

Florian Skopik

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/3316319/publications.pdf>

Version: 2024-02-01

93
papers

1,355
citations

566801

15
h-index

454577

30
g-index

105
all docs

105
docs citations

105
times ranked

1070
citing authors

#	ARTICLE	IF	CITATIONS
1	Combating advanced persistent threats: From network event correlation to incident detection. Computers and Security, 2015, 48, 35-57.	4.0	164
2	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.	4.0	150
3	Modeling and mining of dynamic trust in complex service-oriented systems. Information Systems, 2010, 35, 735-757.	2.4	89
4	System log clustering approaches for cyber security applications: A survey. Computers and Security, 2020, 92, 101739.	4.0	57
5	Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. Computers and Security, 2018, 79, 94-116.	4.0	44
6	Interaction mining and skill-dependent recommendations for multi-objective team composition. Data and Knowledge Engineering, 2011, 70, 866-891.	2.1	35
7	A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures. International Journal of Smart Grid and Clean Energy, 2012, , 22-28.	0.4	34
8	Expert Discovery and Interactions in Mixed Service-Oriented Systems. IEEE Transactions on Services Computing, 2012, 5, 233-245.	3.2	32
9	Start Trusting Strangers? Bootstrapping and Prediction of Trust. Lecture Notes in Computer Science, 2009, , 275-289.	1.0	31
10	Dealing with advanced persistent threats in smart grid ICT networks. , 2014, , .		28
11	A collaborative cyber incident management system for European interconnected critical infrastructures. Journal of Information Security and Applications, 2017, 34, 166-182.	1.8	28
12	Trustworthy interaction balancing in mixed service-oriented systems. , 2010, , .		27
13	Incremental Clustering for Semi-Supervised Anomaly Detection applied on Log Data. , 2017, , .		27
14	From old to new: Assessing cybersecurity risks for an evolving smart grid. Computers and Security, 2016, 62, 165-176.	4.0	25
15	AIT Cyber Range. , 2020, , .		22
16	Runtime Behavior Monitoring and Self-Adaptation in Service-Oriented Systems. , 2010, , .		21
17	Attack Vectors to Metering Data in Smart Grids under Security Constraints. , 2012, , .		21
18	Semi-synthetic data set generation for security software evaluation. , 2014, , .		21

#	ARTICLE	IF	CITATIONS
19	Have it Your Way: Generating Customized Log Datasets With a Model-Driven Simulation Testbed. IEEE Transactions on Reliability, 2021, 70, 402-415.	3.5	21
20	Trust and Reputation Mining in Professional Virtual Communities. Lecture Notes in Computer Science, 2009, , 76-90.	1.0	21
21	The Cycle of Trust in Mixed Service-Oriented Systems. , 2009, , .		20
22	The social smart grid: Dealing with constrained energy resources through social coordination. Journal of Systems and Software, 2014, 89, 3-18.	3.3	20
23	Acquiring Cyber Threat Intelligence through Security Information Correlation. , 2017, , .		19
24	Resource and Agreement Management in Dynamic Crowdsourcing Environments. , 2011, , .		18
25	A Framework for Cyber Threat Intelligence Extraction from Raw Log Data. , 2019, , .		18
26	Privacy issues of smart e-mobility. , 2013, , .		16
27	Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools. Information Systems, 2016, 60, 13-33.	2.4	16
28	Security Is Not Enough! On Privacy Challenges in Smart Grids. International Journal of Smart Grid and Clean Energy, 2012, , 7-14.	0.4	15
29	Behavior Monitoring in Self-Healing Service-Oriented Systems. , 2010, , .		14
30	DISCOVERING AND MANAGING SOCIAL COMPOSITIONS IN COLLABORATIVE ENTERPRISE CROWDSOURCING SYSTEMS. International Journal of Cooperative Information Systems, 2012, 21, 297-341.	0.6	13
31	Time Series Analysis: Unsupervised Anomaly Detection Beyond Outlier Detection. Lecture Notes in Computer Science, 2018, , 19-36.	1.0	13
32	Dealing with Security Alert Flooding: Using Machine Learning for Domain-independent Alert Aggregation. ACM Transactions on Privacy and Security, 2022, 25, 1-36.	2.2	13
33	Establishing national cyber situational awareness through incident information clustering. , 2015, , .		12
34	A structural design for a pan-European early warning system for critical infrastructures. Elektrotechnik Und Informationstechnik, 2015, 132, 117-121.	0.7	12
35	Under false flag: using technical artifacts for cyber attack attribution. Cybersecurity, 2020, 3, .	3.1	12
36	Trusted Interaction Patterns in Large-scale Enterprise Service Networks. , 2010, , .		11

#	ARTICLE	IF	CITATIONS
37	Cyber situational awareness through network anomaly detection: state of the art and new approaches. <i>Elektrotechnik Und Informationstechnik</i> , 2015, 132, 101-105.	0.7	11
38	An Analysis of the Structure and Dynamics of Large-Scale Q/A Communities. <i>Lecture Notes in Computer Science</i> , 2011, , 285-301.	1.0	11
39	AECID: A Self-learning Anomaly Detection Approach based on Light-weight Log Parser Models. , 2018, , .		10
40	Smart Log Data Analytics. , 2021, , .		9
41	Trust-Based Adaptation in Complex Service-Oriented Systems. , 2010, , .		8
42	Bridging socially-enhanced virtual communities. , 2011, , .		8
43	Countering targeted cyber-physical attacks using anomaly detection in self-adaptive Industry 4.0 Systems. <i>Elektrotechnik Und Informationstechnik</i> , 2018, 135, 278-285.	0.7	8
44	Correlating cyber incident information to establish situational awareness in Critical Infrastructures. , 2016, , .		7
45	Discovering Insider Threats from Log Data with High-Performance Bioinformatics Tools. , 2016, , .		7
46	A Collaborative Analysis System for Cross-organization Cyber Incident Handling. , 2016, , .		7
47	Novel Energy Saving Opportunities in Smart Grids Using a Secure Social Networking Layer. , 2012, , .		6
48	Social network mining of requester communities in crowdsourcing markets. <i>Social Network Analysis and Mining</i> , 2012, 2, 329-344.	1.9	6
49	Designing a Cyber Attack Information System for National Situational Awareness. <i>Communications in Computer and Information Science</i> , 2012, , 277-288.	0.4	6
50	Architecture-driven smart grid security management. , 2014, , .		6
51	synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems. <i>Journal of Information Security and Applications</i> , 2020, 54, 102544.	1.8	6
52	Information Management and Sharing for National Cyber Situational Awareness. , 2012, , 217-227.		6
53	Mining and Composition of Emergent Collectives in Mixed Service-Oriented Systems. , 2010, , .		5
54	A decision support model for situational awareness in National Cyber Operations Centers. , 2016, , .		5

#	ARTICLE	IF	CITATIONS
55	Creating Character-based Templates for Log Data to Enable Security Event Classification. , 2020, , .		5
56	Towards Secure Time-Triggered Systems. Lecture Notes in Computer Science, 2012, , 365-372.	1.0	5
57	Cyber Security Challenges in Heterogeneous ICT Infrastructures of Smart Grids. Journal of Communications, 2013, 8, 463-472.	1.3	5
58	Towards Social Crowd Environments Using Service-Oriented Architectures. IT - Information Technology, 2011, 53, .	0.6	4
59	Online Log Data Analysis With Efficient Machine Learning: A Review. IEEE Security and Privacy, 2022, 20, 80-90.	1.5	4
60	Trustworthy incident information sharing in social cyber defense alliances. , 2013, , .		3
61	On demand for situational awareness for preventing attacks on the smart grid. , 2015, , .		3
62	Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators. , 2019, , .		3
63	Managing social overlay networks in semantic open enterprise systems. , 2011, , .		2
64	Iterative Selection of Categorical Variables for Log Data Anomaly Detection. Lecture Notes in Computer Science, 2021, , 757-777.	1.0	2
65	A programming model for self-adaptive open enterprise systems. , 2010, , .		2
66	PRECYSE: Cyber-attack Detection and Response for Industrial Control Systems. , 2014, , .		2
67	A Blueprint for a Pan-European Cyber Incident Analysis System. , 2015, , .		2
68	Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey. IEEE Security and Privacy, 2022, 20, 18-26.	1.5	2
69	Preparing for National Cyber Crises Using Non-linear Cyber Exercises. , 2021, , .		2
70	A Framework for Automatic Labeling of Log Datasets from Model-driven Testbeds for HIDS Evaluation. , 2022, , .		2
71	Social Formation and Interactions in Evolving Service-Oriented Communities. , 2010, , .		1
72	Context-Aware Campaigns in Social Networks. , 2010, , .		1

#	ARTICLE	IF	CITATIONS
73	Context-Aware Interaction Models in Cross-Organizational Processes. , 2010, , .		1
74	Supporting Network Formation through Mining under Privacy Constraints. , 2010, , .		1
75	Opportunistic Information Flows through Strategic Social Link Establishment. , 2011, , .		1
76	Adaptive provisioning of human expertise in service-oriented systems. , 2011, , .		1
77	Beyond gut instincts: Understanding, rating and comparing self-learning IDSs. , 2015, , .		1
78	Trust and Distrust: On Sense and Nonsense in Big Data. IFIP Advances in Information and Communication Technology, 2019, , 81-94.	0.5	1
79	The Seven Golden Principles of Effective Anomaly-Based Intrusion Detection. IEEE Security and Privacy, 2021, 19, 36-45.	1.5	1
80	Survey on Log Clustering Approaches. , 2021, , 13-41.		1
81	Behavior Monitoring in Self-Healing Service-Oriented Systems. , 2011, , 95-116.		1
82	A Self-organising Approach for Smart Meter Communication Systems. Lecture Notes in Computer Science, 2014, , 169-175.	1.0	1
83	Computational Social Network Management in Crowdsourcing Environments. , 2011, , .		0
84	Incremental Log Data Clustering for Processing Large Amounts of Data Online. , 2021, , 43-61.		0
85	AECID: A Light-Weight Log Analysis Approach for Online Anomaly Detection. , 2021, , 99-129.		0
86	Variable Type Detector for Statistical Analysis of Log Tokens. , 2021, , 151-171.		0
87	Time Series Analysis for Temporal Anomaly Detection. , 2021, , 83-98.		0
88	Mobile Web Service Provisioning in Cellular Enterprise. , 2010, , 311-356.		0
89	Collective Intelligence for Crowdsourcing and Community Q&A. , 2014, , 169-177.		0
90	Collective Intelligence for Crowdsourcing and Community Q&A. , 2017, , 1-9.		0

#	ARTICLE	IF	CITATIONS
91	Collective Intelligence for Crowdsourcing and Community Q&A. , 2018, , 278-286.		0
92	Organisationsübergreifender Austausch sicherheitsrelevanter Informationen als Grundlage für Cyber-Lagebilder. , 2018, , 43-80.		0
93	Strategic selection of data sources for cyber attack detection in enterprise networks. , 2022, , .		0