

# Praktiskā pieredze ieviešot IT drošības operāciju centru (SOC)

Vladislavs Minkevičs  
vladislavs.minkevics@rtu.lv

12.12.2023

# Īsi par mani



datu-aizsardzibas-specialistu-sa X +  
https://www.dvi.gov.lv/lv/media/2634/download?attachment  
4 of 6 240%  
263 | Vladislavs | Minkevičs | vladis

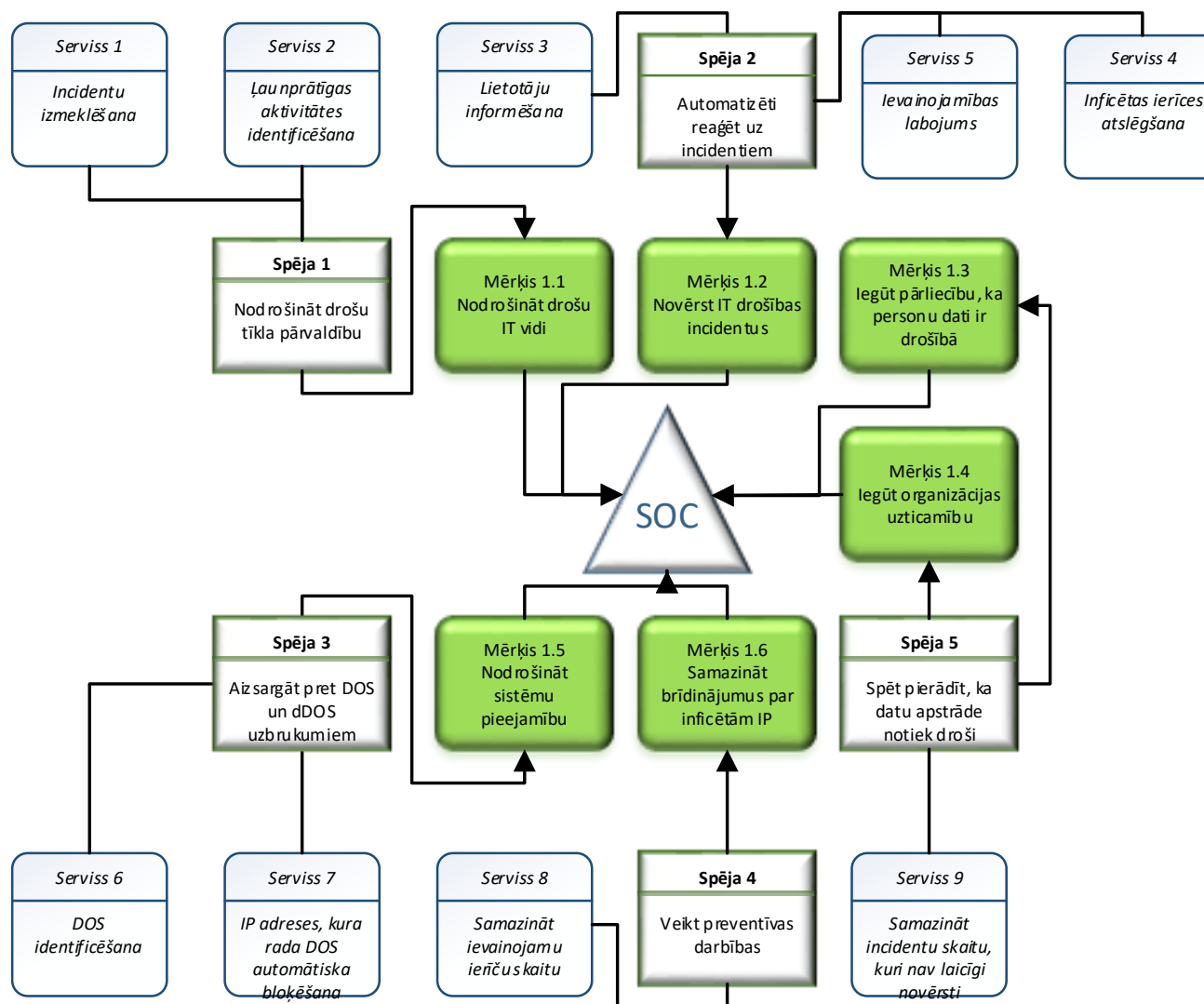
# Ceļojums uz SOC sākās ar Suricata IDS un komūnas signatūrām...



# Nākamie soļi...

- No tīkla datiem eksportējām Netflow izmantojot fprobe 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

Uguns mūra  
dati

Netflow dati

DHCP dati

Citi datu  
avoti

## Analīze

Scenāriju  
datubāze

DGA  
identificēšana

Ļaunprātīgas  
aktivitātes  
identificēšana  
Netflow

Dažādu  
netiešu  
identifikatoru  
apkopošana

Ievainojamību  
testēšana

## Darbība

### Ziņošana lietotājam

SMS

E-pasts

Portāls

### Ziņošana drošībasniekam

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:hlfqtcftlphic.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

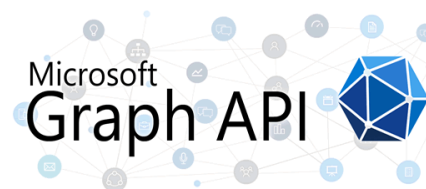
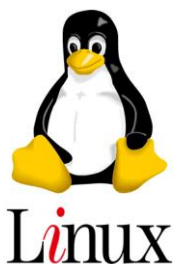
1 Mb-391021, AA23-250A: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475 [DST-IP: 154.6.93.5]

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:hlfqtcftlphic.com

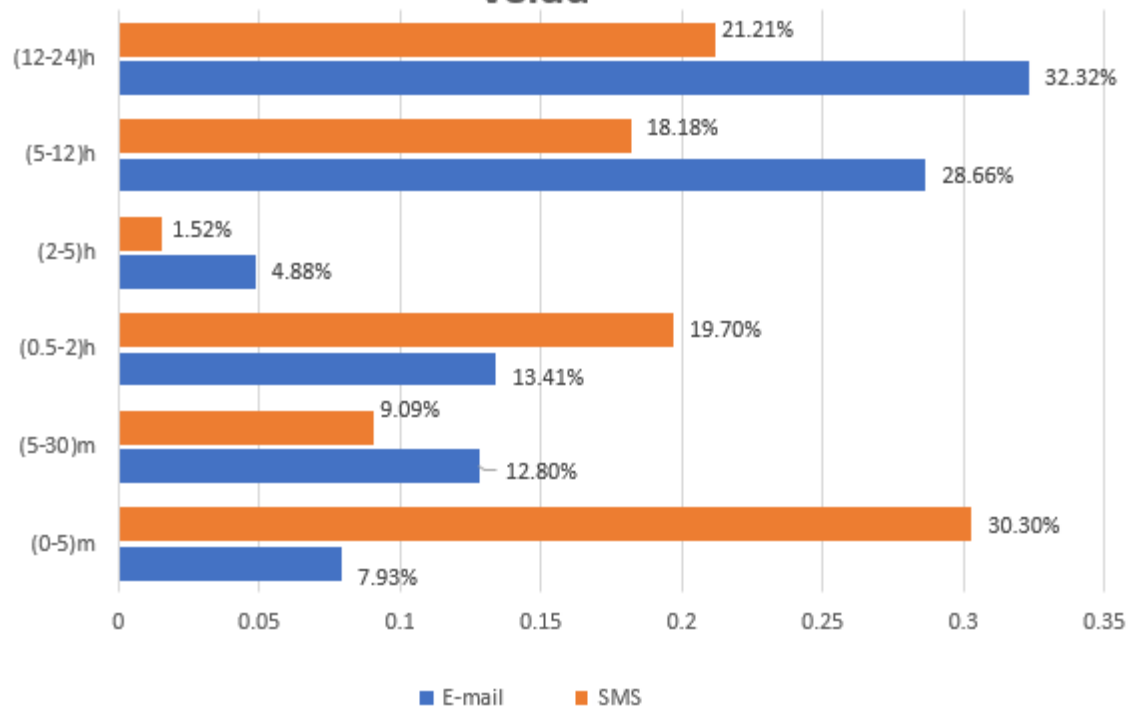
# Galvenās izmantotās tehnoloģijas būvējot SOC



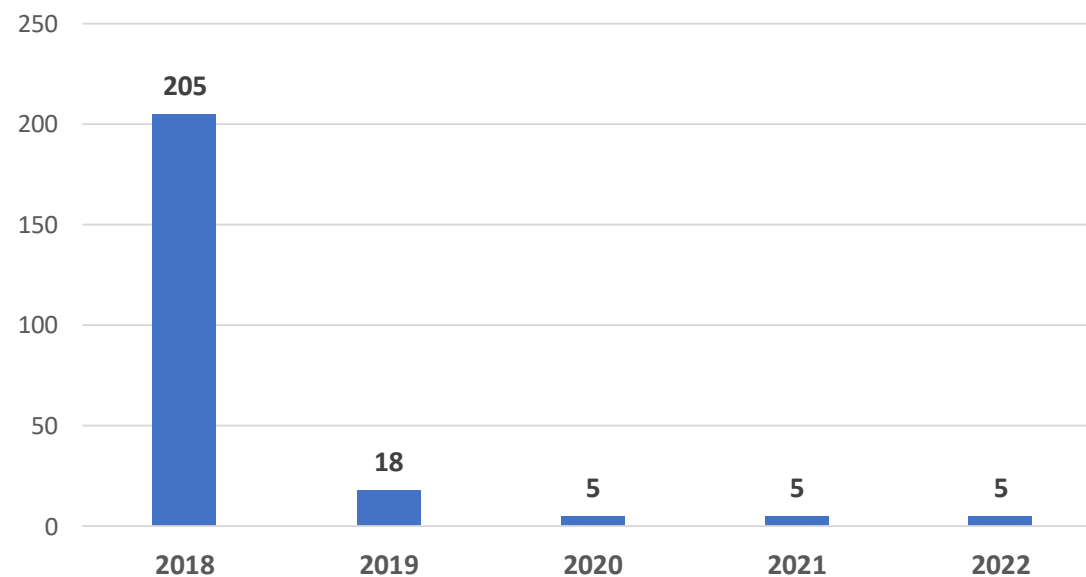


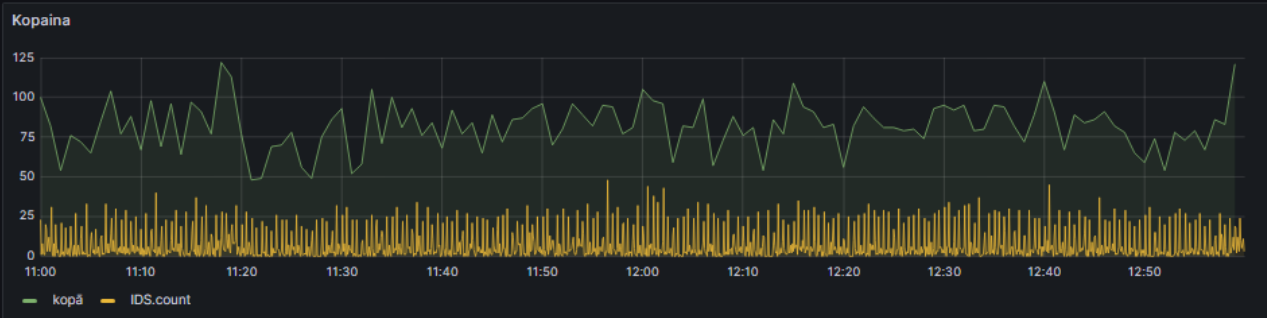
# Statistika

## Lietotāju reakcijas laiks ņemot vērā komunikāciju veidu



## CERT ziņojumi par inficētām ierīcēm RTU tīklā





Unikālas MAC **524**

Kritiskums

IDS.priority **kopā ↓**

Informational	2207
low	1707
4	1340
1	1283
medium	727
3	581

Biezāk redzētās MAC adreses Biezāk redzētās IP adreses

IDS.s_mac	IDS.hostname	Redzēt	IDS.src	Redzēt
94.05.80.80-FE.53	DESKTOP-HATH6Q	480	213.175.95.190	100
90.F0.80.80-83.68	DESKTOP-2THPUS	480	213.175.95.226	200
98.F4.08.53-52.7C	LAPTOP-BKAK6LJH	480	78.154.136.52	244
04.50.84.43-8F.3A	DESKTOP-G2PMACA	476	78.154.137.81	240
24.5E.8E.68-21.28	Darvnc	390	78.154.130.129	240
08.00.84.88-08.88	DESKTOP-D4W33H	370	78.154.142.71	214
90.03.34.01-38.63	LAPTOP-AC76L3R	338	78.154.130.230	207
90.00.57.70-64.9C	WIFI-84CM	306	213.175.95.207	196
70.FE.00.81-27.88	TL-WR841N	276	78.152.0.148	196
40.79.80.84-03.58	DESKTOP-TY8AAA	276	213.175.95.208	193
08.97.88.03-52.80	LAPTOP-COLU88P	238	78.154.136.180	186
84.2E.08.03-54.FE	Darvnc	216	78.154.142.12	172
84.2A.F0-C9-01.75	BTU20-P098	210	78.2.84.186	168
78.00.40.80-F8.48	DESKTOP-0877P5	192	78.154.135.176	162
78.01.71.48-01.88	TL-WR740N	120	78.154.135.84	128
08.9F-C3-89-42.88	Ana	120	213.175.95.208	128
88.0A.34.88-07.80	DESKTOP-D4W33H	78	78.2.85.1	128
78.154.136.178	Ana	78	78.154.136.178	78

Biezāk redzētie Alerti

IDS.threat **Redzē ↓**

Microsoft Windows NTLMSSP Dat...	2700
Dropware/stealthinventoryphisher.c...	1987
ETPRO POLICY Tweak DNS Lookup	372
ET-RFD Levelix Agent POP Conn...	277
WiFiNg Mitr Command and Contr...	240
ET-RFD ZeroTier Related Activity...	178
ETPRO POLICY Tweak DNS Looku...	172
generic/MS2Blasent.c...	137

Īpašie dati

src	Threat	IDS.priority	MAC	hostname	Redzēt	Lietotāj
213.175.95.207	ML_DNS.globeuniversity.org + tcp0	1			4	
78.154.136.232	ML_DNS.analytics.200824.com + tcp0	1	78.FE.00.04-04.81	TL-WR740N	4	
78.2.84.226	DNS.globeuniversity.com	high	90.78.4F.40-41.27	Darvnc@pikem	4	naraku
78.2.84.226	DNS.globeuniversity.com	high	90.78.4F.40-41.27	Darvnc@pikem	3	naraku
78.154.136.180	ML_DNS.brownscheckfraud.com + tcp0	1	74.0C.30-8F-C8.08	TL-WR841N	3	
213.175.95.186	ML_DNS.www.vonmuthbooks.de + tcp0	1			3	
213.175.95.207	ML_DNS.buchhandel.de + tcp0	1			3	
78.152.30.18	ML_DNS.suspension.durchschlag.org + tcp0	1	40.02.82-48-07.84	BTU20-078021	3	
85.254.220.47	Arachnoid2 Command and Control Traffic Detect...	critical	98.80.48-0F-7A.08	LAPTOP-07F4Q28	3	anadu
213.175.95.208	ML_DNS.www.globejournal.com + tcp0	1			3	

Dati

Time	IDS.src	IDS	IDS.dst	IDS.dpi	IDS.threat	IDS	IDS.mac_time	IDS.s_mac	IDS.hostname	IDS.user_id	IDS.payload
2023-12-08 12:58...	85.254.217.2	123	82.193.95.122	37786	ML_296784_Signatures 07828_L0111 2017-IP-82.193.95.122	4					
2023-12-08 12:58...	78.2.85.81	48762	148.112.112.112	53	ET-MALWARE Observed DNS Query to PUP Domain (malware.com)	1	Dec 8 12:58:44	98.21.58-CA-84.7F	W703K18PQ		
2023-12-08 12:58...	85.254.217.2	123	46.109.204.180	32923	ML_296784_Signatures 07828_L0111 2017-IP-46.109.204.180	4					
2023-12-08 12:58...	213.175.95.208	1234	78.154.142.271	53	ML_DNS www.vonmuthbooks.com + tcp0	1					
2023-12-08 12:58...	78.154.136.96	348...	82.223.24.181	5222	DPI_Chat_Joiner/Google Talk Outgoing Message	1	Dec 8 11:48:02	04.04-CA-00-48.25	DESKTOP-CN27CAJ		

# 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