

# Pavel Celeda

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/3994168/publications.pdf>

Version: 2024-02-01

63  
papers

1,312  
citations

933447

10  
h-index

501196

28  
g-index

66  
all docs

66  
docs citations

66  
times ranked

942  
citing authors

#	ARTICLE	IF	CITATIONS
1	Student assessment in cybersecurity training automated by pattern mining and clustering. Education and Information Technologies, 2022, 27, 9231-9262.	5.7	6
2	Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. , 2022, , .		6
3	Encrypted Web traffic dataset: Event logs and packet traces. Data in Brief, 2022, 42, 108188.	1.0	2
4	Applications of educational data mining and learning analytics on data from cybersecurity training. Education and Information Technologies, 2022, 27, 12179-12212.	5.7	3
5	Identification of Attack Paths Using Kill Chain and Attack Graphs. , 2022, , .		4
6	HTTPS Event-Flow Correlation: Improving Situational Awareness in Encrypted Web Traffic. , 2022, , .		0
7	Enriching DNS Flows with Host-Based Events to Bypass Future Protocol Encryption. IFIP Advances in Information and Communication Technology, 2021, , 302-316.	0.7	0
8	Cybersecurity knowledge and skills taught in capture the flag challenges. Computers and Security, 2021, 102, 102154.	6.0	33
9	Dataset of shell commands used by participants of hands-on cybersecurity training. Data in Brief, 2021, 38, 107398.	1.0	7
10	Toolset for Collecting Shell Commands and Its Application in Hands-on Cybersecurity Training. , 2021, , .		2
11	Scalable Learning Environments for Teaching Cybersecurity Hands-on. , 2021, , .		14
12	Cyber Situation Awareness via IP Flow Monitoring. , 2020, , .		3
13	Using TLS Fingerprints for OS Identification in Encrypted Traffic. , 2020, , .		3
14	Predictions of Network Attacks in Collaborative Environment. , 2020, , .		2
15	What Are Cybersecurity Education Papers About?. , 2020, , .		44
16	Predictive Cyber Situational Awareness and Personalized Blacklisting. ACM Transactions on Management Information Systems, 2020, 11, 1-16.	2.8	20
17	KYPO4INDUSTRY. , 2020, , .		2
18	Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. IEEE Communications Surveys and Tutorials, 2019, 21, 640-660.	39.4	172

#	ARTICLE	IF	CITATIONS
19	Data-Driven Intelligence for Characterizing Internet-Scale IoT Exploitations. , 2018, , .		2
20	Assessing Internet-wide Cyber Situational Awareness of Critical Sectors. , 2018, , .		12
21	Toward real-time network-wide cyber situational awareness. , 2018, , .		5
22	Passive os fingerprinting methods in the jungle of wireless networks. , 2018, , .		22
23	Honeypot testbed for network defence strategy evaluation. , 2017, , .		1
24	Toward Stream-Based IP Flow Analysis. , 2017, 55, 70-76.		18
25	On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts. , 2017, , .		11
26	Lessons learned from complex hands-on defence exercises in a cyber range. , 2017, , .		40
27	KYPO Cyber Range: Design and Use Cases. , 2017, , .		52
28	Situational Awareness: Detecting Critical Dependencies and Devices in a Network. Lecture Notes in Computer Science, 2017, , 173-178.	1.3	4
29	Convergent and reliable hybrid home networks. , 2016, , .		4
30	A performance benchmark for NetFlow data analysis on distributed stream processing systems. , 2016, , .		12
31	On Information Value of Top N Statistics. , 2016, , .		1
32	Network traffic characterisation using flow-based statistics. , 2016, , .		15
33	Network Defence Using Attacker-Defender Interaction Modelling. Lecture Notes in Computer Science, 2016, , 127-131.	1.3	1
34	HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting. Eurasip Journal on Information Security, 2016, 2016, .	2.2	60
35	Detecting Advanced Network Threats Using a Similarity Search. Lecture Notes in Computer Science, 2016, , 137-141.	1.3	1
36	A survey of methods for encrypted traffic classification and analysis. International Journal of Network Management, 2015, 25, 355-374.	2.2	229

#	ARTICLE	IF	CITATIONS
37	Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. , 2015, , .		17
38	Report on the 8th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014). Journal of Network and Systems Management, 2015, 23, 794-802.	4.9	2
39	Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX. IEEE Communications Surveys and Tutorials, 2014, 16, 2037-2064.	39.4	288
40	Report on the 7th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet. Journal of Network and Systems Management, 2014, 22, 289-296.	4.9	1
41	Cloud-based security research testbed: A DDoS use case. , 2014, , .		4
42	ACEMIND: The Smart Integrated Home Network. , 2014, , .		7
43	Next Generation Application-Aware Flow Monitoring. Lecture Notes in Computer Science, 2014, , 173-178.	1.3	4
44	Detection of DNS Traffic Anomalies in Large Networks. Lecture Notes in Computer Science, 2014, , 215-226.	1.3	1
45	Enhancing Network Security: Host Trustworthiness Estimation. Lecture Notes in Computer Science, 2014, , 63-68.	1.3	0
46	An investigation into teredo and 6to4 transition mechanisms: Traffic analysis. , 2013, , .		10
47	Design and Evaluation of HTTP Protocol Parsers for IPFIX Measurement. Lecture Notes in Computer Science, 2013, , 136-147.	1.3	15
48	Revealing and analysing modem malware. , 2012, , .		4
49	Traffic Measurement and Analysis of Building Automation and Control Networks. Lecture Notes in Computer Science, 2012, , 62-73.	1.3	8
50	Flow-Based Security Issue Detection in Building Automation and Control Networks. Lecture Notes in Computer Science, 2012, , 64-75.	1.3	11
51	Monitoring of Tunneled IPv6 Traffic Using Packet Decapsulation and IPFIX (Short Paper). Lecture Notes in Computer Science, 2011, , 64-71.	1.3	4
52	Embedded Malware - An Analysis of the Chuck Norris Botnet. , 2010, , .		16
53	Adaptive Multiagent System for Network Traffic Monitoring. IEEE Intelligent Systems, 2009, 24, 16-25.	4.0	43
54	Collaborative approach to network behaviour analysis based on hardware-accelerated FlowMon probes. International Journal of Electronic Security and Digital Forensics, 2009, 2, 35.	0.2	0

#	ARTICLE	IF	CITATIONS
55	Improving Anomaly Detection Error Rate by Collective Trust Modeling. Lecture Notes in Computer Science, 2008, , 398-399.	1.3	1
56	CAMNEP: An intrusion detection system for highspeed networks. Progress in Informatics, 2008, , 65.	0.2	12
57	Collaborative Approach to Network Behavior Analysis. Communications in Computer and Information Science, 2008, , 153-160.	0.5	1
58	High-Speed Network Traffic Acquisition for Agent Systems. , 2007, , .		3
59	Agent-Based Network Intrusion Detection System. , 2007, , .		6
60	Network Intrusion Detection by Means of Community of Trusting Agents. , 2007, , .		9
61	Collaborative Attack Detection in High-Speed Networks. Lecture Notes in Computer Science, 2007, , 73-82.	1.3	2
62	High-Performance Agent System for Intrusion Detection in Backbone Networks. Lecture Notes in Computer Science, 2007, , 134-148.	1.3	2
63	MULTIPARAMETER MULTICHANNEL ANALYSER SYSTEM FOR CHARACTERISATION OF MIXED NEUTRON " " GAMMA FIELD IN THE EXPERIMENTAL REACTOR LR-O. , 2003, , .		22