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

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
### Session I  
*(Session Chair: Ewa Piatkowska)*

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:20</td>
<td>The SOCCRATES Project: Motivation and Aims</td>
<td>Reinder Wolthuis (TNO)</td>
</tr>
<tr>
<td>15:40</td>
<td>ACT: Cyber Threat Intelligence Platform</td>
<td>Siri Bromander (Mnemonic)</td>
</tr>
<tr>
<td>16:00</td>
<td>Threat modelling and attack simulations with MAL and securiCAD</td>
<td>Erik Ringdahl (Foreseeti)</td>
</tr>
<tr>
<td>16:20</td>
<td>Automated Response based on securiCAD recommendations</td>
<td>Frank Fransen (TNO)</td>
</tr>
<tr>
<td></td>
<td><strong>Coffee Break</strong></td>
<td></td>
</tr>
<tr>
<td>17:00</td>
<td>Anomaly Detection (DNS Ninja &amp; ABC tool)</td>
<td>Irina Chiscop (TNO)</td>
</tr>
<tr>
<td>17:20</td>
<td>Adversarial Machine Learning</td>
<td>Ewa Piatkowska (AIT)</td>
</tr>
<tr>
<td>17:40</td>
<td>Open Discussion: Future Challenges for SOCs</td>
<td>Moderator: Paul Smith (AIT)</td>
</tr>
<tr>
<td>18:20</td>
<td>Conclusions and Wrap Up</td>
<td>Reinder Wolthuis (TNO)</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Call type</th>
<th>Innovation Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call ID/Topic</td>
<td>SU-ICT-01-2018</td>
</tr>
<tr>
<td>Start date</td>
<td>September 1&lt;sup&gt;st&lt;/sup&gt; 2019</td>
</tr>
<tr>
<td>Project duration</td>
<td>3 years</td>
</tr>
<tr>
<td>Budget</td>
<td>€ 5.9M</td>
</tr>
<tr>
<td>EU funding</td>
<td>€ 5M</td>
</tr>
<tr>
<td>Coordinator</td>
<td>TNO, The Netherlands</td>
</tr>
</tbody>
</table>
Consortium & Stakeholders

With support of:
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

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

organisations' ICT infrastructure  
new systems  
Malicious infrastructure  
Internet
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

Utilization of CTI for incident detection, analysis & response, incl. attribution and threat actor profiling.

Legend:
- SOCCRATES component
- Existing component
- Component not part of project
- SOCCRATES Rest API
- Existing interface
Identification of attack trends based on malicious infrastructure data and malware analysis data using advanced data analytics (incl. AI and deep learning).
Automated asset discovery & modelling of the ICT infrastructure; machine readable description of an ICT infrastructure.

Attack Defence Graph (ADG) based analysis of emerging threat and ongoing attacks, and determining the best response to these threats and attacks.
Quantify business impact of a threat or attack, and trade-off analysis on response actions.

Business logic data collection & modelling for business impact analysis.
SOCCRATES Component Architecture

Integrates, manages and orchestrates the different components of the platform & Playbook driven orchestration of the five SOCRATES use cases.
SOCCRATES Component Architecture

Integrated front-end for providing insight and advise to SOC analyst: Situational awareness, Option awareness.

Legend:
- ... SOCCRATES component
- ... Existing component
- ... Component not part of project
- SOCCRATES Rest API
Interfaces with the security controls and other functions in infrastructure to (semi-) automatically execute response actions to mitigate a threat or attack.
<table>
<thead>
<tr>
<th>Pilot</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate SOC</td>
<td>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.</td>
</tr>
<tr>
<td>MSSP</td>
<td>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.</td>
</tr>
<tr>
<td>Threat Prediction</td>
<td>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.</td>
</tr>
</tbody>
</table>
SOCCERATES HIGH LEVEL PLANNING

- **Innovation Phase 1**
- **Innovation Phase 2**

- **Phase 1 implementation & test**
- **First pilot**

- **Phase 2 implementation & test**
- **Second pilot**

- **Demo-pilot preparation**
- **Demo-pilot**

- **Final SOCCERATES Event and demo**
<table>
<thead>
<tr>
<th>SOCCRATES Stakeholder Group</th>
<th>SOCCRATES Advisory Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andy de Petter</td>
<td>Head of cyber security intelligence &amp; incident response</td>
</tr>
<tr>
<td>Frode Hommedal</td>
<td>Technical Director Cyber Threat Detection and Response</td>
</tr>
<tr>
<td>Dr. Judith E.Y. Rossebo</td>
<td>Specialist cyber security &amp; infrastructure</td>
</tr>
<tr>
<td>Martin Pekarek</td>
<td>Cybersecurity advisor National Cyber Security Center</td>
</tr>
<tr>
<td>Room for additional members!</td>
<td></td>
</tr>
</tbody>
</table>
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