Attack Defense Graph analysis for supporting SOC and CSIRT operations

Frank Fransen – Senior Scientist at TNO, NL

Erik Ringdahl – Product Director at foreseeti, SE

SOCCRATES

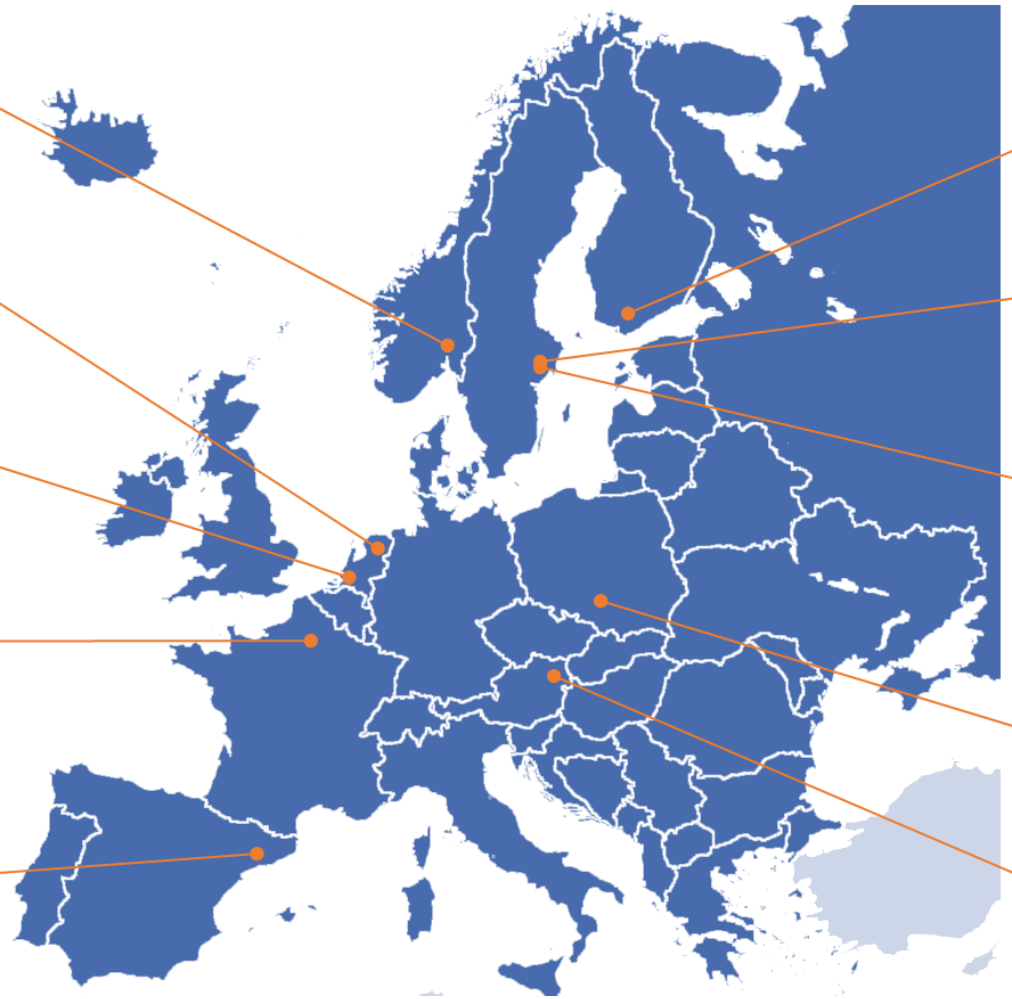
SOC & **C**SIRT **R**esponse to **A**ttacks & **T**hreats
based on attack defence graphs **E**valuation **S**ystems

Project details

Call type	Innovation Action
Call ID/Topic	H2020 SU-ICT-01-2018
Start date	September 1st, 2019
EU funding	€ 5M
Coordinator	TNO, The Netherlands
Website	www.soccrates.eu

SOCCRATES CONSORTIUM

SOCCRATES



mnemonic
Securing your business.

TNO innovation for life

SHADOWSERVER

Institut Mines-Télécom

TELECOM SudParis
Une école de l'IMT

Atos

F-Secure

KTH VETENSKAP OCH KONST

foreseeti

VATTENFALL

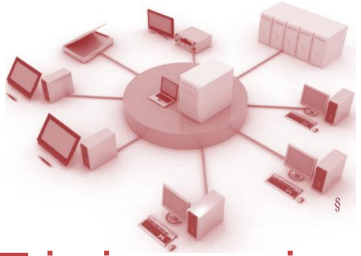
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

BACKGROUND

SOCCRATES

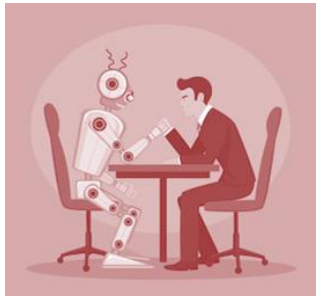
"But the cybersecurity community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in security investments, it has also brought new records in cyber-attacks of all kinds, data breaches, and information loss. From this perspective, one may argue 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



ICT is increasingly complex, changing & interdependent

Increasing number and complexity of attacks



Attacks get more automated, response is human-centered

Shortage of skilled cybersecurity staff

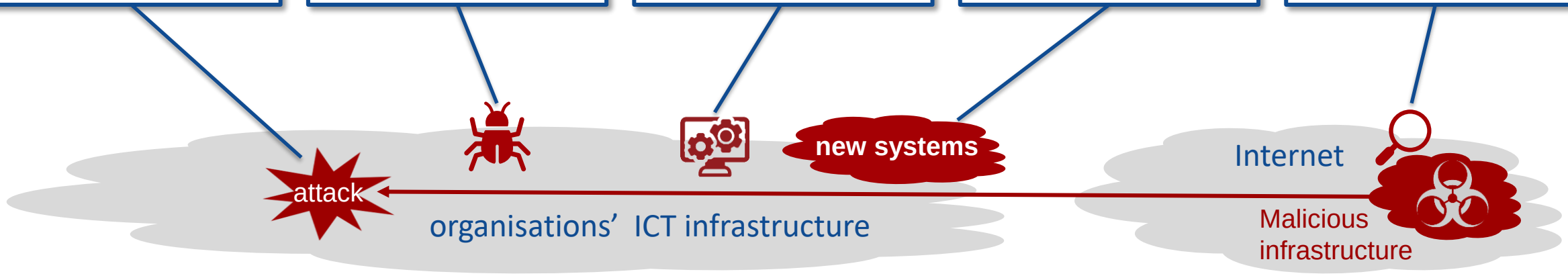
PROJECT OBJECTIVE

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

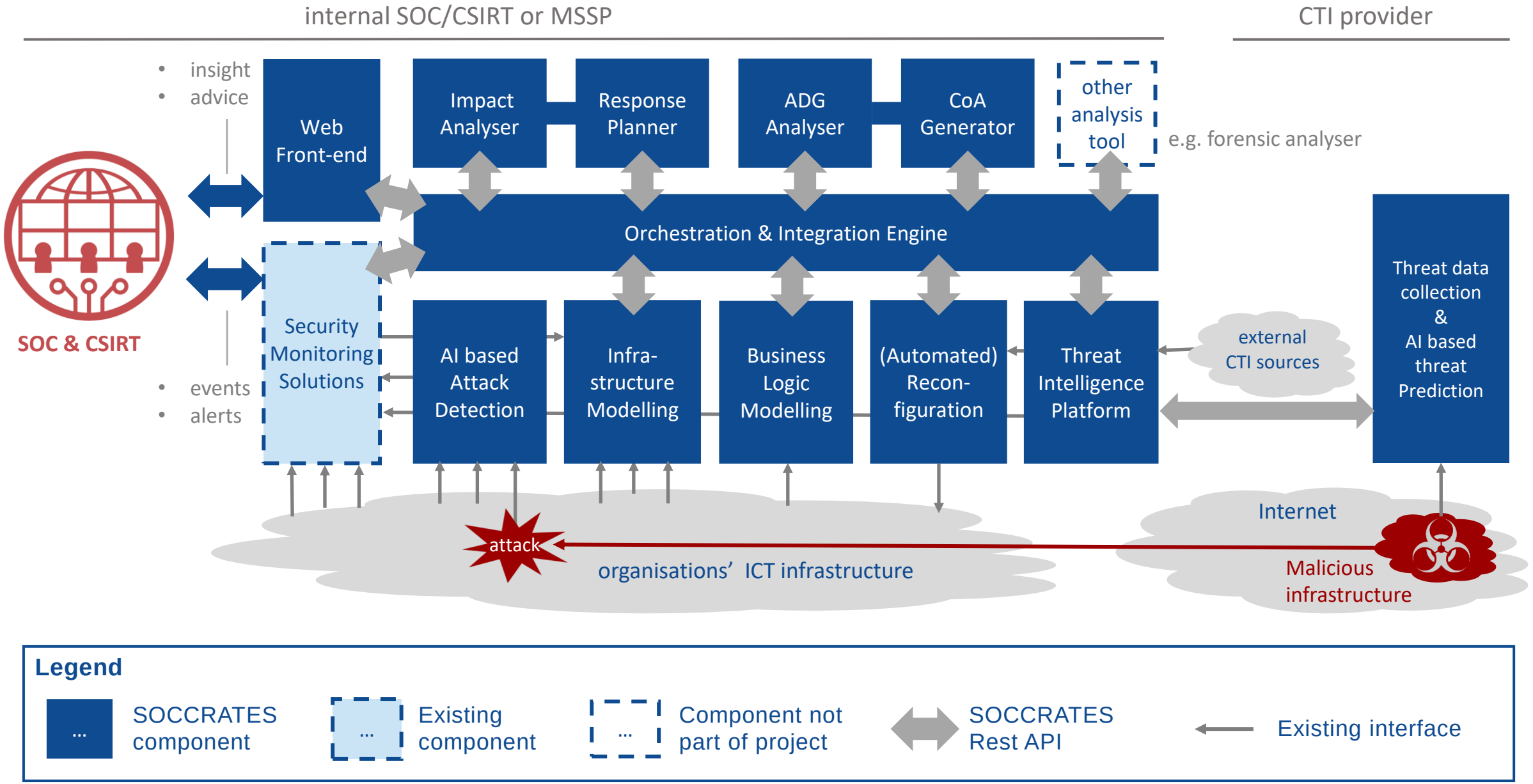
SOCCRATES Use Cases

SOCCRATES

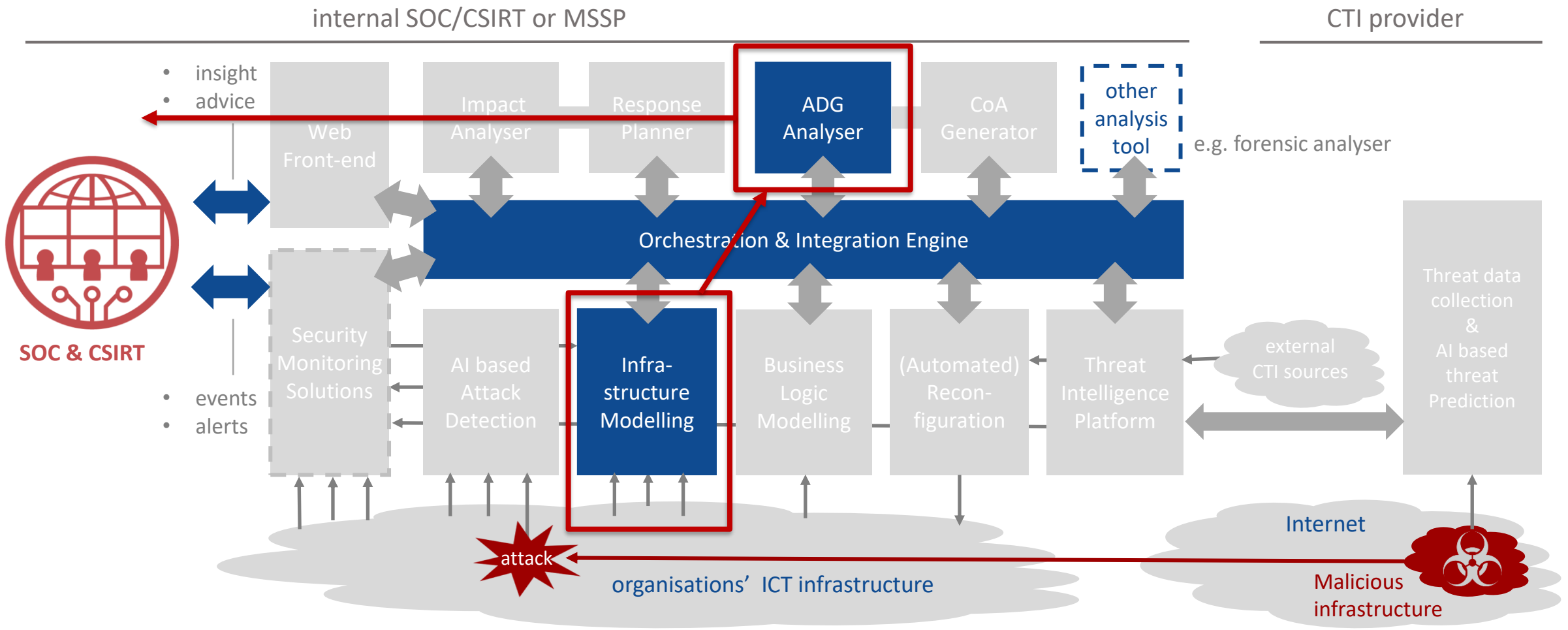
Use Case 1	Use Case 3	Use Case 4	Use Case 5	Use Case 2
Response on Detected Ongoing Attack	***Response on Discovery of New Vulnerable Assets***	***Response on Discovery of System Configuration Change***	***Response on Deployment of New Systems in Infrastructure***	***Response on Reception of New Cyber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



SOCCRATES Component Architecture



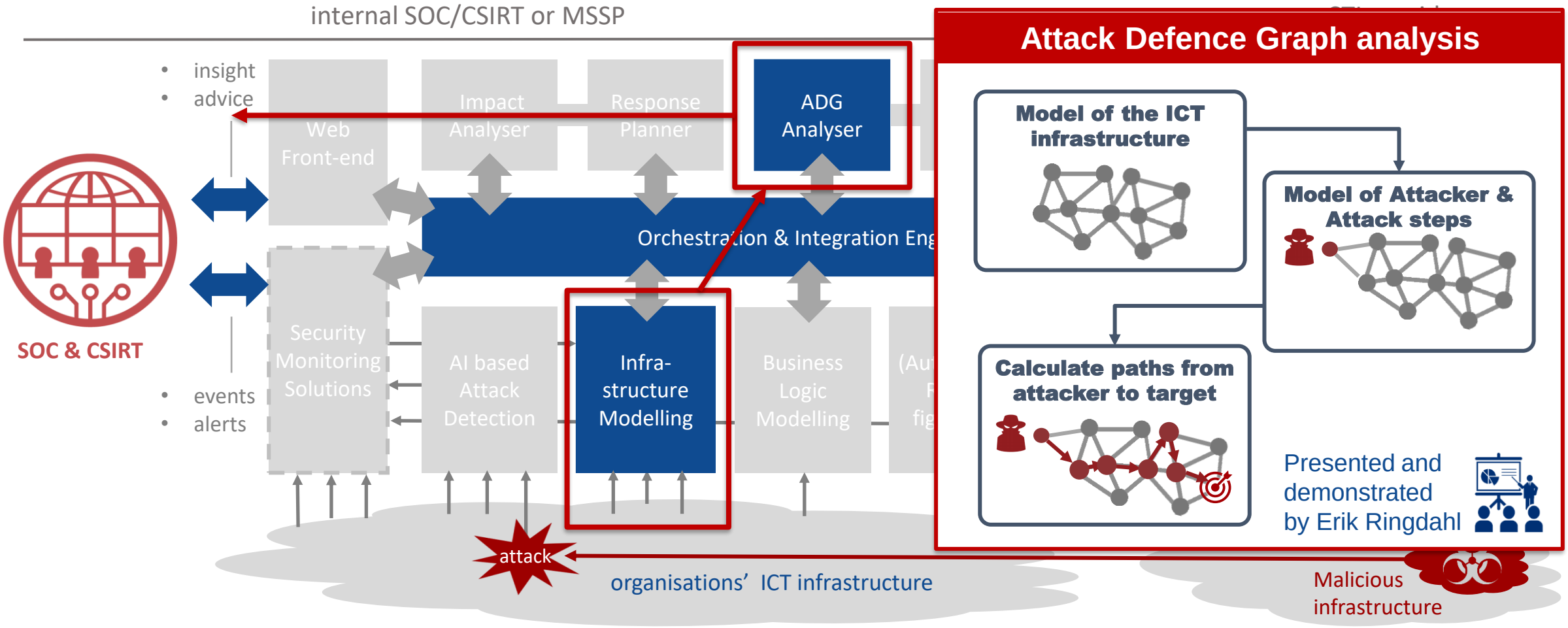
SOCCRATES Component Architecture



Legend

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

SOCCRATES Component Architecture



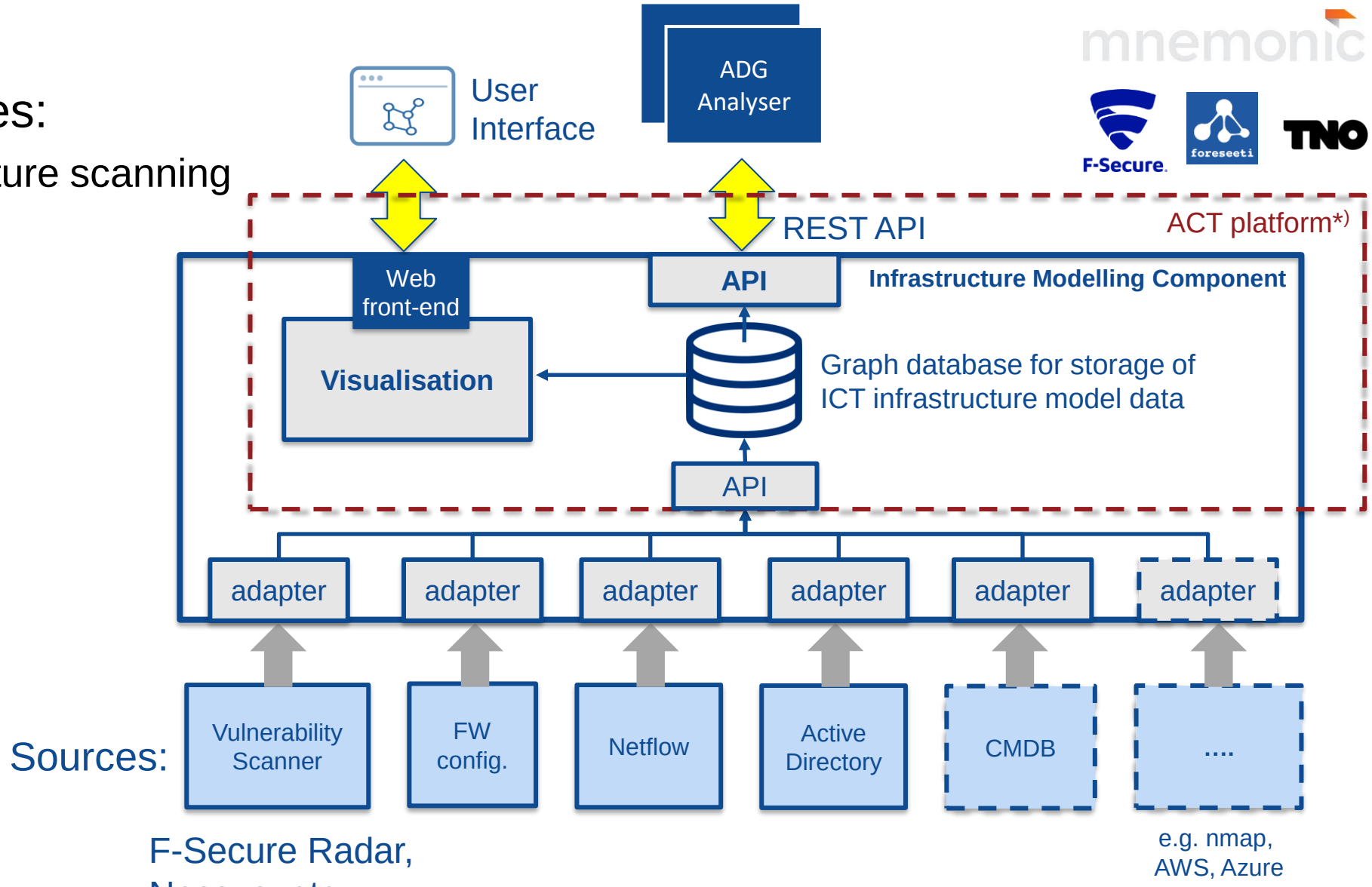
Legend

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

Infrastructure Modelling Component

The main capabilities:

- Automated infrastructure scanning
- Continuous updates
- Normalizes raw data
- Time dimension
- Extendable model
- Multi-organization



*) https://github.com/mnemonic-no/act-platform

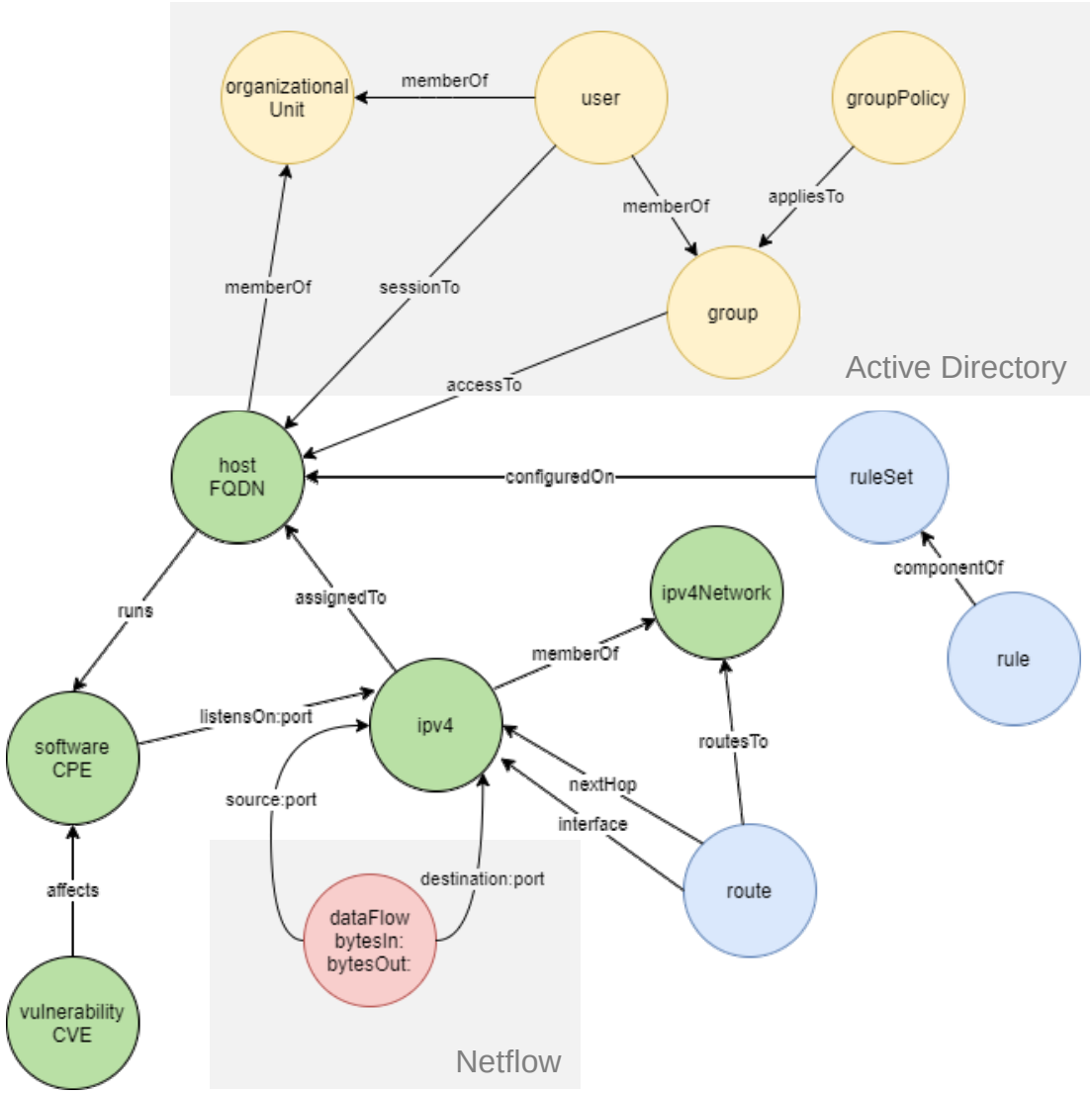
Infrastructure Modelling Component

Initial data objects are:

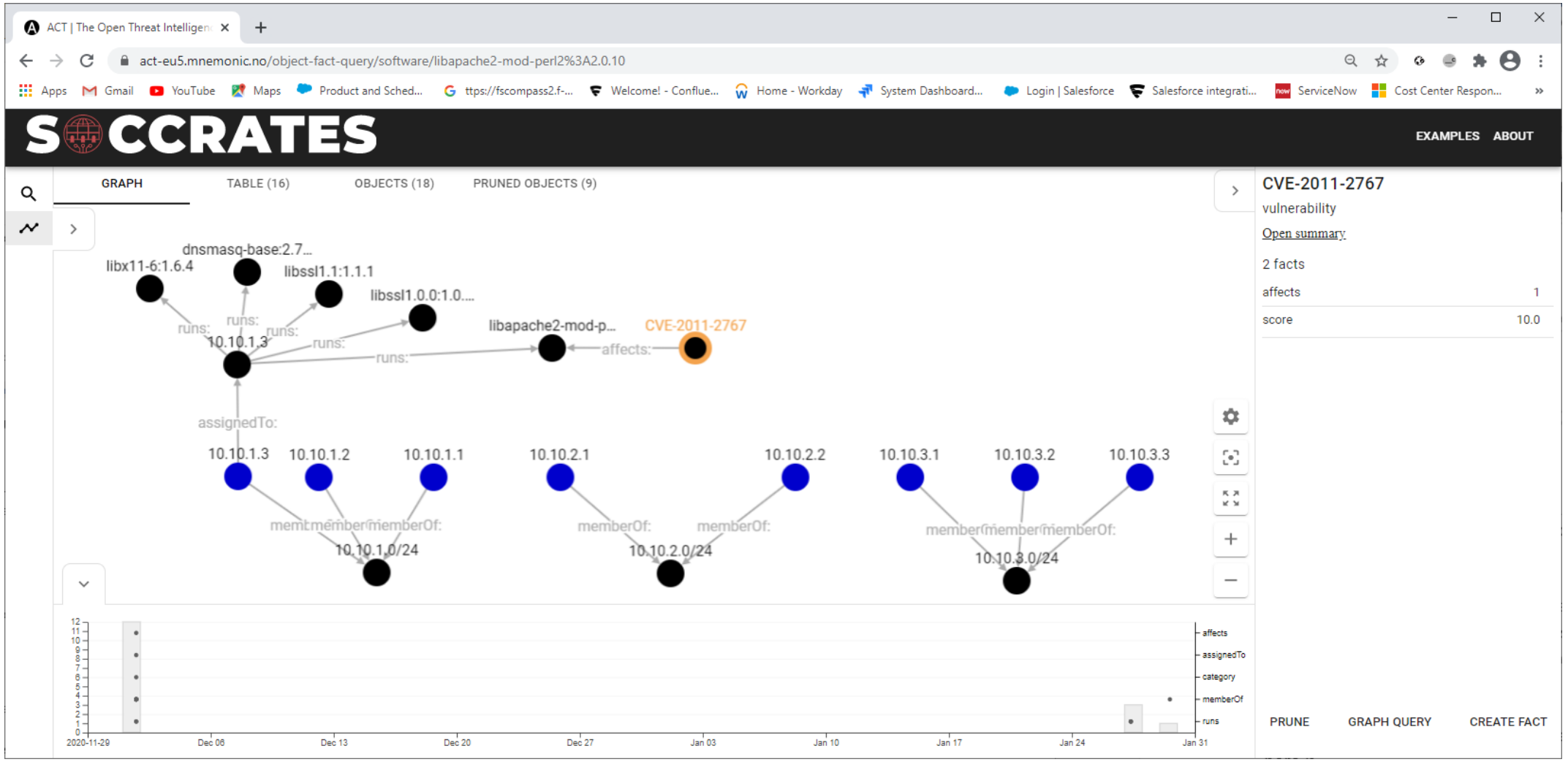
- **Host** - FQDN and related IPv4 addresses
- **Software** - CPE when available, or library name and version; may have open network port(s).
- **Vulnerability** - CVE ID.
- **IPv4 Network** - network segment (e.g. 192.168.0.0/24).
- **Route** is network route between IPv4 Networks
- **Firewall ruleset** limits the network traffic passed through the route

Extension:

- **Active Directory** data
- **Netflow**



Infrastructure Modelling Component

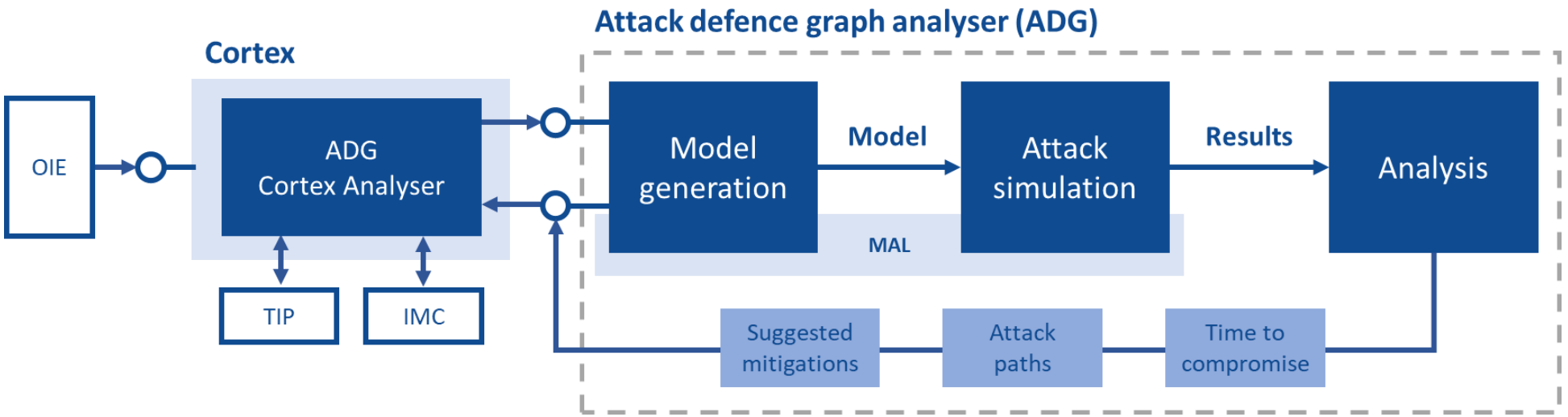


Attack defense graph analyser (ADG)

ADG OVERVIEW

SOCCRATES

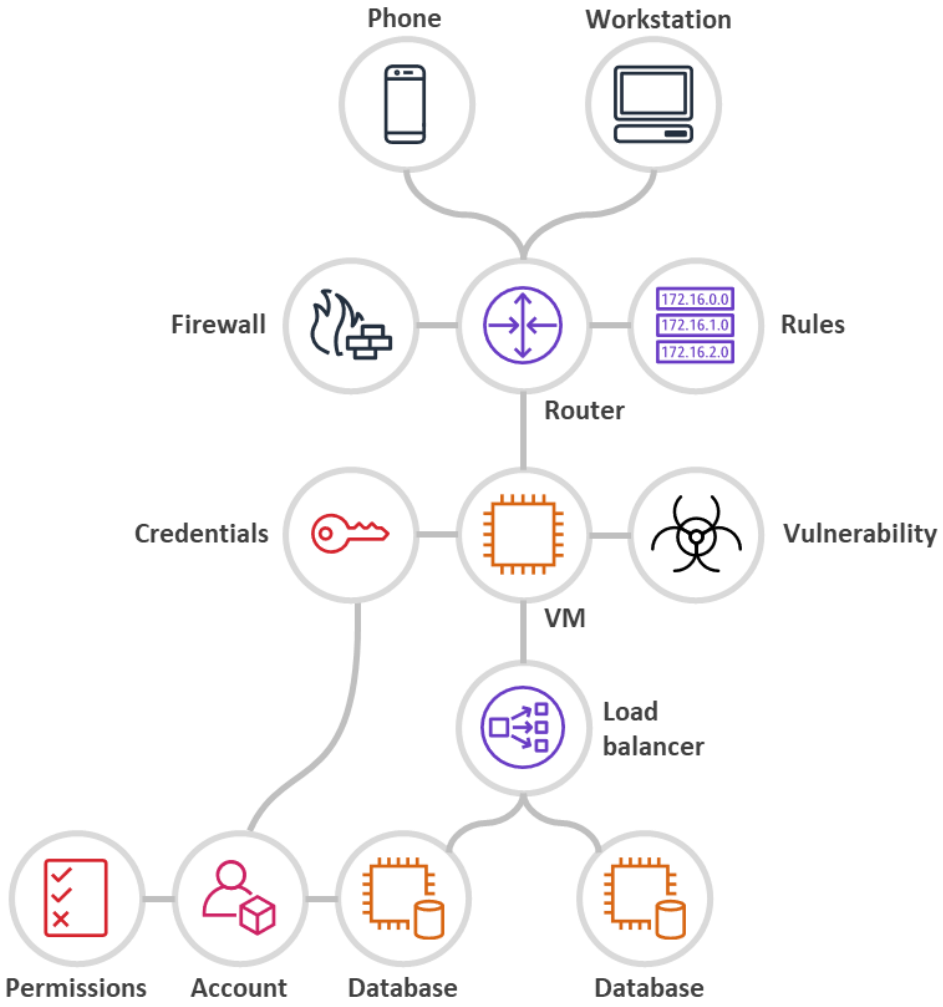
- Perform attack simulations to predict how attacks might propagate in a given infrastructure
- Quantify the probability of a successful attack and attack path with regards to:
  - Current infrastructure and security configuration, changes to the infrastructure, new vulnerabilities or applied mitigations
  - New threat intelligence, threat actors and probable causes and effects of given IOCs



MODEL GENERATION

SOCCRATES

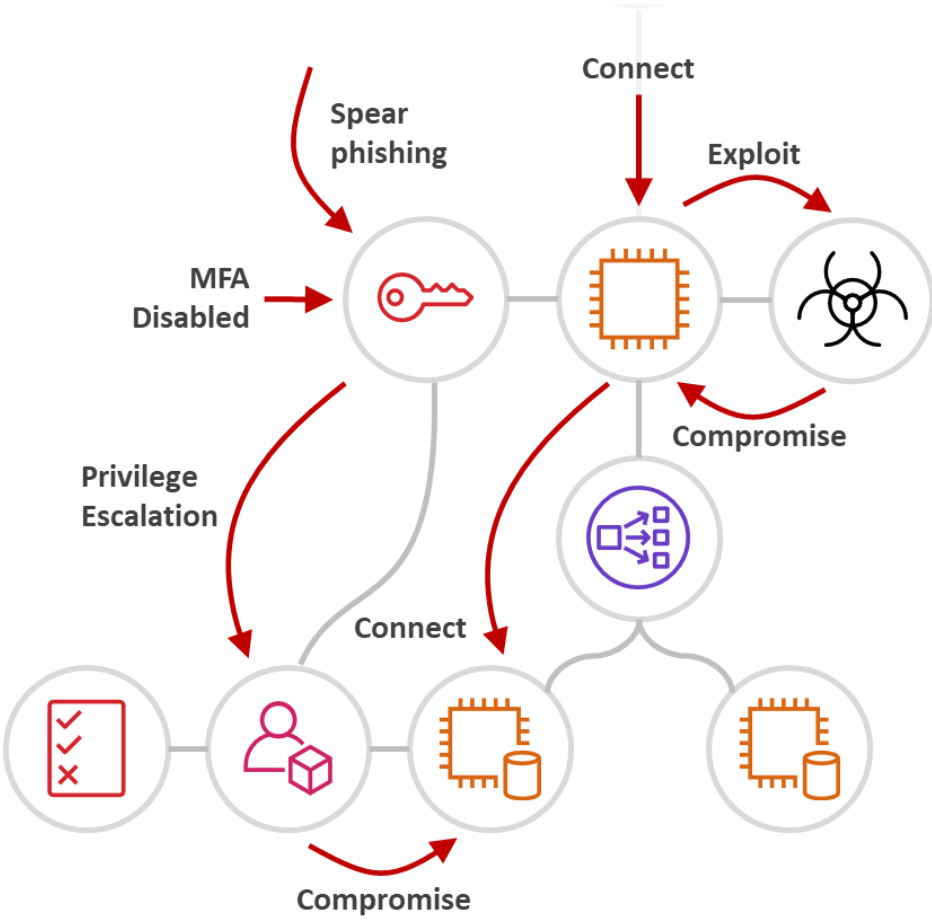
- Models are **generated automatically based on available data**
- Models contains information about everything from users and their security awareness to the technical properties of an application. Defined in MAL.
- Uncertainty can be accounted for with probability of existence and **assumptions and approximations can be made to represent various scenarios**



ATTACK SIMULATIONS

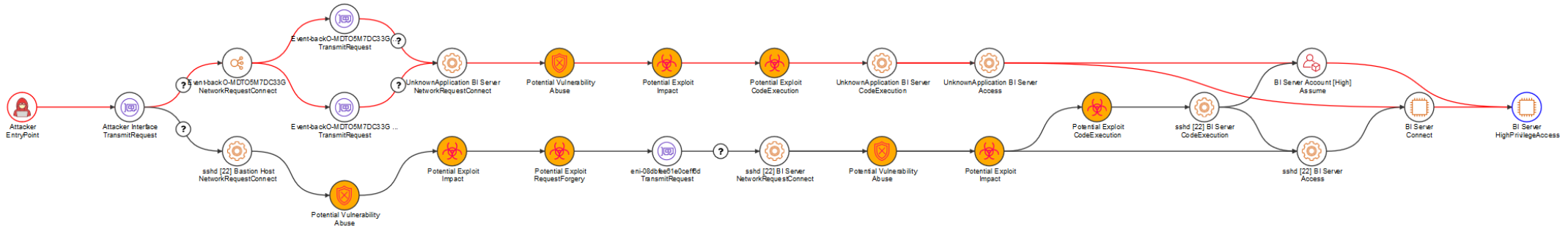
SOCCRATES

- An attacker is placed is in the model to represent the entry point and **given capabilities based on threat intelligence**
- securiCAD simulates attacks on models by using probabilistic inference with Monte Carlo simulations and shortest path calculations
- All attack logic and probabilities are built-in and can be **tailored to specific threat actors and scenarios**
- **Quantifies the probability** of successful attacks in TTC (Time-to-compromise)



ANALYSIS

- Based on the simulation, reports will be generated on probable attack exposure, weaknesses, **impact and critical attack paths to high value assets**
- Critical paths exposes weaknesses, misconfigurations, chokepoints, exploited vulnerabilities and potential mitigations
- **Suggested security controls** will also be provided that can lower the risk exposure which can be applied and evaluated in the model



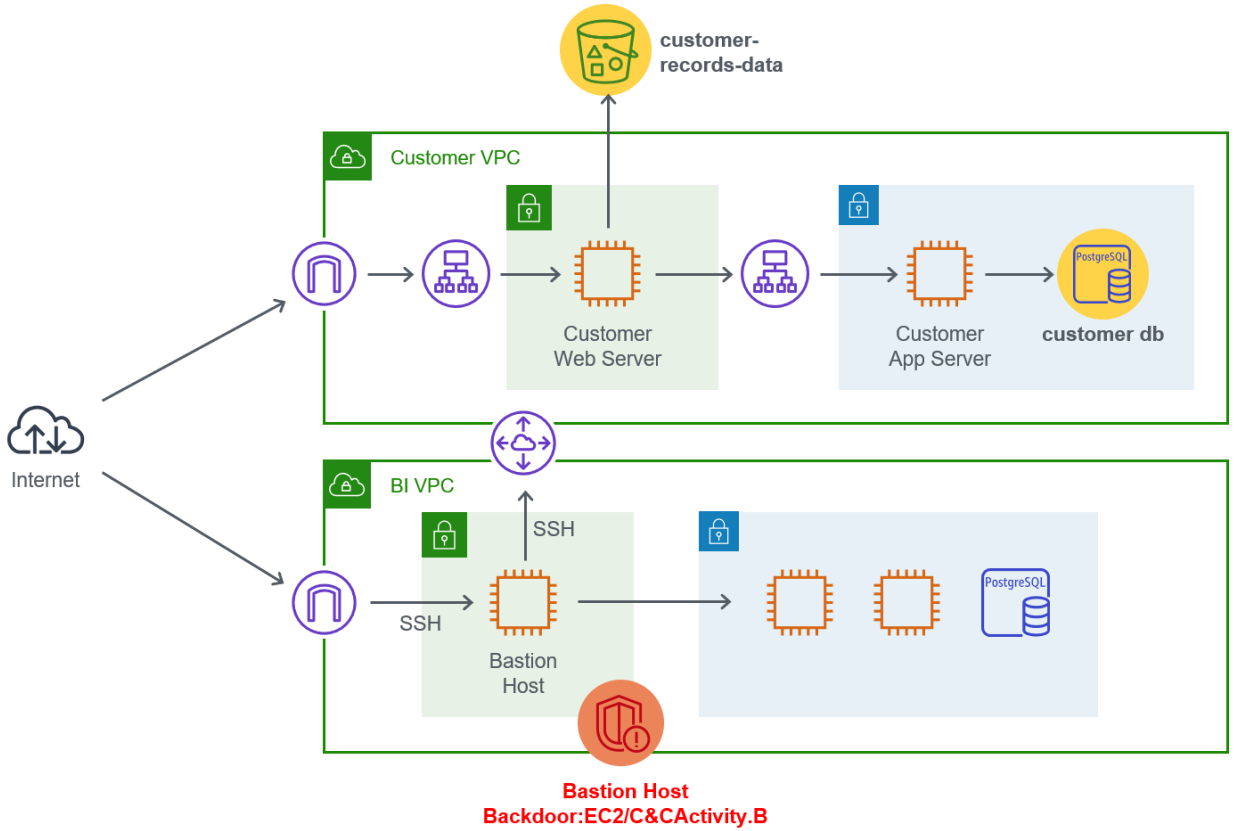
DEMO ENVIRONMENT

SOCCRATES

- Live demo of securiCAD and the ADG functionality

- **Case:**
  - AWS environment with sensitive customer data
  - Command & Control activity detected on Bastion Host

- **Demo:**
  - Impact on and paths to high value assets
  - Attack paths to Bastion Host
  - Top threats and suggested mitigations



Backdoor:EC2/C&CActivity.B
An EC2 instance is querying an IP that is associated with a known command and control server.
This finding informs you that the listed instance within your AWS environment is querying an IP associated with a known command and control (C&C) server […] ***your instance is likely compromised***

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-ec2.html#backdoor-ec2-ccactivityb

Live demo

LINKS AND MORE INFO

SOCCRATES

- Try out the Meta Attack Language (MAL)
  - https://mal-lang.org/
- Try out securiCAD
  - https://github.com/foreseeti/securicad-enterprise-sdk
- ADG and IMC webinar
  - https://www.soccrates.eu/webinars/infrastructure-modelling-adg-analysis/

CONCLUDING REMARKS

SOCCRATES

- Automated threat modeling and attack simulation are beneficial for SOC and CSIRT operations
  - increased speed of operations, and
  - facilitate informed decisions.
- SOCCRATES will pilot the platform in 1st half of 2022.
- Most components will be open sourced
  - some are already open source
  - follow us on www.soccrates.eu or on twitter and linkedin

Contacts

Questions?

Erik Ringdahl
Product director
erik.ringdahl@foreseeti.com

Frank Fransen
Senior Scientist
frank.fransen@tno.nl

www.soccrates.eu
https://www.linkedin.com/groups/13786643/
Twitter: @soccrates_eu