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

# NG-SOC 2019

International Workshop on **Next Generation Security Operations Centers** to be held in conjunction with the 14th International Conference on Availability, Reliability and Security - **ARES 2019**

# TODAY'S AGENDA

SOCCRATES

| | | |
|---|---|---|
| **Session I**<br>*(Session Chair: Ewa Piatkowska)* | | |
| **15:20 – 15:40** | **The SOCCRATES Project: Motivation and Aims** | ***Reinder Wolthuis (TNO)*** |
| 15:40 – 16:00 | ACT: Cyber Threat Intelligence Platform | *Siri Bromander (Mnemonic)* |
| 16:00 – 16:20 | Threat modelling and attack simulations with MAL and securiCAD | *Erik Ringdahl (Foreseeti)* |
| 16:20 – 16:40 | Automated Response based on securiCAD recommendations | *Frank Fransen (TNO)* |
| Coffee Break | | |
| **Session II**<br>*(Session Chair: Reinder Wolthuis)* | | |
| 17:00 – 17:20 | Anomaly Detection (DNS Ninja & ABC tool) | *Irina Chiscop (TNO)* |
| 17:20 – 17:40 | Adversarial Machine Learning | *Ewa Piatkowska (AIT)* |
| 17:40 – 18:20 | Open Discussion: Future Challenges for SOCs | *Moderator: Paul Smith (AIT)* |
| 18:20 – 18:30 | Conclusions and Wrap Up | *Reinder Wolthuis (TNO)* |

# WHY SOCCRATES?

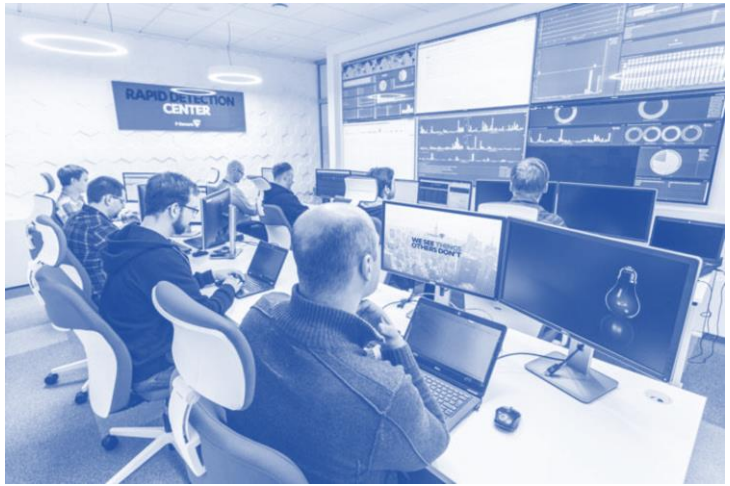
- Society is increasingly depending on reliable ICT.
- Despite heavy investments in their cyber defences, most organizations are unable to keep pace with the ongoing evolution of threats and attack methods due to
  - Increasing complexity and interdependency of ICT
  - Increasing number and complexity of attacks
  - The increasing use of automation by attackers and thus the decreasing available time to respond
  - The shortage of experienced security staff for Security Operation Centers (SOCs) to defend against attacks

- As it stands now, the gap between defenders and attackers will only increase further in the coming years.

- **SOCCRATES** will contribute to the further automation of cyber defences, which is the only way this trend can be stopped and the odds can be evened.

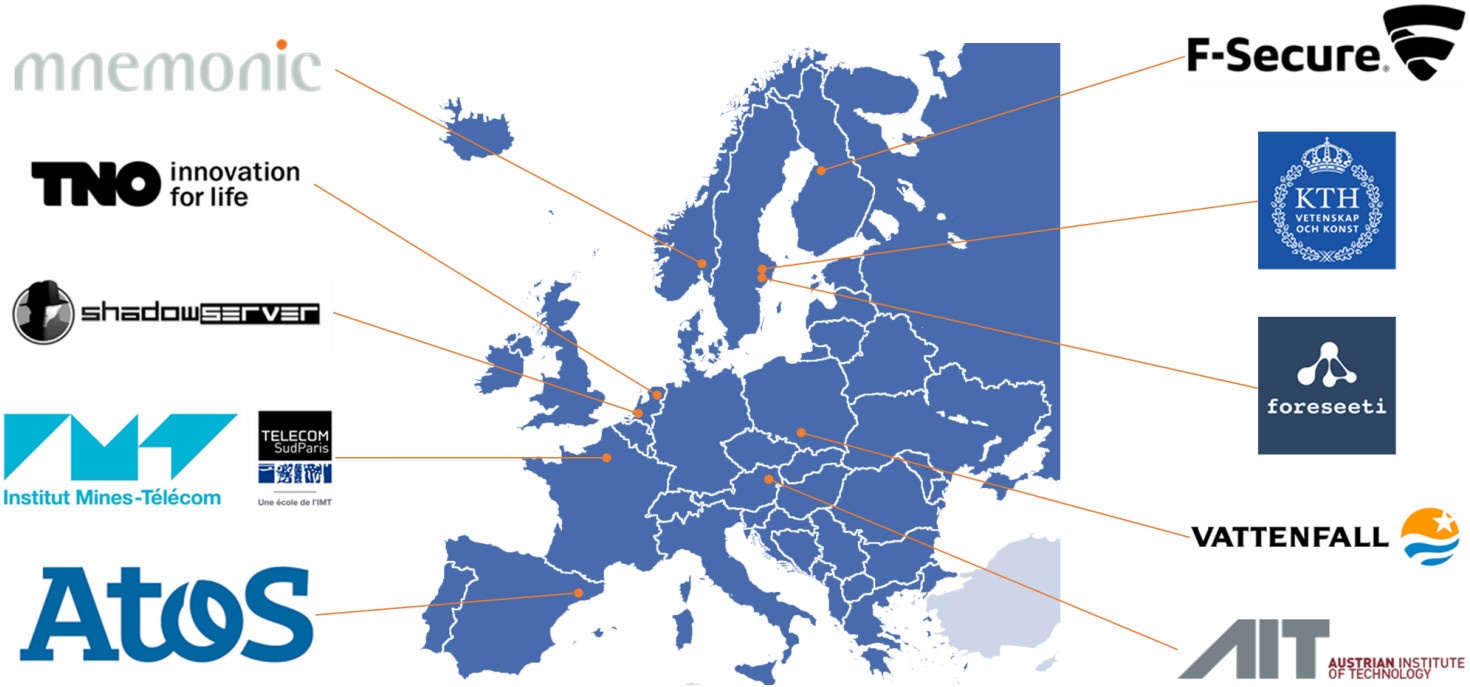
# PROJECT CHARACTERISTICS

| | |
|---|---|
| Call type | Innovation Action |
| Call ID/Topic | SU-ICT-01-2018 |
| Start date | September 1st 2019 |
| Project duration | 3 years |
| Budget | € 5.9M |
| EU funding | € 5M |
| Coordinator | TNO, The Netherlands |



# Consortium & Stakeholders

SOCCRATES




**With support of:** proximus, telenor, ABB, National Cyber Security Centrum, EUROPOL, Rabobank, de volksbank, kpn, amadeus

# 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:

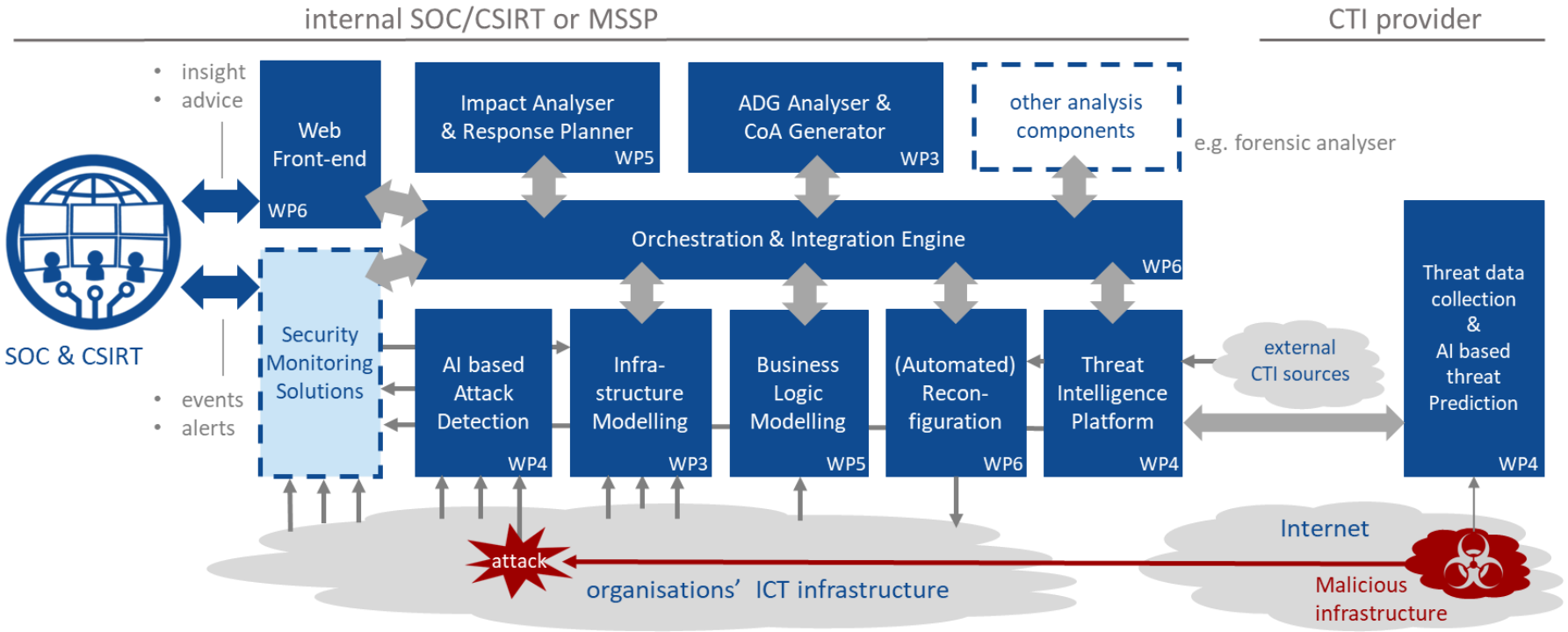
Develop and implement a security automation and decision support platform that enhances the effectiveness of SOC and CSIRT operations.

# SOCCRATES Use Cases

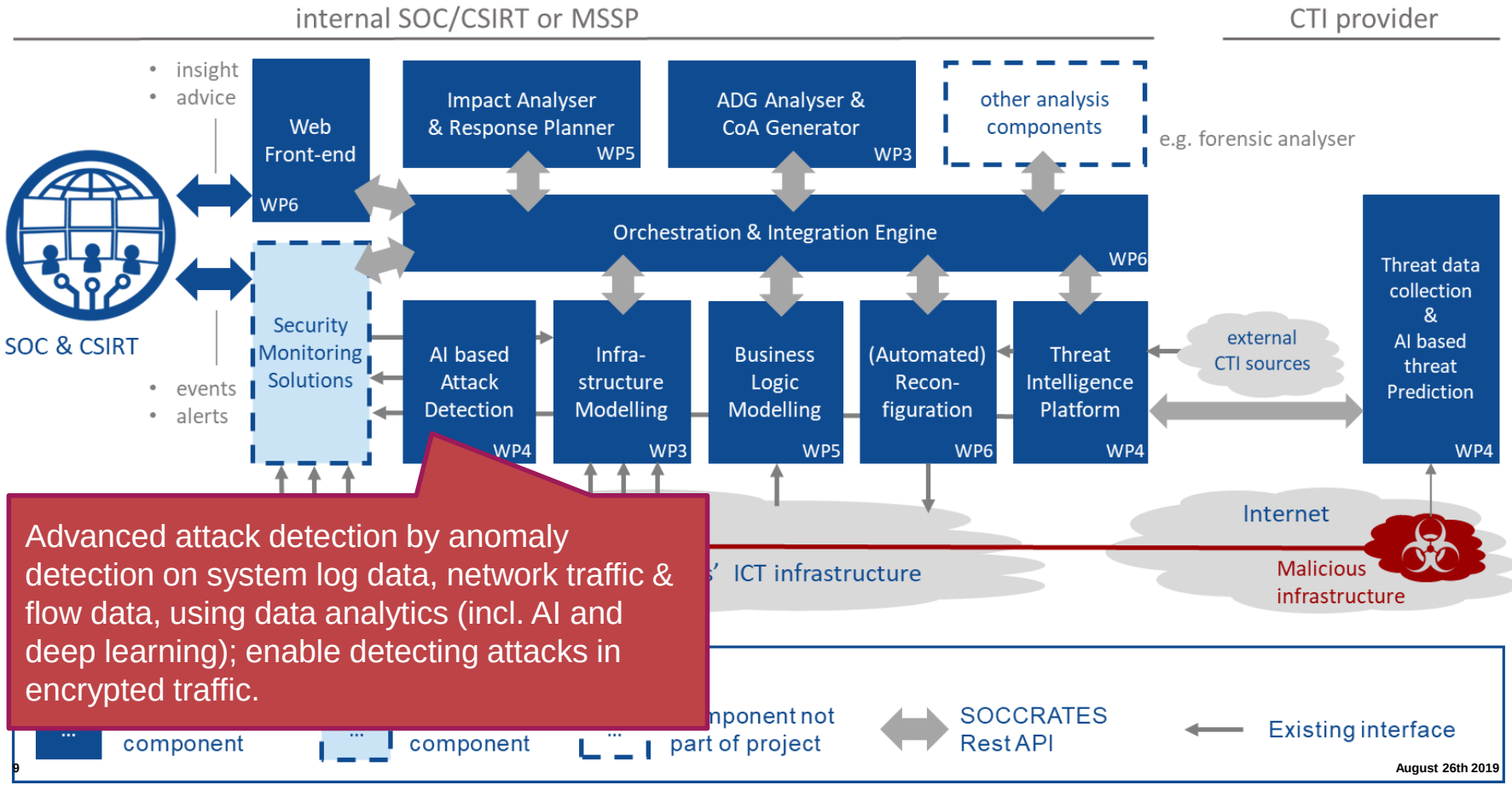
SOCCRATES

| Use Case 1 | Use Case 3 | Use Case 4 | Use Case 5 | Use Case 2 |
|---|---|---|---|---|
| ***Response on Detected Ongoing Attack*** | ***Response on Discovery of New Vulnerable Assets*** | ***Response on Discovery of System Configuration Change*** | ***Response on Deployment of New Systems in Infrastructure*** | ***Response on Reception of New Cyber Threat Intelligence*** |

# SOCCRATES Component Architecture

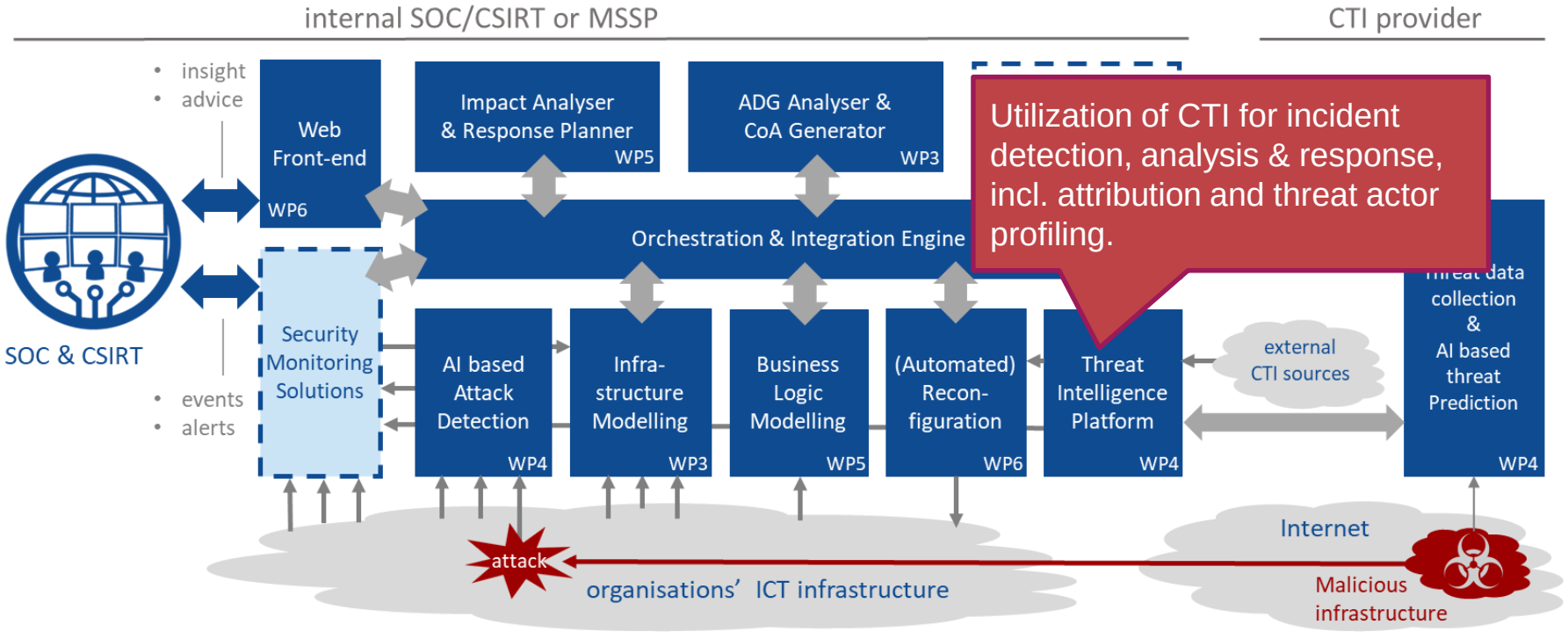


# SOCCRATES Component Architecture




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.

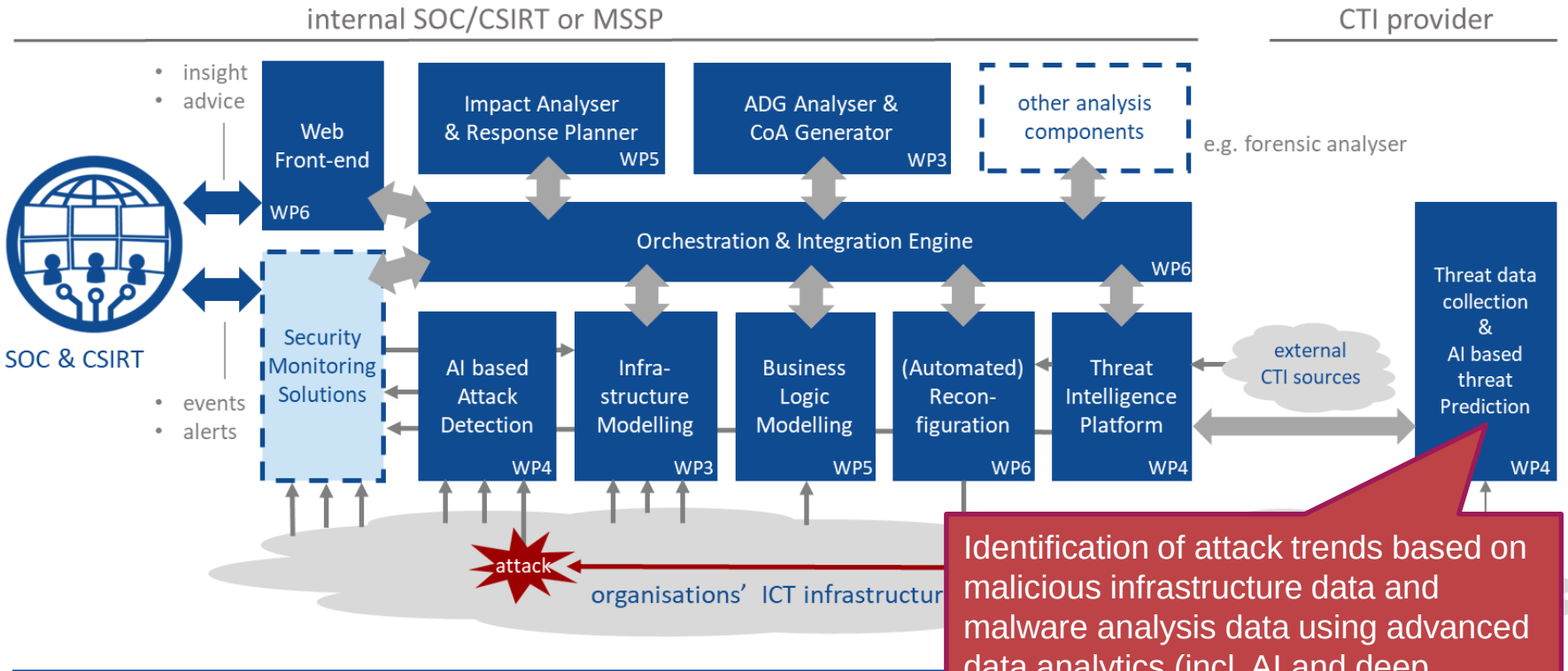
# SOCCRATES Component Architecture



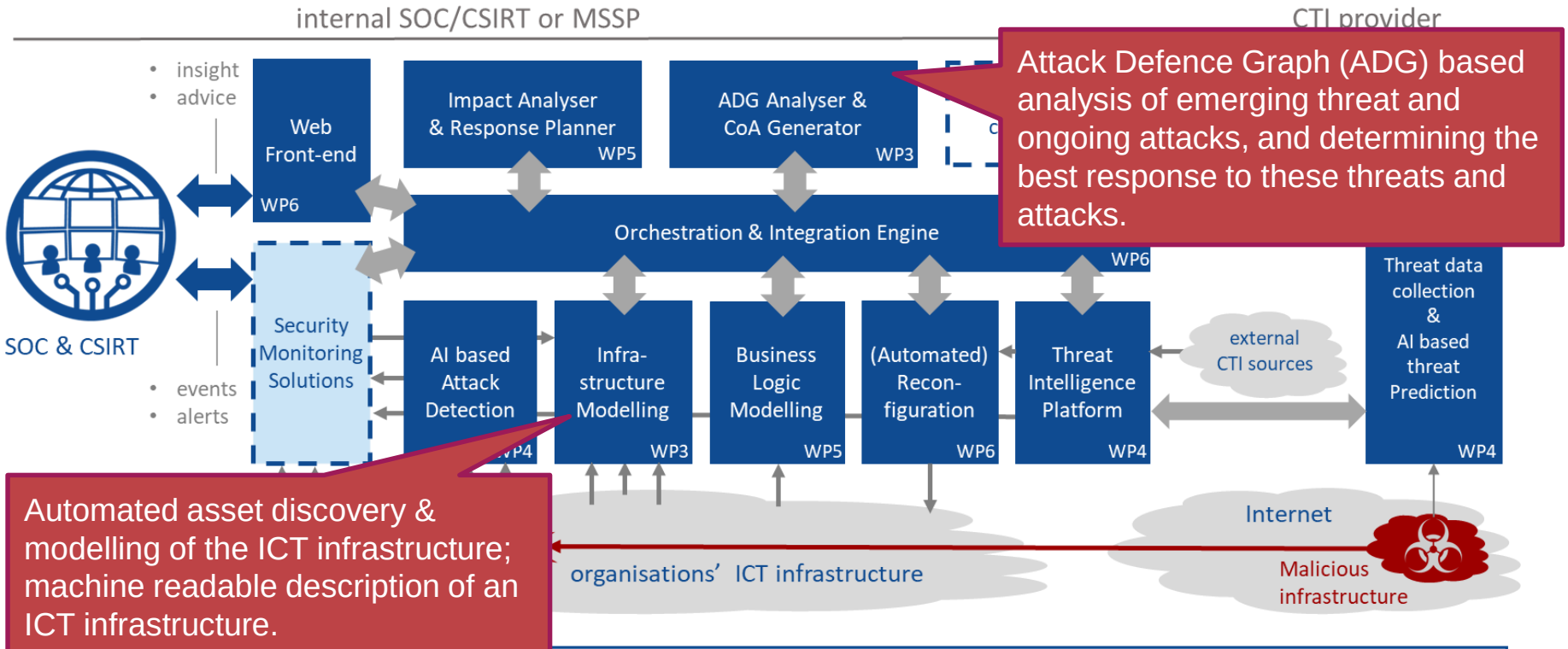

**Legend**

- SOCCRATES component
- Existing component
- Component not part of project
- SOCCRATES Rest API
- Existing interface

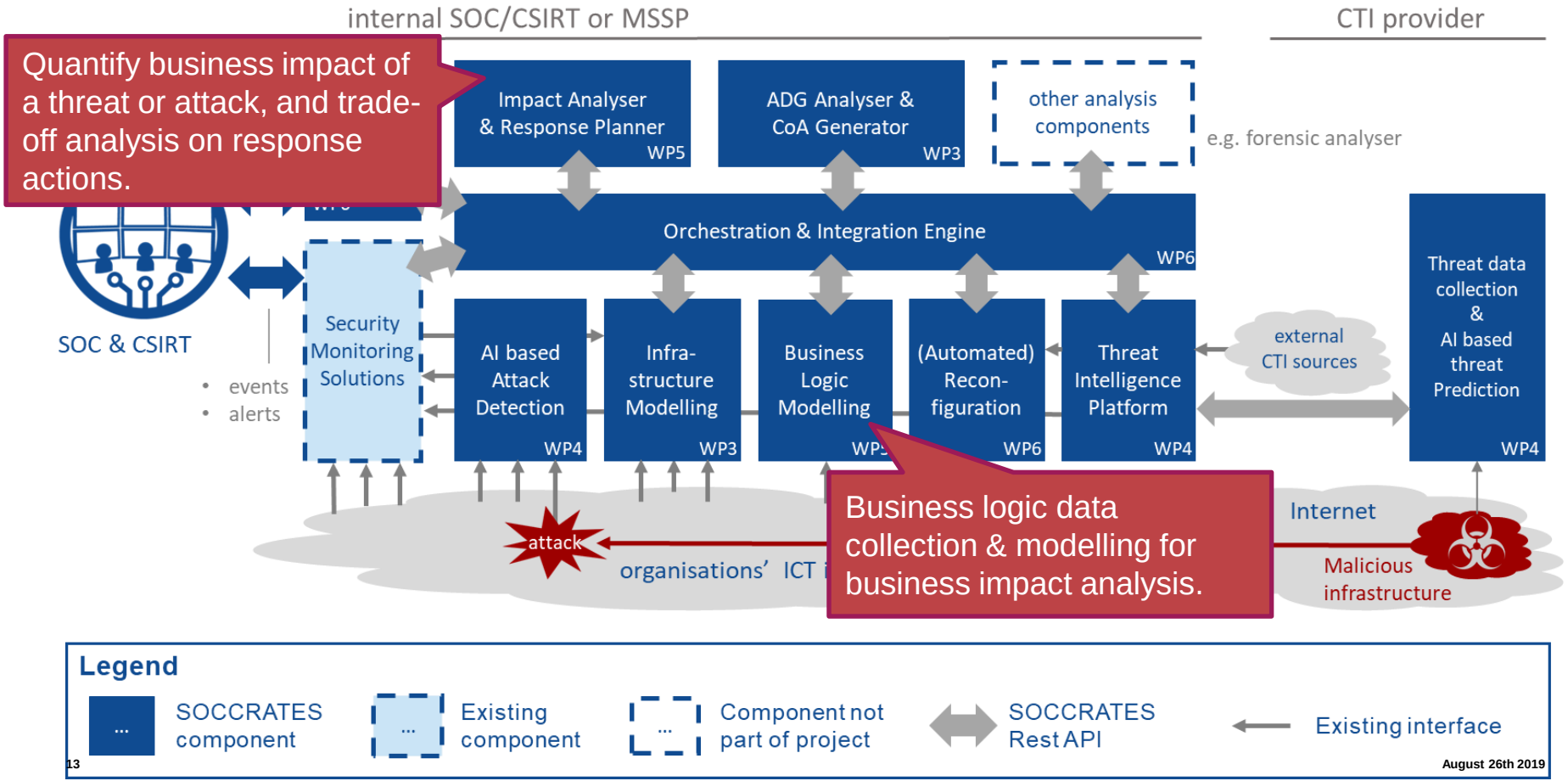
# SOCCRATES Component Architecture



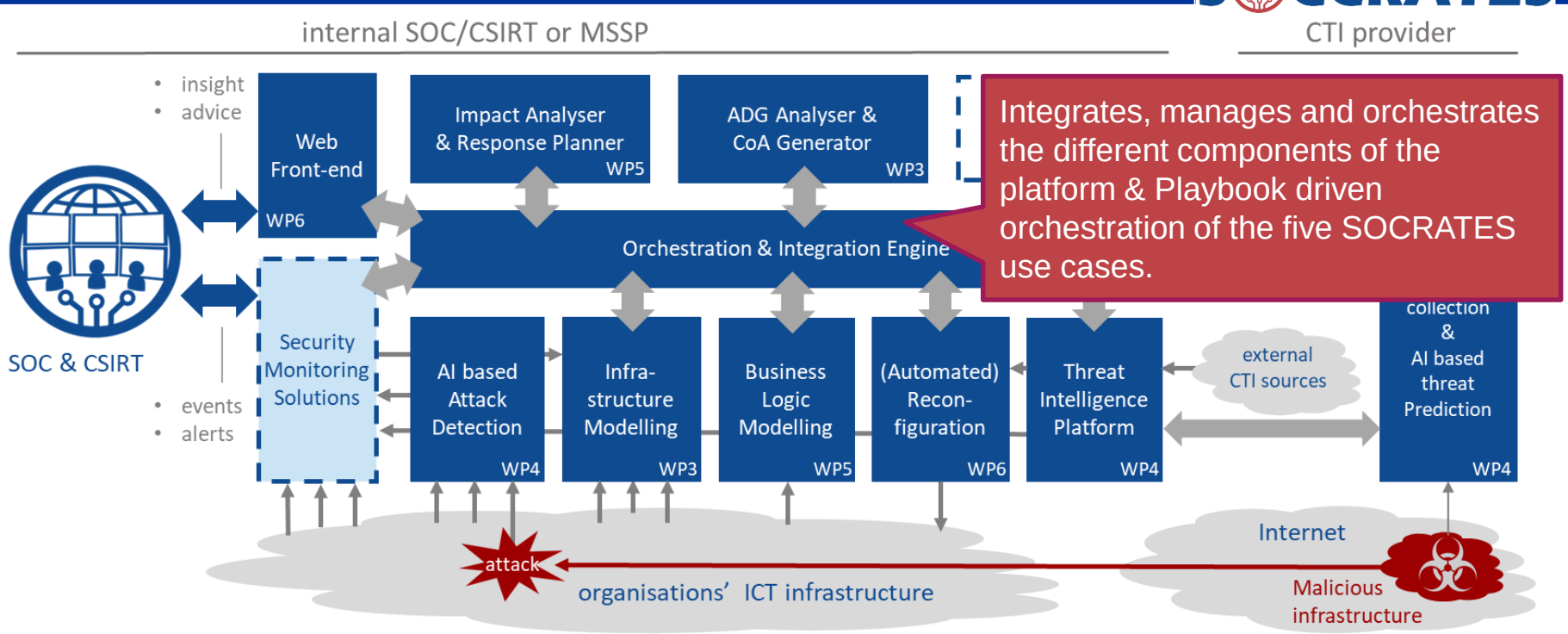
# SOCCRATES Component Architecture



# SOCCRATES Component Architecture



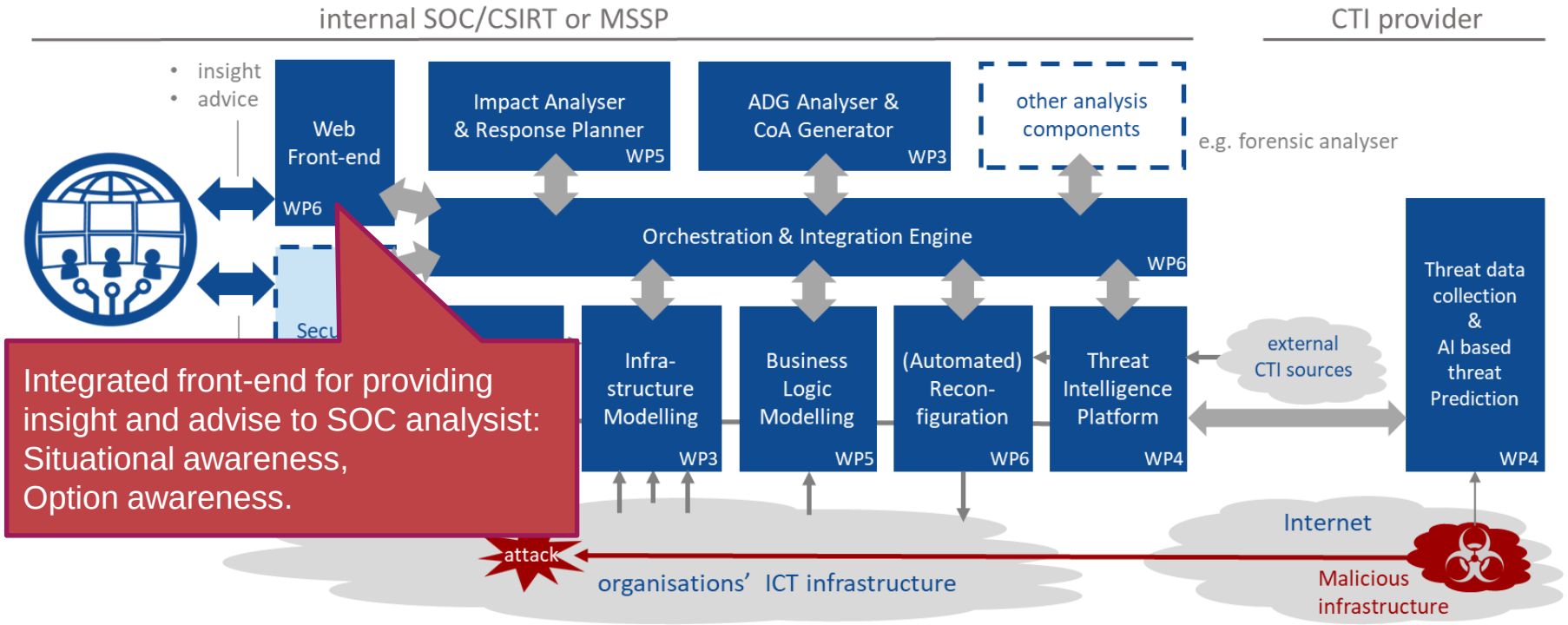
# SOCCRATES Component Architecture



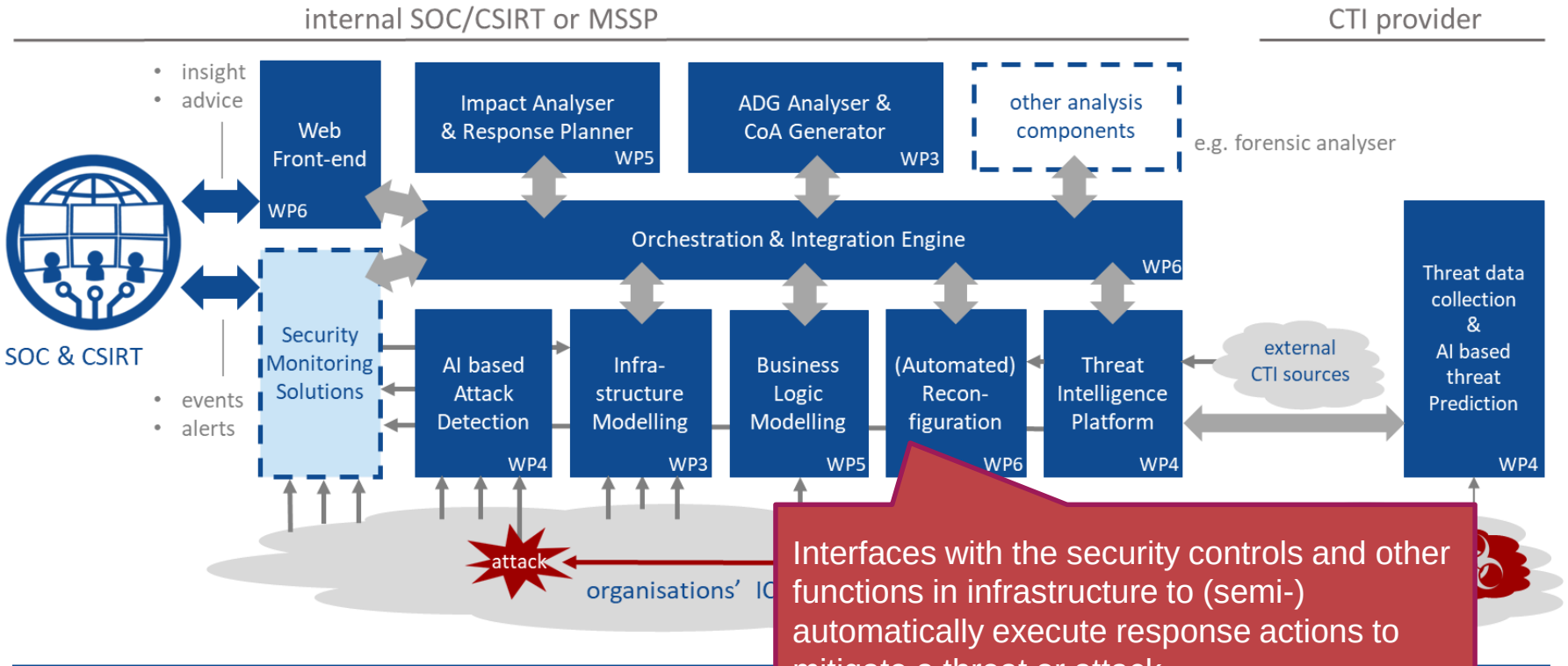

**Legend**

- SOCCRATES component
- Existing component
- Component not part of project
- SOCCRATES Rest API
- Existing interface

# SOCCRATES Component Architecture



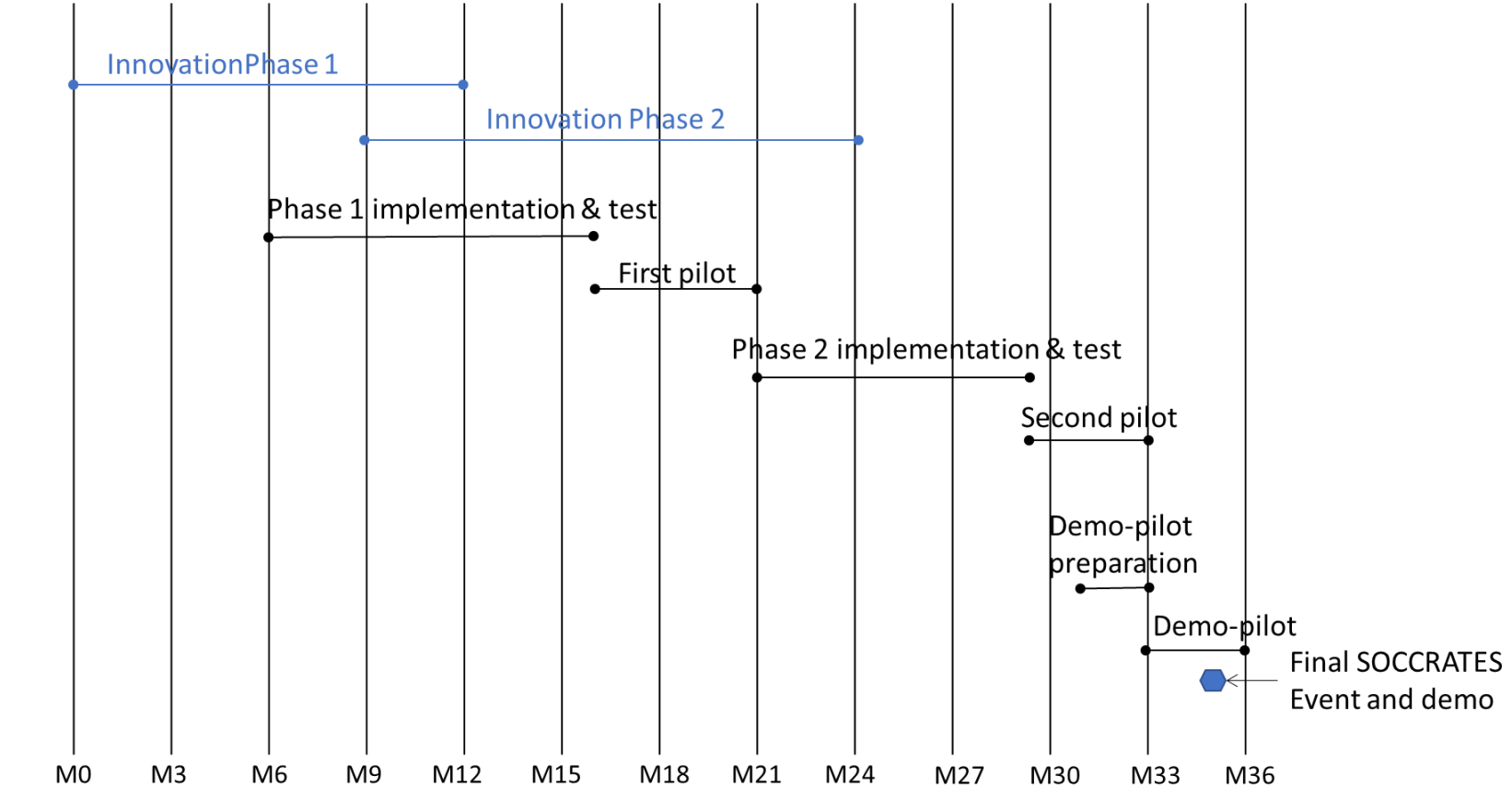
# SOCCRATES Component Architecture



# SOCCRATES Pilots

| Pilot | Description |
|---|---|
| Corporate SOC<br>VATTENFALL | The Vattenfall SOC, located in Poland, is the central security monitoring and response facility that services to all Vattenfall business units and IT.<br>The pilot will focus on SOCCRATES use cases 1 to 5. |
| MSSP<br>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.<br>The pilot will focus on SOCCRATES use cases 1 to 5. |
| Threat Prediction<br>shadowserver | 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. |

# SOCCRATES HIGH LEVEL PLANNING



# STAKEHOLDERS & ADVISORY BOARD

## SOCCRATES Stakeholder Group

de volksbank
kpn
EUROPOL
amadeus
ONVZ zorgverzekeraar
RDW
TDC Group
TOPSECTOR ENERGIE Empowering the new economy
Qbit CYBER SECURITY

**Room for additional members!**

## SOCCRATES Advisory Board

| | | |
|---|---|---|
| Andy de Petter | Head of cyber security intelligence & incident response | proximus Belgium |
| Frode Hommedal | Technical Director Cyber Threat Detection and Response | pwc Norway |
| Dr. Judith E.Y. Rossebo | Specialist cyber security & infrastructure | ABB Norway |
| Martin Pekarek | Cybersecurity advisor National Cyber Security Center | Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid Netherlands |

# Contacts

## Project Coordinator:


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


## Technical Coordinator:


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