



# Call for Papers

## 3<sup>rd</sup> International Workshop on Next Generation Security Operations Centers (NG-SOC 2021)

to be held in conjunction with the 16<sup>th</sup> International Conference on Availability, Reliability and Security (ARES 2021 – <http://www.ares-conference.eu>)

**August 17 – August 20, 2021**

**All-digital Conference**

### Workshop Description

Organisations in Europe face the difficult task of detecting and responding to increasing numbers of cyber-attacks and threats, given that their own ICT infrastructures are complex, constantly changing (e.g. by the introduction of new technologies) and there is a shortage of qualified cybersecurity experts. There is a great need to drastically reduce the time to detect and respond to cyber-attacks. A key means for organizations to stay ahead of the threat is through the establishment of a Security Operations Center (SOC). The primary purpose of a SOC is to monitor, assess and defend the information assets of an enterprise, both on a technical and organizational level.

The aim of this workshop is to create a forum for researchers and practitioners to discuss the challenges associated with SOC operations and focus on research contributions that can be applied to address these challenges. Through cooperation among H2020 European projects, the workshop intends to provide a more comprehensive overview of the promising research-based solutions that enable timely response to emerging threats and support different aspects of the security analysis and recovery process.

The workshop is jointly organized by two H2020 projects: SOCCRATES (<https://www.soccrates.eu/>) and SAPPAN (<https://sappan-project.eu/>).

### Topics of interest include, but are not limited to:

- Collaborative Incident Response and Recovery
- Machine Learning for Security and Privacy
- Intrusion Detection
- Network Security
- Standardization and Sharing of Cybersecurity Knowledge
- Endpoint Security
- Privacy Aspects of Sharing in Cybersecurity
- Cyber Threat Intelligence Utilization
- Situation Awareness and Decision Support Tools for SOC
- Novel Visualization Tools and Approaches for SOC
- Security of Machine Learning
- Attacks against Deep Learning (e.g. Adversarial Examples)
- Malware Identification and Analysis
- Vulnerability Discovery



- Digital Forensics and Attack Attribution
- Natural Language Processing (NLP) for Security
- Threat Trend Modelling and Prediction
- Attack and Defence Modelling
- Host Behaviour Profiling
- User Behaviour Analytics (UBA)
- Advanced Persistent Threat Detection and Analysis
- Security Event Fusion, Correlation and Severity Analysis

## Important Dates

Submission Deadline	 <b>extended to May 7, 2021</b> <del>April 30, 2021</del>
Author Notification	 <b>May 31, 2021</b>
Proceedings Version	 <b>June 13, 2021</b>
ARES EU Symposium	 <b>August 17, 2021</b>
Conference	 <b>August 17 – August 20, 2021</b>

## Submission Guidelines

The submission guidelines valid for the workshop are the same as for the ARES conference. They can be found at <https://www.ares-conference.eu/conference/submission/>.

## Program Committee

Ville Alkkiomäki, F-Secure, Finland  
Manos Athanatos, FORTH-ICS, Greece  
Mathias Ekstedt, KTH, Sweden  
Muriel Figueredo Franco, University of Zurich UZH, Switzerland  
Frank Fransen, TNO, The Netherlands  
Leandros Maglaras, De Montfort University, Leicester, UK  
Preetam Mukherjee, KTH, Sweden  
Dimitrios Serpanos, Industrial Systems Institute, Greece  
Edward Staddon, INRIA, France  
Daniel Tovarnak, Masaryk University, Czech Republic  
Ruben Trapero, ATOS, Spain  
Petr Velan, Masaryk University, Czech Republic  
Daniel Weber, LRZ, Germany  
Markus Wurzenberger, AIT Austrian Institute of Technology, Austria  
Martin Zadnik, CESNET, Czech Republic

## Workshop Chairs

Irina Chiscop, TNO, Netherlands  
Tomas Jirsik, Masaryk University, Brno, Czech Republic  
Avikarsha Mandal, Fraunhofer FIT, Aachen, Germany  
Ewa Piatkowska, AIT Austrian Institute of Technology, Austria