Florian Skopik

List of Publications by Year in Descending Order

89 papers	861 citations	15 h-index	26 g-index
105 ext. papers	1,103 ext. citations	1.8 avg, IF	4.64 L-index

#	Paper	IF	Citations
89	Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey. *IEEE Security and Privacy*, **2022**, 2-10	2	1
88	Automatic Attack Pattern Mining for Generating Actionable CTI Applying Alert Aggregation. *Lecture Notes in Computer Science*, **2022**, 136-161	0.9	0
87	Detecting Unknown Cyber Security Attacks Through System Behavior Analysis. *Lecture Notes in Computer Science*, **2022**, 103-119	0.9	
86	Dealing with Security Alert Flooding: Using Machine Learning for Domain-independent Alert Aggregation. *ACM Transactions on Privacy and Security*, **2022**, 25, 1-36	2.9	1
85	Online Log Data Analysis With Efficient Machine Learning: A Review. *IEEE Security and Privacy*, **2021**, 2-12	2	1
84	Have it Your Way: Generating Customized Log Datasets With a Model-Driven Simulation Testbed. *IEEE Transactions on Reliability*, **2021**, 70, 402-415	4.6	5
83	Incremental Log Data Clustering for Processing Large Amounts of Data Online **2021**, 43-61		
82	AECID: A Light-Weight Log Analysis Approach for Online Anomaly Detection **2021**, 99-129		
81	Variable Type Detector for Statistical Analysis of Log Tokens **2021**, 151-171		
80	Iterative Selection of Categorical Variables for Log Data Anomaly Detection. *Lecture Notes in Computer Science*, **2021**, 757-777	0.9	1
79	Time Series Analysis for Temporal Anomaly Detection **2021**, 83-98		
78	The Seven Golden Principles of Effective Anomaly-Based Intrusion Detection. *IEEE Security and Privacy*, **2021**, 19, 36-45	2	
77	Smart Log Data Analytics **2021**,		4
76	Survey on Log Clustering Approaches **2021**, 13-41		0
75	synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems. *Journal of Information Security and Applications*, **2020**, 54, 102544	3.5	2
74	System log clustering approaches for cyber security applications: A survey. *Computers and Security*, **2020**, 92, 101739	4.9	25
73	Creating Character-based Templates for Log Data to Enable Security Event Classification **2020**,		4

72	AIT Cyber Range **2020**,		8
71	Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, **2020**, 3,	5	4
70	Trust and Distrust: On Sense and Nonsense in Big Data. *IFIP Advances in Information and Communication Technology*, **2019**, 81-94	0.5	
69	A Framework for Cyber Threat Intelligence Extraction from Raw Log Data **2019**,		7
68	Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators **2019**,		1
67	AECID: A Self-learning Anomaly Detection Approach based on Light-weight Log Parser Models **2018** ,		6
66	Organisationsübergreifender Austausch sicherheitsrelevanter Informationen als Grundlage für Cyber-Lagebilder **2018**, 43-80		
65	Countering targeted cyber-physical attacks using anomaly detection in self-adaptive Industry 4.0 Systems. *Elektrotechnik Und Informationstechnik*, **2018**, 135, 278-285	0.4	2
64	Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. *Computers and Security*, **2018**, 79, 94-116	4.9	19
63	Time Series Analysis: Unsupervised Anomaly Detection Beyond Outlier Detection. *Lecture Notes in Computer Science*, **2018**, 19-36	0.9	9
62	A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, **2017**, 34, 166-182	3.5	21
61	Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken. *Datenschutz Und Datensicherheit - DuD*, **2017**, 41, 572-576	0.1	1
60	Incremental Clustering for Semi-Supervised Anomaly Detection applied on Log Data **2017**,		15
59	Acquiring Cyber Threat Intelligence through Security Information Correlation **2017**,		9
58	A Collaborative Analysis System for Cross-organization Cyber Incident Handling **2016**,		6
57	A decision support model for situational awareness in National Cyber Operations Centers **2016**,		3
56	Correlating cyber incident information to establish situational awareness in Critical Infrastructures **2016**,		6
55	Discovering Insider Threats from Log Data with High-Performance Bioinformatics Tools **2016**,		5

54	Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools. *Information Systems*, **2016**, 60, 13-33	2.7	9
53	A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, **2016**, 60, 154-176	4.9	102
52	From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers and Security*, **2016**, 62, 165-176	4.9	18
51	A structural design for a pan-European early warning system for critical infrastructures. *Elektrotechnik Und Informationstechnik*, **2015**, 132, 117-121	0.4	8
50	Combating advanced persistent threats: From network event correlation to incident detection. *Computers and Security*, **2015**, 48, 35-57	4.9	115
49	On demand for situational awareness for preventing attacks on the smart grid **2015**,		1
48	Keine Cyber-Sicherheit ohne Datenschutz. *Datenschutz Und Datensicherheit - DuD*, **2015**, 39, 723-729	0.1	
47	Beyond gut instincts: Understanding, rating and comparing self-learning IDSs **2015**,		1
46	**2015**,		11
45	Cyber situational awareness through network anomaly detection: state of the art and new approaches. *Elektrotechnik Und Informationstechnik*, **2015**, 132, 101-105	0.4	6
44	Semi-synthetic data set generation for security software evaluation **2014**,		13
43	Dealing with advanced persistent threats in smart grid ICT networks **2014**,		19
42	Cyber Attack Information Sharing. *Datenschutz Und Datensicherheit - DuD*, **2014**, 38, 251-256	0.1	2
41	The social smart grid: Dealing with constrained energy resources through social coordination. *Journal of Systems and Software*, **2014**, 89, 3-18	3.3	16
40	Architecture-driven smart grid security management **2014**,		4
39	PRECYSE: Cyber-attack Detection and Response for Industrial Control Systems **2014**,		2
38	A Self-organising Approach for Smart Meter Communication Systems. *Lecture Notes in Computer Science*, **2014**, 169-175	0.9	1
37	Trustworthy incident information sharing in social cyber defense alliances **2013**,		2

36	Privacy issues of smart e-mobility **2013**,		10
35	Cyber Security Challenges in Heterogeneous ICT Infrastructures of Smart Grids. *Journal of Communications*, **2013**, 8, 463-472	0.5	3
34	Expert Discovery and Interactions in Mixed Service-Oriented Systems. *IEEE Transactions on Services Computing*, **2012**, 5, 233-245	4.8	21
33	Social network mining of requester communities in crowdsourcing markets. *Social Network Analysis and Mining*, **2012**, 2, 329-344	2.2	2
32	Attack Vectors to Metering Data in Smart Grids under Security Constraints **2012**,		15
31	Designing a Cyber Attack Information System for National Situational Awareness. *Communications in Computer and Information Science*, **2012**, 277-288	0.3	3
30	Novel Energy Saving Opportunities in Smart Grids Using a Secure Social Networking Layer **2012**,		3
29	DISCOVERING AND MANAGING SOCIAL COMPOSITIONS IN COLLABORATIVE ENTERPRISE CROWDSOURCING SYSTEMS. *International Journal of Cooperative Information Systems*, **2012**, 21, 297-341	0.6	9
28	A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures. *International Journal of Smart Grid and Clean Energy*, **2012**, 22-28	1.4	21
27	Security Is Not Enough! On Privacy Challenges in Smart Grids. *International Journal of Smart Grid and Clean Energy*, **2012**, 7-14	1.4	13
26	Information Management and Sharing for National Cyber Situational Awareness **2012**, 217-227		3
25	Towards Secure Time-Triggered Systems. *Lecture Notes in Computer Science*, **2012**, 365-372	0.9	3
24	Opportunistic Information Flows through Strategic Social Link Establishment **2011**,		1
23	Interaction mining and skill-dependent recommendations for multi-objective team composition. *Data and Knowledge Engineering*, **2011**, 70, 866-891	1.5	30
22	Adaptive provisioning of human expertise in service-oriented systems **2011**,		1
21	Managing social overlay networks in semantic open enterprise systems **2011**,		2
20	Towards Social Crowd Environments Using Service-Oriented Architectures. *IT - Information Technology*, **2011**, 53,	0.4	2
19	Resource and Agreement Management in Dynamic Crowdcomputing Environments **2011**,		13