

Automating defences against cyber operations in computer networks = Arvutivõrkude kaitse automatiseerimine küberoperatsioonide vastu

Pihelgas, Mauno 2021 <https://doi.org/10.23658/taltech.36/2021> https://www.ester.ee/record=b5449710*est
<https://digikogu.taltech.ee/et/Item/beb3e841-9c6e-4496-a73a-17148bc941ef>

Bbuzz : a Bit-aware fuzzing framework for network protocol systematic reverse engineering and analysis

Blumbergs, Bernhards; Vaarandi, Risto MILCOM 2017 - 2017 IEEE Military Communications Conference : Baltimore, Maryland, USA, 23-25 October 2017 / p. 707-712 <https://doi.org/10.1109/MILCOM.2017.8170785>

A breadth-first algorithm for mining frequent patterns from event logs

Vaarandi, Risto Intelligence in Communication Systems : IFIP International Conference, INTELLCOMM 2004, Bangkok, Thailand, November 23-26, 2004 : proceedings 2004 / p. 293-308 https://link.springer.com/chapter/10.1007/978-3-540-30179-0_27

Capability detection and evaluation metrics for cyber security lab exercises

Caliskan, Emin; Tatar, Unal; Bahsi, Hayretidin; Ottis, Rain; Vaarandi, Risto Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017 2017 / p. 407-414 : ill <https://www.scopus.com/record/display.uri?eid=2-s2.0-85018944652&origin=inward&txGid=dad813d957372581ca0932bf6e4fb5d8>

Career development in cyber security: Bootcamp training programs

Caliskan, Emin; Vaarandi, Risto Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS) : Old Dominion University (ODU), Norfolk, Virginia, USA, 12-13 March 2020 / p. 503-511 <https://doi.org/10.34190/ICCWS.20.080>

A clustering algorithm for loglife data sets

Vaarandi, Risto Proceedings of the Eighth Symposium on Programming Languages and Software Tools, SPLST'03 : Kuopio, Finland, June 17-18, 2003 / p. 152-162 <https://www.cs.uku.fi/research/publications/reports/A-2003-1/page152.pdf>

Creating and detecting IPv6 transition mechanism-based information exfiltration covert channels

Blumbergs, Bernhards; Pihelgas, Mauno; Kont, Markus; Maennel, Olaf Manuel; Vaarandi, Risto Secure IT Systems : 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016 : proceedings 2016 / p. 85-100 : ill https://doi.org/10.1007/978-3-319-47560-8_6 [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Conference Proceedings at WOS](#) [Article at WOS](#)

Crossed swords : a cyber red team oriented technical exercise

Blumbergs, Bernhards; Ottis, Rain; Vaarandi, Risto Proceedings of the 18th European Conference on Cyber Warfare and Security, University of Coimbra Portugal, 4-5th July 2019 / p. 37-44 <https://www.scopus.com/record/display.uri?eid=2-s2.0-85070019446&origin=inward&txGid=b3ce06db78a90b7b9e8a79c0d7b1f9c7>

A cyber red team oriented technical exercise

Blumbergs, Bernhards; Ottis, Rain; Vaarandi, Risto Abstracts and conference materials for the 18th European Conference on Cyber Warfare and Security, University of Coimbra Portugal, 4-5th July 2019 / p. 10-11 <https://www.academic-conferences.org/conferences/eccws/eccws-future-and-past/>

DACA : automated attack scenarios and dataset generation

Korving, Frank; Vaarandi, Risto Proceedings of the 18th International Conference on Cyber Warfare and Security, ICCWS 2023, a conference hosted by Towson University, Baltimore County, Maryland, USA, 9-10 March 2023 / p. 550-559 : ill <https://papers.academic-conferences.org/index.php/iccws/article/download/962/938> <https://doi.org/10.34190/iccws.18.1.962>

A data clustering algorithm for mining patterns from event logs

Vaarandi, Risto Proceedings of the 3rd IEEE Workshop on IP Operations & Management (IPOM2003) : Kansas City, Missouri, USA, October 1-3, 2003 / p. 119-126 : tab

Efficient event log mining with LogClusterC

Zhuge, Chen; Vaarandi, Risto The Third IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2017 : The Third IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2017 : The Second IEEE International Conference on Intelligent Data and Security, IEEE IDS 2017 : proceedings : 26-28 May 2017, Beijing, China 2017 / p. 261-266 : tab <http://doi.org/10.1109/BigDataSecurity.2017.26>

Event log analysis with the LogCluster tool

Vaarandi, Risto; Kont, Markus; Pihelgas, Mauno 2016 IEEE Military Communications Conference : MILCOM 2016 : Baltimore, MD, USA, November 1-3, 2016 / p. 982-987 <https://doi.org/10.1109/MILCOM.2016.7795458>

Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol

Visky, Gabor; Rohl, Alexander; Vaarandi, Risto; Katsikas, Sokratis; Maennel, Olaf Manuel 2024 IEEE 49th Conference on Local Computer Networks (LCN) 2024 / 7 p <https://doi.org/10.1109/LCN60385.2024.10639746>

How to build a SOC on a budget

Vaarandi, Risto; Mäses, Sten 2022 IEEE International Conference on Cyber Security and Resilience (CSR) 2022 / p. 171-177 : ill
<https://doi.org/10.1109/CSR54599.2022.9850281>

Hybrid cybersecurity research and education environment for maritime sector

Visky, Gabor; Šiganov, Aleksei; Rehman, Muan ur; Vaarandi, Risto; Bahsi, Hayretidin; Tsiopoulos, Leonidas 2024 IEEE International Conference on Cyber Security and Resilience (CSR) : proceedings 2024 / p. 644-651
<https://doi.org/10.1109/CSR61664.2024.10679392>

Improving learning efficiency and evaluation fairness for cyber security courses : a case study

Caliskan, Emin; Vaarandi, Risto; Lorenz, Birgy Intelligent Computing : Proceedings of the 2019 Computing Conference. Volume 2 2019 / p. 622-638 https://doi.org/10.1007/978-3-030-22868-2_45 [Conference proceedings at Scopus](#) [Article at Scopus](#)

Learning from few cyber-attacks : addressing the class imbalance problem in machine learning-based intrusion detection in software-defined networking

Mirsadeghi, Seyed Mohammad Hadi; Bahsi, Hayretidin; Vaarandi, Risto; Inoubli, Wissem IEEE Access 2023 / p. 140428 - 140442 <https://doi.org/10.1109/ACCESS.2023.3341755> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

LogCluster - a data clustering and pattern mining algorithm for event logs

Vaarandi, Risto; Pihelgas, Mauno 11th International Conference on Network and Service Management, CNSM 2015 : Barcelona, Spain, November 9-13, 2015 2015 / p. 1-7

Netflow based framework for identifying anomalous end user nodes

Vaarandi, Risto; Pihelgas, Mauno Proceedings of the 15th International Conference on Cyber Warfare and Security (ICWS) : Old Dominion University (ODU), Norfolk, Virginia, USA, 12-13 March 2020 2020 / p. 448-456 <https://doi.org/10.34190/ICWS.20.035>

Platform independent event correlation tool for network management

Vaarandi, Risto NOMS 2002 : 2002 IEEE/IFIP Network Operations and Management Symposium "Management Solutions for the New Communications World" : proceedings 2002 / p. 907-909 <https://ieeexplore.ieee.org/document/1015640>

Platform independent tool for local event correlation

Vaarandi, Risto SPLST'2001 : Seventh Symposium on Programming Language and Software Tools : Hungary, University of Szeged, June 15-16, 2001 2001 / p. 119-134 <https://cyber.bibl.u-szeged.hu/index.php/actcybern/article/view/3605>

Programmi RITA tegevuse 1 projekti „Masinõppe ja AI toega teenused“ lõpparuanne

Solvak, Mihkel; Vilo, Jaak; Reisberg, Sulev; Tamm, Sirlu; Oja, Marek; Ligi, Kadri; Unt, Taavi; Võrk, Andres; Leets, Peeter; **Tammet, Tanel; Vaarandi, Risto; Nõmm, Sven; Lepik, Toomas; Lember, Veiko; Nõmmik, Steven; Noordt, Colin Pascal van; Kerikmäe, Tanel** 2022 [Programmi RITA tegevuse 1 projekti „Masinõppe ja AI toega teenused“ lõpparuanne](#)

Simple event correlator - best practices for creating scalable configurations

Vaarandi, Risto; Blumbergs, Bernhards; Caliskan, Emin 2015 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision (CogSIMA 2015) : 9-12 March 2015, Orlando, Florida, USA 2015 / p. 96-100
<http://dx.doi.org/10.1109/COGSIMA.2015.7108181>

Specialized cyber red team responsive computer network operations = Vastutegevusele orienteeritud punase meeskonna küberoperatsioonid

Blumbergs, Bernhards 2019 <https://digi.lib.ttu.ee/i/212015>

A stream clustering algorithm for classifying network IDS alerts

Vaarandi, Risto Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), July 26–28, 2021 : Virtual Conference : proceedings 2021 / p. 14-19 <https://doi.org/10.1109/CSR51186.2021.9527926>

Tools and Techniques for event log analysis

Vaarandi, Risto 2005 https://www.ester.ee/record=b2045293*est

Towards an Open-source Intrusion Detection System Integration Into Marine Vehicles

Visky, Gabor; Khisteva, Dariana; Vaarandi, Risto; Maennel, Olaf Manuel 2024 International Symposium ELMAR Proceedings of ELMAR-2024 : 66th International Symposium ELMAR. 16-18 September 2024, Zadar, Croatia 2024 / p. 263-268
<https://doi.org/10.1109/ELMAR62909.2024.10694518>

An unsupervised framework for detecting anomalous messages from syslog log files

Vaarandi, Risto; Blumbergs, Bernhards; Kont, Markus Network operations and management symposium : cognitive mangement in a cyber world, 23-27 april 2018, Taipei, Taiwan 2018 / 6 p <http://doi.org/10.1109/NOMS.2018.8406283>

Vabavaraalised lahendused infosüsteemide monitooringuks

Vaarandi, Risto A & A 2004 / 4/5, lk. 110-116

