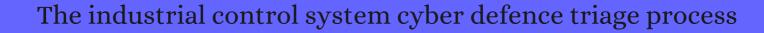
CITATION REPORT List of articles citing



DOI: 10.1016/j.cose.2017.07.009 Computers and Security, 2017, 70, 467-481.

Source: https://exaly.com/paper-pdf/67113811/citation-report.pdf

Version: 2024-04-10

This report has been generated based on the citations recorded by exaly.com for the above article. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

#	Paper	IF	Citations
33	Version control system of CAD documents and PLC projects. <i>Journal of Physics: Conference Series</i> , 2018 , 1015, 042020	0.3	3
32	Vulnerability Analysis of Network Scanning on SCADA Systems. <i>Security and Communication Networks</i> , 2018 , 2018, 1-21	1.9	34
31	A novel online state-based anomaly detection system for process control networks. <i>International Journal of Critical Infrastructure Protection</i> , 2019 , 27, 100323	4.1	4
30	Security gaps assessment of smart grid based SCADA systems. <i>Information and Computer Security</i> , 2019 , 27, 434-452	1.4	4
29	Protecting IoT and ICS Platforms Against Advanced Persistent Threat Actors: Analysis of APT1, Silent Chollima and Molerats. 2019 , 225-255		8
28	A Cyber Kill Chain Based Analysis of Remote Access Trojans. 2019 , 273-299		5
27	Cyber threats for operational technologies. <i>International Journal of System of Systems Engineering</i> , 2020 , 10, 128	0.3	O
26	Attack signal estimation for intrusion detection in industrial control system. <i>Computers and Security</i> , 2020 , 96, 101926	4.9	3
25	Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. <i>Journal of Information Security and Applications</i> , 2020 , 52, 102500	3.5	22
24	Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems. <i>IEEE Transactions on Systems, Man, and Cybernetics: Systems</i> , 2021 , 1-13	7.3	5
23	Analysis of a HIPS Solution Use in Power Systems. <i>Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering</i> , 2021 , 255-264	0.2	
22	A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 2021, 16, 490-	·5 1 339	1
21	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. <i>Computers and Security</i> , 2021 , 109, 102398	4.9	1
20	Analysis of APT Actors Targeting IoT and Big Data Systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a Case Study. 2019 , 257-272		2
19	SAMIIT: Spiral Attack Model in IIoT Mapping Security Alerts to Attack Life Cycle Phases.		8
18	From Cyber Terrorism to Cyber Peacekeeping: Are we there yet?. 2020 ,		0
17	A Threat Hunting Framework for Industrial Control Systems. <i>IEEE Access</i> , 2021 , 9, 164118-164130	3.5	1

CITATION REPORT

16	A cyber incident response and recovery framework to support operators of ICS and Critical National Infrastructure. <i>International Journal of Critical Infrastructure Protection</i> , 2022 , 37, 100505	4.1	1
15	Cybersecurity in the Era of Digital Transformation: The case of Greece. 2020 ,		3
14	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	0.3	2
13	SOC Critical Path: A Defensive Kill Chain Model. <i>IEEE Access</i> , 2022 , 10, 13570-13581	3.5	O
12	Measuring the Impact of Tactical Denial of Sustainability. Lecture Notes in Computer Science, 2022, 537	-5 5 69	
11	Optimizing digital controller of continuous object automatic control system. <i>Vestnik of Astrakhan State Technical University Series Marine Engineering and Technologies</i> , 2022 , 2022, 67-78	0.1	
10	THE ESSENCE OF CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION, NATO AND G7 COUNTRIES. International Journal of Innovative Technologies in Economy, 2022,	0.2	
9	How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks. 2022 ,		2
8	Context-Aware Ontology-based Security Measurement Model. <i>Journal of Information Security and Applications</i> , 2022 , 67, 103199	3.5	
7	Cyber attacks, security data detection, and critical loads in the power systems. 2023 , 169-184		O
6	Industrial control systems cybersecurity: Back to basic cyber hygiene practices. 2022,		O
5	On specification-based cyber-attack detection in smart grids. 2022 , 5,		O
4	Cybersecurity Analysis of Wind Farm Industrial Control System Based on Hierarchical Threat Analysis Model Framework. 2022 ,		О
3	Threats Evaluation of Border Power Plants from the Perspective of Fuel Type and Providing Solutions to Deal with Them: A Case Study of Iran.		O
2	A Survey on Cybersecurity Barrier Management in Process Control Environments. 2022,		0
1	Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. 2023 , 7, 1-33		O