

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>

Comparative analysis of pattern mining algorithms for event logs

Gasimov, Orkhan; **Vaarandi, Risto; Pihelgas, Mauno** 2023 IEEE International Conference on Cyber Security and Resilience (CSR) : Venice, Italy, 2023 2023 / 7 p <https://doi.org/10.1109/CSR57506.2023.10224996>

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](#)

Data quality problem in AI-based network intrusion detection systems studies and a solution proposal

Halisdemir, Emre; Karacan, Hacer; **Pihelgas, Mauno; Lepik, Toomas**; Cho, Sungbaek 14th International Conference on Cyber Conflict : Keep Moving 2022 / p. 367-383 https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf

Design and implementation of an availability scoring system for cyber defence exercises

Pihelgas, Mauno 14th International Conference on Cyber Warfare and Security (ICWS 2019) : Stellenbosch University, South Africa, 28 February - 1 March 2019 : Proceedings 2019 / p. 329-337 <http://toc.proceedings.com/48113webtoc.pdf> ["ICWS 2019"](#)

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 2016 / p. 982-987 <https://doi.org/10.1109/MILCOM.2016.7795458>

Frankenstack : real-time cyberattack detection and feedback system for technical cyber exercises

Pihelgas, Mauno; Kont, Markus Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), July 26–28, 2021 : Virtual Conference : proceedings 2021 / p. 396-402 <https://doi.org/10.1109/CSR51186.2021.9527923>

Frankenstack : toward real-time red team feedback

Kont, Markus; Pihelgas, Mauno; Maennel, Kaie; Blumbergs, Bernhards; **Lepik, Toomas** MILCOM 2017 - 2017 IEEE Military Communications Conference : Baltimore, Maryland, USA, 23-25 October 2017 2017 / p. 400-405 : ill <https://doi.org/10.1109/MILCOM.2017.8170852> [Journal metrics at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

Insider threat detection study [Online resource]

Kont, Markus; Pihelgas, Mauno; Wojtkowiak, Jesse; Trinberg, Lorena; **Osula, Anna-Maria** 2015 https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

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

LSPR23: A novel IDS dataset from the largest live-fire cybersecurity exercise

Dijk, Allard; Halisdemir, Emre; Melella, Cosimo; Schu, Alari; **Pihelgas, Mauno**; Meier, Roland Journal of Information Security and Applications 2024 / art. 103847, 14, p. : ill <https://doi.org/10.1016/j.jisa.2024.103847> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

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>

Service measurement map for large-scale cyber defense exercises

Pihelgas, Mauno; Rubio Melon, Francisco Jesus; **Priisalu, Jaan** Cyber Defence Situation Awareness : STO-MP-IST-148 2016 / p. 9-1 - 9-10 : ill <http://dx.doi.org/10.14339/STO-MP-IST-148>