

CfP: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2017)

Submitted by Anonymous on Thu, 11/17/2016 - 11:00am

Call for Paper

International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2017)

June 19-20, 2017, London, UK

IEEE is the Technical Co-Sponsor (TCS) of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2017), an international refereed conference dedicated to the advancement of the principles, methods and applications of situation awareness on Cyber Systems, Business Information Systems (BIS), Computer Network Defence (CND), Critical National Infrastructures (CNI), Cyber Physical Systems (CPS) and Internet of Things (IoTs).

The aim of the CyberSA 2017 is to encourage participation and promotion of collaborative scientific, industrial and academic inter-workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies. The purpose is to build bridges between academia and industry, and to encourage interplay of different cultures.

CyberSA 2017 invites researchers and industry practitioners to submit papers that encompass principles, analysis, design, methods and applications. All submitted papers are independently peer-reviewed.

The conference proceedings will be submitted for consideration for publishing and listing on the following bibliographic indexes: IEEE Computer Society Digital Library, IEEE Xplore Digital Library, DBLP Computer Science, Scopus, CiteSeerX, Computer Science Index, EI Compendex, Academic Search Complete, CiteULike, Google Scholar & Microsoft Academic Search.

Details

CyberSA 2017 is co-located with other conferences as part of Cyber Science

2017.

Posters will be presented during the conference.

Industry track is available for discussing and publishing pilot and proof of concepts.

Work in Progress track is available for preliminary work.

Research Ideas track is available for ideas in early stages assessment.

PhD Seminar track is available for discussing and publishing early PhD thesis research.

Submission Deadline

Deadline for all paper submissions, that is, both full papers and extended abstracts for Poster, WIP, PoC, Research Idea and PhD Seminar presentations is 14th January 2017.

All Industry track, Work in Progress track, Research Ideas track and PhD Seminar track will be published in the conference proceedings. Interested participants, please submit your proposal using the online submission system hosted by Easychair Conference Portal.

Full paper submission should be via Easychair Conference Portal.

Topics of Interest

Original papers are invited on recent advances in Cyber Situation Awareness, Data Analytics and Assessment. The topics in CyberSA 2017 include but not limited to:

Situation Awareness in Emerging Areas

Situation Awareness in Software Defined Networks
Security Monitoring, Scale of Things and Limits to Monitoring
Block Chain Technology in Security
IoT Detection and Software Driven Applications Security
Situation Awareness in Mobile Computing
Standardisation of Cyber Situation Awareness
Search, Triage, Examination and Forensics in Cloud Computing
Cyber SA in Chaotic Computing
Cyber SA in Large Scale IDS Deployments

Situation Awareness Assessments

Assessment models and methodologies for Cyber SA
Cyber Situation Awareness Evaluation Recommendation
Cyber SA Maturity Models and Frameworks
Cyber SA for Social Networks

Social Media Analysis

Social Network Interaction and Intelligence
Web Analytics & Security Incident Response
Organised and collaborative Maps and Networks
Cyber Behavioural Analytics and Profiling
Collaborative Situation Awareness for Decision Making

Collaborative Defense Approach

Situation Assessment & Decision Making
Defense Strategy for the Enhancement of Situation Awareness
Situation Assessment, Resolution and Decision Loop
Individual vs. Team SA
Group and Team SA

Risk Management, Governance and Compliance

Trust, Privacy and Anonymity Issues
Digital Forensic Information Analysis
Enterprise Information Security Policies, Standards and Procedures
Risks posed by Wireless Networks, including through the use of Mobile Computing, BYOD, Wearable in CND environment

Cyber Situation Awareness Tools & Techniques

Fuzzy Logic
Rough Set
Artificial Neural Networks
Artificial Intelligence
Genetic Algorithm
Evidence Theory (DST)
Bayesian Networks & Set Theory
Big Data Analytics
Game Theory
Graph Theory

Network Situation Awareness

Cyber Attack Scenarios
Situation-Aware and Context-Aware Network Applications
CERTs and CSIRTs
Security Event and Information Management
Application Security, Audits and Penetration Testing

Human Factor Cognitive

Workload
Perception
Stress
Knowledge

Training and Expertise
Risk Assessment and Decision Making
Forecasting and Prediction
Operator SA & Team SA

National and Critical Infrastructure Security Issues

Information Security
Cyber Security
Database Security
Application Security
Law Enforcement and Surveillance
Border Protection and Controls
Cyber Warfare and Counter Terrorism

Situation Awareness in Military Operations

Military Doctrinal in Situation Awareness
C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)
Computer Network Operations
Computer Network Defense
Mission Awareness, Command and Control

Cyber Situation Analytics

Attack Graphs
Advanced Security Incident Analysis
Sensor Correlation and Cross-Correlation
Implementing Situation Awareness Systems
Information Security Metrics and Measurements

Cyber Situation Awareness Frameworks

Proactive Defense Strategies
Instance-Based Learning
Adaptive Neural Logic
Human-Assisted Decision Control
Human in the Loop
Automated Self-Responder

Fusion Centres

Tools for Metric Optimisation
Visualisation and Digital Analytics
Data Mining
Filtration, Selection, and Risk-Based Prioritisation
Metrics for Evaluation and Assessment
Usefulness of Multisensor Data Fusion

Information Data Fusion
Sensor Fusion for Security Incident Analysis
Security Incident Analysis
Data Association & Correlation
Security Information Visualisation
Data Analytics
Security Monitoring

Situation Awareness Applications

Situation Awareness in C4ISR
Situation Awareness in Cyber Command and Control Centres
Situation Awareness in Intrusion Defense
Situation Awareness in Cyber Physical Systems (CPS)
Situation Awareness for Internet of Things (IoTs), Enterprise Internet of Things (EIoTs)
Open Source Applications

Cyber Situation Awareness Designs, Solutions and Services

Functional Requirements for Situation-aware services
Non-Functional Requirements for Situation-aware Services and solutions
Interface Design
Interoperability
Dynamism
Complexity
Performance
Automation
Realtime Processing

Situation Awareness Training

Research and development in Situation Awareness
Simulation and Testbeds in Cyber Situation Awareness
Experimentation & Instrumentation
Modelling
Knowledge-base
Theoretical Underpinnings in Situation Awareness
Team and Group SA
Cyber Situation Awareness Methods, Training and Education

Best Papers

The best paper of each section will be selected and their author(s) will receive a corresponding Award Certificate. Authors of the Best 20%-25% papers presented at the conference will be invited to adapt their papers for their publication in one of the special issues peer reviewed journals.

[? CfP: 2016 Annual Computer Security Applications Conference \(ACSAC\) Call for Presentations: 28th Annual IEEE Software Technology Conference \(STC 2017\) ?](#)



[Calls for Papers](#)
