

Marc Dacier

List of Publications by Citations

Source: <https://exaly.com/author-pdf/8715658/marc-dacier-publications-by-citations.pdf>

Version: 2024-04-27

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

29
papers

940
citations

13
h-index

29
g-index

29
ext. papers

1,097
ext. citations

1.9
avg, IF

3.89
L-index

#	Paper	IF	Citations
29	Towards a taxonomy of intrusion-detection systems. <i>Computer Networks</i> , 1999 , 31, 805-822	5.4	375
28	A revised taxonomy for intrusion-detection systems. <i>Annales Des Telecommunications/Annals of Telecommunications</i> , 2000 , 55, 361-378	2	123
27	Intrusion Detection Using Variable-Length Audit Trail Patterns. <i>Lecture Notes in Computer Science</i> , 2000 , 110-129	0.9	73
26	Cyber SA: Situational Awareness for Cyber Defense. <i>Advances in Information Security</i> , 2010 , 3-13	0.7	58
25	A framework for attack patterns discovery in honeynet data. <i>Digital Investigation</i> , 2008 , 5, S128-S139	3.3	55
24	SGNET: A Worldwide Deployable Framework to Support the Analysis of Malware Threat Models 2008 ,		29
23	Automatic Handling of Protocol Dependencies and Reaction to 0-Day Attacks with ScriptGen Based Honeypots. <i>Lecture Notes in Computer Science</i> , 2006 , 185-205	0.9	28
22	On a multicriteria clustering approach for attack attribution. <i>SIGKDD Explorations: Newsletter of the Special Interest Group (SIG) on Knowledge Discovery & Data Mining</i> , 2010 , 12, 11-20	4.6	21
21	Honeypot trace forensics: The observation viewpoint matters. <i>Future Generation Computer Systems</i> , 2011 , 27, 539-546	7.5	20
20	An Analysis of Rogue AV Campaigns. <i>Lecture Notes in Computer Science</i> , 2010 , 442-463	0.9	19
19	The WOMBAT Attack Attribution Method: Some Results. <i>Lecture Notes in Computer Science</i> , 2009 , 19-37	0.9	18
18	A strategic analysis of spam botnets operations 2011 ,		18
17	The MEERKATS Cloud Security Architecture 2012 ,		15
16	Technical perspective They do click, don't they?. <i>Communications of the ACM</i> , 2009 , 52, 98-98	2.5	11
15	Fixed- vs. variable-length patterns for detecting suspicious process behavior. <i>Journal of Computer Security</i> , 2000 , 8, 159-181	0.8	11
14	SGNET: Implementation insights 2008 ,		9
13	Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making 2009 ,		8

12	Actionable Knowledge Discovery for Threats Intelligence Support Using a Multi-dimensional Data Mining Methodology 2008 ,		8
11	Visualization of actionable knowledge to mitigate DRDoS attacks 2016 ,		8
10	The Quest for Multi-headed Worms. <i>Lecture Notes in Computer Science</i> , 2008 , 247-266	0.9	7
9	Fixed vs. variable-length patterns for detecting suspicious process behavior. <i>Lecture Notes in Computer Science</i> , 1998 , 1-15	0.9	6
8	Honeypot Traces Forensics: The Observation Viewpoint Matters 2009 ,		5
7	Malicious BGP hijacks: Appearances can be deceiving 2014 ,		4
6	Assessing Cybercrime Through the Eyes of the WOMBAT. <i>Advances in Information Security</i> , 2010 , 103-136.	0.7	4
5	The MINESTRONE Architecture Combining Static and Dynamic Analysis Techniques for Software Security 2011 ,		3
4	Automating the Analysis of Honeypot Data (Extended Abstract). <i>Lecture Notes in Computer Science</i> , 2008 , 406-407	0.9	2
3	Gone Rogue: An Analysis of Rogue Security Software Campaigns 2009 ,		1
2	Scraping Airlines Bots: Insights Obtained Studying Honeypot Data 2021 , 2, 3-28		1
1	On the Resilience of the Dependability Framework to the Intrusion of New Security Threats. <i>Lecture Notes in Computer Science</i> , 2011 , 238-250	0.9	