

**SECURITY AUTOMATION**

MARKTDAG CYBER SECURITY 2020 | 12 March 2020 | ir. F. Fransen

**TNO** innovation for life

TNO Teams:

- H. Kerkdijk, J.P. Wijbenga, F. Fransen
- P.W. Zuraniewski, F. Falconieri, N. Gervasoni, B.M.M. Gijsen, F. Fransen

1

**TNO** innovation for life

**AGENDA**

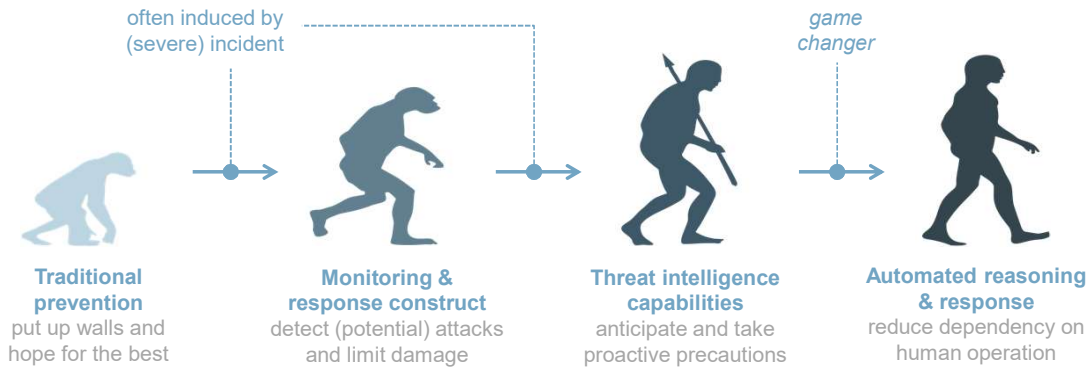
- TNO's vision**
- Security Decision Support**
- Automated Response**

**SOCCRATES**

SRP Threat Landscaping - Third Participant Workshop

2

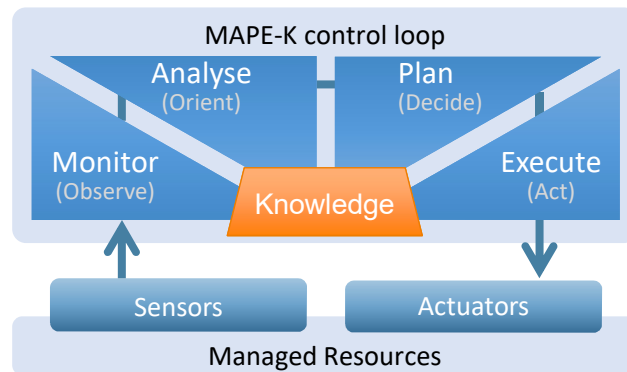
## EVOLUTION OF RESILIENCE STRATEGIES



Security Decision Support workshop | 12 February 2020

3

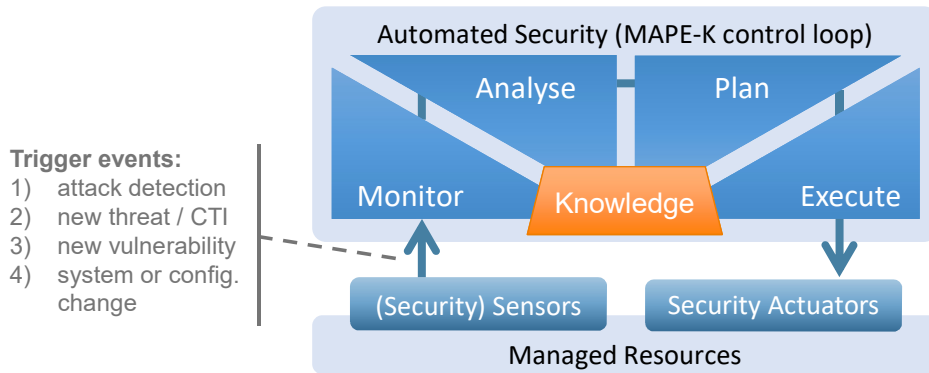
## SECURITY AUTOMATION & ORCHESTRATION MAPE-K / OODA



Automated Security

4

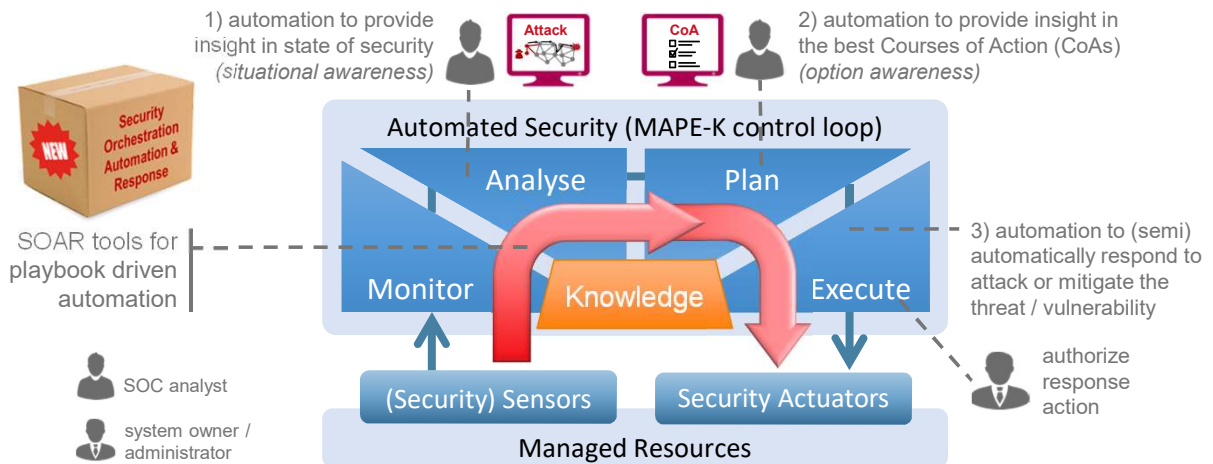
## SECURITY AUTOMATION & ORCHESTRATION TNO's view



Automated Security

5

## SECURITY AUTOMATION & ORCHESTRATION TNO's view

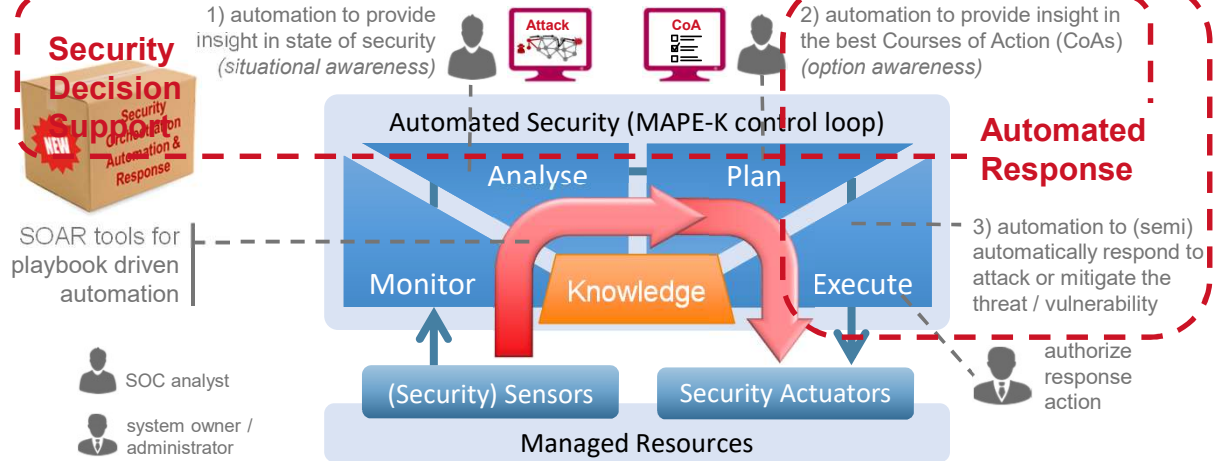


Automated Security

6

## SECURITY AUTOMATION & ORCHESTRATION

### Workshop scope



7

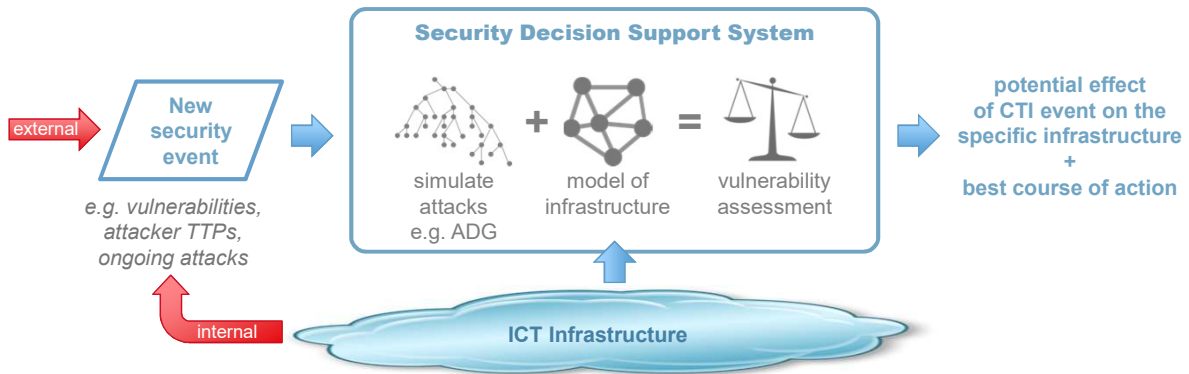
## AGENDA

- TNO's vision
- Security Decision Support
- Automated Response



8

## SECURITY DECISION SUPPORT

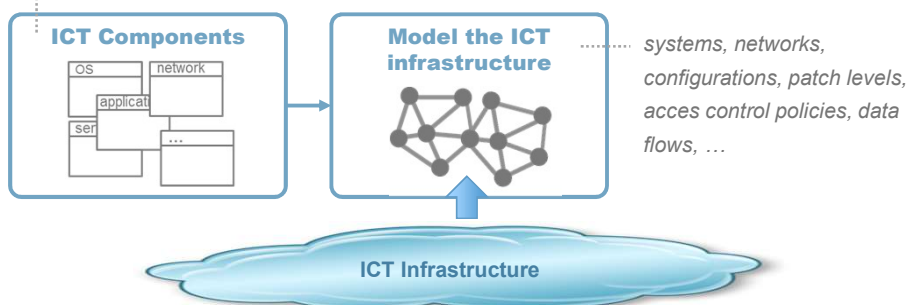


Automated Security

9

## CORE FUNCTIONAL COMPONENTS

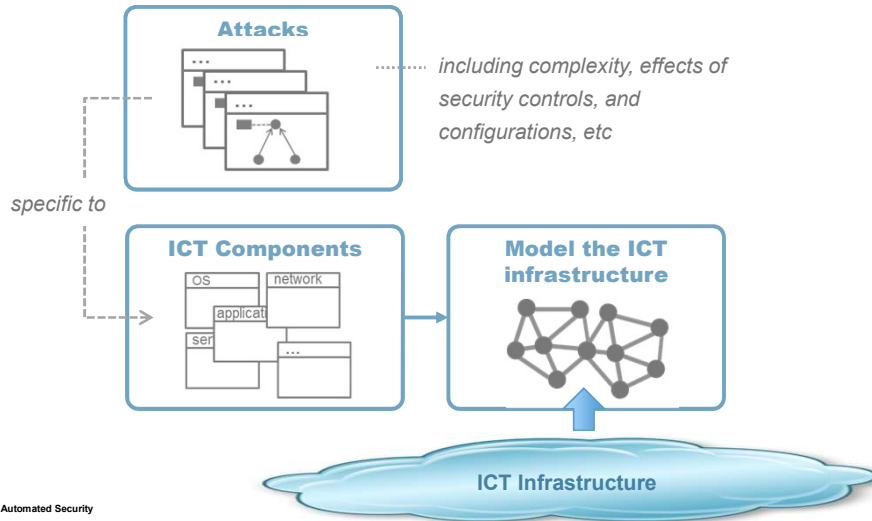
clients, servers, OS, applications,  
 firewalls, IDSs, routers...



Automated Security

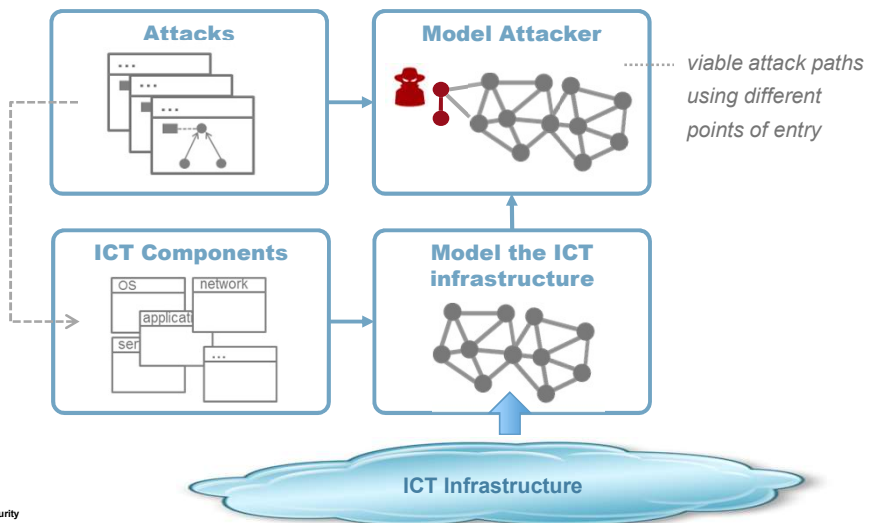
10

## CORE FUNCTIONAL COMPONENTS

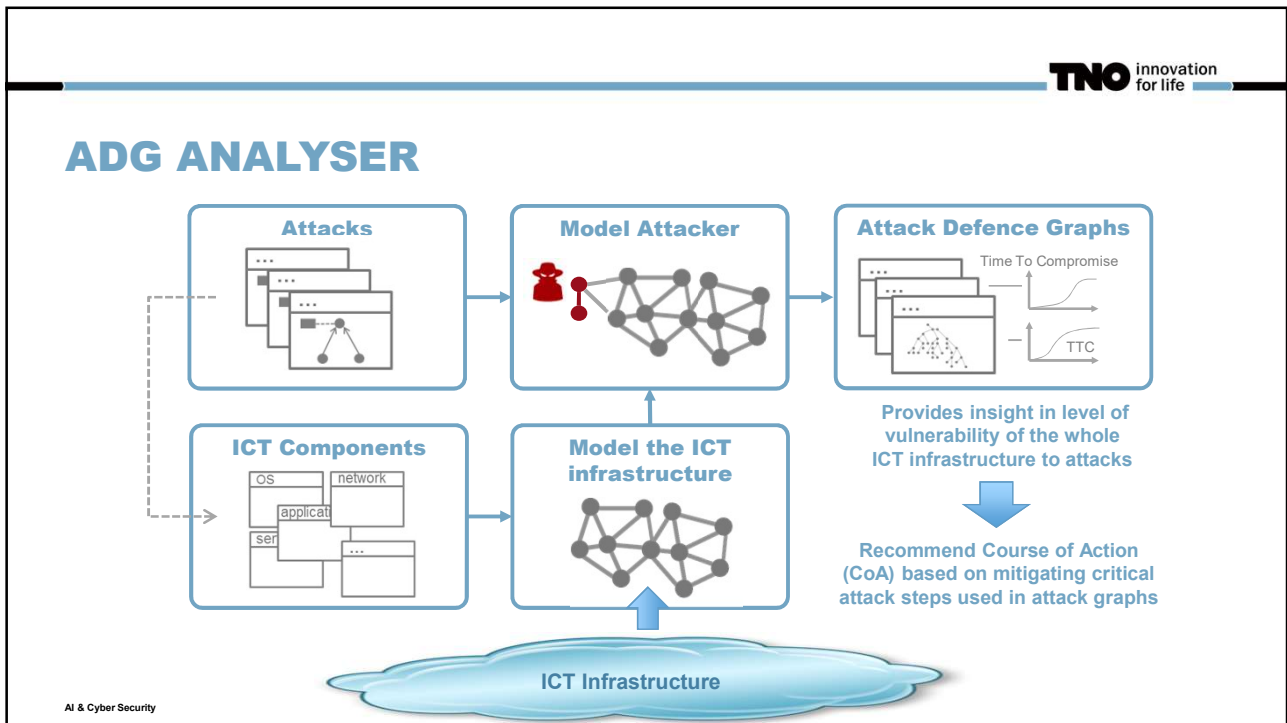


11

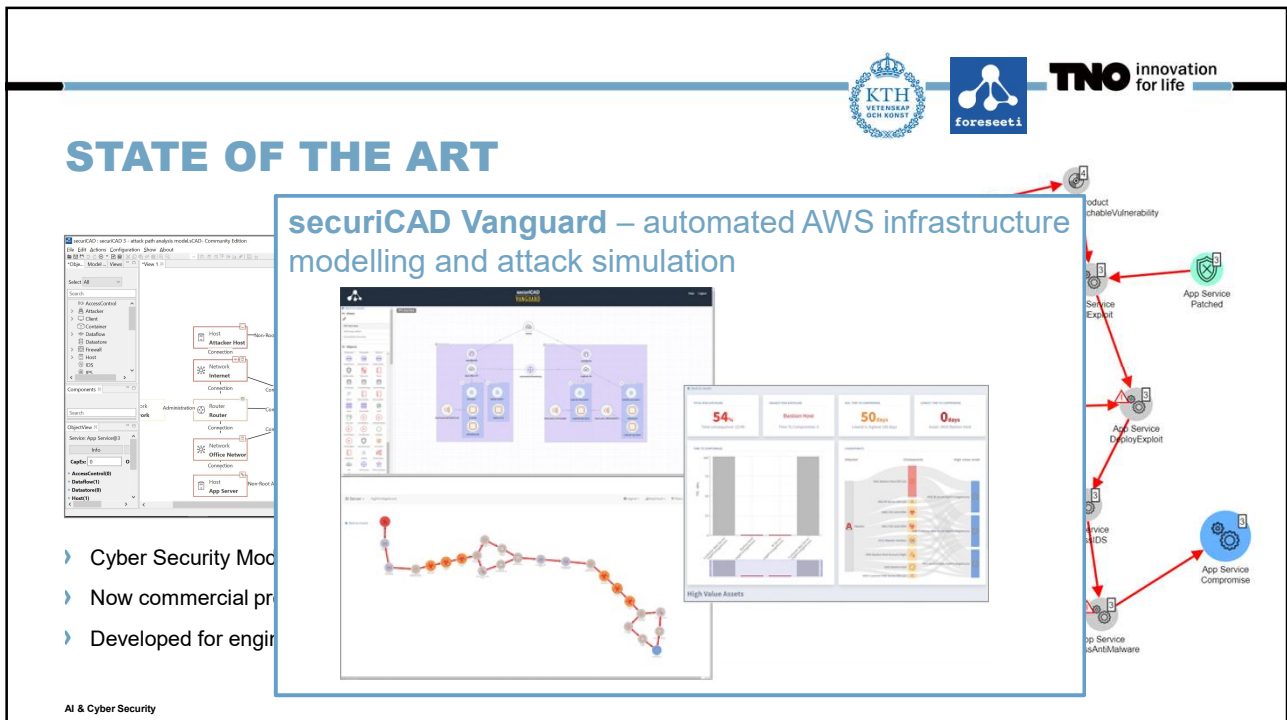
## CORE FUNCTIONAL COMPONENTS



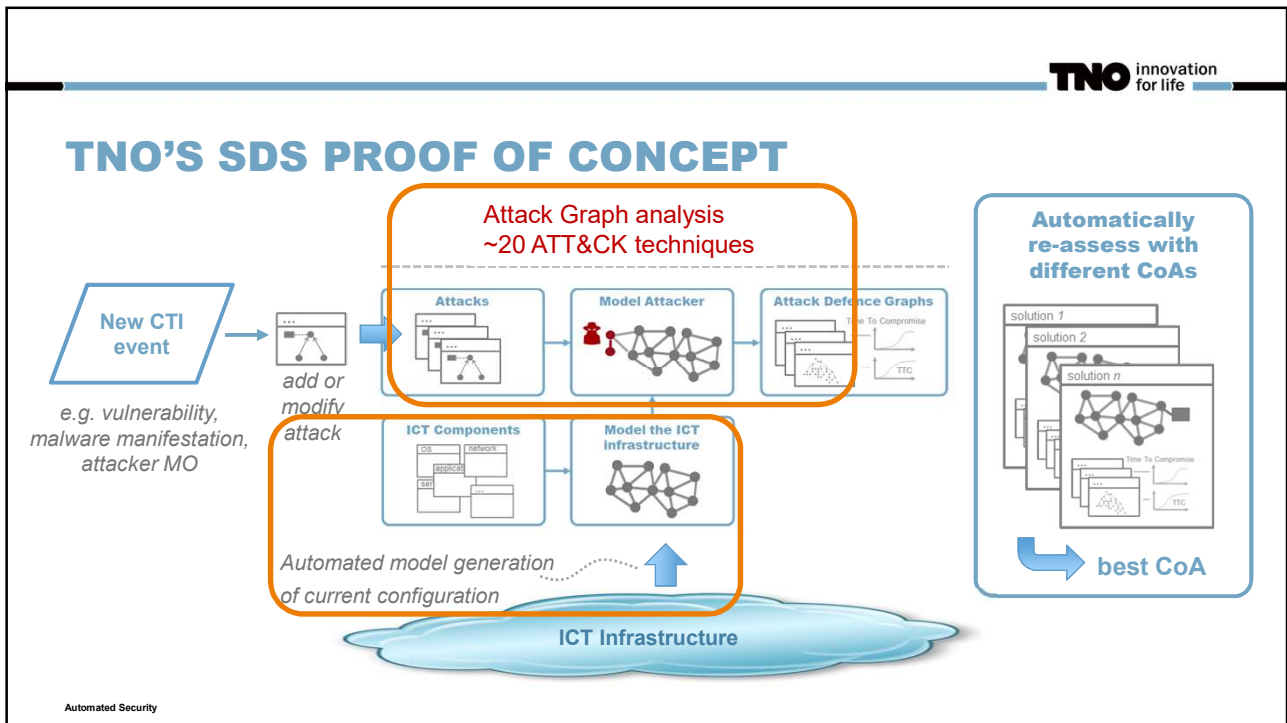
12



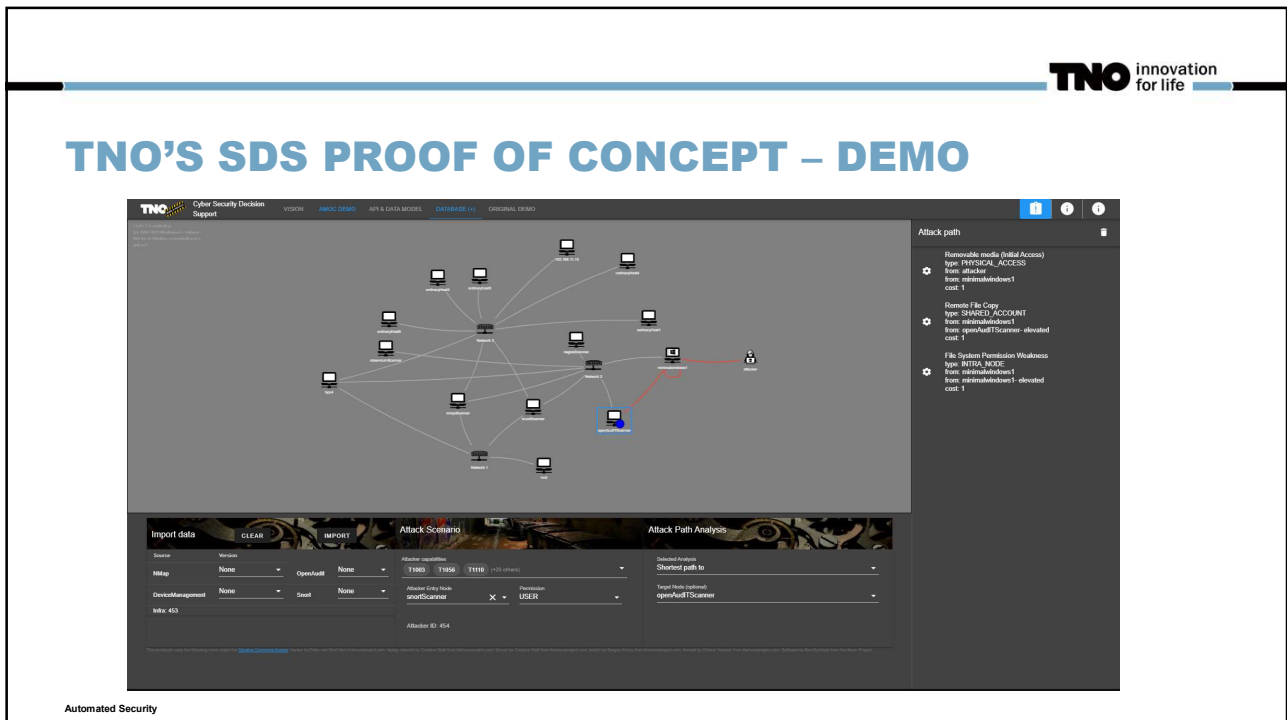
13



14



15



16



# AGENDA

TNO's vision

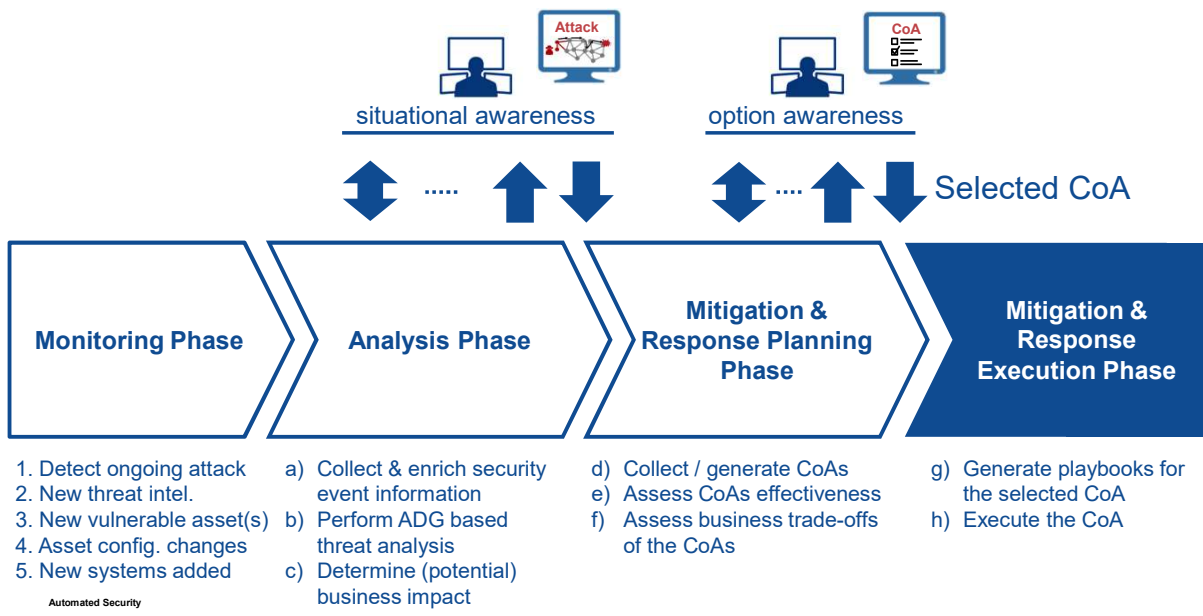
Security Decision Support

Automated Response

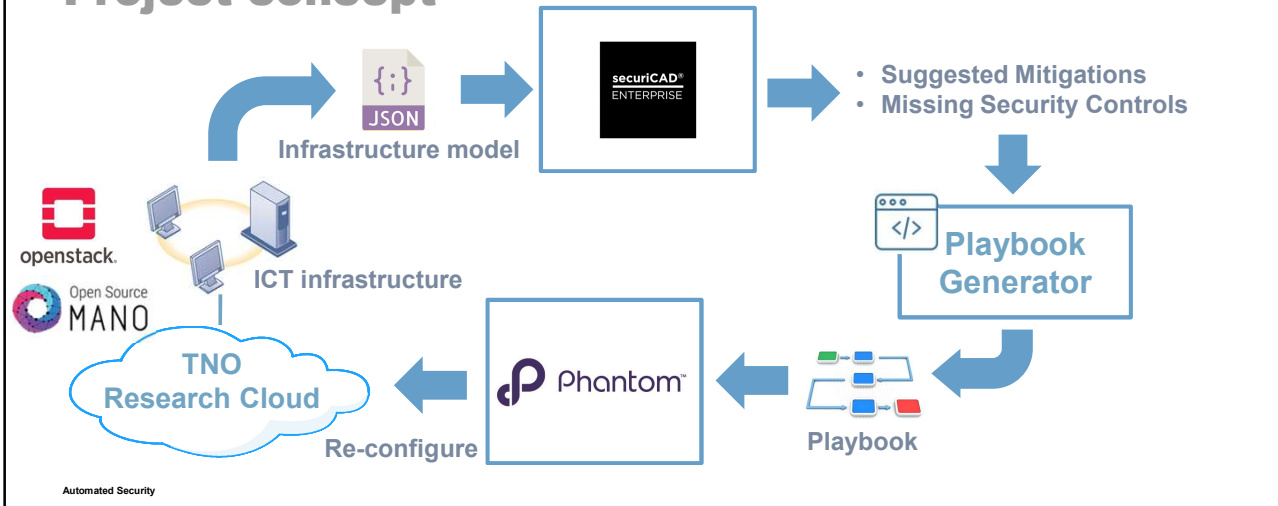


SRP Threat Landscaping – Third Participant Workshop

# AUTOMATED RESPONSE



## AUTOMATIC PLAYBOOK GENERATION Project concept



19

## SECURICAD – RECOMMENDATIONS

The interface shows two panels. The 'Suggested Mitigations' panel lists items like 'Install Antimalware', 'Enforce Multi-factor Authentication', and 'Train your users to be security-aware'. The 'Missing Objects' panel lists 'Missing HDS', 'Missing Zone Management', and 'Missing Unauthenticated Vulnerability Scanners'.

- API call to fetch simulation results in json
- Suggested mitigations are high-level / abstract, not all technical (e.g. train users to be security-aware)

20

## SECURICAD – RECOMMENDATIONS

The screenshot shows the securiCAD | ENTERPRISE interface. On the left is a 'Views' pane with 'Objects' and 'Object Explorer'. The main area is an 'Overview' network diagram. A callout box highlights a host labeled 'Stage srv 2'. The callout shows a list of defenses for this host:

- Defenses
  - ASLR
  - AntiMalware
    - Probability 0 (Default: 0.0)
  - DEP
  - Hardened
  - HostFirewall
  - Patched
  - ProperlyConfigured
  - StaticARPTables

Automated Security

21

## PHANTOM PLAYBOOKS & OPERATION

The screenshot shows the Phantom interface for editing a playbook named 'c2\_investigate\_and\_contain'. The main area displays a flowchart of operations. Two callouts are present:

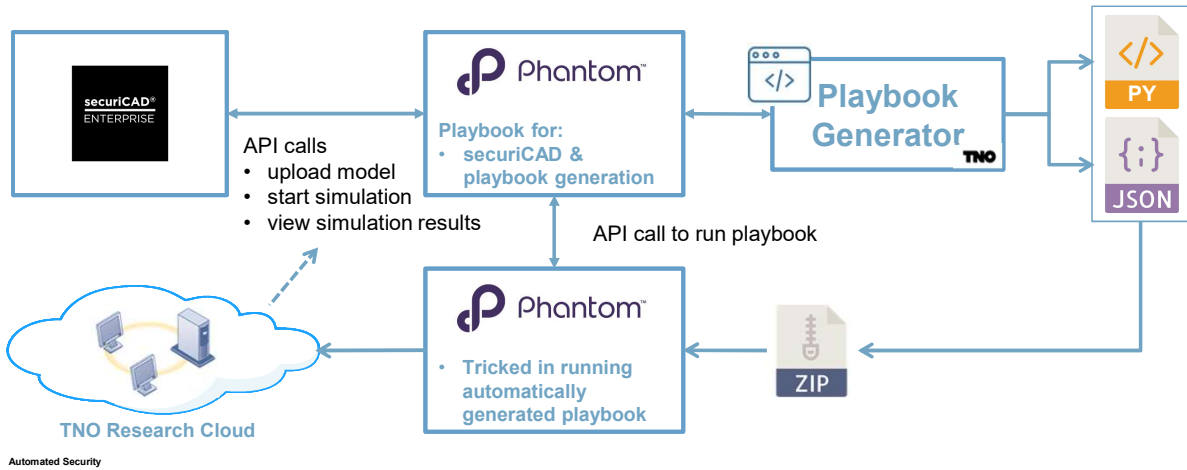
- PY**: Python functions for each of the operations in the playbook
- JSON**: JSON specification of how the operations are arranged and meta data for visualisation

- › We are able to generate a playbook for a recommended CoA
- › Phantom provides very limited API to load and run a playbooks.

Automated Security

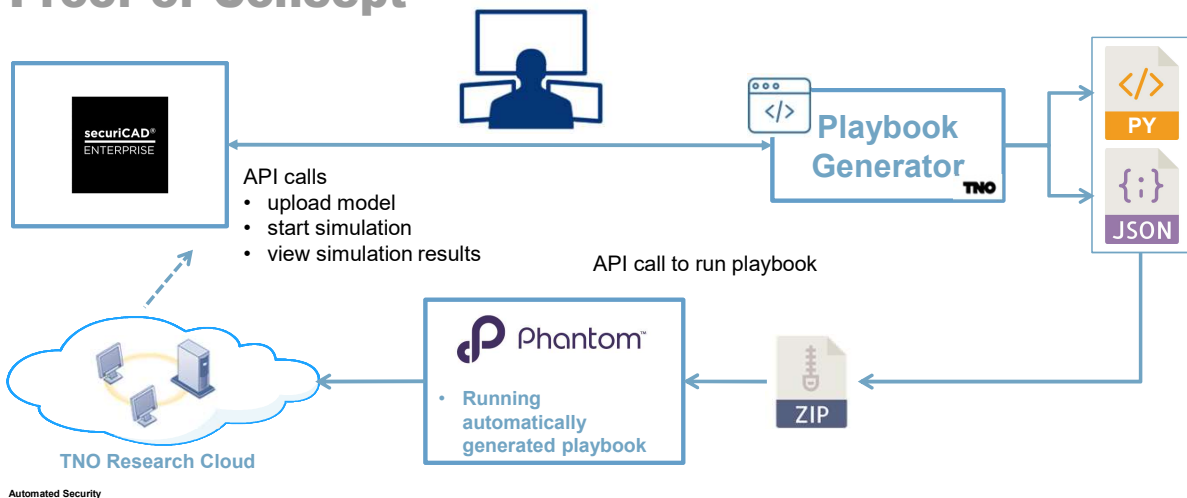
22

## AUTOMATIC PLAYBOOK GENERATION Tool chain



23

## AUTOMATIC PLAYBOOK GENERATION Proof of Concept



24

**TNO** innovation for life


## AGENDA

- TNO's vision
- Security Decision Support
- Automated Response

**SOC CRATES**

SRP Threat Landscaping – Third Participant Workshop

25














# SOC CRATES

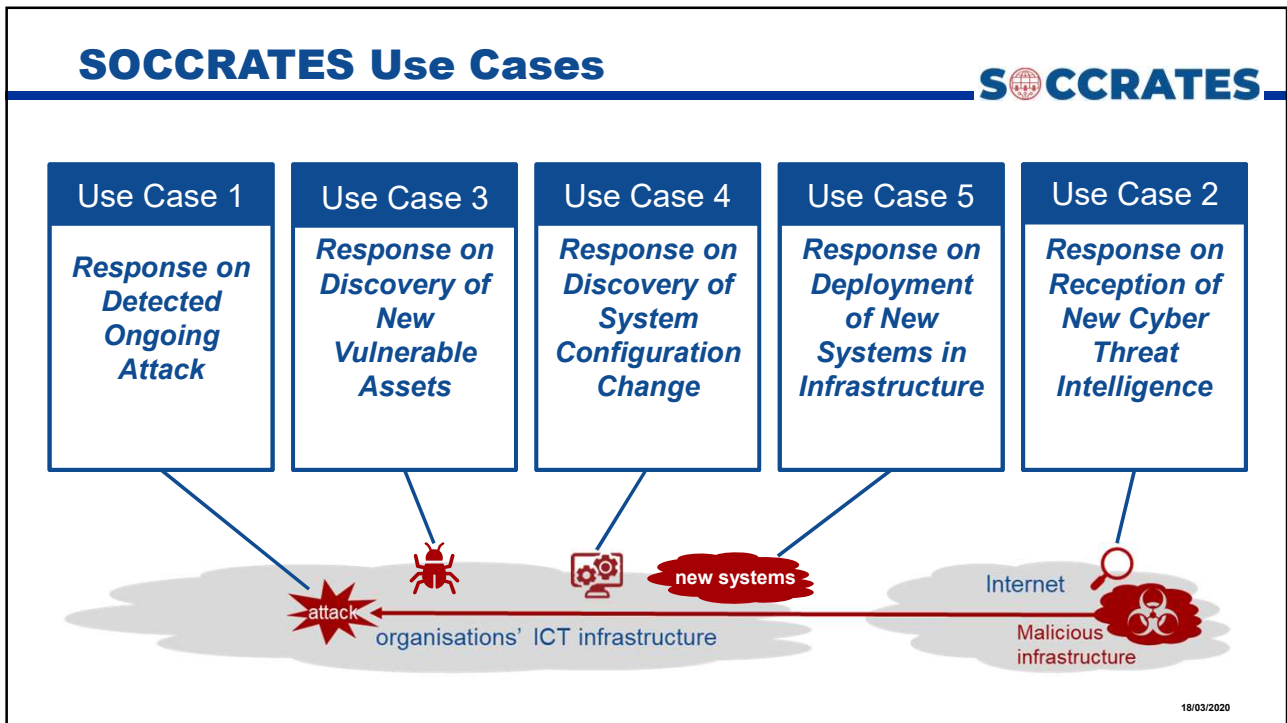
**SOC & CSIRT Response to Attacks & Threats**  
based on attack defense graphs Evaluation Systems

**Project details**

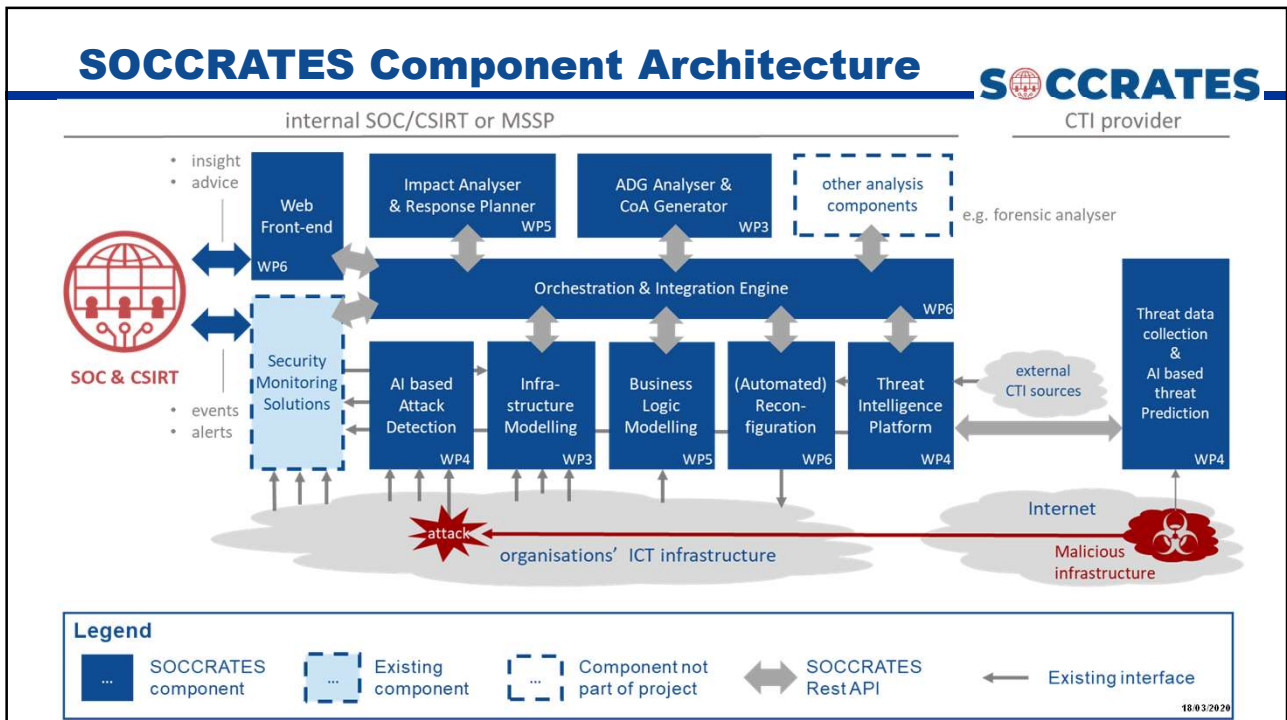
Call type	Innovation Action
Call ID/Topic	SU-ICT-01-2018
Start date	September 1 <sup>st</sup> , 2019
EU funding	€ 5M   GA 833481
Coordinator	TNO, The Netherlands
Website	<a href="http://www.soccrates.eu">www.soccrates.eu</a>






26



27





28

SOCCRATES Pilots		SOCCRATES
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.	

11/03/2020

29

Contacts		SOCCRATES
<p>Project Coordinator:</p> <div style="border: 1px solid #ccc; padding: 10px; text-align: center;">   <p>Reinder Wolthuis                              +31 6 5191 33 79                              reinder.wolthuis@tno.nl</p> </div>	<p>Technical Coordinator:</p> <div style="border: 1px solid #ccc; padding: 10px; text-align: center;">   <p>Frank Fransen                              +31 6 53 72 49 00                              frank.fransen@tno.nl</p> </div>	
<p><a href="https://www.soccrates.eu/">https://www.soccrates.eu/</a></p> <p>Contact us if you want to join the stakeholder group</p>		

11/03/2020

30

