squalio
cloud consulting

Žurnālfaili - prakse, padomi un ieteikumi

Didzis Balodis, CISSP, CISA
Infrastruktūras un drošības risinājumu nodaļas vadītājs

2017. gada oktobrī

SATURS...

01
Kāpēc?

02
Teorija

- Izaicinājumi
- Grūtības

03
Prakse un ieteikumi

- Piemēri
- Praktiskie aspekti
- Secinājumi

SIA «SQUALIO cloud consulting»

- Viens no Latvijas vadošajiem IT uzņēmumiem;
- Saknes 1997. gadā.

Meklē mūs

squaliocc.com
blogs.squalio.com
facebook.com/SQUALIOcloudconsulting/
linkedin.com/organization/15212970/

DARBĪBAS VIRZIENI

Programmatūru izstrāde

Risinājumu ieviešana

IT drošība un audits

Dalība ES projektos

KĀDĒĻ?

- Ārējas prasības (MK 442, FKTK, ISO 27001/2 u.c.)
- Notikumu izmeklēšana
- Preventīva analīze

Software | Vulnerability Information | Reputation Center | Library | TALOS | Support Commu

MONDAY, SEPTEMBER 18, 2017

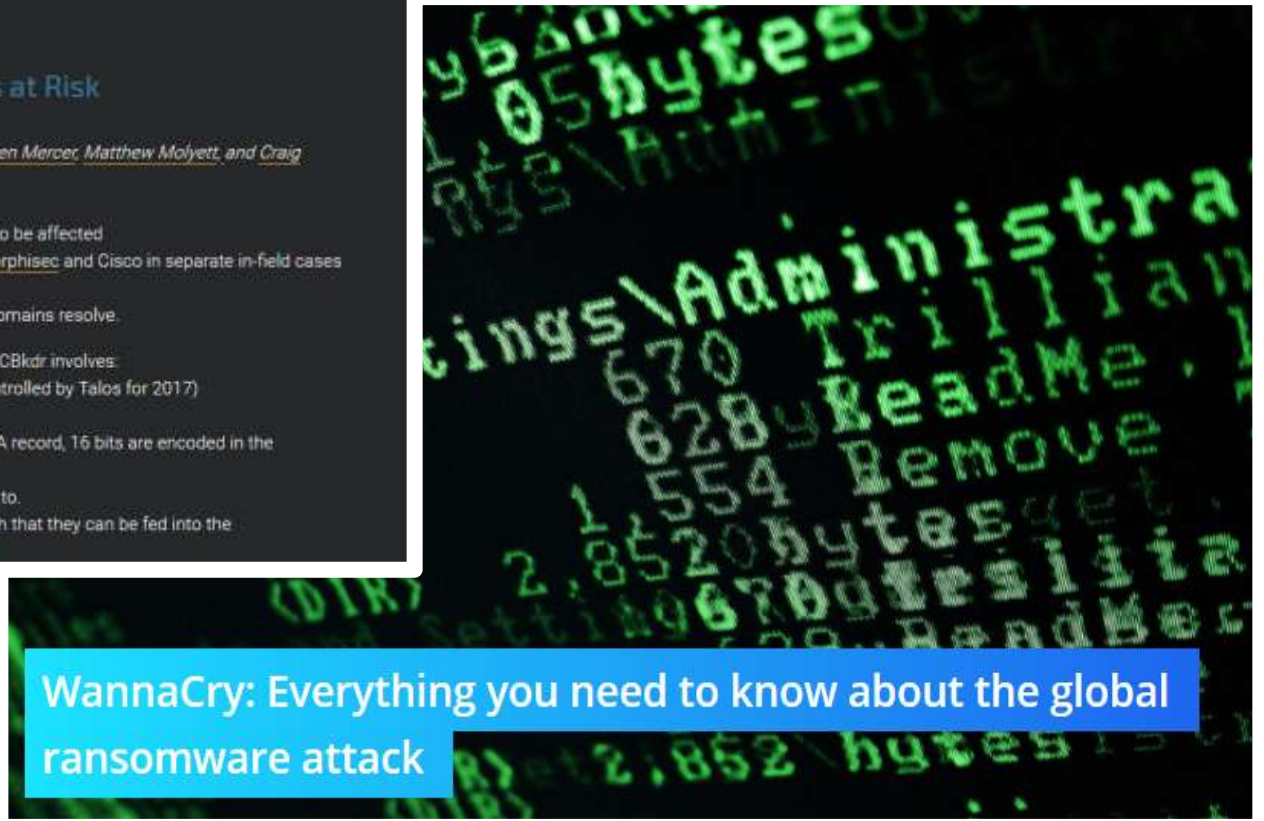
CCleanup: A Vast Number of Machines at Risk

This post was authored by: Edmund Brumaghin, Ross Gibb, Warren Mercer, Matthew Molyett, and Craig Williams

Update 9/18: CCleaner Cloud version 1.07.3191 is also reported to be affected
Update 9/19: This issue was discovered and reported by both Morphisec and Cisco in separate in-field cases and reported separately to Avast.
Update 9/19: There has been some confusion on how the DGA domains resolve.

The fallback command and control scheme in use by the CCBkdr involves:
1. Generating a Monthly Domain name (all of which are controlled by Talos for 2017)
2. Request the A records for the domain.
3. 16 bits of the true destination IP are encoded in the first A record, 16 bits are encoded in the second A record
4. The true destination IP is then computed and connected to.

To control the connections Talos has to create two IPs such that they can be fed into the application to resolve to the sinkhole IP.



WannaCry: Everything you need to know about the global ransomware attack

Admini…

Photo by Tim Gouw on Unsplash

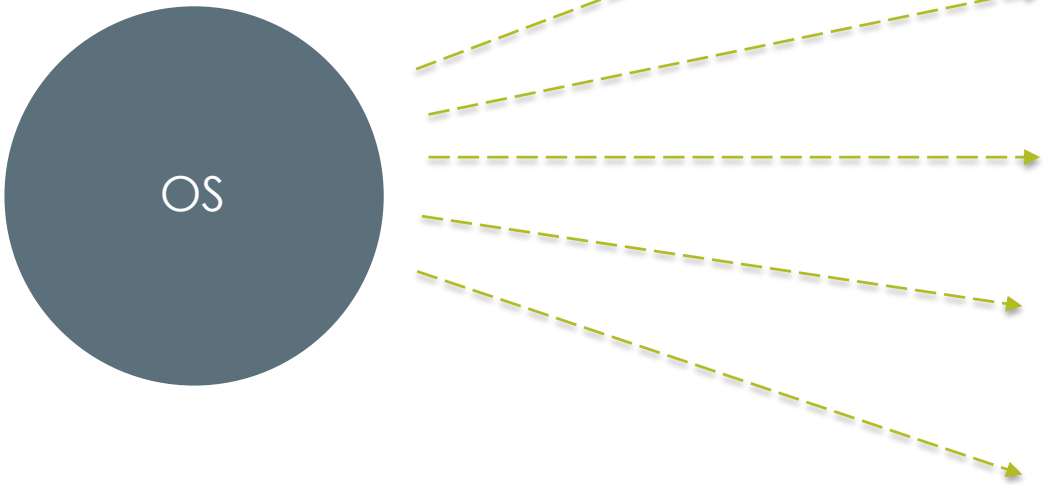
Lietotāji…

Photo

«Ārējie spēki»

Photo by Miriam Espacio on Unsplash

KO AUDITĒT?



Logon/ logoff

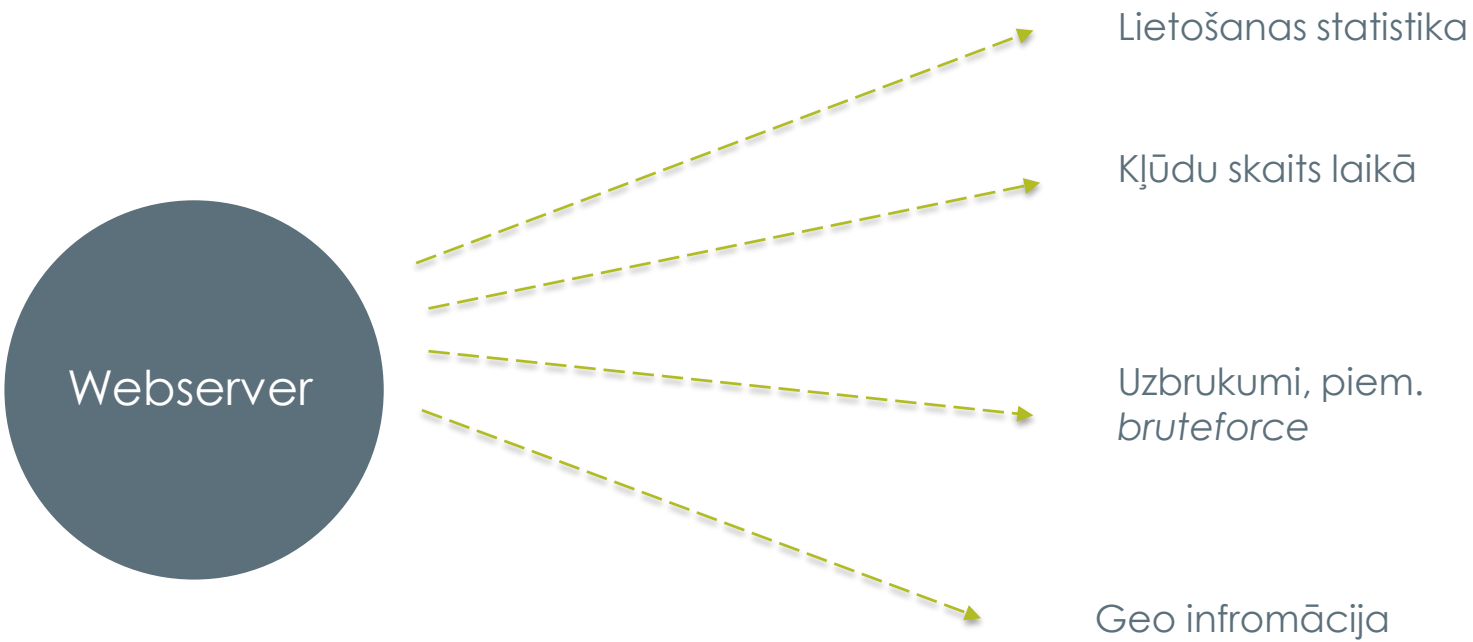
Administratīvās darbības ar kontiem un grupām

Paroļu nomaiņas

Sekmīgi/ nesekmīgi piekļuves mēģinājumi

Failu sistēmas monitorings u.c.

KO AUDITĒT?


Webserver
Lietošanas statistika
Kļūdu skaits laikā
Uzbrukumi, piem. *bruteforce*
Geo infromācija

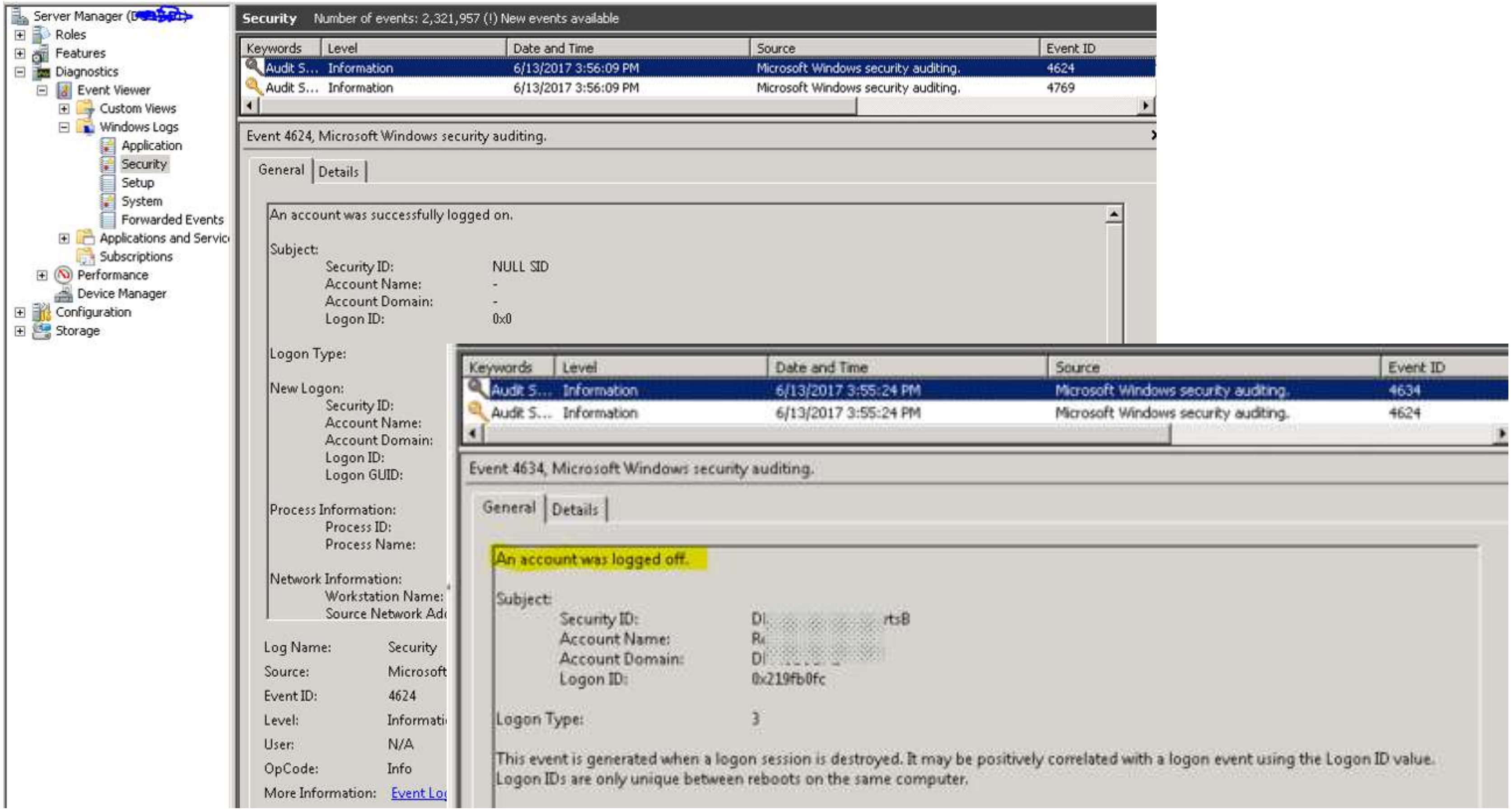
WINDOWS AD AUDITĀCIJA | IZAICINĀJUMI

Vairāki AD domēna kontrolieri

Milzīgs auditācijas ierakstu skaits

Noklusētie iestatījumi nav pietiekami

PIEMĒRI



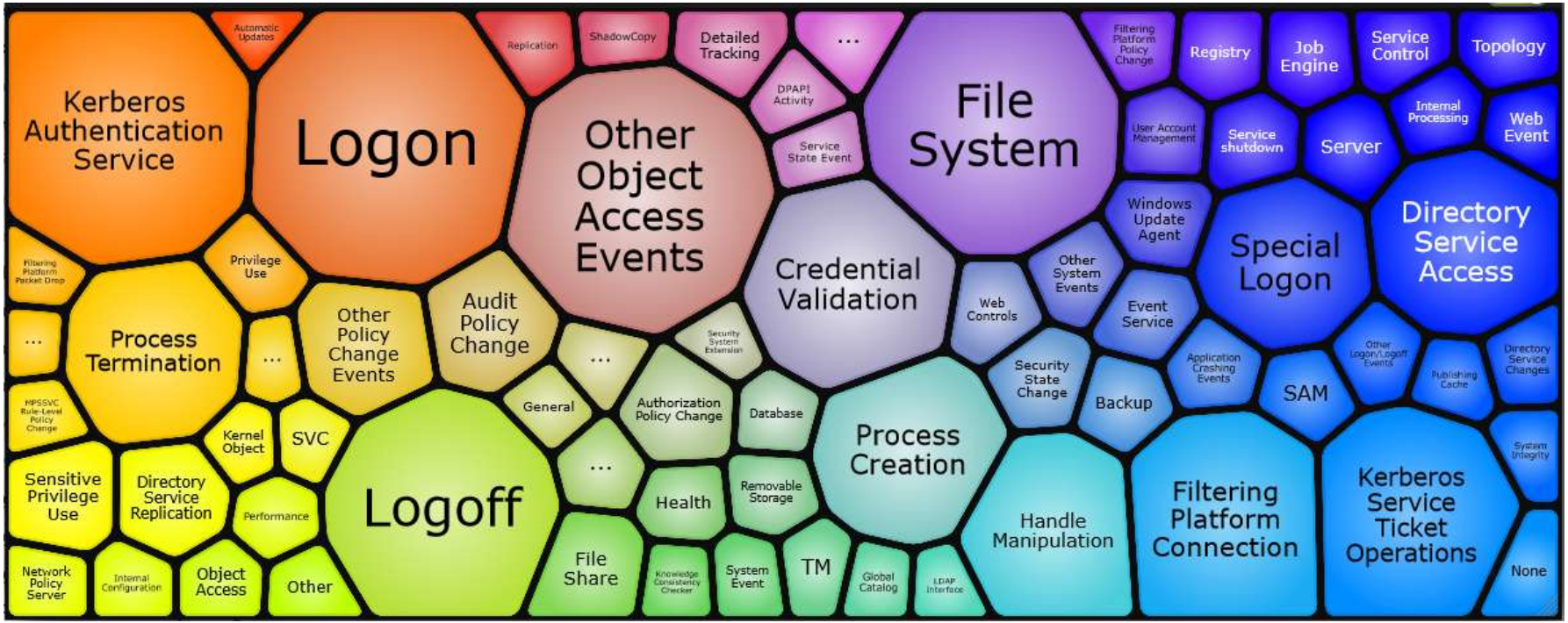
Server Manager ([redacted])
Roles
Features
Diagnostics
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Servic
Subscriptions
Performance
Device Manager
Configuration
Storage
Security Number of events: 2,321,957 (!) New events available
Keywords | Level | Date and Time | Source | Event ID
Audit S... Information 6/13/2017 3:56:09 PM Microsoft Windows security auditing. 4624
Audit S... Information 6/13/2017 3:56:09 PM Microsoft Windows security auditing. 4769
Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type:
New Logon:
Security ID:
Account Name:
Account Domain:
Logon ID:
Logon GUID:
Process Information:
Process ID:
Process Name:
Network Information:
Workstation Name:
Source Network Ad
Log Name: Security
Source: Microsoft
Event ID: 4624
Level: Informati
User: N/A
OpCode: Info
More Information: Event Lo
Keywords | Level | Date and Time | Source | Event ID
Audit S... Information 6/13/2017 3:55:24 PM Microsoft Windows security auditing. 4634
Audit S... Information 6/13/2017 3:55:24 PM Microsoft Windows security auditing. 4624
Event 4634, Microsoft Windows security auditing.
General
Details
An account was logged off.
Subject:
Security ID: [redacted]
Account Name: [redacted]
Account Domain: [redacted]
Logon ID: 0x219fb0fc
Logon Type: 3
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

WINDOWS EVENT LOGIKA

Windows event category	# of subcategories	# of event IDs
Account Logon	3	9
Account Management	6	58
Detailed Tracking	4	8
DS Access	4	16
Logon/Logoff	9	48
Object Access	12	77
Policy Change	7	95
Privilege Use	1	3
System	5	53
Total:	**51**	**367**

Subcategories	# of event IDs
Application Group Management	8
Computer Account Management	2
Distribution Group Management	14
Other Account Management Events	2
Security Group Management	16
User Account Management	16

STATISTIKA – 9 SERVERI, 24 H



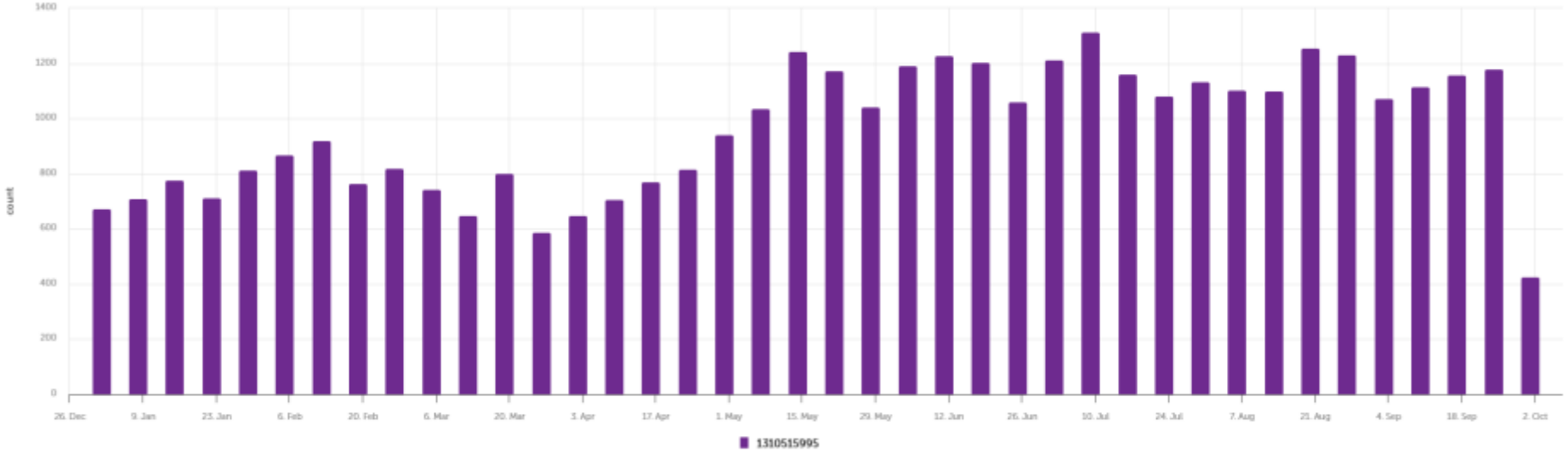
1 780 000 auditācijas ierakstu =1 minūtē – 1236, sekundē 20.

PRAKTISKIE PIEMĒRI

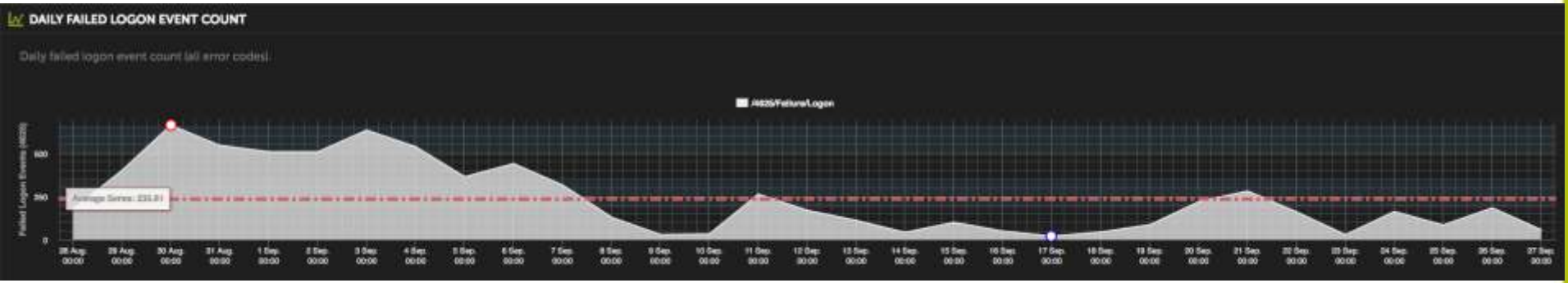
JAUTĀJUMI

- Vai man jāuztraucas par WannaCry un CCcleaner ievainojamību?
- Kāda ir neveiksmīgo ielogošanās mēģinājumu statistika?
- Kādi jauni AD konti un grupas tiek izveidoti vai dzēsti?
- Kādi ir biežākie login failed iemesli?
- Vai pastāv ”aizdomīgi” savienojumi no/uz iekštīklu/ārtīklu?

WannaCry ietekme

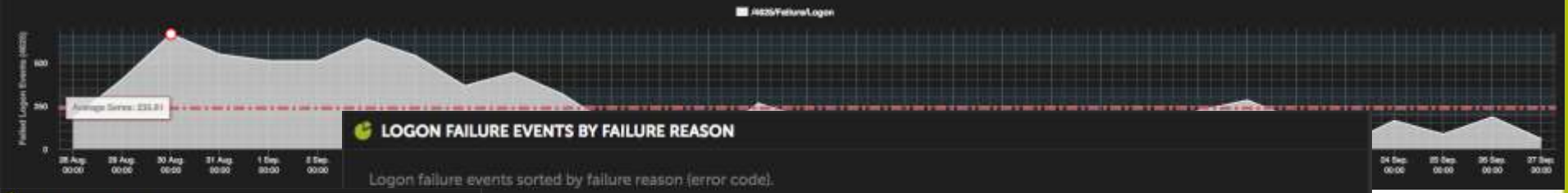


Count of dropped packets on 1 dstIP, dst port 445, per week


DAILY FAILED LOGON EVENT COUNT
Daily failed logon event count (all error codes)
/4625/FailureLogon
Failed Logon Events (4625)
600
300
0
Average Series: 233.81
28 Aug 00:00
29 Aug 00:00
30 Aug 00:00
31 Aug 00:00
1 Sep 00:00
2 Sep 00:00
3 Sep 00:00
4 Sep 00:00
5 Sep 00:00
6 Sep 00:00
7 Sep 00:00
8 Sep 00:00
9 Sep 00:00
10 Sep 00:00
11 Sep 00:00
12 Sep 00:00
13 Sep 00:00
14 Sep 00:00
15 Sep 00:00
16 Sep 00:00
17 Sep 00:00
18 Sep 00:00
19 Sep 00:00
20 Sep 00:00
21 Sep 00:00
22 Sep 00:00
23 Sep 00:00
24 Sep 00:00
25 Sep 00:00
26 Sep 00:00
27 Sep 00:00

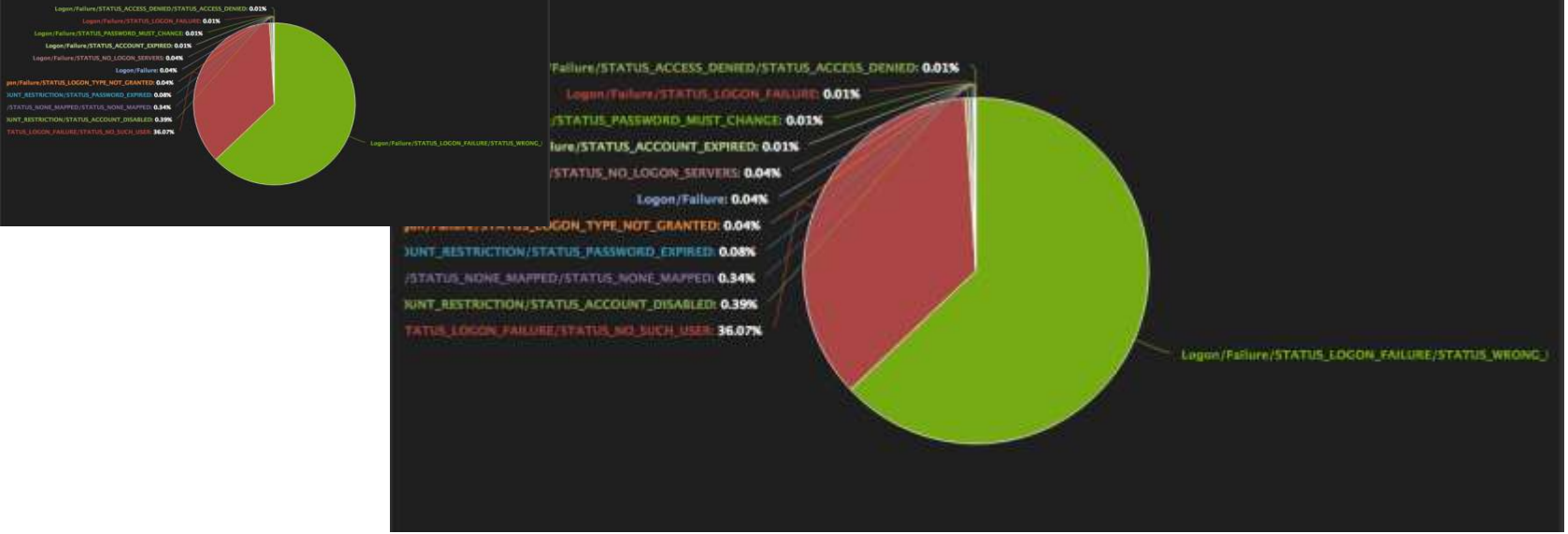
DAILY FAILED LOGON EVENT COUNT

Daily failed logon event count (all error codes).



LOGON FAILURE EVENTS BY FAILURE REASON

Logon failure events sorted by failure reason (error code).



LOGON FAILURE EVENTS BY FAILURE REASON

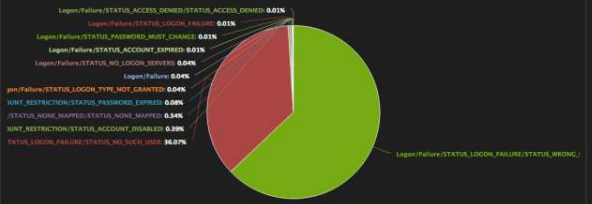
Logon failure events sorted by failure reason (error code).

DAILY FAILED LOGON EVENT COUNT

Daily failed logon event count (all error codes)

LOGON FAILURE EVENTS BY FAILURE REASON

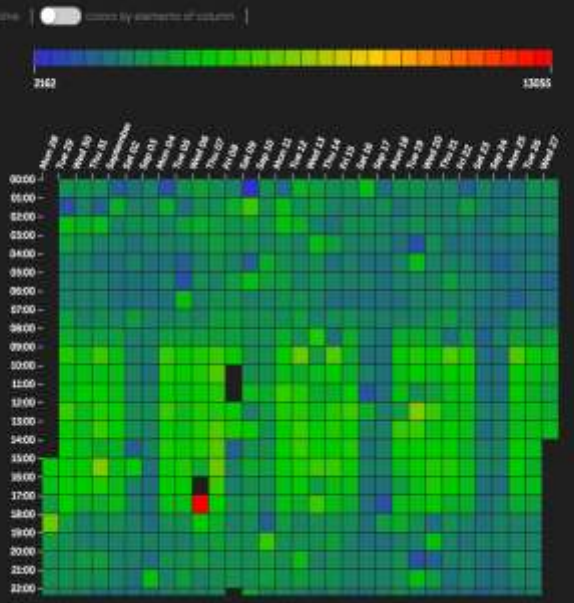
Logon failure events sorted by failure reason (error code).



FAILED LOGON EVENTS BY LOGON TYPE

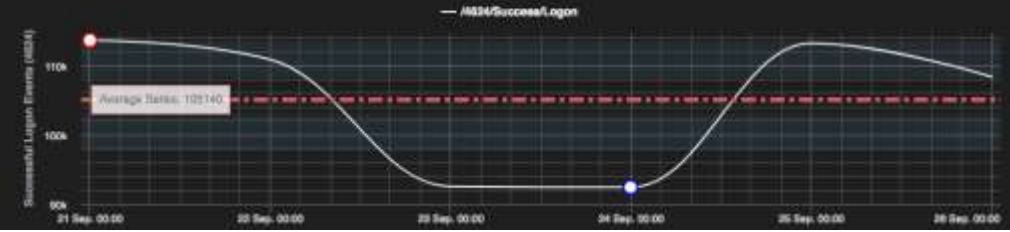
Failed logon event count by logon type.

LOGIN SUCCESS



DAILY SUCCESSFUL LOGON EVENTS

Daily successful logon event count (WEEKLY)



MOST FREQUENT LOGON FAILURE EVENTS

Frequent logon failures sorted by error code, username, source IP and workstation (Top100).

LOGONTYPESTR	MAINSTATUSCODE	SUBSTATUSCODE	USERNAME	SRCIP	WORKSTATION	COUNT
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	NIL	17	NI	2,601
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	DP/	17	NE	1,963
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	BIC	17	BI RT-WORK	1,688
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/ js	17 0	NE C	487
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/	17 20	NE C	192
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	D\s	17 30	DC	93
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	TES	17 0	TE	72
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	\ell	10	EL S	38
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/	17 3	NE C	33
Network	STATUS_ACCOUNT_RESTRICTION	STATUS_ACCOUNT_DISABLED	\gu	17 1	\\1 L4	30
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/	17 4	NE C	30
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	.\A	17 13	SV	27
Service	STATUS_NONE_MAPPED	STATUS_NONE_MAPPED	-\-		-	26
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/	17 8	WI 4K6RL9U	21
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	DB	17 51	DE /M	20
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	NB	17 06	NE	15
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	\erl om	17 23	NE	13
Network	STATUS_LOGON_FAILURE	STATUS_WRONG_PASSWORD	NB	17 5	NE C	11
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	DP/	17 5	NE	11
Network	STATUS_LOGON_FAILURE	STATUS_NO_SUCH_USER	NB	17 10	NE	10

Account adminstration

User Account Administration

Active Directory management & administration

Preferences

No refresh selected

Last update:
2017.06.1[redacted]

ACCOUNTS CREATED

List of accounts created in the given period

USERNAME	CREATEDBY	COUNT	%
D[redacted]	ad[redacted]	2	28.57%
D[redacted]	ad[redacted]	1	14.29%
D[redacted]tL	ad[redacted]	1	14.29%
D[redacted]min	ad[redacted]	1	14.29%
D[redacted]2	ad[redacted]	1	14.29%
D[redacted]	ad[redacted]	1	14.29%

ACCOUNTS DELETED

List of accounts deleted in the given time period

USERNAME	DELETEDBY	COUNT	%
D[redacted]	ad[redacted]	1	33.33%
D[redacted]	ad[redacted]	1	33.33%
D[redacted]	ad[redacted]	1	33.33%

ACCOUNTS DISABLED

List of accounts disabled in the given time period

USERNAME	DISABLEDBY	COUNT	%
D[redacted]VI$	ar[redacted]	2	22.2
D[redacted]	ar[redacted]	2	22.2
D[redacted]VI$	tr[redacted]	1	11.11
D[redacted]	ar[redacted]	1	11.11
D[redacted]	ar[redacted]	1	11.11
D[redacted]	ar[redacted]	1	11.11
D[redacted]	ar[redacted]	1	11.11

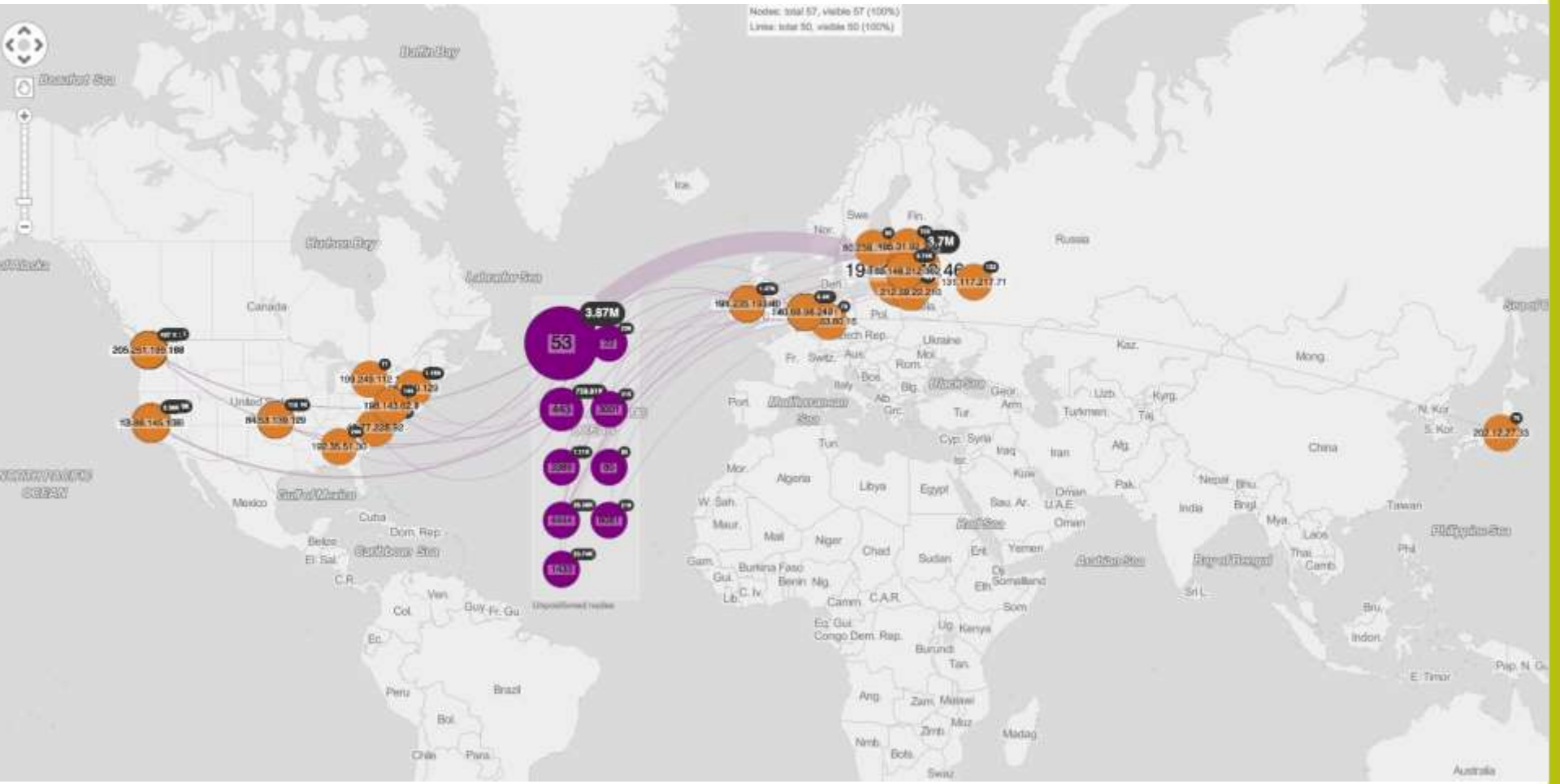
PASSWORD CHANGE FREQUENCY

Frequency of privileged users changing passwords of user accounts

ADMINISTRATION ACTIVITY

Total administrative actions (e.g. password change, account creation, deletion etc.)

File access monitoring


Nodes: total 57, visible 57 (100%)
Links: total 50, visible 50 (100%)
Canada
Mexico
Cuba
Dom. Rep.
Caribbean Sea
Gulf of Mexico
Hudson Bay
Labrador Sea
Baffin Bay
Beaufort Sea
Greenland Sea
Barents Sea
Russia
Ukraine
Kaz.
Mong.
China
India
Iran
Iraq
Afg.
Pak.
Saudi Arabia
Arabian Sea
Mediterranean Sea
Black Sea
Caspian Sea
Red Sea
Libya
Egypt
Algeria
Sudan
Chad
Niger
Mali
Nigeria
Kenya
Ethiopia
Somalia
Congo Dem. Rep.
Angola
Zambia
Zimbabwe
Namibia
Botswana
Madagascar
Peru
Brazil
Bolivia
Chile
Paraguay
Colombia
Venezuela
Ecuador
Australia
Indonesia
Philippine Sea
Taiwan
Japan
3.87M
53
3.7M

AR KO SĀKT?

Photo by Goh Rhy Yan on Unsplash

DEFINĒ MĒRĶI!

Photo by Aaron Thomas on Unsplash

SĀC AR VIENKĀRŠO

Photo by Igor Peftiev on Unsplash

PAPLAŠINI UN ATTĪSTI PĒC VAJADZĪBAS

Photo by Andhika Soreng on Unsplash

MĒRĶIS

ATBILSTĪBA

ANALĪZE

PREVENSIJA

VIENKĀRŠĀS LIETAS

IZPĒTE

KONFIGURĒŠANA

NOVĒRTĒŠANA

NOPIETNĀ PIEEJA

SIEM

MACHINE LEARNING

ADVANCED ANALYTICS

AIZIET!

Photo by rawpixel.com on Unsplash

ALTERNATĪVA - SIEM AS A SERVICE