Technical Aspects of Cyber Kill Chain

DOI: 10.1007/978-3-319-22915-7_40
Communications in Computer and Information Science, 2015, , 438-452.

#	Paper	IF	Citations
68	Hybrid Intrusion Detection in Information Systems. **2016**,		3
67	Multi-dimensional structural data integration for proactive cyber-defence. **2017**,		
66	On the Impact of Kernel Code Vulnerabilities in IoT Devices. **2017**,		3
65	Scientific workflow execution system based on mimic defense in the cloud environment. *Frontiers of Information Technology and Electronic Engineering*, **2018**, 19, 1522-1536	2.2	11
64	Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture. **2018**,		4
63	A System Attack Surface Based MTD Effectiveness and Cost Quantification Framework. **2018**,		1
62	An Analysis of Cyber Security Attack Taxonomies. **2018**,		7
61	Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. **2019**,		7
60	Enhancing the Reliability of NFV with Heterogeneous Backup. **2019**,		1
59	A Positive Feedback Mechanism of Adaptive Dynamic System. *IOP Conference Series: Materials Science and Engineering*, **2019**, 569, 042009	0.4	
58	A Cyber Kill Chain Based Analysis of Remote Access Trojans. **2019**, 273-299		5
57	Security Threats Against LTE Networks: A Survey. *Communications in Computer and Information Science*, **2019**, 242-256	0.3	1
56	Identification of Bugs and Vulnerabilities in TLS Implementation for Windows Operating System Using State Machine Learning. *Communications in Computer and Information Science*, **2019**, 348-362	0.3	1
55	On the practical integration of anomaly detection techniques in industrial control applications. *International Journal of Critical Infrastructure Protection*, **2019**, 24, 48-68	4.1	5
54	Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, **2020**, 3,	5	4
53	A Receding-Horizon MDP Approach for Performance Evaluation of Moving Target Defense in Networks. **2020**,		2
52	Incidents Are Meant for Learning, Not Repeating: Sharing Knowledge About Security Incidents in Cyber-Physical Systems. *IEEE Transactions on Software Engineering*, **2020**, 1-1	3.5	1

51	Protecting scientific workflows in clouds with an intrusion tolerant system. *IET Information Security*, **2020**, 14, 157-165	1.4	2
50	HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Transactions on Knowledge and Data Engineering*, **2020**, 1-1	4.2	16
49	Hacking Tool Identification in Penetration Testing. **2020**,		0
48	A Dynamic Processing Algorithm for Variable Data in Intranet Security Monitoring. *Lecture Notes in Computer Science*, **2021**, 147-156	0.9	
47	A Human Factor Approach to Threat Modeling. *Lecture Notes in Computer Science*, **2021**, 139-157	0.9	1
46	Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack. *Lecture Notes in Computer Science*, **2021**, 37-52	0.9	
45	Human-Machine Cooperation and Optimizing Strategies for Cyberspace OSINT Analysis. *Lecture Notes in Networks and Systems*, **2022**, 634-642	0.5	
44	The Seven Golden Principles of Effective Anomaly-Based Intrusion Detection. *IEEE Security and Privacy*, **2021**, 19, 36-45	2	
43	Machine Learning-Based Cyber Attacks Targeting on Controlled Information. *ACM Computing Surveys*, **2022**, 54, 1-36	13.4	24
42	Stochastic Model of the Simple Cyber Kill Chain: Cyber Attack Process as a Regenerative Process. *Lecture Notes in Computer Science*, **2020**, 355-365	0.9	1
41	Moving Target Defense Based on Adaptive Forwarding Path Migration for Securing the SCADA Network. *Security and Communication Networks*, **2021**, 2021, 1-15	1.9	
40	Comprehensive Study in Preventive Measures of Data Breach Using Thumb-Sucking. *Lecture Notes in Computer Science*, **2018**, 57-65	0.9	
39	Preparing Smart Cities for Ransomware Attacks. **2020**,		0
38	Cyber Mission Operations: A Literature Review. *Advances in Intelligent Systems and Computing*, **2020**, 31-37	0.4	
37	Evaluation Methods of WEB Security Threats Based on Situation Change. **2020**,		
36	Beyond Labeling: Using Clustering to Build Network Behavioral Profiles of Malware Families. **2021**, 381-409		3
35	Cyber Threat Hunting Through Automated Hypothesis and Multi-Criteria Decision Making. **2020**,		0
34	Plenty of Phish in the Sea: Analyzing Potential Pre-attack Surfaces. *Lecture Notes in Computer Science*, **2020**, 272-291	0.9	1

33	A Serious Game-Based Peer-Instruction Digital Forensics Workshop. *IFIP Advances in Information and Communication Technology*, **2020**, 127-141	0.5	1
32	Design and Development of System for Post-infection Attack Behavioral Analysis. *Advances in Intelligent Systems and Computing*, **2021**, 554-565	0.4	
31	Knowing the unknown: The hunting loop. *International Journal of Advanced and Applied Sciences*, **2022**, 9, 8-19	1.2	
30	A Study of Evaluation Methods of WEB Security Threats Based on Multi-stage Attack. **2020**,		
29	Credential Intelligence Agency: A Threat Intelligence Approach to Mitigate Identity Theft. *Communications in Computer and Information Science*, **2022**, 115-138	0.3	
28	APT-Dt-KC: advanced persistent threat detection based on kill-chain model. *Journal of Supercomputing*, **2022**, 78, 8644	2.5	1
27	SDGen: A Scalable, Reproducible and Flexible Approach to Generate Real World Cyber Security Datasets. *Communications in Computer and Information Science*, **2022**, 102-115	0.3	3
26	TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. *Cybersecurity*, **2022**, 5,	5	1
25	APTSID: An Ensemble Learning Method for APT Attack Stage Identification. **2021**,		
24	Polymer: An Adaptive Kill Chain Expanding Cyber Threat Hunting to Multi-Platform Environments. **2021**,		
23	Towards Countering the Insider Reconnaissance Using a Combination of Shuffling and Diversity Moving Target Defense Techniques. *Engineering, Technology & Applied Science Research*, **2021**, 11, 7745-7749	1	
22	How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks. **2022**,		2
21	Minimum Prediction Error at an Early Stage in Darknet Analysis. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, **2022**, 18-30	0.2	
20	Survey and Taxonomy of Adversarial Reconnaissance Techniques. *ACM Computing Surveys*,	13.4	1
19	Lightweight On-Demand Honeypot Deployment for Cyber Deception. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2022**, 294-312	0.2	0
18	Potential cyber-threats against Canada's critical infrastructure: an investigation of online discussion forums. *Criminal Justice Studies*, 1-24	0.9	
17	Pikachu: Temporal Walk Based Dynamic Graph Embedding for Network Anomaly Detection. **2022**,		
16	Identification of Attack Paths Using Kill Chain and Attack Graphs. **2022**,		

15	Improving detection of scanning attacks on heterogeneous networks with Federated Learning. *Performance Evaluation Review*, **2022**, 49, 118-123	0.4	0
14	Improving Network-Based Anomaly Detection in Smart Home Environment. *Sensors*, **2022**, 22, 5626	3.8	0
13	Automatic online quantification and prioritization of data protection risks. **2022**,		
12	Advisory. **2022**,		
11	SAMGRID: Security Authorization and Monitoring Module Based on SealedGRID Platform. **2022**, 22, 6527		0
10	Threats Modeling and Anomaly Detection in the Behaviour of a System - A Review of Some Approaches. **2022**, 1-27		0
9	A deep learner model for multi-language webshell detection.		0
8	Cyber Kill Chain Analysis of Five Major US Data Breaches. **2022**, 12, 1-15		1
7	Threat Actors Tenacity to Disrupt: Examination of Major Cybersecurity Incidents (December 2022). **2022**, 1-1		0
6	Offensive Machine Learning Methods and the Cyber Kill Chain. **2023**, 125-145		0
5	Toward deceiving the intrusion attacks in containerized cloud environment using virtual private cloud-based moving target defense.		0
4	Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement.		0
3	A Framework for Developing Tabletop Cybersecurity Exercises. **2023**, 116-133		0
2	Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach. **2023**, 44-63		0
1	HVA_CPS proposal: a process for hazardous vulnerability analysis in distributed cyber-physical systems. 9, e1249		0