ARES Conference
International Conference on Availability, Reliability and Security

International Workshop on Next Generation Security Operations Centers (NG-SOC 2021)

held in conjunction with the
16th International Conference on Availability, Reliability and Security (ARES 2021)
https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2021/

Workshop Agenda (Tuesday, 17th of August 2020 | 13:45 – 18:45)

Time		Talk	Duration [min]
13:45	14:00	Welcome and Workshop Overview *Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)*	15
Session 1 *Session Chair: Irina Chiscop (TNO, Netherlands)*			60
14:00	14:20	System for Continuous Collection of Contextual Information for Network Security Management and Incident Handling *Martin Husák (Masaryk University, Czechia),* *Martin Laštovička (Masaryk University, Czechia), and* *Daniel Tovarňák (Masaryk University, Czechia)*	20
14:20	14:40	On the Evaluation of Sequential Machine Learning for Network Intrusion Detection *Andrea Corsini (University of Modena and Reggio Emilia, Italy),* *Shanchieh Jay Yang (Rochester Institute of Technology, USA) and* *Giovanni Apruzzese (University of Liechtenstein, Liechtenstein)*	20
14:40	15:00	A Recommender System for Tracking Vulnerabilities *Philip Huff (University of Arkansas, USA),* *Kylie McClanahan (University of Arkansas, USA),* *Thao Le (Bastazo, Inc., USA), and* *Qinghua Li (University of Arkansas, USA)*	20
15:00	15:30	*Coffee break*	30
Session 2 *Session Chair: Tomáš Jirsík (Masaryk University, Czechia)*			80
15:30	16:10	**Keynote: Title (TBD)** Frode Hommedal, *Chief Technology Officer and head of Cyber Threat Operations (Defendable, Norway)*	30 +10 Q&A
16:10	16:30	Combining anomaly detection models for more reliable attack detection *Dmitriy Komashinskiy (F-Secure, Finland)*	20
16:30	16:50	Quantitative Impact Analysis *Christophe Kiennert (Télécom SudParis, France)*	20
16:50	17:15	*Coffee break*	25

Session 3 *Session Chair: Avikarsha Mandal (Fraunhofer FIT, Germany)*			80
17:15	17:35	Adversary Emulation Planner: Generating MITRE ATT&CK Technique Sequences *Martin Eian (mnemonic, Norway)*	20
17:35	17:55	Graph-based Network Traffic Analysis for Incident Investigation *Milan Cermak (Masaryk University, Czechia)*	20
17:55	18:15	Automated Infrastructure Modelling – Foundation for Security Operations *Ville Alkkiomäki (F-Secure, Finland)*	20
18:15	18:35	Taking a look at the *.ch zone with a DGA detector *Mischa Obrecht (DreamLab Technologies AG, Switzerland)*	20
18:35	18:45	Wrap Up *Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)*	10