Common Vulnerability Scoring System

IEEE Security and Privacy

4, 85-89

DOI: 10.1109/msp.2006.145

Citation Report

#	Article	IF	Citations
1	An early application of the Bell Labs Security framework to analyze vulnerabilities in the Internet telephony domain. Bell Labs Technical Journal, 0, 12, 7-19.	0.7	2
2	Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 2008, 28, 483-491.	10.5	67
3	Learning from Software Security Testing. , 2008, , .		5
4	A Study and Implementation of Vulnerability Assessment and Misconfiguration Detection. , 2008, , .		11
5	Application of Security Metrics in Auditing Computer Network Security: A Case Study. , 2008, , .		9
6	Fortification of IT Security by Automatic Security Advisory Processing. , 2008, , .		7
7	Lightweight Vulnerability Management System. Journal of Information Processing, 2008, 16, 157-164.	0.3	0
8	An Approach for Security Assessment of Network Configurations Using Attack Graph. , 2009, , .		24
9	Analysis of a Security Incident of Open Source Middleware – Case Analysis of 2008 Debian Incident of OpenSSL. , 2009, , .		0
10	Metrics for network forensics conviction evidence. , 2009, , .		5
11	Evidential structures and metrics for network forensics. International Journal of Internet Technology and Secured Transactions, 2010, 2, 250.	0.3	2
12	Expanding topological vulnerability analysis to intrusion detection through the incident response intelligence system. Information Management and Computer Security, 2010, 18, 291-309.	1.2	4
13	Fuzzy Classification Metrics for Scanner Assessment and Vulnerability Reporting. IEEE Transactions on Information Forensics and Security, 2010, 5, 613-624.	4.5	10
14	k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks. Lecture Notes in Computer Science, 2010, , 573-587.	1.0	60
15	Measure Large Scale Network Security Using Adjacency Matrix Attack Graphs. , 2010, , .		1
16	Quantitative Evaluation of Related Web-Based Vulnerabilities. , 2010, , .		0
17	A new approach to evaluating security assurance. , 2011, , .		1
18	Information Security for Service Oriented Computing: Ally or Antagonist. , 2011, , .		0

#	Article	IF	Citations
19	Network Threat Assessment Based on Alert Verification. , 2011, , .		1
20	CNSSA: A Comprehensive Network Security Situation Awareness System. , 2011, , .		13
21	A software application to analyze the effects of temporal and environmental metrics on overall CVSS v2 score. , 2011, , .		9
22	Cybersecurity risk testing of substation phasor measurement units and phasor data concentrators. , 2011, , .		41
23	A multi-layer tree model for enterprise vulnerability management. , 2011, , .		1
24	EVMAT. , 2011, , .		10
25	An adaptive target tracking scheme for binary wireless sensor networks. , 2011, , .		1
26	An Analysis of CVSS v2 Environmental Scoring. , 2011, , .		8
27	Research on the fuzzy comprehensive evaluation for information system security risk. , 2011, , .		1
28	The use of application scanners in software product quality assessment. , 2011, , .		2
29	A move in the security measurement stalemate. , 2012, , .		9
30	Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis. Journal of Management Information Systems, 2012, 28, 305-338.	2.1	29
31	Analytical framework for measuring network security using exploit dependency graph. IET Information Security, 2012, 6, 264-270.	1.1	8
32	Extending Attack Graph-Based Security Metrics and Aggregating Their Application. IEEE Transactions on Dependable and Secure Computing, 2012, 9, 75-85.	3.7	104
33	Intrinsically Secure Next-Generation Networks. Bell Labs Technical Journal, 2012, 17, 17-36.	0.7	0
34	A Cyber-Security Storm MAP. , 2012, , .		0
35	Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics. , 2012, , .		39
36	Secure dynamic routing protocols based on Cross-Layer Network Security Evaluation. , 2012, , .		0

#	Article	IF	Citations
37	Boosting Logical Attack Graph for Efficient Security Control. , 2012, , .		1
38	Improving VRSS-based vulnerability prioritization using analytic hierarchy process. Journal of Systems and Software, 2012, 85, 1699-1708.	3.3	53
39	Exploring attack graph for cost-benefit security hardening: A probabilistic approach. Computers and Security, 2013, 32, 158-169.	4.0	89
40	A Quantitative Measure of the Security Risk Level of Enterprise Networks. , 2013, , .		5
41	Predictive vulnerability scoring in the context of insufficient information availability. , 2013, , .		9
42	A Unified Framework for Measuring a Network's Mean Time-to-Compromise. , 2013, , .		22
43	A Genetic Algorithm Approach for the Most Likely Attack Path Problem. , 2013, , .		2
44	A novel approach to evaluate software vulnerability prioritization. Journal of Systems and Software, 2013, 86, 2822-2840.	3.3	27
45	Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information. IEEE Transactions on Smart Grid, 2013, 4, 235-244.	6.2	140
46	Objective metrics for firewall security: A holistic view. , 2013, , .		3
47	A probabilistic cost-efficient approach for mobile security assessment. , 2013, , .		3
48	A taxonomy framework based on ITUâ€TXâ€805 security architecture for quantitative determination of computer network vulnerabilities. Security and Communication Networks, 2013, 6, 864-880.	1.0	2
49	A model for quantitative security measurement and prioritisation of vulnerability mitigation. International Journal of Security and Networks, 2013, 8, 139.	0.1	4
50	Risk assessment and analysis through population-based attack graph modelling. , 2013, , .		10
51	Toward Automated Reduction of Human Errors Based on Cognitive Analysis. , 2013, , .		1
52	Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks, 2013, 6, 1087-1116.	1.0	19
53	AVQS: Attack Route-Based Vulnerability Quantification Scheme for Smart Grid. Scientific World Journal, The, 2014, 2014, 1-6.	0.8	1
54	A response selection model for intrusion response systems: Response Strategy Model (RSM). Security and Communication Networks, 2014, 7, 1831-1848.	1.0	2

#	Article	IF	Citations
55	Application of Mean Time-to-Compromise and VEA-bility security metrics in auditing computer network security. , 2014, , .		2
56	An evidential network forensics analysis with metrics for conviction evidence. , 2014, , .		0
57	Risk management in embedded devices using metering applications as example. , 2014, , .		3
58	An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities. Communications in Computer and Information Science, 2014, , 322-340.	0.4	4
59	SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures. IEEE Transactions on Smart Grid, 2014, 5, 3-13.	6.2	90
60	DAG-based attack and defense modeling: Donâ€™t miss the forest for the attack trees. Computer Science Review, 2014, 13-14, 1-38.	10.2	211
61	k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 30-44.	3.7	120
62	The algorithm model for cumulative vulnerability risk assessment. International Journal of Internet Protocol Technology, 2014, 8, 150.	0.2	0
63	Modeling and analysis of stepping stone attacks. , 2014, , .		8
64	Vulnerability evaluation based on CVSS and environmental information statistics. , 2015, , .		2
65	A vulnerability's lifetime. , 2015, , .		4
66	Reference Ontology for Cybersecurity Operational Information. Computer Journal, 2015, 58, 2297-2312.	1.5	26
67	Evaluation of isolation in virtual machine environments encounter in effective attacks against memory. Security and Communication Networks, 2015, 8, 4396-4406.	1.0	2
68	Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems. Energies, 2015, 8, 5266-5286.	1.6	23
69	Difficulty-level metric for cyber security training. , 2015, , .		4
70	Vulnerability database analysis for 10 years for ensuring security of cyber critical green infrastructures. , 2015, , .		2
71	Enabling security-aware virtual machine placement in IaaS clouds. , 2015, , .		2
72	Study on the distribution of CVSS environmental score. , 2015, , .		4

#	Article	IF	Citations
73	Towards Automated Generation and Visualization of Hierarchical Attack Representation Models. , 2015, , .		6
74	Power System Reliability Evaluation With SCADA Cybersecurity Considerations. IEEE Transactions on Smart Grid, 2015, 6, 1707-1721.	6.2	180
75	Pareto-Optimal Adversarial Defense of Enterprise Systems. ACM Transactions on Information and System Security, 2015, 17, 1-39.	4.5	37
76	Automatic vulnerability detection for weakness visualization and advisory creation. , 2015, , .		3
77	Exploring risk flow attack graph for security risk assessment. IET Information Security, 2015, 9, 344-353.	1.1	26
78	Exploiting curse of diversity for improved network security. , 2015, , .		6
79	Automatic detection of vulnerabilities for advanced security analytics. , 2015, , .		5
80	Towards a multiobjective framework for evaluating network security under exploit attacks. , 2015, , .		3
81	Information Disclosure and the Diffusion of Information Security Attacks. Information Systems Research, 2015, 26, 565-584.	2.2	63
82	A Bayesian network model for likelihood estimations of acquirement of critical software vulnerabilities and exploits. Information and Software Technology, 2015, 58, 304-318.	3.0	14
83	Security issues and threats that may affect the hybrid cloud of FINESCE. Network Protocols and Algorithms, 2016, 8, 26.	1.0	10
84	Moving Target Network Defense Effectiveness Evaluation Based on Change-Point Detection. Mathematical Problems in Engineering, 2016, 2016, 1-11.	0.6	13
85	Risk assessment and attack graph generation for collaborative infrastructures: a survey. International Journal of Critical Computer-Based Systems, 2016, 6, 204.	0.1	2
86	A New Risk Assessment Framework Using Graph Theory for Complex ICT Systems. , 2016, , .		6
87	Security analysis of forwarding strategies in network time measurements using Openflow. , 2016, , .		1
88	Exploring security metrics for electric grid infrastructures leveraging attack graphs. , 2016, , .		5
89	Cyber-physical Vulnerability Assessment in Manufacturing Systems. Procedia Manufacturing, 2016, 5, 1060-1074.	1.9	34
90	Case Studies of Network Defense with Attack Graph Games. IEEE Intelligent Systems, 2016, 31, 24-30.	4.0	36

#	Article	IF	Citations
91	Network security risk assessment method based on HMM and attack graph model. , 2016, , .		33
92	An assessment method of vulnerabilities in electric CPS cyber space. , 2016, , .		1
93	Using temporal probabilistic logic for optimal monitoring of security events with limited resources. Journal of Computer Security, 2016, 24, 735-791.	0.5	6
94	Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks. IEEE Transactions on Information Forensics and Security, 2016, 11, 1071-1086.	4.5	92
95	Software Vulnerability Detection Methodology Combined with Static and Dynamic Analysis. Wireless Personal Communications, 2016, 89, 777-793.	1.8	17
96	Multilayered Impact Evaluation Model for Attacking Missions. IEEE Systems Journal, 2016, 10, 1304-1315.	2.9	14
97	Taxonomy of information security risk assessment (ISRA). Computers and Security, 2016, 57, 14-30.	4.0	134
98	An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. Journal of Manufacturing Systems, 2017, 43, 339-351.	7.6	61
99	Threat Modeling for Cloud Data Center Infrastructures. Lecture Notes in Computer Science, 2017, , 302-319.	1.0	11
100	Diversity-aware, Cost-effective Network Security Hardening Using Attack Graph. Communications in Computer and Information Science, 2017, , 1-15.	0.4	1
101	Predicting Exploitations of Information Systems Vulnerabilities Through Attackersâ€™ Characteristics. IEEE Access, 2017, 5, 26063-26075.	2.6	15
102	Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks. Computers and Security, 2017, 64, 16-43.	4.0	29
103	Model-Based Quantitative Network Security Metrics: A Survey. IEEE Communications Surveys and Tutorials, 2017, 19, 2704-2734.	24.8	61
104	Mining social networks of open source CVE coordination. , 2017, , .		3
105	A decoy chain deployment method based on SDN and NFV against penetration attack. PLoS ONE, 2017, 12, e0189095.	1.1	7
106	Honeypot Baselining for Zero Day Attack Detection. International Journal of Information Security and Privacy, 2017, 11, 63-74.	0.6	3
107	Exploring Attack Graphs for Security Risk Assessment: A Probabilistic Approach. Wuhan University Journal of Natural Sciences, 2018, 23, 171-177.	0.2	7
108	Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Electronics, 2018, 65, 8153-8162.	5.2	93

#	Article	IF	Citations
109	Establishing evolutionary game models for CYBer security information EXchange (CYBEX). Journal of Computer and System Sciences, 2018, 98, 27-52.	0.9	30
110	Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. Annals of Nuclear Energy, 2018, 112, 646-654.	0.9	12
111	Analyzing Complex Non-Trivial Network using Attack Set Generation by Genetic Algorithm. , 2018, , .		0
112	A Cyber Risk Based Moving Target Defense Mechanism for Microservice Architectures. , 2018, , .		14
113	Risk Assessment for Cyber Attacks in Feeder Automation System. , 2018, , .		6
114	Optimal Prevention and Control Strategy Against Preconceive Faults in Electric Cyber-Physical System. , 2018, , .		1
115	Industry-Wide Analysis of Open Source Security. , 2018, , .		3
116	Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems. , 2018, , .		8
117	A Quantitative Risk Analysis Model and Simulation Of Enterprise Networks. , 2018, , .		2
118	Reliability Assessment of Distribution Network Considering Cyber Attacks. , 2018, , .		9
119	Advanced Petya Ransomware and Mitigation Strategies. , 2018, , .		7
120	Security Assessment of Dynamic Networks with an Approach of Integrating Semantic Reasoning and Attack Graphs. , 2018, , .		5
121	Comprehensive Security Assessment of Combined MTD Techniques for the Cloud. , 2018, , .		14
122	The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay. , 2018, , .		23
123	Enhancing Microgrid Resiliency Against Cyber Vulnerabilities. , 2018, , .		6
125	Understanding vulnerabilities in plugin-based web systems. , 2018, , .		8
126	Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud. Lecture Notes in Computer Science, 2018, , 326-345.	1.0	19
127	Evaluation for Combination of Shuffle and Diversity on Moving Target Defense Strategy for Cloud Computing. , 2018, , .		16

#	Article	IF	Citations
128	The Evolving State of Medical Device Cybersecurity. Biomedical Instrumentation and Technology, 2018, 52, 103-111.	0.2	18
129	Surviving unpatchable vulnerabilities through heterogeneous network hardeningÂoptions. Journal of Computer Security, 2018, 26, 761-789.	0.5	7
130	Risk based Security Enforcement in Software Defined Network. Computers and Security, 2018, 78, 321-335.	4.0	7
131	Modelling and automatic mapping of cyber security requirements for industrial applications: Survey, problem exposition, and research focus. , 2018, , .		7
132	Toward A Code Pattern Based Vulnerability Measurement Model. , 2018, , .		0
133	Automatic Vulnerability Classification Using Machine Learning. Lecture Notes in Computer Science, 2018, , 3-17.	1.0	2
134	Research on Security Vulnerabilities Based on Artificial Intelligence. Lecture Notes in Computer Science, 2019, , 377-387.	1.0	0
135	Measuring and Enhancing Microgrid Resiliency Against Cyber Threats. IEEE Transactions on Industry Applications, 2019, 55, 6303-6312.	3.3	43
136	Hardening networks against strategic attackers using attack graph games. Computers and Security, 2019, 87, 101578.	4.0	16
137	Mitigating the insider threat of remote administrators in clouds through maintenance task assignments. Journal of Computer Security, 2019, 27, 427-458.	0.5	1
138	Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events. Applied Sciences (Switzerland), 2019, 9, 3003.	1.3	10
139	Toward a reliability measurement framework automated using deep learning. , 2019, , .		1
140	A New Model for Securing Networks Based on Attack Graph. , 2019, , .		1
141	Vulnerability Severity Prediction With Deep Neural Network. , 2019, , .		10
142	How Secure Is Your IoT Network?. , 2019, , .		7
143	Challenges and Opportunities for Model-Based Security Risk Assessment of Cyber-Physical Systems. Advanced Sciences and Technologies for Security Applications, 2019, , 25-47.	0.4	4
144	Optimizing the network diversity to improve the resilience of networks against unknown attacks. Computer Communications, 2019, 145, 96-112.	3.1	16
146	Risk Assessment for Cyberattack in Active Distribution Systems Considering the Role of Feeder Automation. IEEE Transactions on Power Systems, 2019, 34, 3230-3240.	4.6	40

#	Article	IF	Citations
147	Multi-criteria Decision Making Model for Vulnerabilities Assessment in Cloud Computing regarding Common Vulnerability Scoring System. , 2019, , .		5
148	Modeling Stepping Stone Attacks with Constraints in Cyber Infrastructure. , 2019, , .		0
149	CyPhyR: a cyberâ€physical analysis tool for measuring and enabling resiliency in microgrids. IET Cyber-Physical Systems: Theory and Applications, 2019, 4, 313-321.	1.9	18
150	Automated Characterization of Software Vulnerabilities. , 2019, , .		7
151	Risk Prioritization by Leveraging Latent Vulnerability Features in a Contested Environment. , 2019, , .		7
152	Zero-day Vulnerability Inspired Hazard Assessment for Autonomous Driving Vehicles. , 2019, , .		3
153	Software Vulnerability and Application Security Risk. Information Resources Management Journal, 2019, 32, 48-57.	0.8	6
154	A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys and Tutorials, 2019, 21, 1851-1877.	24.8	230
155	Dynamic defense strategy against advanced persistent threat under heterogeneous networks. Information Fusion, 2019, 49, 216-226.	11.7	18
156	An analysis and classification of public information security data sources used in research and practice. Computers and Security, 2019, 82, 140-155.	4.0	22
157	Cost-aware securing of IoT systems using attack graphs. Ad Hoc Networks, 2019, 86, 23-35.	3.4	23
158	A look at the time delays in CVSS vulnerability scoring. Applied Computing and Informatics, 2019, 15, 129-135.	3.7	47
159	A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Electronics, 2020, 67, 2371-2379.	5.2	45
160	Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud. Future Generation Computer Systems, 2020, 111, 507-522.	4.9	14
161	The effect of Bellwether analysis on software vulnerability severity prediction models. Software Quality Journal, 2020, 28, 1413-1446.	1.4	14
162	CASeS: Concurrent Contingency Analysis-Based Security Metric Deployment for the Smart Grid. IEEE Transactions on Smart Grid, 2020, 11, 2676-2687.	6.2	15
163	Hybrid Firmware Analysis for Known Mobile and IoT Security Vulnerabilities. , 2020, , .		17
164	An automated framework for evaluating open-source web scanner vulnerability severity. Service Oriented Computing and Applications, 2020, 14, 297-307.	1.3	5

#	Article	IF	Citations
165	Factor of Security (FoS): Quantifying the Security Effectiveness of Redundant Smart Grid Subsystems. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	3.7	5
166	Risk Assessment in IT Infrastructure. , 2020, , .		1
167	An Unsupervised Learning-Based Network Threat Situation Assessment Model for Internet of Things. Security and Communication Networks, 2020, 2020, 1-11.	1.0	6
168	Security-aware dynamic VM consolidation. Egyptian Informatics Journal, 2020, 22, 277-277.	4.4	6
169	A Suite of Metrics for Calculating the Most Significant Security Relevant Software Flaw Types. , 2020, , .		3
170	Efficient Algorithm for Providing Live Vulnerability Assessment in Corporate Network Environment. Applied Sciences (Switzerland), 2020, 10, 7926.	1.3	7
171	Towards end-to-end Cyberthreat Detection from Twitter using Multi-Task Learning. , 2020, , .		7
172	Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs. IEEE Transactions on Control of Network Systems, 2020, 7, 1585-1596.	2.4	20
173	A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence. Annals of Nuclear Energy, 2020, 142, 107432.	0.9	11
174	A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System. , 2020, , .		9
175	Beyond Herd Immunity Against Strategic Attackers. IEEE Access, 2020, 8, 66365-66399.	2.6	2
176	Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants. Reliability Engineering and System Safety, 2020, 201, 106878.	5.1	26
177	An Automated Security Analysis Framework and Implementation for MTD Techniques on Cloud. Lecture Notes in Computer Science, 2020, , 150-164.	1.0	4
178	Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networksâ€™ Resilience Against Zero-Day Attacks. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 310-324.	3.7	16
179	Software vulnerability prioritization using vulnerability description. International Journal of Systems Assurance Engineering and Management, 2021, 12, 58-64.	1.5	18
180	Evaluating the effectiveness of shuffle and redundancy MTD techniques in the cloud. Computers and Security, 2021, 102, 102091.	4.0	13
181	Association Analysis-Based Cybersecurity Risk Assessment for Industrial Control Systems. IEEE Systems Journal, 2021, 15, 1423-1432.	2.9	13
182	On Parallel Real-Time Security Improvement Using Mixed-Integer Programming. IEEE Access, 2021, 9, 58824-58837.	2.6	1

#	Article	IF	Citations
183	Quality and Reliability Metrics for IoT Systems: A Consolidated View. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 635-650.	0.2	4
184	Machine Learning Algorithms for Conversion of CVSS Base Score from 2.0 to 3.x. Lecture Notes in Computer Science, 2021, , 255-269.	1.0	3
185	An Automated Post-Mortem Analysis of Vulnerability Relationships using Natural Language Word Embeddings. Procedia Computer Science, 2021, 184, 953-958.	1.2	4
186	Industrial Cyberâ€“Physical System Defense Resource Allocation Using Distributed Anomaly Detection. IEEE Internet of Things Journal, 2022, 9, 22304-22314.	5.5	5
187	A Zero Trust Hybrid Security and Safety Risk Analysis Method. Journal of Computing and Information Science in Engineering, 2021, 21, .	1.7	18
188	Communication Vulnerabilities in Electric Mobility HCP Systems: A Semi-Quantitative Analysis. Smart Cities, 2021, 4, 405-428.	5.5	5
189	Cyberâ€physical component ranking for risk sensitivity analysis using betweenness centrality. IET Cyber-Physical Systems: Theory and Applications, 2021, 6, 139-150.	1.9	12
190	Towards Practical Cybersecurity Mapping of STRIDE and CWE â€" a Multi-perspective Approach. , 2021, , .		4
191	ISM-AC: an immune security model based on alert correlation and software-defined networking. International Journal of Information Security, 2022, 21, 191-205.	2.3	5
192	Multi-Component Risk Assessment Using Cyber-Physical Betweenness Centrality. , 2021, , .		1
193	A survey of new orientations in the field of vehicular cybersecurity, applying artificial intelligence based methods. Transactions on Emerging Telecommunications Technologies, 2021, 32, e4325.	2.6	5
194	Evaluation indicators for open-source software: a review. Cybersecurity, 2021, 4, .	3.1	7
195	On the Flow of Software Security Advisories. IEEE Transactions on Network and Service Management, 2021, 18, 1305-1320.	3.2	7
196	Is Vulnerability Report Confidence Redundant? Pitfalls Using Temporal Risk Scores. IEEE Security and Privacy, 2021, 19, 44-53.	1.5	4
197	Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. Annals of Nuclear Energy, 2021, 158, 108287.	0.9	8
198	Vulnerability Exposure Driven Intelligence in Smart, Circular Cities. Digital Threats Research and Practice, 2022, 3, 1-18.	1.7	3
199	A Network Security Situational Awareness Framework Based on Situation Fusion. Lecture Notes in Computer Science, 2021, , 345-355.	1.0	3
200	Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement. IEEE Access, 2021, 9, 49662-49682.	2.6	18

#	Article	IF	Citations
202	GDPiRated â€“ Stealing Personal Information On- and Offline. Lecture Notes in Computer Science, 2019, , 367-386.	1.0	10
203	Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis. , 2020, , 109-129.		2
204	Cloud-Based Simulation Platform for Quantifying Cyber-Physical Systems Resilience. Simulation Foundations, Methods and Applications, 2020, , 349-384.	0.8	3
205	User-Centric Security Assessment of Software Configurations: A Case Study. Lecture Notes in Computer Science, 2014, , 196-212.	1.0	2
206	Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks. Lecture Notes in Computer Science, 2014, , 494-511.	1.0	30
207	Approximate Solutions for Attack Graph Games with Imperfect Information. Lecture Notes in Computer Science, 2015, , 228-249.	1.0	19
208	Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options. Lecture Notes in Computer Science, 2017, , 509-528.	1.0	10
209	Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks. , 2017, , 1-23.		24
210	Refining CVSS-Based Network Security Metrics by Examining the Base Scores. , 2017, , 25-52.		8
211	An Attack Graph-Based Probabilistic Security Metric. Lecture Notes in Computer Science, 2008, , 283-296.	1.0	216
212	An ACO Based Approach for Detection of an Optimal Attack Path in a Dynamic Environment. Lecture Notes in Computer Science, 2010, , 509-520.	1.0	2
213	Integrating Manual and Automatic Risk Assessment for Risk-Based Testing. Lecture Notes in Business Information Processing, 2012, , 159-180.	0.8	30
214	A Response Strategy Model for Intrusion Response Systems. International Federation for Information Processing, 2012, , 573-578.	0.4	4
215	Software Vulnerability Prioritization: A Comparative Study Using TOPSIS and VIKOR Techniques. Asset Analytics, 2019, , 405-418.	0.4	6
216	An automatic software vulnerability classification framework using term frequency-inverse gravity moment and feature selection. Journal of Systems and Software, 2020, 167, 110616.	3.3	17
217	Autonomous Security Analysis and Penetration Testing. , 2020, , .		29
218	Using variability modeling to support security evaluations. , 2020, , .		5
219	RUCKUS. , 2020, , .		2

#	Article	IF	Citations
220	A survey of methods supporting cyber situational awareness in the context of smart cities. Journal of Big Data, 2020, 7, .	6.9	19
221	A Novel Automatic Severity Vulnerability Assessment Framework. Journal of Communications, 2015, , .	1.3	5
222	Web Assessment of Libyan Government e-Government Services. International Journal of Advanced Computer Science and Applications, 2018, 9, .	0.5	5
223	Are Markets for Vulnerabilities Effective?. MIS Quarterly: Management Information Systems, 2012, 36, 43.	3.1	64
224	Distributed Analysis Tool for Vulnerability Prioritization in Corporate Networks. , 2020, , .		5
225	Improving Security for SCADA Control Systems. Informing Science and IT Education Conference, 0, , .	0.0	7
226	Cybersecurity: A Statistical Predictive Model for the Expected Path Length. Journal of Information Security, 2016, 07, 112-128.	0.4	11
229	Modeling and Simulation Approaches for Cybersecurity Impact Analysis: State-of-the-Art. , 2021, , .		3
230	Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. Applied Sciences (Switzerland), 2021, 11, 9812.	1.3	18
231	A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks. Applied Sciences (Switzerland), 2021, 11, 9972.	1.3	24
232	NETWORK SECURITY EVALUATION BASED ON SIMULATION OF MALFACTORâ€™S BEHAVIOR. , 2006, , .		1
233	A Framework for risk assessment of information technology in the corporate environment. The International Journal of Forensic Computer Science, 2007, , 75-88.	1.3	3
234	A Framework for Vulnerability Analysis during Software Maintenance. Communications in Computer and Information Science, 2011, , 282-287.	0.4	1
236	Improving Cloud Survivability through Dependency based Virtual Machine Placement. , 2012, , .		5
237	Novel Compositing Method for Quantification of Wireless Network Security. Communications in Computer and Information Science, 2012, , 1-6.	0.4	0
238	Towards Quantitative Risk Management for Next Generation Networks. Lecture Notes in Computer Science, 2012, , 229-239.	1.0	0
239	A Software Security Assessment System Based On Analysis of Vulnerabilities. Journal of Convergence Information Technology, 2012, 7, 211-219.	0.1	2
240	A New CVSS-Based Tool to Mitigate the Effects of Software Vulnerabilities. International Journal for Information Security Research, 2012, 2, 178-182.	0.3	2

#	Article	IF	Citations
242	Attack Graph-Based Risk Assessment and Optimisation Approach. Journal of Internet Technology and Secured Transaction, 2014, 3, 220-231.	0.2	1
243	Automated Exploit Detection using Path Profiling - The Disposition Should Matter, Not the Position. , 2015, , .		1
245	An Approach of Security Risk Evaluation Based on the Bayesian Attack Graph. Open Cybernetics and Systemics Journal, 2015, 9, 953-960.	0.3	2
246	Which country's end devices are most sharing vulnerabilities in East Asia?. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1281-1291.	0.1	0
247	Execution Path Classification for Vulnerability Analysis and Detection. Communications in Computer and Information Science, 2016, , 293-317.	0.4	0
248	Cost-Effective and Active Security Verification Framework for Web Application Vulnerabilities. KIPS Transactions on Computer and Communication Systems, 2016, 5, 189-196.	0.1	0
249	Quantitative Assessment Of General Cyber-Attack And Optimal Strategy-Selection Modelling In CPPS. , 2017, , .		0
250	Evaluating the Network Diversity of Networks Against Zero-Day Attacks. , 2017, , 117-140.		3
251	Quantitative Evaluation of Cyber-Attacks on a Hypothetical School Computer Network. Journal of Information Security, 2019, 10, 103-116.	0.4	2
252	Threat Modeling for Cloud Infrastructures. EAI Endorsed Transactions on Security and Safety, 2019, 5, 156246.	0.5	4
253	A Survey of Machine Learning Techniques Used to Combat Against the Advanced Persistent Threat. Communications in Computer and Information Science, 2019, , 159-172.	0.4	2
254	On Incorporating Security Parameters in Service Level Agreements. , 2019, , .		1
255	What Todayâ€™s Serious Cyber Attacks on Cars Tell Us: Consequences for Automotive Security and Dependability. Lecture Notes in Computer Science, 2019, , 270-285.	1.0	1
256	Data Security Threats Sources. Advances in Knowledge Acquisition, Transfer and Management Book Series, 2019, , 153-171.	0.1	0
257	Challenges in Quantifying an Adversaryâ€™s Cyber Access to Critical Infrastructures. Lecture Notes in Computer Science, 2020, , 18-28.	1.0	0
258	An Effective Semantic Security Metric for Industrial Cyber-Physical Systems. , 2020, , .		2
259	Towards a Zero Trust Hybrid Security and Safety Risk Analysis Method. , 2020, , .		5
260	The Creation of Network Intrusion Fingerprints by Graph Homomorphism. WSEAS Transactions on Information Science and Applications, 2020, 17, 124-131.	0.2	1

#	Article	IF	Citations
261	A Role Modeling Based Approach for Cyber Threat Analysis. Communications in Computer and Information Science, 2020, , 76-100.	0.4	0
262	A Proximity-Based Measure for Quantifying the Risk of Vulnerabilities. Communications in Computer and Information Science, 2020, , 41-59.	0.4	0
263	A Security Qualification Matrix to Efficiently Measure Security in Cyber-Physical Systems. , 2020, , .		2
264	Network Attack Path Selection and Evaluation Based on Q-Learning. Applied Sciences (Switzerland), 2021, 11, 285.	1.3	3
265	Cyclic Bayesian Attack Graphs: A Systematic Computational Approach. , 2020, , .		8
266	A Data-Mining Based Study of Security Vulnerability Types and Their Mitigation in Different Languages. Lecture Notes in Computer Science, 2020, , 1019-1034.	1.0	2
267	Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?. Creative Education, 2020, 11, 2541-2558.	0.2	0
268	A Quantitative Study of Vulnerabilities in the Internet of Medical Things. , 2020, , .		4
269	A Variational Generative Network Based Network Threat Situation Assessment. Lecture Notes in Computer Science, 2020, , 479-491.	1.0	1
270	Farsighted Risk Mitigation of Lateral Movement Using Dynamic Cognitive Honeypots. Lecture Notes in Computer Science, 2020, , 125-146.	1.0	4
271	Precisely Characterizing Security Impact in a Flood of Patches via Symbolic Rule Comparison. , 2020, , .		13
272	Towards Effective Identification and Rating of Automotive Vulnerabilities. , 2020, , .		3
273	AUTOMATED PENETRATION TESTING METHOD USING DEEP MACHINE LEARNING TECHNOLOGY. Advanced Information Systems, 2021, 5, 119-127.	0.1	4
274	An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities. Communications in Computer and Information Science, 2014, , 322-340.	0.4	1
275	Design and research of network security threat detection and traceability system based on AI. , 2021, , .		0
276	Continuous Security through Integration Testing in an Electronic Health Records System. , 2020, , .		1
277	Improving Interpretability for Cyber Vulnerability Assessment Using Focus and Context Visualizations. , 2020, , .		8
278	Cyber Situation Awareness Monitoring and Proactive Response for Enterprises on the Cloud. , 2020, , .		3

#	Article	IF	Citations
279	LICALITYâ€”Likelihood and Criticality: Vulnerability Risk Prioritization Through Logical Reasoning and Deep Learning. IEEE Transactions on Network and Service Management, 2022, 19, 1746-1760.	3.2	6
280	Super Learner Ensemble for Anomaly Detection and Cyber-Risk Quantification in Industrial Control Systems. IEEE Internet of Things Journal, 2022, 9, 13279-13297.	5.5	7
281	Twin Based Continuous Patching To Minimize Cyber Risk. European Journal for Security Research, 2021, 6, 211-227.	2.0	2
282	The Secret Life of Software Vulnerabilities: A Large-Scale Empirical Study. IEEE Transactions on Software Engineering, 2023, 49, 44-63.	4.3	20
283	Prioritizing vulnerability patches in large networks. Expert Systems With Applications, 2022, 193, 116467.	4.4	2
284	A novel approach to continuous CVE analysis on enterprise operating systems for system vulnerability assessment. International Journal of Information Technology (Singapore), 2022, 14, 1433-1443.	1.8	2
285	Time Series Network Data Enabling Distributed Intelligenceâ€”A Holistic IoT Security Platform Solution. Electronics (Switzerland), 2022, 11, 529.	1.8	2
286	Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud. IEEE Transactions on Emerging Topics in Computing, 2022, , 1-1.	3.2	5
287	Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 1154-1168.	3.7	2
288	Examining Penetration Tester Behavior in the Collegiate Penetration Testing Competition. ACM Transactions on Software Engineering and Methodology, 2022, 31, 1-25.	4.8	4
289	CRESS: Framework for Vulnerability Assessment of Attack Scenarios in Hardware Reverse Engineering. , 2021, , .		5
290	Crown Jewels Analysis using Reinforcement Learning with Attack Graphs. , 2021, , .		8
291	A CVSS-based Vulnerability Assessment Method for Reducing Scoring Error. , 2021, , .		2
292	Research on Smart Home Security Threat Modeling based on STRIDE-IAHP-BN. , 2021, , .		0
293	Optimal Security Protection Selection Strategy Based on Markov Model Attack Graph. Journal of Physics: Conference Series, 2021, 2132, 012020.	0.3	0
294	IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization. Journal of Network and Computer Applications, 2022, 203, 103398.	5.8	7
295	Cybersecurity Roadmap for Active Buildings. Green Energy and Technology, 2022, , 219-249.	0.4	2
296	Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings. Applied Sciences (Switzerland), 2022, 12, 5005.	1.3	4

#	Article	IF	Citations
297	Predicting CVSS Metric via Description Interpretation. IEEE Access, 2022, 10, 59125-59134.	2.6	6
298	Attributes Based Bayesian Unknown Hazards Assessment for Digital Twin Empowered Autonomous Driving. , 2021, , .		1
299	Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System With IoTs. IEEE Internet of Things Journal, 2023, 10, 7469-7479.	5.5	4
300	Consider the Consequences: A Risk Assessment Approach for Industrial Control Systems. Security and Communication Networks, 2022, 2022, 1-19.	1.0	5
301	Integrated Clinical Environment Security Analysis Using Reinforcement Learning. Bioengineering, 2022, 9, 253.	1.6	6
302	PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification. Journal of Network and Computer Applications, 2022, 205, 103440.	5.8	7
303	GridAttackAnalyzer: A Cyber Attack Analysis Framework for Smart Grids. Sensors, 2022, 22, 4795.	2.1	4
304	Security and Privacy Analysis of Smartphone-Based Driver Monitoring Systems from the Developerâ€™s Point of View. Sensors, 2022, 22, 5063.	2.1	1
305	Distributed Detection of Anomalies in the Network Flow Using Generative Adversarial Networks. , 2022, , .		2
306	XLNet-Based Prediction Model for CVSS Metric Values. Applied Sciences (Switzerland), 2022, 12, 8983.	1.3	3
307	Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems. Cybersecurity, 2022, 5, .	3.1	8
308	The Semantic Processing Pipeline: Quantifying the Network-Wide Impact of Security Tools. , 2020, , .		0
309	Protection Strategy Selection Model Based on Genetic Ant Colony Optimization Algorithm. Mathematics, 2022, 10, 3938.	1.1	1
310	Cyber Situational Awareness Frontiers. , 2022, , 43-75.		0
311	Risk assessment in distribution networks considering cyber coupling. International Journal of Electrical Power and Energy Systems, 2023, 145, 108650.	3.3	2
312	Reliability Assessment of Cyber-Physical Generation System. Iranian Journal of Science and Technology - Transactions of Electrical Engineering, 0, , .	1.5	0
313	Counterfeit object-oriented programming vulnerabilities: an empirical study in Java. , 2022, , .		1
314	Data Privacy Threat Modelling for Autonomous Systems: A Survey From the GDPR's Perspective. IEEE Transactions on Big Data, 2023, 9, 388-414.	4.4	2

#	Article	IF	Citations
315	Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities. International Journal of Electrical Power and Energy Systems, 2023, 147, 108892.	3.3	9
316	A Game-Theoretic Method for Defending Against Advanced Persistent Threats in Cyber Systems. IEEE Transactions on Information Forensics and Security, 2023, 18, 1349-1364.	4.5	6
317	Optimal Security Protection Strategy Selection Model Based on Q-Learning Particle Swarm Optimization. Entropy, 2022, 24, 1727.	1.1	0
318	A Quantification Method for the Heterogeneity of Mimic Control Plane in SDN. Electronics (Switzerland), 2022, 11, 3864.	1.8	0
319	Research on vulnerability of classification method of a complex information system. , 2022, , .		0
320	Data-driven Predictive Model of Windows 10's Vulnerabilities. , 2022, , .		0
321	A Hybrid Decision-making Approach to Security Metrics Aggregation in Cloud Environments. , 2022, , .		1
322	Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. Entropy, 2023, 25, 47.	1.1	7
323	Feasible Time Delay Attacks Against the Precision Time Protocol. , 2022, , .		1
325	Robust Moving Target Defense Against Unknown Attacks: A Meta-reinforcement Learning Approach. Lecture Notes in Computer Science, 2023, , 107-126.	1.0	0
326	Attack Graph Embedded Machine Learning Platform For Cyber Situational Awareness. , 2022, , .		0
327	Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework. Expert Systems With Applications, 2023, 221, 119734.	4.4	1
328	Security Analysis of Cyber-Physical Systems Using Reinforcement Learning. Sensors, 2023, 23, 1634.	2.1	4
329	Software Fault Tolerance in Real-Time Systems: Identifying the Future Research Questions. ACM Computing Surveys, 2023, 55, 1-30.	16.1	5
330	A Survey of Advanced Information Fusion System: from Model-Driven to Knowledge-Enabled. Data Science and Engineering, 2023, 8, 85-97.	4.6	1
333	Applying CVSS to Vulnerability Scoring in Cyber-Biological Systems. , 2023, , 115-134.		1
334	Tool-Based Approach on Digital Vulnerability Management Hub (VMH) by Using TheHive Platform. Springer Proceedings in Mathematics and Statistics, 2023, , 175-189.	0.1	0
336	CVE Records of Known Exploited Vulnerabilities. , 2023, , .		0

#	Article	IF	Citations
337	A Curriculum Framework for Autonomous Network Defense using Multi-agent Reinforcement Learning. , 2023, , .		2
338	VIET: A Tool forÂExtracting Essential Information fromÂVulnerability Descriptions forÂCVSS Evaluation. Lecture Notes in Computer Science, 2023, , 386-403.	1.0	0
339	VPnet: A Vulnerability Prioritization Approach Using Pointer Network andÂDeep Reinforcement Learning. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 307-325.	0.2	0
341	DRIVERS: A platform for dynamic risk assessment of emergent cyber threats for industrial control systems. , 2023, , .		0
342	Inferring Attack Paths in Networks with Periodic Topology Changes. , 2022, , .		0
345	UNI-CERT: A Unified Computer Emergency Response Teams Model for Malware Information Sharing Platform. , 2023, , .		0
346	Automatic Detection of API Access Control Vulnerabilities in Decentralized Web3 Applications. , 2023, , .		0
347	Discernment and Perusal of Software Vulnerability. Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 115-140.	0.4	0
353	Realistic Attacks with Realistic Attackers: An Information-Security Risk Analysis of an Automatic Metering Infrastructure. , 2023, , .		0
355	An ontology-based model for evaluating cloud attack scenarios in CATS â€“ a serious game in cloud security. , 2023, , .		0
356	Security Assessment of Low Earth Orbit (LEO) with Software-Defined Networking (SDN) Structure. , 2023, , .		0
357	Vulnerability Data Assessment and Management Based on Passive Scanning Method and CVSS. , 2023, , .		0
358	Can We Trust the Default Vulnerabilities Severity?. , 2023, , .		0
359	Automotive Software Security Engineering based on the ISO 21434. , 2023, , .		0
360	Merging FMEA and Digital Twins to Improve Trustfulness. , 2023, , .		0
361	Vulnerably (Mis)Configured? Exploring 10 Years of Developers' Q&As on Stack Overflow. , 2024, , .		0
362	Security Risk Visualization for Open-Source Software based on Vulnerabilities, Repositories, and Dependencies. , 2023, , .		0
363	Modeling and Risk Assessment of Cyber Attacks in Distribution Grid Cyber-physical Systems. , 2023, , .		0

#	Article	IF	Citations