Hein S Venter

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/4123173/publications.pdf

Version: 2024-02-01

114	1,559	430874 18	477307 29
papers	citations	h-index	g-index
125	125	125	828
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Social engineering attack examples, templates and scenarios. Computers and Security, 2016, 59, 186-209.	6.0	103
2	A taxonomy for information security technologies. Computers and Security, 2003, 22, 299-307.	6.0	61
3	Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International (Online), 2019, 1, 61-67.	1.3	50
4	Social engineering attack framework. , 2014, , .		47
5	Social engineering attack detection model: SEADM. , 2010, , .		45
6	Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences, 2018, 50, 552-591.	1.2	43
7	Harmonised digital forensic investigation process model. , 2012, , .		39
8	Performance Costs of Software Cryptography in Securing New-Generation Internet of Energy Endpoint Devices. IEEE Access, 2018, 6, 9303-9323.	4.2	38
9	Towards an Ontological Model Defining the Social Engineering Domain. IFIP Advances in Information and Communication Technology, 2014, , 266-279.	0.7	38
10	Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, 2015, 60, 885-893.	1.6	37
11	On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. Australian Journal of Forensic Sciences, 2018, 50, 209-238.	1.2	33
12	The use of self-organising maps for anomalous behaviour detection in a digital investigation. Forensic Science International, 2006, 162, 33-37.	2.2	31
13	The architecture of a digital forensic readiness management system. Computers and Security, 2013, 32, 73-89.	6.0	30
14	A Comprehensive and Harmonized Digital Forensic Investigation Process Model. Journal of Forensic Sciences, 2015, 60, 1467-1483.	1.6	29
15	Toward a General Ontology for Digital Forensic Disciplines. Journal of Forensic Sciences, 2014, 59, 1231-1241.	1.6	28
16	On the importance of standardising the process of generating digital forensic reports. Forensic Science International: Reports, 2019, 1, 100008.	0.8	26
17	Mobile Botnet Detection Using Network Forensics. Lecture Notes in Computer Science, 2010, , 57-67.	1.3	25
18	Necessity for ethics in social engineering research. Computers and Security, 2015, 55, 114-127.	6.0	24

#	Article	IF	Citations
19	Adding Digital Forensic Readiness as a Security Component to the IoT Domain. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8, 1.	0.4	24
20	Digital forensic readiness in the cloud. , 2013, , .		23
21	Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?. Digital Investigation, 2019, 30, 73-89.	3.2	23
22	A cognitive approach for botnet detection using Artificial Immune System in the cloud. , 2014, , .		21
23	Social Engineering Attack Detection Model: SEADMv2. , 2015, , .		21
24	Testing the harmonised digital forensic investigation process model-using an Android mobile phone. , 2013, , .		20
25	Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem. , 2018, , .		20
26	Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Science International: Reports, 2020, 2, 100117.	0.8	19
27	Digital Forensic Readiness Framework for Ransomware Investigation. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2019, , 91-105.	0.3	19
28	Towards a Digital Forensic Readiness Framework for Public Key Infrastructure systems. , 2011, , .		17
29	Using time-driven activity-based costing to manage digital forensic readiness in large organisations. Information Systems Frontiers, 2012, 14, 1061-1077.	6.4	17
30	A generic Digital Forensic Readiness model for BYOD using honeypot technology. , 2016, , .		17
31	Adding event reconstruction to a Cloud Forensic Readiness model. , 2015, , .		16
32	A natural human language framework for digital forensic readiness in the public cloud. Australian Journal of Forensic Sciences, 2021, 53, 566-591.	1.2	16
33	How an IoT-enabled â€œsmart refrigeratorâ€• can play a clandestine role in perpetuating cyber-crime. , 2017, , .		15
34	A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. Wiley Interdisciplinary Reviews Forensic Science, 2019, 1, .	2.1	15
35	Observing Consistency in Online Communication Patterns for User Re-Identification. PLoS ONE, 2016, 11, e0166930.	2.5	15
36	Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness. , 2011, , .		14

#	Article	IF	Citations
37	Digital forensic readiness in a cloud environment. , 2013, , .		14
38	Mobile forensics using the harmonised digital forensic investigation process. , 2014, , .		14
39	Ontologyâ€driven perspective of CFRaaS. Wiley Interdisciplinary Reviews Forensic Science, 2020, 2, e1372.	2.1	14
40	A prototype for achieving digital forensic readiness on wireless sensor networks. , 2011, , .		13
41	A Harmonized Process Model for Digital Forensic Investigation Readiness. IFIP Advances in Information and Communication Technology, 2013, , 67-82.	0.7	13
42	Leveraging Human Thinking Style for User Attribution in Digital Forensic Process. International Journal on Advanced Science, Engineering and Information Technology, 2017, 7, 198.	0.4	13
43	A Forensic Readiness Model for Wireless Networks. International Federation for Information Processing, 2010, , 107-117.	0.4	13
44	Standardising vulnerability categories. Computers and Security, 2008, 27, 71-83.	6.0	12
45	Digital forensics in the Cloud: The state of the art. , 2015, , .		12
46	Digital forensic readiness framework based on behavioral-biometrics for user attribution. , 2017, , .		12
47	PIDS: a privacy intrusion detection system. Internet Research, 2004, 14, 360-365.	4.9	11
48	Simulating adversarial interactions between intruders and system administrators using OODA-RR. , 2007, , .		11
49	CVSS Metric-Based Analysis, Classification and Assessment of Computer Network Threats and Vulnerabilities. , 2018, , .		11
50	Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures. , 2017, , .		10
51	User attribution based on keystroke dynamics in digital forensic readiness process. , 2017, , .		10
52	Windows registry harnesser for incident response and digital forensic analysis. Australian Journal of Forensic Sciences, 2020, 52, 337-353.	1.2	10
53	Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes. , 2020, , .		10
54	Smart Microgrid Energy Market: Evaluating Distributed Ledger Technologies for Remote and Constrained Microgrid Deployments. Electronics (Switzerland), 2021, 10, 714.	3.1	10

#	Article	IF	Citations
55	Smart Digital Forensic Readiness Model for Shadow IoT Devices. Applied Sciences (Switzerland), 2022, 12, 730.	2.5	10
56	Vulnerability forecastingâ€"a conceptual model. Computers and Security, 2004, 23, 489-497.	6.0	9
57	Finite State Machine for the Social Engineering Attack Detection Model: SEADM. SAIEE Africa Research Journal, 2018, 109, 133-148.	1.2	9
58	Polychronicity tendency-based online behavioral signature. International Journal of Machine Learning and Cybernetics, 2019, 10, 2103-2118.	3.6	9
59	Implementation guidelines for a harmonised digital forensic investigation readiness process model. , 2013, , .		8
60	Social engineering from a normative ethics perspective. , 2013, , .		8
61	Introduction of concurrent processes into the digital forensic investigation process. Australian Journal of Forensic Sciences, 2016, 48, 339-357.	1.2	8
62	CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent. African Journal of Science, Technology, Innovation and Development, 2019, 11, 749-769.	1.6	8
63	Ontology for Reactive Techniques in Digital Forensics. , 2019, , .		8
64	Digital forensic application requirements specification process. Australian Journal of Forensic Sciences, 2019, 51, 371-394.	1.2	8
65	Digital forensic readiness in operational cloud leveraging <scp>ISO</scp>/<scp>IEC</scp> 27043 guidelines on security monitoring. Security and Privacy, 2021, 4, e149.	2.7	8
66	A Model for Digital Evidence Admissibility Assessment. IFIP Advances in Information and Communication Technology, 2017, , 23-38.	0.7	8
67	Considerations Towards a Cyber Crime Profiling System. , 2008, , .		7
68	Adding digital forensic readiness to electronic communication using a security monitoring tool. , 2011, , .		7
69	Guidelines for procedures of a harmonised digital forensic process in network forensics. , 2012, , .		7
70	Towards a framework for enhancing potential digital evidence presentation. , 2013, , .		7
71	Vulnerability forecastingâ€"a conceptual model. Computers and Security, 2004, 23, 489-497.	6.0	7
72	Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems. SAIEE Africa Research Journal, 2016, 107, 104-120.	1.2	6

#	ARTICLE	IF	CITATIONS
73	Attributing users based on web browser history. , 2017, , .		6
74	Underlying finite state machine for the social engineering attack detection model. , 2017, , .		6
75	Developing a Secure, Smart Microgrid Energy Market using Distributed Ledger Technologies. , 2019, , .		6
76	Secure Storage Model for Digital Forensic Readiness. IEEE Access, 2022, 10, 19469-19480.	4.2	6
77	Assessment Of Vulnerability Scanners. Network Security, 2003, 2003, 11-16.	0.8	5
78	Towards a prototype for guidance and implementation of a standardized digital forensic investigation process. , 2014, , .		5
79	Security issues in the security cyber supply chain in South Africa. Technovation, 2014, 34, 392-393.	7.8	5
80	ISO/IEC 27043:2015 â€" Role and application. , 2016, , .		5
81	A heuristics for HTTP traffic identification in measuring user dissimilarity. Human-Intelligent Systems Integration, 2020, 2, 17-28.	2.5	5
82	Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. , 2020, , .		5
83	Data packet intercepting on the internet: How and why? A closer look at existing data packet-intercepting tools. Computers and Security, 1998, 17, 683-692.	6.0	4
84	Network Security: Important Issues. Network Security, 2000, 2000, 12-16.	0.8	4
85	A security privacy aware architecture and protocol for a single smart card used for multiple services. Computers and Security, 2010, 29, 393-409.	6.0	4
86	Adding digital forensic readiness to the email trace header. , 2010, , .		4
87	Measuring semantic similarity between digital forensics terminologies using web search engines. , 2012, , .		4
88	A digital forensic model for providing better data provenance in the cloud. , 2014, , .		4
89	FReadyPass: a digital forensic ready passport to control access to data across jurisdictional boundaries. Australian Journal of Forensic Sciences, 2019, 51, 583-595.	1.2	4
90	Proof of Concept of the Online Neighbourhood Watch System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2016, , 78-93.	0.3	4

#	Article	IF	Citations
91	Towards Privacy Taxonomy-Based Attack Tree Analysis for the Protection of Consumer Information Privacy. , 2008, , .		3
92	Information Privacy in Two Dimensions - Towards a Classification Scheme for Information Privacy Research. , 2010, , .		3
93	Selection and ranking of remote hosts for digital forensic investigation in a Cloud environment. , 2013, , .		3
94	Automated RAM analysis mechanism for windows operating system for digital investigation. , 2017, , .		3
95	Forensic Profiling of Cyber-Security Adversaries based on Incident Similarity Measures Interaction Index. , 2018, , .		3
96	Mapping digital forensic application requirement specification to an international standard. Forensic Science International: Reports, 2020, 2, 100137.	0.8	3
97	CBAC4C: conflictâ€based VM isolation control for cloud computing. International Transactions in Operational Research, 2022, 29, 372-395.	2.7	3
98	Real-time Risk Analysis on the Internet. IFIP Advances in Information and Communication Technology, 1999, , 11-27.	0.7	3
99	Practical Approach to Urban Crime Prevention in Developing Nations. , 2020, , .		3
100	Applying The Biba Integrity Model to Evidence Management. , 2007, , 317-327.		3
101	Using Object-Oriented Concepts to Develop a High-Level Information Privacy Risk Management Model. , 2009, , .		2
102	Understanding the Level of Compliance by South African Institutions to the Protection of Personal Information (POPI) Act. , 2016, , .		2
103	High-level online user attribution model based on human Polychronic-Monochronic tendency. , 2017, , .		2
104	Scenario-Based Digital Forensic Investigation of Compromised MySQL Database. , 2019, , .		2
105	Implementing Forensic Readiness Using Performance Monitoring Tools. International Federation for Information Processing, 2012, , 261-270.	0.4	2
106	Vulnerabilities categories for intrusion detection systems. Computers and Security, 2002, 21, 617-619.	6.0	1
107	User-generated digital forensic evidence in graphic design applications. , 2012, , .		1
108	Evaluation and analysis of a software prototype for guidance and implementation of a standardized digital forensic investigation process. , 2015, , .		1

#	Article	IF	Citations
109	A model for the design of next generation e-supply chain digital forensic readiness tools. , 2015, , .		1
110	Personal Anomaly-based Intrusion Detection Smart Card Using Behavioural Analysis. International Federation for Information Processing, 2007, , 217-228.	0.4	1
111	LOCATING AND TRACKING DIGITAL OBJECTS IN THE CLOUD. IFIP Advances in Information and Communication Technology, 2015, , 287-301.	0.7	1
112	Digital forensic readiness for branchless banking. , 2015, , .		0
113	Cursory View of IoT-Forensic Readiness Framework Based on ISO/IEC 27043 Recommendations. Lecture Notes in Networks and Systems, 2021, , 229-239.	0.7	0
114	A Conceptual Model for Consent Management in South African e-Health Systems for Privacy Preservation. Communications in Computer and Information Science, 2020, , 69-82.	0.5	0