2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018)

Scotland, United Kingdom
11-12 June 2018

IEEE

IEEE Catalog Number: CFP18C12-POD
ISBN: 978-1-5386-4566-6

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18C12-POD
ISBN (Print-On-Demand):	978-1-5386-4566-6
ISBN (Online):	978-1-5386-4565-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Contents

Sponsor / Technical Co-Sponsor (TCS) / Partnership

Preface

CyberSA 2018 Programme Committee

Invited Keynotes

Keynote Seminar 1

A Cyber Science Challenge: Evaluating Residual Risks and Propagating Harm
Professor Sadie Creese

Keynote Seminar 2

Describing a CyberSA Analysis Model
Dr Cyril Onwubiko

Keynote Seminar 3

Getting Real about the Reasons for Insecure Behaviours
Professor Karen Renaud

Keynote Seminar 4

The Challenge to Policing in Investigating Cybercrime
Detective Inspector Eamonn Keane

Keynote Seminar 5

Internet of Things – A Hacker Perspective
Associate Professor Jens Myrup Pedersen

Keynote Seminar 6

An Imposter's Journey into Infosec
Stu Hirst

CyberSA 2018 - Track 1: Adaptive Cyber Defence Operations

Chapter 1
Development and evaluation of information elements for simplified cyber-incident reports 1
Patrik Lif, Teodor Sommestad, Dennis Granåsen

Chapter 2
Towards an Adaptable System-based Classification Design for Cyber Identity 11
Mary C. (Kay) Michel and Michael C. King

Chapter 3
The Landscape of Industrial Control Systems (ICS) Devices on the Internet 13
Wei Xu, Yaodong Tao and Xin Guan

Chapter 4
Can We Evaluate the Impact of Cyber Security Information Sharing? 21
Adam Zibak and Andrew Simpson

CyberSA 2018 - Track 2: CyberSA Emerging Tools and Techniques

Chapter 5
Compound Password System for Mobile 23
Zachary Hills, David F. Arppe, Amin Ibrahim, and Khalil El-Khatib

Chapter 6
Analysis of Adversarial Movement Through Characteristics of Graph Topological Ordering 27
Nima Asadi, Aunshul Rege, and Zoran Obradovic

Chapter 7
Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools 33
Eliana Stavrou

Chapter 8
Towards Situational Awareness of Botnet Activity in the Internet of Things 37
Christopher D. McDermott, Andrei V. Petrovski, Farzan Majdani

CyberSA 2018 - Track 3: Malware Economics and Advanced Ransomware Analysis

Chapter 9
Malware Economics and its Implication to Anti-Malware Situational Awareness 45
Arun Lakhotia, Vivek Notani and Charles LeDoux

Chapter 10
Cluster analysis for deobfuscation of malware variants during ransomware attacks 53
Anthony Arrott, Arun Lakhotia, Ferenc Leitold and Charles LeDoux

Chapter 11
Cyber security: Influence of patching vulnerabilities on the decision-making of hackers and analysts 62
Zahid Maqbool, V.S. Chandrasekhar Pammi and Varun Dutt

Chapter 12
A Netnographic Study on the Dark Net Ecosystem for Ransomware 70
Yara Fareed Fahmy Bayoumy, Per H°akon Meland and Guttorm Sindre

CyberSA 2018 - Track 4: Situational Awareness, Cyber Kill Chain, Threat Intel and CyberOps
Chapter 13
CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process 78
Cyril Onwubiko

Chapter 14
Multilayer Perceptron Neural Network for Detection of Encrypted VPN Network Traffic 86
Shane Miller, Kevin Curran and Tom Lunney

Chapter 15
Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture 94
Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh, Moosung Park

Chapter 16
A Taxonomy of Malicious Traffic for Intrusion Detection Systems 102
Hanan Hindy, Elike Hodo, Ethan Bayne, Amar Seeam, Robert Atkinson and Xavier Bellekens

CyberSA 2018 - Track 5: Human Factors, Cognition, Cyber Policy and GDPR
Chapter 17
A Human Vulnerability Assessment Methodology 106
Andrea Cullen and Lorna Armitage

Chapter 18
How to Make Privacy Policies both GDPR-Compliant and Usable 108
Karen Renaud and Lynsay A. Shepherd

CIRC 2018 - Track 1: Security Metrics for Cyber Insurance and Protection
Chapter 19
Cyber Insurance and Security Interdependence: Friends or Foes? 116
Ganbayar Uuganbayar, Artsiom Yautsiukhin, and Fabio Martinelli

Chapter 20
When to Treat Security Risks with Cyber Insurance 120

Per H°akon Meland and Fredrik Seehusen

CyberSA 2018 - Track 6: Machine Learning and Blockchain in CyberSA

Chapter 21

Redesign of Gaussian Mixture Model for Efficient and Privacy-preserving Speaker Recognition 128

S Rahulamathavan, X Yao, R Yogachandran, K Cumanan, and M Rajarajan

CIRC 2018 - Track 2: Collaborative Insurance Data for Strategic Investment Risk Decisions

Chapter 22

Cyber Risk Economics Capability Gaps Research Strategy 136

Erin Kenneally, Lucien Randazzese and David Balenson

Chapter 23

Towards Integrating Insurance Data into Information Security Investment Decision Making 142

Daniel W. Woods and Andrew C. Simpson