LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS

VESPC / PAŠVALDĪBU IESPĒJAS UN IEGUVUMI

Artūrs Filatovs
LVRTC / Kiberaizsardzības biznesa virziena vadītājs

LVRTC

Vīzija

Droša, jaudīga un iekļaujoša digitālā Latvija.

Kas agrāk bija neiespējams, šodien ir digitāls.

#digiTuvi

Misija

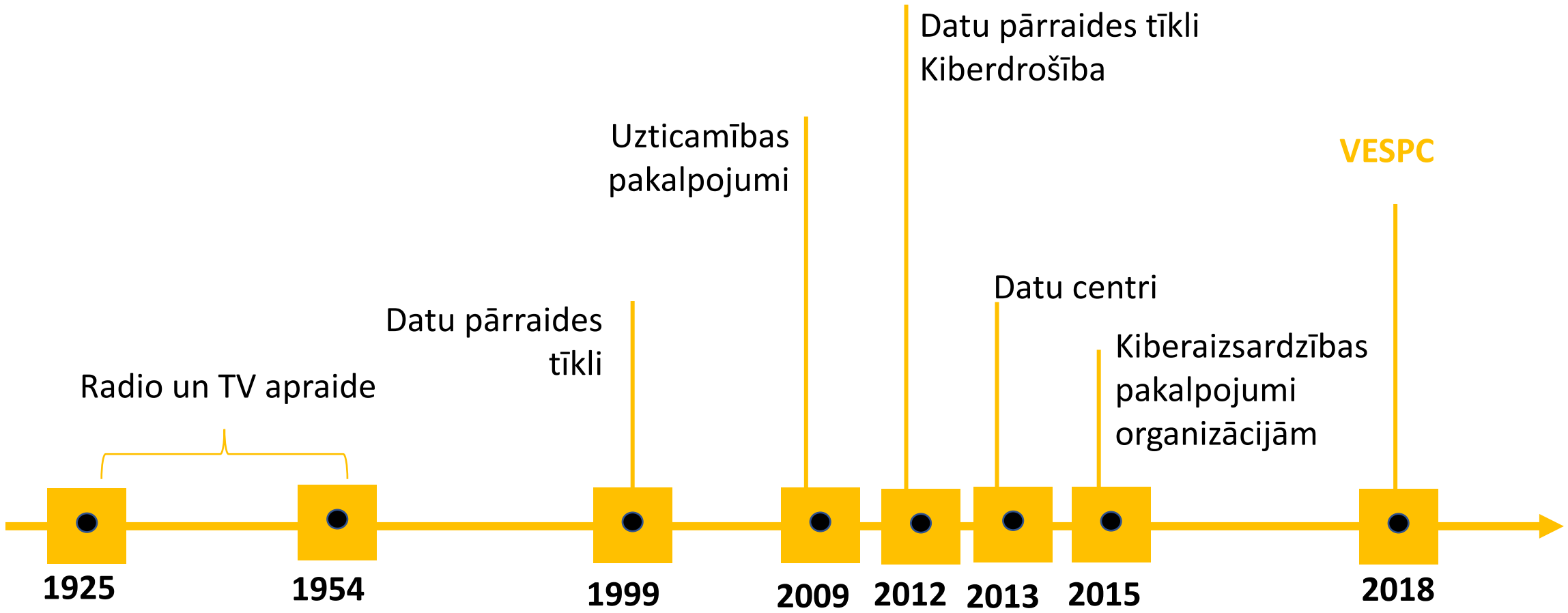
Nodrošināt un attīstīt augstas pieejamības, integritātes un drošības informācijas un komunikācijas tehnoloģiju infrastruktūru un pakalpojumus, stiprinot valsts efektīvu pārvaldi un drošību, kā arī sekmējot tautsaimniecības izaugsmi.

Vērtības

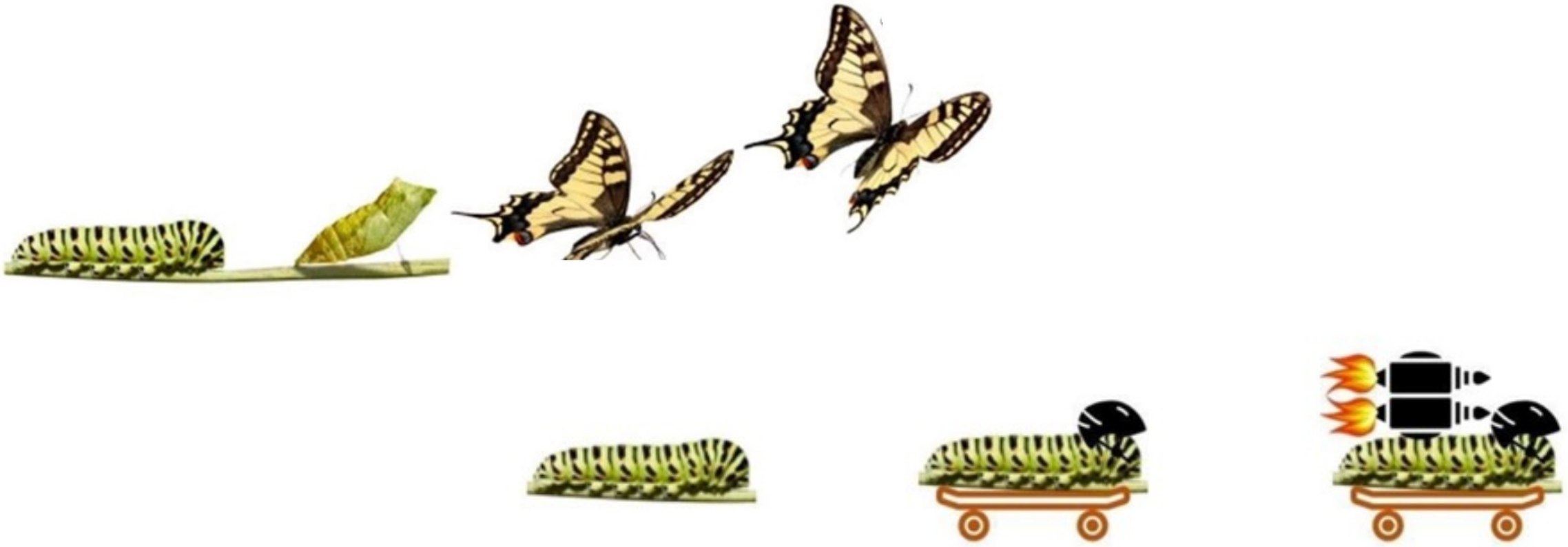
ATBILDĪBA
Ar atbildību par mums uzticēto

ATTĪSTĪBA
Ar drošu skatu augšup

ATVĒRTĪBA
Ar atvērtu prātu


Datu pārraides tīkli
Kiberdrošība
Uzticamības pakalpojumi
VESPC
Datu centri
Datu pārraides tīkli
Kiberaizsardzības pakalpojumi organizācijām
Radio un TV apraide
1925
1954
1999
2009
2012
2013
2015
2018

VAI TRANSFORMĒJOT BIZNESA PROCESUS TRANSFORMĒJAS ARĪ KIBERDROŠĪBA?



LVRTC

1/6

UZSKATA, KA IR PAKĻAUTI KIBERUZBRUKUMA RISKAM

4/5

VISPĀR NEDOMĀ PAR SAVU DARBA FAILU DROŠĪBU

95%

UZSKATA, KA PERSONĪGĀ KIBERDROŠĪBA IR VIRS VIDĒJĀ

75%

NAV IZDARĪJUŠI VISU, LAI PASARGĀTU SEVI NO KIBERUZBRUKUMIEM

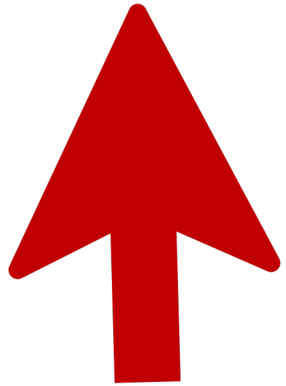
LVRTC

JAUNI TEHNOLOĢISKIE RISINĀJUMI

LVRTC

59,2%

Uzņēmumu saskaras ar grūtībām rekrutēt IT cilvēkus*



Resursu izmaksu pieaugums

*Centrālā statistikas pārvalde

LVRTC

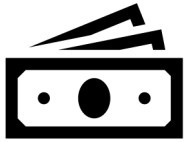

CYBERscape
v2.5
Network & Infrastructure Security
Web Security
Endpoint Security
Application Security
Mobile Security
Identity & Access Management
Security Incident Response
Security Analytics
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
2500+

LVRTC

UZBRUKUMA PIEMĒRS

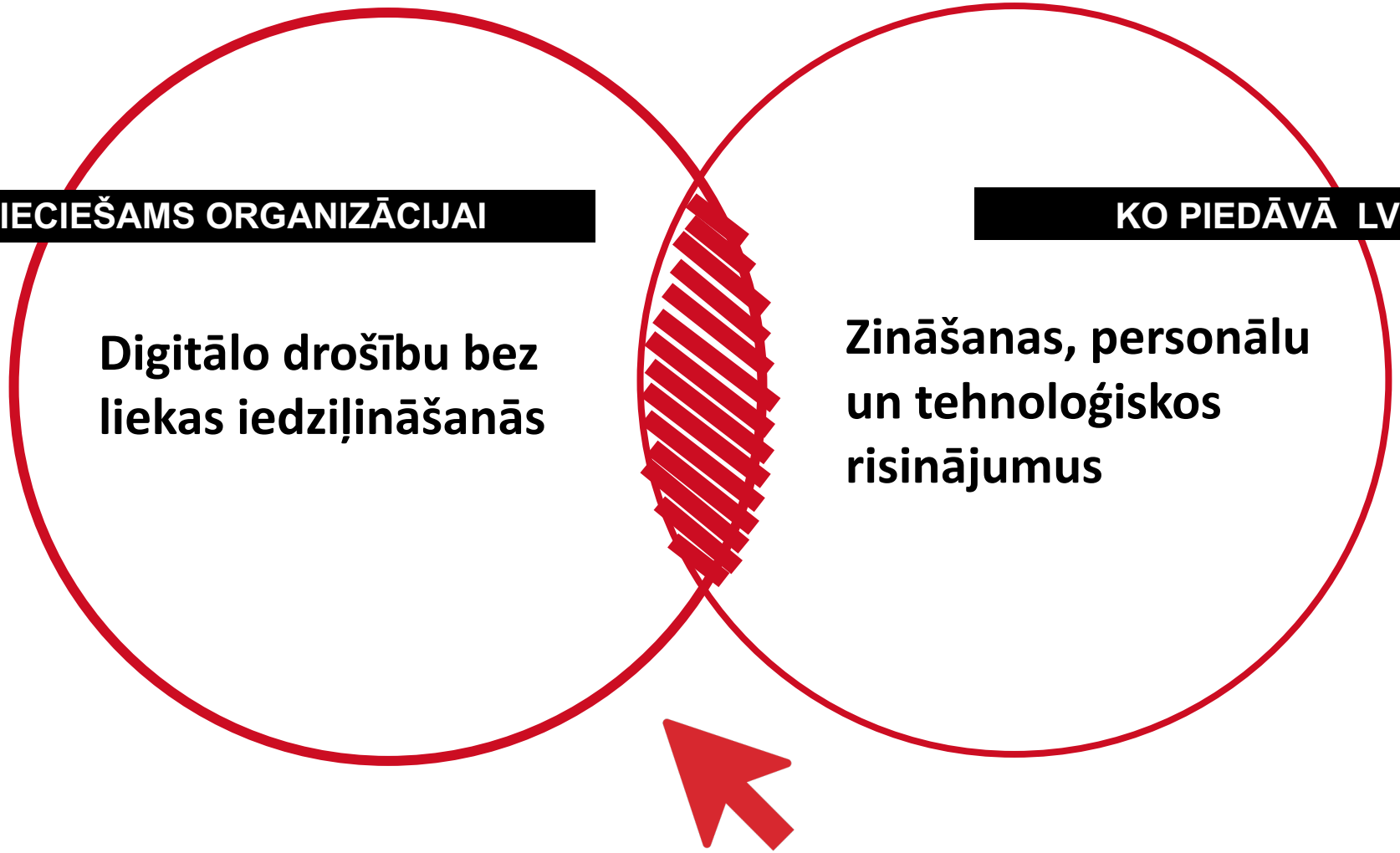
Time [UTC]	Description
[redacted] 15:34:22	Threat actor authenticates to the VPN at [redacted]
16:47:19	First internal activity: SMB scan
16:48:57	Successful authentication using the 'guest' account
16:57:42	Threat actor login to the domain controller [redacted] using the [redacted] account
18:51:12	PowerShell RAT executed on [redacted]
20:49:12	GPO is created, spreading the ransomware as a scheduled task.

= RISKS =



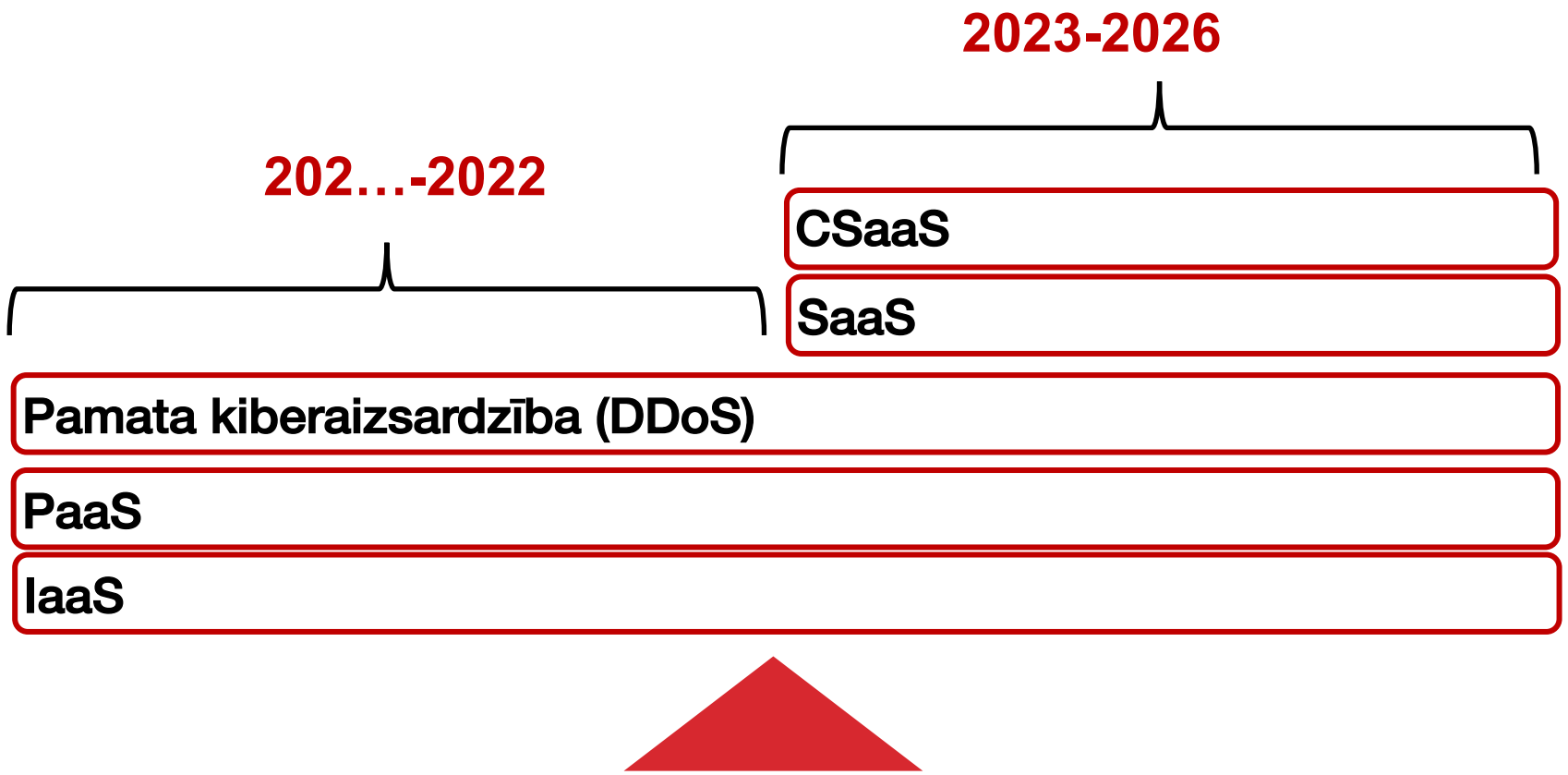
23 dienas

LVRTC



CEĻAM GAISĀ KIBERDROŠĪBU

IESKATIES NĀKTONĒ| LVRTC 2023-2026

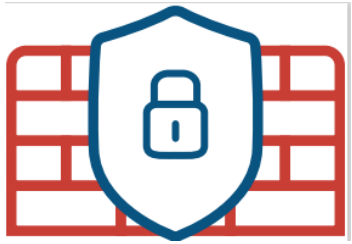


LVRTC

DROŠĪBAS VADĪBAS CENTRS (SOC)

IEVANOJAMĪBA RISKU PĀRVALDĪBA

IELAUŠANĀS TESTĒŠANA – KIBERDRAUDU IZLŪKOŠANA UN ŠĶIROŠANA



PRIVILIĢĒTU LIETOTĀJU KONTROLE

KIBERPOLIGONS

APMĀCĪBAS
SIMULĀCIJAS
TESTĒŠANA

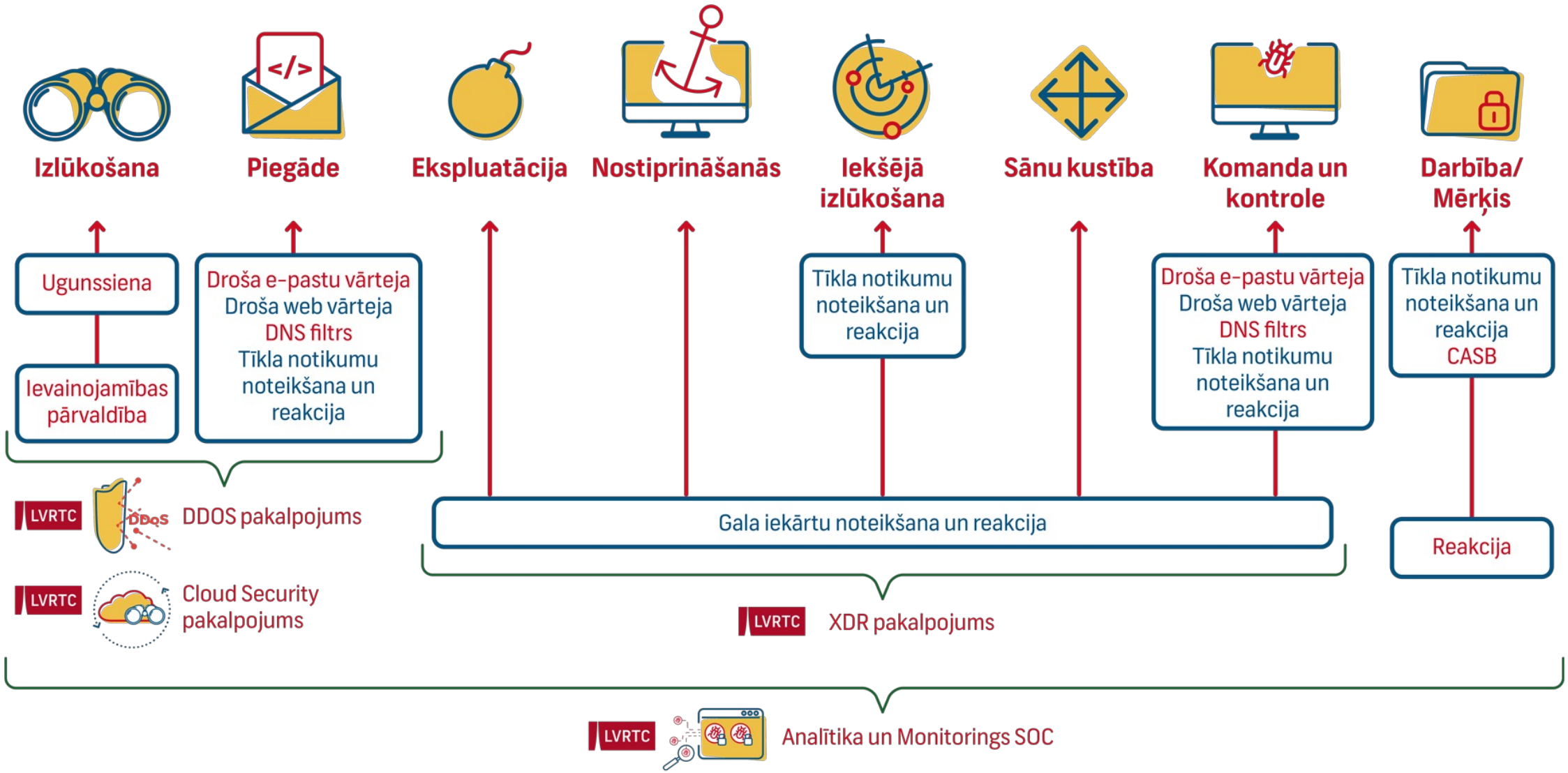
AIZSARDZĪBA

WAF KĀ PAKALPOJUMS

EDR/XDR

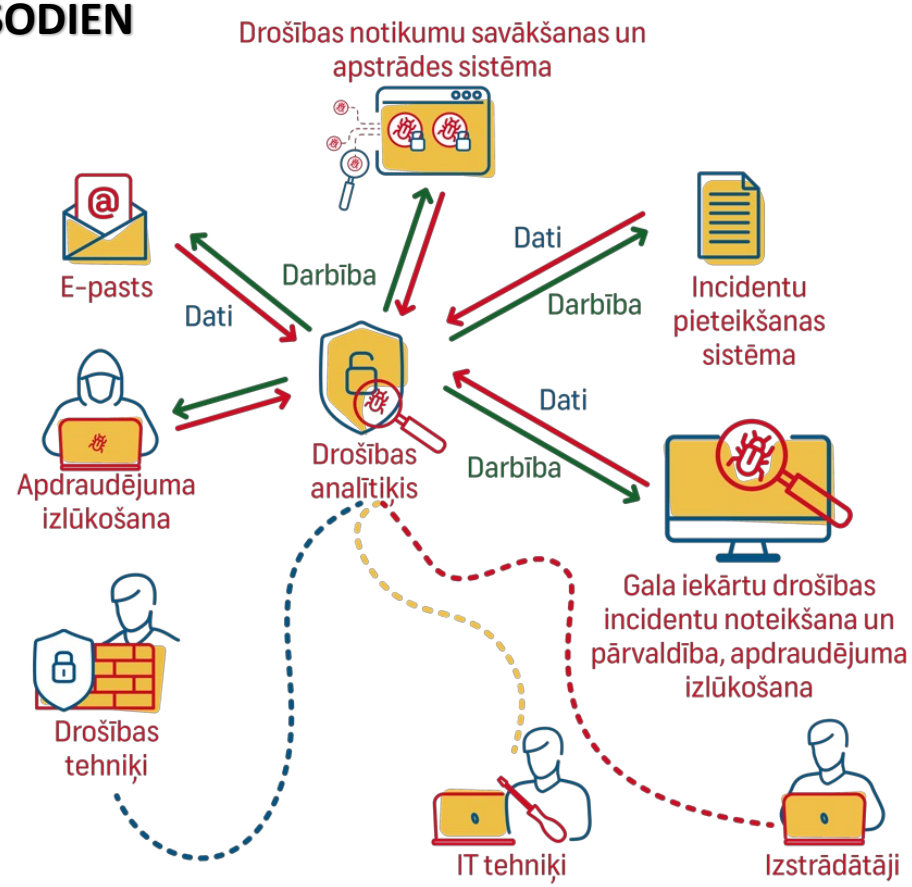
MĀKOŅPAKALPOJUMU DROŠĪBA

UZBRUCĒJU SOĻI UN MŪSU AIZSARDZĪBAS SPĒJAS

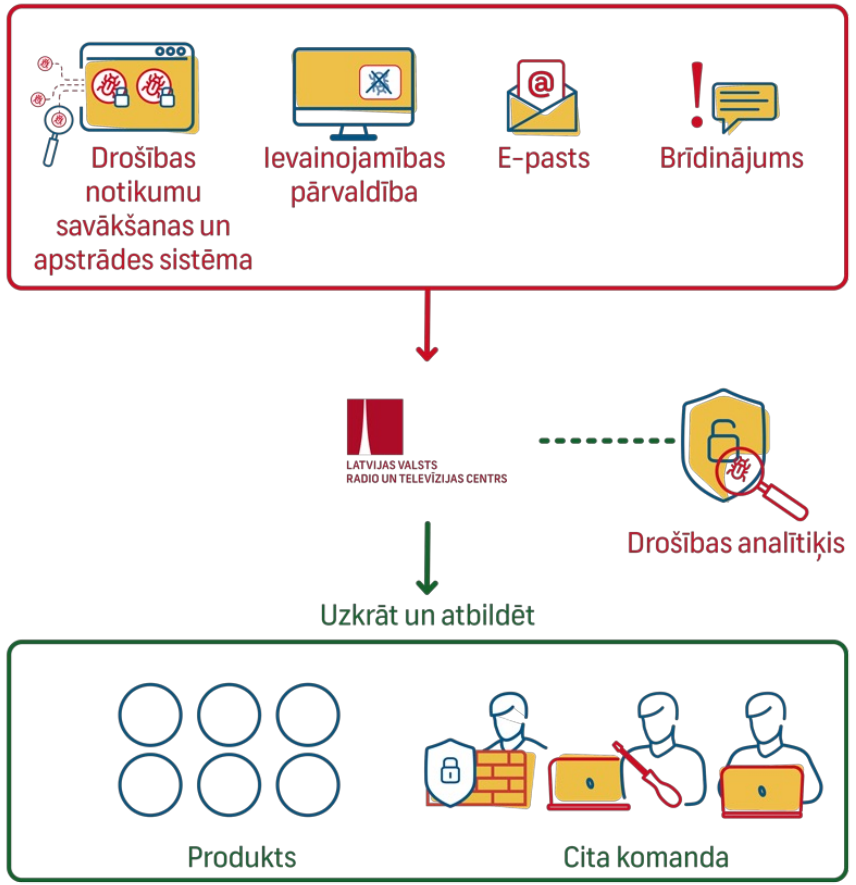


UZLABOTS PROCESS UZLABOTA DROŠĪBA

ŠODIEN



RĪTDIEN




LVRTC
KIBERDROŠĪBA
LVRTC GAUMĒ
4 jautājumi un 4 godīgas atbildes

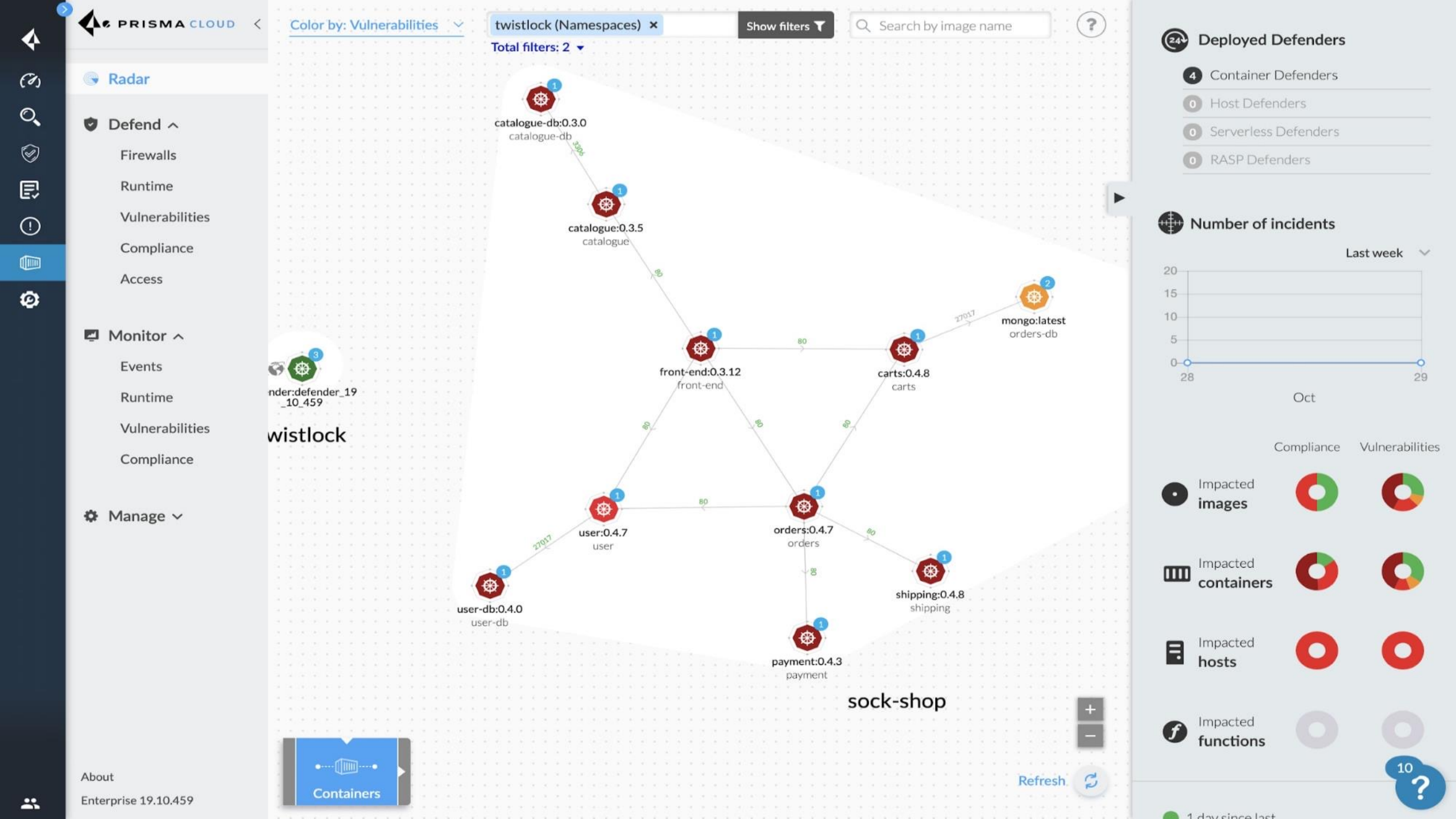
LVRTC

1
IZLŪKOŠANA

Nepareizas konfigurācijas nepilnības
125 334 unikālas IP adreses

Ļaunprātīgs kods
9801 unikāla IP adrese

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija


PRISMA CLOUD
Radar
Defend
Firewalls
Runtime
Vulnerabilities
Compliance
Access
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage
About
Enterprise 19.10.459
Color by: Vulnerabilities
twistlock (Namespaces) ×
Show filters
Total filters: 2
Search by image name
catalogue-db:0.3.0
catalogue-db
3306
catalogue:0.3.5
catalogue
80
front-end:0.3.12
front-end
carts:0.4.8
carts
mongo:latest
orders-db
27017
user:0.4.7
user
orders:0.4.7
orders
user-db:0.4.0
user-db
shipping:0.4.8
shipping
payment:0.4.3
payment
sock-shop
wistlock
Containers
Refresh
Deployed Defenders
4 Container Defenders
0 Host Defenders
0 Serverless Defenders
0 RASP Defenders
Number of incidents
Last week
20
15
10
5
0
28
29
Oct
Compliance
Vulnerabilities
Impacted images
Impacted containers
Impacted hosts
Impacted functions
10

Radar

Defend

Monitor

Events

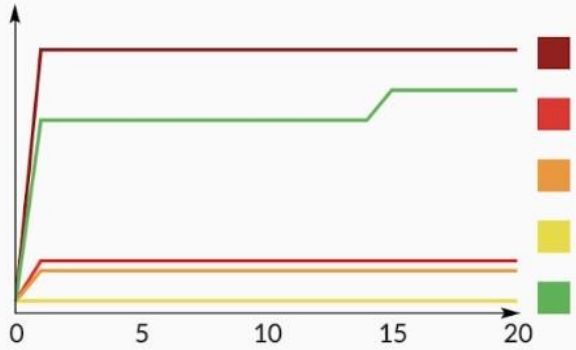
Runtime

Vulnerabilities

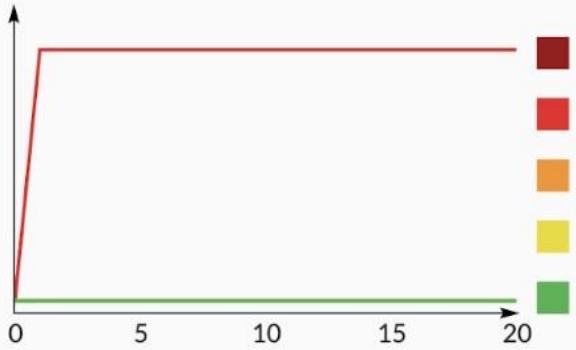
Compliance

Manage

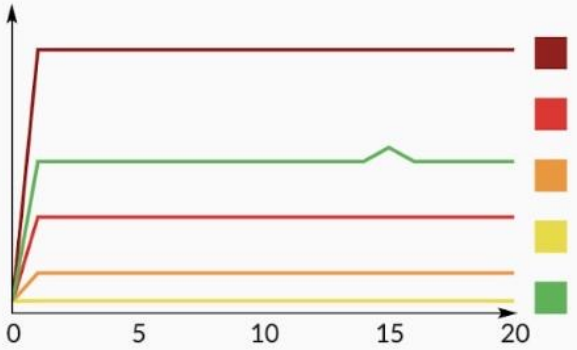
Impacted **containers** over time (30 days)



Impacted **hosts** over time (30 days)



Impacted **images** over time (30 days)



Top 10 most critical vulnerabilities (CVEs)

Images | Hosts

CSV

Search for specific CVEs

ID	Risk Score (0-100)	Risk Factors	Impacted Packages	Impacted Images
CVE-2018-1270	95	8	spring framework_spring-core:2.5.6	2.8%
CVE-2019-14379	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.1, com.fasterxml.jackson.core...	11.1%
CVE-2018-14718	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.1, com.fasterxml.jackson.core...	11.1%
CVE-2018-14719	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.1, com.fasterxml.jackson.core...	11.1%
CVE-2018-7489	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.1, com.fasterxml.jackson.core...	11.1%
CVE-2016-8735	91	5	apache tomcat_tomcat-embed-core:8.5.4	5.6%

LVRTC

#2
PELĒKĀ ZONA

Asset Inventory

New Try the new filters!

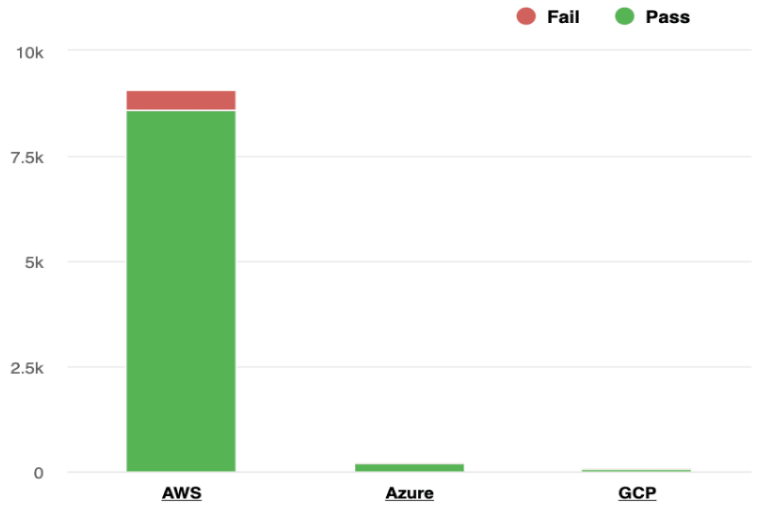
Unique Assets

9418	8855	30	420	113	563
Total	Pass	Low	Medium	High	Fail
		View Alerts	View Alerts	View Alerts	View Alerts

Asset Trend

Assets By Classification

Cloud Type



1 Group By Selected

Search

SERVICE NAME	CLOUD	TOTAL	PASS	FAIL	HIGH	MEDIUM	LOW	COVERAGE
Amazon VPC	aws	1022	800	222	68	154	0	78%
AWS Lambda	aws	575	490	85	2	83	0	85%
Amazon EC2	aws	1680	1647	33	4	11	18	98%
AWS IAM	aws	3528	3495	33	5	18	10	99%
Amazon API Gateway	aws	58	26	32	0	32	0	45%
Amazon S3	aws	39	15	24	20	4	0	39%

ASSET INVENTORY

Most Recent

ACCOUNT GROUP

Search for Account Group

CLOUD ACCOUNT

Search for Cloud Account

CLOUD REGION

Search for Cloud Region

CLOUD TYPE

- Select All
- Alibaba Cloud
- AWS
- Azure
- GCP
- OCI

CLOUD SERVICE

Search for Cloud Service

- Select All
- Amazon EC2
- Amazon S3
- Amazon VPC
- Azure Storage
- Azure Virtual Network

Clear All

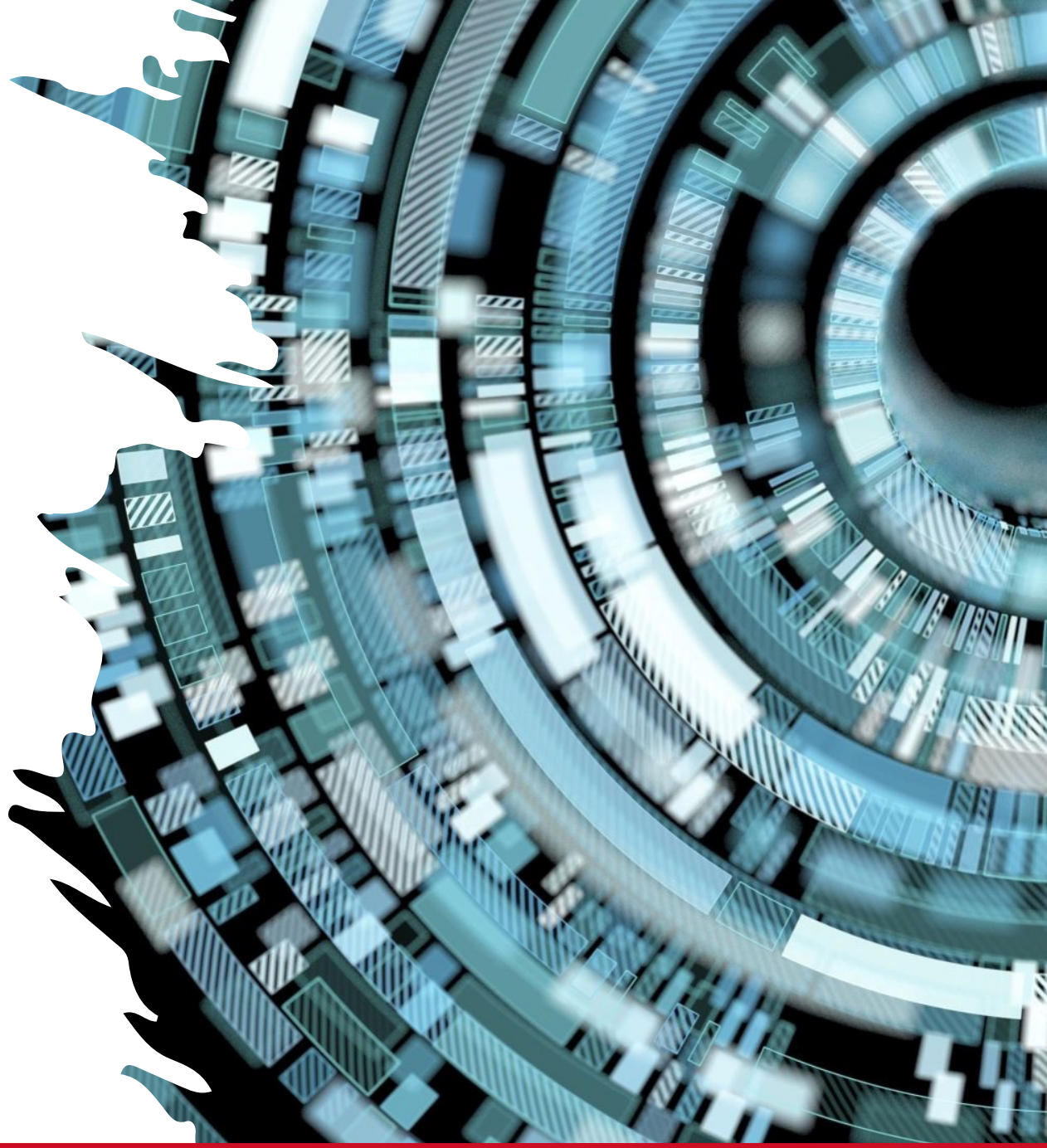
1887

Trial

LVRTC

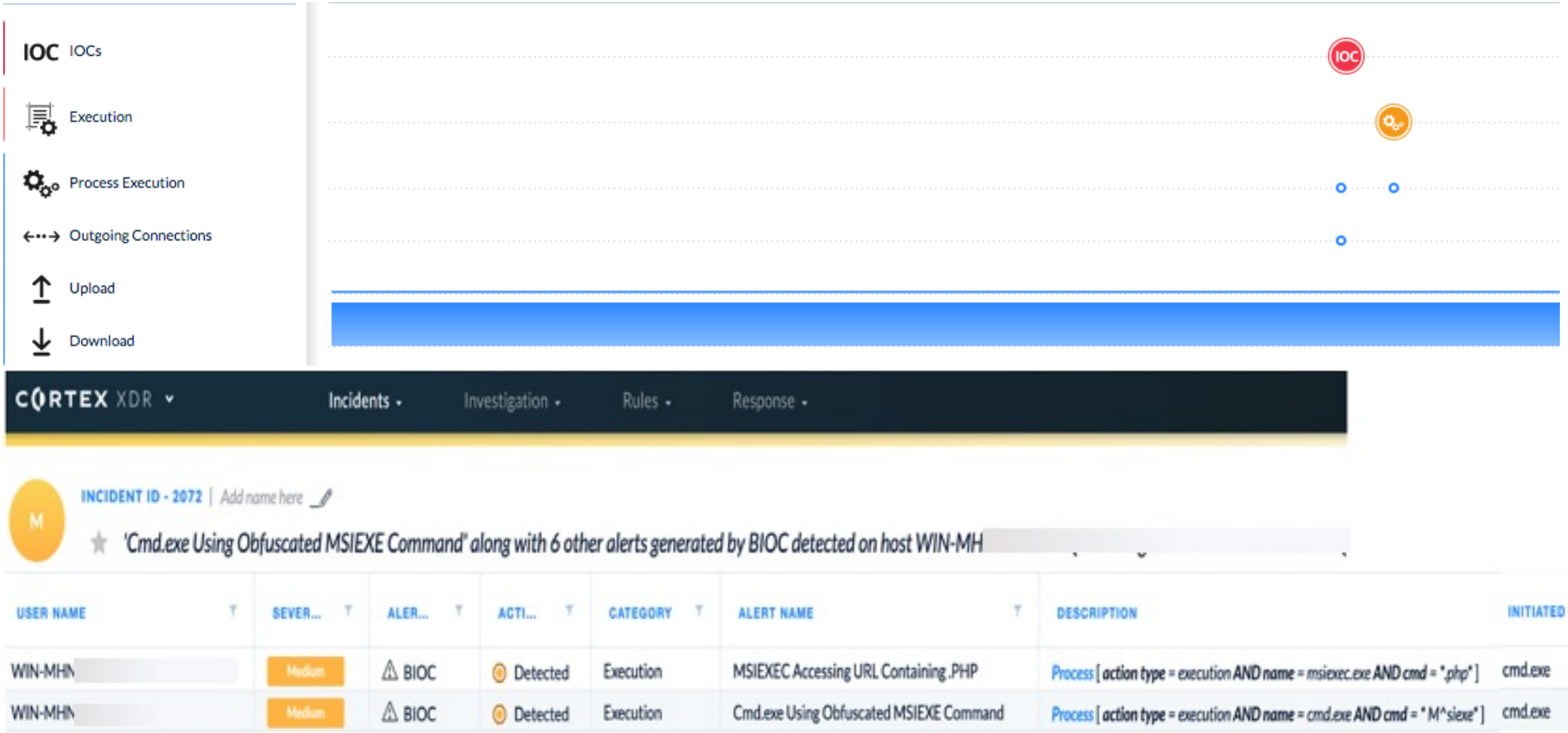
#3

E-PASTI UN PIKŠĶERĒŠANA



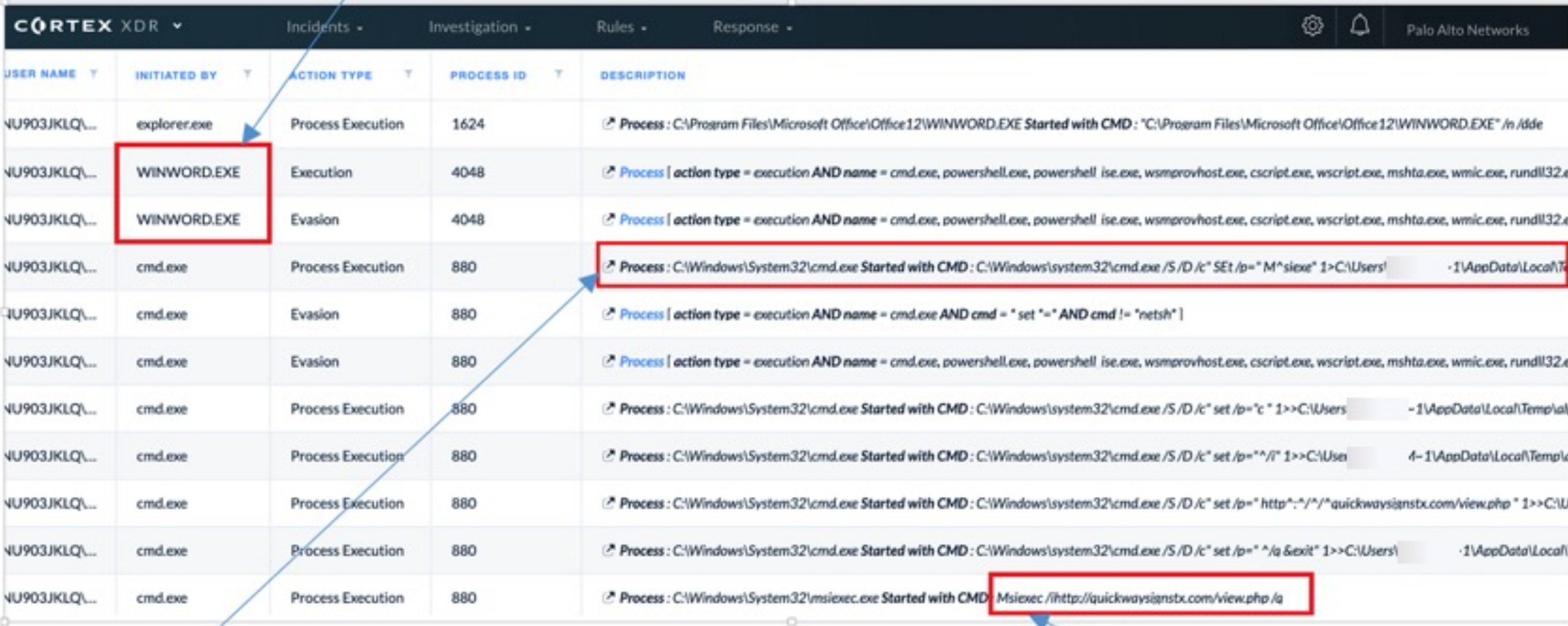
LVRTC

KOMPROMITĒŠANAS IDENTIFIKĀCIJA



LVRTC

MS Word launched and macro executed



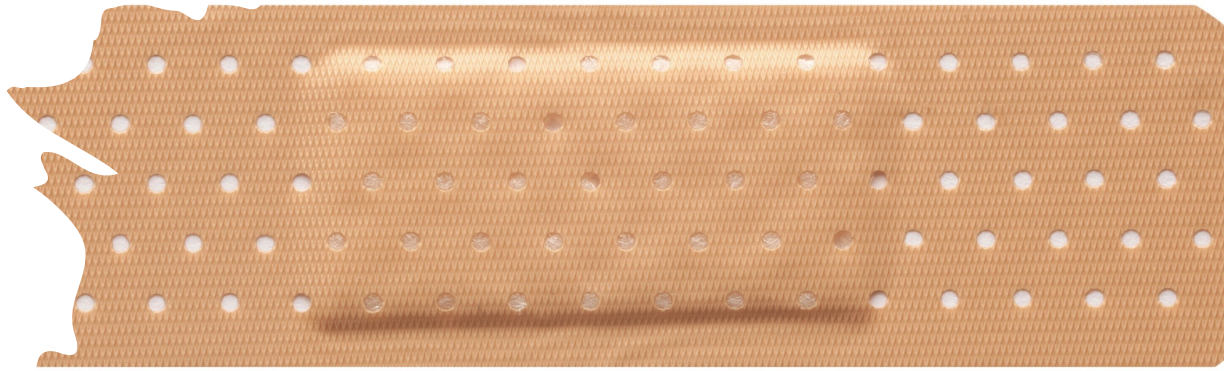
Batch file alpaca.bat created

Msiexec executed and downloads MSI payload

LVRTC

#4

SIEM UN INCIDENTU ANALĪZE

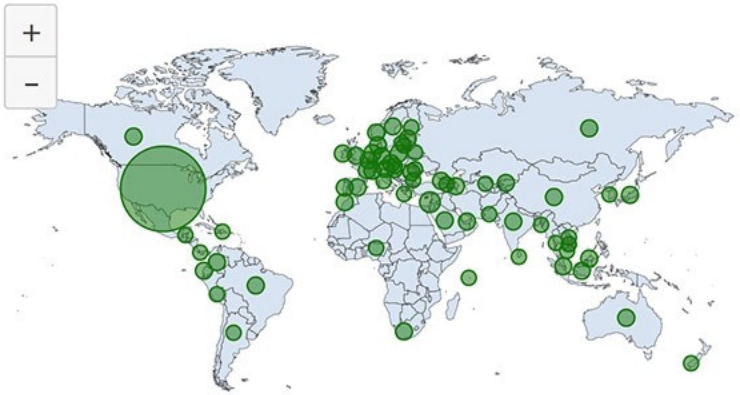


Managed by Threat Hunting

Cloud and Identity

Last Updated: Mar 1st 14:10

Cloud Location



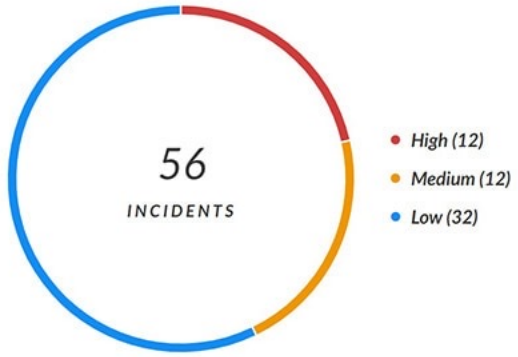
Update Interval 24 hrs | Last Update: Mar 1st 2022 10:25:54 Update Now

Top Incidents (Top 10)

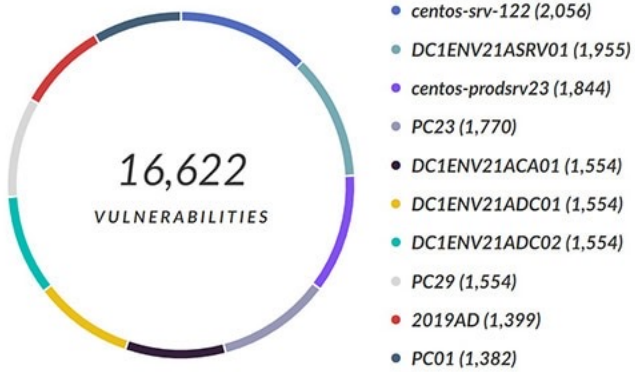
SEVERITY	DESCRIPTION		ALERTS BREAKDOWN
High	'Staged Malware Ac...	11	[• 9 ...
High	'DGA:yhhv0cvui7rj.r...	8	[• 8]
High	3 'Manipulation of d...	3	[• 3]
High	'Suspicious API call f...	5	[• 2 ...
High	2 'Manipulation of d...	2	[• 2]
High	'Suspicious API call f...	2	[• 1 ...
High	'Manipulation of def...	2	[• 1 ...
High	'Manipulation of def...	1	[• 1]
High	'WildFire Malware' ...	1	[• 1]

Alerts By MITRE Tactic

Open Incidents by Severity (Last 30 days)

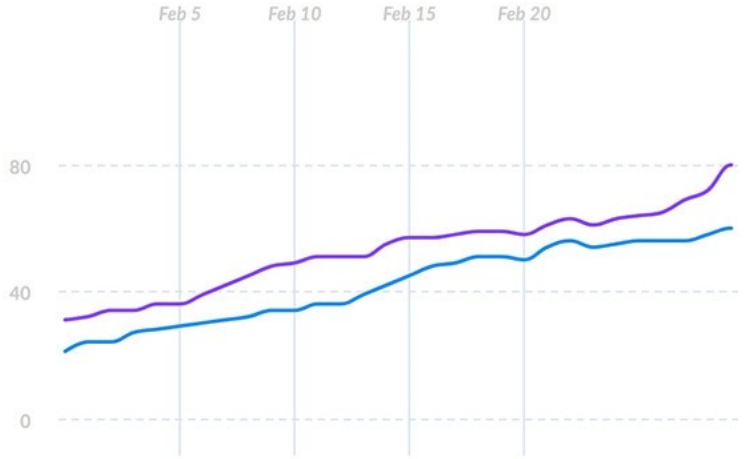


Top 10 Vulnerable Endpoints



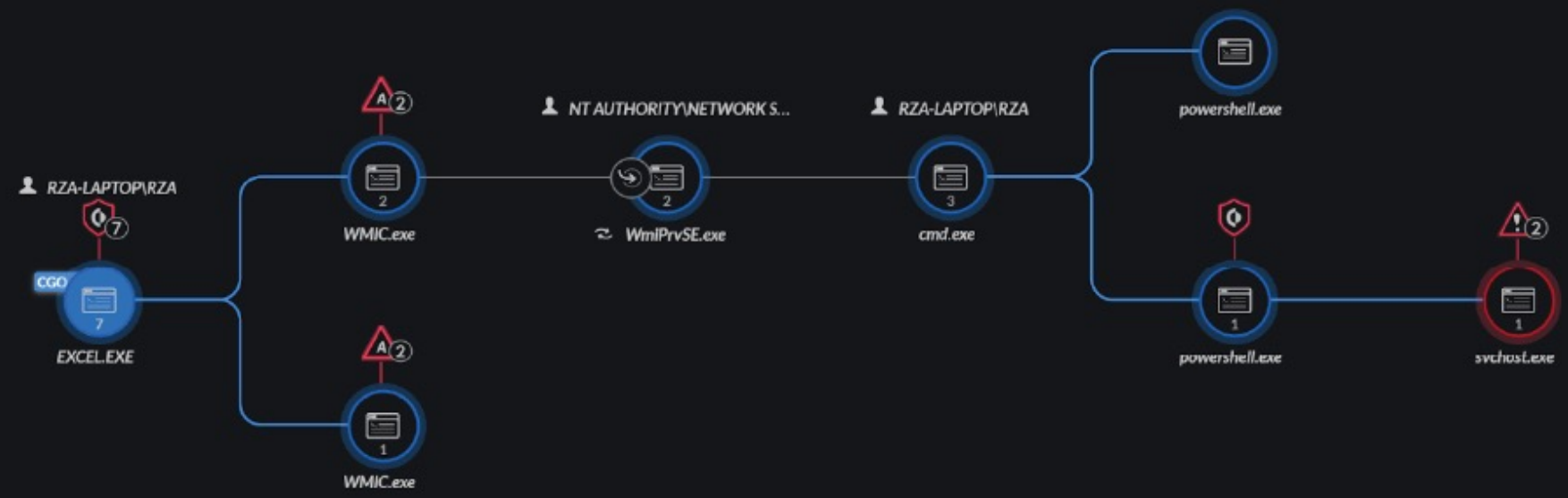
Total Incidents

Aged
Total Unresolved Incidents



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

Actions



PATH
C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME
Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE
Benign

SHA256
6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME
RZA-LAPTOP\RZA

MD5
4954c459b45a06727bdbeb7f2f55...

SIGNATURE
Signed by Microsoft Corporation

CMD
"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

ALL ACTIONS 472 Results	ALERT 7 Results	PROCESS 3 Results	NETWORK 69 Results	FILE 197 Results	REGISTRY 27 Results	MODULE 176 Results	NETWORK CONNECTIONS 69 Results

Filter

TIMESTAMP	USER NAME	INITIATED BY	INITIATOR PID	INITIATOR TID	ACTION TYPE	DESCRIPTION

LVRTC

VESPC – VALSTS ELEKTRONISKO SAKARU PAKALPOJUMU CENTRS

Tehnisko līdzekļu un pakalpojumu kopums,
kas publiskajai personai, publiskās
personas kapitālsabiedrībai un publiskās personas
kontrolētai kapitālsabiedrībai nodrošina infrastruktūru
ar augstu konfidencialitāti, integritāti un pieejamību
informācijas sistēmām un ar tām saistītajiem
tehnoloģiskajiem risinājumiem, kā arī pakalpojumus.

Elektronisko sakaru likums |MK, instrukcija Nr. 5 | Valsts elektronisko sakaru pakalpojumu centra nodrošināšanas kārtība;
|Deleģēšanas līgums.

19 PAKALPOJUMI

LVRTC

KĀ PIETEIKTIES VESPC

Organizācija nosūta pieteikumu Vides aizsardzības un reģionālās attīstības ministrijai (VARAM)

VARAM darba grupa izskata pieteikumu

VARAM lēmums "Par atbalstu IS iekļaušanai un izvietošanai VESPC"

Organizācija un VAS Latvijas Valsts radio un televīzijas centrs (LVRTC) saskaņo:

- pakalpojuma cenu
- tehnisko risinājumu un resursu apjoma pieejamību

Organizācija nosūta VARAM apliecinājumu, ka nosacījumi ir saskaņoti ar LVRTC

VARAM protokollēmums "Par atbalstu IS iekļaušanai un izvietošanai VESPC"

Organizators un LVRTC noslēdz līgumu

Slēdzot līgumu par VESPC pakalpojumiem, organizācijai nav jāpiemēro Publisko iepirkumu likums vai Sabiedrisko pakalpojumu sniedzēja iepirkuma likums.

! Līgumu var slēgt arī ilgterminā – 2035. gadam

Ministru kabineta instrukcija Nr. 5 Valsts elektronisko sakaru pakalpojumu centra nodrošināšanas kārtība

Paldies par uzmanību

ATBILDĪBA / ATTĪSTĪBA / ATVĒRTĪBA

Droša, jaudīga un iekļaujoša digitālā Latvija.