Praktiskā pieredze ieviešot IT drošības operāciju centru (SOC)

Vladislavs Minkevičs

vladislavs.minkevics@rtu.lv

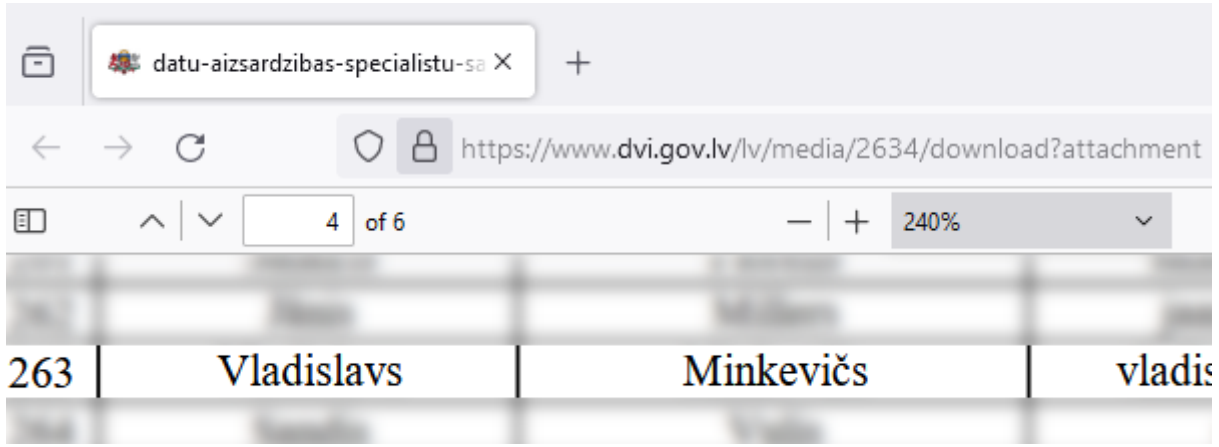
12.12.2023

Īsi par mani

CISA Certified Information Systems Auditor
An ISACA® Certification

MORE THAN 20 YEARS EXPERIENCE

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®



Ceļojums uz SOC sākās ar Suricata IDS un komūnas signatūrām…

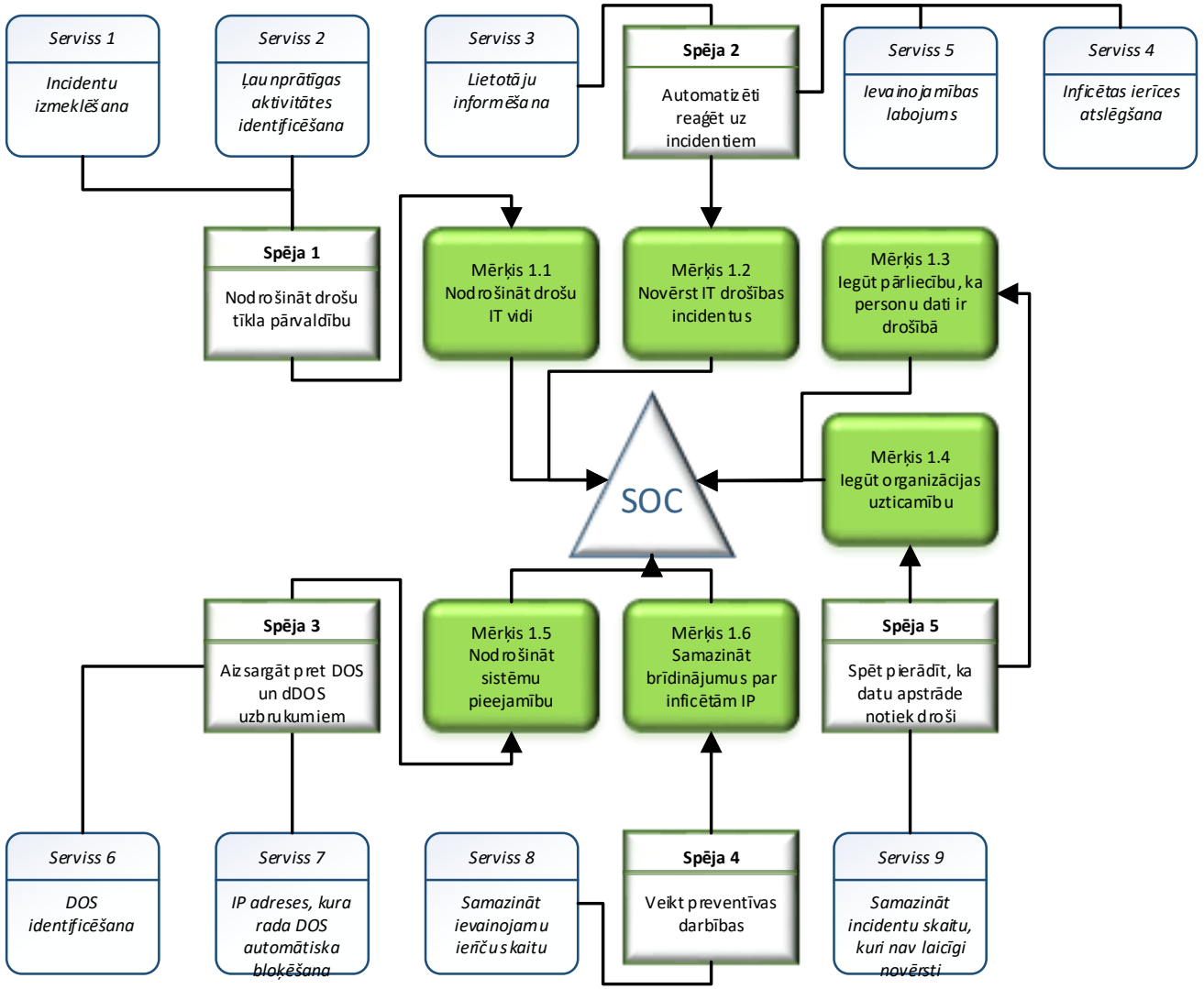
Avots: duckduckgo.com meklētājs

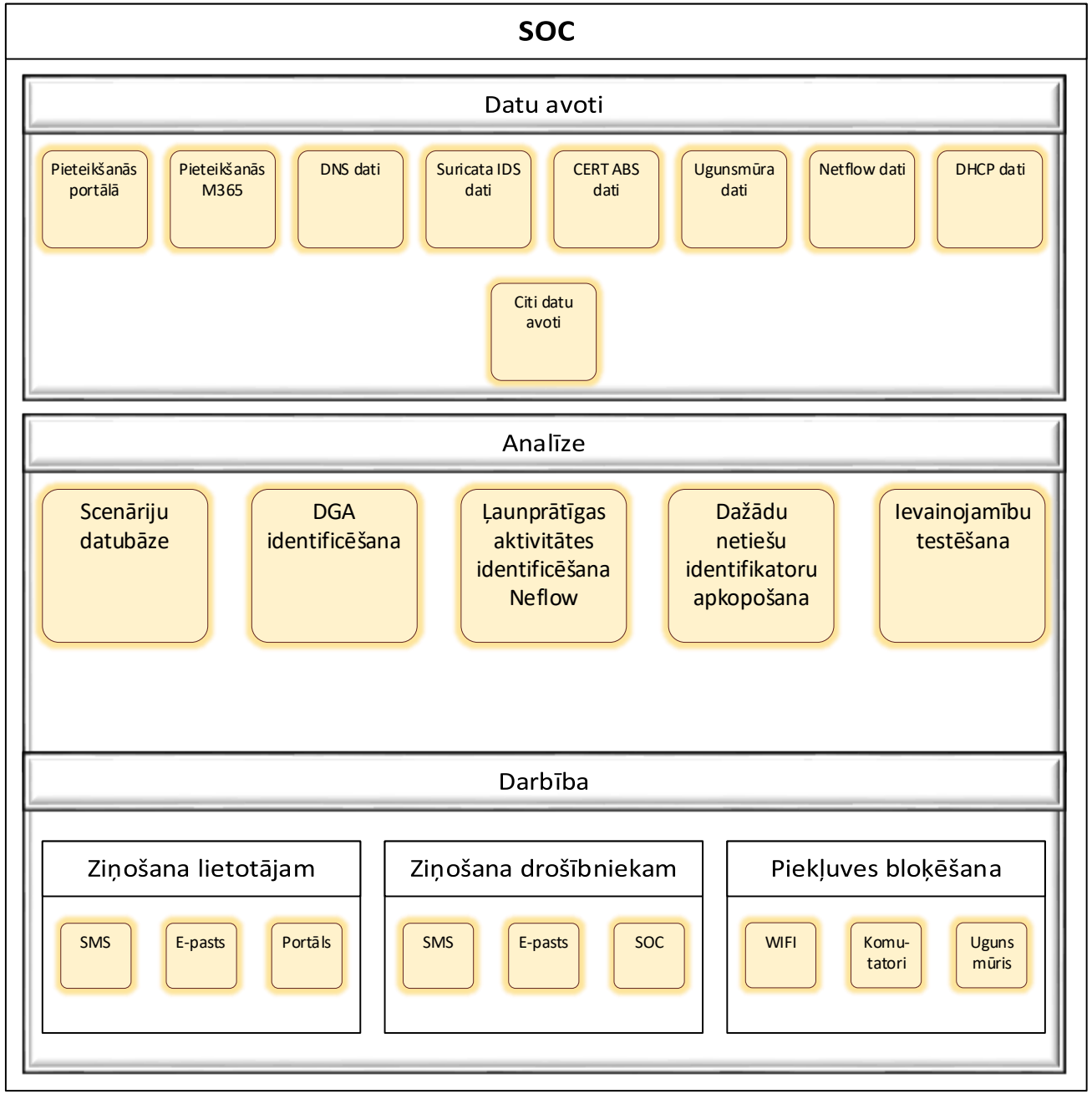
SURICATA®

Nākamie soļi...

- No tīkla datiem eksportējām Netflow izmantojot frobe un nfdump
- No tīkla datiem eksportējām DNS pieprasījumus izmantojot Python un tcpdump
- Izstrādājām dažādus Python skriptus, lai identificētu skanēšanu no iekšējā tīkla un paroles minēšanu
- Uzstādījām Apache Kafka platformu, uz kuru tika nosūtīti auditācijas pieraksti no dažādiem avotiem, piemēram autentifikācijas dati u.c
- Izveidojām galveno apstrādes moduli, kurš saņem informāciju no Apache Kafka un apstrādā to, ņemot vērā izveidotos scenārijus, kā arī pieņem lēmumu par automatizētu reakciju uz identificēto draudu
- Papildinājām SOC ar jauniem datu avotu moduļiem
- Papildinājām SOC ar papildu datu apstrādes moduļiem, piemēram DGA identificēšana u.c.

Spējā pieeja




SOC
Datu avoti
Pieteikšanās portālā
Pieteikšanās M365
DNS dati
Suricata IDS dati
CERT ABS dati
Ugunsmūra dati
Netflow dati
DHCP dati
Citi datu avoti
Analīze
Scenāriju datubāze
DGA identificēšana
Ļaunprātīgas aktivitātes identificēšana Neflow
Dažādu netiešu identifikatoru apkopošana
Ievainojamību testēšana
Darbība
Ziņošana lietotājam
SMS
E-pasts
Portāls
Ziņošana drošībniekam
SMS
E-pasts
SOC
Piekļuves bloķēšana
WIFI
Komu-tatori
Uguns mūris

Vienas inficētas ierīces portrets

33 ML_DNS:mhdprkwje.com

32 ML_DNS:iyqvcmhodrwy.com

16 ML_DNS:hlrfqtcftlphic.com

15 ML_DNS:smtpbprnro.com

6 Mn-355482, Warzone RAT (AveMaria) in RAR (.z) email attachment [DST-IP: 62.102.148.158]

2 DGA:smtpbprnro.com

2 DGA:mhdprkwje.com

2 DGA:iyqvcmhodrwy.com

1 ML_DNS:smtpbprnro.com

1 Non-RFC Compliant LDAP Traffic on Port 389

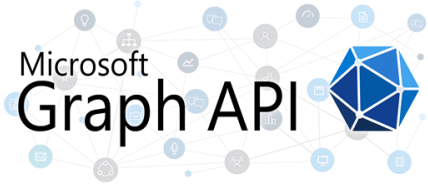
1 Mb-391021, AA23-250A: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475 [DST-IP: 154.6.93.5]

1 Mn-276203, Cyber attack on the Ukrinform information and communication system (CERT-UA#5850) [DST-IP: 194.28.172.81]

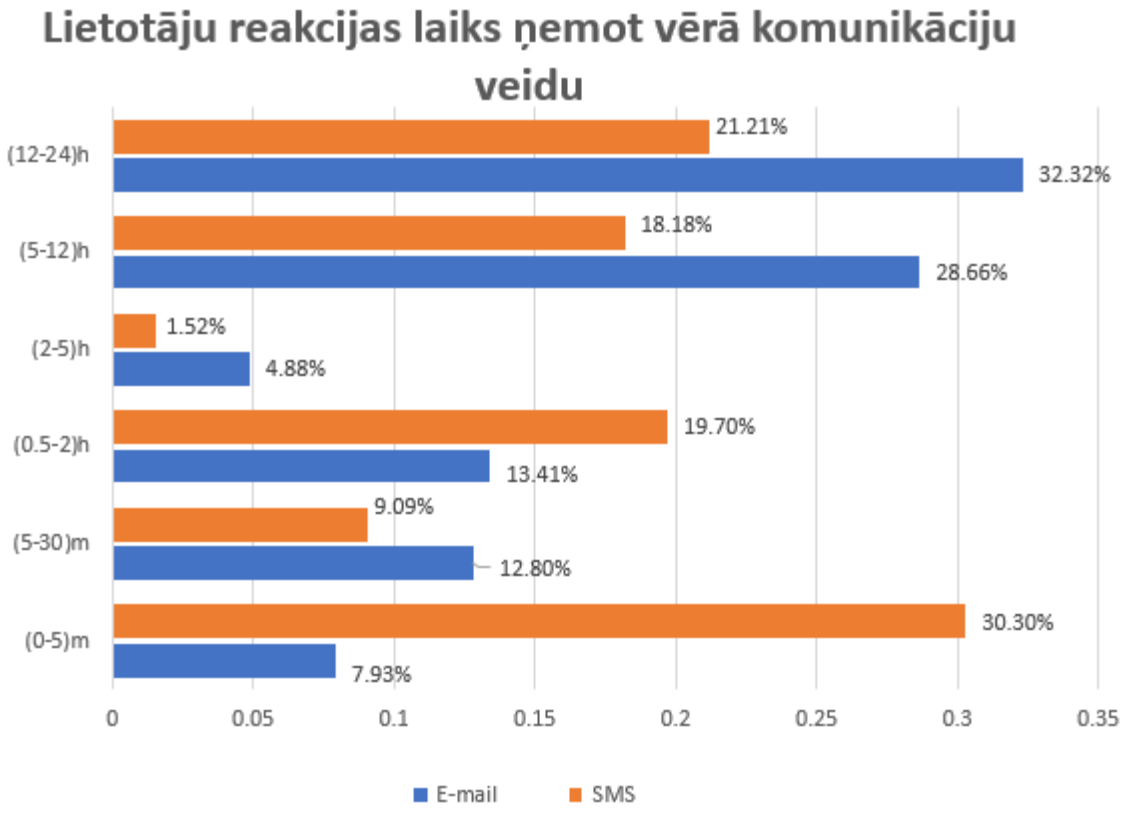
1 ML_DNS:iyqvcmhodrwy.com

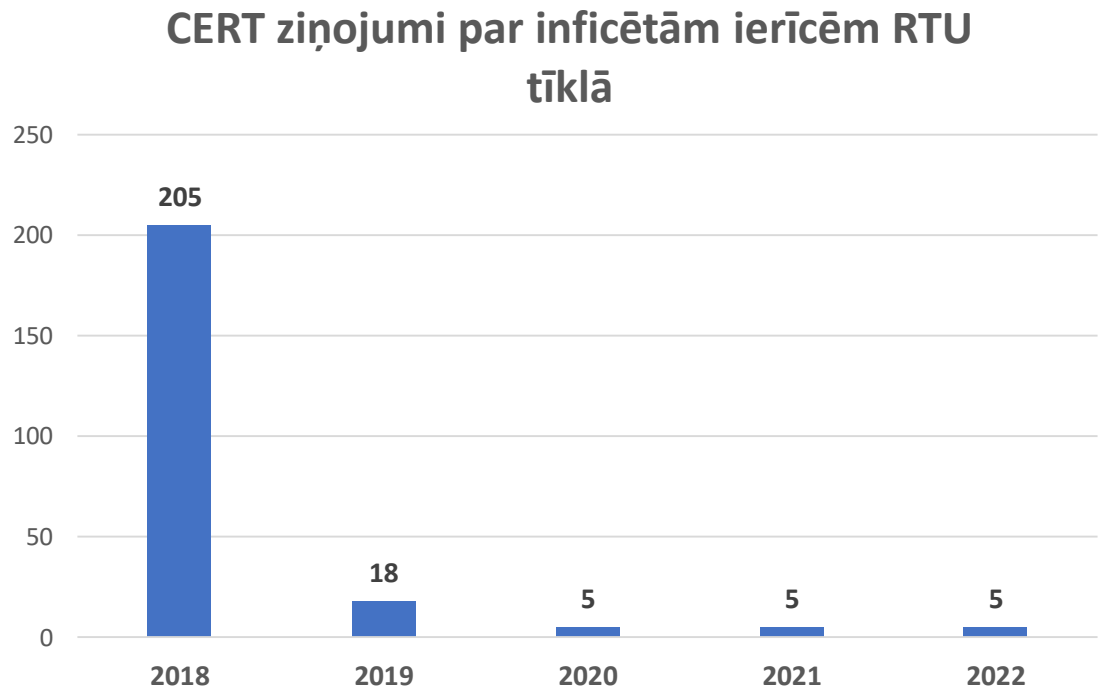
1 DGA:hlrfqtcftlphic.com

Galvenās izmantotās tehnoloģijas būvējot SOC



Statistika


Lietotāju reakcijas laiks ņemot vērā komunikāciju veidu
(12-24)h
(5-12)h
(2-5)h
(0.5-2)h
(5-30)m
(0-5)m
21.21%
32.32%
18.18%
28.66%
1.52%
4.88%
19.70%
13.41%
9.09%
12.80%
30.30%
7.93%
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
E-mail
SMS

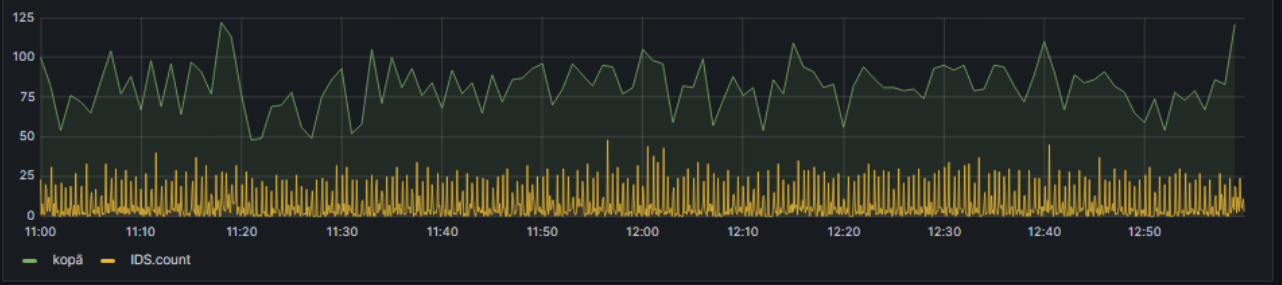

CERT ziņojumi par inficētām ierīcēm RTU tīklā
250
200
150
100
50
0
205
18
5
5
5
2018
2019
2020
2021
2022

Search or jump to... ctrl+k

Home › Dashboards › IDS panelis_new

Add

Kopaina



Unikālas MAC

524

Kritiskums

IDS.priority	kopā ↓
informational	[redacted]
low	[redacted]
4	[redacted]
1	[redacted]
medium	[redacted]
3	[redacted]

Biežāk redzētie Alerti

IDS.threat	Redzē
Microsoft Windows NTLMSSP Det...	[redacted]
Suspicious obfuscated PowerShell c...	[redacted]
ETPRO POLICY Tiktok DNS Lookup	[redacted]
ET INFO Leveraging Agent P2P Comm...	[redacted]
RMRig Miner Command and Contr...	[redacted]
ET INFO ZeroTier Related Activity...	[redacted]
ETPRO POLICY Tiktok DNS Lookup	[redacted]
generic TROJWasset.cy	[redacted]

Biežāk redzētās MAC adreses

IDS.s_mac	IDS.hostname	Redzēt
[redacted]	[redacted]	[redacted]

Biežāk redzētās IP adreses

IDS.src	Redzēt
[redacted]	[redacted]

Īpašie dati

src	Threat	IDS.priority	MAC	hostname	Redzēt	Lietotāj
[redacted]						

Dati

Time ↓	IDS.src	IDS	IDS.dst	IDS.dp	IDS.threat	IDS	IDS.mac_time	IDS.s_mac	IDS.hostname	IDS.user_id	IDS.payload
[redacted]											

Secinājumi

1) Mūsdienu apstākļos nepieciešams maksimāli automatizēt SOC, tāpēc uz scenārijiem bāzēta pieeja ir viens no risinājumiem
2) Jo labāk uzrakstīti scenāriji, jo vairāk par drošību atbildīgās personas var pievērsties svarīgākiem uzdevumiem
3) Šāds adaptējams un modulārs SOC var tikt papildināts ar papildu moduļiem, neietekmējot pārējās sistēmas darbu
4) SOC ir būvēts izmantojot atvērtā koda risinājumus, tāpēc to var uzbūvēt jebkura organizācija ar pietiekami entuziastiskiem IT cilvēkiem ☺

Publikācijas

- Minkevičs V., Kampars J. IS Security Governance Capability Design for Higher Education Organization. No: 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS 2018): Proceedings, Latvija, Rīga, 29.-29. novembris, 2018. Piscataway: IEEE, 2018, 66.-70.lpp. ISBN 978-1-7281-0099-9. e-ISBN 978-1-7281-0098-2. Pieejams: doi:10.1109/ITMS.2018.8552975
- Minkevičs V., Kampars J. Methods, models and techniques to improve information system's security in large organizations: included in registration In Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 1 2020: ICEIS, 632-639, 2020, ISBN: 978-989-758-423-7
- Minkevičs V., Kampars J., Artificial intelligence and big data driven IS security management solution with applications in higher education organizations, 17th International Conference on Network and Service Management, 2021, Izmir, Turkey doi:10.23919/CNSM52442.2021.9615575
- Minkevičs V., Kampars J., Grabis J., Managing Information System Security in Higher Education Organizations, IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) 2023.gada 27-29 aprīlis, Viļņa, Lietuva. doi: 10.1109/AIEEE58915.2023.10134911

Paldies par uzmanību

vladislavs.minkevics@rtu.lv