Fisa de verificare a standardelor minimale stabilite prin OM 6129 / 2016

Candidat **Conf. dr. ing. Ciprian-Pavel Oprișa**
Domeniul **Calculatoare si Tehnologia Informatiei**

Nr. Crt	Domeniul activ.	Categorii si restrictii		Subcategorii		Indicatori (kpi)	Numar	Punctaj
0	1	2		3		5	6	7
1	Activitatea didactica si profesionala (A1)	Carti de autor sau capitole [1] de specialitate in edituri cu ISBN	Carti / monografii	A1.1.1	internationale	50 sau 100 / nr. autori	0	0
				A1.1.2	nationale	50 / nr. autori	1	50
		Material didactic / lucrari didactice publicate la edituri cu ISBN	Manuale didactice	A1.2.1		40 / nr. autori	3	68
						Total punctaj (A1)		**118.00**
2	Activitatea de cercetare (A2)	Articole in reviste cotate ISI si lucrari in volumele unor manifestari stiintifice indexate ISI		A2.1		(25+30 * factor impact[3]) / nr. de autori	27	452.53
		Articole in reviste si volumele unor manifestari stiintifice indexate in alte baze de date internationale (BDI) [4]		A2.2		20 / nr. de autori	8	70.00
		Proprietate intelectuala, brevete de inventie, certificate ORDA		A2.3.1	internationale	35 / nr. de autori	0	0.00
				A2.3.2	nationale	25 / nr. de autori	0	0.00
		Granturi/proiecte de cercetare castigate prin competitie [6] sau contracte cu agenti economici in valoare de minim 10.000 dolari USA echivalent incasati [6]	Director / responsabil partener	A2.4.1.1	internationale	20 * ani de desfasurare	3	200.00
				A2.4.1.2	nationale	10 * ani de desfasurare	0	0.00
			Membru in echipa	A2.4.2.1	internationale	4 * ani de desfasurare	3	30.00
				A2.4.2.2	nationale	2 * ani de desfasurare	0	0.00
						Total punctaj (A2)		**752.53**
3	Recunoasterea si impactul activitatii (A3)	Citari [7] in carti, reviste si volume ale unor manifestari stiintifice		A3.1.1	carti, ISI [8]	8 / nr aut art. citat	74	324.81
				A3.1.2	BDI [4]	4 / nr aut art. citat	38	54.58
		Membru in colectivele de redactie sau comitetele stiintifice ale revistelor indexate ISI, chari, co-chair sau membru in comitetele de organizare ale manifestarilor stiintifice internationale indexate ISI [9]		A.3.2		10	1	10.00
		Membru in colectivele de redactie sau comitetele stiintifice ale revistelor indexate BDI, chari, co-chair sau membru in comitetele de organizare ale manifestarilor stiintifice internationale indexate BDI [4]		A3.3		6	0	0.00
		Premii in domeniu conferite de Academia Romana, ASTR, AOSR, sau premii internationale de prestigiu		A3.4		15	1	15.00
						Total punctaj (A3)		**404.39**

Conditii minimale Ai		Necesar Abilitare	Realizat
Nr.	Domeniu de activitate (A)		
A1	Activitatea didactica / profesionala (A1)	100	118.00
A2	Activitatea de cercetare (A2)	600	752.53
A3	Recunoasterea impactului activitatii (A3)	150	404.39
Total (A)		850	1274.92

Baza de date	H-index
Web of Science	6
Scopus	8
Google Scholar	9
Scor H-index	**7.2**

Conditii minimale obligatorii pe subcategorii		Necesar Abilitare	Realizat	
A1.1.1 - A1.1.2	Carti de specialitate	1 carte	1	
A2.1	Articole in reviste cotate si in volumele unor manifestari stiintifice indexate ISI proceedings	15 (3 art.ISI cotate Q1 sau Q2 [11])	27	(3 art.ISI Q1/Q2)
A2.4.1	Granturi / proiecte de cercetare castigate prin competitie (Director / Responsabil Partener)	2	3	
A3.1.1	Numar de citari in carti, reviste si volume ale unor manifestari stiintifice ISI (WOS) [12]	25	74	
	Factor de impact ISI cumulat pentru publicatii [13]	10	19.45	

Anexa: datele pentru calculul indeplinirii criteriilor A1.1.1, A1.1.2, A1.2.1

A1.1.1 - Carti, monografii, capitole ca autor - internationale

Nr.	Autori	Nr. Autori	Titlu capitol / carte	Editura	Anul	Punctaj
1						0
			Total carti internationale		0	0

A1.1.2 - Carti, monografii, capitole ca autor - nationale

Nr.	Autori	Nr. Autori	Titlu capitol / carte	Editura	Anul	Punctaj
1	C. Oprișa	1	Machine Learning Techniques for the Analysis and Detection of Malicious Software ISBN 978-606-737-511-4 https://biblioteca.utcluj.ro/files/carti-online-cu-coperta/511-4.pdf	UTPRESS	2021	50
			Total carti nationale		1	50

A1.2.1. Manuale didactice

Nr.	Autori	Nr. Autori	Titlu	Editura	Anul	Punctaj
1	C. Oprișa	1	Dezvoltarea aplicatiilor Android si securitatea dispozitivelor mobile ISBN 978-606-737-221-2	UTPRESS	2017	40
2	C. Oprișa, A. Hangan, M. Neagu, E. Cebuc, G. Sebestyen	5	Programare în limbaj de asamblare ISBN 978-606-737-333-2 https://biblioteca.utcluj.ro/files/carti-online-cu-coperta/333-2.pdf	UTPRESS	2018	8
3	C. Oprișa, A. Coleșa	2	Sisteme de operare. Îndrumător de laborator ISBN 978-606-737-512-1 https://biblioteca.utcluj.ro/files/carti-online-cu-coperta/512-1.pdf	UTPRESS	2021	20
			Total materiale didactice		3	68

Anexa: datele pentru calculul indeplinirii criteriilor A2.1, A2.2

A2.1 Articole in reviste cotate si in volumele unor manifestari stiintifice indexate ISI proceedings 25 +30* factor impact / nr. Autori

Nr.	Autori	Titlu lucrare / revista (conferinta)	Factor de impact	Nr. Autori	Punctaj	
1	C. Pop, V. Chifu, I. Salomie, M. Dinșoreanu, T. David, V. Acreţoaie, A. Nagy, C. Oprișa	Biologically-inspired Clustering of Semantic Web Services. Birds or Ants Intelligence?. In Concurrency and Computation: Practice and Experience, 2012 https://doi.org/10.1002/cpe.1853 https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.1853	1.5	8	8.75	
2	C. Oprișa, A. Coleșa, I. Ignat	A Metric for Evaluating the Usability of File Systems. In 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2012 https://doi.org/10.1109/SYNASC.2012.45 https://ieeexplore.ieee.org/abstract/document/6481027	0.25	3	10.83	
3	C. Oprișa, G. Cabău, A. Coleșa	From plagiarism to malware detection. In 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2014 https://doi.org/10.1109/SYNASC.2013.37 https://ieeexplore.ieee.org/abstract/document/6821154	0.25	3	10.83	
4	C. Oprișa, M. Checicheș, A. Nândrean	Locality-sensitive hashing optimizations for fast malware clustering. In IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP), 2014 https://doi.org/10.1109/ICCP.2014.6936960 https://ieeexplore.ieee.org/abstract/document/6936960	0.25	3	10.83	
5	C. Oprișa, G. Cabău, G. Sebestyen Pal	A new string distance for computing binary code similarities. In IEEE 10th International Conference on Intelligent Computer Communication and Processing (ICCP), 2014 https://doi.org/10.1109/ICCP.2014.6936986 https://ieeexplore.ieee.org/abstract/document/6936986	0.25	3	10.83	
6	C. Oprișa, G. Cabău, A. Coleșa	Automatic code features extraction using bio-inspired algorithms. In Journal of Computer Virology and Hacking Techniques, 2014 https://doi.org/10.1007/s11416-013-0191-6 https://link.springer.com/article/10.1007/s11416-013-0191-6	1.9	3	27.33	
7	C. Oprișa	A MinHash Approach for Clustering Large Collections of Binary Programs. In 20th International Conference on System Controls and Computer Science 2015, 2015 https://doi.org/10.1109/CSCS.2015.27 https://ieeexplore.ieee.org/abstract/document/7168423	0.25	1	32.5	
8	C. Oprișa, G. Cabău, G. Sebestyen Pal	Malware clustering using suffix trees. In JOURNAL OF COMPUTER VIROLOGY AND HACKING TECHNIQUES, 2016 https://doi.org/10.1007/s11416-014-0227-6 https://link.springer.com/article/10.1007/s11416-014-0227-6	1.9	3	27.33	
9	C. Oprișa, N. Ignat	A Measure of Similarity for Binary Programs with a Hierarchical Structure. In 11th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2015 https://doi.org/10.1109/ICCP.2015.7312615 https://ieeexplore.ieee.org/abstract/document/7312615	0.25	2	16.25	
10	C. Oprișa, G. Cabău, G. Sebestyen Pal	Semi-automated Verdicts Assignment for Potentially Malicious Programs. In 11th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2015 https://doi.org/10.1109/ICCP.2015.7312616 https://ieeexplore.ieee.org/abstract/document/7312616	0.25	3	10.83	
11	C. Oprișa, D. Gavriluț, G. Cabău	A scalable approach for detecting plagiarized mobile applications. In KNOWLEDGE AND INFORMATION SYSTEMS, 2016 https://doi.org/10.1007/s10115-015-0903-y https://link.springer.com/article/10.1007/s10115-015-0903-y	3.1	3	39.33	Q2
12	G. Cabău, M. Buhu, C. Oprișa	Malware classification using filesystem footprints. In IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2016 https://doi.org/10.1109/AQTR.2016.7501294 https://ieeexplore.ieee.org/abstract/document/7501294	0.25	3	10.83	
13	G. Cabău, M. Buhu, C. Oprișa	Malware classification based on dynamic behavior. In 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2016 https://doi.org/10.1109/SYNASC.2016.057 https://ieeexplore.ieee.org/abstract/document/7829629	0.25	3	10.83	
14	D. Domnița, C. Oprișa	A Genetic Algorithm for Obtaining Memory Constrained Near-Perfect Hashing. In 21st IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR THETA), 2018 https://doi.org/10.1109/AQTR.2018.8402794 https://ieeexplore.ieee.org/abstract/document/8402794	0.25	2	16.25	
15	F. Moldovan, C. Oprișa	A Framework for Threats Analysis Using Software-Defined Networking. In 14th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2018 https://doi.org/10.1109/ICCP.2018.8516636 https://ieeexplore.ieee.org/abstract/document/8516636	0.25	2	16.25	
16	A. Lungana-Niculescu, A. Coleșa, C. Oprișa	False Positive Mitigation in Behavioral Malware Detection Using Deep Learning. In 14th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2018 https://doi.org/10.1109/ICCP.2018.8516611 https://ieeexplore.ieee.org/abstract/document/8516611	0.25	3	10.83	
17	A. Mihalca, C. Oprișa, R. Potolea	Hunting for Malware Code in Massive Collections. In 2020 22nd IEEE International Conference on Automation, Quality and Testing, Robotics - THETA, AQTR 2020 - Proceedings, 2020 https://doi.org/10.1109/AQTR49680.2020.9129948 https://ieeexplore.ieee.org/abstract/document/9129948	0.25	3	10.83	
18	F. Moldovan, P. Sătmărean, C. Oprișa	An Analysis of HTTP Attacks on Home IoT Devices. In 2020 22nd IEEE International Conference on Automation, Quality and Testing, Robotics - THETA, AQTR 2020 - Proceedings, 2020 https://doi.org/10.1109/AQTR49680.2020.9129980 https://ieeexplore.ieee.org/abstract/document/9129980	0.25	3	10.83	
19	P. Sătmărean, C. Oprișa	Web Servers Protection Using Anomaly Detection for HTTP Requests. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020 https://doi.org/10.1007/978-3-030-42051-2_6 https://link.springer.com/chapter/10.1007/978-3-030-42051-2_6	0.25	2	16.25	
20	O. Valea, C. Oprișa	Towards Pentesting Automation Using the Metasploit Framework. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, ICCP 2020, 2020 https://doi.org/10.1109/ICCP51029.2020.9266234 https://ieeexplore.ieee.org/abstract/document/9266234	0.25	2	16.25	
21	A. Crișan, G. Florea, L. Halasz, C. Lemnaru, C. Oprișa	Detecting Malicious URLs Based on Machine Learning Algorithms and Word Embeddings. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, ICCP 2020, 2020 https://doi.org/10.1109/ICCP51029.2020.9266139 https://ieeexplore.ieee.org/abstract/document/9266139	0.25	5	6.5	
22	C.G. Artene, C. Oprișa, C.N. Buțincu, F. Leon	Finding Patient Zero and Tracking Narrative Changes in the Context of Online Disinformation Using Semantic Similarity Analysis. Mathematics 11.9, 2023 https://doi.org/10.3390/math11092053 https://www.mdpi.com/2227-7390/11/9/2053	2.2	4	22.75	Q1
23	A. Mihalca, C. Oprișa	Impact of Library Code in Binary Similarity Systems, International Conference on Ubiquitous Security, 2023 https://doi.org/10.1007/978-981-97-1274-8_3 https://link.springer.com/chapter/10.1007/978-981-97-1274-8_3	0.25	2	16.25	
24	A.A. Jîrcan, C. Oprisa	MEPHISTO: a Red Team Tool for Offensive Security, 2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP), 2024 https://doi.org/10.1109/ICCP63557.2024.10793019 https://ieeexplore.ieee.org/abstract/document/10793019	0.25	2	16.25	
25	A. Dumitras, C.M. Mocan, C. Oprisa	A Feature Engineering Approach for Detecting Phishing E-mails, 2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP), 2024 https://doi.org/10.1109/ICCP63557.2024.10793001 https://ieeexplore.ieee.org/abstract/document/10793001	0.25	3	10.83	
26	D.E. Petrean, R. Potolea, C. Oprisa	Packed Code Detection using Shannon Entropy and Homomorphic Encrypted Executables, 2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP), 2024 https://doi.org/10.1109/ICCP63557.2024.10793050 https://ieeexplore.ieee.org/abstract/document/10793050	0.25	3	10.83	
27	R. Petrache, C. Oprisa, C. Lemnaru	Unveiling Hidden Structures: Multi-Platform IoT Malware Analysis Using Graph Embeddings, IEEE Access, 2025 https://doi.org/10.1109/ACCESS.2025.3583549 https://ieeexplore.ieee.org/abstract/document/11052297	3.6	3	44.33	Q2
			Factor impact cumulat	**19.45**		
			Total punctaj A2.1		**27**	**452.53**

A2.2. Articole in reviste si volumele unor manifestari stiintifice indexate in alte baze de date internationale (BDI) 20 / nr. de autori

Nr.	Autori	Titlu lucrare / revista (conferinta)	Baza de date	Nr. Autori	Punctaj
1	A. Nagy, C. Oprişa, I. Salomie, C. Pop, V. Chifu, M. Dinşoreanu	Particle swarm optimization for clustering semantic web services. In Proceedings - 2011 10th International Symposium on Parallel and Distributed Computing, ISPDC 2011, 2011 https://doi.org/10.1109/ISPDC.2011.33 https://ieeexplore.ieee.org/abstract/document/6108270	SCOPUS, DBLP, IEEE	6	3.33
2	C. Oprişa, G. Cabău, G. Sebestyen Pal	Multi-centroid Cluster Analysis in Malware Research. In Advances in Intelligent Systems and Computing, 2018 https://doi.org/10.1007/978-3-319-69710-9_7 https://link.springer.com/chapter/10.1007/978-3-319-69710-9_7	SCOPUS	3	6.67
3	A. Mihalca, C. Oprişa	Full Content Search in Malware Collections. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019 https://doi.org/10.1007/978-3-030-12085-6_12 https://link.springer.com/chapter/10.1007/978-3-030-12085-6_12	SCOPUS	2	10.00
4	R. Rentea, C. Oprişa	Fast Clustering for Massive Collections of Malicious URLs, 2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP), 2021 https://doi.org/10.1109/ICCP53602.2021.9733623 https://ieeexplore.ieee.org/abstract/document/9733623	SCOPUS, IEEE	2	10.00
5	V. Moşolea, C. Oprişa	Detecting Domain Generation Algorithms in Malware Traffic Using Constrained Resources, 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398684 https://ieeexplore.ieee.org/abstract/document/10398684	SCOPUS, IEEE	2	10.00
6	M. Mărmureanu, C. Oprişa	MITRE Tactics Inference from Splunk Queries, 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398612 https://ieeexplore.ieee.org/abstract/document/10398612	SCOPUS, IEEE	2	10.00
7	A. Păcurar, C. Oprişa	Using Artificial Intelligence to Fight Clickbait in Romanian News Articles, 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398606 https://ieeexplore.ieee.org/abstract/document/10398606	SCOPUS, IEEE	2	10.00
8	B.A. Grama, C. Oprisa	A Virtual Machine Management Platform in Computer Science Education, 2024 11th International Conference on Electrical and Electronics Engineering (ICEEE), 2024 https://doi.org/10.1109/ICEEE62185.2024.10779309 https://ieeexplore.ieee.org/document/10779309	SCOPUS, IEEE	2	10.00
		Total punctaj A2.2		**8**	**70.00**

Anexa: datele pentru calculul indeplinirii criteriilor A2.3.1, A2.3.2

A2.3.1 Proprietate intelectuala, brevete de inventie, certificate ORDA - Internationale - Punctaj: 35 / nr. Autori 35 / nr. de autori

Nr.	Tip	Denumire	Anul	Nr. Autori	Punctaj
1					0
			Total punctaj A2.3.1	0	0

A2.3.2 Proprietate intelectuala, brevete de inventie, certificate ORDA - nationale - Punctaj: 25 / nr. Autori 25 / nr. de autori

Nr.	Tip	Denumire	Anul	Nr. Autori	Punctaj
1					0
			Total punctaj A2.3.2	0	0

Anexa: datele pentru calculul indeplinirii criteriilor A2.4.1.1, A2.4.1.2, A2.4.2.1, A2.4.2.2

A2.4.1.1 Granturi/proiecte castigate prin competitie: Director Proiect - internationale 20 * Nr. Ani

Nr.	Tip: nat / internat.	Denumire proiect	Perioada	Nr. Ani	Punctaj
1	International	SMESEC – Cybersecurity for Small and Medium-Sized Enterprises Horizon 2020, GA 740787 https://cordis.europa.eu/project/id/740787	2017-2020	3	60
2	International	CONSOLE - Cybersecurity for Resilient Software Development Digital Europe, GA 101128070 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101128070	2023-2026	3	60
3	International	EU-INSPIRE - INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU workforcE Digital Europe, GA 101190054 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101190054	2025-2028	4	80
		Total punctaj A2.4.1.1		**3**	**200**

A2.4.1.2 Granturi/proiecte castigate prin competitie: Director Proiect - nationale 10*Nr. Ani

Nr.	Tip: nat / internat.	Denumire proiect	Perioada	Nr. Ani	Punctaj
1				0	0
2				0	0
		Total punctaj A2.4.1.2		**0**	**0**

A2.4.2.1 Granturi/proiecte castigate prin competitie: membru in echipa - Internationale 4 * Nr. Ani

Nr.	Tip: nat / internat.	Denumire proiect	Perioada	Nr. Ani	Punctaj
1	International	CIPSEC – Enhancing Critical Infrastructure Protection with innovative SECurity framework Horizon 2020, GA 700378 https://cordis.europa.eu/project/id/700378	2016-2019	3	12
2	International	GEIGER Cybersecurity Counter Horizon 2020, GA 883588 https://cordis.europa.eu/project/id/883588	2020-2022	2.5	10
3	International	Cybersecurity Seminars Nr. contract 2024-348638 https://cyberseminars.withgoogle.com/grantees	2024-2026	2	8
		Total punctaj A2.4.2.1		**3**	**30**

A2.4.2.2 Granturi/proiecte castigate prin competitie: membru in echipa - nationale 2*Nr. Ani

Nr.	Tip: nat / internat.	Denumire proiect	Perioada	Nr. Ani	Punctaj
1					0
2					0
		Total punctaj A2.4.2.2		**0**	**0**

Anexa: datele pentru calculul indeplinirii criteriilor A3.1.1, A3.1.2

A3.1.1 Citari in carti, reviste si volume ale unor manifestari stiintifice - Carti, ISI

Nr.	Articol citat	Articol care citeaza	Nr. autori art.citat	Punctaj	2*Punctaj [8]
1	A. Nagy, C. Oprişa, I. Salomie, C. Pop, V. Chifu, M. Dinşoreanu. Particle swarm optimization for clustering semantic web servicesParticle swarm optimization for clustering semantic web services. In Proceedings - 2011 10th International Symposium on Parallel and Distributed Computing, ISPDC 2011, 2011 https://doi.org/10.1109/ISPDC.2011.33 https://ieeexplore.ieee.org/abstract/document/6108270	I.R.P. Joe and P. Varalakshmi. A two phase approach for efficient clustering of web services. In Advances in Intelligent Systems and Computing, 2016 https://doi.org/10.1007/978-981-10-0251-9_17 https://link.springer.com/chapter/10.1007/978-981-10-0251-9_17	6	1.33	
		G. Spezzano. Using Service Clustering and Self-Adaptive MOPSO-CD for QoS-Aware Cloud Service Selection. In Procedia Computer Science, 2016 https://doi.org/10.1016/j.procs.2016.04.245 https://www.sciencedirect.com/science/article/pii/S1877050916302782	6	1.33	
2	C.B. Pop, V.R. Chifu, I. Salomie, M. Dinsoreanu, T. David, V. Acretoaie, A. Nagy and C. Oprisa. Biologically-inspired clustering of semantic Web services. Birds or ants intelligence?. In Concurrency Computation Practice and Experience, 2012 https://doi.org/10.1002/cpe.1853 https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.1853	ZhangBing Zhou, Mohamed Sellami, Walid Gaaloul, Mahmoud Barhamgi and Bruno Defude. Data Providing Services Clustering and Management for Facilitating Service Discovery and Replacement. In IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, 2013 https://doi.org/10.1109/TASE.2012.2237551 https://ieeexplore.ieee.org/document/6422338	8	2	Q1
		G. Tian, P. Liu, Y. Peng and C. Sun. Tagging augmented neural topic model for semantic sparse Web service discovery. In Concurrency Computation, 2018 https://doi.org/10.1002/cpe.4448 https://onlinelibrary.wiley.com/doi/10.1002/cpe.4448	8	1	
		X.P. Liu, W.C. Dou, X. Wang. User Grouping for Sharing Services with Capacity Limit. In IEEE TRANSACTIONS ON SERVICES COMPUTING, 2021 https://doi.org/10.1109/TSC.2018.2810120 https://ieeexplore.ieee.org/document/8303754	8	2	Q1
		N. Agarwal, G. Sikka, L.K. Awasthi. A systematic literature review on web service clustering approaches to enhance service discovery, selection and recommendation. Computer Science Review, 2022 https://doi.org/10.1016/j.cosrev.2022.100498 https://www.sciencedirect.com/science/article/pii/S157401372200034X	8	1	
		L. Purohit, S.S. Rathore, S. Kumar. Feature selection and clustering based web service selection using QoSs. Applied Intelligence, 2023 https://doi.org/10.1007/s10489-022-04042-w https://link.springer.com/article/10.1007/s10489-022-04042-w	8	1	
3	C. Oprişa, G. Cabău and A. Coleşa. From plagiarism to malware detection. In Proceedings - 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2013, 2013 https://doi.org/10.1109/SYNASC.2013.37 https://ieeexplore.ieee.org/abstract/document/6821154	D. Qiu, J. Sun and H. Li. Improving Similarity Measure for Java Programs Based on Optimal Matching of Control Flow Graphs. In International Journal of Software Engineering and Knowledge Engineering, 2015 https://doi.org/10.1142/S0218194015500229 https://www.worldscientific.com/doi/abs/10.1142/S0218194015500229	3	2.67	
		M. Novak, M. Joy and D. Kermek. Source-code Similarity Detection and Detection Tools Used in Academia: A Systematic Review. In ACM TRANSACTIONS ON COMPUTING EDUCATION, 2019 https://doi.org/10.1145/3313290 https://dl.acm.org/doi/10.1145/3313290	3	5.34	Q1
4	C. Oprisa, M. Checiches and A. Nandrean. Locality-sensitive hashing optimizations for fast malware clustering. In Proceedings - 2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing, ICCP 2014, 2014 https://doi.org/10.1109/ICCP.2014.6936960 https://ieeexplore.ieee.org/abstract/document/6936960	A.P. Namanya, I.U. Awan, J.P. Disso and M. Younas. Similarity hash based scoring of portable executable files for efficient malware detection in IoT. In Future Generation Computer Systems, 2020 https://doi.org/10.1016/j.future.2019.04.044 https://www.sciencedirect.com/science/article/pii/S0167739X18325913	3	5.34	Q1
		N. Nissim, O. Lahav, A. Cohen, Y. Elovici and L. Rokach. Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud. In Computers and Security, 2019 https://doi.org/10.1016/j.cose.2019.101590 https://www.sciencedirect.com/science/article/pii/S016740481831188X	3	5.34	Q1
		Y. Cohen and D. Hendler. Scalable Detection of Server-Side Polymorphic Malware. In Knowledge-Based Systems, 2018 https://doi.org/10.1016/j.knosys.2018.05.024 https://www.sciencedirect.com/science/article/pii/S0950705118302545	3	5.34	Q1
		M. Howard, A. Pfeffer, M. Dalai and M. Reposa. Predicting signatures of future malware variants. In Proceedings of the 2017 12th International Conference on Malicious and Unwanted Software, MALWARE 2017, 2018 https://doi.org/10.1109/MALWARE.2017.8323965 https://ieeexplore.ieee.org/document/8323965	3	2.67	
		A.P. Namanya, Q.K.A. Mirza, H. Al-Mohannadi, I.U. Awan and J.F.P. Disso. Detection of malicious portable executables using evidence combinational theory with fuzzy hashing. In Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016, 2016 https://doi.org/10.1109/FiCloud.2016.21 https://ieeexplore.ieee.org/document/7575849	3	2.67	
		M. Arefkhani and M. Soryani. Malware clustering using image processing hashes. In Iranian Conference on Machine Vision and Image Processing, MVIP, 2016 https://doi.org/10.1109/IranianMVIP.2015.7397539 https://ieeexplore.ieee.org/document/7397539	3	2.67	
		G. Cabău, A.T. Sălăgean and G. Sebestyen-Pal. Realtime file processing based on Map-Reduce framework. In Proceedings - 2015 IEEE 11th International Conference on Intelligent Computer Communication and Processing, ICCP 2015, 2015 https://doi.org/10.1109/ICCP.2015.7312716 https://ieeexplore.ieee.org/document/7312716	3	2.67	
		N. Tonci, S. Rivault, M. Bamh, S. Robert, S. Limet, M. Torquati. LSH SimilarityJoin pattern in FastFlow. International Journal of Parallel Programming, 2024 https://doi.org/10.1007/s10766-024-00772-1 https://link.springer.com/article/10.1007/s10766-024-00772-1	3	2.67	
		T. Muralidharan, A. Cohen, N. Gerson, N. Nissim. File packing from the malware perspective: Techniques, analysis approaches, and directions for enhancements, 2022 https://doi.org/10.1145/3530810 https://dl.acm.org/doi/abs/10.1145/3530810	3	5.34	Q1
		M. Petersen, C. Hardegen, U. Buehler.Generative Pattern Dissemination for Collaborative Intrusion Detection. In 2023 6th Conference on Cloud and Internet of Things (CIoT), 2023 https://doi.org/10.1109/CIoT57267.2023.10084911 https://ieeexplore.ieee.org/document/10084911	3	2.67	
		A. Cohen, N. Nissim and Y. Elovici. MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images. In IEEE ACCESS, 2020 https://doi.org/10.1109/ACCESS.2020.2969022 https://ieeexplore.ieee.org/abstract/document/8967109	3	5.34	Q2
		J. Gonzalez. If at first you don't succeed, trie, trie again: Correcting TLSH scalability claims for large-dataset malware forensics. In FORENSIC SCIENCE INTERNATIONAL-DIGITAL INVESTIGATION, 2025 https://doi.org/10.1016/j.fsidi.2025.301922 https://www.sciencedirect.com/science/article/pii/S2666281725000617	3	2.67	
5	C. Oprisa. A MinHash approach for clustering large collections of binary programs. In Proceedings - 2015 20th International Conference on Control Systems and Computer Science, CSCS 2015, 2015 https://doi.org/10.1109/CSCS.2015.27 https://ieeexplore.ieee.org/abstract/document/7168423	R. Hassanian-esfahani and M.-J. Kargar. Sectional MinHash for near-duplicate detection. In Expert Systems with Applications, 2018 https://doi.org/10.1016/j.eswa.2018.01.014 https://www.sciencedirect.com/science/article/pii/S0957417418300149	1	16	Q1
		S. Wang, L. Zhang, Y. Zhang, J. Sun, C. Pang, G. Tian and N. Cao. Natural language semantic construction based on cloud database. In Computers, Materials and Continua, 2018 https://doi.org/10.32604/cmc.2018.03884 https://www.techscience.com/cmc/v57n3/22990	1	8	
6	C. Oprişa, G. Cabău and G. Sebestyen Pal. Malware clustering using suffix trees. In Journal of Computer Virology and Hacking Techniques, 2016 https://doi.org/10.1007/s11416-014-0227-6 https://link.springer.com/article/10.1007/s11416-014-0227-6	M.H. Alaeiyan and S. Parsa. Automatic loop detection in the sequence of system calls. In Conference Proceedings of 2015 2nd International Conference on Knowledge-Based Engineering and Innovation, KBEI 2015, 2016 https://doi.org/10.1109/KBEI.2015.7436133 https://ieeexplore.ieee.org/document/7436133	3	2.67	
		R.A. Ognev, E.V. Zhukovskii and D.P. Zegzhda. Clustering of Malicious Executable Files Based on the Sequence Analysis of System Calls. In Automatic Control and Computer Sciences, 2019 https://doi.org/10.3103/S0146411619080212 https://link.springer.com/article/10.3103/S0146411619080212	3	2.67	
		Yehonatan Cohen and Danny Hendler. Scalable Detection of Server-Side Polymorphic Malware. In KNOWLEDGE-BASED SYSTEMS, 2018 https://doi.org/10.1016/j.knosys.2018.05.024 https://www.sciencedirect.com/science/article/pii/S0950705118302545	3	5.34	Q1
		C.K. Ng, F. Jiang, L.Y. Zhang and W. Zhou. Static malware clustering using enhanced deep embedding method. In Concurrency Computation, 2019 https://doi.org/10.1002/cpe.5234 https://onlinelibrary.wiley.com/doi/10.1002/cpe.5234	3	2.67	

		S.K.J. Rizvi, M.M. Fraz.Robust malware clustering of windows portable executables using ensemble latent representation and distribution modeling. Concurrency and Computation: Practice and Experience, 2023 https://doi.org/10.1002/cpe.7621 https://onlinelibrary.wiley.com/doi/10.1002/cpe.7621	3	2.67	
		Fatima Al Shamsi, Wei Lee Woon and Zeyar Aung. Discovering Similarities in Malware Behaviors by Clustering of API Call Sequences. In 25th International Conference on Neural Information Processing (ICONIP), 2018 https://doi.org/10.1007/978-3-030-04212-7_11 https://link.springer.com/chapter/10.1007/978-3-030-04212-7_11	3	2.67	
7	C. Oprişa, D. Gavriluţ and G. Cabău. A scalable approach for detecting plagiarized mobile applications. In Knowledge and Information Systems, 2016 https://doi.org/10.1007/s10115-015-0903-y https://link.springer.com/article/10.1007/s10115-015-0903-y	B. Fang, Y. Jia, X. Li, A. Li and X. Wu. Big Search in Cyberspace. In IEEE Transactions on Knowledge and Data Engineering, 2017 https://doi.org/10.1109/TKDE.2017.2699675 https://ieeexplore.ieee.org/document/7914645	3	5.34	Q1
		G. Ajaeiya, I.H. Elhajj, A. Chehab, A. Kayssi and M. Kneppers. Mobile Apps identification based on network flows. In Knowledge and Information Systems, 2018 https://doi.org/10.1007/s10115-017-1111-8 https://link.springer.com/article/10.1007/s10115-017-1111-8	3	5.34	Q2
8	G. Cabau, M. Buhu and C.P. Oprisa. Malware classification based on dynamic behavior. In Proceedings - 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2016, 2017 https://doi.org/10.1109/SYNASC.2016.057 https://ieeexplore.ieee.org/abstract/document/7829629	J. Fu, J. Xue, Y. Wang, Z. Liu and C. Shan. Malware Visualization for Fine-Grained Classification. In IEEE Access, 2018 https://doi.org/10.1109/ACCESS.2018.2805301 https://ieeexplore.ieee.org/abstract/document/8290767	3	5.34	Q2
		G. D'Angelo, M. Ficco and F. Palmieri. Malware detection in mobile environments based on Autoencoders and API-images. In Journal of Parallel and Distributed Computing, 2020 https://doi.org/10.1016/j.jpdc.2019.11.001 https://www.sciencedirect.com/science/article/pii/S0743731519302436	3	5.34	Q1
		Y. Zhang, X. Chang, Y. Lin, J. Misic and V.B. Misic. Exploring Function Call Graph Vectorization and File Statistical Features in Malicious PE File Classification. In IEEE Access, 2020 https://doi.org/10.1109/ACCESS.2020.2978335 https://ieeexplore.ieee.org/abstract/document/9023948	3	5.34	Q2
		L. Yang and J. Liu. TuningMalconv: Malware Detection with Not Just Raw Bytes. In IEEE Access, 2020 https://doi.org/10.1109/ACCESS.2020.3014245 https://ieeexplore.ieee.org/abstract/document/9157851	3	5.34	Q2
		J.W. Mikhail, J.C. Williams and G.R. Roelke. procmonML: Generating evasion resilient host-based behavioral analytics from tree ensembles. In Computers and Security, 2020 https://doi.org/10.1016/j.cose.2020.102002 https://www.sciencedirect.com/science/article/pii/S0167404820302753	3	5.34	Q1
		Vinita Verma, Sunil K. Muttoo and V. B. Singh. Multiclass malware classification via first- and second-order texture statistics. In COMPUTERS & SECURITY, 2020 https://doi.org/10.1016/j.cose.2020.101895 https://www.sciencedirect.com/science/article/pii/S0167404820301681	3	5.34	Q1
		T.N. Witte. Phantom malware: Conceal malicious actions from malware detection techniques by imitating user activity. In IEEE Access, 2020 https://doi.org/10.1109/ACCESS.2020.3021743 https://ieeexplore.ieee.org/abstract/document/9186656	3	5.34	Q2
		M. Ficco. Detecting IoT malware by markov chain behavioral models. In Proceedings - 2019 IEEE International Conference on Cloud Engineering, IC2E 2019, 2019 https://doi.org/10.1109/IC2E.2019.00037 https://ieeexplore.ieee.org/document/8790169	3	2.67	
		C.S. Veerappan, P.L.K. Keong, Z. Tang and F. Tan. Taxonomy on malware evasion countermeasures techniques. In IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, 2018 https://doi.org/10.1109/WF-IoT.2018.8355202 https://ieeexplore.ieee.org/document/8355202	3	2.67	
		Luo, X., Fan, H., Yin, L., Jia, S., Zhao, K. and Yang, H. CAG-Malconv: A Byte-Level Malware Detection Method With CBAM and Attention-GRU. IEEE Transactions on Network and Service Management, 2024 https://doi.org/10.1109/TNSM.2024.3424565 https://ieeexplore.ieee.org/document/10589435	3	5.34	Q1
		A.S.M. Ahsan-Ul-Haque, M.S. Hossain and M. Atiquzzaman. Sequencing System Calls for Effective Malware Detection in Android. In 2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings, 2018 https://doi.org/10.1109/GLOCOM.2018.8647967 https://ieeexplore.ieee.org/document/8647967	3	2.67	
		Aurangzeb, S., Aleem, M., Khan, M.T., Loukas, G. and Sakellari, G. AndroDex: Android Dex images of obfuscated malware. Scientific data, 2024 https://doi.org/10.1038/s41597-024-03027-3 https://www.nature.com/articles/s41597-024-03027-3	3	5.34	Q1
		Chuang, H.Y., Chen, J.L. and Ma, Y.W. Malware Detection and Classification Based on Graph Convolutional Networks and Function Call Graphs. IT Professional, 2023 https://doi.org/10.1109/MITP.2023.3264509 https://ieeexplore.ieee.org/abstract/document/10174714	3	5.34	Q2
		Xing, X., Jin, X., Elahi, H., Jiang, H. and Wang, G. A malware detection approach using autoencoder in deep learning. Ieee Access, 2022 https://doi.org/10.1109/ACCESS.2022.3155695 https://ieeexplore.ieee.org/abstract/document/9723074	3	5.34	Q2
		Yang, C., Xu, J., Liang, S., Wu, Y., Wen, Y., Zhang, B. and Meng, D. DeepMal: maliciousness-Preserving adversarial instruction learning against static malware detection. Cybersecurity, 2021 https://doi.org/10.1186/s42400-021-00079-5 https://link.springer.com/article/10.1186/s42400-021-00079-5	3	5.34	Q1
		Ahmad Jalal, Majid Ali Khan Quaid and Abdul S. Hasan. Wearable Sensor-Based Human Behavior Understanding and Recognition in Daily Life for Smart Environments. In 16th International Conference on Frontiers of Information Technology (FIT), 2018 https://doi.org/10.1109/FIT.2018.00026 https://ieeexplore.ieee.org/abstract/document/8616975	3	2.67	
9	A.M. Lungana-Niculescu, A. Colesa and C. Oprisa. False positive mitigation in behavioral malware detection using deep learning. In Proceedings - 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing, ICCP 2018, 2018 https://doi.org/10.1109/ICCP.2018.8516611 https://ieeexplore.ieee.org/abstract/document/8516611	D. López, I. Aguilera-Martos, M. García-Barzana, F. Herrera, D. Garcia-Gil, J. Luengo. Fusing anomaly detection with false positive mitigation methodology for predictive maintenance under multivariate time series. Information Fusion, 2023 https://doi.org/10.1016/j.inffus.2023.101957 https://www.sciencedirect.com/science/article/pii/S1566253523002737	3	5.34	Q1
		M. Rhode, L. Tuson, P. Burnap and K. Jones. LAB to SOC: Robust Features for Dynamic Malware Detection. In Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - DSN 2019 Industry Track, 2019 https://doi.org/10.1109/DSN-Industry.2019.00010 https://ieeexplore.ieee.org/document/8805762	3	2.67	
10	C. Oprişa, G. Cabău and G. Sebestyen Pal. Multi-centroid Cluster Analysis in Malware Research. In Advances in Intelligent Systems and Computing, 2018 https://doi.org/10.1007/978-3-319-69710-9_7 https://link.springer.com/chapter/10.1007/978-3-319-69710-9_7	S.A. Abed and H.M. Rais. Solving the Minimum Dominating Set Problem of Partitioned Graphs Using a Hybrid Bat Algorithm. In 4th International Conference of Reliable Information and Communication Technology (IRICT), 2019 https://doi.org/10.1007/978-3-030-33582-3_37 https://link.springer.com/chapter/10.1007/978-3-030-33582-3_37	3	2.67	
11	A. Crişan, G. Florea, L. Halasz, C. Lemnaru, C. Oprişa. Detecting Malicious URLs Based on Machine Learning Algorithms and Word Embeddings. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, 2020 https://doi.org/10.1109/ICCP51029.2020.9266139 https://ieeexplore.ieee.org/abstract/document/9266139	Loh, P.K., Lee, A.Z. and Balachandran, V. Towards a hybrid security framework for phishing awareness education and defense. Future Internet, 2024 https://doi.org/10.3390/fi16030086 https://www.mdpi.com/1999-5903/16/3/86	5	3.2	Q2
		Alsaffar, M., Aljaloud, S., Mohammed, B.A., Al-Mekhlafi, Z.G., Almurayziq, T.S., Alshammari, G. and Alshammari, A. Detection of Web Cross-Site Scripting (XSS) Attacks. Electronics, 2022 https://doi.org/10.3390/electronics11142212 https://www.mdpi.com/2079-9292/11/14/2212	5	1.6	
		Aljabri, M., Altamimi, H.S., Albelali, S.A., Al-Harbi, M., Alhuraib, H.T., Alotaibi, N.K., Alahmadi, A.A., Alhaidari, F., Mohammad, R.M.A. and Salah, K. Detecting malicious URLs using machine learning techniques: review and research directions. IEEE Access, 2022 https://doi.org/10.1109/ACCESS.2022.3222307 https://ieeexplore.ieee.org/abstract/document/9950508	5	3.2	Q2
		Yuan, J., Liu, Y. and Yu, L. A novel approach for malicious URL detection based on the joint model. Security and Communication Networks, 2021 https://doi.org/10.1155/2021/4917016 https://onlinelibrary.wiley.com/doi/full/10.1155/2021/4917016	5	1.6	
		Zahid, S., Mazhar, M.S., Abbas, S.G., Hanif, Z., Hina, S. and Shah, G.A. Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. Internet of Things, 2023 https://doi.org/10.1016/j.iot.2023.100766 https://www.sciencedirect.com/science/article/pii/S2542660523000896	2	8	Q1
		Holm, H. Lore a red team emulation tool. IEEE Transactions on Dependable and Secure Computing, 2022 https://doi.org/10.1109/TDSC.2022.3160792 https://ieeexplore.ieee.org/document/9740000	2	8	Q1

12	O. Valea, C. Oprişa. Towards Pentesting Automation Using the Metasploit Framework. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, 2020 https://doi.org/10.1109/ICCP51029.2020.9266234 https://ieeexplore.ieee.org/abstract/document/9266234	Nebbione, G. and Calzarossa, M.C. A methodological framework for ai-assisted security assessments of active directory environments. Ieee Access, 2023 https://doi.org/10.1109/ACCESS.2023.3244490 https://ieeexplore.ieee.org/abstract/document/10042410	2	8	Q2
		Kumar, Y. and Subba, B. Stacking ensemble-based HIDS framework for detecting anomalous system processes in windows based operating systems using multiple word embedding. Computers & Security, 2023 https://doi.org/10.1016/j.cose.2022.102961 https://www.sciencedirect.com/science/article/pii/S0167404822003534	2	8	Q1
		Greco, C., Fortino, G., Crispo, B. and Choo, K.K.R. AI-enabled IoT penetration testing: state-of-the-art and research challenges. Enterprise Information Systems, 2023 https://doi.org/10.1080/17517575.2022.2130014 https://www.tandfonline.com/doi/full/10.1080/17517575.2022.2130014	2	8	Q2
		Haque, M.U., Kholoosi, M.M. and Babar, M.A. Kgsecconfig: A knowledge graph based approach for secured container orchestrator configuration. In 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2022 https://doi.org/10.1109/SANER53432.2022.00057 https://ieeexplore.ieee.org/document/9825815	2	4	
		Vimala, K. and Fugkeaw, S. VAPE-BRIDGE: Bridging OpenVAS results for automating metasploit framework. In 2022 14th International Conference on Knowledge and Smart Technology (KST), 2022 https://doi.org/10.1109/KST53302.2022.9729085 https://ieeexplore.ieee.org/document/9729085	2	4	
		Forain, I., de Oliveira Albuquerque, R. and de Sousa Júnior, R.T. REVS: A Vulnerability Ranking Tool for Enterprise Security. In 24th International Conference on Enterprise Information Systems (ICEIS), 2022 https://doi.org/10.5220/0011068600003179 https://www.scitepress.org/Link.aspx?doi=10.5220/0011068600003179	2	4	
		François, M., Arduin, P.E. and Merad, M. Artificial Intelligence & Cybersecurity: A Preliminary Study of Automated Pentesting with Offensive Artificial Intelligence. In International Conference on Information and Knowledge Systems, 2021 https://doi.org/10.1007/978-3-030-85977-0_10 https://link.springer.com/chapter/10.1007/978-3-030-85977-0_10	2	4	
		G. Sánchez, O. Olayinka and A. Pasikhani. Web application penetration testing with artificial intelligence: a systematic review. In 2024 22nd International Symposium on Network Computing and Applications (NCA), 2024 https://doi.org/10.1109/NCA61908.2024.00043 https://ieeexplore.ieee.org/document/10945297	2	4	
		S.L. Schröer, G. Apruzzese, S. Human, P. Laskov, H.S. Anderson, E. W. Bernroider, A. Fass, B. Nassi, V. Rimmer, F. Roli and S. Salam. SoK: On the offensive potential of AI. In 2025 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), 2025 https://doi.org/10.1109/SaTML64287.2025.00021 https://ieeexplore.ieee.org/document/10992500	2	4	
		R. Acheampong, D.M. Popovici, T.C. Balan, A. Rekeraho and I.A. Oprea. A Cybersecurity Risk Assessment for Enhanced Security in Virtual Reality. Information, 2025 https://doi.org/10.3390/info16060430 https://www.mdpi.com/2078-2489/16/6/430	2	8	Q2
13	C. Oprişa, G. Cabău and A. Coleşa. Automatic code features extraction using bio-inspired algorithms. In Journal of Computer Virology and Hacking Techniques, 2014 https://doi.org/10.1007/s11416-013-0191-6 https://link.springer.com/article/10.1007/s11416-013-0191-6	S.J. Jeong. A loop splitting method for single loops with non-uniform dependences. In Journal of Computer Virology and Hacking Techniques, 2014 https://doi.org/10.1007/s11416-014-0208-9 https://link.springer.com/article/10.1007/s11416-014-0208-9	3	2.67	
14	C. Oprisa and N. Ignat. A Measure of Similarity for Binary Programs with a Hierarchical Structure. In 11th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2015 https://doi.org/10.1109/ICCP.2015.7312615 https://ieeexplore.ieee.org/abstract/document/7312615	A. Nappa, P. Papadopoulos, M. Varvello, D.A. Gomez, J. Tapiador and A. Lanzi. Pow-how: An enduring timing side-channel to evade online malware sandboxes. In European Symposium on Research in Computer Security, 2021 https://doi.org/10.1007/978-3-030-88418-5_5 https://link.springer.com/chapter/10.1007/978-3-030-88418-5_5	2	4	
		A. Nappa, A. Ùbeda-Portugués, P. Papadopoulos, M. Varvello, J. Tapiador and A. Lanzi. Scramblesuit: an effective timing side-channels framework for malware sandbox evasion. In Journal of Computer Security, 2022 https://doi.org/10.3233/JCS-220005 https://journals.sagepub.com/doi/abs/10.3233/JCS-220005	2	4	
15	A. Mihalca, C. Oprisa and R. Potolea. Hunting for Malware Code in Massive Collections. In 22nd IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2020 https://doi.org/10.1109/AQTR49680.2020.9129948 https://ieeexplore.ieee.org/abstract/document/9129948	M. Brengel and C. Rossow. YARIX: Scalable YARA-based Malware Intelligence. In 30th USENIX Security Symposium (USENIX Security 21), 2021 ISBN 978-1-939133-24-3 https://www.usenix.org/conference/usenixsecurity21/presentation/brengel	3	2.67	
16	A. Pacurar and C. Oprisa. Using artificial intelligence to fight clickbait in romanian news articles. In 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398606 https://ieeexplore.ieee.org/abstract/document/10398606	Gherheş, V., Fărcaşiu, M.A. and Cernicova-Buca, M. Are ChatGPT-Generated Headlines Better Attention Grabbers than Human-Authored Ones? An Assessment of Salient Features Driving Engagement with Online Media. Journalism and Media, 2024 https://doi.org/10.3390/journalmedia5040110 https://www.mdpi.com/2673-5172/5/4/110	2	8	Q2
17	M. Marmureanu and C. Oprisa. MITRE tactics inference from Splunk queries. In 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398612 https://ieeexplore.ieee.org/abstract/document/10398612	Binbeshr, F., Imam, M., Ghaleb, M., Hamdan, M., Rahim, M.A. and Hammoudeh, M. The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches. IEEE Open Journal of the Computer Society, 2025 https://doi.org/10.1109/OJCS.2025.3536800 https://ieeexplore.ieee.org/abstract/document/10858372	2	8	Q1
18	V. Mosolea and C. Oprisa. Detecting domain generation algorithms in malware traffic using constrained resources. In 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), 2023 https://doi.org/10.1109/ICCP60212.2023.10398684 https://ieeexplore.ieee.org/abstract/document/10398684	Jeremiah, D., Rafiq, H., Ta, V.T., Usman, M., Raza, M. and Awais, M. NIOM-DGA: Nature-inspired optimised ML-based model for DGA detection. Computers & Security, 2025 https://doi.org/10.1016/j.cose.2025.104561 https://www.sciencedirect.com/science/article/pii/S0167404825002500	2	8	Q1
19	R. Rentea and C. Oprisa. Fast clustering for massive collections of malicious URLs. In 2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP), 2021 https://doi.org/10.1109/ICCP53602.2021.9733623 https://ieeexplore.ieee.org/abstract/document/9733623	Wang, C., Yu, Y., Pu, A., Shi, F. and Huang, C. Spotlight on Video Piracy Websites: Familial Analysis Based on Multidimensional Features. In KNOWLEDGE SCIENCE, ENGINEERING AND MANAGEMENT, KSEM 2022, PT III, 2022 https://doi.org/10.1007/978-3-031-10989-8_22 https://link.springer.com/chapter/10.1007/978-3-031-10989-8_22	2	4	
				74	324.81

A3.1.2 Citari in carti, reviste si volume ale unor manifestari stiintifice - BDI

Nr.	Articol citat	Articol care citeaza	Nr. autori art.citat	Punctaj
1	A. Nagy, C. Oprişa, I. Salomie, C. Pop, V. Chifu, M. Dinşoreanu. Particle swarm optimization for clustering semantic web servicesParticle swarm optimization for clustering semantic web services. In Proceedings - 2011 10th International Symposium on Parallel and Distributed Computing, ISPDC 2011, 2011 https://doi.org/10.1109/ISPDC.2011.33 https://ieeexplore.ieee.org/abstract/document/6108270	I.R. Praveen Joe and P. Varalakshmi. An analysis on web-service-generated data to facilitate service retrieval. In Applied Mathematics and Information Sciences, 2019 http://doi.org/10.18576/amis/130107 https://www.naturalspublishing.com/Article.asp?ArtcID=17275	6	0.67
		S.S. Kamath and V.S. Ananthanarayana. A bio-inspired, incremental clustering algorithm for semantics-based web service discovery. In International Journal of Reasoning-based Intelligent Systems, 2015 https://doi.org/10.1504/IJRIS.2015.072953 https://www.inderscienceonline.com/doi/abs/10.1504/IJRIS.2015.072953	6	0.67
		W. Chen and J. Li. Agile services oriented virtualization of web services. In Proceedings - IEEE 6th International Symposium on Theoretical Aspects of Software Engineering, TASE 2012, 2012 https://doi.org/10.1109/TASE.2012.37 https://ieeexplore.ieee.org/abstract/document/6269639	6	0.67
		M.H. Hasan, J. Jaafar and M.F. Hassan. Fuzzy-based clustering of web services' quality of service: A review. In Journal of Communications, 2014 https://doi.org/10.12720/jcm.9.1.81-90 https://www.jocm.us/uploadfile/2014/0123/20140123015630493.pdf	6	0.67
2	C.B. Pop, V.R. Chifu, I. Salomie, M. Dinsoreanu, T. David, V. Acretoaie, A. Nagy and C. Oprisa. Biologically-inspired clustering of semantic Web services. Birds or ants intelligence?. In Concurrency Computation Practice and Experience, 2012 https://doi.org/10.1002/cpe.1853 https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.1853	N. Agarwal, G. Sikka and L.K. Awasthi. Web Service Clustering Approaches to Enhance Service Discovery: A Review. In Lecture Notes in Electrical Engineering, 2021 https://doi.org/10.1007/978-981-15-8297-4_3 https://link.springer.com/chapter/10.1007/978-981-15-8297-4_3	8	0.5
		M.H. Hasan, J. Jaafar and M.F. Hassan. Fuzzy-based clustering of web services' quality of service: A review. In Journal of Communications, 2014 https://doi.org/10.12720/jcm.9.1.81-90 https://www.jocm.us/uploadfile/2014/0123/20140123015630493.pdf	8	0.5
3	C. Oprisa, M. Checiches and A. Nandrean. Locality-sensitive hashing optimizations for fast malware clustering. In Proceedings - 2014 IEEE 10th International Conference on Intelligent Computer Communication and	H. Naderi, P. Vinod, M. Conti, S. Parsa and M.H. Alaeiyan. Malware signature generation using locality sensitive hashing. In Communications in Computer and Information Science, 2019 https://doi.org/10.1007/978-981-13-7561-3_9 https://link.springer.com/chapter/10.1007/978-981-13-7561-3_9	3	1.33

	Processing, ICCP 2014, 2014 https://doi.org/10.1109/ICCP.2014.6936960 https://ieeexplore.ieee.org/abstract/document/6936960	M.M. Pic. A dedicated crawling engine to reduce apps distribution risks. In Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016, 2017 https://doi.org/10.1109/EISIC.2016.056 https://ieeexplore.ieee.org/document/7870229	3	1.33
4	C. Oprisa. A MinHash approach for clustering large collections of binary programs. In Proceedings - 2015 20th International Conference on Control Systems and Computer Science, CSCS 2015, 2015 https://doi.org/10.1109/CSCS.2015.27 https://ieeexplore.ieee.org/abstract/document/7168423	S. Abed, L. Waleed, G. Aldamkhi and K. Hadi. Enhancement in data security and integrity using minhash technique. In Indonesian Journal of Electrical Engineering and Computer Science, 2021 https://doi.org/10.11591/ijeecs.v21.i3.pp1739-1750 https://ijeecs.iaescore.com/index.php/IJEECS/article/view/22773	1	4
5	C. Oprişa, G. Cabău and G. Sebestyen Pal. Malware clustering using suffix trees. In Journal of Computer Virology and Hacking Techniques, 2016 https://doi.org/10.1007/s11416-014-0227-6 https://link.springer.com/article/10.1007/s11416-014-0227-6	H. Naderi, P. Vinod, M. Conti, S. Parsa and M.H. Alaeiyan. Malware signature generation using locality sensitive hashing. In Communications in Computer and Information Science, 2019 https://doi.org/10.1007/978-981-13-7561-3_9 https://link.springer.com/chapter/10.1007/978-981-13-7561-3_9	3	1.33
6	G. Cabau, M. Buhu and C.P. Oprisa. Malware classification based on dynamic behavior. In Proceedings - 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2016, 2017 https://doi.org/10.1109/SYNASC.2016.057 https://ieeexplore.ieee.org/abstract/document/7829629	N. Li, Z. Zhang, X. Che, Z. Guo and J. Cai. A Survey on Feature Extraction Methods of Heuristic Malware Detection. In Journal of Physics: Conference Series, 2021 https://doi.org/10.1088/1742-6596/1757/1/012071 https://iopscience.iop.org/article/10.1088/1742-6596/1757/1/012071	3	1.33
		U. Nandagopal and S. Thirumalaivelu. Classification of Malware with MIST and N-Gram Features Using Machine Learning. In International Journal of Intelligent Engineering and Systems, 2021 https://doi.org/10.22266/ijies2021.0430.29 https://www.inass.org/2021/2021043029.pdf	3	1.33
		M.A. Kerrich, A. Addaim and L. Damej. Proposed Solution for HID Fileless Ransomware Using Machine Learning. In Communications in Computer and Information Science, 2020 https://doi.org/10.1007/978-3-030-61143-9_15 https://link.springer.com/chapter/10.1007/978-3-030-61143-9_15	3	1.33
7	G. Cabau, M. Buhu and C. Oprisa. Malware Classification Using Filesystem Footprints. In IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2016 https://doi.org/10.1109/AQTR.2016.7501294 https://ieeexplore.ieee.org/abstract/document/7501294	M. Bala. Android Malware Classification using Neural Nets. In International Journal of Recent Research Aspects, 2017 ISSN 2349-7688 https://www.ijrra.net/Vol4issue4/IJRRA-04-04-06.pdf	3	1.33
		N. Bhargava, A. Jain, A. Kumar, D.N. Le. Detection of Malicious Executables Using Rule Based Classification Algorithms. In Proceedings of the First International Conference on Information Technology and Knowledge Management, 2018 https://doi.org/10.15439/2017km04 https://annals-csis.org/Volume_14/drp/04.html	3	1.33
8	O. Valea, C. Oprişa. Towards Pentesting Automation Using the Metasploit Framework. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, 2020 https://doi.org/10.1109/ICCP51029.2020.9266234 https://ieeexplore.ieee.org/abstract/document/9266234	Kumar, B., Bejo, S.P., Kedia, R., Banerjee, P., Jha, P. and Dehury, M.K. Kali Linux based Empirical Investigation on Vulnerability Evaluation using Pen-Testing tools. In 2023 World Conference on Communication & Computing (WCONF), 2023 https://doi.org/10.1109/WCONF58270.2023.10235163 https://ieeexplore.ieee.org/document/10235163	2	2
		Şimşek, M.M. and Atılgan, E. Attacks on availability of iot middleware protocols: A case study on mqtt. Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi, 2023 https://doi.org/10.53608/estudambilisim.1297052 https://dergipark.org.tr/tr/pub/estudambilisim/issue/76737/1297052	2	2
		Saber, V., ElSayad, D., Bahaa-Eldin, A.M. and Fayed, Z. Automated penetration testing, a systematic review. In 2023 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), 2023 https://doi.org/10.1109/MIUCC58832.2023.10278377 https://ieeexplore.ieee.org/document/10278377	2	2
		Lang, W. Data Security Testing for Sensor Networks in IoT Environments. In 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2023 https://doi.org/10.1109/I-SMAC58438.2023.10290460 https://ieeexplore.ieee.org/document/10290460	2	2
		de Sá, A.O., Prado, C.B., Flavio, M.L. and Carmo, L.F. Intelligent Attacks on Cyber-Physical Systems and Critical Infrastructures. In Modern Technologies Enabling Innovative Methods for Maritime Monitoring and Strengthening Resilience in Maritime Critical Infrastructures, 2024 https://doi.org/10.3233/NICSP240033 https://ebooks.iospress.nl/doi/10.3233/NICSP240033	2	2
		Al Sharaa, B. and Thuneibat, S. Ethical hacking: real evaluation model of brute force attacks in password cracking. Indonesian Journal of Electrical Engineering and Computer Science, 2024 https://doi.org/10.11591/ijeecs.v33.i3.pp1653-1659 https://ijeecs.iaescore.com/index.php/IJEECS/article/view/35491	2	2
		Rallabandi, S. and Sundaram, A.M. Generating a multi-OS fully undetectable malware (FUD) and analyzing it afore and after steganography. In 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2022 https://doi.org/10.1109/ICAC3N56670.2022.10074511 https://ieeexplore.ieee.org/document/10074511	2	2
		Sivamanikanta, M., Abbas, M.A.M. and Das, P. Exploring the capabilities of the metasploit framework for effective penetration testing. In International Conference on Data Science and Network Engineering, 2023 https://doi.org/10.1007/978-981-99-6755-1_35 https://link.springer.com/chapter/10.1007/978-981-99-6755-1_35	2	2
		Singhdeo, T.J., Reeja, S.R., Bhavsar, A. and Satapathy, S. Penetration Testing of Web Server Using Metasploit Framework and DVWA. In International Conference on Frontiers of Intelligent Computing: Theory and Applications, 2023 https://doi.org/10.1007/978-981-99-6706-3_17 https://link.springer.com/chapter/10.1007/978-981-99-6706-3_17	2	2
		Turtiainen, H., Costin, A., Polyakov, A. and Hämäläinen, T. Offensive Machine Learning Methods and the Cyber Kill Chain. In Artificial Intelligence and Cybersecurity: Theory and Applications, 2022 https://doi.org/10.1007/978-3-031-15030-2_6 https://link.springer.com/chapter/10.1007/978-3-031-15030-2_6	2	2
		Fugkeaw, S., Hak, L., Ploysopond, N., Apichonkit, W. and Lahankaew, S. LightPEN: Optimizing the Vulnerability Exposures for Lightweight Penetration Test. In 2023 15th International Conference on Knowledge and Smart Technology (KST), 2023 https://doi.org/10.1109/KST57286.2023.10086896 https://ieeexplore.ieee.org/document/10086896	2	2
		Zhang, P., Wang, W., Zhang, D., Wu, H., Han, L. and Zhao, Q., 2024, December. Automated Security Penetration Testing Based on Machine Learning. In 2024 4th International Conference on Electronic Information Engineering and Computer Communication (EIECC), 2024 https://doi.org/10.1109/EIECC64539.2024.10929572 https://ieeexplore.ieee.org/document/10929572	2	2
		Toggi, A., Bose, B., Naidu, D. and Srivastava, R. Metasploit Based Automated Penetration Testing Using Reinforcement Learning. In 2024 First International Conference for Women in Computing (InCoWoCo), 2024 https://doi.org/10.1109/InCoWoCo64194.2024.10863399 https://ieeexplore.ieee.org/abstract/document/10863399	2	2
9	A. Crişan, G. Florea, L. Halasz, C. Lemnaru, C. Oprişa. Detecting Malicious URLs Based on Machine Learning Algorithms and Word Embeddings. In Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, 2020 https://doi.org/10.1109/ICCP51029.2020.9266139 https://ieeexplore.ieee.org/abstract/document/9266139	G. Pradeepa and R. Devi. Malicious domain detection using nlp methods—a review. In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), 2022 https://doi.org/10.1109/SMART55829.2022.10046882 https://ieeexplore.ieee.org/document/10046882	5	0.8
		X. D. Hoang, D. Le Minh and T.T.T. Ninh. A cnn-based model for detecting malicious URLs. In 2023 RIVF International Conference on Computing and Communication Technologies (RIVF), 2023 https://doi.org/10.1109/RIVF60135.2023.10471782 https://ieeexplore.ieee.org/document/10471782	5	0.8
		Mahmud, T., Hossain, G.S., Ali, M.H., Hasan, T., Aziz, M.F.B.A., Aziz, M.T., Hossain, M.S. and Andersson, K. A Machine Learning-Based Framework for Malicious URL Detection in Cybersecurity. In 2025 8th International Conference on Information and Computer Technologies (ICICT), 2025 https://doi.org/10.1109/ICICT64582.2025.00016 https://ieeexplore.ieee.org/document/11058465	5	0.8
		Parasuraman, M., Abirami, G., Krishnan, B., Munnangi, A.K. and Kumaresan, M. Collaborative Filtering of Malicious Information from the MULTImedia Data Using s. In 2023 International Conference on Computer Science and Emerging Technologies (CSET), 2023 https://doi.org/10.1109/CSET58993.2023.10346953 https://ieeexplore.ieee.org/document/10346953	5	0.8
		Macharla, A., Kumar, G.K. and Rani, D.M. Detection and classification of malicious URLs based on machine learning models. In 7th IET Smart Cities Symposium (SCS 2023), 2023 https://doi.org/10.1049/icp.2024.0877 https://ieeexplore.ieee.org/abstract/document/10510723	5	0.8
		Kumar, S., Prasanthi, B., Dharmajee Rao, D.T.V., Vinoda Reddy, G., Maddela Parameswar, G. and Tulasiram, D. Malicious URL Classification Using Temporal Convolutional Neural Network. In International Conference on Frontiers of Intelligent Computing: Theory and Applications, 2024 https://doi.org/10.1007/978-981-96-2124-8_34 https://link.springer.com/chapter/10.1007/978-981-96-2124-8_34	5	0.8

		Devi, M.S., Gupta, U., Sahu, K., Das, R.J. and Ramesh, S.V. Cardinal Correlated Oversampling for Detection of Malicious Web Links Using Machine Learning. In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT, 2021 https://doi.org/10.1007/978-981-16-3728-5_36 https://link.springer.com/chapter/10.1007/978-981-16-3728-5_36	5	0.8
10	A.M. Lungana-Niculescu, A. Colesa and C. Oprisa. False positive mitigation in behavioral malware detection using deep learning. In Proceedings - 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing, ICCP 2018, 2018 https://doi.org/10.1109/ICCP.2018.8516611 https://ieeexplore.ieee.org/abstract/document/8516611	Yaffe, D. and Hendler, D. Early Detection of In-Memory Malicious Activity Based on Run-Time Environmental Features. In International Symposium on Cyber Security Cryptography and Machine Learning, 2021 https://doi.org/10.1007/978-3-030-78086-9_29 https://link.springer.com/chapter/10.1007/978-3-030-78086-9_29	3	1.33
11	C. Oprişa, D. Gavriluţ and G. Cabău. A scalable approach for detecting plagiarized mobile applications. In Knowledge and Information Systems, 2016 https://doi.org/10.1007/s10115-015-0903-y https://link.springer.com/article/10.1007/s10115-015-0903-y	Muhammad, A.H. and Oyong, I. Revisiting the challenges and surveys in text similarity matching and detection methods. In Jurnal Informatika, 2022 https://doi.org/10.26555/jifo.v16i3.a23471 https://journal.uad.ac.id/index.php/JIFO/article/view/23471	3	1.33
12	A. Jircan and C. Oprisa. MEPHISTO: a Red Team Tool for Offensive Security. In 2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP), 2024 https://doi.org/10.1109/ICCP63557.2024.10793019 https://ieeexplore.ieee.org/abstract/document/10793019	Karagiannis, S., Kasotakis, A., Magkos, E. and Ntantogian, C. Red vs. Blue Team Training Scenarios for 5G/6G Networks. In International Conference on Availability, Reliability and Security, 2025 https://doi.org/10.1007/978-3-032-00642-4_3 https://link.springer.com/chapter/10.1007/978-3-032-00642-4_3	2	2
			Total punctaj A3.1.2	38	54.58

Anexa: datele pentru calculul indeplinirii criteriilor A3.3.1, A3.3.2, A3.3.3

A3.2 Membru in colectivele de redactie sau comitetele stiintifice ale revistelor indexate ISI, chari, co-chair sau membru in comitetele de organizare ale manifestarilor stiintifice internationale [9]

Nr.	Nume Jurnal	URL	Anul
1	2025 IEEE International Conference on Cyber Security and Resilience	https://www.ieee-csr.org/iosec/	2025
2			
3			
4			
5			
6			
		Total Punctaj A3.2	**1**

A3.3 Membru in colectivele de redactie sau comitetele stiintifice ale revistelor indexate BDI, chari, co-chair sau membru in comitetele de organizare ale manifestarilor stiintifice internationale indexate BdI [4]

Nr.	Nume Jurnal	URL	Anul
1			
2			
3			
4			
		Total Punctaj A3.3	**0**

Anexa: datele pentru calculul indeplinirii criteriilor A3.4.1, A3.4.2

A3.4 Premii in domeniu conferite de Academia Romana, ASTR, AOSR, sau premii internationale de prestigiu

Nr.	Anul	Descriere premiu
1	2013	Best Paper Award pentru articolul "Automatic code features extraction using bio-inspired algorithms" la conferinta EICAR 2013
2		
3		
4		

Total Punctaj A3.4 **1**

A3.4.2 Premii nationale in domeniu

Nr.	Anul	Descriere premiu
1		
2		
3		
4		

Total Punctaj A3.4.1 **0**

Bitdefender®

15A Orhideelor St.
Orhideea Towers, district 6
Bucharest, 060071, Romania

To Whom It May Concern:

We hereby that Ciprian OPRIȘA had the role of Technical Project Leader during the implementation of SMESEC Project, Grant Agreement No 740787, between 2017 and 2020.

17th of May 2021

Nicoleta REITU

Bitdefender
Global Leader
In Cybersecurity

15A Orhideelor St.
Orhideea Towers, district 6
Bucharest, 060071, Romania

Adeverință

Prin aceasta adeverim că, Ciprian Pavel OPRIȘA participă, în calitate de **Responsabil Partener**, în cadrul proiectului *CONSOLE, "Cybersecurity for Resilient Software Development"*, numărul GA: 101128070. Proiectul se desfășoară în perioada: 01/11/2023 – 31/10/2026.

19/09/2025

Nicoleta REITU

Bitdefender
Global Leader
In Cybersecurity

15A Orhideelor St.
Orhideea Towers, district 6
Bucharest, 060071, Romania

Adeverință

Prin aceasta adeverim că, Ciprian Pavel OPRIȘA participă, în calitate de **Responsabil Partener**, în cadrul proiectului *EU-iNSPIRE, "INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU"*, numărul GA: 101190054. Proiectul se desfășoară în perioada: 01/01/2025 – 31/12/2028.

19/09/2025

Nicoleta REITU

BITDEFENDER s.r.l.
Strada Delea Veche, nr. 24,
DV24 Offices, clădirea A,
024102, Sector 2, București
www.bitdefender.com

Nr. ieșire: 64 / 9.01.2017

Atestarea participării în proiectele de C-D co-finanțate din Fondurile Structurale, de Coeziune și naționale

Prin prezenta atestăm că:

Ciprian OPRIȘA

a participat în cadrul următorului proiect:

Nr.	Titlul proiectului	Program	Poziția în cadrul proiectului	Perioada de implementare	Valoarea proiectului (Lei)
1.	CIPSEC - *Enhancing Critical Infrastructure Protection with innovative SECurity framework*	Horizon 2020	Cercetător	Mai 2016 – Aprilie 2019	1.653.750

Nr. 145 / 31.07.2025

ADEVERINȚĂ

Subsemnatul, Prof. Dr. Ing. Stelian Brad, în calitate de Director de Proiect în cadrul Cluj IT Cluster, certific prin prezenta că domnul **Ciprian Oprișa** a fost implicat în cadrul proiectului de cercetare-dezvoltare **GEIGER – Cybersecurity Counter / Shielding Small Businesses against Cyber Threats**, finanțat prin Programul Orizont 2020 al Uniunii Europene, în baza **Grant Agreement nr. 883588**.

Domnul Ciprian Oprișa a contribuit la activitățile proiectului pe toată perioada de derulare a acestuia, desfășurând activități relevante în domeniul securității cibernetice, dezvoltării de instrumente pentru evaluarea riscurilor și diseminării rezultatelor tehnice.

Această adeverință este eliberată la cererea domniei sale, în scopul includerii în dosarul de abilitare.

Data: 31.07.2025
Semnătură:

Prof. Dr. Ing. Stelian Brad
Director de Proiect
Cluj IT Cluster