SOCCRATES: Automated Security Decision Support for SOCs and CSIRTs

Martin Eian (mnemonic, NO)
Frank Fransen (TNO, NL)

TLP: CLEAR
**SOC & CSIRT Response to Attacks & Threats based on attack defence graphs Evaluation Systems**

<table>
<thead>
<tr>
<th><strong>Project details</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Call type</strong></td>
<td>Innovation Action</td>
</tr>
<tr>
<td><strong>Call ID/Topic</strong></td>
<td>H2020 SU-ICT-01-2018</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>Sept. 2019 – Oct. 2022</td>
</tr>
<tr>
<td><strong>EU funding</strong></td>
<td>€ 5M</td>
</tr>
<tr>
<td><strong>Coordinator</strong></td>
<td>TNO, The Netherlands</td>
</tr>
<tr>
<td><strong>Website</strong></td>
<td><a href="http://www.soccrates.eu">www.soccrates.eu</a></td>
</tr>
</tbody>
</table>
Develop and implement a security automation and decision support platform that enhances the effectiveness of SOC and CSIRT operations.
SOCRATES Use Cases

Use Case 1
Response on Detected Ongoing Attack

Use Case 3
Response on Discovery of New Vulnerable Assets

Use Case 4
Response on Discovery of System Configuration Change

Use Case 5
Response on Deployment of New Systems in Infrastructure

Use Case 2
Response on Reception of New Cyber Threat Intelligence

Internet
Malicious infrastructure
new systems
organisations’ ICT infrastructure
attack
SOCCRATES Use Cases – different view

increase **cyber resilience** (UC2 - UC5)
remove vulnerabilities & mitigate threats

imbue with **new systems**
ICT infrastructure changes
vulnerabilities
threat intelligence

**ongoing attack**
active adversary

**improve incident response** (UC1)

**attack**

**direct enforceable CoAs**

**CAUTION**
cyberattack in progress

**post incident improvements**

**Threat Response / Remedy CoA**

**Attack Response CoA**
SOCRATES Use Cases – General Flow

Human-in-the-loop

Monitoring Phase

Analysis Phase

Mitigation & Response Planning Phase

Mitigation & Response Execution Phase

situational awareness

option awareness

Attack

CoA

Human-in-the-loop
AI based Attack Detection

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

Face to face

Malicious
infrastructure

external CTI sources

Malicious
infrastructure

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

SOC & CSIRT

Malicious
infrastructure

Security Monitoring Solutions

• insight
• advice

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts

Web Front-end

Impact Analyser

Response Planner

ADG Analyser

CoA Generator

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat data collection & AI based threat Prediction

CTI provider

Orchestration & Integration Engine

Internet

Malicious infrastructure

Threat Intelligence Platform

Response Planner

ADG Analyser

CoA Generator

other analysis tool

e.g. forensic analyser

Security Monitoring Solutions

• events
• alerts
MAIN INNOVATIONS

internal SOC/CSIRT or MSSP

- insight
- advice
- Web Front-end
- Impact Analyser
- Response Planner
- ADG Analyser
- CoA Generator

CTI provider

other analysis tool

- e.g. forensic analyser
- Threat data collection & AI based threat prediction

SOC & CSIRT

- events
- alerts
- Security Monitoring Solutions
- AI based Attack Detection
- Business Logic Modelling
- (Automated) Reconfiguration
- Threat Intelligence Platform

Orchestration & Integration Engine

Infra-structure Modelling

- Actual machine-readable model of the infrastructure

Malicious infrastructure

Internet

June 5th, 2023
MAIN INNOVATIONS

internal SOC/CSIRT or MSSP

- Web Front-end
- Security Monitoring Solutions
- AI based Attack Detection
- Infra-structure Modelling
- Business Logic Modelling
- (Automated) Reconfiguration
- Threat Intelligence Platform

Orchestration & Integration Engine

- Impact Analyser
- ADG Analyser

Response Planner

CoA Generator

CTI provider

- other analysis tool
  e.g. forensic analyser

- Threat data collection & AI based threat Prediction

Internet

Malicious infrastructure

Automated security reasoning (Attack Simulation & Real-time Business Impact Assessment)

June 5th, 2023
Main Innovations

**SOC & CSIRT**
- Internal SOC/CSIRT or MSSP
- CTI Provider

**Orchestration & Integration Engine**
- Web Front-end
- Impact Analyser
- ADG Analyser
- CoA Generator
- Orchestration & Integration Engine

**Security Monitoring Solutions**
- AI based Attack Detection
- Infrastructure Modelling
- Business Logic Modelling
- (Automated) Recon-figuration

**Response Planner**

**Impact Analyser**

**ADG Analyser**

**CoA Generator**

**External CTI Sources & AI based Threat Prediction**

**Internet**

**Malicious Infrastructure**

**Organisations’ ICT Infrastructure**

**Automated generation, assessment and execution of response actions**

June 5th, 2023
Main innovations:

- Model of the infrastructure
- Automated security reasoning
- Automated Response

Lessons learned & Take away
## Model of the Infrastructure

### What we needed

- Machine readable model of the infrastructure
- Correlate multiple data sources
- Detect changes and trigger workflows

### What we learned

- Ability to detect changes useful to SOC analysts
- Correlation is a major challenge
- Scalability in operational environments
### What we needed

- Attack simulation on the infrastructure, triggered by security event
- Real-time business impact assessment on compromised asset, or response action

### What we did

**Model of the ICT infrastructure**
- Calculate paths from attacker to target

**Business Process Model**
- Integrated Attack Defence Graph (ADG) analysis tool, called securiCAD.

**Business Impact assessment**
- Combined infrastructure model and business process model to calculate impact on the business

### What we learned

- Security Analysts: "It provides unique contextual understanding"
- Security Reasoning services need to be event-driven asynchronous
- Availability of Business Process Models not trivial
**AUTOMATED RESPONSE**

### What we needed

- Generate Courses of Action (CoAs)
- Rank CoAs (effectiveness vs business impact)
- Execute CoAs

### What we did

**CoA Generator**
- CoA Generator uses ADG tool iteratively. ⇒ *Generic countermeasures*

**Response Planner**
- Response Planner. ⇒ *Direct enforceable CoAs*

### What we learned

- Containment CoAs
- Analyst trust
- Importance of UI

---

**Diagram:**
- CACAO
- OpenC2
- SOC Proxy
- Option awareness

---

*June 5th, 2023*
OUTLINE

Introduction

Main innovations:

Model of the infrastructure → Automated security reasoning → Automated Response

Lessons learned & Take away

June 5th, 2023
LESSONS LEARNED

What we have learned about running such a large ambitious project

1. Common software development platform & best practices
   - Include performance / stress testing capability

2. Start early with setting up a realistic test environment
   - Plan sufficient time for integration

3. On-site validation
   - MSSP SOC/CSIRT

June 5th, 2023
LESSONS LEARNED

What we have learned about security automation for SOCs & CSIRTs

1. Unique contextual understanding → improve analyst decisions
   • New vulnerabilities and infrastructure changes

2. Value of structured and predefined workflows
   • Make analysts reflect on threats, events and effects

3. Analyst trust is paramount
   • All recommendations must provide clear and visible evidence

June 5th, 2023
security automation & decision support can enhance the effectiveness of SOC & CSIRT operations

www.soccrates.eu
Q&A

mnemonic

Martin Eian
meian@mnemonic.no

TNO

Frank Fransen
frank.fransen@tno.nl

www.soccrates.eu