



DataSys 2020 Congress
September 27, 2020 to October 01, 2020 - Lisbon, Portugal

- **AICT 2020**, The Sixteenth Advanced International Conference on Telecommunications
- **ICIW 2020**, The Fifteenth International Conference on Internet and Web Applications and Services
- **ICIMP 2020**, The Tenth International Conference on Internet Monitoring and Protection
- **SMART 2020**, The Ninth International Conference on Smart Cities, Systems, Devices and Technologies
- **IMMM 2020**, The Tenth International Conference on Advances in Information Mining and Management
- **INFOCOMP 2020**, The Tenth International Conference on Advanced Communications and Computation
- **MOBILITY 2020**, The Tenth International Conference on Mobile Services, Resources, and Users
- **SPWID 2020**, The Sixth International Conference on Smart Portable, Wearable, Implantable and Disability-oriented Devices and Systems
- **ACCSE 2020**, The Fifth International Conference on Advances in Computation, Communications and Services

InfoSys 2020 Congress
September 27, 2020 to October 01, 2020 - Lisbon, Portugal

- **ICNS 2020**, The Sixteenth International Conference on Networking and Services
- **ICAS 2020**, The Sixteenth International Conference on Autonomic and Autonomous Systems
- **ENERGY 2020**, The Tenth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies
- **WEB 2020**, The Eighth International Conference on Building and Exploring Web Based Environments
- **DBKDA 2020**, The Twelfth International Conference on Advances in Databases, Knowledge, and Data Applications
- **SIGNAL 2020**, The Fifth International Conference on Advances in Signal, Image and Video Processing
- **BIOTECHNO 2020**, The Twelfth International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies

SoftNet 2020 Congress
October 18, 2020 to October 22, 2020 - Porto, Portugal

- **ICSEA 2020**, The Fifteenth International Conference on Software Engineering Advances
- **ICSNC 2020**, The Fifteenth International Conference on Systems and Networks Communications
- **CENTRIC 2020**, The Thirteenth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services
- **VALID 2020**, The Twelfth International Conference on Advances in System Testing and Validation Lifecycle
- **SIMUL 2020**, The Twelfth International Conference on Advances in System Simulation
- **SOTICS 2020**, The Tenth International Conference on Social Media Technologies, Communication, and Informatics
- **INNOV 2020**, The Ninth International Conference on Communications, Computation, Networks and Technologies
- **HEALTHINFO 2020**, The Fifth International Conference on Informatics and Assistive Technologies for Health-Care, Medical Support and Wellbeing

InfoWare 2020 Congress
October 18, 2020 to October 22, 2020 - Porto, Portugal

- **ICCGI 2020**, The Fifteenth International Multi-Conference on Computing in the Global Information Technology
- **ICWMC 2020**, The Sixteenth International Conference on Wireless and Mobile Communications
- **VEHICULAR 2020**, The Ninth International Conference on Advances in Vehicular Systems, Technologies and Applications
- **INTERNET 2020**, The Twelfth International Conference on Evolving Internet
- **COLLA 2020**, The Tenth International Conference on Advanced Collaborative Networks, Systems and Applications
- **INTELL 2020**, The Ninth International Conference on Intelligent Systems and Applications
- **VISUAL 2020**, The Fifth International Conference on Applications and Systems of Visual Paradigms
- **HUSO 2020**, The Sixth International Conference on Human and Social Analytics
- **BRAININFO 2020**, The Fifth International Conference on Neuroscience and Cognitive Brain Information

NexTech 2020 Congress
October 25, 2020 to October 29, 2020 - Nice, France

- **UBICOMM 2020**, The Fourteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies
- **ADVCOMP 2020**, The Fourteenth International Conference on Advanced Engineering Computing and Applications in Sciences
- **SEMAPRO 2020**, The Fourteenth International Conference on Advances in Semantic Processing
- **AMBIENT 2020**, The Tenth International Conference on Ambient Computing, Applications, Services and Technologies
- **EMERGING 2020**, The Twelfth International Conference on Emerging Networks and Systems Intelligence
- **DATA ANALYTICS 2020**, The Ninth International Conference on Data Analytics
- **GLOBAL HEALTH 2020**, The Ninth International Conference on Global Health Challenges
- **CYBER 2020**, The Fifth International Conference on Cyber-Technologies and Cyber-Systems

ComputationWorld 2020 Congress
October 25, 2020 to October 29, 2020 - Nice, France

- **SERVICE COMPUTATION 2020**, The Twelfth International Conference on Advanced Service Computing
- **CLOUD COMPUTING 2020**, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization
- **FUTURE COMPUTING 2020**, The Twelfth International Conference on Future Computational Technologies and Applications
- **COGNITIVE 2020**, The Twelfth International Conference on Advanced Cognitive Technologies and Applications
- **ADAPTIVE 2020**, The Twelfth International Conference on Adaptive and Self-Adaptive Systems and Applications
- **CONTENT 2020**, The Twelfth International Conference on Creative Content Technologies
- **PATTERNS 2020**, The Twelfth International Conference on Pervasive Patterns and Applications
- **COMPUTATION TOOLS 2020**, The Eleventh International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking
- **BUSTECH 2020**, The Tenth International Conference on Business Intelligence and Technology

NetWare 2020 Congress
November 15, 2020 to November 19, 2020 - Valencia, Spain

- **SENSORCOMM 2020**, The Fourteenth International Conference on Sensor Technologies and Applications
- **SENSORDEVICES 2020**, The Eleventh International Conference on Sensor Device Technologies and Applications
- **SECURWARE 2020**, The Fourteenth International Conference on Emerging Security Information, Systems and Technologies
- **AFIN 2020**, The Twelfth International Conference on Advances in Future Internet
- **CENICS 2020**, The Thirteenth International Conference on Advances in Circuits, Electronics and Micro-electronics
- **ICQNM 2020**, The Fourteenth International Conference on Quantum, Nano/Bio, and Micro Technologies
- **FASSI 2020**, The Sixth International Conference on Fundamentals and Advances in Software Systems Integration
- **GREEN 2020**, The Fifth International Conference on Green Communications, Computing and Technologies

DigitalWorld 2020 Congress
November 21, 2020 to November 25, 2020 - Valencia, Spain

- **ICDS 2020**, The Fourteenth International Conference on Digital Society
- **ACHI 2020**, The Thirteenth International Conference on Advances in Computer-Human Interactions
- **GEOProcessing 2020**, The Twelfth International Conference on Advanced Geographic Information Systems, Applications, and Services
- **eTELEMED 2020**, The Twelfth International Conference on eHealth, Telemedicine, and Social Medicine
- **eLML 2020**, The Twelfth International Conference on Mobile, Hybrid, and On-line Learning
- **eKNOW 2020**, The Twelfth International Conference on Information, Process, and Knowledge Management
- **ALLSENSORS 2020**, The Fifth International Conference on Advances in Sensors, Actuators, Metering and Sensing
- **SMART ACCESSIBILITY 2020**, The Fifth International Conference on Universal Accessibility in the Internet of Things and Smart Environments

NexComm 2021 Congress
April 18 - 22, 2021 - Porto, Portugal

submission deadline: January 19, 2021

ThinkMind // [CYBER 2018, The Third International Conference on Cyber-Technologies and Cyber-Systems](#) // [View article cyber_2018_2_20_88014](#)

Prototype Open-Source Software Stack for the Reduction of False Positives and Negatives in the Detection of Cyber Indicators of Compromise and Attack

Authors:
Steve Chan

Keywords: Threat Intelligence Processing Framework (TIPF); Security Orchestration (SO); Log [Analysis] and Correlation Engine (LCE); Container- Orchestration System (COS); Dynamic Service Discovery (DSD).

Abstract:
A prototypical solution stack (Solution Stack #1) with chosen Open-Source Software (OSS) components for an experiment was enhanced by hybridized OSS amalgams (e.g., Suricata and Sagan; Kubernetes, Nomad, Cloudify and Helios; MineMeld and Hector) and supplemented by select modified algorithms (e.g., modified N-Input Voting Algorithm [NIVA] modules and a modified Fault Tolerant Averaging Algorithm [FTAA] module) leveraged by ensemble method machine learning. The preliminary results of the prototype solution stack (Stack #2) indicate a reduction, with regards to cyber Indicators of Compromise (IOC) and indicators of attack (IOA), of false positives by approximately 15% and false negatives by approximately 47%.

Pages: 39 to 48

Copyright: Copyright (c) IARIA, 2018

Publication date: November 18, 2018

Published in: conference

ISSN: 2519-8599

ISBN: 978-1-61208-683-5

Location: Athens, Greece

Dates: from November 18, 2018 to November 22, 2018

