Automated Response based on SecuriCAD Recommendations

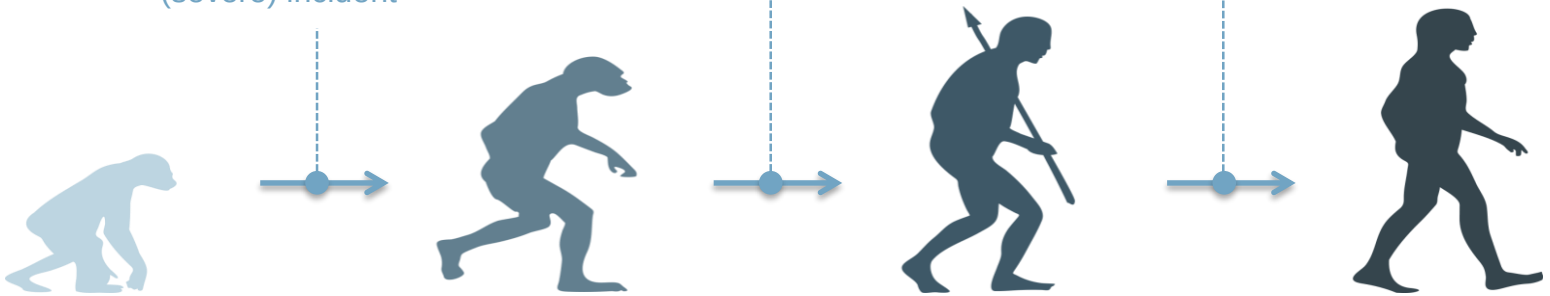
Workshop on Next Generation Security Operations Centers (NG-SOC 2019) | Ir. F. Fransen

TNO innovation for life

EVOLUTION OF RESILIENCE STRATEGIES

- **shortage** of skilled resources
- increasing **volume** of security events
- detection & response **time** is lagging behind
- ICT infrastructure increasingly **complex**

often induced by
(severe) incident



Traditional prevention
put up walls and hope for the best

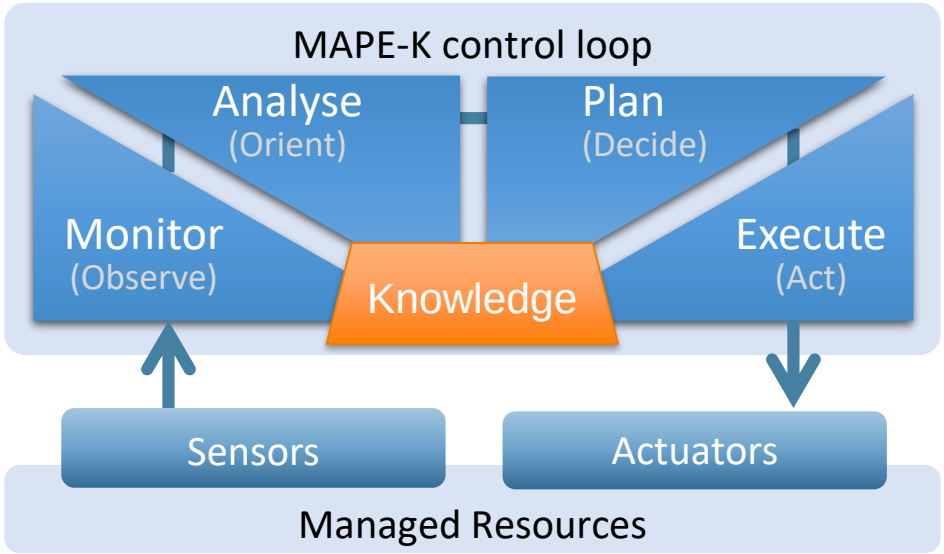
Monitoring & response construct
detect (potential) attacks and limit damage

Threat intelligence capabilities
anticipate and take proactive precautions

Autonomous response & recovery
reduce dependency on human operation

SECURITY AUTOMATION & ORCHESTRATION

MAPE-K / OODA

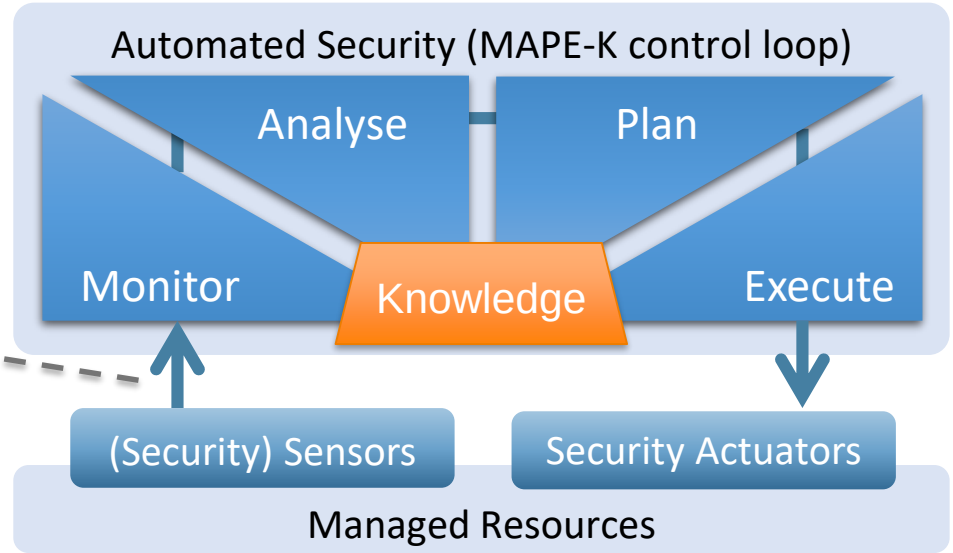


SECURITY AUTOMATION & ORCHESTRATION

TNO's view

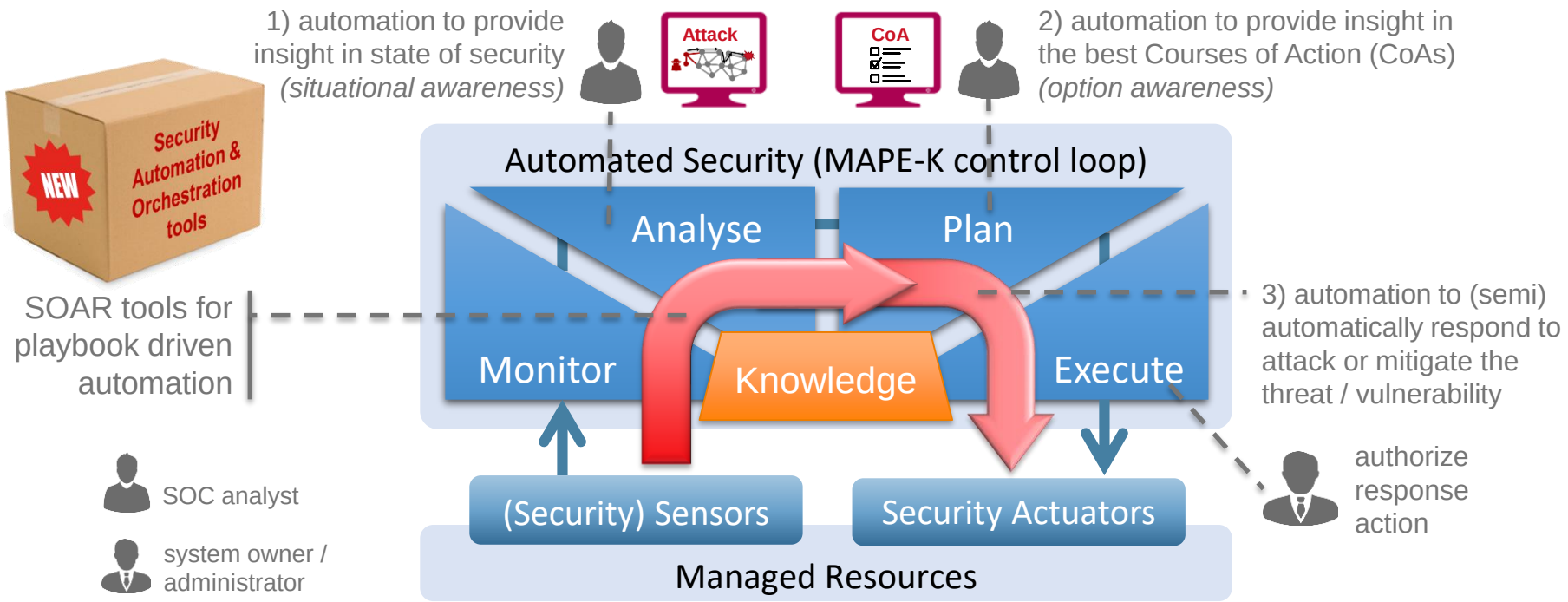
Trigger events:

1) attack detection
2) new threat / CTI
3) new vulnerability
4) system or config. change



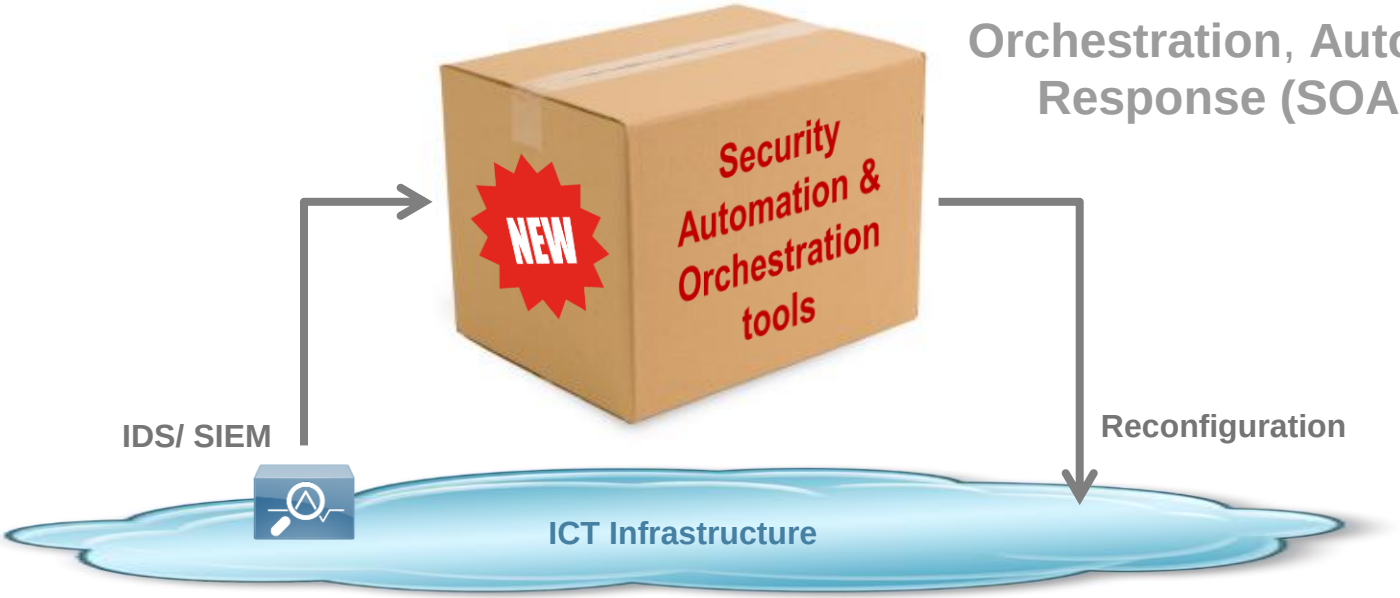
SECURITY AUTOMATION & ORCHESTRATION

TNO's view

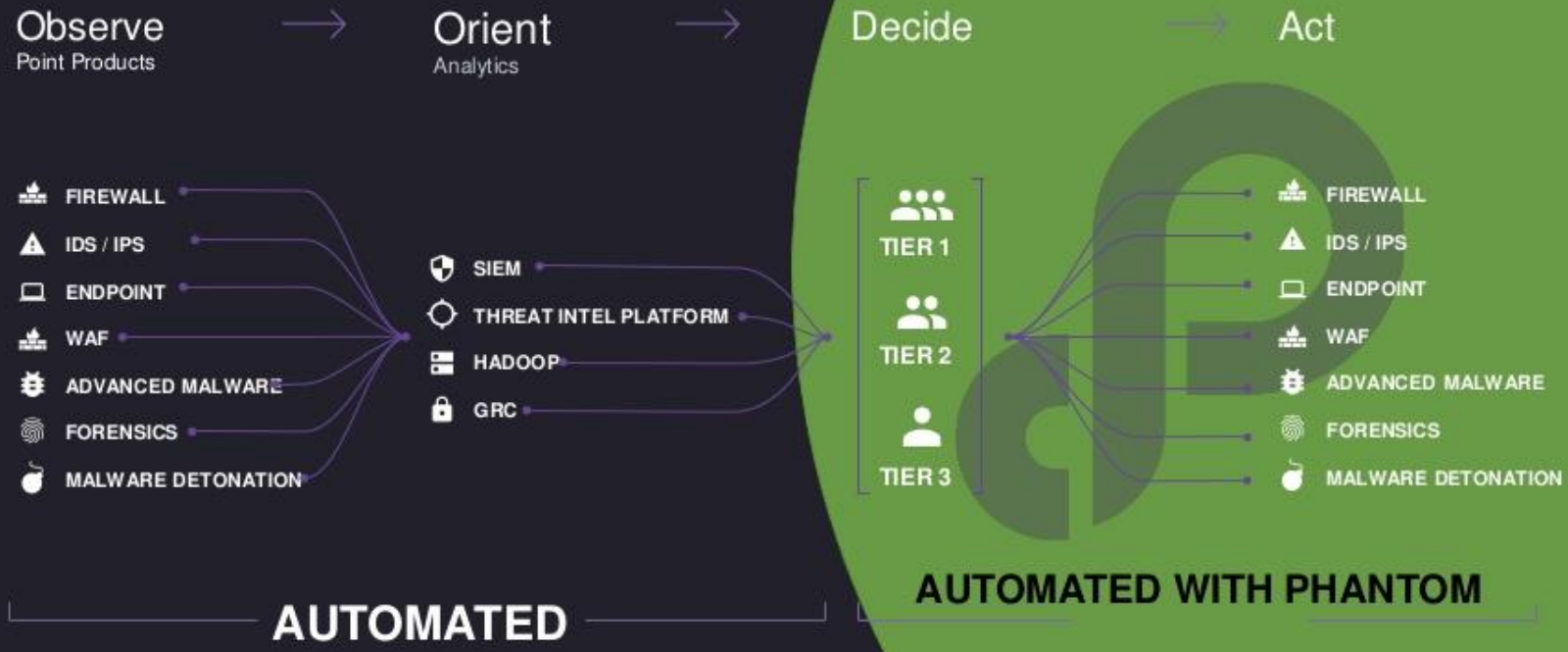


SECURITY AUTOMATION & ORCHESTRATION

Also referred to as **Security Orchestration**, **Automation** & **Response (SOAR)** tools



Automating Security Operations



Same People x Less Time = Lower Cost

Automating Security Operations

Observe
Point Products

→

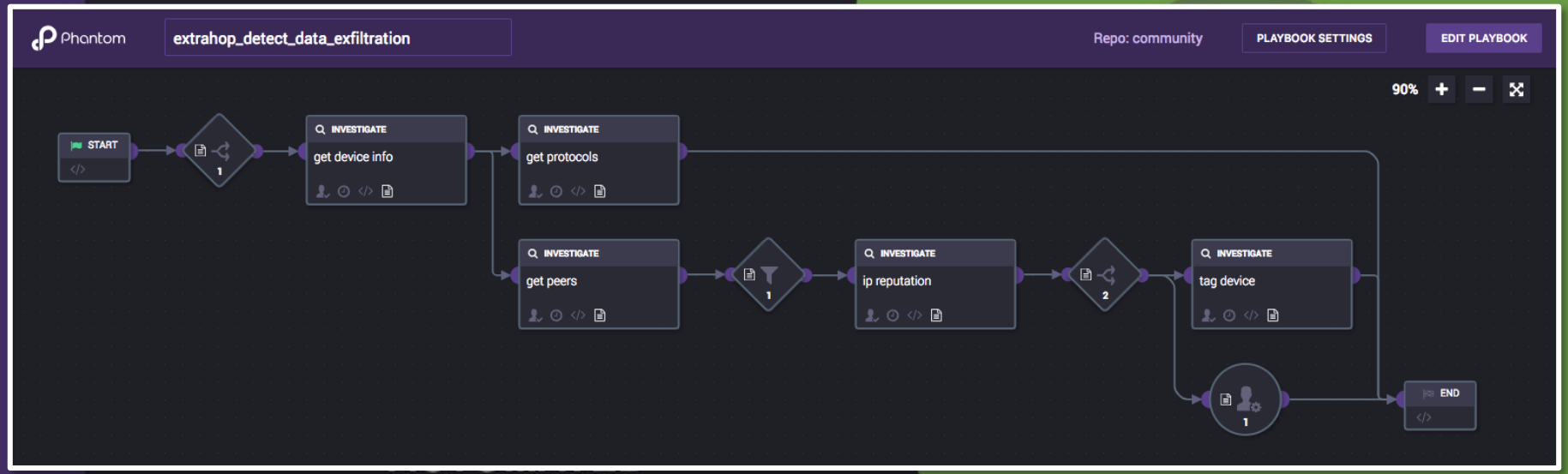
Orient
Analytics

→

Decide

→

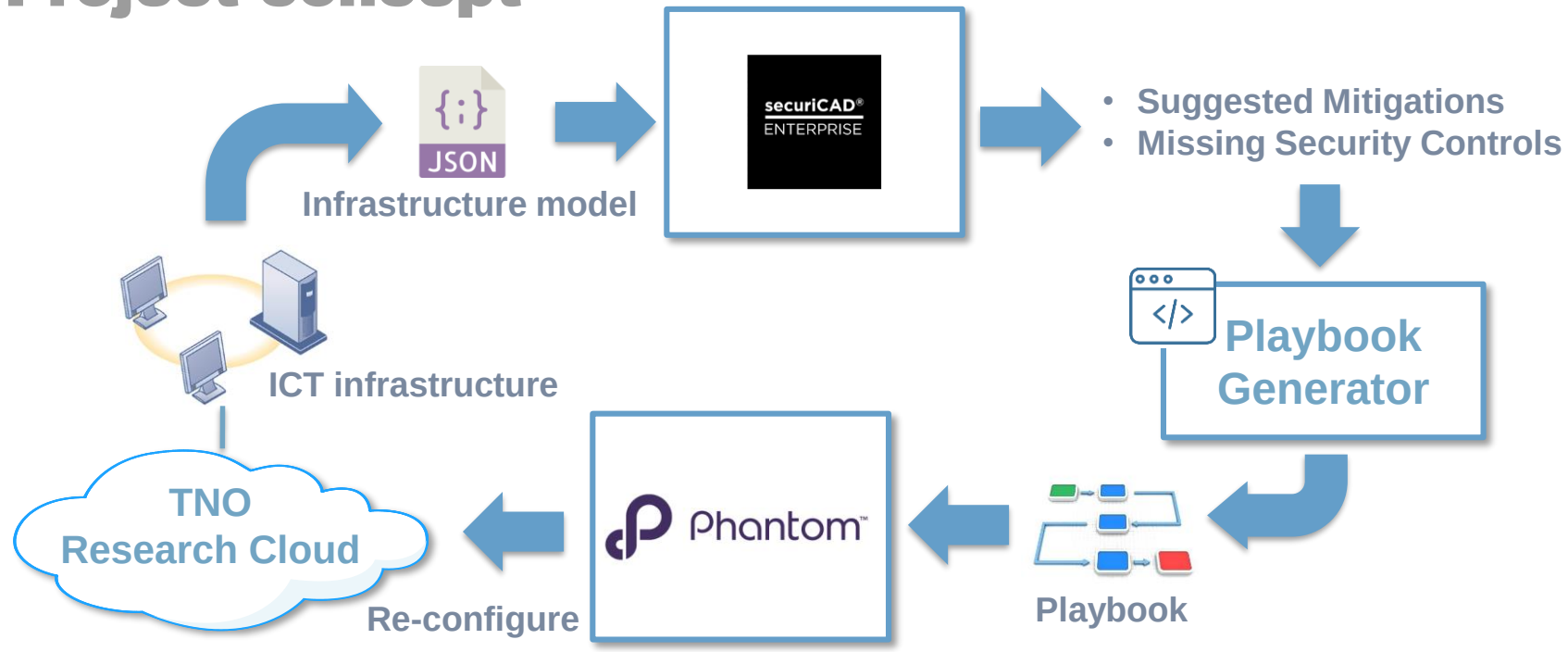
Act



Same People x Less Time = Lower Cost

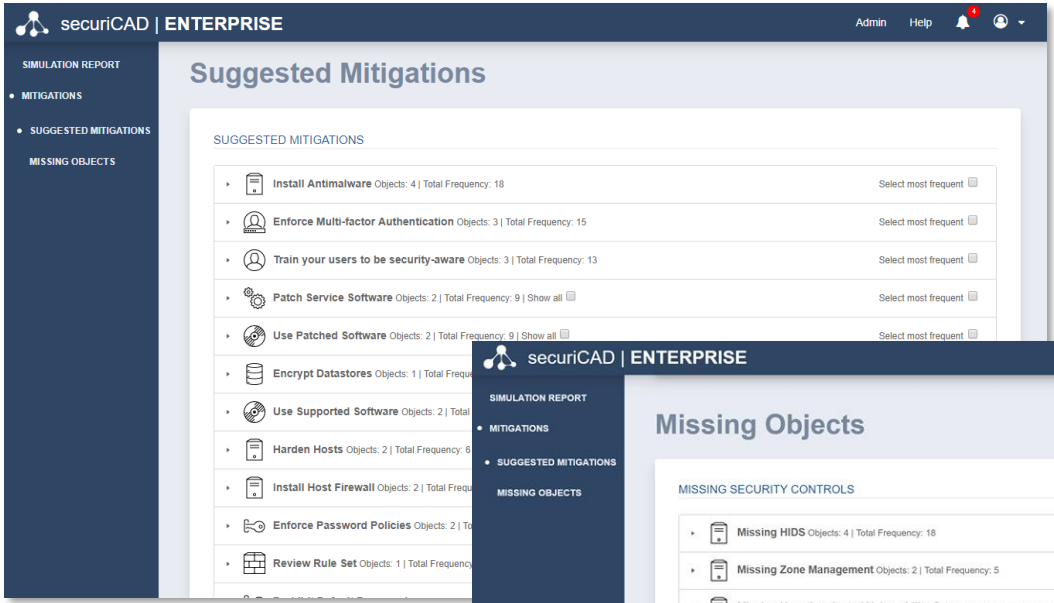
AUTOMATIC PLAYBOOK GENERATION

Project concept



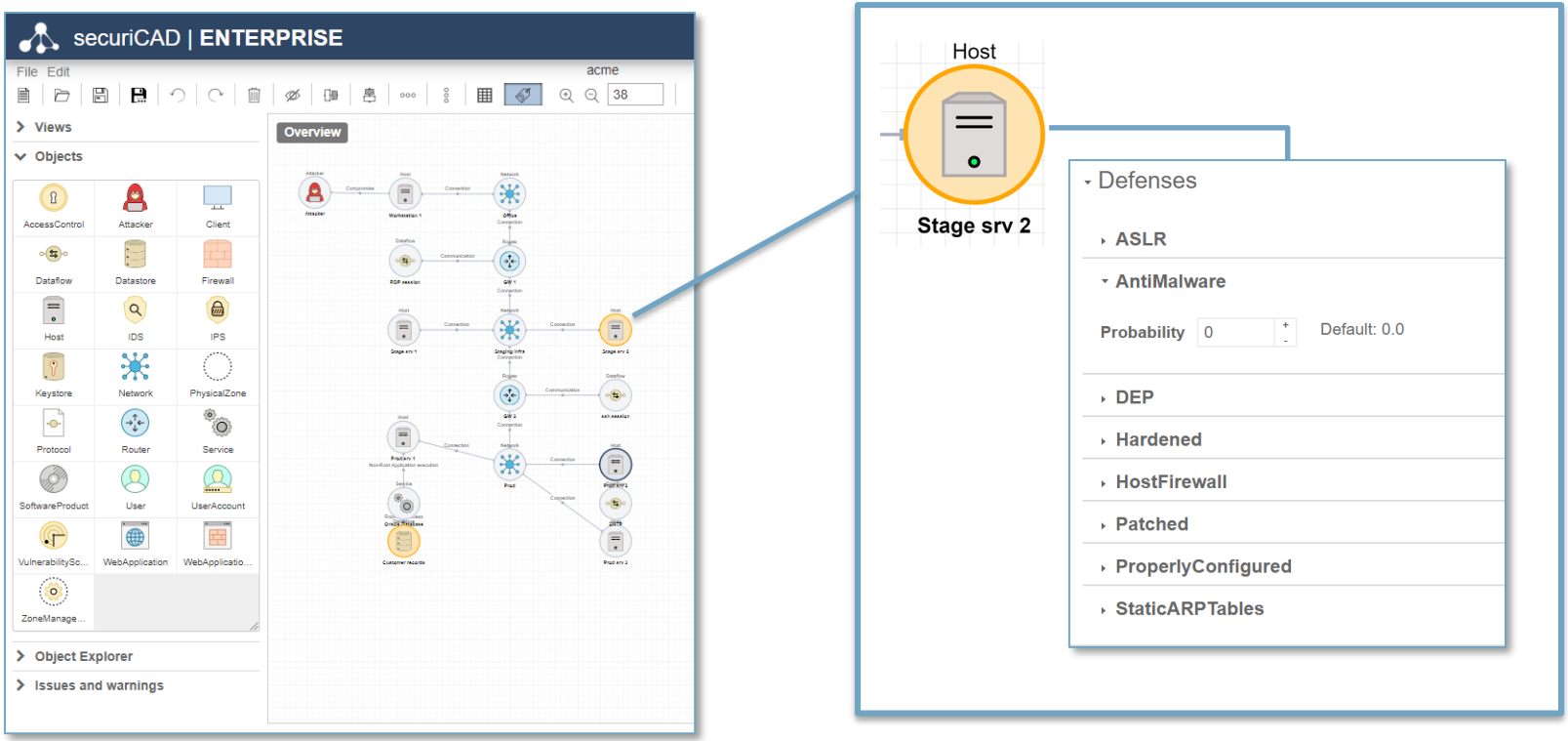
SECURICAD – RECOMMENDATIONS

- API call to fetch simulation results in json

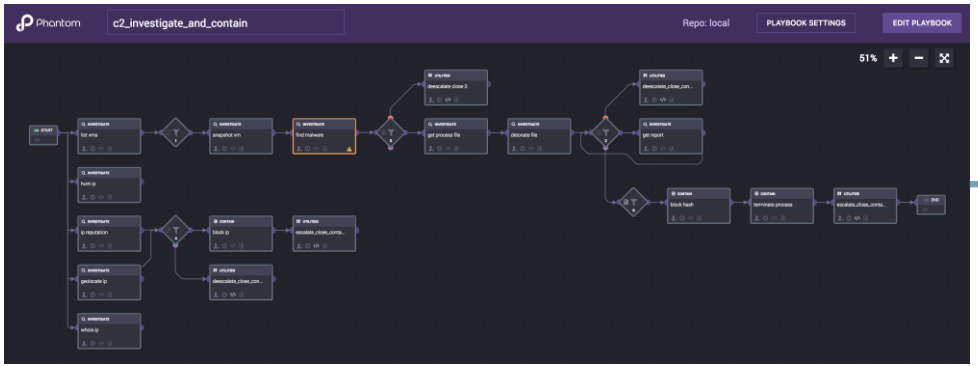


- Suggested mitigations are high-level / abstract, not all technical (e.g. train users to be security-aware)

SECURICAD – RECOMMENDATIONS



PHANTOM PLAYBOOKS & OPERATION

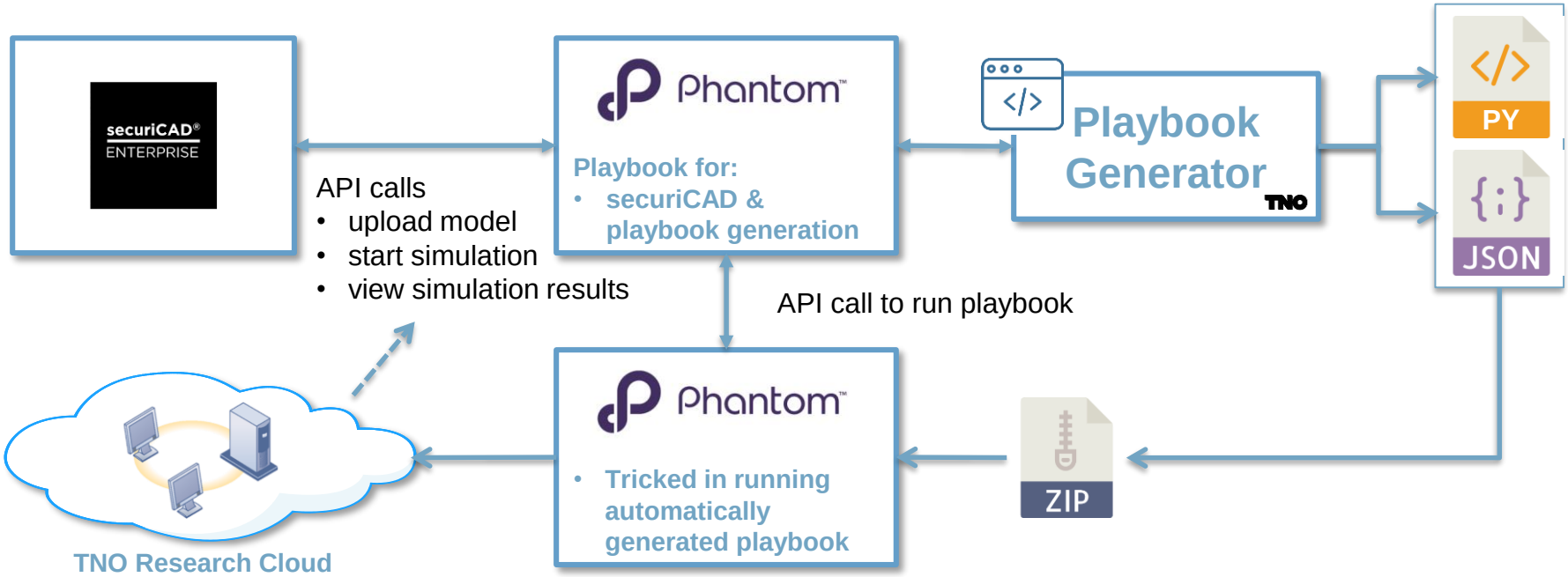


- Python functions for each of the operations in the playbook

- JSON specification of how the operations are arranged and meta data for visualisation

- We are able to generate a playbook for a recommended CoA by combining pre-defined Python code and assigning parameters for the particular case.
- Phantom does not provide an API to load a (externally) created playbooks. Phantom does have a rest API to run a playbook. We have to ‘trick’ Phantom in executing our (externally) generated playbook.

AUTOMATIC PLAYBOOK GENERATION
Tool chain



AUTOMATIC PLAYBOOK GENERATION
Conclusion

- State of the art is not yet ready for this automated response scenario
- SecuriCAD recommendation are a bit high level / abstract
- Playbooks can be automatically generated, but Phantom is not designed for this scenario

SOCCRATES has some work to do

THANK YOU FOR YOUR ATTENTION
Take a look:
TIME.TNO.NL
TNO innovation for life