, pilot,

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 main objective of SOCCRATES is to develop and implement a security automation and decision support platform for SOCs and CSIRTs that will significantly improve an organisation's capability to quickly and effectively detect and respond to new cyber threats and ongoing attacks. In order to validate the platform's capabilities, five different use cases will be evaluated across three different pilot sites. This document describes the use cases in detail, as well as the pilot site requirements with KPIs.

The five use cases to be evaluated are:

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

The SOCCRATES platform will be deployed and validated at two pilot sites: Vattenfall and mnemonic. The Vattenfall Security Operation Center (SOC), located in Poland, is the central security monitoring and response facility for Vattenfall business units and IT. mnemonic provides SOC and CSIRT services to a wide range of different customers, covering all major verticals and both the public and private sectors. A third pilot site, Shadowserver, will be used for testing and validating the SOCCRATES threat prediction technology. Shadowserver collects a large amount of threat data by monitoring malicious infrastructures.

Contributor(s)	Martin Eian (mnemonic), Sebastiaan Tesink, Frank Fransen (TNO), Maciej Kosz, Rafał Kondracki, Pawel Babski (Vattenfall) Piotr Kijewski (Shadowserver)

Reviewer(s)	Per Eliason (Foreseeti) Christophe Kiennert (IMT)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	02/12/2019
Remarks	none

TABLE OF CONTENTS

TABLE OF CONTENTS 4
1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 5
1.1 The SOCCRATES project 5
1.2 This deliverable 6
1.3 Structure of this deliverable 7
2 SOCCRATES PLATFORM OVERVIEW 8
2.1 Introduction 8
2.2 SOCCRATES component architecture 8
3 USE CASE ANALYSIS 11
3.1 Introduction 11
3.2 Use Case 1: Response on Detected Ongoing Attack 14
3.3 Use Case 2: Response on Newly Received Cyber Threat Intelligence 24
3.4 Use Case 3: Response on Newly Discovered Vulnerable Assets 31
3.5 Use Case 4: Response on Discovered System Configuration Change 35
3.6 Use Case 5: Response on Deployment of New Systems in Infrastructure 39
4 SOCCRATES PILOT SITES 44
4.1 Pilot site #1: Deployment at the corporate SOC of VTF 44
4.2 Pilot site #2: Deployment at the MSSP SOC of mnemonic 46
4.3 Pilot site #3: Deployment of Threat Trend Prediction at Shadowserver 49
4.4 Collective requirements for pilot sites 50
5 REFERENCES 52
6 ABBREVIATIONS 53
ANNEX A – SWIMLANE DIAGRAMS UC1 55
ANNEX B – SWIMLANE DIAGRAM UC2 61
ANNEX C – SWIMLANE DIAGRAM UC3 63
ANNEX D – SWIMLANE DIAGRAM UC4 65
ANNEX E – SWIMLANE DIAGRAM UC5 67

1 Introduction – Rationale of this document

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.

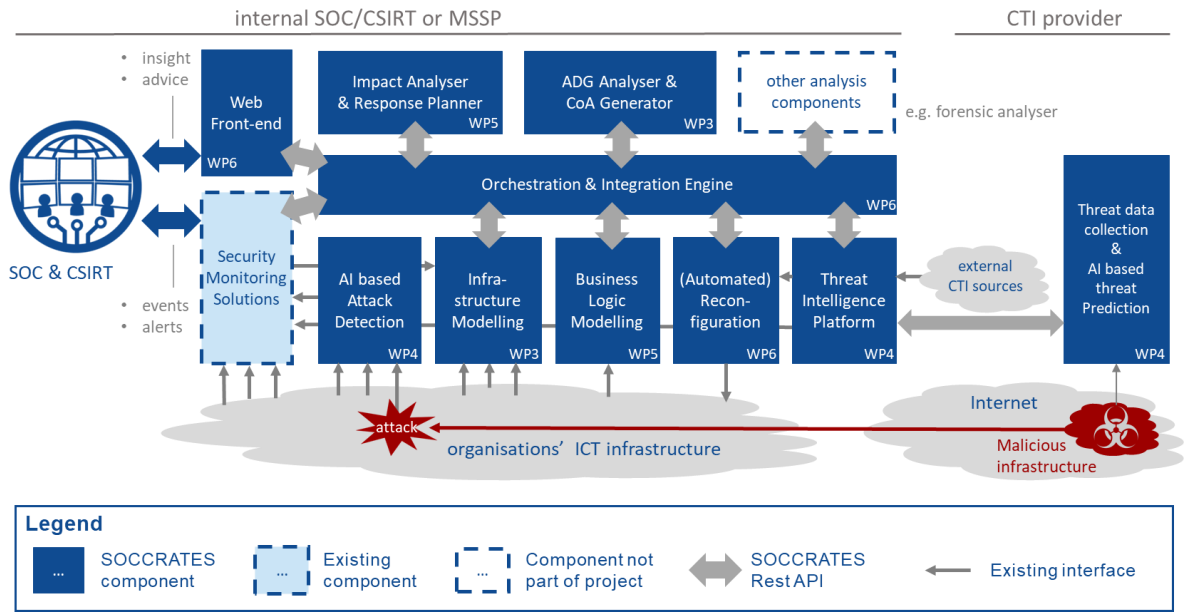


Figure 1.1 – The SOCCRATES platform

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

This deliverable describes the five use cases that represent different security operations that the SOCCRATES platform should support. These five use cases are:

- 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 New Vulnerable Assets
- Use Case 4: Response on Discovered System Configuration Change
- Use Case 5: Response on Deployment of New Systems in Infrastructure

By analysing the use cases the interactions between the different SOCCRATES platform components are identified, and the data elements is identified that is exchanged during these interactions. In addition, the analysis also identifies requirements for the test environments and pilot sites in order to test and validate the SOCCRATES platform.

The SOCCRATES platform will be implemented and tested in two pilot sites that represent different application scenarios: an organisation internal SOC with a large complicated on-prem infrastructure (i.e. at Vattenfall; pilot site #1), and a Managed Security Service Provider (MSSP) that provides operational security services to several customers (i.e. at mnemonic; pilot site #2).
In the pilots, specific focus will be put on the advantages of automation in SOC/CSIRT operations. The project will validate that the automation with the SOCCRATES platform will reduce the time that SOC/CSIRT staff spends on average on security events so that qualified staff can dedicate more time to complex tasks such as threat hunting. The pilots will also validate that the SOCCRATES platform contributes to more efficient/appropriate courses of actions when responding to security incidents. To this end, these pilots will be setup such that the Mean Time To Detection (MTTD) and the effectiveness of courses of action in SOC and CSIRT operations can be measured.

In addition, SOCCRATES will develop tools to support the analysis of large amount of malicious infrastructure and malware forensic data. The goal of the analysis is to identify malicious activity trends, and to utilize this novel type of cyber threat intelligence within the SOCCRATES platform. At a third pilot site the analysis of a large amount of malicious infrastructure and malware forensic data will be tested and evaluated (i.e. at Shadowserver; pilot site #3).

In this deliverable the pilot sites as well as the requirements for the deployment of the SOCCRATES platform at these pilot sites are described.

1.3 Structure of this deliverable

Section 0 presents the capabilities and the architecture of the SOCCRATES platform. Section 3 presents the five use cases that represent different security operations that the SOCCRATES platform should support. Section 4 presents the pilot site requirements for the pilots at Vattenfall, mnemonic and Shadowserver. Section 5 contains the references, and Section 6 contains abbreviations. Annex A-E present the swimlane diagrams for each of the five use cases presented in Section 3.

2 SOCCRATES platform overview

2.1 Introduction

The SOCCRATES platform will have the following capabilities:

1. automated asset discovery & modelling of the ICT infrastructure providing an accurate and correct machine-readable description of an ICT infrastructure;
2. cyber-attack detection on large amount of network and log data using advanced data analytics techniques (incl. AI and deep learning), capable of detecting advanced attacks, even in the case of encrypted network traffic;
3. analyse emerging threats and ongoing attacks by means of Attack Defence Graph (ADG) based analysis, and determining the best response to these threats and attacks;
4. quantify the (potential) business impact of emerging threats and ongoing attacks, by means of business impact modelling, and determine business trade-offs of possible response actions;
5. Cyber Threat Intelligence (CTI) utilization in incident detection, analysis and response, including adversary attribution and threat actor profiling;
6. automated analysis on large amount of malicious infrastructure and malware data to identify and predict new trends.

To achieve these capabilities, the SOCCRATES partners have carefully selected a set of components and tools. All the components are based on existing developments at one or more of the partners. During the project, these will be enhanced and integrated into one orchestrated platform such that they will seamlessly work together.

2.2 SOCCRATES component architecture

Figure 1.1 depicts the SOCCRATES platform component architecture. The central component is the *Orchestration and Integration Engine* that facilitates communication and exchange of information between components, and orchestrates the activities taken by the SOCCRATES platform when it is triggered.

In the same figure, underneath the Orchestration and Integration Engine all components are depicted that directly interact with the ICT infrastructure or the components that collect (threat) intelligence from external sources (a.o. the Infrastructure Modelling Component and Threat Intelligence Platform). Above the Orchestration and Integration Engine the analysis components are depicted (i.e. Impact Analyser & Response Planner, ADG Analyser & CoA Generator, and other analysis components). To the left of the Orchestration and Integration Engine, the existing SOC and CSIRT are depicted as well as the Security Monitoring Solutions implemented by the organisation. Although the Security Monitoring Solution is not part of the SOCCRATES platform, it is able to trigger it, and interact with it, as will be specified in the use cases.

The *Threat Data Collection & Threat Prediction* component depicted on the right belongs to an organisation that collects large amounts of threat data from malicious infrastructures. This component is thus outside the scope of the SOCCRATES platform that is located at the internal SOC or MSSP. It is integrated with the SOCCRATES platform via the Threat Intelligence Platform (TIP), one of the SOCCRATES platform components.

The SOCCRATES platform components are described below.

- *Infrastructure modelling* – this component provides a model of the current ICT infrastructure in a common reference description language. To build this model, the component collects data from a variety of available IT and security management tools, such as network scanners, asset discovery tools, vulnerability scanners, EDR solutions, and CMDBs. The ICT infrastructure model will include properties and facts that are relevant from a cyber security point of view. SOCCRATES will use this model to present the SOC analyst with insight into system structures and configurations, what systems are vulnerable, how detected attacks propagate through the infrastructure, and to provide other SOCCRATES components (such as Attack Defence Graph analyser & Course of Action Generator) with an accurate and up-to-date model of the ICT infrastructure for further analysis. Moreover, the component can trigger events to the Orchestration and Integration Engine based on particular changes over time (e.g. new assets discovered, particular changes in the configuration of an asset).
- *AI based Attack Detection* – this component provides advanced cyber-attack detection capability based on integrated anomaly detection on system log data, network traffic and flow data, using advanced techniques such as AI and machine learning. The component will report detected security events to existing Security Monitoring Solutions, such as Security Information and Event Management (SIEM).
- *Threat Intelligence Platform* – SOCCRATES platform will integrate a Threat Intelligence Platform (TIP) that collects and stores CTI from a diverse set of sources, that automatically fuses, enriches and correlates the collected CTI, and that provides interfaces for accessing the CTI. Next to the more operational CTI (e.g. Indicators of Compromise (IoC)), the TIP will in particularly be oriented towards the collection and analysis of the more strategic and tactical threat intelligence (e.g. threat actors, campaigns, Tactics, Techniques and Procedures (TTPs)). Among other things, SOCCRATES will use this component to trigger analysis of new threats on the organization's own ICT infrastructure, the adversary attribution of ongoing attacks, and to provide Adversary Emulation Plans (AEPs) as input to the ADG analyser to enable prediction of how a particular threat actor will be likely to attack the target infrastructure.
- *Attack Defence Graph analyser & Course of Action Generator* – Attack Defence Graph analyser can be used to predict how attacks propagate over a given ICT infrastructure. In SOCCRATES this is used to predict the potential effect of a new threat, a new vulnerability, a change in the system configuration, etc. In addition, when an attack is detected the ADG based analysis can be used to determine if and how the attacker may compromise other systems. SOCCRATES will use this to provide the SOC / CSIRT analyst with detailed insight into what systems can be compromised and how likely that is. The Course of Action Generator uses ADG and reinforcement learning to generate a possible set of relevant courses of actions and to rank them according to the attack limiting effects. The output of the ADG and CoA generator will be used as input for the Response Planner to prioritize the Courses of Action.
- *Business Logic Modelling* – this component provides a model of the business layer running on top of the ICT infrastructure. To build this model, the component builds onto the infrastructure modelling component to extend it in order to model the relationship between ICT assets and the business missions of the organization. The business logic is captured through several means, such as the modelling of business processes (e.g. BPMN), organization structure captured in directories (e.g. LDAP, Microsoft Active Directory), or network management analysis (naming schemes, network partitioning, network dependencies). The component thus generates a model of the business logic of the ICT infrastructure. SOCCRATES will use this component to provide business logic model data as input to the Impact Analyser & Response Planner.
- *Impact Analyser & Response Planner* – this component will quantify the impact of an attack or threat to the business, and quantify the impact of the different Courses of Action proposed by

the CoA generator for a specific attack. In addition, the component will support the identification, selection and deployment planning of selected CoAs. SOCCRATES will use this component to provide the SOC / CSIRT analysts with detailed insight into the (potential) impact of a new threat or ongoing attack, and to provide insight into the trade-offs of the generated course of actions, such that the SOC / CSIRT analyst can make informed decisions and deploy the selected courses of action.

- *Orchestration & Integration Engine* – this component integrates, manages and orchestrates the different components of the platform. It serves as the central element for the communication and exchange of information between components. It enables (semi-)automated orchestration of the activities to analyse security events (see SOCCRATES Use Cases), generate and assess the possible response actions to this security event, and plan and trigger the execution of the best response action. An orchestration process will be based on predefined playbooks that can be initiated by the SOC analyst, or automatically by existing security monitoring solutions (e.g. detected attack or discovered vulnerable asset), the threat intelligence platform (i.e. new threat intelligence) and the Infrastructure Modelling component (e.g. new assets discovered). The orchestration component will provide an interface to define playbooks.
- *(Automated) Reconfiguration* – the component provides the capability to interface with the security controls and other functions in the infrastructure to execute selected response actions to react to an emerging threat or detected attack. The component will provide a generic and extendible framework to interface with multiple types of system, such as network reconfiguration using SDN, and reconfiguration using OASIS OpenC2 based interface.
- *Web Front-End* – this component is the front-end used for accessing all functionalities and cybersecurity information provided by the SOCCRATES platform. The front-end will provide cybersecurity information to support the SOC and CSIRT operations in a user-friendly manner, but also enable configuration and management of the SOCCRATES platform components.
- *Threat Data Collection & Threat Prediction* – This component is focused on the identification of malicious activity trends based on large amounts of malicious infrastructure and malware forensic data using advanced data analytical techniques, including AI and deep learning. The type of predictions strongly depends on the available data. The goal of the component is to identify malicious activity trends to enable organisations to anticipate and take precautions for upcoming attacks that use the predicted techniques. This component is intended to be deployed in organisations that collect large amounts of adversarial behaviour data and malicious infrastructure data. The component will have an interface to allow the Threat Intelligence Platform of SOCCRATES platform to collect this advanced cyber threat intelligence.

3 Use Case analysis

3.1 Introduction

To guide the development of the SOCCRATES platform, the project will rely on five use cases. These use cases have been selected to represent the most relevant situations in which an organisation needs to reassess the security state, and determine if and how to react 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. The use cases are graphically depicted in Figure 3.1.

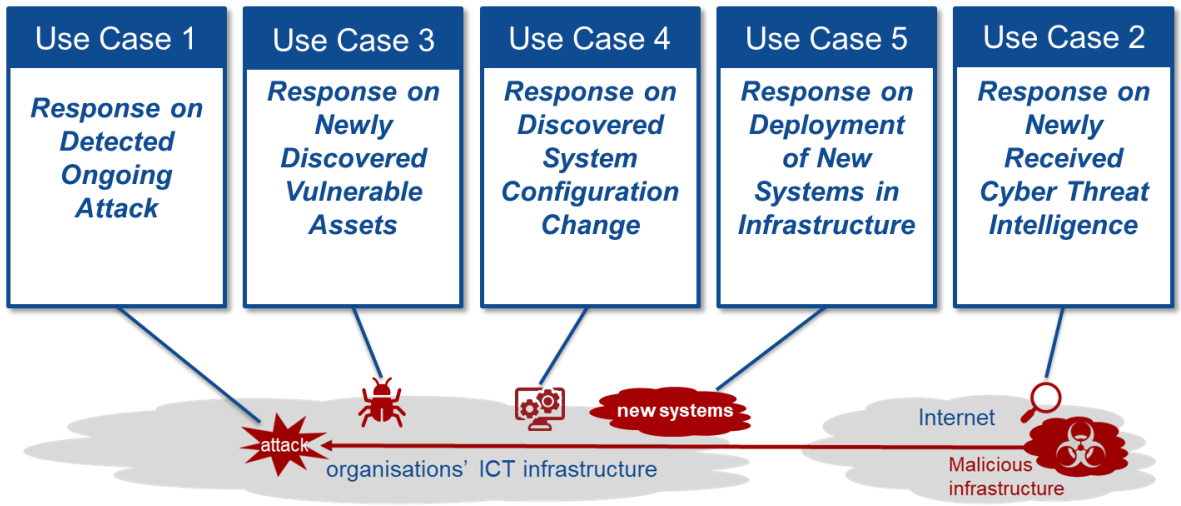


Figure 3.1 – The SOCCRATES Use Cases

- ***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 security measures are needed.

3.1.1 Approach of the analysis

The goal of the use case analysis is to identify which of the SOCCRATES platform components will interact, when and for what purpose. This will guide the specification and developments of the interfaces and of the Orchestration and Integration Engine. Furthermore, this will also guide the development of the test environment and setup of the pilot sites.

For each of the use cases the workflow of the interactions between the SOCCRATES platform components has been identified and described. In addition, the workflow has been depicted in a swimlane diagram. Furthermore, the involved components, the identified interfaces and data models have been listed. For each use case, the requirements for the testing environment and the pilot sites have also been identified. For those use cases with separate scenarios, the specifics for each scenario have been analysed and described.

We identified that the workflow for each of the use cases can be divided into four phases as depicted in Figure 3.2:

1. *Monitoring phase* – in this phase the system monitors security events specific to the use case, which triggers the SOCCRATES platform;
2. *Analysis phase* – in this phase the SOCCRATES platform will automatically analyse the security event to create situational awareness for the SOC analyst;
3. *Mitigation & response planning phase* – in this phase the SOCCRATES platform will automatically generate courses of action (CoAs) and assess these based on an effectiveness and business trade-off. This provides option awareness for the SOC analyst / CSIRT member.
4. *Mitigation & response execution phase* – 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.

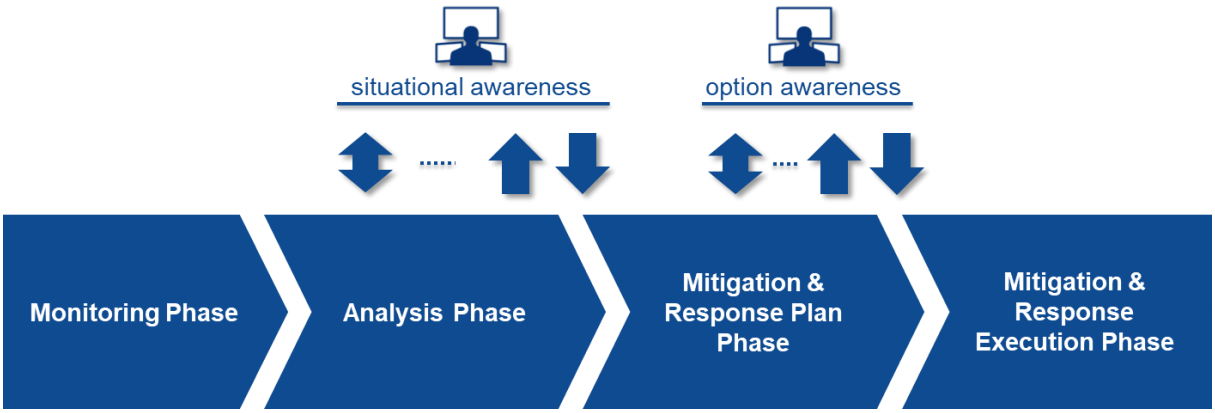


Figure 3.2 – Four phases of the SOCCRATES use cases

Although these four phases are applicable for all the SOCCRATES use cases, it is less straightforward for use case 1. This is due to the fact that use case 1 is about an ongoing attack which typically will initiate an incident response with an active threat actor. Information Security Incident management, as for instance described in NIST SP800 61 [SP800-61] and the ISO/IEC 27035 series [ISO27035], consists of several phases or stages: preparation, detection, analysis, containment, eradication, recovery and post-incident activities. In the Table 3-1 these stages are described. Detection and analysis are *Incident Detection Operations*. Containment, eradication and recovery are *Incident Response Operations*.

Note that the transition from one incident response stage to another is done after a certain condition is met. For example, the transition from analysis to containment is done after the detected security event is classified as a security incident. The transition from containment to eradication is done after the incident is fully contained. If during eradication or recovery stage it is detected that the inci-

dent is not yet fully contained, the incident response process goes back to containment stage. Furthermore, in the containment stage the incident response team may activate additional monitoring to identify the full extent of the incident. This does not mean that the incident response process moves back to detection stage.

The four phases of the SOCCRATES use cases can, however, be seen as a control loop. Meaning that for use case 1, the monitoring, analysis, plan, execution phases could be passed several times within a particular incident response stage. In use case 1, these four phases of the SOCCRATES use case share knowledge of the particular incident response stage it is in, through the Orchestration and Integration Engine.

Table 3-1 Information security incident response stages

Preparation	As the name implies, in this phase all activities are under taken for establishing an effective incident response management capability.
Incident detection operations	
Detection	The detection phase of incident response management involves the detection of security events (by both manual and automatic means).
Analysis	During the analysis phase the detected security events are assessed to determine whether to classify events as information security incidents. The initial analysis should provide enough information to prioritize subsequent activities, such as containment of the incident.
Incident response operations	
Containment	The containment phase aims to prevent the threat actor from accessing, exfiltrating, tampering or destroying data or other information, destroying valuable evidence and tampering with systems, and using systems to attack other systems. Only after a successful containment of the attack, the incident response process will continue with the eradication phase.
Eradication	After an incident has been contained, eradication is typically necessary to eliminate any vulnerability or backdoor that would allow the threat actor to regain access. If during this phase there are signs that containment was unsuccessful, the incident response operation moves back to containment phase.
Recovery	In the recovery phase the service, data or system is restored to its normal operational state. If during this phase there are signs that containment (or eradication) was unsuccessful, the incident response operation moves back to the containment phase.
Post-incident activities	And finally, a very important phase, but often omitted, the post-incident activities which has the objective to learn and improve in order to prevent similar incidents in the future. This may also include sharing information with others.

Although the SOCCRATES platform is intended to automate tasks in incident detection operation and incident response operations, it was decided to limit the scope of the SOCCRATES project to the containment stage of the incident response operations. The reasons for this are the following:

1. Incident response operation stages “eradication” and “recovery” are typically performed by IT systems and network administrators. MSSPs and large internal SOCs are typically not in the

lead in these incident response stages. The main focus of the SOCCRATES platform is to support the MSSP and internal SOC, and as such the SOCCRATES platform should focus on supporting the main tasks of SOCs and CSIRTs.

2. Eradication and recovery operations will more likely be automated using general IT management systems. It is therefore more likely that the SOCCRATES platform will handover eradication and recovery tasks to an IT management system. Indeed, the SOCCRATES platform needs to support these activities by identifying what needs to be done and handing this over.
3. Eradication and recovery are very specific to the particular systems within an ICT environment and to the existing IT operations. Main challenges for automation of tasks in the eradication and recovery stages are on the integration with IT system and IT operations, which is not the primary focus of the SOCCRATES project. As the resources of the SOCCRATES project are limited, it is necessary for the project to focus on the most important functions and (promised) innovations. With this in mind, SOCCRATES has set priority to reduce the Mean Time To Detection (MTTD) and to increase the speed and effectiveness of incident containment.

In the Figure 3.3 the incident management stages are depicted with the scope of SOCCRATES use case 1.

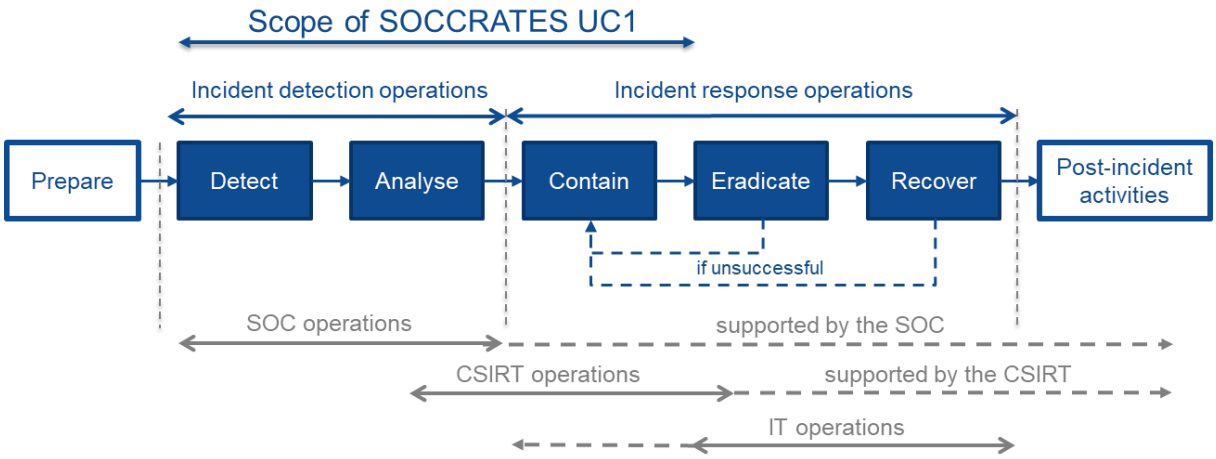


Figure 3.3 – Incident management stages with the scope of SOCCRATES use case 1

3.2 Use Case 1: Response on Detected Ongoing Attack

3.2.1 Introduction

This use case is oriented towards automatically analysing and determining the response to a detected ongoing attack. The use case and envisioned improvement can be explained by first describing the current situation and next the improved situation with the SOCCRATES platform.

Current situation

Organisations typically have automated attack detection and correlation tools (e.g. SIEM) that provide alerts of potential security incidents and present them to a human analyst for analysis and verification. Nowadays it is also common to collect Indicators of Compromise (IoCs) and use them for monitoring. The analysis and response are typically undertaken by human analysts. This may include

determining the scope of the compromise, the (potential) impact and possible responses. Most organizations lack the data and systems to accurately determine the full extent of their infrastructure, which makes it difficult and time consuming to assess the attack and determine the response.

SOCCRATES platform improvement
The SOCCRATES platform automatically collects data on affected assets, collects the current infrastructure model and plots the attack, collects related CTI and performs adversary attribution, determines business impact so far, and recommends immediate actions. The SOCCRATES platform predicts possible next steps of attack, determines the impact of those future steps, determines possible response to mitigate the attack and/or next steps, determines trade-offs for those responses. All the results will be presented to the SOC analyst as actionable insight and advice. When the SOC analysts selects the desired action, the SOCCRATES platform automatically prepares the related playbook.

The detection, analysis and response can differ according to the type of attack, at which stage of the cyber-attack kill chain the detection takes place, or to the type of targeted system(s). To ensure that the SOCCRATES platform is agnostic on these differences, a comprehensive set of scenarios have been defined. The different attack types that were initially distinguished are: a) ransomware attack on a single system, b) targeted ransomware on many systems, c) APT style espionage attack and d) web application attack with focus on personal data theft. As there is overlap between the attack techniques in the first three proposed attack scenarios, it was decided to distinguish these scenarios per attack detection stage. Attack stages have typically been expressed by means of the cyber kill chain, as introduced in 2011 by the Lockheed-Martin corporation [Hut05]. The cyber kill chain distinguishes the following phases: 1) reconnaissance, 2) weaponization, 3) delivery, 4) exploitation, 5) installation, 6) Command and Control (CC), and 7) Actions on Objective (e.g. data exfiltration, data destruction, or encryption for ransom). As not all attacks follow these specific stages, it is nowadays more common to refer to tactics and techniques outlined in the MITRE ATT&CK framework[1]. The scenarios have thus been segmented according to the type of attacks and the detected ATT&CK tactic. These scenarios are:

- Scenario 1.1: Detection of Initial Access / Execution / Command & Control
- Scenario 1.2: Detection of (internal) Discovery / Lateral Movement
- Scenario 1.3: Detection of Exfiltration (of confidential data and/or personal data)
- Scenario 1.4: Detection of web application attack (with personal data theft)

Combined with the incident management stages, as described in section 3.1.1, the workflow of the use case 1 has been divided into five stages as depicted in Figure 3.4.

[1] https://attack.mitre.org/

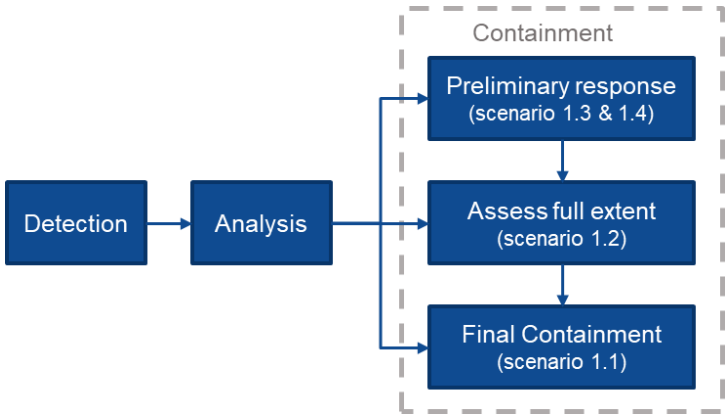


Figure 3.4 Workflow stages of use case 1

3.2.2 Detection stage

3.2.2.1 Workflow in SOCCRATES platform

In the detection stage a security event is detected by a certain security monitoring solution. This can be the *AI based Attack Detection* that reports a security event to a SIEM. If the security event triggers an alert on the SIEM with a high/critical severity, the SIEM will trigger the *Orchestration & Integration Engine* to start an analysis of the security alert.

The swimlane diagram of this workflow is depicted in Annex A.

3.2.2.2 Analysis

Components

- AI based Attack Detection
- SIEM
- Orchestration & Integration Engine

Interfaces

All interfaces have a unique reference based on the provider, input and response it provides. Numbers are according to the following schema: INTF<prefix>.<sequence>.

Prefix	Component
1	Security Monitoring Solution
2	Orchestration & Integration Engine
3	Infrastructure Modelling Component
4	Threat Intelligence Platform
5	Business Impact analyser
6	Attack Defence Graph analyser
7	Web Front End
8	CoA Generator
9	Response Planner
10	Threat Data Collection & Threat Prediction

For the detection phase of use case 1, the following interfaces were defined:

Interface Reference	INTF1.01
Provider	Security Monitoring Solution
Input	Security event from the AI based Attack Detection
Response	-

Interface Reference	INTF2.01
Provider	Orchestration & Integration Engine
Input	Security alert – trigger analysis
Response	-

Data models

- Security Event Data

Requirements for test & pilot environments

- The test environments & pilot sites must support AI based Attack Detection.
- The test environments & pilot sites must support a SIEM that can trigger the Orchestration & Integration Engine.

3.2.3 Analysis stage

The goal of the analysis stage is to determine if the detected security event can be classified as a security incident.

3.2.3.1 Workflow in SOCCRATES platform

1) The *Orchestration & Integration Engine* requests the current infrastructure model (M_n) from the *Infrastructure Modelling Component* (IMC).
2) The *Infrastructure Modelling Component* produces the new current model M_n, stores the new infrastructure model and informs the Orchestration & Integration Engine with pointer to location in the store of M_n.

The *Orchestration & Integration Engine* will now go into a triage stage in which it will enrich the security event data in order to determine if this must be classified as a security incident. This will typically include the following steps:

3) The Orchestration & Integration Engine requests the Threat Intelligence Platform (TIP) for CTI related to the security event data.
4) The *TIP* provides CTI related to the security event data. This may include IoCs for additional monitoring.
5) The *Orchestration & Integration Engine* queries the *Security Monitoring Solution* for historical events related to the IoCs and/or requests the *Security Monitoring Solution* to start monitoring for the IoCs.
6) The *Security Monitoring Solution* provides the results of the request.

7) The *Orchestration & Integration Engine* requests the business impact from the *Impact Analyser* for each of the (critical) systems that are potentially affected.
8) The *Impact analyser* performs a business impact analysis on the asset(s) and type of compromise provided by the *Orchestration & Integration Engine*, and returns the business impact per asset.
9) The *Orchestration & Integration Engine* forwards the enriched security event information to the *Web Front-End* for presentation to the SOC analyst. The SOC analyst must determine if it is a security incident.

If yes, the *Orchestration & Integration Engine* is triggered to perform further analysis.

10) The *Orchestration & Integration Engine* requests the Security Monitoring Solution to start monitoring for IoCs related to the Incident.
11) The Security Monitoring Solution informs the Orchestration & Integration Engine of detected security events and stores the security events in a separate security incident data store.
12) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to assess the possible next attack steps. This may be specifically requested for a set of critical assets that are likely targets for the threat actor's campaign.
13) The *Attack Defence Graph analyser* returns the attack paths and list of assets for which the Time To Compromise (TTC) was significantly reduced due to the location of the threat actor (e.g. compromised host) within the Infrastructure Model.
14) The *Orchestration & Integration Engine* requests the Impact Analyser the determine the (potential) business impact for the (critical) assets for which the TTC was changed.
15) The *Impact Analyser* performs a business impact analysis on the assets and type of compromise and returns the business impact for the requested assets.
16) The *Orchestration & Integration Engine* forwards the enriched security event information to the *Web Front-End* for presentation to the SOC analyst. The SOC analyst must determine if it is a security incident.

The *SOC analyst* decides based on the presented information whether to continue with:

a. Determine containment strategy and initiate execution (scenario 1.1).
b. Assess full extent of the incident (scenario 1.2).
c. Preliminary response to the incident to prevent further impact (scenario 1.3 & 1.4).

The swimlane diagram of this workflow is depicted in Annex A.

3.2.3.2 Analysis

Components

- Security Monitoring Solution (e.g. SIEM)
- Attack Defence Graph analyser
- Impact Analyser
- Infrastructure Modelling Component
- Orchestration & Integration Engine
- Threat Intelligence Platform (TIP)
- Web Front-End

Interfaces

Interface Reference	INTF3.01
Provider	Infrastructure Modelling Component
Input	Request new model

Response	Infrastructure model

Interface Reference	INTF4.01
Provider	Threat Intelligence Platform
Input	Observed security event data
Response	Threat intelligence, including relevant IoCs

Interface Reference	INTF1.02
Provider	Security Monitoring Solution
Input	Collect historical event related to IoCs, time period
Response	Security events

Interface Reference	INTF1.03
Provider	Security Monitoring Solution
Input	Start real time monitoring on IoCs
Response	Security events

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	(List of) Asset ID, type of compromise
Response	Business Impact per requested asset

Interface Reference	INTF6.01
Provider	Attack Defence Graph analyser
Input	Infrastructure model (incl. attacker location and critical assets)
Response	Results of ADG analysis • Attack paths • ΔTTC for (critical) assets

Interface Reference	INTF7.01
Provider	Web Front End
Input	Security Event Information
Response	-

Data models

- Security Event Information
- Infrastructure model
- Threat intelligence, including relevant IoCs
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)
- Asset ID, type of compromise
- Business Impact

Requirements for test & pilot environments

- A *Security Monitoring Solution* must be present that is able to store and analyse historical incident information based on presented IoCs.
- A *Security Monitoring Solution* must be present that can be triggered to initiate monitoring on IoCs.
- The test environments & pilot sites must be able to support infrastructure modelling.
- The test environments & pilot sites must be able to assess business impact based on impacted assets.
- The test environments & pilot sites must provide a Threat Intelligence Platform that can provide CTI information based on security event data of observations.
- The test environments & pilot sites must run the SOCCRATES platform components listed above.

3.2.4 Containment stage – Preliminary response

In scenario 1.3 the detection takes place at the exfiltration stage of the attack. This directly impacts the organisation, and it is thus important to quickly stop the exfiltration. Furthermore, when detecting a web application attack, as is assumed in scenario 1.4, it may be important to immediately respond to stop potential direct impact. The workflows of these two scenarios will therefore continue with containment stage – Preliminary response. The objective of this stage is to immediately prevent further impact by determining and executing a preliminary response.

3.2.4.1 Workflow in SOCCRATES platform

The workflow mainly consists of determining the preliminary response (e.g. blocking exfiltration traffic) and preparing the playbook for preliminary response. As this type of response is typically straightforward, it is expected that the preliminary response strategy can typically be looked up in a set of preliminary response strategies. After initiating this first intervention, the flow will continue with a thorough analysis on how the attacker got at this stage of the attack, by performing a lateral movement analysis.

The Swimlane diagram of this workflow is depicted in Annex A.

3.2.4.2 Analysis

Components

- Orchestration & Integration Engine

Interfaces

-

Data models

-

Requirements for test & pilot environments

- The test environments & pilot sites must support some form of (automated) reconfiguration component that is able to interact with the Orchestration & Integration Engine in order to execute a preliminary response.

3.2.5 Containment stage – Determine full extent of the incident

In scenario 1.2, the detection takes place at (internal) Discovery / Lateral Movement stage of the attack. At the detection stage, it may not immediately be clear what the full extent of the security incident is. The goal of this part of the incident response stage is to analyse how the attacker was able to get to this attack stage and identify what is compromised. The workflow for this scenario will therefore continue after the analysis stage with the containment stage – Determine full extent of the incident.

A reverse (or initial) path analysis is performed by the ADG Analyser, providing the most likely path(s) the attacker took to get at this position. Based on this information, more data are collected from the Threat Intel Platform and the SIEM.

3.2.5.1 Workflow in SOCCRATES platform

1) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to produce attack paths that could have led to the detected security event. This can for instance be produced by generating the attack paths to the compromised hosts with the attacker placed outside the organisation's ICT infrastructure.
2) The *Attack Defence Graph analyser* returns the attack paths to the compromised host.
3) The *Orchestration & Integration Engine* may request the *TIP* for current IoCs for the attack steps in the identified attack paths.
4) The *TIP* provides IoCs related to the attack steps.
5) The *Orchestration & Integration Engine* queries the *Security Monitoring Solution* for historical events related to the IoCs and/or requests the Security Monitoring Solution to start monitoring for the IoCs.
6) The *Security Monitoring Solution* provides the results of the request.
7) The Orchestration & Integration Engine triggers the workflow for the containment stage - Determine the containment strategy, with an overview of all affected assets and accounts.

The swimlane diagram of this workflow is depicted in Annex A.

3.2.5.2 Analysis

Components

- Security Monitoring Solution (e.g. SIEM)
- Attack Defence Graph analyser
- Orchestration & Integration Engine
- Threat Intelligence Platform (TIP)

Interfaces

Interface Reference	INTF6.01
Provider	Attack Defence Graph analyser
Input	Infrastructure model (incl. attacker location, critical asset=compromised asset)

Response	Results of ADG analysis • Attack paths • ΔTTC for (critical) assets

Interface Reference	INTF4.02
Provider	Threat Intelligence Platform
Input	Attack step (from ADG analyser)
Response	IoCs

Interface Reference	INTF1.02
Provider	Security Monitoring Solution
Input	Collect historical event related to IoCs, time period
Response	Security events

Data models

- Security Event Information
- Infrastructure model
- IoCs
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)

Requirements for test & pilot environments

- A *Security Monitoring Solution* must be present that is able to store and request historical incident information based on presented IoCs.
- The test environments & pilot sites must provide a Threat Intelligence Platform that can provide CTI information based on initial attack path attributes.

3.2.6 Containment stage – Determine containment strategy & initiate execution

The goal of the containment stage is to fully contain the compromise. All scenarios of use case 4 will end the containment stage with this workflow. In scenario 1.1 the detection takes place at the initial access, execution or Command & Control stage of the attack. When detection takes place in these stages, the security incident may still only have affected a single system. During the analysis this must be assured, and the SOC analysist would select to go immediately to Containment stage – Determine containment strategy & initiate execution. This selection may also be automated.

3.2.6.1 Workflow in SOCCRATES platform

1) If a single system has been affected, the *Orchestration & Integration Engine* will directly determine the containment strategy for this single system (typically quarantine and forensic analysis), and prepare the playbook for this containment strategy. Next the workflow is triggered for execution of the playbook by the *(Automated) Reconfiguration component*.
2) If multiple systems and accounts have been compromised the *Orchestration & Integration Engine* continues and tries to determine the best containment strategy.
3) The *Orchestration & Integration Engine* requests the business impact data from the *Impact Analyser* for each of the (critical) system that are compromised.

4) The *Impact analyser* performs a business impact analysis for each of the requested assets and type of compromise and returns the results.
5) The *Orchestration & Integration Engine* requests the *CoA Generator* to determine the best courses of action to contain the security incident. The *Orchestration & Integration Engine* provided a list of the compromised assets, accounts and all known attack paths.
6) The *CoA Generator* determines different containment strategies and provides metrics on the effectiveness of each of these CoAs.
7) The *Orchestration & Integration Engine* requests the *Impact Analyser & Response Planner* to determine the Return on Response Investment (RORI) for each of the Courses of Action.
8) The *Response Planner* produces a prioritized list of containment strategies with RORI.
9) The *Orchestration & Integration Engine* forwards the results of the containment strategies analysis to the *Web Front-End* for presentation to the SOC analyst.
10) The SOC analyst may select a preferred Course of Action. For the selected containment strategy, a playbook is generated. Next the workflow is triggered for execution of the playbook by the *(Automated) Reconfiguration component*.

The swimlane diagram of this workflow is depicted in Annex A.

3.2.6.2 Analysis

Components

- CoA Generator
- Impact Analyser & Response Planner
- Orchestration & Integration Engine
- Web Front-End

Interfaces

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	(List of) Asset ID, type of compromise
Response	Business Impact per requested asset

Interface Reference	INTF8.02
Provider	CoA generator
Input	Request containment strategies • Infrastructure model • Compromised asset(s) and accounts • Detected attack path
Response	• List of Coas for the identified containment strategies • Effectiveness metric of each of the CoAs

Interface Reference	INTF9.01
Provider	Response Planner
Input	List of CoAs (including measure of effectiveness)
Response	List of prioritized CoAs with per CoA: • RORI

Data models

- Infrastructure model
- Attack paths,
- AssetID (that have been compromised), type of compromise per asset
- Accounts (that have been compromised)
- Business Impact
- Courses of Action (CoA)
- Effectiveness of CoA
- Return Of Response Investment (RORI)
- Playbook to execute CoA

Requirements for test & pilot environments

- Impact analyser must be aware of the link between impacted systems and business processes.
- The proposed CoAs generated by the CoA generator must be applicable to the test & pilot environment.
- In order to calculate the RORI and time slots, possible countermeasures and their costs must be known for the test & pilot environment.
- An (Automated) Reconfiguration Component must be available that can deal with the countermeasures proposed in the generated playbook.

3.3 Use Case 2: Response on Newly Received Cyber Threat Intelligence

3.3.1 Introduction

This use case is oriented towards automatically analysing and determining the response to newly received Cyber Threat Intelligence (CTI), as well as the production of CTI at Shadowserver and the distribution of this CTI to SOCCRATES platform components. The use case is therefore spilt into two separate scenarios:

- Scenario 2.1: SOCCRATES platform receives new CTI
- Scenario 2.2: Delivery of CTI derived from a.o. malware forensic data

In the following sections these scenarios will be described and analysed separately. However, in many cases we envision scenario 2.2 to be effectively a sub-scenario of 2.1 in terms of influence on the SOCCRATES platform. In all these cases scenario 2.2 provides the low-level input needed to make higher level decisions by the SOCCRATES platform.

3.3.2 Scenario 2.1: SOCCRATES platform receives new CTI

The envisioned improvement can be explained by first describing the current situation and next the improved situation with the SOCCRATES platform.

Current situation

Automated exchange of cyber threat intelligence has just recently started. Organisation can now deploy Threat Intelligence Platforms that can automatically collect, enrich, correlate and share CTI. Some platforms have the capability to execute scripted actions, such as add IoC to the SIEM. A human analyst must manually assess most CTI events to determine the effect and potential impact on an organisation's infrastructure.

SOCCRATES platform improvement
The SOCCRATES platform analyses the effect of this new threat intelligence on the current infrastructure model using ADG based analysis. If the threat leads to new attack paths the SOCCRATES platform determines the potential business impact, determines possible CoAs to proactively mitigate the threat, and determines trade-offs to prioritize these CoAs. All the results will be presented to the SOC analyst as actionable insight and advice. When the SOC analyst selects the desired action, the SOCCRATES platform automatically initiates this action.

3.3.2.1 Workflow in SOCCRATES platform

1) A *Threat Intelligence Platform (TIP)* collects CTI from different CTI feeds and sources. The TIP typically automatically enriches and correlates the CTI with existing CTI and stores the result. If the threat information could result in new attack paths through the ICT infrastructure, then the TIP initiates analysis by the SOCCRATES platform by triggering the *Orchestration & Integration Engine*. This assessment may be both TIP user initiated or automatic.
2) The Orchestration & Integration Engine requests the current infrastructure model (M_n) from the *Infrastructure Modelling Component* (IMC).
3) The *Infrastructure Modelling Component* produces the new current model M_n, stores the new infrastructure model and informs the *Orchestration & Integration Engine* with (a pointer to) location in the store of M_n.
4) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to analyse the new infrastructure model M_n, with and without the new threat information.
5) The *Attack Defence Graph analyser* performs the analysis on the infrastructure model with and without the new threat information. For the new threat information, the ADG analyser has to update the parameters on (among others) the likelihood of certain attack techniques.
6) The *Attack Defence Graph analyser* returns the difference in Time To Compromise (TTC) for each business relevant system, due to the discovery of the vulnerable systems.
7) The *Orchestration & Integration Engine* requests the business impact data from the *Impact Analyser* for each of the (critical) system for which the TTC was changed (significantly) due to the ne threat information.
8) The *Impact analyser* performs a business impact analysis on the list of assets and type of compromise provided by the *Orchestration & Integration Engine*, and returns the business impact per asset.
9) The *Orchestration & Integration Engine* forwards the results (ΔTTC and BI per asset) to the *Web Front-End* for presentation to the SOC analyst.
10) The *SOC analyst* decides whether to start the generation of CoAs.
    a. If the SOC analyst decides that it is not necessary to generate a list of CoAs for the selected asset(s), the process stops.
    b. If the SOC analyst decides that, based on presented information, it is necessary to start looking for the best CoA, the orchestrator is triggered to start the *Course of Action Generator*.

11) The *Orchestration & Integration Engine* requests the *Course of Action Generator* to generate a list of possible CoAs to mitigate the risks due to the new threat information, based on infrastructure model M_n, and the (critical) systems that need to be protected.
12) The *CoA Generator* produces a list of Courses of Action, and may check the *Threat Intel Platform* (TIP) based on the CVE to get recommended CoAs for the new threat. For each CoA, a metric for the change in TTC is included (i.e. effectiveness of CoA).
13) The *Orchestration & Integration Engine* requests the *Impact Analyser & Response Planner* to determine the Return on Response Investment (RORI) for each of the Courses of Action.
14) The *Response Planner* produces a prioritized list of Courses of Action with RORI. Note that the CoAs may differ in time when deployed (e.g. patch during the weekend).
15) The *Orchestration & Integration Engine* forwards the results to the *Web Front-End* for presentation to the SOC analyst.
16) The SOC analyst may select a preferred Course of Action:
    a. Take no further action.
    b. Trigger the *Orchestration & Integration Engine* to generate the playbook for the selected Courses of Action. Next the workflow is triggered for execution of the playbook by the *(Automated) Reconfiguration component*.

It is relevant to note that we can distinguish many kinds of CTI that an organisation can nowadays collect, ranging from operational (e.g. Indicators of Compromise) to strategical (e.g. attacker campaigns). In the definition of the use case we identified that the type of CTI has not much influence on the whole workflow and interactions between the SOCCRATES platform components, but mainly has consequences on the parameters that are sent to the ADG analyser for the analysis. To illustrate this, we identified the following sub-scenarios:

1. New information on a threat, such as an increase in use of a particular attack technique;
2. New information on a vulnerability, such as exploit code available on public websites;
3. New information on the attack techniques used by a particular threat actor (i.e. update of the Adversary Emulation Plan of that threat actor).

In the case of new information on a particular attack technique (i.e. sub-scenario 1), the first issue is whether the attack technique is already present in the ADG Analyser. If not, then the attack technique must first be modelled. KTH developed Meta Attack Language (MAL) for this purpose. If the attack technique is already present in the ADG Analyser and the information is regarding the increased use of the attack technique, then it means that the parameter for the likelihood of this attack technique must be modified accordingly.
For the case of new information on a vulnerability (i.e. sub-scenario 2), then this will typically mean that the Common Vulnerability Scoring System (CVSS)[2] score has changed due to the change in the Temporal Score of the CVSS. The ADG Analyser only has to modify the CVSS score for the particular vulnerability in the configuration file.
The case for the new information on the attack techniques used by a particular threat actor (i.e. sub-scenario 3), is a bit more extensive. The attacker behaviour can for instance be described in a so-called Adversary Emulation Plan[3]. The ADG Analyser should be able to receive such an Adversary Emulation Plan and perform an ADG analysis according to the information entailed in the plan, i.e.

[2] https://www.first.org/cvss/
[3] https://attack.mitre.org/resources/adversary-emulation-plans/

set of attack techniques and the order in which the techniques (and possibly procedures, tools and malware) are deployed.

3.3.2.2 Analysis

Findings & issues

- There is a need for central storage.
- The TIP must be capable of reporting a new threat information in a structured way such that the ADG Analyser can update the parameters for the analysis.
- The infrastructure model must contain up-to-date information on the importance of assets and the impact on confidentiality, integrity and availability when compromised.
- The ADG analyser must provide some metric on the effectiveness of the CoAs for the analysis by Response Planner.
- There is a need for further analysis on how the Business Impact & Response Planner gets information on business processes. How the Business Logic Modelling component interacts with the Business Impact & Response Planner is for further study.

Components

- Attack Defence Graph analyser
- CoA Generator
- Impact Analyser & Response Planner
- Infrastructure Modelling Component
- Orchestration & Integration Engine
- Threat Intelligence Platform (TIP)
- Web Front-End

Interfaces

Interface Reference	INTF2.02
Provider	Orchestration & Integration Engine
Input	Trigger workflow new threat intelligence • Threat information
Response	-

Interface Reference	INTF3.01
Provider	Infrastructure Modelling Component
Input	Request new model
Response	Infrastructure model

Interface Reference	INTF6.01
Provider	Attack Defence Graph analyser
Input	• Infrastructure model • Threat Information Update (e.g. change in likelihood attack techniques, change in CVSS)
Response	Results of ADG analysis • Attack paths

	• ΔTTC for (critical) assets

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	(List of) Asset ID, type of compromise
Response	Business Impact per requested asset

Interface Reference	INTF8.01
Provider	CoA Generator
Input	Infrastructure model, asset(s) for which the TTC need to be reduced
Response	• List of CoAs • Effectiveness metric of each of the CoAs

Interface Reference	INTF9.01
Provider	Response Planner
Input	• CoA • Effectiveness metric
Response	• RORI

Interface Reference	INTF7.02
Provider	Web Front-end
Input	Results of ADG & business impact analysis • Infrastructure model • TTC • CoA • RORI
Response	-

Data models

- Infrastructure model
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)
- Business Impact
- Courses of Action (CoA)
- Effectiveness of CoA
- Return Of Response Investment (RORI)
- Threat Information Update (e.g. change in likelihood attack techniques, change in CVSS)
- Adversary Emulation Plan
- Playbook to execute CoA

Requirements for test & pilot environments

- The test environments & pilot sites must be able to support infrastructure modelling.
- The test environments & pilot sites must provide a Threat Intelligence Platform that can trigger analysis by the SOCCRATES platform for new threat information.

- The test environments & pilot sites must run the SOCCRATES platform components listed above.

3.3.3 Scenario 2.2: Delivery of CTI derived from a.o. malware forensic data

In this scenario the focus is on the production of CTI at Shadowserver and the distribution of this CTI to SOCCRATES platform components. The unique basis for this CTI is the sandbox malware report repository. In section 4.3 a description of the capabilities and envisioned innovation at Shadowserver is given. In this section the focus is on the envisioned CTI that can be provided and which SOCCRATES Component will consume it.

At Shadowserver the *Threat Data Collection & Threat Prediction* component will be setup. This component will use machine learning/deep learning/AI analysis on the collected threat data to produces advanced threat intelligence. This is made available via an API. Within the SOCCRATES platform we identified two components that could interact with the *Threat Data Collection & Threat Prediction* via the API to collect the CTI, these are[4] (see also Figure 3.5):

1. *Threat Intelligence Platform* – the TIP is the logical component to collect and analyse CTI and trigger an analysis such as described in scenario 2.1 or support incident detection and incident response operations such as described in use case 1.
2. *AI based Attack Detection* – the attack detection component can directly leverage from the information that the *Threat Data Collection & Threat Prediction* can provide. For example, the Domain Generated Algorithms (DGAs) and samples of malicious behaviour (e.g. in network traffic) can be used to train the AI based Attack Detection.

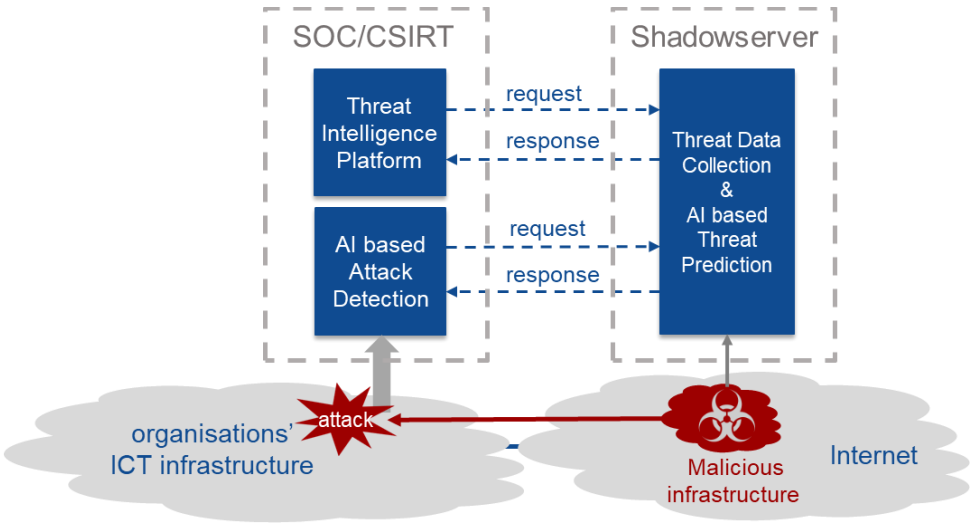


Figure 3.5 – Interaction with *Threat Data Collection & Threat Prediction* component

For now, the following sub-scenarios are foreseen:

- *CTI enrichment at the TIP.* The *TIP* receives a hash of a malware sample, either via internal incident response operations, or external CTI feed, request the *Threat Data Collection &*

[4] Initially the idea was that the *TIP* would interact with the *Threat Data Collection & Threat Prediction* component, but for data that is directly relevant for the operation of the *AI based Attack Detection*, such as the training sets, it was decided that the *AI based Attack Detection* component can directly interact with the *Threat Data Collection & Threat Prediction* component.

Threat Prediction to report what it knows about this malware (e.g. classify it to the malware family).

- *The TIP collects the latest CTI report.* Periodically the *TIP* requests the latest report(s) of the threat intelligence produced by AI-based analysis of large amount of sandbox malware reports. The *Threat Data Collection & Threat Prediction* will provide the analysis results in a machine-readable data format.
- *AI-based Attack Detection* collects training data. Periodically the *AI-based Attack Detection* component requests the latest training data produced by AI-based analysis of large amount of sandbox malware reports. The *Threat Data Collection & Threat Prediction* will provide the analysis results in a machine-readable data format.

3.3.3.1 Analysis

Findings & issues

- The Shadowserver malware sandbox report repository is a live, constantly updated repository operating in production. The file samples being ingested are representative of the threats being seen in the industry. Nevertheless, false positives in the form of benign files, can also be ingested. This means that any malicious behaviour training set generated over this data may be "polluted" if not sufficiently filtered.
- In addition to the above, the threat environment is constantly evolving. For example, it is possible that the threats of yesterday or today that utilize DGAs for building botnet resilience may disappear in the near future or evolve, rendering algorithms developed or training datasets obtained over older data less effective. Algorithms developed may need to take this into account.
- The exact type of threat intelligence that will be provided by the Threat Data Collection & Threat Prediction is largely dependent on the above developments. For this reason, we are not able to specify exactly what type of threat intelligence will be made available through the API for now (though we do list some general categories above). The exact TI will change in accordance with the findings of the developed algorithms (as well as evolving threat environment) and will be better determined by the time of the D4.2 Threat Identification and Threat Trend prediction - Initial Prototype.
- The main SOCCRATES platform components interacting with the Threat Data Collection & Threat Prediction component are the Threat Intelligence Platform (TIP) and AI based Attack Detection. Information derived through the Threat Data Collection & Threat Prediction component may then be used by these components as specified in Scenario 2.1 SOCCRATES platform receives new CTI or potentially even other UC, for example UC1 Response on Detected Ongoing Attack.

Components

- Threat Data Collection & Threat Prediction
- Threat Intelligence Platform (TIP)
- AI based Attack Detection

Interfaces

Note: These may be subject to change.

Interface Reference	INTF10.01
Provider	Threat Data Collection & Threat Prediction

Input	Indicators for Malware (e.g. hash)
Response	Malware classification information

Interface Reference	INTF10.02
Provider	Threat Data Collection & Threat Prediction
Input	<to be defined>
Response	latest threat intelligence report (e.g. Malicious Traffic Patterns)

Interface Reference	INTF10.03
Provider	Threat Data Collection & Threat Prediction
Input	<to be defined>
Response	latest AI training data

Data models

- Indicators for Malware (e.g. hash)
- Malware classification information
- Malicious Traffic Patterns
- AI Trainings sets

Requirements for test & pilot environments

No additional requirements identified.

3.4 Use Case 3: Response on Newly Discovered Vulnerable Assets

3.4.1 Introduction

This use case is oriented towards automatically analysing and determining the response to the discovery of a vulnerable asset. First the current situation is described and next the envisioned improvement with the SOCCRATES platform is presented.

Current situation

Many organisations perform vulnerability scans within their networks, scanning network services and hosts for vulnerable software. These vulnerability scanners generate many alerts that have to be evaluated by human security analysts. The security analyst has to decide whether the alert is a false positive and which course of action should be taken, considering possible business impact and downtime of the services involved. Based on the CVE information, the analyst may also decide to check for IOCs within the infrastructure, based on logs and network captures (i.e. threat hunting). However, most organizations however, lack the data and systems to accurately determine the full extent of their infrastructure, which makes it difficult and time consuming to assess the exposure of vulnerabilities and consequences of misuse in attacks. Furthermore, it is challenging to determine and assess the possible response options for mitigating vulnerabilities.

SOCCRATES platform improvement

The SOCCRATES platform automatically collects data on infrastructure, including vulnerability scan results. When new vulnerable assets are detected the orchestrator is triggered. The current model of the infrastructure will be assessed to determine if due to the new vulnerable assets new attack paths

are possible that could lead to a higher risk for compromise. The SOCCRATES platform can also determine the best courses of action to mitigate the threat of compromise within a certain period (incl. patch cycles). This assessment includes a trade-off analysis. The SOC analyst will be presented with the results of the assessments and can select the desired action. The SOCCRATES platform automatically initiates this action.

3.4.2 Workflow in SOCCRATES platform

The starting point of this scenario is a report from a vulnerability scanner, that periodically scans the infrastructure for vulnerable assets, and indicates a new vulnerability on one of the assets. The vulnerability scanner itself is out of scope of the SOCCRATES platform, but it is assumed that it is regularly updated, and is capable of providing output in a structured report to the Orchestration & Integration engine. The interaction between the SOCCRATES platform components for this use case are described below. This workflow is depicted in a Swimlane diagram in Annex C.

1) A vulnerability scanner periodically scans the infrastructure for vulnerable systems. The vulnerability management system stores the result and compares the vulnerability score of the asset with the previous scan score. If the vulnerability score differs from the previous score for this object, the orchestrator is triggered with a list of asset IDs and related CVEs.
2) The *Orchestration & Integration Engine* requests the current infrastructure model (M_n) from the *Infrastructure Modelling Component* (IMC).
3) The *Infrastructure Modelling Component* produces the new current model M_n, stores the new infrastructure model and informs the *Orchestration & Integration Engine* with pointer to location in the store of M_n
4) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to analyse the new infrastructure model M_n, with and without the reported vulnerabilities in assets.
5) The *Attack Defence Graph analyser* performs the analysis on the infrastructure model with and without the vulnerabilities. The *Attack Defence Graph analyser* returns the difference in Time To Compromise (TTC) for each business relevant system, due to the discovery of the vulnerable systems.
6) The *Orchestration & Integration Engine* requests the business impact data from the *Impact Analyser* for each of the (critical) system for which the TTC was changed (significantly) due to the newly discovered vulnerability in the systems.
7) The *Impact analyser* performs a business impact analysis on the list of assets and type of compromise provided by the *Orchestration & Integration Engine*, and returns the business impact per asset.
8) The *Orchestration & Integration Engine* forwards the results (ΔTTC and BI per asset) to the *Web Front-End* for presentation to the SOC analyst.
9) The *SOC analyst* decides whether or not to start the generation of CoAs.
    a. If the SOC analyst decides that it is not necessary to generate a list of CoAs for the selected asset(s), the process stops.
    b. If the SOC analyst decides that, based on presented information, it is necessary to start looking for the best CoA, the orchestrator is triggered to start the *Course of Action Generator*.
10) The *Orchestration & Integration Engine* requests the *Course of Action Generator* to generate a list of possible CoAs for the changed assets, based on infrastructure model M_n, and the (critical) systems that need to be protected.

11) The *CoA Generator* produces a list of Courses of Action, and may check the Threat Intel Platform (TIP) based on the CVE to get recommended CoAs for this vulnerability. For each CoA a metric for the change in TTC is included (i.e. effectiveness of CoA).
12) The *Orchestration & Integration Engine* requests the *Impact Analyser & Response Planner* to determine the Return on Response Investment (RORI) for each of the Courses of Action.
13) The *Impact Analyser & Response Planner* produces a prioritized list of Courses of Action with RORI. Note that the CoAs may differ in time when deployed (e.g. patch during the weekend).
14) The *Orchestration & Integration Engine* forwards the results to the *Web Front-End* for presentation to the SOC analyst.
15) The SOC analyst may select a preferred Course of Action:
    a. Take no further action.
    b. Trigger the *Orchestration & Integration Engine* to generate the playbook for the selected Courses of Action. Next the workflow is triggered for execution of the playbook by the *(Automated) Reconfiguration component*.

3.4.3 Analysis

Findings & issues

- The workflow after the initial discovery of a vulnerability are similar to scenarios from Use Cases 4 and 5.
- The level of detail and exchange format of the information provided by the vulnerability scanner is not defined in detail yet.

Components

- Attack Defence Graph analyser
- CoA Generator
- Impact Analyser & Response Planner
- Infrastructure Modelling Component
- Orchestration & Integration Engine
- Web Front-End
- Security Monitoring Solutions

Interfaces

Interface Reference	INTF2.03
Provider	Orchestration & Integration Engine
Input	Trigger workflow new vulnerability • Asset Identifier • CVE
Response	<to be defined>

Interface Reference	INTF3.01
Provider	Infrastructure Modelling Component
Input	Request new model
Response	Infrastructure model

Interface Reference	INTF6.02

Provider	Attack Defence Graph analyser
Input	Infrastructure models: • Without vulnerability • With vulnerability
Response	Results of ADG analysis (incl. TTC of critical assets in infrastructure model): • Without vulnerability • With vulnerability

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	(List of) Asset ID, type of compromise
Response	Business impact per requested asset

Interface Reference	INTF7.02
Provider	Web Front-end
Input	Report containing: • Delta TTC per asset • Business impact per asset
Response	

Interface Reference	INTF2.04
Provider	Orchestrator & Integration Engine
Input	Trigger for CoA generation
Response	<to be defined>

Interface Reference	INTF8.01
Provider	CoA generator
Input	Infrastructure model
Response	• List of CoAs • Effectiveness metric of each of the CoAs

Interface Reference	INTF9.01
Provider	Response Planner
Input	List of CoAs (including measure of effectiveness)
Response	List of prioritized CoAs with per CoA: • RORI

Interface Reference	INTF7.02
Provider	Web Front-end
Input	List of CoAs with per CoA: • RORI • TTC improvement
Response	<to be defined>

Interface Reference	INTF2.05
Provider	Orchestration and Integration Engine
Input	Selected CoA – Trigger playbook preparation
Response	-

Data models

- Infrastructure model
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)
- Business Impact
- Courses of Action (CoA)
- Effectiveness of CoA
- Return Of Response Investment (RORI)
- Playbooks related to CoA
- Business process model

Requirements for test & pilot environments

- The vulnerability scanner should be able to scan assets (at least) from within the same network segment in order to get similar results to a potential attacker
- The vulnerability scanner should be able to publish results to the *Orchestration and Integration Engine*.

3.5 Use Case 4: Response on Discovered System Configuration Change

3.5.1 Introduction

The ICT infrastructure of an organisation is a dynamic environment, in which configurations of assets will change during their lifetime. At the start of this use case, a system configuration change is detected, and the SOCCRATES platform will respond to this change by assessing new possible attack paths enabled by the change, assessing potential business impact, and deciding on the most appropriate mitigatory actions to take. The SOCCRATES platforms aims to improve the current state within an organisation as described below.

Current situation

In general, IT departments deploy and (unit) test system configuration changes in separated environments, before releasing them to the production environment. Changes will be deployed either manually or by using configuration management systems. While changing system configurations on a single asset, the assessment of the impact on the entire infrastructure is often overlooked. Therefore, the introduction of a change could lead to unexpected additional attack paths.

SOCCRATES platform improvement

The Infrastructure Modelling Component is periodically triggered by either the “Orchestration & Integration Engine”, or the “Infrastructure Modelling Component”. It can also be automatically triggered by the “Automatic Reconfiguration Component”. After the initial discovery of the configuration change, the SOCCRATES platform automatically assesses if the configuration change introduces new vulnerabilities and attack paths, and determines potential impact when the vulnerable configuration

change is exploited, which actions are needed to reduce the exposure of the configuration change, and trade-offs of these actions. All the results will be presented to the SOC analyst as actionable insight and advice. When the SOC analyst selects the desired action, the SOCCRATES platform automatically initiates this action (e.g. reconfigure).

3.5.2 Workflow on SOCCRATES platform

Once the "Infrastructure Modelling Component" discovers a configuration change, the exact same steps (i.e. from step 2 onwards) are used as in scenario 3.1. This workflow is depicted in a Swimlane diagram in Annex D.

1) Either the *Vulnerability Scanner* (see Use Case 3) or the *Infrastructure Modelling Component* triggers the *Orchestration & Integration Engine* to request a new assessment due to (significant) configuration change in one or more assets.
2) The *Orchestration & Integration Engine* requests the current infrastructure model (M_n) from the *Infrastructure Modelling Component* (IMC).
3) The *Infrastructure Modelling Component* produces the new current model M_n, stores the new infrastructure model and informs the *Orchestration & Integration Engine* with pointer to location in the store of M_n.
4) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to analyse the new infrastructure model M_n, with and without the system configuration change.
5) The *Attack Defence Graph analyser* performs the analysis on the infrastructure model with and without the new system configuration change. For the configuration change, the ADG analyser has to update the parameters on among others the likelihood of certain attack techniques (see below). The *Attack Defence Graph analyser* returns the difference in Time To Compromise (TTC) for each business relevant system, due to the discovery of the configuration change.
6) The *Orchestration & Integration Engine* requests the business impact data from the *Impact Analyser* for each of the (critical) system for which the TTC was changed (significantly) due to the configuration change.
7) The *Impact analyser* performs a business impact analysis on the list of assets impacted provided by the *Orchestration & Integration Engine*, and returns the business impact per asset.
8) The *Orchestration & Integration Engine* forward the results (ΔTTC and BI per asset) to the *Web Front-End* for presentation to the SOC analyst.
9) The *SOC analyst* decides whether to start the generation of CoAs.
    a. If the SOC analyst decides that it is not necessary to generate a list of CoAs for the selected asset(s), the process stops.
    b. If the SOC analyst decides that, based on presented information, it is necessary to start looking for the best CoA, the orchestrator is triggered to start the *Course of Action Generator*.
10) The *Orchestration & Integration Engine* requests the *Course of Action Generator* to generate a list of possible CoAs to mitigate the risks due to the configuration change, based on infrastructure model M_n, and the (critical) systems that need to be protected.
11) The *CoA Generator* produces a list of Courses of Action. For each CoA, a metric for the change in TTC is included (i.e. effectiveness of CoA).
12) The *Orchestration & Integration Engine* requests the *Impact Analyser & Response Planner* to determine the Return on Response Investment (RORI) for each of the Courses of Action.
13) The *Response Planner* produces a prioritized list of Courses of Action with RORI. Note that the CoAs may differ in time when deployed (e.g. patch during the weekend).

14) The *Orchestration & Integration Engine* forwards the results (TTC, RORI and timeslots) to the *Web Front-End* for presentation to the SOC analyst.
15) The SOC analyst may select a preferred Course of Action:
    a. Take no further action.
    b. Trigger the *Orchestration & Integration Engine* to generate the playbook for the selected Courses of Action and execute this using the interfaces provided by *the (Automated) Re-configuration component*.

3.5.3 Analysis

Findings & issues

- Either the *vulnerability scanner*, or the *Infrastructure Modelling Component* must be able to trigger the discovery of changed configurations. The component that will trigger this is not yet decided upon. An alternative approach is where the Orchestration & Integration Engine periodically requests a new infrastructure model M_n and start an analysis of the new and previous requested infrastructure model M_{n-1}.
- The ADG analyser must provide some metric on the effectiveness of the CoAs for the analysis by the Response Planner.

Components

- Attack Defence Graph analyser
- CoA Generator
- Impact Analyser & Response Planner
- Infrastructure Modelling Component
- Orchestration & Integration Engine
- Web Front-End
- Automatic Reconfiguration Component

Interfaces

Interface Reference	INTF2.06
Provider	Orchestration & Integration Engine
Input	Trigger to assessment due to configuration change in one or more assets
Response	-

Interface Reference	INTF302
Provider	Infrastructure Modelling Component
Input	List of: • Asset Identifier • Configuration change
Response	Infrastructure model

Interface Reference	INTF6.02
Provider	Attack Defence Graph analyser

Input	Infrastructure models: • Without configuration change • With configuration change
Response	Results of ADG analysis (incl. TTC of critical assets in infrastructure model): • Without configuration change • With configuration change

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	List of impacted assets
Response	Business impact per impacted asset

Interface Reference	INTF7.02
Provider	Web Front-end
Input	Report containing: • Delta TTC per asset • Business impact per asset
Response	

Interface Reference	INTF2.04
Provider	Orchestrator & Integration Engine
Input	Trigger for CoA generation
Response	-

Interface Reference	INTF8.01
Provider	CoA generator
Input	Infrastructure model, asset(s) for which the TTC need to be reduced
Response	• List of CoAs • Effectiveness metric of each of the CoAs

Interface Reference	INTF9.01
Provider	Response Planner
Input	List of CoAs (including measure of effectiveness)
Response	List of prioritized CoAs with per CoA: • RORI

Interface Reference	INTF7.02
Provider	Web Front-end
Input	List of CoAs with per CoA: • RORI • TTC improvement
Response	-

Interface Reference	INTF2.05
Provider	Orchestration and Integration Engine
Input	Selected CoA – Trigger playbook preparation
Response	<to be defined>

Data models

- Infrastructure model
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)
- Business Impact
- Courses of Action (CoA)
- Effectiveness of CoA
- Return Of Response Investment (RORI)
- Playbooks related to CoA
- Business process model

Requirements for test & pilot environments

- No additional requirements

3.6 Use Case 5: Response on Deployment of New Systems in Infrastructure

3.6.1 Introduction

The introduction of new systems in an existing or new ICT infrastructure may introduce new unforeseen attack paths. The SOCCRATES platforms aims to improve the current state within an organisation as described below.

Current situation

Currently, continuous vulnerability management and attack detection can automatically detect new systems in the infrastructure. This event may trigger a vulnerability scanner to check whether it can find any vulnerable service on this particular asset. However, there are no automated assessment tools to determine if new attack paths are introduced to other parts of the infrastructure and what countermeasures should be taken.

SOCCRATES platform improvement

The SOCCRATES platform automatically assesses if the new systems introduce new attack paths, determines the potential business impact of these new attack paths, determines what security measures are needed to mitigate the new threats, and determines the trade-offs in order to prioritize the security measures. All the results will be presented to the SOC analyst as actionable insight and advice. When the SOC analysts selects the desired action, the SOCCRATES platform automatically initiates this action (e.g. trigger the automated reconfiguration component).

3.6.2 Workflow on SOCCRATES platform

The process of updating the infrastructure model may be triggered (periodically) by either the *Infrastructure Modelling Component*, the *Orchestration & Integration Engine*, or the *Automated Reconfiguration Component.* After this initial discovery of a new system, the exact same steps (i.e. from step 2 onwards) are used as in use case 3. This workflow is depicted in a Swimlane diagram in Annex E.

1) The *Infrastructure Modelling Component* triggers the *Orchestration & Integration Engine* to (periodically) request a new infrastructure model from the *Infrastructure Modelling Component*.
2) The *Orchestration & Integration Engine* requests the current infrastructure model (M_n) from the *Infrastructure Modelling Component* (IMC).
3) The *Infrastructure Modelling Component* produces the new current model M_n, stores the new infrastructure model and informs the *Orchestration & Integration Engine* with pointer to location in the store of M_n.
4) The *Orchestration & Integration Engine* requests the *Attack Defence Graph analyser* to analyse the new infrastructure model M_n, with and without the newly discovered system(s).
5) The *Attack Defence Graph analyser* performs the analysis on the infrastructure model with and without the new systems. For the infrastructure change, the ADG analyser has to update the parameters on among others the likelihood of certain attack techniques (see below). The *Attack Defence Graph analyser* returns the difference in Time To Compromise (TTC) for each business relevant system, due to the discovery of the new system(s).
6) The *Orchestration & Integration Engine* requests the business impact data from the *Impact Analyser* for each of the (critical) system for which the TTC was changed (significantly) due to the newly discovered system.
7) The *Impact analyser* performs a business impact analysis on the list of assets impacted provided by the *Orchestration & Integration Engine*, and returns the business impact per asset.
8) The *Orchestration & Integration Engine* forwards the results (ΔTTC and BI per asset) to the *Web Front-End* for presentation to the SOC analyst.
9) The *SOC analyst* decides whether to start the generation of CoAs.
    a. If the SOC analyst decides that it is not necessary to generate a list of CoAs for the selected asset(s), the process stops.
    b. If the SOC analyst decides that, based on presented information, it is necessary to start looking for the best CoA, the orchestrator is triggered to start the *Course of Action Generator*.
10) The *Orchestration & Integration Engine* requests the *Course of Action Generator* to generate a list of possible CoAs to mitigate the risks due to the newly discovered systems, based on infrastructure model M_n, and the (critical) systems that need to be protected.
11) The *CoA Generator* produces a list of Courses of Action. For each CoA, a metric for the change in TTC is included (i.e. effectiveness of CoA).
12) The *Orchestration & Integration Engine* requests the *Impact Analyser & Response Planner* to determine the Return on Response Investment (RORI) for each of the Courses of Action.
13) The *Response Planner* produces a prioritized list of Courses of Action with RORI. Note that the CoAs may differ in time when deployed (e.g. patch during the weekend).
14) The *Orchestration & Integration Engine* forwards the results (TTC, RORI and timeslots) to the *Web Front-End* for presentation to the SOC analyst.
15) The SOC analyst may select a preferred Course of Action:
    a. Take no further action.

b. Trigger the *Orchestration & Integration Engine* to generate the playbook for the selected Courses of Action and execute this using the interfaces provided by *the (Automated) Re-configuration component*

3.6.3 Analysis

Findings & issues

- Either a *vulnerability scanner* or the *Infrastructure Modelling Component* must be able to trigger the discovery of new systems and services. An alternative approach is where the *Orchestration & Integration Engine* periodically requests a new infrastructure model M_n and start an analysis of the new and previous requested infrastructure model M_{n-1}.
- The *Infrastructure Modelling Component* must be able to produce infrastructure models before and after the discovery of new systems.

Components

- Attack Defence Graph analyser
- CoA Generator
- Impact Analyser & Response Planner
- Infrastructure Modelling Component
- Orchestration & Integration Engine
- Web Front-End
- Automated Reconfiguration Component

Interfaces

Interface Reference	INTF2.06
Provider	Orchestration & Integration Engine
Input	Trigger assessment due to introduction of new systems
Response	None

Interface Reference	INTF3.02
Provider	Infrastructure Modelling Component
Input	List of: • Asset Identifier • New assets
Response	Infrastructure model

Interface Reference	INTF6.02
Provider	Attack Defence Graph analyser
Input	Infrastructure models: • Without configuration newly discovered assets • With configuration newly discovered assets
Response	TTC of infrastructure model: • Without configuration newly discovered assets • With configuration newly discovered assets

Interface Reference	INTF5.01
Provider	Business Impact analyser
Input	List of impacted assets
Response	Business impact per impacted asset

Interface Reference	INTF7.02
Provider	Web Front-end
Input	Report containing: • Delta TTC per asset • Business impact per asset • RORI
Response	-

Interface Reference	INTF2.04
Provider	Orchestrator & Integration Engine
Input	Trigger for CoA generation
Response	-

Interface Reference	INTF8.01
Provider	CoA generator
Input	Infrastructure model
Response	• List of CoAs • Effectiveness metric of each of the CoAs

Interface Reference	INTF9.01
Provider	Response Planner
Input	List of CoAs (including measure of effectiveness)
Response	List of prioritized CoAs with per CoA: • RORI

Interface Reference	INTF7.02
Provider	Web Front-end
Input	List of CoAs with per CoA: • RORI • TTC improvement
Response	-

Interface Reference	INTF2.05
Provider	Orchestration and Integration Engine
Input	Selected CoA – Trigger playbook preparation
Response	-

Data models

- Infrastructure model
- Results of ADG analysis (e.g. attack paths, TTC per asset, type of compromise per asset)
- Business Impact
- Courses of Action (CoA)
- Effectiveness of CoA
- Return Of Response Investment (RORI)
- Playbooks related to CoA
- Business process model

Requirements for test & pilot environments

- Some form of (automatic) reconfiguration component must be in place at the test & pilot environment in order to execute the countermeasures described in the playbook.

4 SOCCRATES pilot sites

The SOCCRATES platform will be deployed and validated at two pilot sites (i.e. Vattenfall and mnemonic). In addition, a third pilot site (i.e. Shadowserver) at which a large amount of threat data is collected by monitoring malicious infrastructures is used for testing and validating the SOCCRATES threat prediction technology.

4.1 Pilot site #1: Deployment at the corporate SOC of VTF

The Vattenfall Security Operation Center (SOC), located in Poland, is the central security monitoring and response facility that services to Vattenfall business units and IT. The scope of the monitoring includes IT infrastructure. The SOC provides the following services to Vattenfall group:

- Logs storage, analysis and correlation
- Threat and Vulnerability Management
- Vulnerability Discovery & Assessment
- Forensic investigations
- Incident response & malware analysis
- Security reporting

Like most of the SOCs, VTF SOC is using many different tools to gain proper reaction speed and detection rate, therefore is using solutions like SOAR, SIEMs, external and internal intelligence sources, log sources, CMDB and IRM. We try to keep our security specialist's knowledge diverse, therefore exploring key competences in several areas like: network administration, Windows and UNIX administration, SIEM administration and data analytics, security systems integrations, incident handling, penetration testing, forensic, malware analysis, scripting, OT, ITIL, knowledge about relevant methodologies etc.

4.1.1 Current situation

The Vattenfall SOC has been separated from the NOC and expanded the number of security operators. All the SOC processes and services can be improved. The Vattenfall SOC is continuously working on improving the services.

4.1.2 Desired situation

The table below lists KPIs to measure the desired improvement by using the SOCCRATES platform.

Table 4-1. KPIs to measure impact of SOCCRATES platform.

KPI	Improvement
Prototype successfully generates a correct model of the pilot infrastructure (all UCs).	>=2
Prototype successfully improves detection capability (incl. detecting attacks in encrypted traffic that was not detected otherwise) (UC1)	20%
Prototype successfully reduces total time of detection and response (UC1)	50%
Prototype successfully reduces total time from collection, analysis and determining pro-active mitigation new CTI (UC2)	50%

Prototype successfully analyses the vulnerability of an asset in the context of the whole infrastructure, that could cause an incident otherwise. (UC3)	>=5
Prototype reduces the time spent on analyses of the severity of vulnerable assets. (UC3)	50%
Prototype proposes at least one course of action that is more efficient/appropriate than what would otherwise have been proposed by a human analyst using templates (UC4 & UC5).	>=5
Prototype reduces the time spent on analysis and determining a course of action (UC4 & UC5).	50%

4.1.3 Vattenfall pilot site requirements

The Vattenfall pilot site provides an enterprise IT infrastructure with a datacentre (DC) network and an office network. The DC network consists of selected VLANs, /24 netmask, a mix of Linux/UNIX and Windows host, and the scope for the pilot is approximately 1000 hosts. The office network consists of selected VLANs, both wired and wireless with mostly Windows clients, and the scope for the pilot is approximately 200 hosts.

The existing security tools that are available for integration include:

- SIEM / Log Management solution
  - Raw or indexed / normalized logs
  - Logs from security tools: Firewall, Web Proxy, IPS, DNS, Vulnerability Scanner
- Selected Layer-3 device (Firewall / Router / L-3 Switch)

The security data available for AI based attack detection include the sources listed above plus NetFlow data.

The SOC and CSIRT processes related to the SOCCRATES use cases include Incident Response, IT Security Monitoring, and Threat & Vulnerability Management.

The pilot will use simulated attack data, but real attack data could be considered if available. The pilot will cover all (non-harmful) use cases.

What are the constraints for deployment of SOCCRATES components at the pilot sites?

- What are the requirements for deployment?
  - Tools are installed at premises on hardware managed by the pilot site provider
  - Tools have to be able to operate without connection to outside (e.g. cloud)
  - What type of VMs, container virtualisations can be supported?
    - VMware vSphere
  - Sensors
    - Physical devices are preferable
    - 1Gbps interfaces at least
    - Traffic mirroring as solution (span port if no TAP devices are available)
    - Communication between sensors and other (analysis) components must be encrypted
  - Analysis components:

        - Virtual appliances are preferable
        - Need to know HW requirements in advance to secure resources and also:
            - What kind of OSes / distributions will be running
            - How many devices - new VLAN to be created
        - All components which will be connected to network, will be network-isolated
        - 2 weeks of quarantine before first usage
- What data may and may not leave the pilot site premises.
    - Source data includes infrastructure model, vulnerability scan data, network traffic data, detected attack events
        - No data can leave Vattenfall premises unless explicitly agreed
    - Can the results of AI based detection tools, or the ADG analyser be exported?
        - Depends on the level of details – needs to be explicitly agreed
    - Any hardware components need to be wiped before return
- Can remote access by SOCCRATES partners/developer to SOCCRATES component be allowed? (e.g. to support configuration or collect and assess results of analysis)
    - No remote access unless explicitly agreed.
        - Interactive sessions not allowed
        - Unidirectional data flows to be considered
        - Restricted terminal access vs. remote hands (telco/video + local support) to be considered
        - Any external SSL/TLS traffic can be intercepted

4.2 Pilot site #2: Deployment at the MSSP SOC of mnemonic

mnemonic provides SOC and CSIRT services to a wide range of different customers, covering all major verticals and both the public and private sectors. The services are delivered through Argus, mnemonic's proprietary platform for managed detection and response. Argus provides a wide array of capabilities, including:

- Multi-user and multi-tenant support with role-based and explicit access control of every event
- Large scale normalisation, correlation, analysis and escalation across multiple heterogeneous data sources (network traffic, infrastructure logs, endpoints)
- Support for complex multi-stage detection rules
- Automated continuous vulnerability management
- Asset database
- Business context for assets
- Automated enrichment and integration with threat intelligence sources
- Automated extraction and deployment of indicators when a new threat is detected
- Integration with advanced threat detection technologies (e.g. sandboxes)
- Automated reporting
- Integrated customer portal

4.2.1 Current situation

mnemonic provides security monitoring and incident response for customers with different infrastructures, business processes, vulnerabilities and priorities. Most organisations today struggle to

maintain an up-to-date view of their own infrastructure and the dependencies from business processes to infrastructure, and the processes in place to maintain this information are in most cases manual. Manual processes are time-consuming and error-prone, thus the documentation of infrastructure and business process dependencies may diverge from reality. For a managed security services provider, it is prohibitively expensive to use manual processes to maintain infrastructure models mapped to business processes for every single customer.

A clear understanding of infrastructure and business process dependencies is required to assess the business impact of a security incident, and machine-readable models are required in order to automate this assessment and propose the best course of action to respond to the security incident. Currently, mnemonic handles infrastructure modelling and business process mapping manually. The recommended course of action for responding to a security incident is determined manually by a human analyst, with the support of templates for the response to common classes of security incidents.

mnemonic continually strives to improve the detection capabilities. We are a heavy user of threat intelligence, with both automated and manual (human analyst) consumption. One significant shortcoming of the state of the art in threat intelligence is the lack of machine-readable representations of tactical threat intelligence, e.g. tactics, techniques and procedures. Machine-readable representations of procedures can be used to detect adversaries even when no indicators of compromise are available, which drastically improves the capability to detect advanced persistent threats (APTs). mnemonic currently uses hand-written detection rules to detect procedures, but this approach does not scale well. We aim to develop machine-readable representations of procedures that can be automatically transformed to detection rules for different security technologies. Such representations can also be used to generate adversary emulation plans (AEPs) as input to attack-defence graph (ADG) analysis systems.

mnemonic already uses techniques from artificial intelligence (AI) to enhance detection capabilities. However, there is a lot of room for improvement, and we are constantly looking for novel applications of AI for the detection of security incidents.

4.2.2 Desired situation

The desired improvements to mnemonic's current services from the SOCCRATES project include:

- (Semi-)automated modelling of customer infrastructure
- (Semi-)automated assessment of security incident impact
- (Semi-)automated suggestion for course of action
- Improved detection capabilities

The same KPIs as those for Vattenfall will be used Vattenfall (see **Table 4-1**).

4.2.3 mnemonic pilot site requirements

The mnemonic pilot site provides an enterprise IT infrastructure with a datacentre (DC) network and an office network. The DC network consists of a mix of Linux/UNIX and Windows servers. The office network consists of a mix of Windows, Linux and BSD clients, both wired and wireless. Additionally, mnemonic has a demo customer infrastructure. Third-party access to project partners could be allowed to the demo infrastructure, but not to the production infrastructure. mnemonic could also contact customers to arrange a pilot involving customer networks, but that would have to be explicitly agreed.

The existing security tools that are available for integration include:

- Argus Managed Detection and Response Platform
  - Raw logs and normalized logs in Argus Event Format (AEF)
  - Logs from security tools: Firewalls, Web Proxy, EDR, AV, IDS, DNS, Vulnerability Scanner
  - Argus API integration documentation is available here: https://docs.mnemonic.no/display/public/API/mnemonic+API+documentation

The security data available for AI based attack detection include the sources listed above plus NetFlow data, PassiveDNS, HTTP access logs, file carving, and JA3 TLS fingerprints.

The SOC and CSIRT processes related to the SOCCRATES use cases include Incident Response, IT Security Monitoring, Threat Intelligence, and Threat & Vulnerability Management.

The pilot will use simulated attack data, but real attack data could be considered if available. The first pilot will validate isolated components, while the full pilot will cover all use cases.

What are the constraints for deployment of SOCCRATES components at the pilot sites?

- What are the requirements for deployment?
  - Tools are installed at premises on hardware managed by the pilot site provider
  - Tools have to be able to operate without connection to outside (e.g. cloud)
  - What type of VMs, container virtualisations can be supported?
    - VMware ESX
  - Sensors
    - Use of existing sensors is preferred
  - Analysis components:
    - Virtual appliances are preferable
    - Need to know HW requirements in advance to secure resources and also:
      - What kind of OSes / distributions will be running
      - How many devices
    - All components which will be connected to network, will be network-isolated
- What data may and may not leave the pilot site premises.
  - Source data includes infrastructure model, vulnerability scan data, network traffic data, detected attack events
    - No data can leave mnemonic premises unless explicitly agreed
  - Can the results of AI based detection tools, or the ADG analyser be exported?
    - Depends on the level of details – needs to be explicitly agreed
  - Any hardware components need to be wiped before return
- Can remote access by SOCCRATES partners/developer to SOCCRATES component be allowed? (e.g. to support configuration or collect and assess results of analysis)
  - No remote access to the production infrastructure unless explicitly agreed.
    - Interactive sessions not allowed
    - Unidirectional data flows to be considered
    - Restricted terminal access vs. remote hands (telco/video + local support) to be considered
    - Any external SSL/TLS traffic can be intercepted

4.3 Pilot site #3: Deployment of Threat Trend Prediction at Shadowserver

Shadowserver is at its core a threat data collection project on a massive scale, which enables the organization to function as a global observatory of threats propagating on the Internet. This knowledge can be used to augment the capabilities of SOCS/CSIRTS, which can apply this knowledge to supplement internal threat detection and response systems available to them.

Over the past 10 years, The Shadowserver Foundation has built its own, unique, internal sandbox system that only has been available to Shadowserver's staff and volunteers. As this proprietary sandbox system has not been made available to the wider security researcher community or the public, it has not been possible for criminals to easily test their malware against it.

Malware samples ingested by Shadowserver are analysed using their sandboxes on a daily basis. Shadowserver has 2000 virtual sandboxes and nearly 300 bare metal sandboxes at its disposal. Each malware sample that is run in a sandbox generates an analysis report. Analysis reports from these sandbox runs include recorded network traffic from a live Internet connection, host level changes (registry, filesystem, process, etc) and AV classification. Any associated snort rulesets or yara rules being triggered are also reported.

Shadowserver possesses a unique malware repository, containing over 1.17 billion malware samples, which is increasing in size at around 600 000 unique (by hash) samples per day. Shadowserver runs collected malware samples through its large array of 29 AV engines and virtual and physical sandboxes with live internet connections, to perform, store and make searchable the results of detailed static and dynamic analysis. They use these data to extract command and control (C2) information, identify criminal infrastructures, better understand cybercriminal behaviour. The collected data are used to provide free of cost victim remediation reports to National CERTs and network owners, and to provide behind the scenes support to Law Enforcement investigations.

4.3.1 Current situation

Currently, malicious activity occurring when malware samples are executed in Shadowserver's sandbox platform is detected and categorized when the observed activity explicitly matches static, hard coded signatures and rules. This can be a list of forward predicted domain names from known DGA (Domain Generation Algorithm) seeds, static IoCs for IP addresses or hashes, or triggering of specific yara or snort signatures that match pre-set binary file or network traffic (IDS) signatures.

4.3.2 Desired situation

Shadowserver's existing data sets and analysis capabilities would be enhanced and expanded through the application of new machine learning/deep learning/AI algorithms for big-data sets developed with project partners. This would for example include some of the following:

- improving the detection and classification of malware based on the results of sandbox executions;
- automatic identification of different characteristics of malicious behaviour (such as Domain Generation Algorithms - DGAs);
- grouping of malicious host level behaviour and network traffic into clusters;
- developing novel ways to describe these clusters;
- identification of anomalies in malicious traffic - outliers or changes of trends in malware behaviours;

- building an API that would enable easy and fast access to the latest signatures/rules of malicious behaviours based on the above analysis

4.3.3 Shadowserver Pilot Site Requirements

The focus of Pilot Site #3 is the analysis of Shadowserver sandbox malware report data. The Shadowserver Pilot is operated in three instances:

1) the testing/training instance

2) the Shadowserver full sandbox report repository

3) the API

In the first instance, testing/training data will be made available by Shadowserver to SOCCRATES project WP4 partners (TNO/AIT) that are focused on developing machine learning/deep learning/AI analysis of threat data. There may be multiple testing/training datasets made available, each focusing on specific features of sandbox data. The training set will provide a full view of the selected features over a set time period (e.g. a week or month). Initial training sets will focus on DNS and DGA related data. Remote access to this data will be provided using an ELK (Elasticsearch/Logstash/Kibana) stack enabled in a VM prepared by Shadowserver. Partners will be able to experiment and explore the dataset. Shadowserver will work with TNO and AIT to explain the datasets, identify what features are of interest and determine what results would be desirable (I.e. define success). Based on this iterative process, new algorithms will be proposed, tested and initially refined.

The second instance of the pilot is the full Shadowserver sandbox malware report repository. Once the algorithms developed in the test/training instance of the pilot are deemed sufficient for broader testing, Shadowserver will apply them internally on the full (or a wider set) of malware analysis reports in their repository. While project partners will not have access to the full repository, Shadowserver will share back with them the aggregated results necessary for any further refinement of the algorithms. Once an algorithm is found that provides useful results, it will be applied to the malware repository on a regular basis.

The third instance of the Pilot site is an API, accessible to WP4 partners and selected vetted external partners (National CSIRTs, LE, industry) during the pilot phase. The API will make available results obtained from machine learning/deep learning/AI analysis of threat data. The API will be utilised for UC2.2 – delivery of threat intelligence produced by AI-based analysis of large amount of sandbox malware reports. The API will either be queried by the T4.1 AI based Anomaly Detectors, which apply the data to network/log traffic, or the TIP (ACT) in T4.4.

The following KPIs will be used in the Shadowserver Pilot (see **Table 4-2**):

Table 4-2. KPIs to measure impact in Pilot site #3.

KPI	Improvement
Prototype successfully detects X new DGA seed from known malware family?	X >= 25
Prototype successfully detects X new, previously unknown malware DGA?	X >= 5
Prototype successfully clusters X malware families	X >= 30
Prototype successfully generate X new detection signatures/rules	X >= 20
New API successfully used by X partners	X >= 10

4.4 Collective requirements for pilot sites

The SOCCRATES platform and/or modules to be deployed during the pilots at Vattenfall and mnemonic will operate in environments with a mix of Linux/UNIX and Windows hosts. The SOCCRATES platform has to meet the following requirements for deployment at the pilot sites:

- Installed on premise on hardware managed by the pilot site provider
- Operated without connection to the outside (e.g. cloud)
- Deployed on VMware vSphere/ESX
- Use existing sensors or deploy sensors with:
    - Physical devices are preferable
    - 1Gbps interfaces at least
    - Traffic mirroring as solution (span port if no TAP devices are available)
    - Communication between sensors and other (analysis) components must be encrypted
- No data can leave the pilot site unless explicitly agreed
- Operated without remote access to the pilot site from other project partners

For the first Shadowserver pilot, the AI based Anomaly Detectors will access the data in an ElasticSearch/Logstash/Kibana (ELK) stack. The final pilot will provide an API to be accessed by the AI based Anomaly Detectors or the Threat Intelligence Platform (TIP).

5 References

[SP800-61] Paul Cichonski. Tom Millar, TimGrance, and Karen Scarfone, *"Computer Security Incident Handling Guide",* NIST Special Publication 800-61 Revision 2, August2012.

[ISO27035] ISO/IEC 27035-1:2016, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.

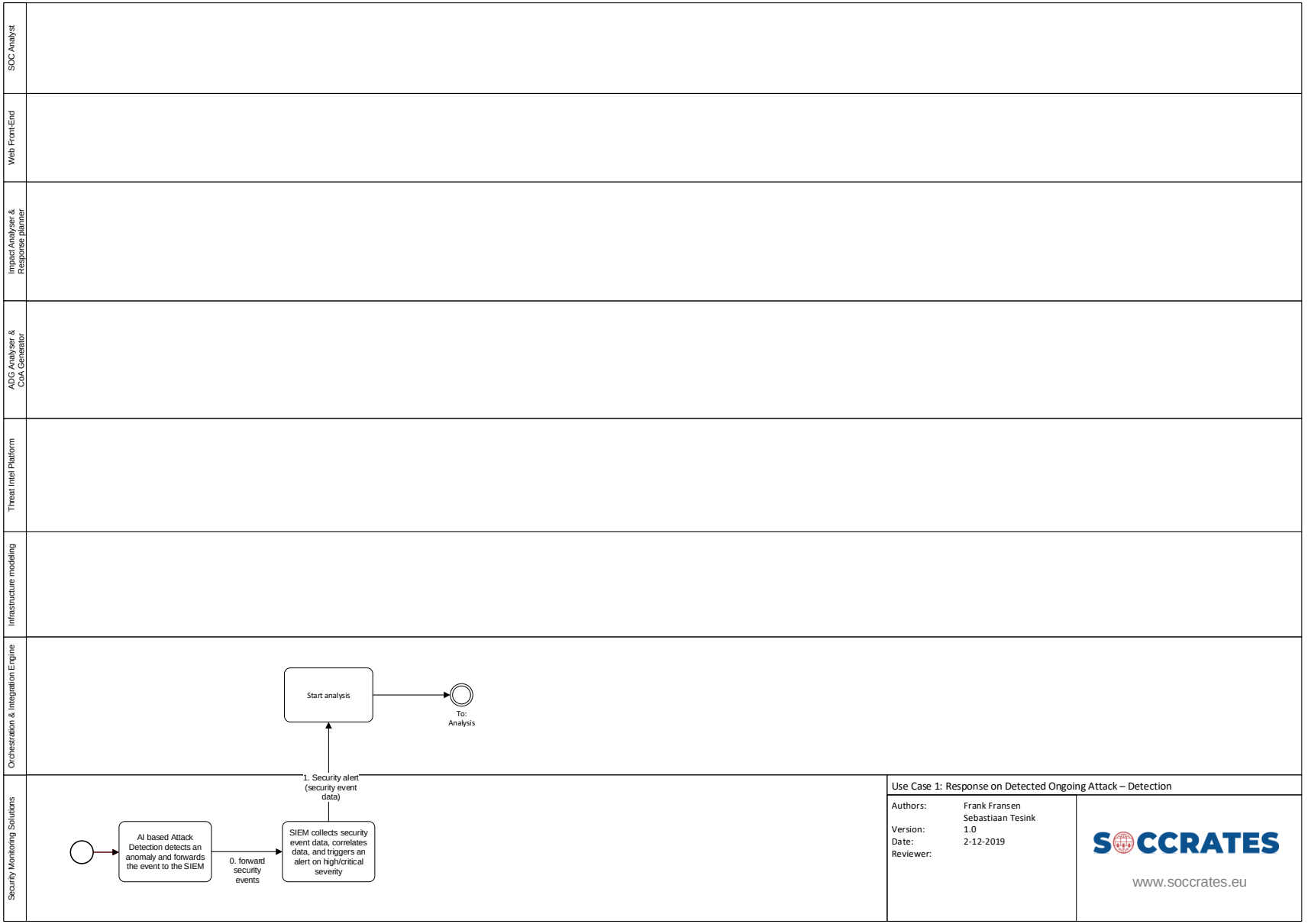
[Hut05] E.M. Hutchins, M.J. Clopp, P.D. Rohan, M. Amin, Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation (2011), pp. 1-14, July 2005

6 Abbreviations

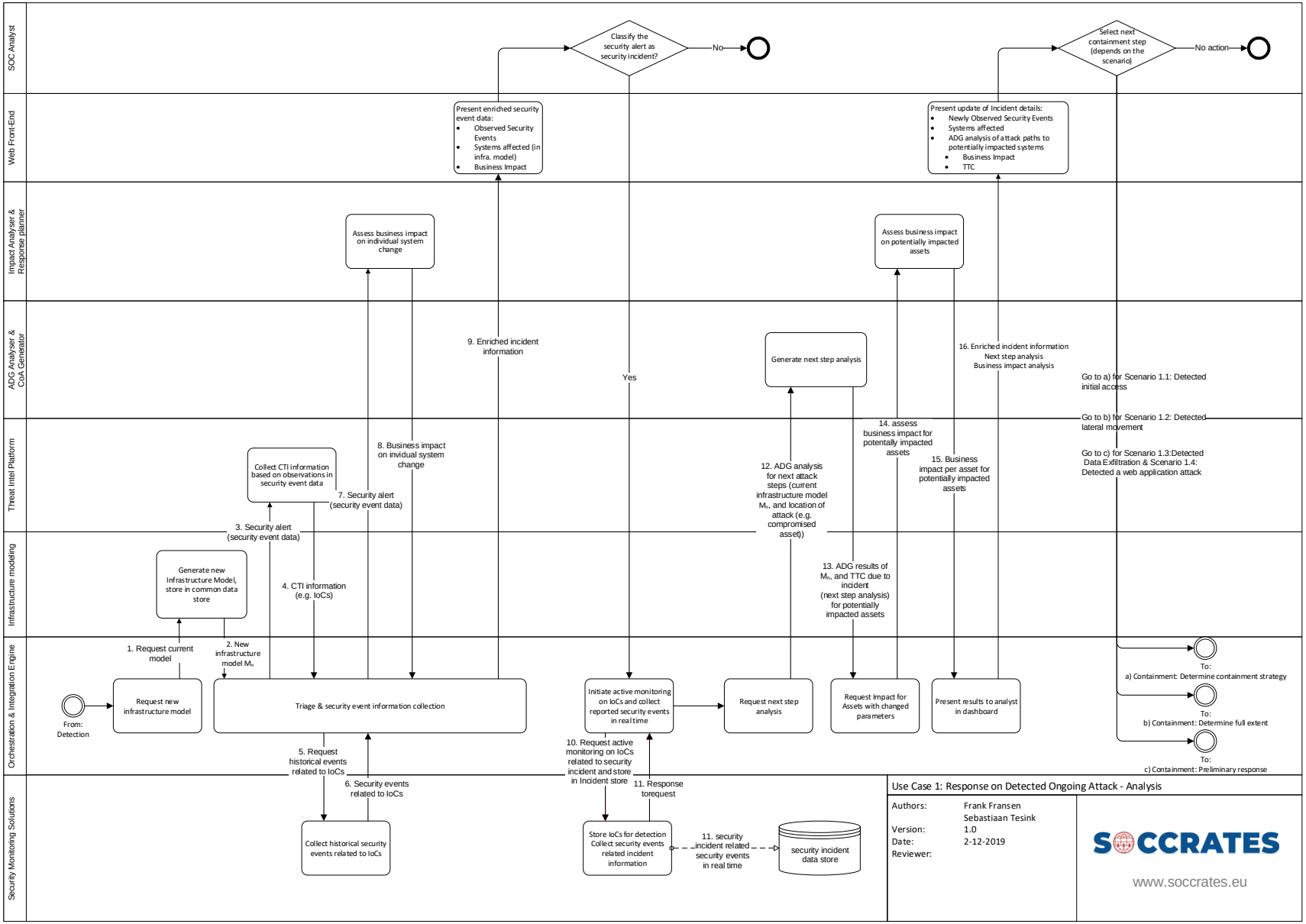
Acronym	Description
ACT	semi-Automated Cyber Threat intelligence
ADG	Attack Defence Graph
AEF	Argus Event Format
AI	Artificial Intelligence
AIT	AIT Austrian Institute of technology
API	Application Programming Interface
APT	Advance Persistent Threat
ATOS	ATOS Spain
AV	AntiVirus
BPMN	Business Process Model 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
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*)
MNM	mnemonic
MSSP	Managed Security Service Provider
MTTD	Mean Time To Detection
NOC	Network Operations Centre
OT	Operational Technology
OS	Operating System

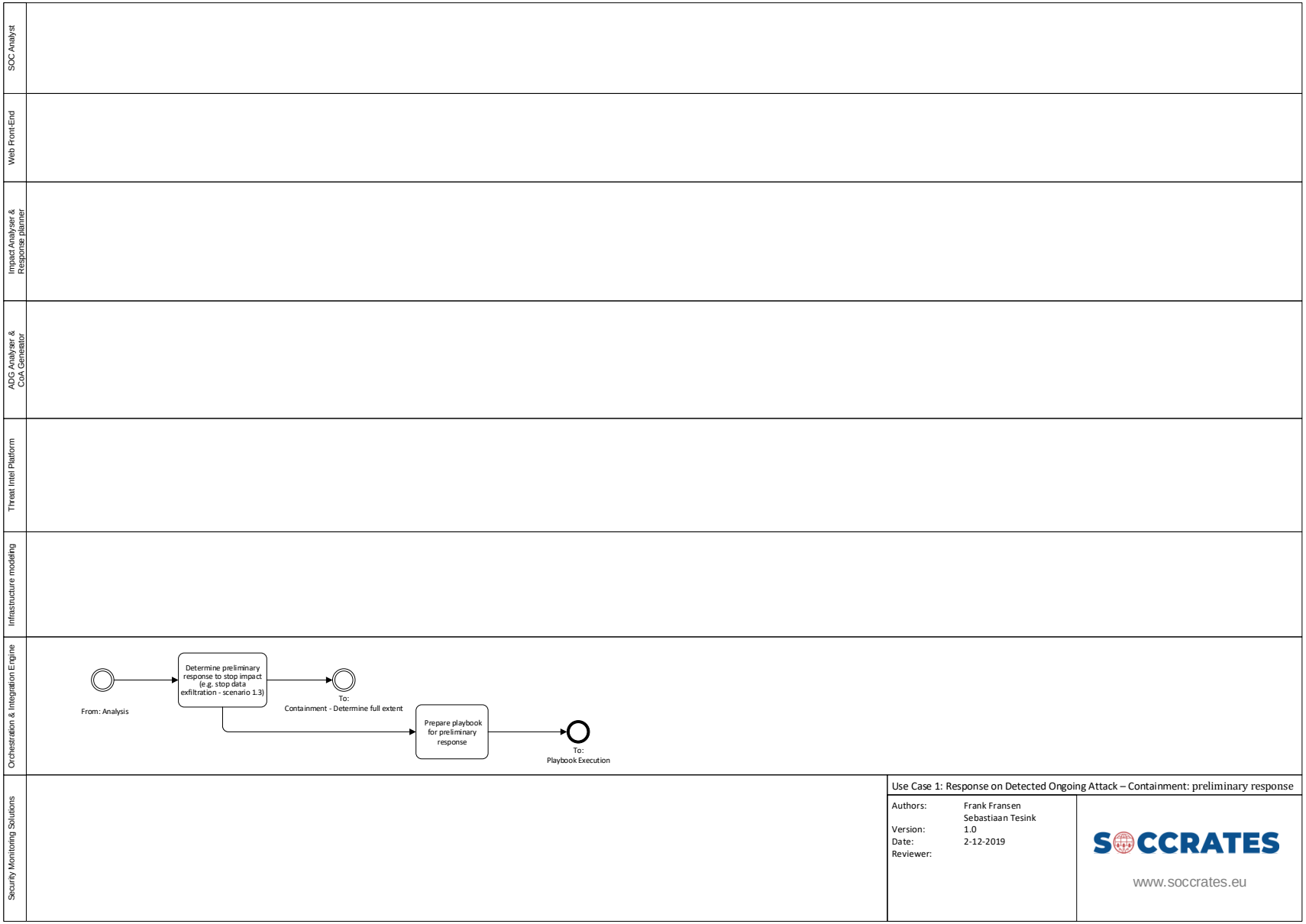
RORI	Return on Response Investment
SDN	Software Defined Network
SHS	Shadowserver
SIEM	Security information and event management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Centre
SOCCRATES	SOC & CSIRT Response to Attacks & Threats based on attack defence graph Evaluation 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

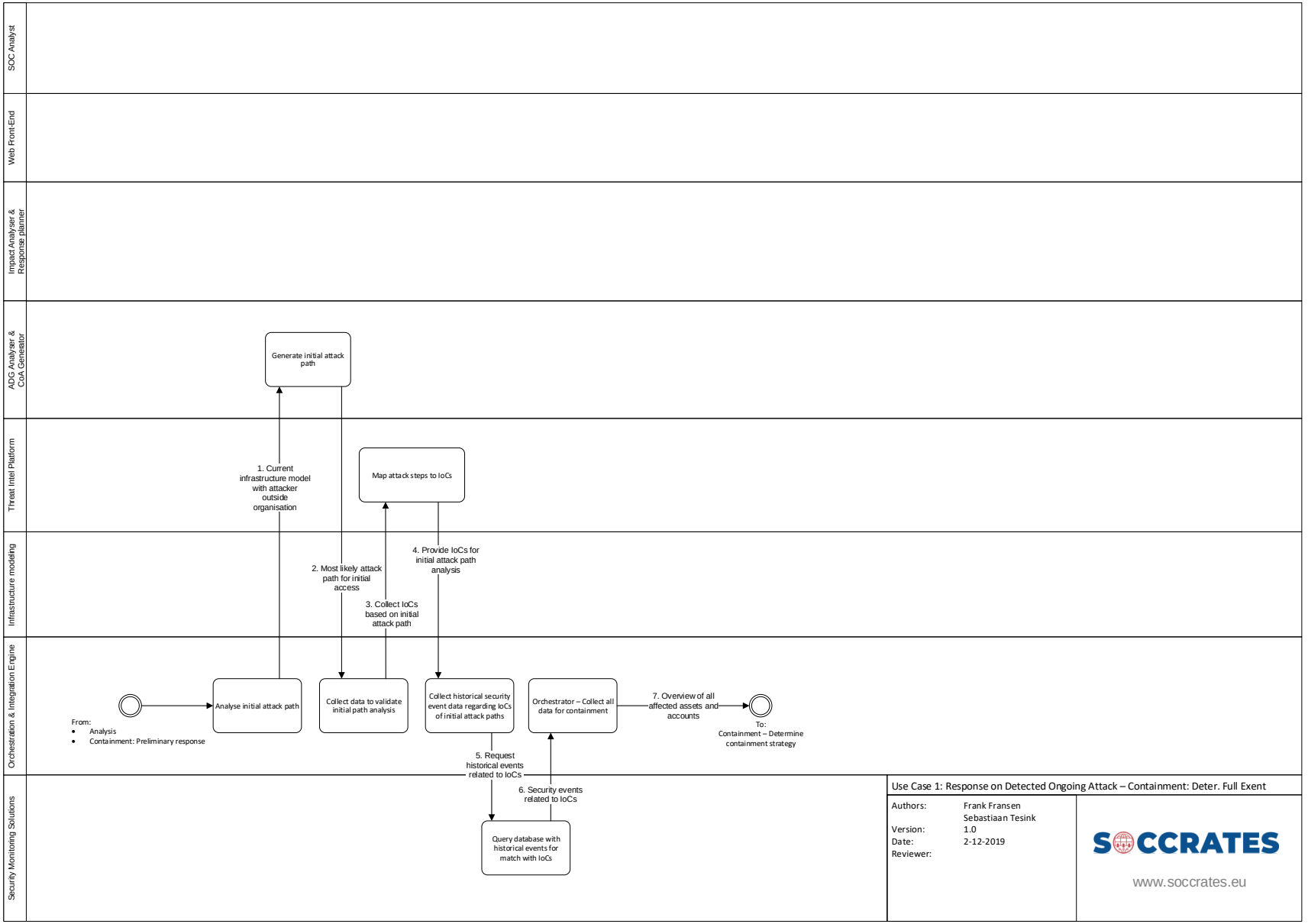
Annex A – Swimlane diagrams UC1

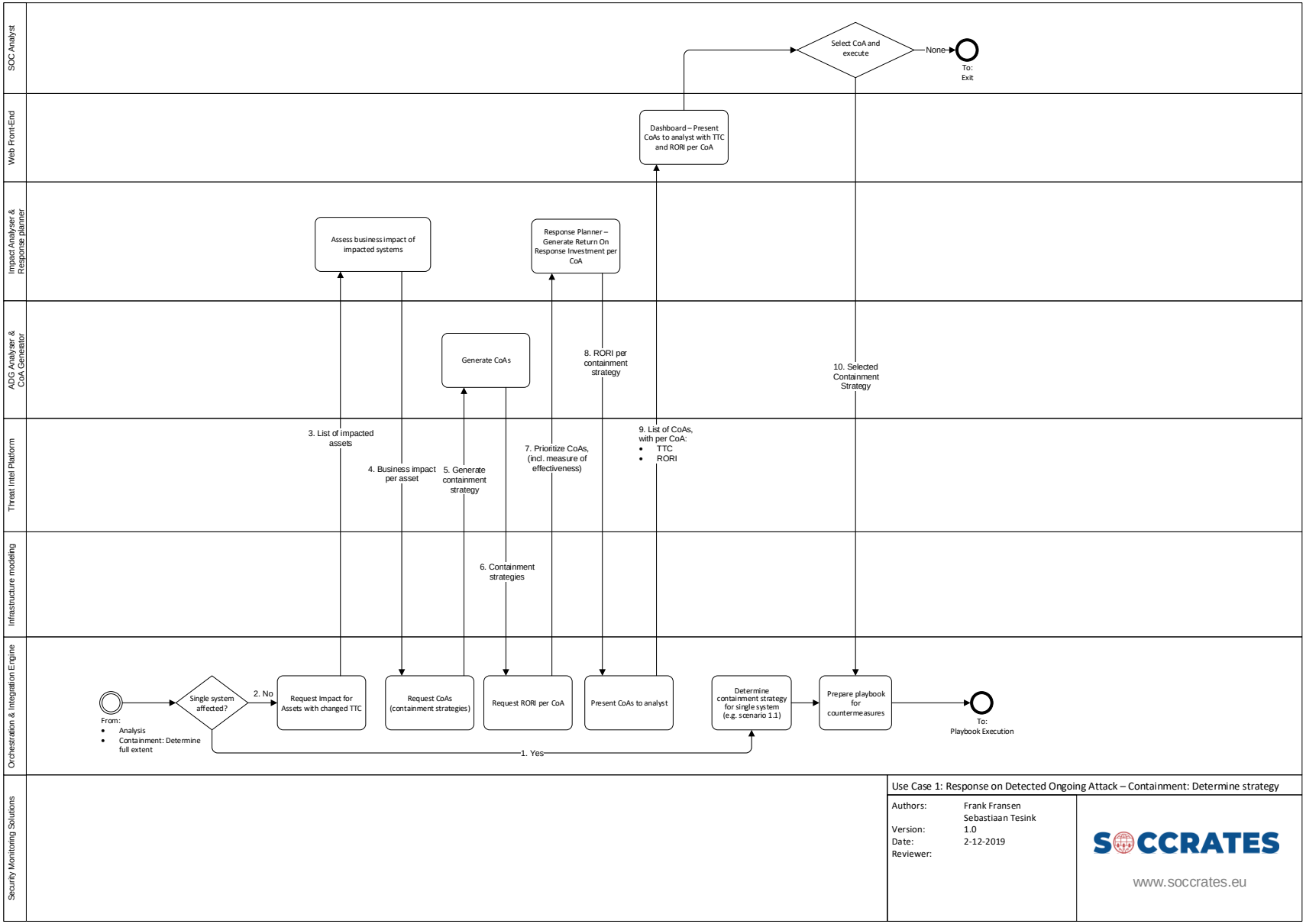


Classification level: Public

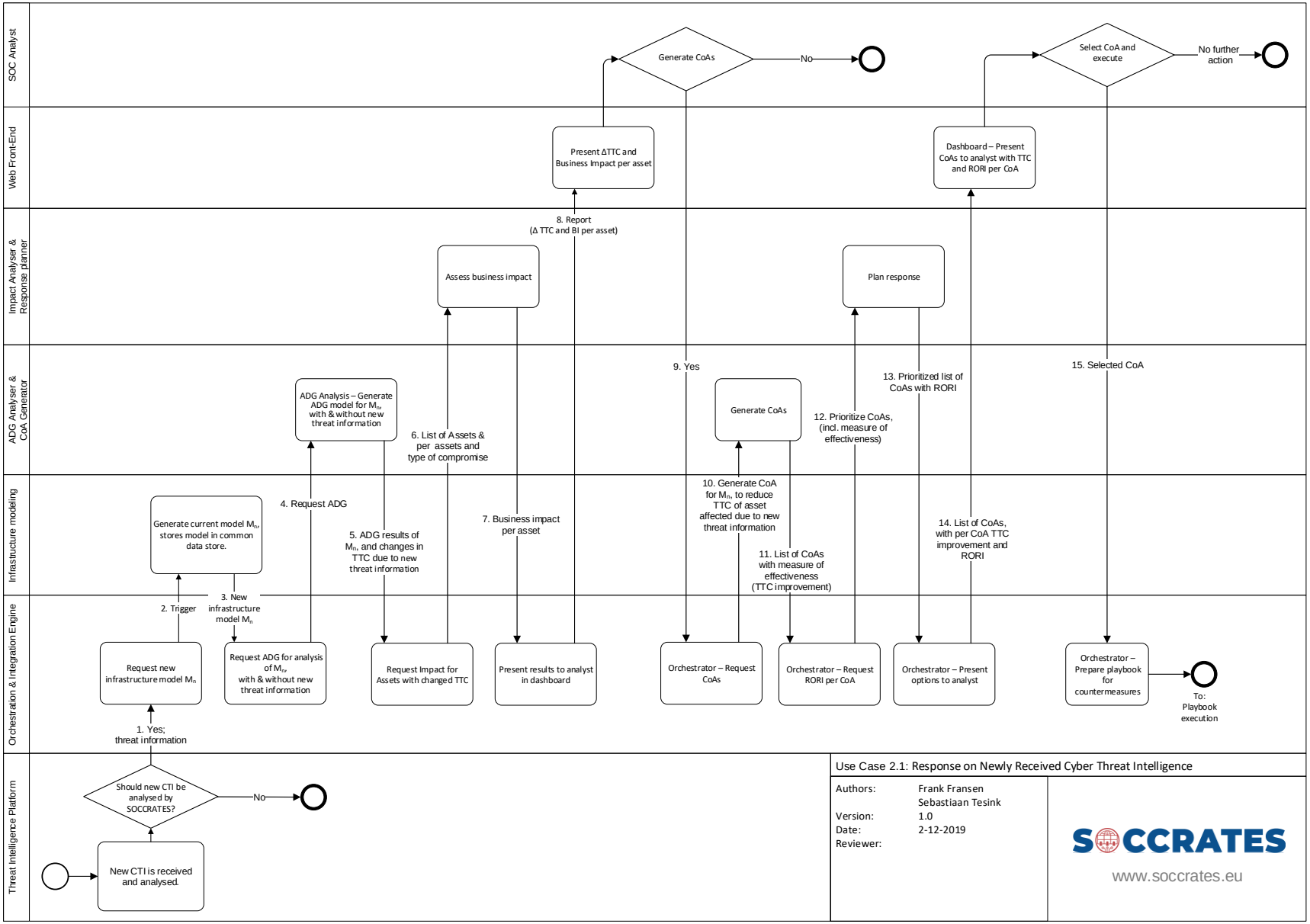

SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Threat Intel Platform
Infrastructure modeling
Orchestration & Integration Engine
Security Monitoring Solutions
Classify the security alert as security incident?
No
Present enriched security event data:
Observed Security Events
Systems affected (in infra. model)
Business Impact
Assess business impact on individual system change
9. Enriched incident information
Yes
Collect CTI information based on observations in security event data
8. Business impact on invidual system change
7. Security alert (security event data)
3. Security alert (security event data)
Generate new Infrastructure Model, store in common data store
4. CTI information (e.g. IoCs)
1. Request current model
2. New infrastructure model M_n
From: Detection
Request new infrastructure model
Triage & security event information collection
5. Request historical events related to IoCs
6. Security events related to IoCs
Collect historical security events related to IoCs
Initiate active monitoring on IoCs and collect reported security events in real time
10. Request active monitoring on IoCs related to security incident and store in Incident store
11. Response torequest
Store IoCs for detection Collect security events related incident information
11. security incident related security events in real time
security incident data store
Generate next step analysis
12. ADG analysis for next attack steps (current infrastructure model M_n, and location of attack (e.g. compromised asset))
Request next step analysis
Assess business impact on potentially impacted assets
14. assess business impact for potentially impacted assets
13. ADG results of M_n, and TTC due to incident (next step analysis) for potentially impacted assets
Request Impact for Assets with changed parameters
15. Business impact per asset for potentially impacted assets
Present results to analyst in dashboard
Select next containment step (depends on the scenario)
No action
Present update of Incident details:
Newly Observed Security Events
Systems affected
ADG analysis of attack paths to potentially impacted systems
Business Impact
TTC
16. Enriched incident information Next step analysis Business impact analysis
Go to a) for Scenario 1.1: Detected initial access
Go to b) for Scenario 1.2: Detected lateral movement
Go to c) for Scenario 1.3:Detected Data Exfiltration & Scenario 1.4: Detected a web application attack
To: a) Containment: Determine containment strategy
To: b) Containment: Determine full extent
To: c) Containment: Preliminary response
Use Case 1: Response on Detected Ongoing Attack - Analysis
Authors: Frank Fransen, Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu


SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Threat Intel Platform
Infrastructure modeling
Orchestration & Integration Engine
Security Monitoring Solutions
From: Analysis
Determine preliminary response to stop impact (e.g. stop data exfiltration - scenario 1.3)
To: Containment - Determine full extent
Prepare playbook for preliminary response
To: Playbook Execution
Use Case 1: Response on Detected Ongoing Attack – Containment: preliminary response
Authors: Frank Fransen
Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu


SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Threat Intel Platform
Infrastructure modeling
Orchestration & Integration Engine
Security Monitoring Solutions
Generate initial attack path
1. Current infrastructure model with attacker outside organisation
Map attack steps to IoCs
2. Most likely attack path for initial access
3. Collect IoCs based on initial attack path
4. Provide IoCs for initial attack path analysis
From:
Analysis
Containment: Preliminary response
Analyse initial attack path
Collect data to validate initial path analysis
Collect historical security event data regarding IoCs of initial attack paths
Orchestrator – Collect all data for containment
7. Overview of all affected assets and accounts
To:
Containment – Determine containment strategy
5. Request historical events related to IoCs
6. Security events related to IoCs
Query database with historical events for match with IoCs
Use Case 1: Response on Detected Ongoing Attack – Containment: Deter. Full Exent
Authors: Frank Fransen
Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu

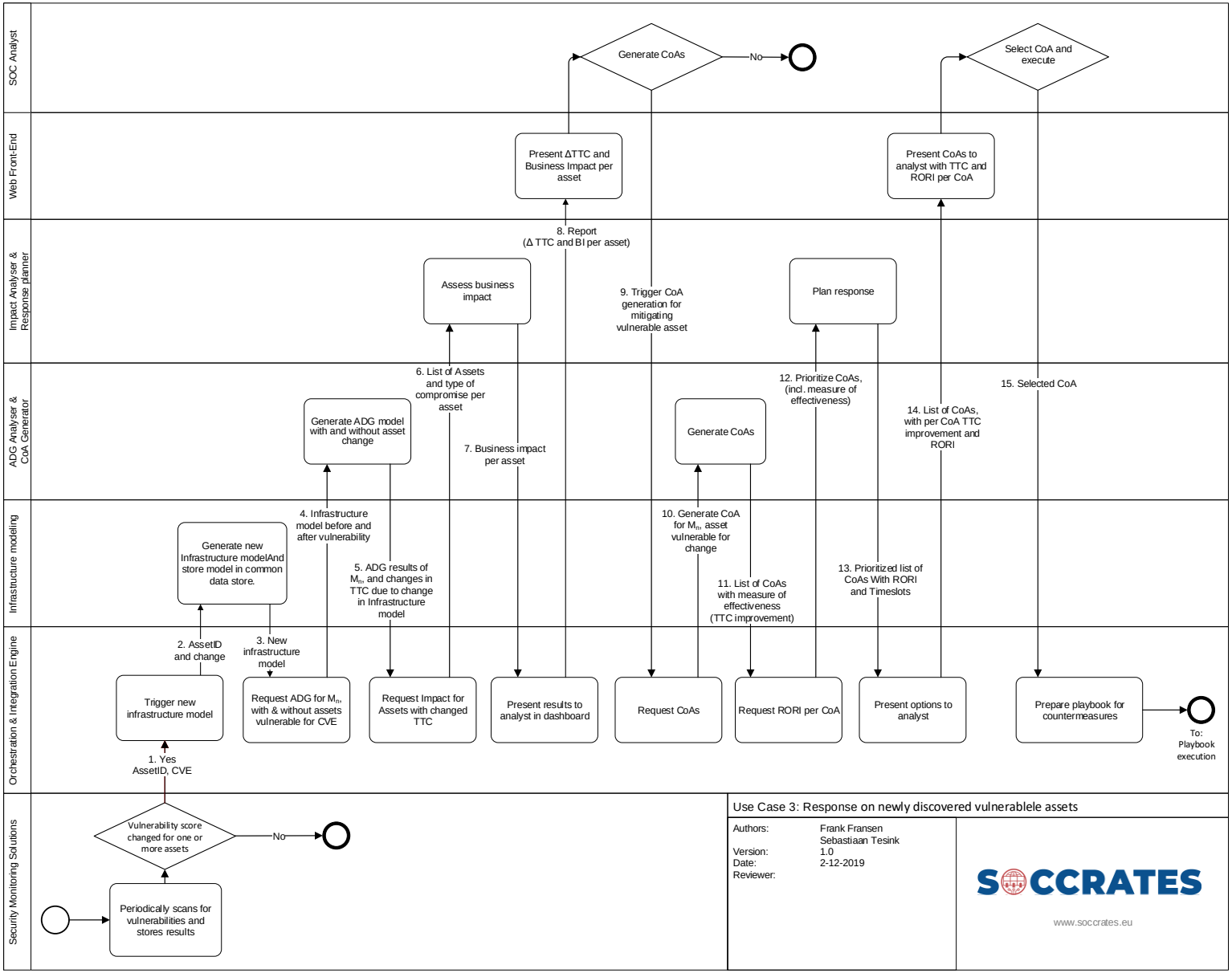

SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Threat Intel Platform
Infrastructure modeling
Orchestration & Integration Engine
Security Monitoring Solutions
Select CoA and execute
None
To: Exit
Dashboard – Present CoAs to analyst with TTC and RORI per CoA
Assess business impact of impacted systems
Response Planner – Generate Return On Response Investment per CoA
Generate CoAs
8. RORI per containment strategy
10. Selected Containment Strategy
3. List of impacted assets
4. Business impact per asset
5. Generate containment strategy
7. Prioritize CoAs, (incl. measure of effectiveness)
9. List of CoAs, with per CoA:
TTC
RORI
6. Containment strategies
From:
Analysis
Containment: Determine full extent
Single system affected?
2. No
Request Impact for Assets with changed TTC
Request CoAs (containment strategies)
Request RORI per CoA
Present CoAs to analyst
Determine containment strategy for single system (e.g. scenario 1.1)
Prepare playbook for countermeasures
To: Playbook Execution
1. Yes
Use Case 1: Response on Detected Ongoing Attack – Containment: Determine strategy
Authors: Frank Fransen, Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu

Annex B – Swimlane diagram UC2

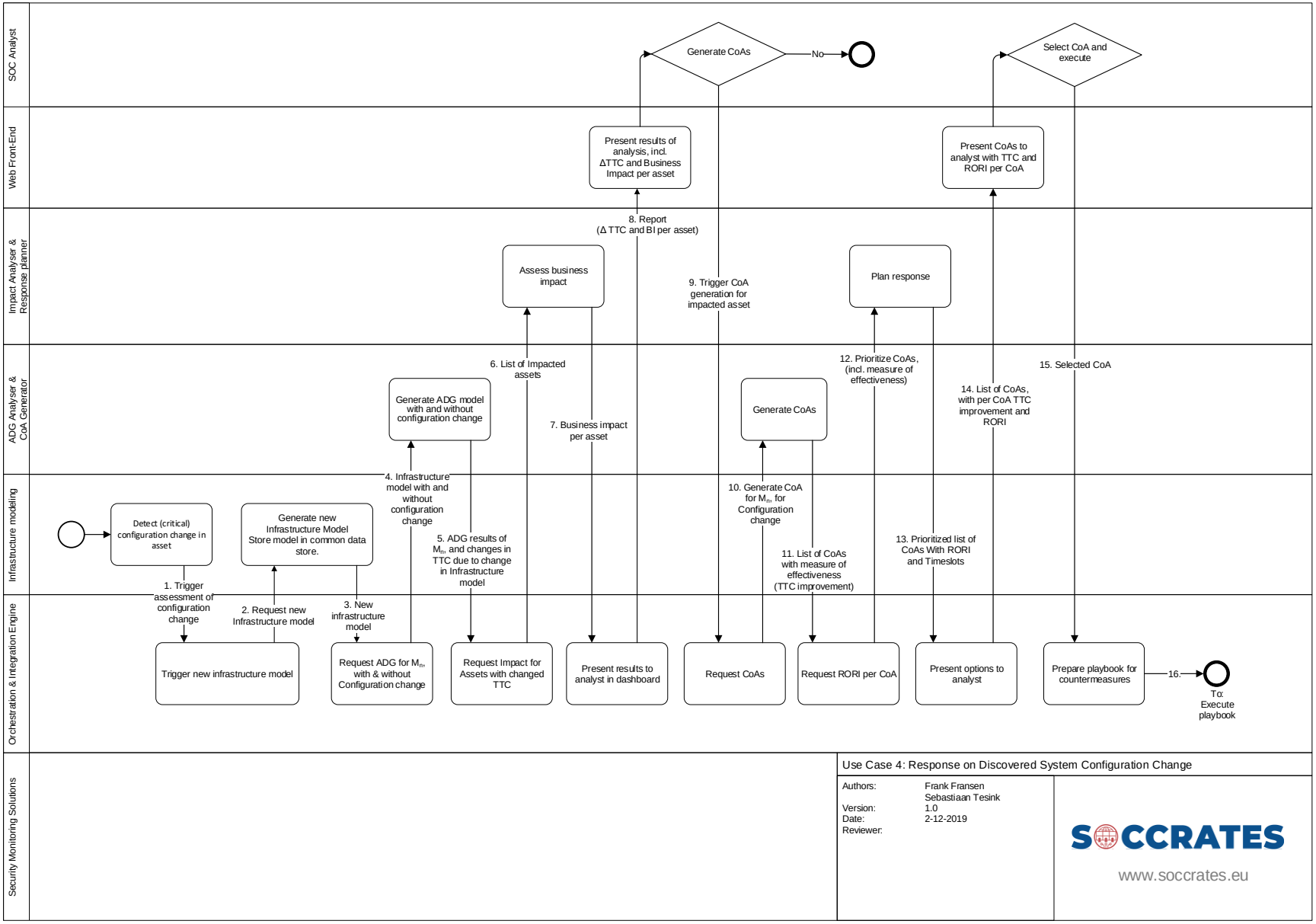


Classification level: Public

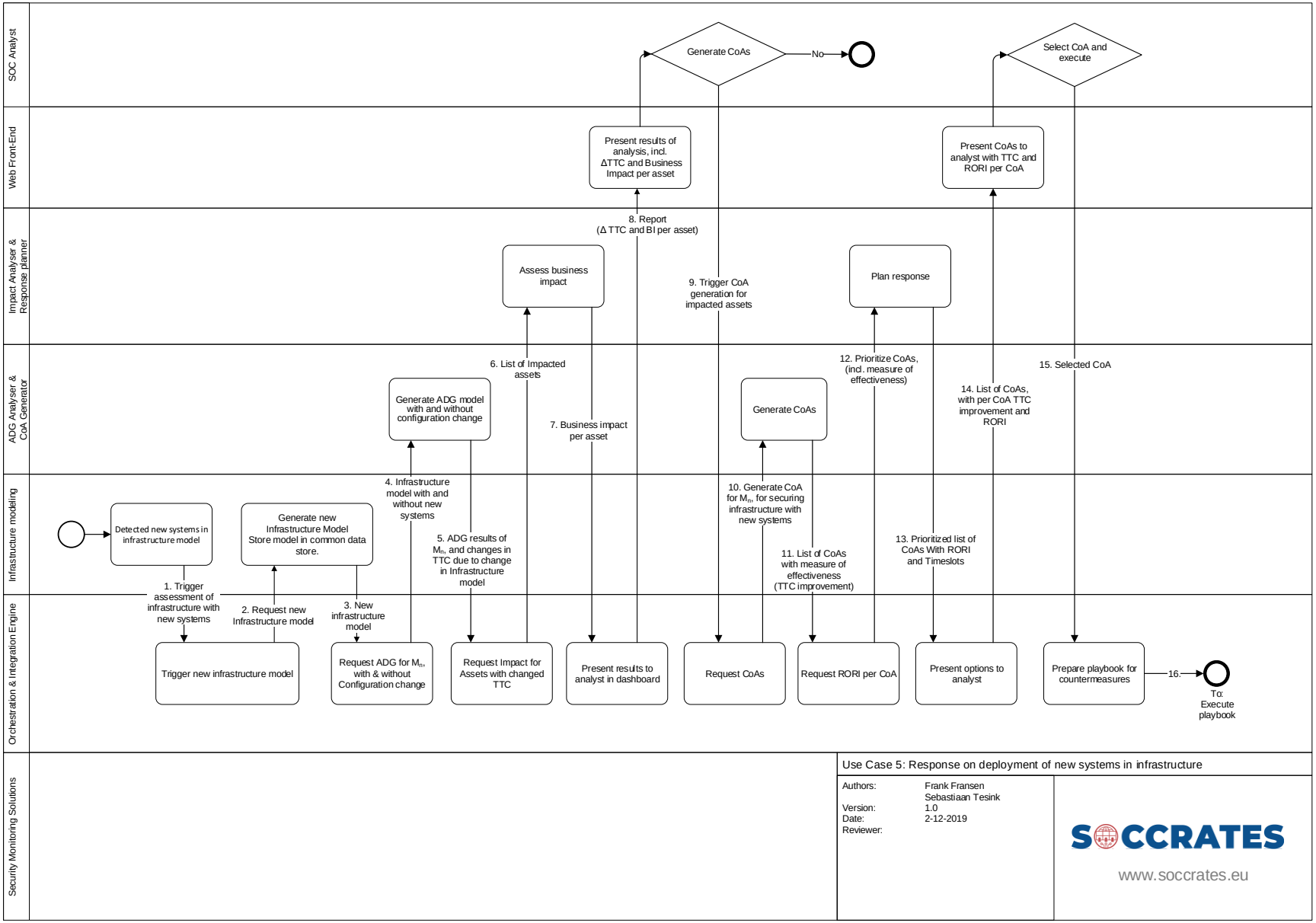
Annex C – Swimlane diagram UC3


SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Infrastructure modeling
Orchestraton & Integration Engine
Security Monitoring Solutions
Generate CoAs
No
Select CoA and execute
Present ΔTTC and Business Impact per asset
Present CoAs to analyst with TTC and RORI per CoA
8. Report (Δ TTC and BI per asset)
Assess business impact
9. Trigger CoA generation for mitigating vulnerable asset
Plan response
6. List of Assets and type of compromise per asset
12. Prioritize CoAs, (incl. measure of effectiveness)
15. Selected CoA
Generate ADG model with and without asset change
7. Business impact per asset
Generate CoAs
14. List of CoAs, with per CoA TTC improvement and RORI
4. Infrastructure model before and after vulnerability
10. Generate CoA for M_n, asset vulnerable for change
Generate new Infrastructure modelAnd store model in common data store.
5. ADG results of M_n, and changes in TTC due to change in Infrastructure model
11. List of CoAs with measure of effectiveness (TTC improvement)
13. Prioritized list of CoAs With RORI and Timeslots
2. AssetID and change
3. New infrastructure model
Trigger new infrastructure model
Request ADG for M_n, with & without assets vulnerable for CVE
Request Impact for Assets with changed TTC
Present results to analyst in dashboard
Request CoAs
Request RORI per CoA
Present options to analyst
Prepare playbook for countermeasures
To: Playbook execution
1. Yes AssetID, CVE
Vulnerability score changed for one or more assets
No
Periodically scans for vulnerabilities and stores results
Use Case 3: Response on newly discovered vulnerablele assets
Authors: Frank Fransen, Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu

Annex D – Swimlane diagram UC4


SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Infrastructure modeling
Orchestraton & Integration Engine
Security Monitoring Solutions
Generate CoAs
No
Select CoA and execute
Present results of analysis, incl. ΔTTC and Business Impact per asset
Present CoAs to analyst with TTC and RORI per CoA
8. Report (Δ TTC and BI per asset)
Assess business impact
9. Trigger CoA generation for impacted asset
Plan response
6. List of Impacted assets
12. Prioritize CoAs, (incl. measure of effectiveness)
15. Selected CoA
Generate ADG model with and without configuration change
7. Business impact per asset
Generate CoAs
14. List of CoAs, with per CoA TTC improvement and RORI
4. Infrastructure model with and without configuration change
10. Generate CoA for M_n, for Configuration change
Detect (critical) configuration change in asset
Generate new Infrastructure Model Store model in common data store.
5. ADG results of M_n, and changes in TTC due to change in Infrastructure model
11. List of CoAs with measure of effectiveness (TTC improvement)
13. Prioritized list of CoAs With RORI and Timeslots
1. Trigger assessment of configuration change
2. Request new Infrastructure model
3. New infrastructure model
Trigger new infrastructure model
Request ADG for M_n, with & without Configuration change
Request Impact for Assets with changed TTC
Present results to analyst in dashboard
Request CoAs
Request RORI per CoA
Present options to analyst
Prepare playbook for countermeasures
16.
To: Execute playbook
Use Case 4: Response on Discovered System Configuration Change
Authors: Frank Fransen
Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu

Annex E – Swimlane diagram UC5


SOC Analyst
Web Front-End
Impact Analyser & Response planner
ADG Analyser & CoA Generator
Infrastructure modeling
Orchestraton & Integration Engine
Security Monitoring Solutions
Generate CoAs
No
Select CoA and execute
Present results of analysis, incl. ΔTTC and Business Impact per asset
Present CoAs to analyst with TTC and RORI per CoA
8. Report (Δ TTC and BI per asset)
Assess business impact
9. Trigger CoA generation for impacted assets
Plan response
6. List of Impacted assets
12. Prioritize CoAs, (incl. measure of effectiveness)
15. Selected CoA
Generate ADG model with and without configuration change
7. Business impact per asset
Generate CoAs
14. List of CoAs, with per CoA TTC improvement and RORI
4. Infrastructure model with and without new systems
10. Generate CoA for Mn, for securing infrastructure with new systems
Detected new systems in infrastructure model
Generate new Infrastructure Model Store model in common data store.
5. ADG results of Mn, and changes in TTC due to change in Infrastructure model
11. List of CoAs with measure of effectiveness (TTC improvement)
13. Prioritized list of CoAs With RORI and Timeslots
1. Trigger assessment of infrastructure with new systems
2. Request new Infrastructure model
3. New infrastructure model
Trigger new infrastructure model
Request ADG for Mn, with & without Configuration change
Request Impact for Assets with changed TTC
Present results to analyst in dashboard
Request CoAs
Request RORI per CoA
Present options to analyst
Prepare playbook for countermeasures
16.
To: Execute playbook
Use Case 5: Response on deployment of new systems in infrastructure
Authors: Frank Fransen
Sebastiaan Tesink
Version: 1.0
Date: 2-12-2019
Reviewer:
SOCCRATES
www.soccrates.eu