Data-Driven Security
In this thematic Series, we solicit original contributions on data-driven security, and encourage all international researchers and practitioners in the related areas to present emerging advanced theories and techniques. All submissions will undergo rigorous peer review and accepted articles will be published within the journal as a collection.

All the original research that is powered by data intelligence is welcome and the areas include but not restricted to:

- Malware analysis and detection
- Binary code analysis
- Autonomous vehicle security
- Big data security and privacy
- Artificial Intelligence security and privacy
- Vulnerability discovery and diagnosis
- Exploit and security patch generation
- Blockchain security and privacy
- IoT security and privacy

Key dates
Paper Submission: August 15, 2019
1st round notification: October 15, 2019
Revision due: November 15, 2019
Final notification: December 1, 2019

Guest Editors
Yang Liu <yangliu@ntu.edu.sg>
Xinming Ou <xou@usf.edu>
Xinyu Xing <xxing@ist.psu.edu>
Guozhu Meng <mengguozhu@iie.ac.cn>

Submission Instructions
Prospective authors are invited to prepare and submit manuscripts following the instructions at: https://cybersecurity.springeropen.com/submission-guidelines; the complete manuscript should be submitted through: http://www.editorialmanager.com/cyse/default.aspx

To ensure that you submit to the correct thematic series please select the appropriate thematic series ‘Data-Driven Security’ in the ‘Additional Information’. In addition, indicate within your cover letter that you wish your manuscript to be considered as part of the thematic series on Data-Driven Security.