SOCCRATES

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

Project details

Call type	Innovation Action
Call ID/Topic	SU-ICT-01-2018
Start date	September 1st, 2019
EU funding	€ 5M
Coordinator	TNO, The Netherlands

BACKGROUND

SOCCRATES

"But the cybersecurity community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in security investments, it has also brought new records in cyber-attacks of all kinds, data breaches, and information loss. From this perspective, one may argue that there is a market failure in cyber-security; that is, the increased defence levels and expenses cannot successfully reduce levels of cyberthreat exposure."

ENISA's Threat Landscape Report, 2017

- Increasing complexity and interdependency of ICT
- Increasing number and complexity of attacks
- Increasing use of automation by attackers – *response depends on human*
- Shortage of skilled security staff for Security Operation Centers (SOCs)

Challenge & Objectives

SOCCRATES

- **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?

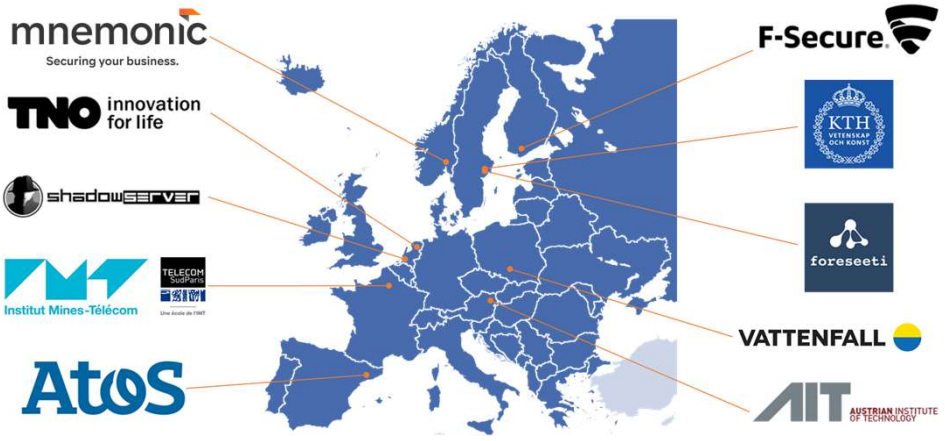
- **Main objective:**

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

10/12/2019

Consortium & Stakeholders

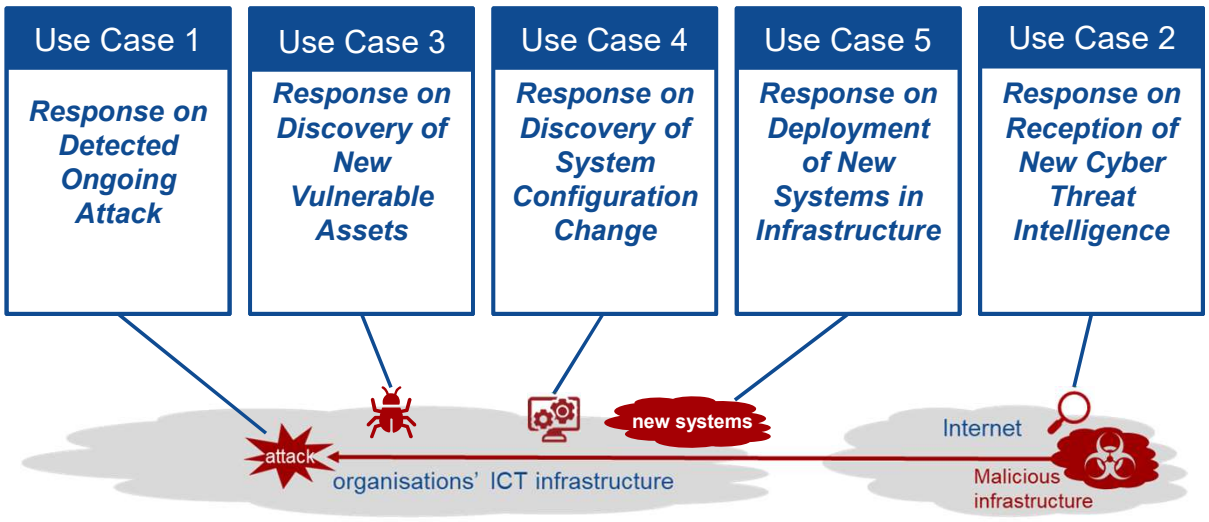
SOCCRATES



With support of: proximus telenor ABB EUROPOL Rabobank de volksbank kpn amadeus

10/12/2019

SOCCRATES Use Cases



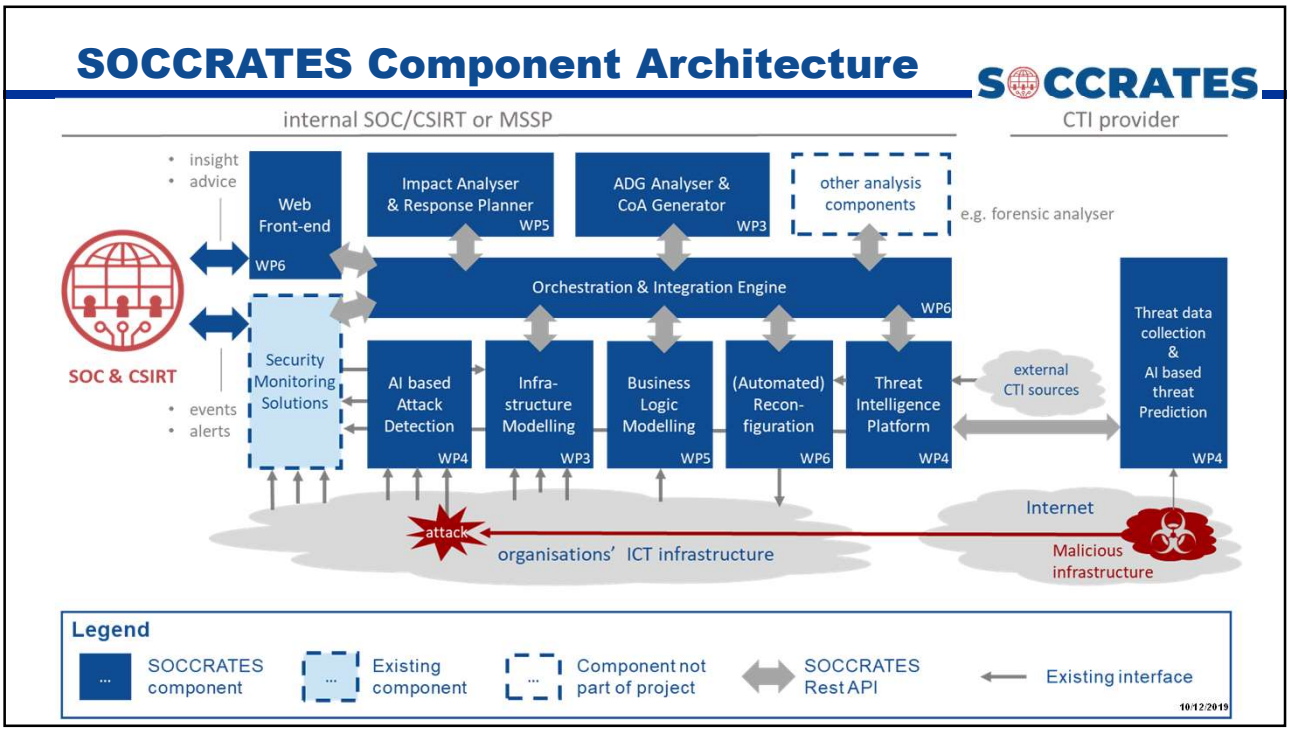
10/12/2019

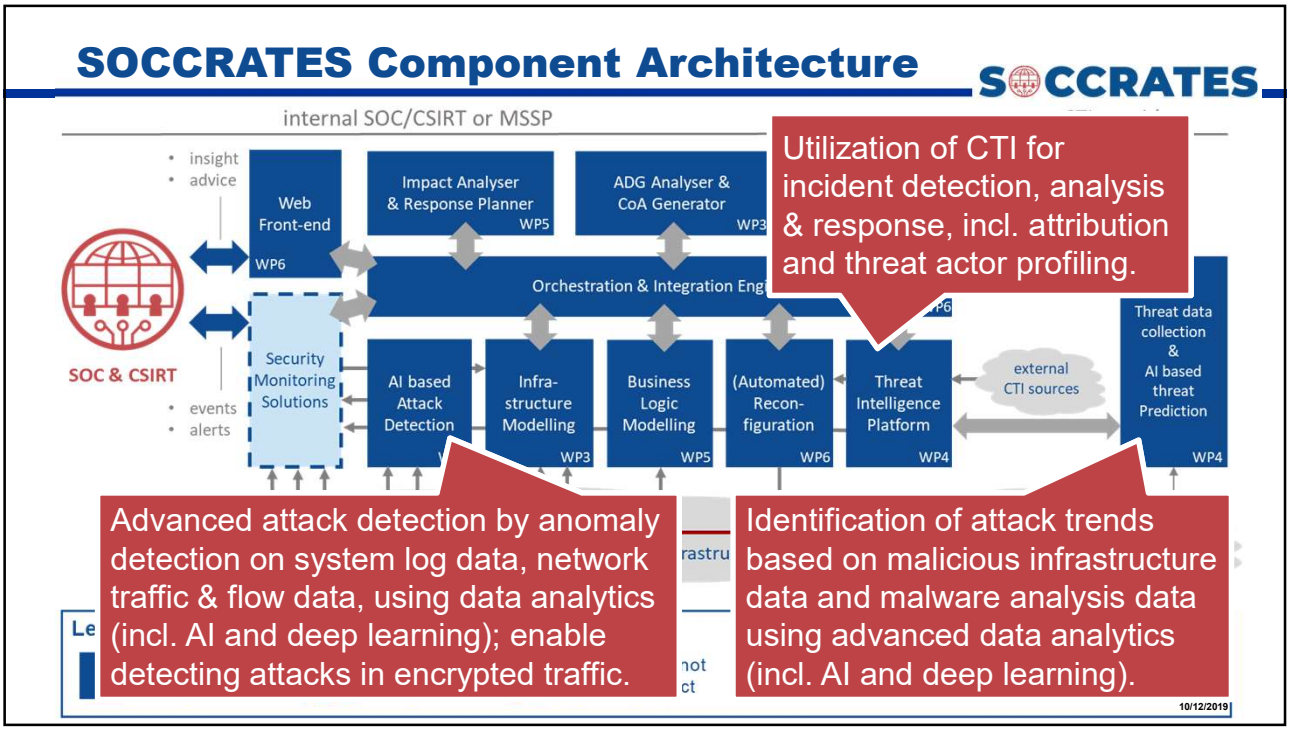
SOCCRATES Use Cases

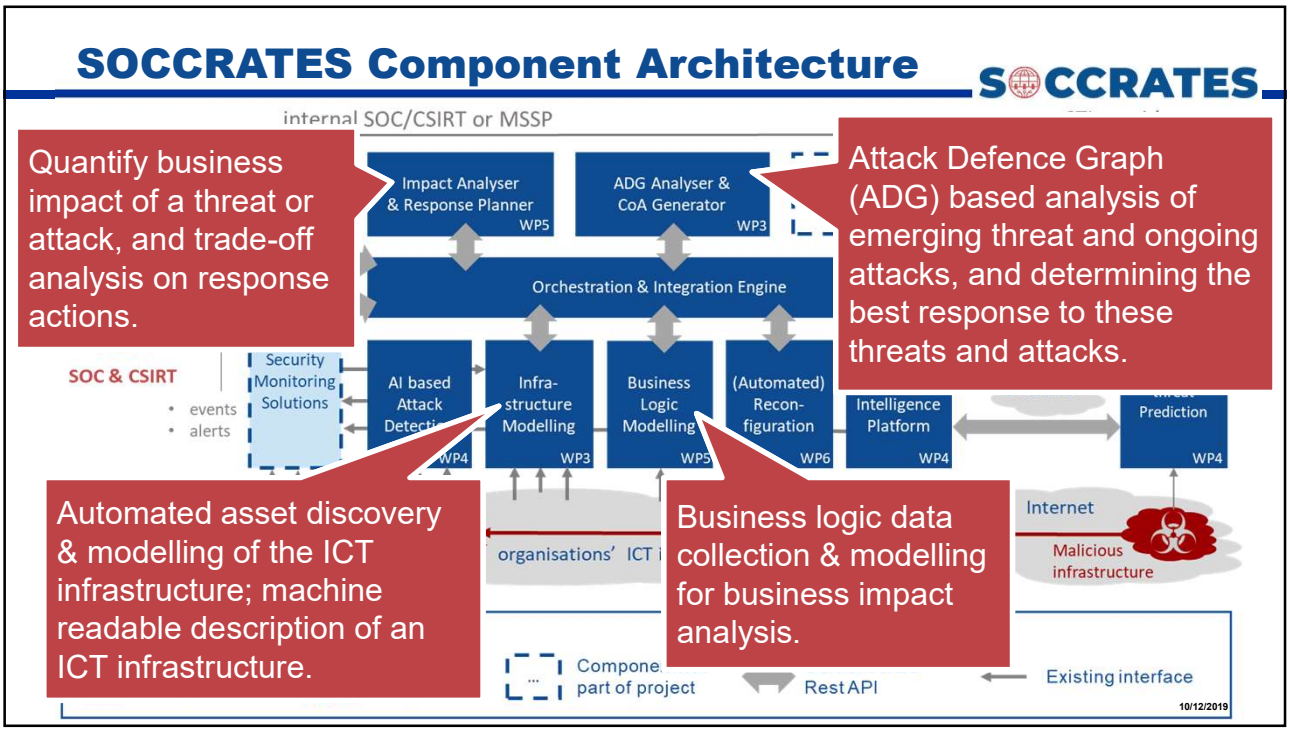
The platform enables security automation and decision support in **five use cases:**

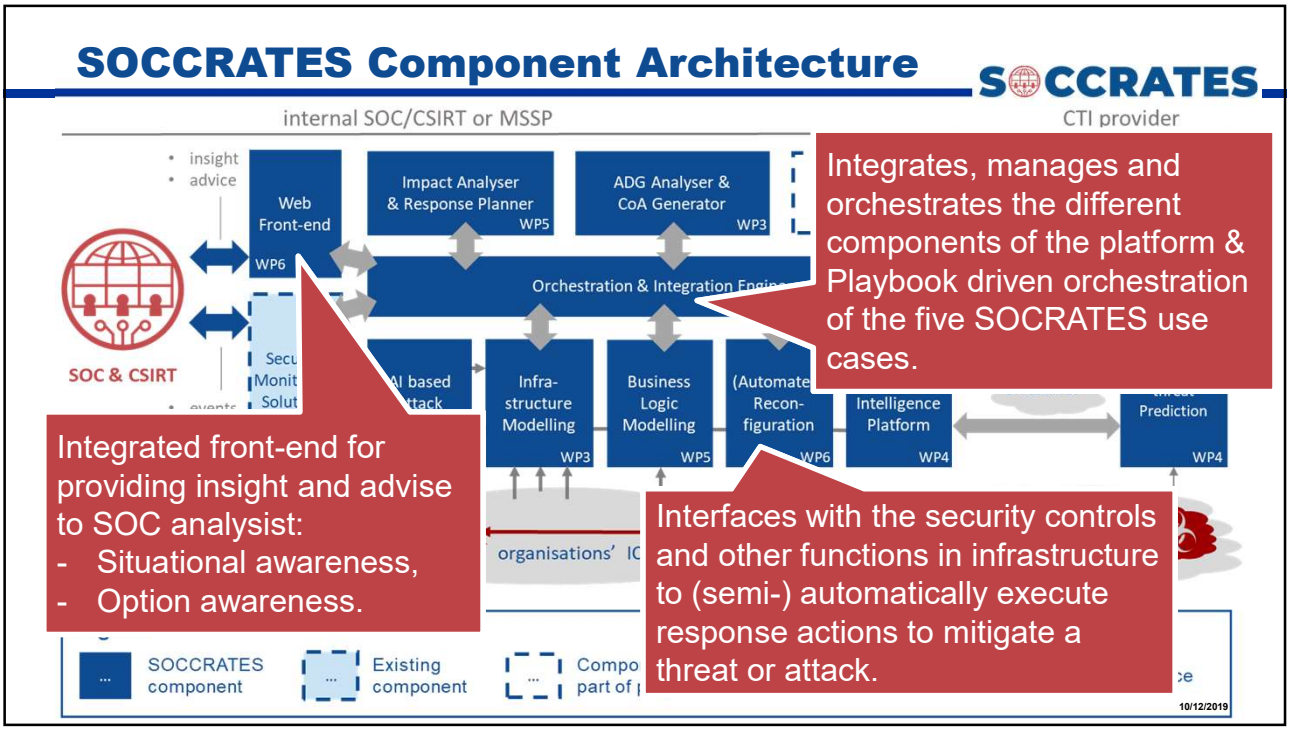
1. ***Response on Detected Ongoing Attack****;* Detection of ongoing attacks and automatically analyse the attack, automatically determine the best response, and initiate deployment of the selected response.
2. ***Response on Reception of New Cyber Threat Intelligence****;* Continuously collect new threat information, automatically analyse the potential business impact and determine best options for proactive mitigation.
3. ***Response on Discovery of New Vulnerable Assets****;* Automatically detect vulnerabilities on assets in the ICT infrastructure, assess if they enable new attack paths, determine and initiate mitigation actions.
4. ***Response on Discovery of 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.
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.

10/12/2019


SOCCRATES Component Architecture
SOCCRATES
internal SOC/CSIRT or MSSP
CTI provider
insight
advice
Web Front-end
WP6
Impact Analyser & Response Planner
WP5
ADG Analyser & CoA Generator
WP3
other analysis components
e.g. forensic analyser
Orchestration & Integration Engine
WP6
SOC & CSIRT
Security Monitoring Solutions
events
alerts
AI based Attack Detection
WP4
Infra-structure Modelling
WP3
Business Logic Modelling
WP5
(Automated) Recon-figuration
WP6
Threat Intelligence Platform
WP4
external CTI sources
Threat data collection & AI based threat Prediction
WP4
Internet
attack
organisations' ICT infrastructure
Malicious infrastructure
Legend
SOCCRATES component
Existing component
Component not part of project
SOCCRATES Rest API
Existing interface
10/12/2019


SOCCRATES Component Architecture
SOCCRATES
internal SOC/CSIRT or MSSP
Utilization of CTI for incident detection, analysis & response, incl. attribution and threat actor profiling.
insight
advice
Web Front-end
WP6
Impact Analyser & Response Planner
WP5
ADG Analyser & CoA Generator
WP3
Orchestration & Integration Eng
SOC & CSIRT
Security Monitoring Solutions
events
alerts
AI based Attack Detection
Infra-structure Modelling
WP3
Business Logic Modelling
WP5
(Automated) Recon-figuration
WP6
Threat Intelligence Platform
WP4
external CTI sources
Threat data collection & AI based threat Prediction
WP4
Advanced attack detection by anomaly detection on system log data, network traffic & flow data, using data analytics (incl. AI and deep learning); enable detecting attacks in encrypted traffic.
Identification of attack trends based on malicious infrastructure data and malware analysis data using advanced data analytics (incl. AI and deep learning).
10/12/2019


SOCCRATES Component Architecture
SOCCRATES
internal SOC/CSIRT or MSSP
Quantify business impact of a threat or attack, and trade-off analysis on response actions.
Impact Analyser & Response Planner WP5
ADG Analyser & CoA Generator WP3
Attack Defence Graph (ADG) based analysis of emerging threat and ongoing attacks, and determining the best response to these threats and attacks.
Orchestration & Integration Engine
SOC & CSIRT
Security Monitoring Solutions
events
alerts
AI based Attack Detecti
Infra-structure Modelling WP3
Business Logic Modelling WP5
(Automated) Recon-figuration WP6
Intelligence Platform WP4
Prediction WP4
Automated asset discovery & modelling of the ICT infrastructure; machine readable description of an ICT infrastructure.
Business logic data collection & modelling for business impact analysis.
Internet
Malicious infrastructure
organisations' ICT
Compone
part of project
Rest API
Existing interface
10/12/2019


SOCCRATES Component Architecture
SOCCRATES
internal SOC/CSIRT or MSSP
CTI provider
insight
advice
Web Front-end WP6
Impact Analyser & Response Planner WP5
ADG Analyser & CoA Generator WP3
Integrates, manages and orchestrates the different components of the platform & Playbook driven orchestration of the five SOCRATES use cases.
Orchestration & Integration Engine
SOC & CSIRT
Secu
Monit
Solut
AI based
Infra-structure Modelling WP3
Business Logic Modelling WP5
(Automate
Recon-figuration WP6
Intelligence Platform WP4
Prediction WP4
Integrated front-end for providing insight and advise to SOC analysist:
- Situational awareness,
- Option awareness.
Interfaces with the security controls and other functions in infrastructure to (semi-) automatically execute response actions to mitigate a threat or attack.
organisations' IC
SOCCRATES component
Existing component
Compo
part of
10/12/2019

SOCCRATES Pilots

Pilot	Description
Corporate SOC	The Vattenfall SOC, located in Poland, is the central security monitoring and response facility that services to all Vattenfall business units and IT. The pilot will focus on SOCCRATES use cases 1 to 5.
MSSP	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 pilot will focus on SOCCRATES use cases 1 to 5.
Threat Prediction	Shadow Server investigates malicious Internet activity, collecting and analysing large volumes of malware and related data, and shares data with stakeholders at no cost. The pilot will focus on SOCCRATES use case 2.

10/12/2019

Contacts

Project Coordinator:

TNO innovation for life

Reinder Wolthuis
+31 6 5191 33 79
reinder.wolthuis@tno.nl

Technical Coordinator:

TNO innovation for life

Frank Fransen
+31 6 53 72 49 00
frank.fransen@tno.nl

10/12/2019