Marc Dacier

List of Publications by Year
in descending order

29 papers	1,336 citations	840585 11 h-index	887953 17 g-index
29 all docs	29 docs citations	29 times ranked	787 citing authors

#	Article	IF	Citations
1	Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999, 31, 805-822.	3.2	533
2	A revised taxonomy for intrusion-detection systems. Annales Des Telecommunications/Annals of Telecommunications, 2000, 55, 361-378.	1.6	203
3	Intrusion Detection Using Variable-Length Audit Trail Patterns. Lecture Notes in Computer Science, 2000, , 110-129.	1.0	105
4	Cyber SA: Situational Awareness for Cyber Defense. Advances in Information Security, 2010, , 3-13.	0.9	84
5	A framework for attack patterns' discovery in honeynet data. Digital Investigation, 2008, 5, S128-S139.	3.2	66
6	Automatic Handling of Protocol Dependencies and Reaction to 0-Day Attacks with ScriptGen Based Honeypots. Lecture Notes in Computer Science, 2006, , 185-205.	1.0	39
7	SGNET: A Worldwide Deployable Framework to Support the Analysis of Malware Threat Models. , 2008, , .		33
8	An Analysis of Rogue AV Campaigns. Lecture Notes in Computer Science, 2010, , 442-463.	1.0	31
9	A strategic analysis of spam botnets operations. , 2011, , .		26
10	On a multicriteria clustering approach for attack attribution. SIGKDD Explorations: Newsletter of the Special Interest Group (SIG) on Knowledge Discovery & Data Mining, 2010, 12, 11-20.	3.2	25
11	Honeypot trace forensics: The observation viewpoint matters. Future Generation Computer Systems, 2011, 27, 539-546.	4.9	23
12	The WOMBAT Attack Attribution Method: Some Results. Lecture Notes in Computer Science, 2009, , 19-37.	1.0	21
13	The MEERKATS Cloud Security Architecture. , 2012, , .		20
14	Visualization of actionable knowledge to mitigate DRDoS attacks. , 2016, , .		19
15	Technical perspectiveThey do click, don't they?. Communications of the ACM, 2009, 52, 98-98.	3.3	17
16	Fixed vs. variable-length patterns for detecting suspicious process behavior. Lecture Notes in Computer Science, 1998, , 1-15.	1.0	13
17	Fixed- vs. variable-length patterns for detecting suspicious process behavior. Journal of Computer Security, 2000, 8, 159-181.	0.5	13
18	SGNET: Implementation insights. , 2008, , .		10

#	Article	IF	Citations
19	Actionable Knowledge Discovery for Threats Intelligence Support Using a Multi-dimensional Data Mining Methodology. , 2008, , .		10
20	The Quest for Multi-headed Worms. Lecture Notes in Computer Science, 2008, , 247-266.	1.0	9
21	Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making. , 2009, , .		8
22	Honeypot Traces Forensics: The Observation Viewpoint Matters. , 2009, , .		6
23	Malicious BGP hijacks: Appearances can be deceiving. , 2014, , .		6
24	Assessing Cybercrime Through the Eyes of the WOMBAT. Advances in Information Security, 2010, , 103-136.	0.9	5
25	Scraping Airlines Bots: Insights Obtained Studying Honeypot Data. International Journal of Cyber Forensics and Advanced Threat Investigations, 2021, 2, 3-28.	1.2	4
26	The MINESTRONE Architecture Combining Static and Dynamic Analysis Techniques for Software Security. , 2011, , .		3
27	Gone Rogue: An Analysis of Rogue Security Software Campaigns. , 2009, , .		2
28	Automating the Analysis of Honeypot Data (Extended Abstract). Lecture Notes in Computer Science, 2008, , 406-407.	1.0	2
29	On the Resilience of the Dependability Framework to the Intrusion of New Security Threats. Lecture Notes in Computer Science, 2011, , 238-250.	1.0	0