HervÃ© Debar

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3039006/publications.pdf

Version: 2024-02-01

79 papers	2,686 citations	361296 20 h-index	206029 48 g-index
83 all docs	83 docs citations	83 times ranked	1406 citing authors

#	Article	IF	Citations
1	A Survey on Game-Theoretic Approaches for Intrusion Detection and Response Optimization. ACM Computing Surveys, 2019, 51, 1-31.	16.1	37
2	Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems, 2018, 83, 535-552.	4.9	37
3	ArOMA: An SDN based autonomic DDoS mitigation framework. Computers and Security, 2017, 70, 482-499.	4.0	54
4	Selection of Pareto-efficient response plans based on financial and operational assessments. Eurasip Journal on Information Security, 2017, 2017, .	2.4	6
5	Security Issues and Mitigation in Ethernet POWERLINK. Lecture Notes in Computer Science, 2017, , 87-102.	1.0	2
6	StemJail. , 2016, , .		1
7	New Types of Alert Correlation for Security Information and Event Management Systems. , 2016, , .		9
8	Selection of Mitigation Actions Based on Financial and Operational Impact Assessments. , 2016, , .		5
9	ML: DDoS Damage Control with MPLS. Lecture Notes in Computer Science, 2016, , 101-116.	1.0	0
10	Towards an Automated and Dynamic Risk Management Response System. Lecture Notes in Computer Science, 2016, , 37-53.	1.0	6
11	Attack Volume Model: Geometrical Approach and Application. Lecture Notes in Computer Science, 2016, , 242-257.	1.0	1
12	Hybrid Risk Assessment Model Based on Bayesian Networks. Lecture Notes in Computer Science, 2016, , 21-40.	1.0	4
13	On the Isofunctionality of Network Access Control Lists. , 2015, , .		2
14	Automated Classification of C&C Connections Through Malware URL Clustering. IFIP Advances in Information and Communication Technology, 2015, , 252-266.	0.5	9
15	TLS Record Protocol. , 2015, , .		3
16	Policy Enforcement Point Model. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2015, , 278-286.	0.2	2
17	Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats (APTs). , 2015, , .		1
18	Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index. Computers and Electrical Engineering, 2015, 47, 13-34.	3.0	28

#	Article	IF	Citations
19	Using a 3D Geometrical Model to Improve Accuracy in the Evaluation and Selection of Countermeasures Against Complex Cyber Attacks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2015, , 538-555.	0.2	9
20	RORI-based countermeasure selection using the OrBAC formalism. International Journal of Information Security, 2014, 13, 63-79.	2.3	27
21	Classification of SSL Servers based on their SSL Handshake for Automated Security Assessment. , 2014, , .		7
22	Attribute-Based Mining Process for the Organization-Based Access Control Model. , 2013, , .		0
23	Parsifal: Writing efficient and robust binary parsers, quickly. , 2013, , .		1
24	A TCP delay-based mechanism for detecting congestion in the Internet. , 2013, , .		4
25	An Adaptive Mitigation Framework for Handling Suspicious Network Flows via MPLS Policies. Lecture Notes in Computer Science, 2013, , 297-312.	1.0	0
26	Service Dependencies-Aware Policy Enforcement Framework Based on Hierarchical Colored Petri Net. Communications in Computer and Information Science, 2013, , 313-321.	0.4	0
27	An ontology-driven approach to model SIEM information and operations using the SWRL formalism. International Journal of Electronic Security and Digital Forensics, 2012, 4, 104.	0.1	9
28	Limitation of Honeypot/Honeynet Databases to Enhance Alert Correlation. Lecture Notes in Computer Science, 2012, , 203-217.	1.0	6
29	HADEGA: A novel MPLS-based mitigation solution to handle network attacks. , 2012, , .		7
30	VESPA. , 2012, , .		20
31	Cross-domain vulnerabilities over social networks. , 2012, , .		3
32	Combination approach to select optimal countermeasures based on the RORI index. , 2012, , .		5
33	One year of SSL internet measurement. , 2012, , .		20
34	Challenges for Advanced Security Monitoring â€“ The MASSIF Project. Lecture Notes in Computer Science, 2012, , 222-223.	1.0	3
35	Individual Countermeasure Selection Based on the Return On Response Investment Index. Lecture Notes in Computer Science, 2012, , 156-170.	1.0	16
36	Botnets: Lifecycle and Taxonomy. , 2011, , .		34

#	Article	IF	Citations
37	Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources. , 2011, , .		6
38	Challenges for Cloud Networking Security. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2011, , 298-313.	0.2	17
39	Service Dependencies in Information Systems Security. Lecture Notes in Computer Science, 2010, , 1-20.	1.0	7
40	Formalization of Viruses and Malware Through Process Algebras. , 2010, , .		10
41	A Service Dependency Model for Cost-Sensitive Intrusion Response. Lecture Notes in Computer Science, 2010, , 626-642.	1.0	58
42	Caching P2P Traffic: What Are the Benefits for an ISP?. , 2010, , .		4
43	Ex-SDF: An Extended Service Dependency Framework for Intrusion Impact Assessment. IFIP Advances in Information and Communication Technology, 2010, , 148-160.	0.5	0
44	Processing intrusion detection alert aggregates with time series modeling. Information Fusion, 2009, 10, 312-324.	11.7	69
45	Functional polymorphic engines: formalisation, implementation and use cases. Journal in Computer Virology, 2009, 5, 247-261.	1.9	5
46	XeNA: an access negotiation framework using XACML. Annales Des Telecommunications/Annals of Telecommunications, 2009, 64, 155-169.	1.6	22
47	A logic-based model to support alert correlation in intrusion detection. Information Fusion, 2009, 10, 285-299.	11.7	64
48	An ontology-based approach to react to network attacks. International Journal of Information and Computer Security, 2009, 3, 280.	0.2	29
49	A Service Dependency Modeling Framework for Policy-Based Response Enforcement. Lecture Notes in Computer Science, 2009, , 176-195.	1.0	5
50	Malware Behavioral Detection by Attribute-Automata Using Abstraction from Platform and Language. Lecture Notes in Computer Science, 2009, , 81-100.	1.0	20
51	Malware as interaction machines: a new framework for behavior modelling. Journal in Computer Virology, 2008, 4, 235-250.	1.9	7
52	Behavioral detection of malware: from a survey towards an established taxonomy. Journal in Computer Virology, 2008, 4, 251-266.	1.9	166
53	An ontology-based approach to react to network attacks. , 2008, , .		10
54	Analysis of Computer Infection Risk Factors Based on Customer Network Usage. , 2008, , .		13

#	Article	IF	Citations
55	Negotiation of Prohibition: An Approach Based on Policy Rewriting. International Federation for Information Processing, 2008, , 173-187.	0.4	0
56	Resource Classification Based Negotiation in Web Services. , 2007, , .		1
57	Enabling automated threat response through the use of a dynamic security policy. Journal in Computer Virology, 2007, 3, 195-210.	1.9	35
58	Using Contextual Security Policies for Threat Response. Lecture Notes in Computer Science, 2006, , 109-128.	1.0	14
59	An extended RBAC profile of XACML. , 2006, , .		25
60	Security information management as an outsourced service. Information Management and Computer Security, 2006, 14, 417-435.	1.2	12
61	Network and information systems security. Annales Des Telecommunications/Annals of Telecommunications, 2006, 61, 242-244.	1.6	0
62	WebAnalyzer: accurate detection of HTTP attack traces in web server logs. Annales Des Telecommunications/Annals of Telecommunications, 2006, 61, 682-704.	1.6	5
63	Time series modeling for IDS alert management. , 2006, , .		57
64	Improving security management through passive network observation. , 2006, , .		5
65	Intrusion Detection: Introduction to Intrusion Detection and Security Information Management. Lecture Notes in Computer Science, 2005, , 207-236.	1.0	13
66	An Infrastructure for Distributed Event Acquisition. , 2005, , 349-365.		2
67	Monitoring IDS Background Noise Using EWMA Control Charts and Alert Information. Lecture Notes in Computer Science, 2004, , 166-187.	1.0	21
68	Correlation of Intrusion Symptoms: An Application of Chronicles. Lecture Notes in Computer Science, 2003, , 94-112.	1.0	103
69	M2D2: A Formal Data Model for IDS Alert Correlation. Lecture Notes in Computer Science, 2002, , 115-137.	1.0	154
70	Evaluation of the Diagnostic Capabilities of Commercial Intrusion Detection Systems. Lecture Notes in Computer Science, 2002, , 177-198.	1.0	16
71	Aggregation and Correlation of Intrusion-Detection Alerts. Lecture Notes in Computer Science, 2001, , 85-103.	1.0	384
72	A revised taxonomy for intrusion-detection systems. Annales Des Telecommunications/Annals of Telecommunications, 2000, 55, 361-378.	1.6	203

#	Article	IF	Citations
73	Fixed- vs. variable-length patterns for detecting suspicious process behavior. Journal of Computer Security, 2000, 8, 159-181.	0.5	13
74	Intrusion Detection Using Variable-Length Audit Trail Patterns. Lecture Notes in Computer Science, 2000, , 110-129.	1.0	105
75	Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999, 31, 805-822.	3.2	533
76	Authenticating public terminals. Computer Networks, 1999, 31, 861-870.	3.2	40
77	Fixed vs. variable-length patterns for detecting suspicious process behavior. Lecture Notes in Computer Science, 1998, , 1-15.	1.0	13
78	Honeypots: practical means to validate malicious fault assumptions practical experience report. , 0, , .		16
79	Combining Technical and Financial Impacts for Countermeasure Selection. Electronic Proceedings in Theoretical Computer Science, EPTCS, 0, 165, 1-14.	0.8	1