SOCCRATES: Automated Security Decision Support for SOCs and CSIRTs

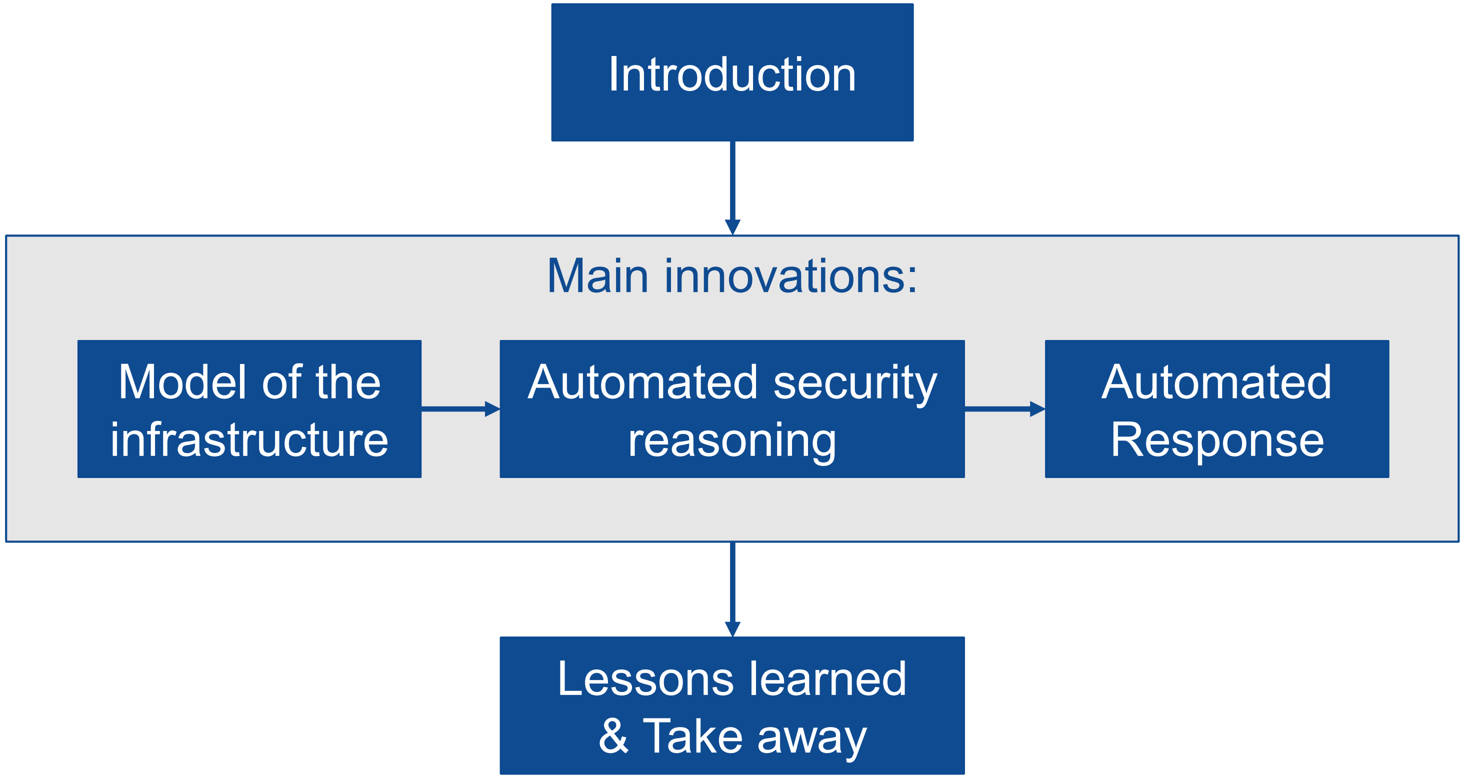
Martin Eian (mnemonic, NO)

Frank Fransen (TNO, NL)

TLP: CLEAR

OUTLINE

SOCCRATES



Introduction

Main innovations:

Model of the infrastructure

Automated security reasoning

Automated Response

Lessons learned & Take away

June 5th, 2023

SOCCRATES

SOC & **C**SIRT **R**esponse to **A**ttacks & **T**hreats based on attack defence graphs **E**valuation **S**ystems

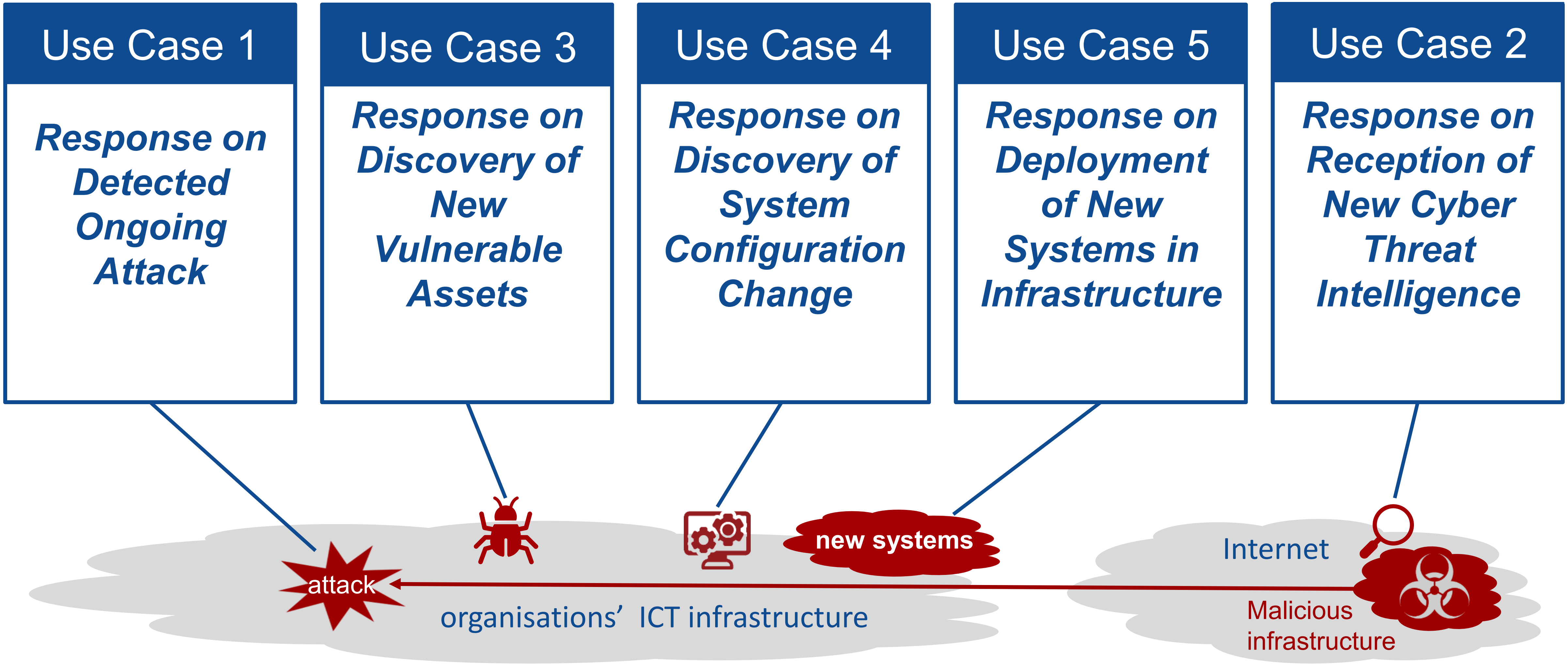
Project details

Call type	Innovation Action
Call ID/Topic	H2020 SU-ICT-01-2018
Duration	Sept. 2019 – Oct. 2022
EU funding	€ 5M
Coordinator	TNO, The Netherlands
Website	www.soccrates.eu

PROJECT OBJECTIVE

Develop and implement a security automation and decision support platform that enhances the effectiveness of SOC and CSIRT operations.

SOCCRATES Use Cases



Use Case 1

Response on Detected Ongoing Attack

Use Case 3

Response on Discovery of New Vulnerable Assets

Use Case 4

Response on Discovery of System Configuration Change

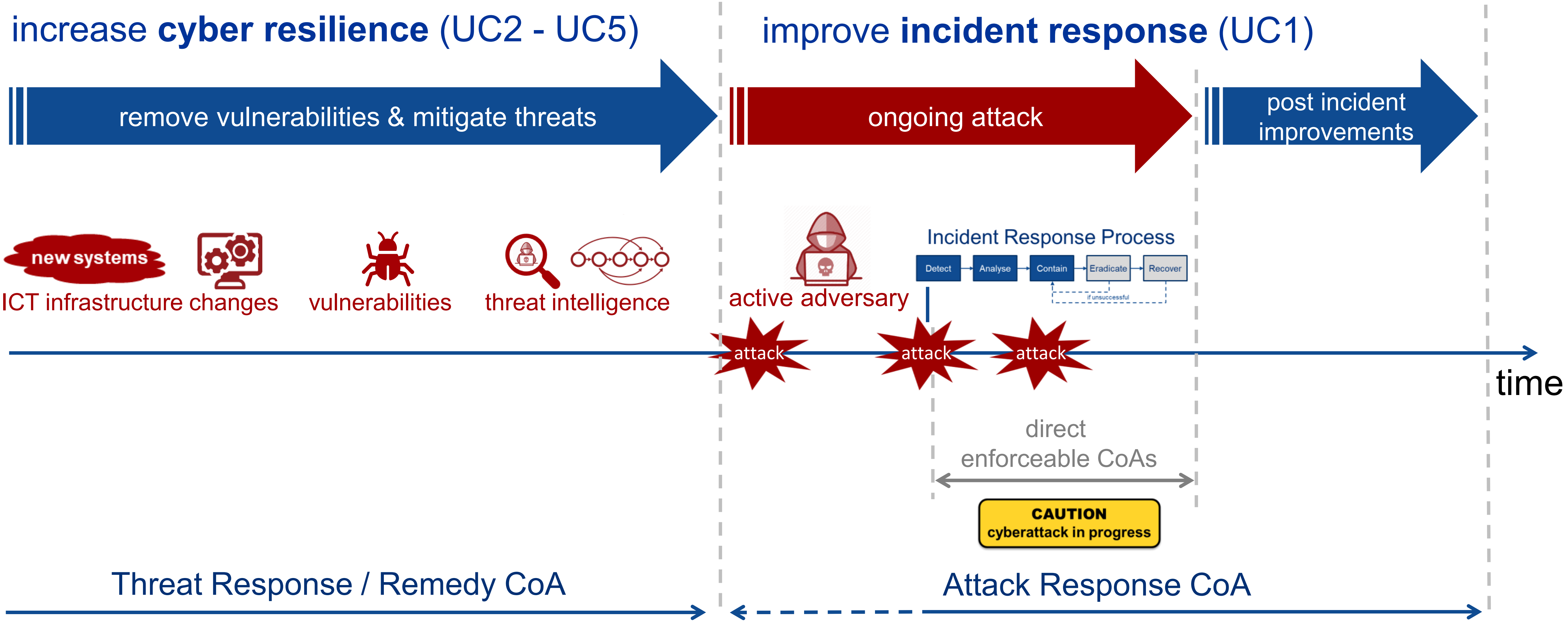
Use Case 5

Response on Deployment of New Systems in Infrastructure

Use Case 2

Response on Reception of New Cyber Threat Intelligence

SOCCRATES Use Cases – different view



increase **cyber resilience** (UC2 - UC5)

improve **incident response** (UC1)

remove vulnerabilities & mitigate threats

ongoing attack

post incident improvements

new systems

ICT infrastructure changes

vulnerabilities

threat intelligence

active adversary

Incident Response Process

Detect → Analyse → Contain → Eradicate → Recover

attack

attack

attack

time

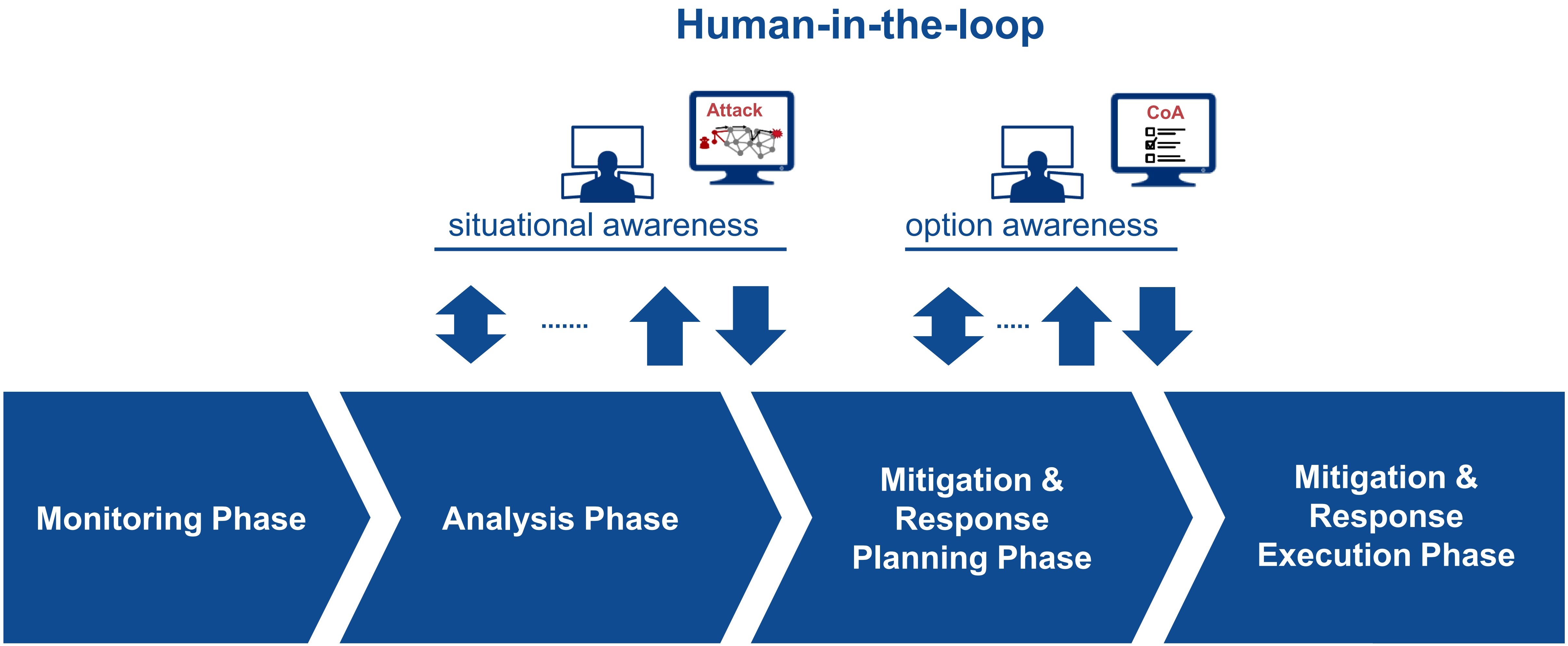
direct enforceable CoAs

CAUTION
cyberattack in progress

Threat Response / Remedy CoA

Attack Response CoA

SOCCRATES Use Cases – General Flow



Human-in-the-loop

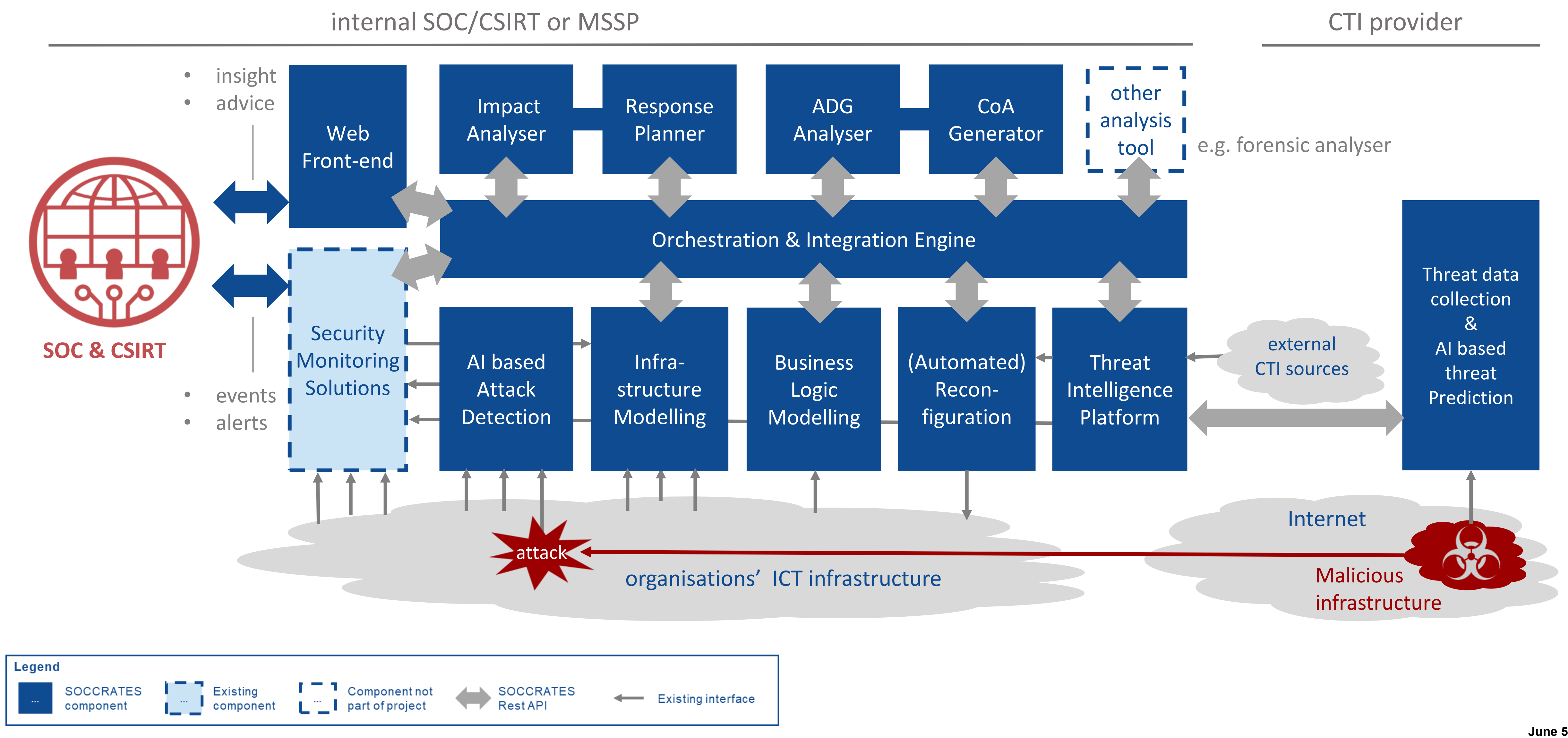
Monitoring Phase

Analysis Phase

Mitigation & Response Planning Phase

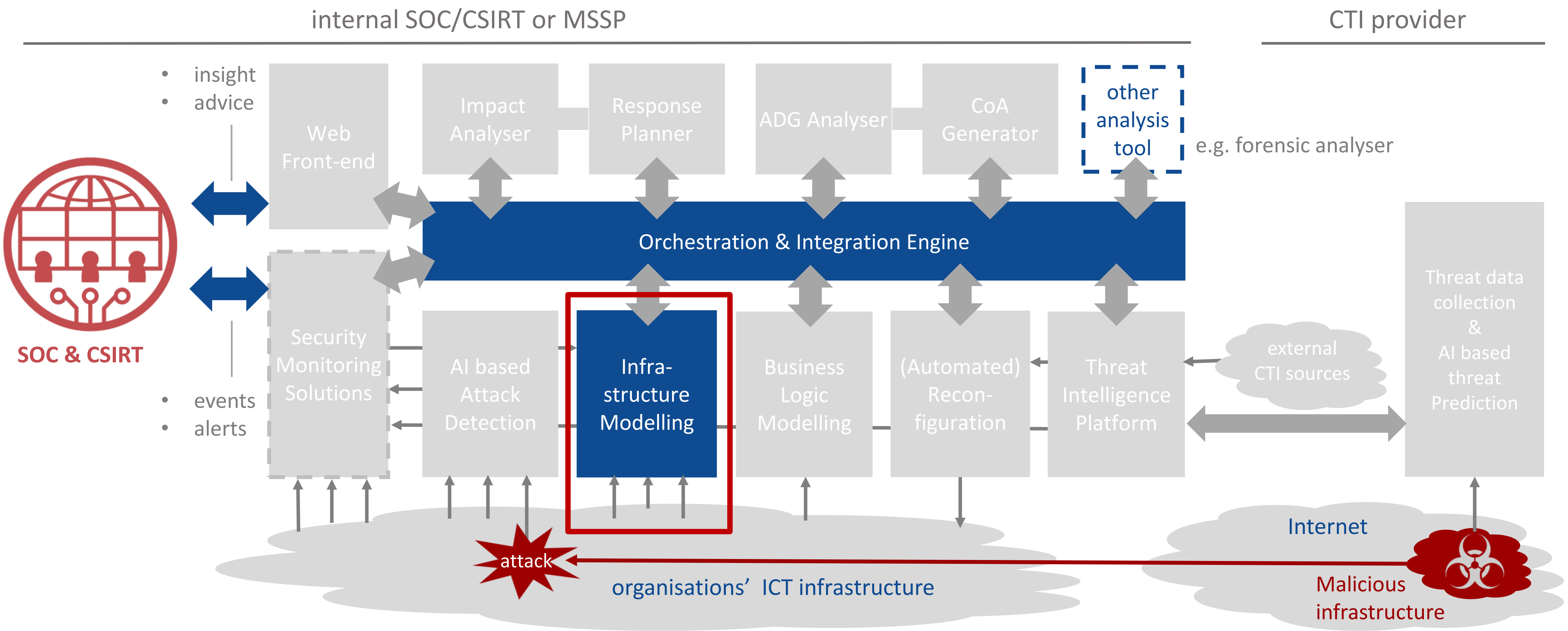
Mitigation & Response Execution Phase

SOCCRATES PLATFORM



June 5th, 2023

MAIN INNOVATIONS



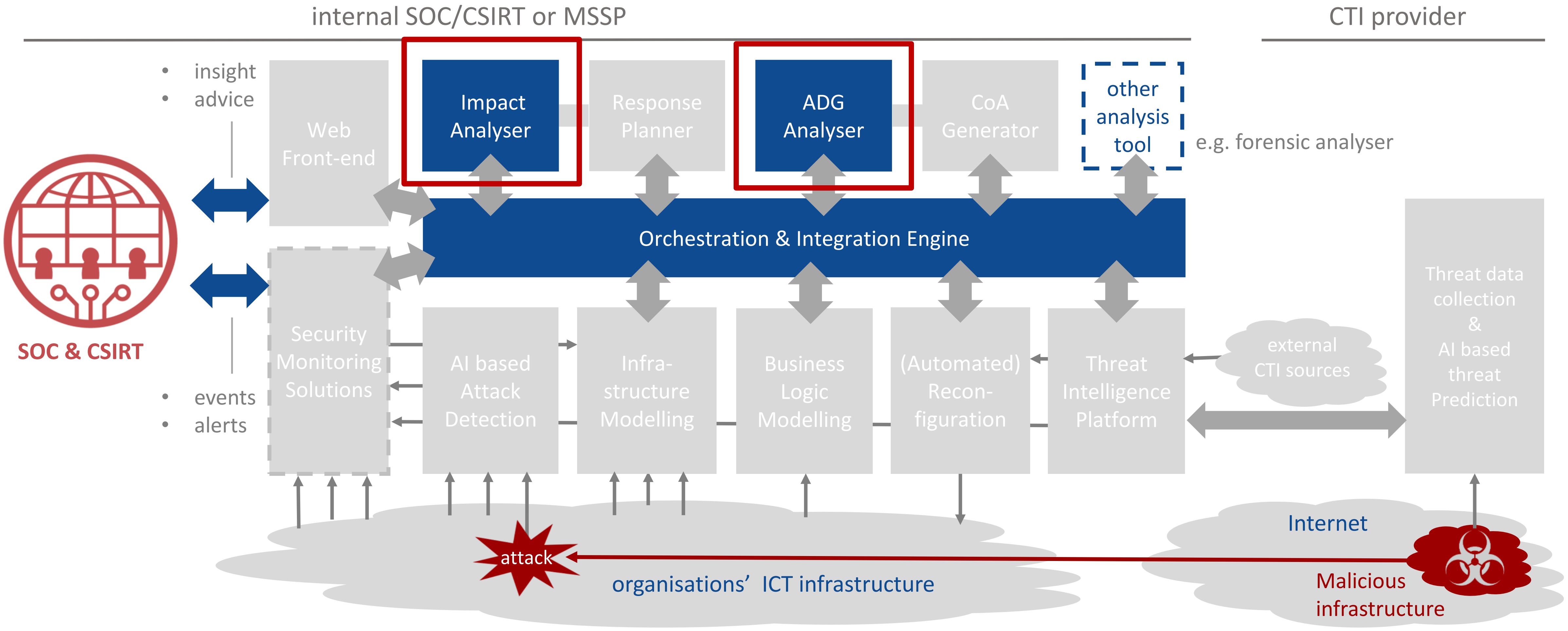
internal SOC/CSIRT or MSSP
CTI provider
insight
advice
events
alerts
SOC & CSIRT
Web Front-end
Security Monitoring Solutions
Impact Analyser
Response Planner
ADG Analyser
CoA Generator
other analysis tool
e.g. forensic analyser
Orchestration & Integration Engine
AI based Attack Detection
Infra-structure Modelling
Business Logic Modelling
(Automated) Recon-figuration
Threat Intelligence Platform
external CTI sources
Threat data collection & AI based threat Prediction
attack
organisations' ICT infrastructure
Internet
Malicious infrastructure

Actual machine-readable model of the infrastructure

June 5th, 2023

MAIN INNOVATIONS

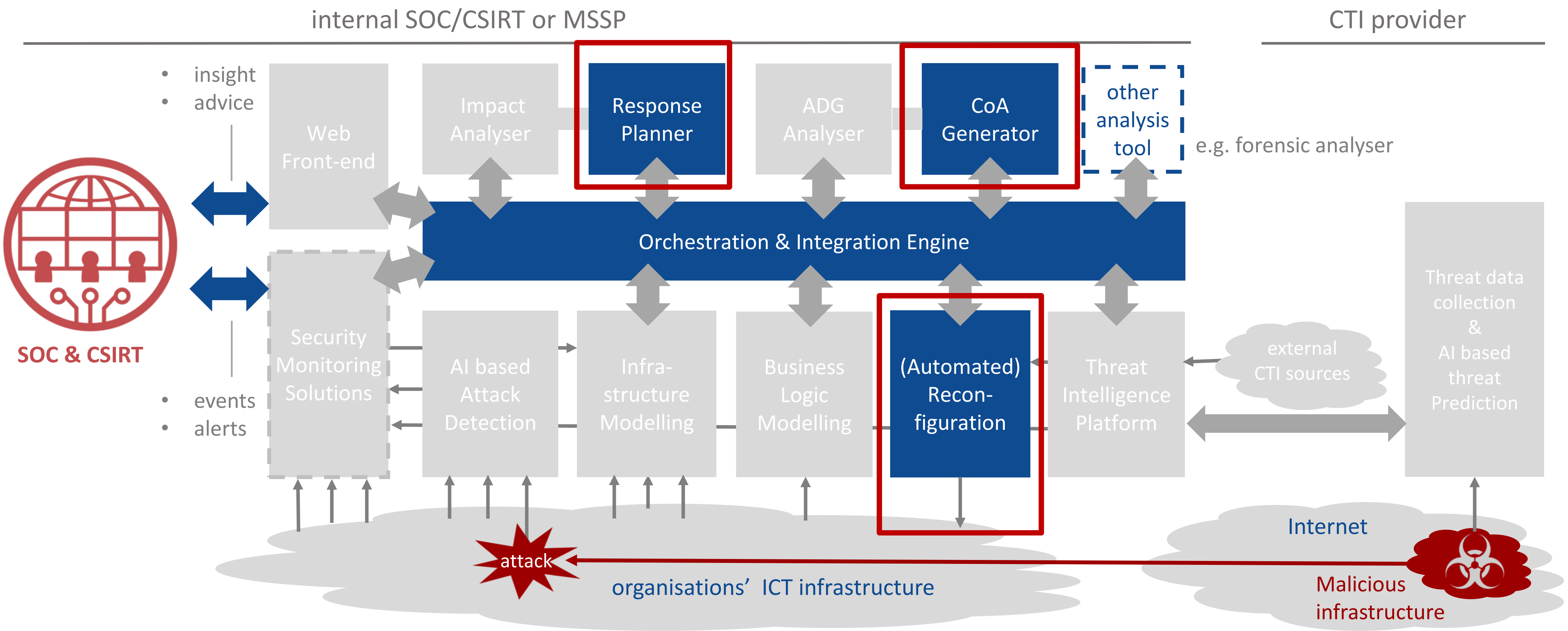
SOCCRATES



internal SOC/CSIRT or MSSP
CTI provider
insight
advice
events
alerts
SOC & CSIRT
Web Front-end
Impact Analyser
Response Planner
ADG Analyser
CoA Generator
other analysis tool
e.g. forensic analyser
Orchestration & Integration Engine
Security Monitoring Solutions
AI based Attack Detection
Infra-structure Modelling
Business Logic Modelling
(Automated) Recon-figuration
Threat Intelligence Platform
external CTI sources
Threat data collection & AI based threat Prediction
Internet
attack
organisations' ICT infrastructure
Malicious infrastructure

Automated security reasoning (Attack Simulation & Real-time Business Impact Assessment)

MAIN INNOVATIONS

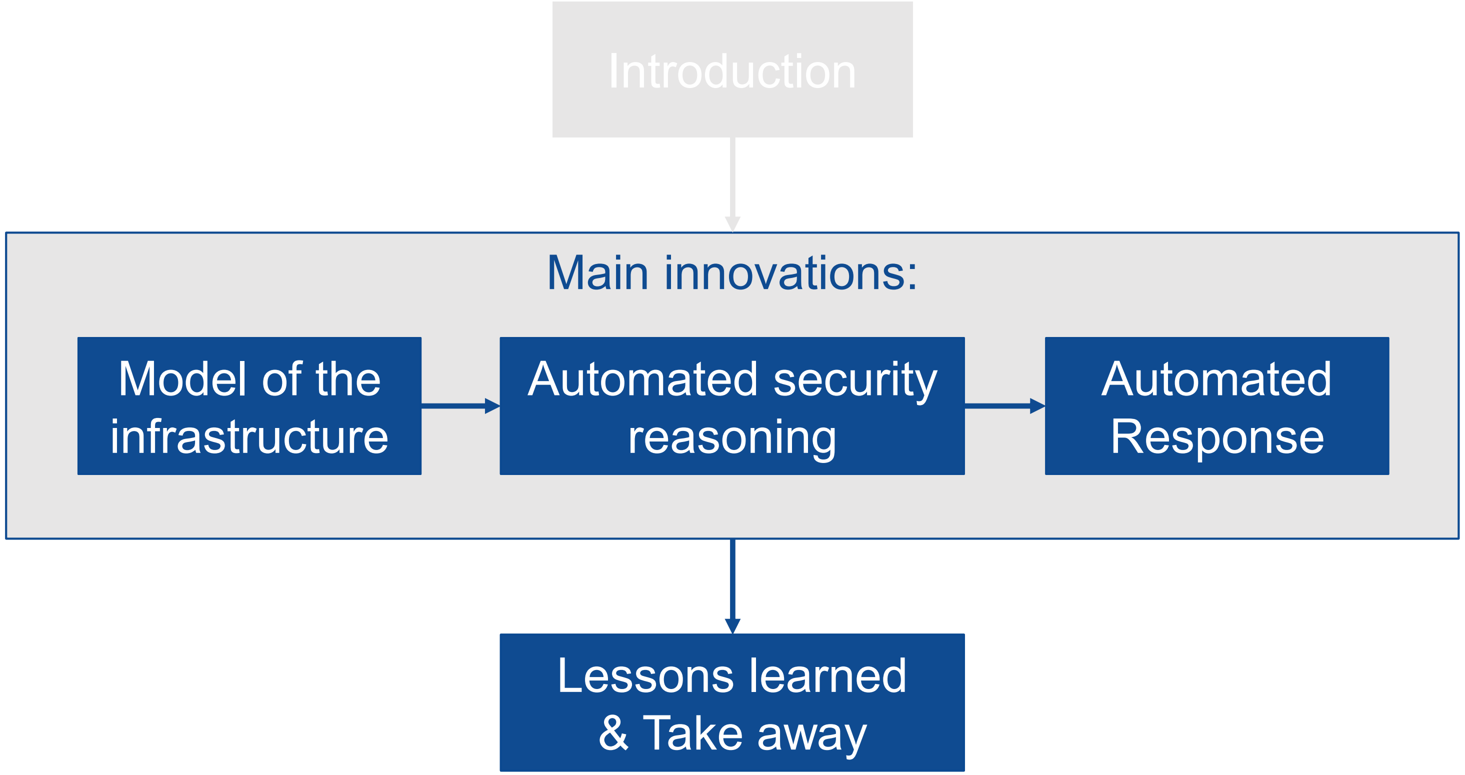


internal SOC/CSIRT or MSSP
CTI provider
insight
advice
events
alerts
SOC & CSIRT
Web Front-end
Security Monitoring Solutions
Impact Analyser
Response Planner
ADG Analyser
CoA Generator
other analysis tool
e.g. forensic analyser
Orchestration & Integration Engine
AI based Attack Detection
Infra-structure Modelling
Business Logic Modelling
(Automated) Reconfiguration
Threat Intelligence Platform
external CTI sources
Threat data collection & AI based threat Prediction
Internet
attack
organisations' ICT infrastructure
Malicious infrastructure

Automated generation, assessment and execution of response actions

OUTLINE

SOCCRATES



Introduction

Main innovations:

Model of the infrastructure

Automated security reasoning

Automated Response

Lessons learned & Take away

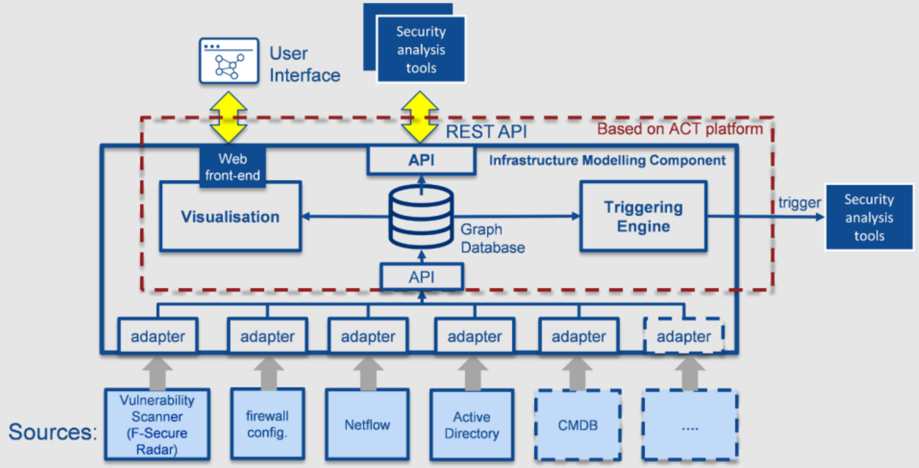
MODEL OF THE INFRASTRUCTURE

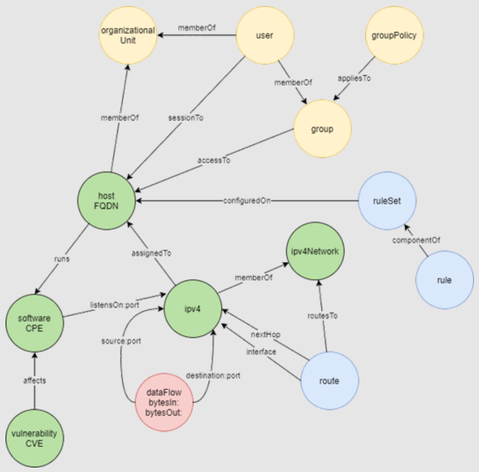
SOCCRATES

What we needed

- Machine readable model of the infrastructure
- Correlate multiple data sources
- Detect changes and trigger workflows

What we did





What we learned

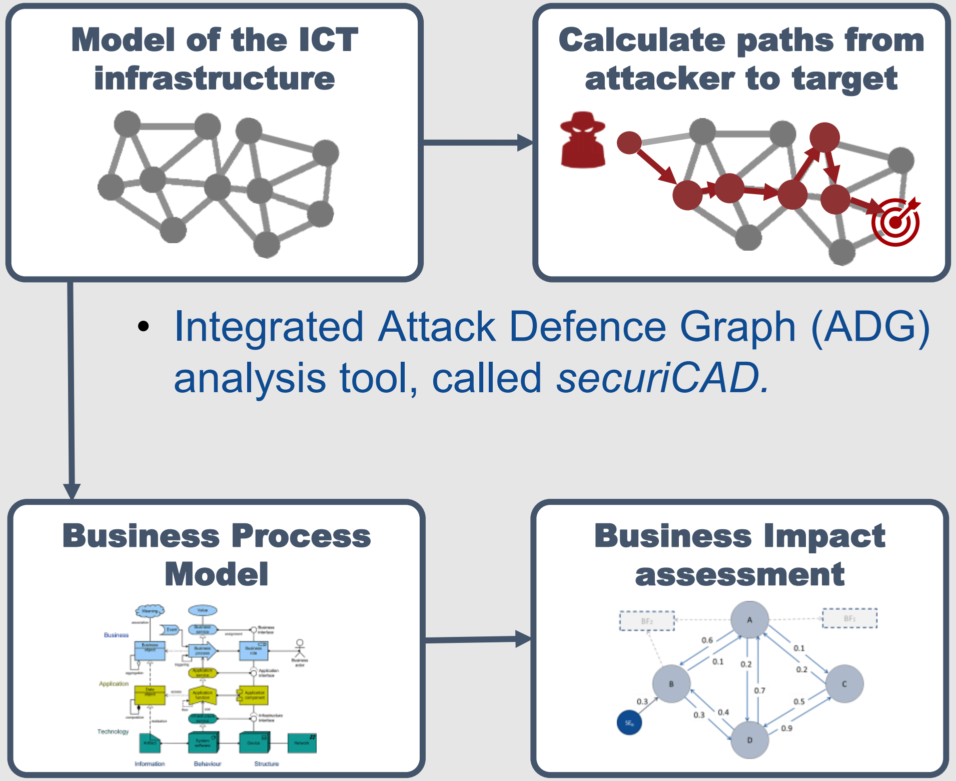
- Ability to detect changes useful to SOC analysts
- Correlation is a major challenge
- Scalability in operational environments

AUTOMATED SECURITY REASONING

What we needed

- Attack simulation on the infrastructure, triggered by security event
- Real-time business impact assessment on compromised asset, or response action

What we did


Model of the ICT infrastructure
Calculate paths from attacker to target
Business Process Model
Business Impact assessment

- Integrated Attack Defence Graph (ADG) analysis tool, called *securiCAD.*
- Combined *infrastructure model* and *business process model* to calculate impact on the business

What we learned

- Security Analysts: *"It provides unique contextual understanding"*
- Security Reasoning services need to be event-driven asynchronous
- Availability of *Business Process Models* not trivial

AUTOMATED RESPONSE

What we needed

- Generate Courses of Action (CoAs)
- Rank CoAs (effectiveness vs business impact)
- Execute CoAs

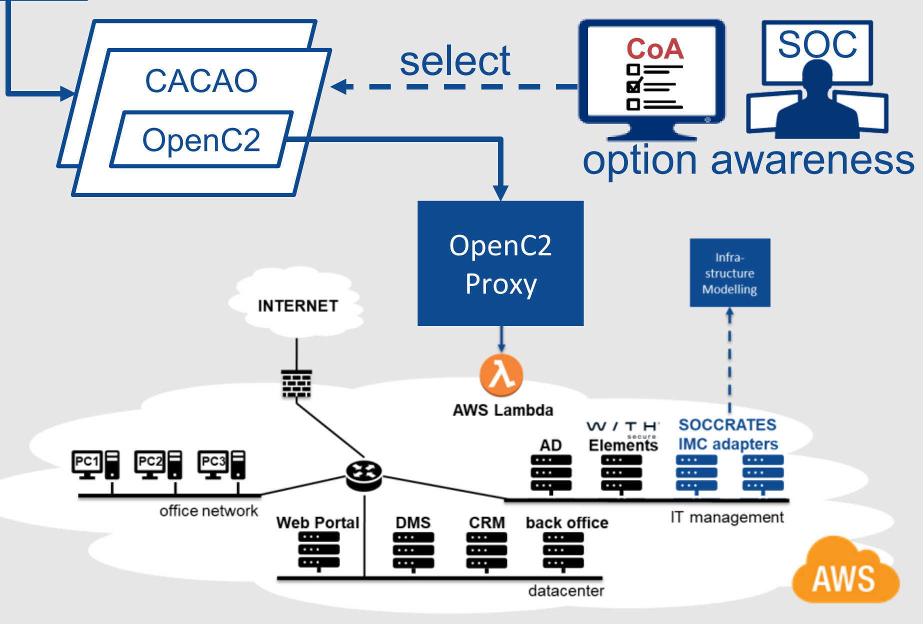
What we did

CoA Generator

CoA Generator uses ADG tool iteratively.
⇨ *Generic countermeasures*

Response Planner

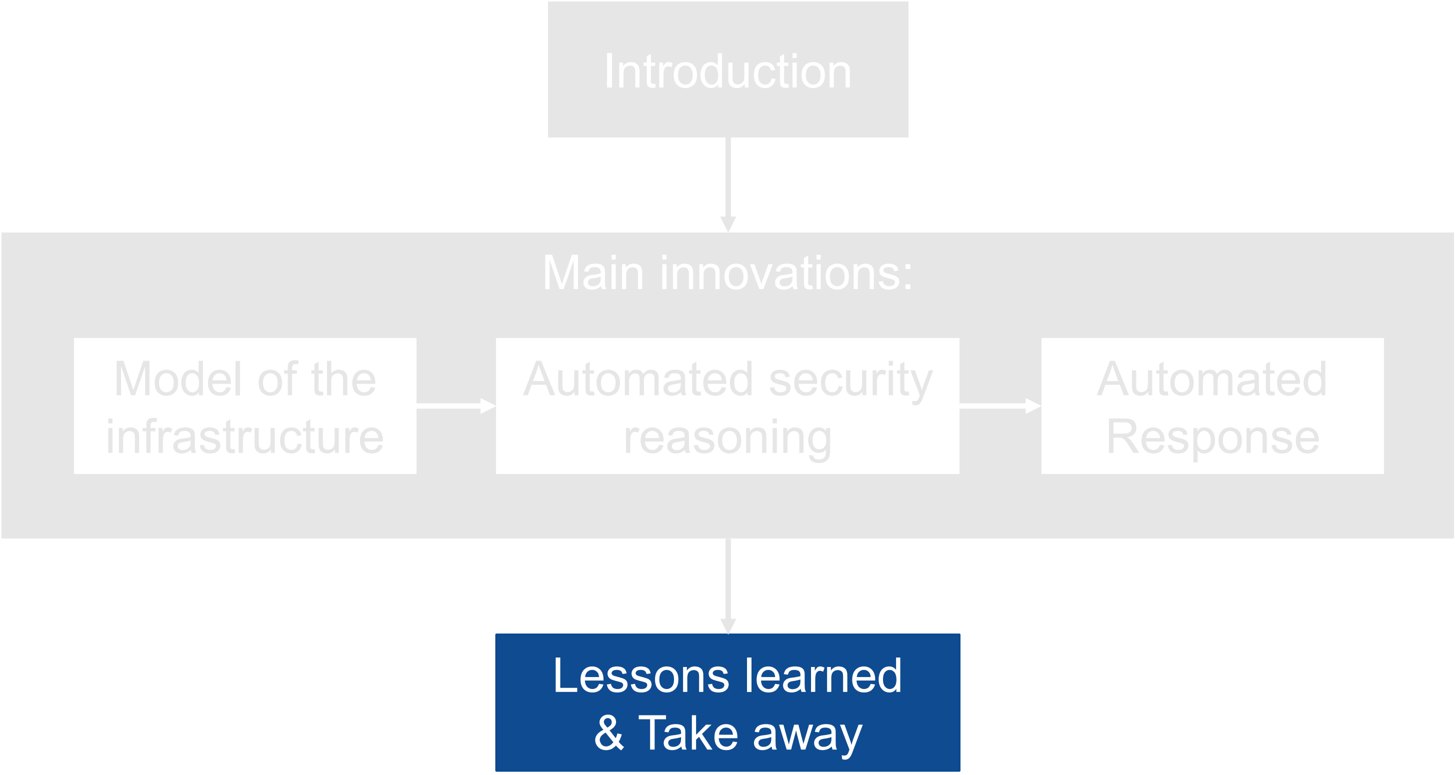
Response Planner.
⇨ *Direct enforceable CoAs*



What we learned

- Containment CoAs
- Analyst trust
- Importance of UI

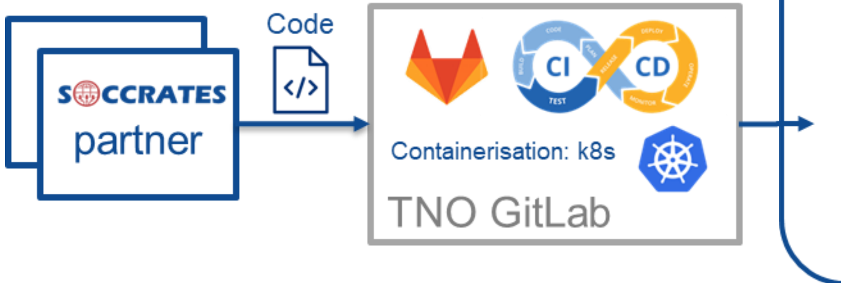
OUTLINE

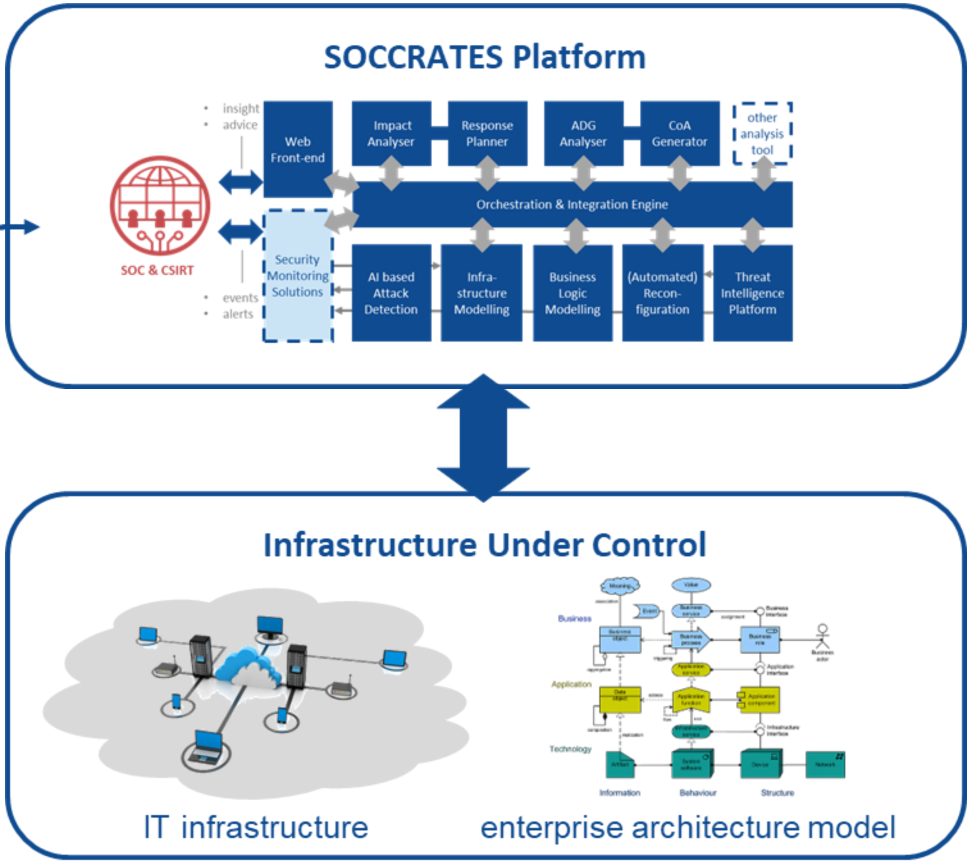

Introduction
Main innovations:
Model of the infrastructure
Automated security reasoning
Automated Response
Lessons learned & Take away

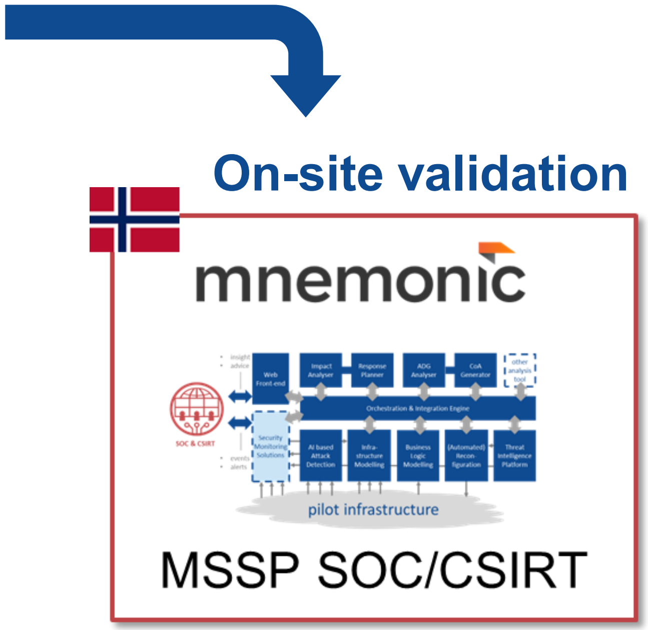
LESSONS LEARNED

What we have learned about running such a large ambitious project

1 Common software development platform & best practices







2 Start early with setting up a realistic test environment

- Include performance / stress testing capability

3 Performance tests, and Plan sufficient time for integration

LESSONS LEARNED

What we have learned about security automation for SOCs & CSIRTs

1

Unique contextual understanding → improve analyst decisions

- New vulnerabilities and infrastructure changes

2

Value of structured and predefined workflows

- Make analysts reflect on threats, events and effects

3

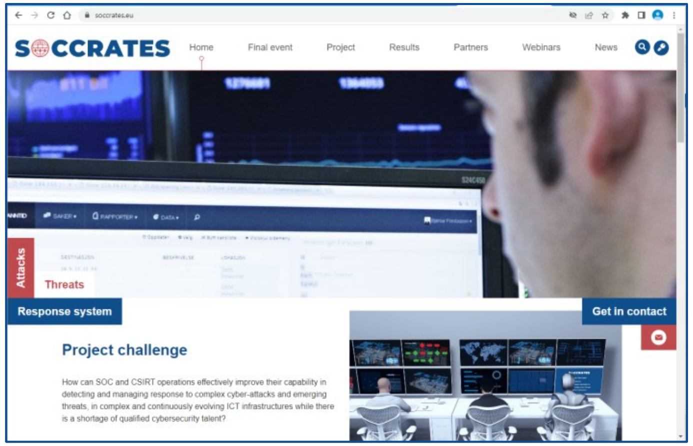
Analyst trust is paramount

- All recommendations must provide clear and visible evidence

TAKE AWAY

SOCCRATES

security automation & decision support can enhance the effectiveness of SOC & CSIRT operations



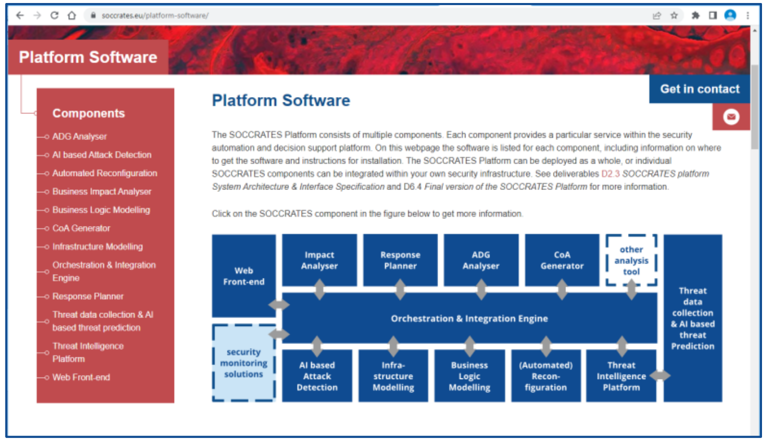
Project challenge

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?

SOCCRATES

Vision, Roadmap & Guidance for SOC

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


soccrates.eu/platform-software/
Platform Software
Get in contact
Components
ADG Analyser
AI based Attack Detection
Automated Reconfiguration
Business Impact Analyser
Business Logic Modelling
CoA Generator
Infrastructure Modelling
Orchestration & Integration Engine
Response Planner
Threat data collection & AI based threat prediction
Threat Intelligence Platform
Web Front-end
Web Front-end
Impact Analyser
Response Planner
ADG Analyser
CoA Generator
other analysis tool
Threat data collection & AI based threat Prediction
Orchestration & Integration Engine
security monitoring solutions
AI based Attack Detection
Infra-structure Modelling
Business Logic Modelling
(Automated) Recon-figuration
Threat Intelligence Platform

Platform Software

The SOCCRATES Platform consists of multiple components. Each component provides a particular service within the security automation and decision support platform. On this webpage the software is listed for each component, including information on where to get the software and instructions for installation. The SOCCRATES Platform can be deployed as a whole, or individual SOCCRATES components can be integrated within your own security infrastructure. See deliverables D2.3 *SOCCRATES platform System Architecture & Interface Specification* and D6.4 *Final version of the SOCCRATES Platform* for more information.

Click on the SOCCRATES component in the figure below to get more information.

www.soccrates.eu

mnemonic Securing your business. VATTENFALL WITH secure Atos Institut Mines-Télécom TELECOM SudParis Une école de l'IMT KTH VETENSKAP OCH KONST foreseeti TNO innovation for life AIT AUSTRIAN INSTITUTE OF TECHNOLOGY SHADOWSERVER

Q&A

mnemonic

Martin Eian

meian@mnemonic.no

TNO innovation for life

Frank Fransen

frank.fransen@tno.nl

www.soccrates.eu