

CITATION REPORT

List of articles citing

Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP)

DOI: 10.1108/13685201211266015

Journal of Money Laundering Control, 2012, 15, 430-441.

Source: <https://exaly.com/paper-pdf/53478378/citation-report.pdf>

Version: 2024-04-09

This report has been generated based on the citations recorded by exaly.com for the above article. 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.

#	Paper	IF	Citations
34	Challenges to Automated Allegory Resolution in Open Source Intelligence. 2012 ,		
33	Identifying Cyber Predators through Forensic Authorship Analysis of Chat Logs. 2012 ,		7
32	Modelling the effect of deception on investigations using open source intelligence (OSINT). <i>Journal of Money Laundering Control</i> , 2013 , 16, 238-248	0.8	1
31	. 2013 ,		5
30	A methodology for estimating the tangible cost of data breaches. <i>Journal of Information Security and Applications</i> , 2014 , 19, 321-330	3.5	22
29	Mining Malware to Detect Variants. 2014 ,		21
28	Be Careful Who You Trust: Issues with the Public Key Infrastructure. 2014 ,		2
27	Authorship analysis of aliases: Does topic influence accuracy?. <i>Natural Language Engineering</i> , 2015 , 21, 497-518	1.1	4
26	Maximising Eyeballs but Facilitating Cybercrime? Ethical Challenges for Online Advertising in New Zealand. 2015 ,		1
25	Global adversarial capability modeling. 2015 ,		2
24	Computational Techniques for Predicting Cyber Threats. <i>Advances in Intelligent Systems and Computing</i> , 2015 , 247-253	0.4	9
23	A cyber-threat analytic model for autonomous detection of virtual property theft. <i>Information and Computer Security</i> , 2017 , 25, 358-381	1.4	2
22	Intrusion Prediction Systems. <i>Studies in Computational Intelligence</i> , 2017 , 155-174	0.8	11
21	Socio-economic factors in cybercrime: Statistical study of the relation between socio-economic factors and cybercrime. 2017 ,		1
20	Predicting Cyber-Events by Leveraging Hacker Sentiment. <i>Information (Switzerland)</i> , 2018 , 9, 280	2.6	20
19	Security Challenges of Vehicle Recovery for Urban Air Mobility Contexts. 2019 ,		2
18	AVOCAD: Adaptive Terrorist Comms Surveillance and Interception using Machine Learning. 2019 ,		1

17	Cybersecurity data science: an overview from machine learning perspective. <i>Journal of Big Data</i> , 2020 , 7,	11.7	86
16	Packing resistant solution to group malware binaries. <i>International Journal of Security and Networks</i> , 2020 , 15, 123	0.5	0
15	Cybersecurity hazards and financial system vulnerability: a synthesis of literature. <i>Risk Management</i> , 2020 , 22, 239-309	2.5	6
14	Security analytics for real-time forecasting of cyberattacks. <i>Software - Practice and Experience</i> , 2020 , ,	2.5	1
13	Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. <i>Information (Switzerland)</i> , 2020 , 11, 168	2.6	12
12	What matters for financial inclusions? Evidence from emerging economy. <i>International Journal of Finance and Economics</i> , 2021 ,	1.5	
11	Detecting Illicit Drugs on Social Media Using Automated Social Media Intelligence Analysis (ASMIA). <i>Lecture Notes in Computer Science</i> , 2012 , 66-76	0.9	12
10	Indirect Attribution in Cyberspace. <i>Advances in Digital Crime, Forensics, and Cyber Terrorism</i> , 2015 , 246-262	2	1
9	Named Entity Resolution in Social Media. 2016 , 21-36		
8	Gathering Intelligence on High-Risk Advertising and Film Piracy: A Study of the Digital Underground. 2016 , 89-102		1
7	The Economics of Cybercrime. <i>ACM Transactions on Management Information Systems</i> , 2019 , 10, 1-23	2	4
6	A Descriptive Analytics of the Occurrence and Predictive Analytics of Cyber Attacks During the Pandemic. <i>Advanced Sciences and Technologies for Security Applications</i> , 2021 , 123-159	0.6	1
5	Characterizing Building Automation System Attacks and Attackers. 2022 ,		0
4	Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning: A Review. <i>Journal of Cybersecurity and Privacy</i> , 2022 , 2, 527-555	4	2
3	A deeper look into cybersecurity issues in the wake of Covid-19: A survey. 2022 ,		0
2	Cyber Attacker Profiling for Risk Analysis Based on Machine Learning. 2023 , 23, 2028		0
1	Exploring the global geography of cybercrime and its driving forces. 2023 , 10,		0