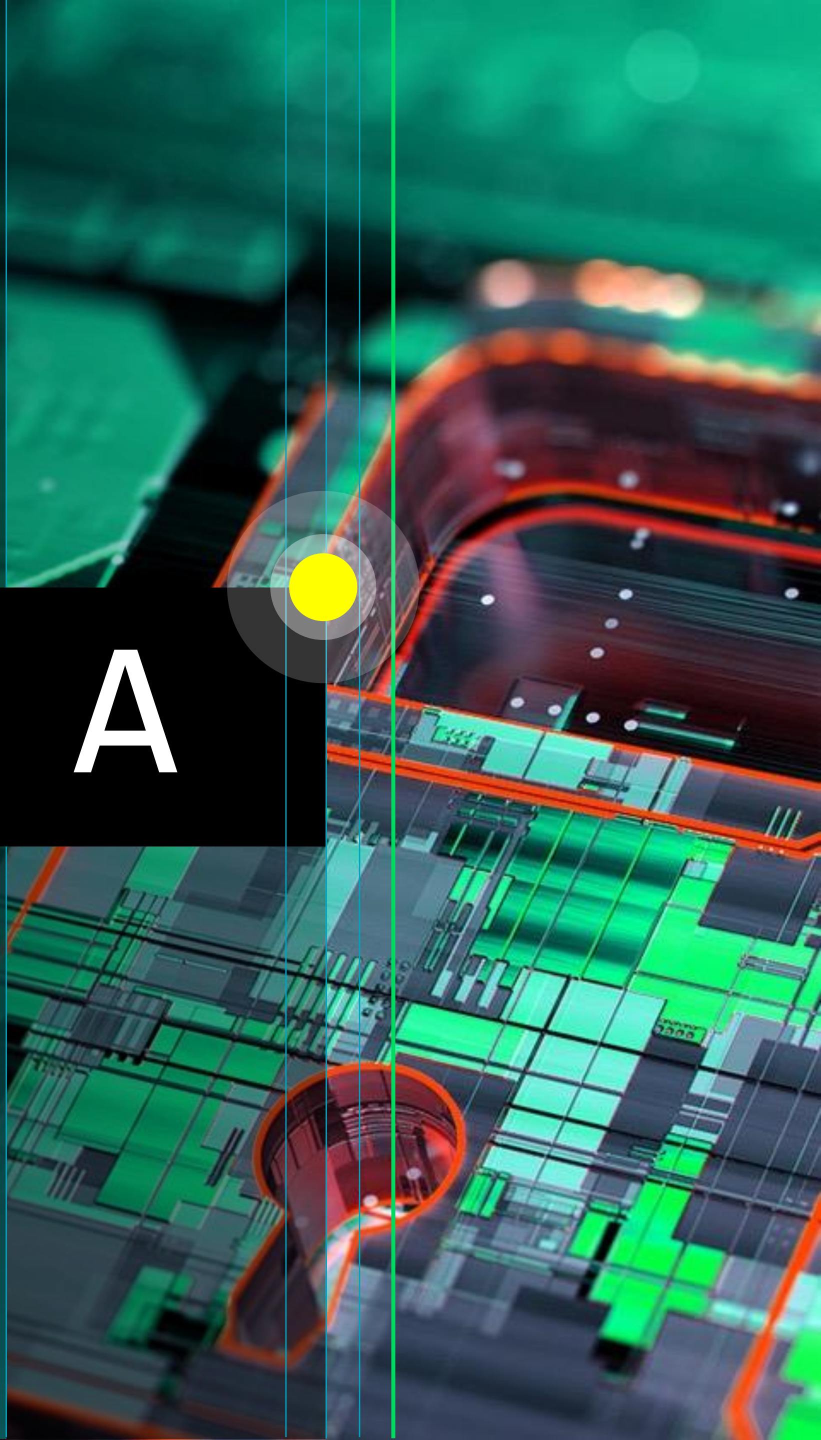
UKRENERGO
National power company

CYBERSECURITY IN A Wartime



23.02.2022

23:00

The community had noticed problems with availability of resources of Ukrainian organizations – DDoS attacks had started

24.02.2022

01:00

DDoS on Ukrenergo – some of the services were violated. The amount of automatically blocked by WAF requests was about 1 720 000.

04:00

Started to block request on WAF and Firewalls manually by malicious IP-addresses and countries

09:00

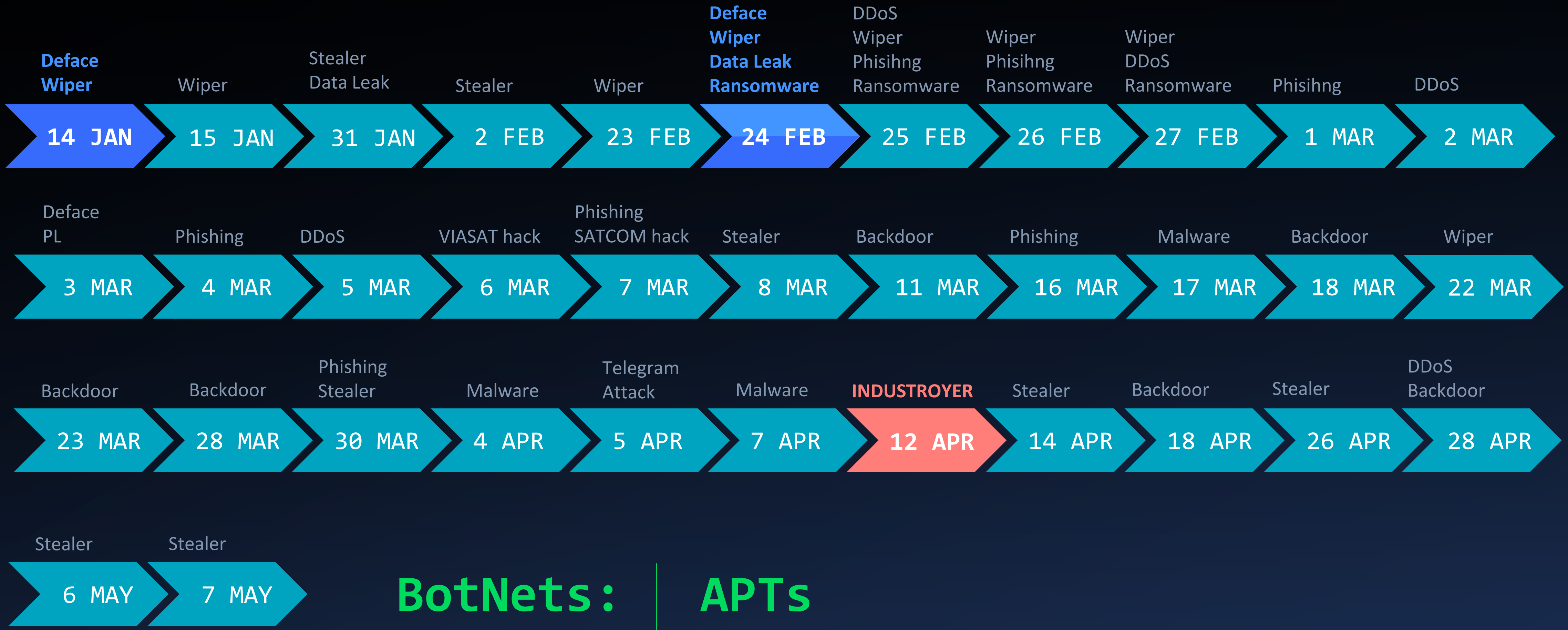
The access to Ukrenergo infrastructure was available only from Ukraine and ENTSOE members

12:00

All services were up, situation stabilized, everything worked as usual

More than 20 000 IP-addresses were manually blocked and more than 100 000 automatically for first 2 weeks.

Cyberattacks timeline: NPC Ukrenergo



Deface **Wiper**	**14 JAN**
Wiper	15 JAN
Stealer Data Leak	31 JAN
Stealer	2 FEB
Wiper	23 FEB
Deface **Wiper** **Data Leak** **Ransomware**	**24 FEB**
DDoS Wiper Phisihng Ransomware	25 FEB
Wiper Phisihng Ransomware	26 FEB
Wiper DDoS Ransomware	27 FEB
Phisihng	1 MAR
DDoS	2 MAR
Deface PL	3 MAR
Phishing	4 MAR
DDoS	5 MAR
VIASAT hack	6 MAR
Phishing SATCOM hack	7 MAR
Stealer	8 MAR
Backdoor	11 MAR
Phishing	16 MAR
Malware	17 MAR
Backdoor	18 MAR
Wiper	22 MAR
Backdoor	23 MAR
Backdoor	28 MAR
Phishing Stealer	30 MAR
Malware	4 APR
Telegram Attack	5 APR
Malware	7 APR
INDUSTROYER	**12 APR**
Stealer	14 APR
Backdoor	18 APR
Stealer	26 APR
DDoS Backdoor	28 APR
Stealer	6 MAY
Stealer	7 MAY

COUNTRIES:

🇧🇾 🇷🇺

BotNets:

Mirai,
Gafgyt,
IRCbot,
Ripprbot,
Moobot

APTs

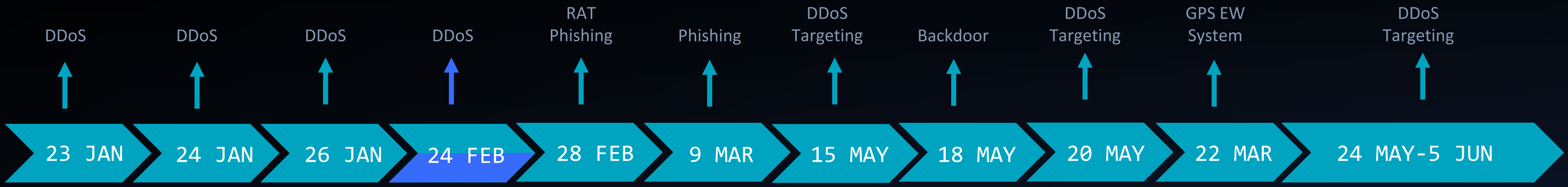
Primitive Bear
EmberBear
BerserkBear
FreeCivilian

VOODOO Bearaka
Sandworm
Ghostwriter
LockBit

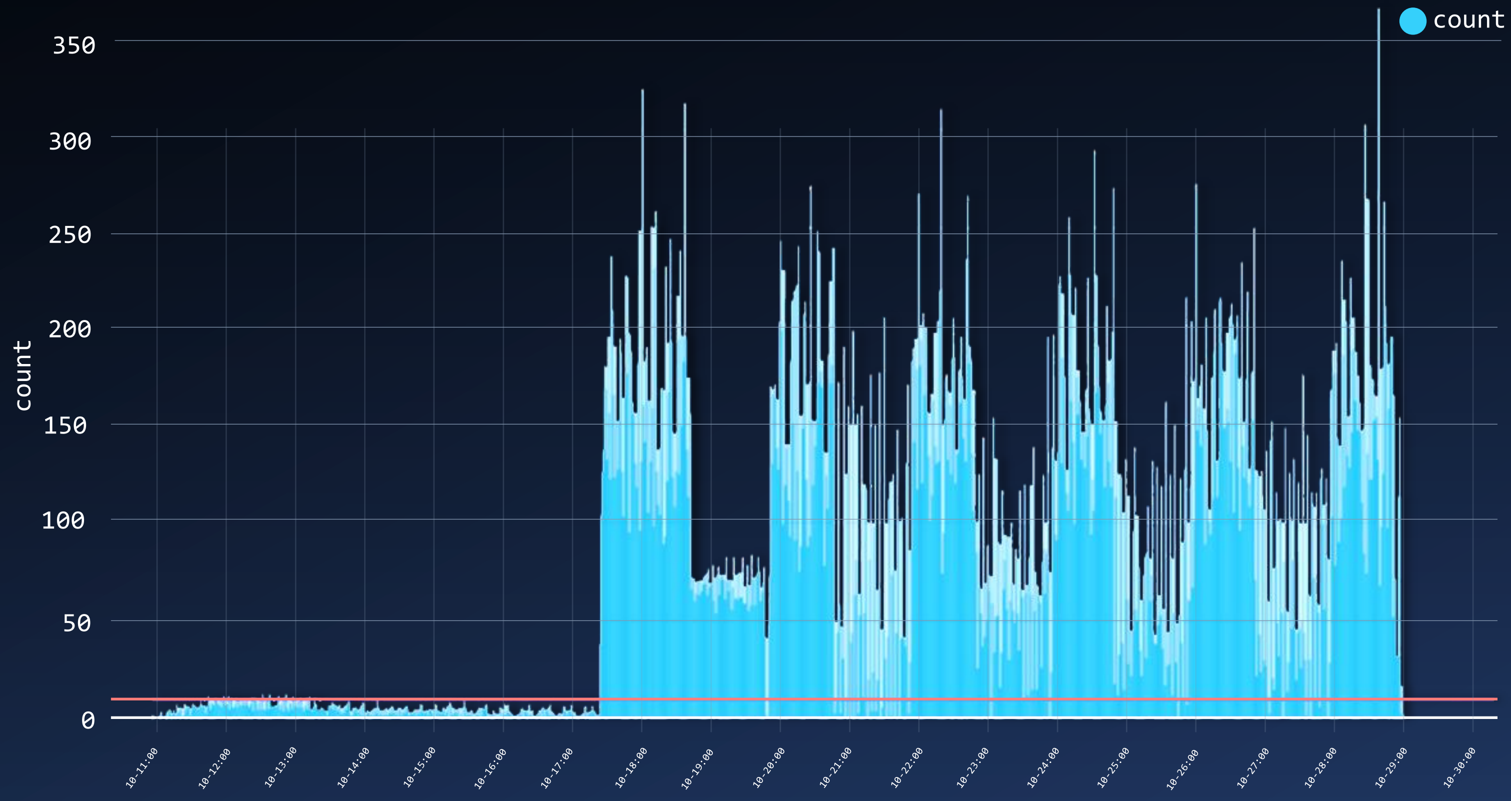
Vermint
APT28
TA416
XDSpy

DEV-0586
DEV-0665
Conti ransomware

Cyberattacks timeline: NPC Ukrenergo



- DDoS — 23 JAN
- DDoS — 24 JAN
- DDoS — 26 JAN
- DDoS — 24 FEB
- RAT Phishing — 28 FEB
- Phishing — 9 MAR
- DDoS Targeting — 15 MAY
- Backdoor — 18 MAY
- DDoS Targeting — 20 MAY
- GPS EW System — 22 MAR
- DDoS Targeting — 24 MAY-5 JUN



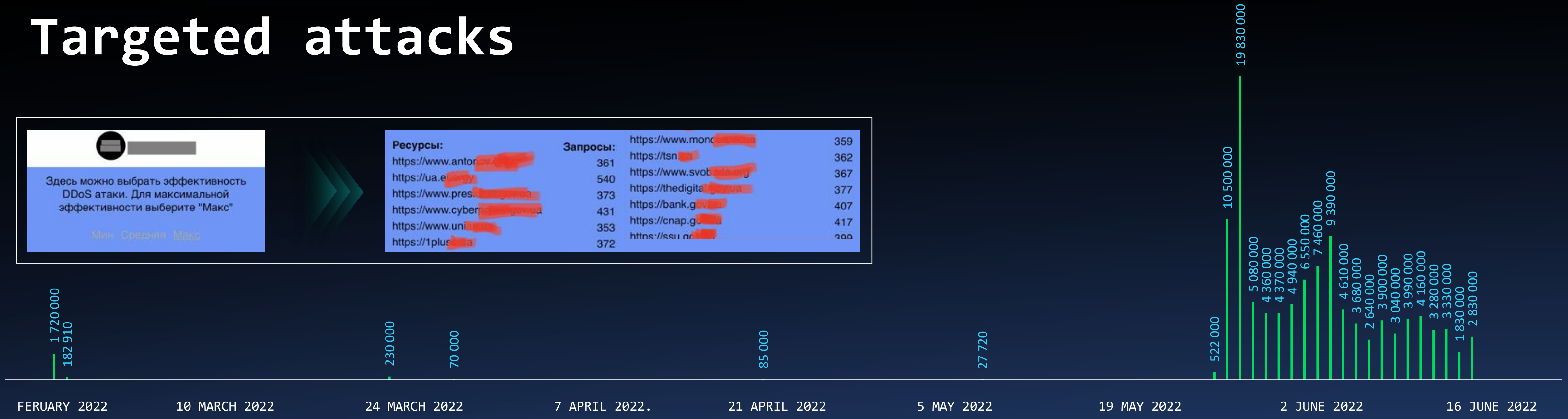
COUNTRIES: 🇧🇾 🇷🇺

BotNets:
Ripprbo,
Mirai,
Gafgyt,
IRCbot,
Moobot

APTs

VOODOO Bear aka *Sandworm*
Primitive Bear
BerserkBear
Ghostwriter
EmberBear
DEV-0586
DEV-0665
Vermint
APT28

Targeted attacks



[redacted]

Здесь можно выбрать эффективность DDoS атаки. Для максимальной эффективности выберите "Макс"

Мин Средняя Макс

Ресурсы:	Запросы:		
https://www.anton[redacted]	361	https://www.mon[redacted]	359
https://ua.e[redacted]	540	https://tsn[redacted]	362
https://www.pres[redacted]	373	https://www.svob[redacted]	367
https://www.cyber[redacted]	431	https://thedigita[redacted]	377
https://www.uni[redacted]	353	https://bank.g[redacted]	407
https://1plus[redacted]	372	https://cnap.g[redacted]	417
		https://ssu.g[redacted]	399

Events summary

(About Firewall Events)

Total 107.66M

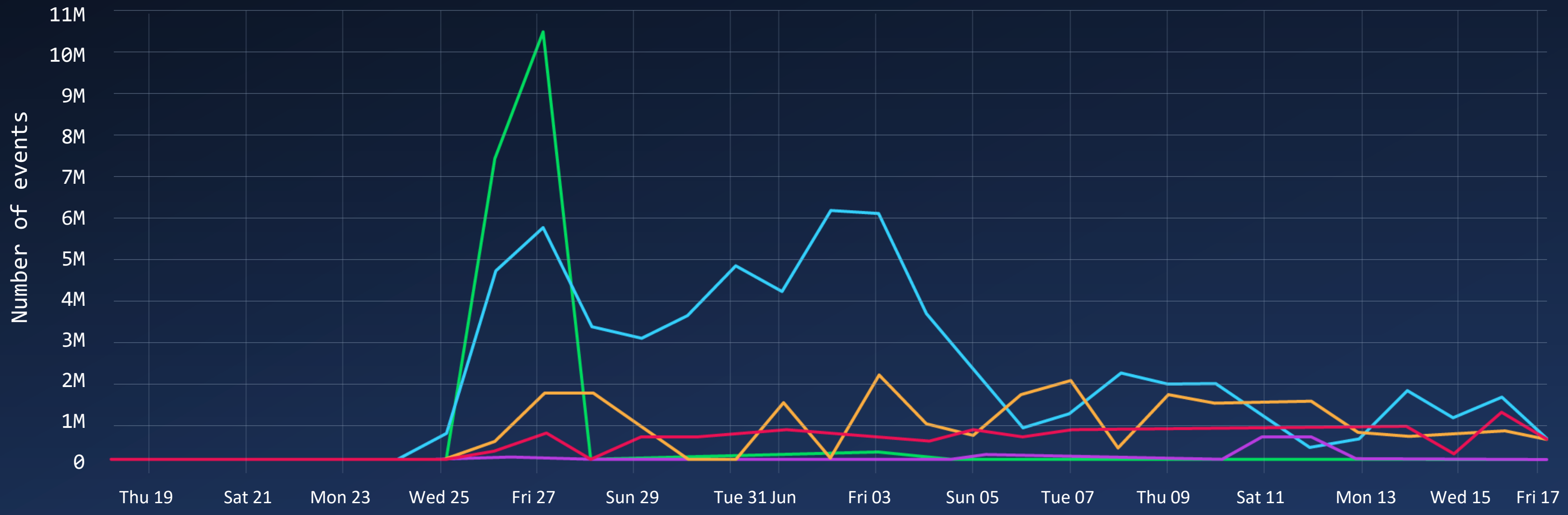
● Russian Fed. 57.17M

● Ukraine 19.73M

● USA 17.92M

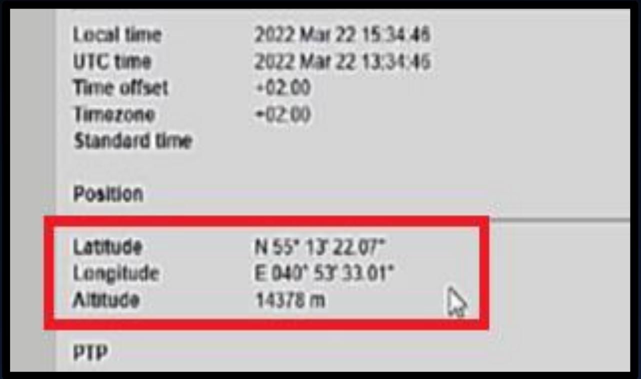
● Peru 11.63M

● Belarus 1.26M



GPS jamming (22.03.2022)

Substation clock was changed into Moscow local time – attackers changed positioning coordinates

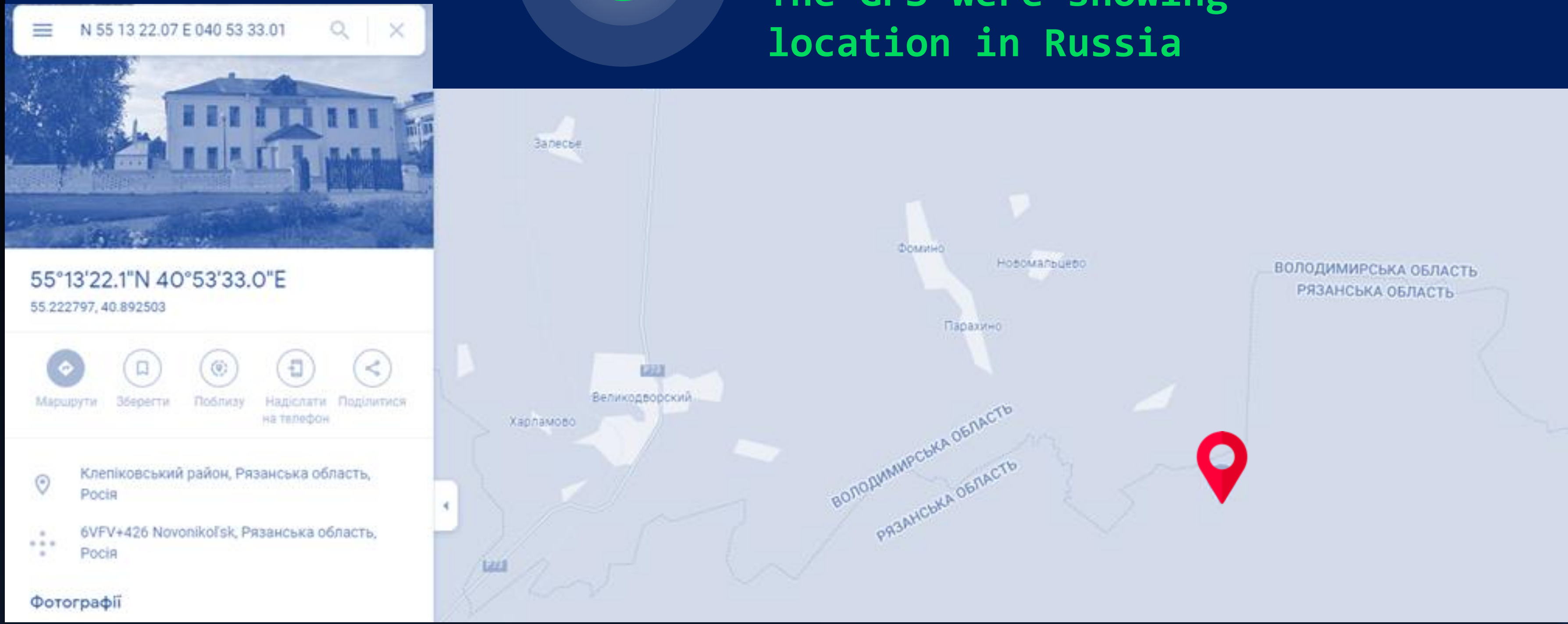


```
Local time        2022 Mar 22 15:34:46
UTC time          2022 Mar 22 13:34:46
Time offset       +02:00
Timezone          +02:00
Standard time

Position

Latitude          N 55° 13' 22.07"
Longitude         E 040° 53' 33.01"
Altitude          14378 m

PTP
```



N 55 13 22.07 E 040 53 33.01

55°13'22.1"N 40°53'33.0"E

55.222797, 40.892503

Клепіковський район, Рязанська область, Росія

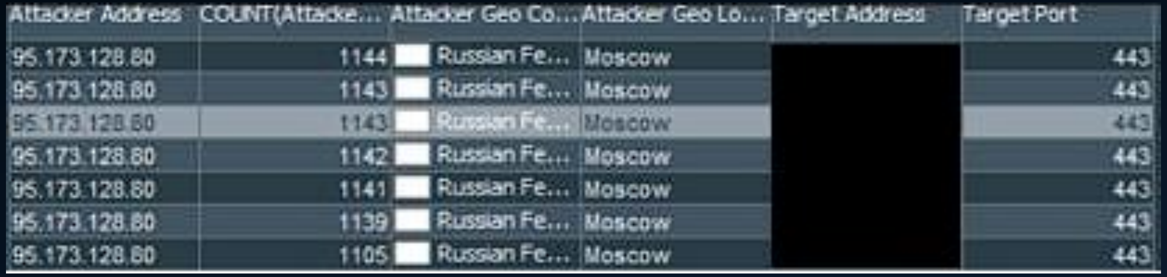
6VFV+426 Novonikol'sk, Рязанська область, Росія

Фотографії

The GPS were showing location in Russia

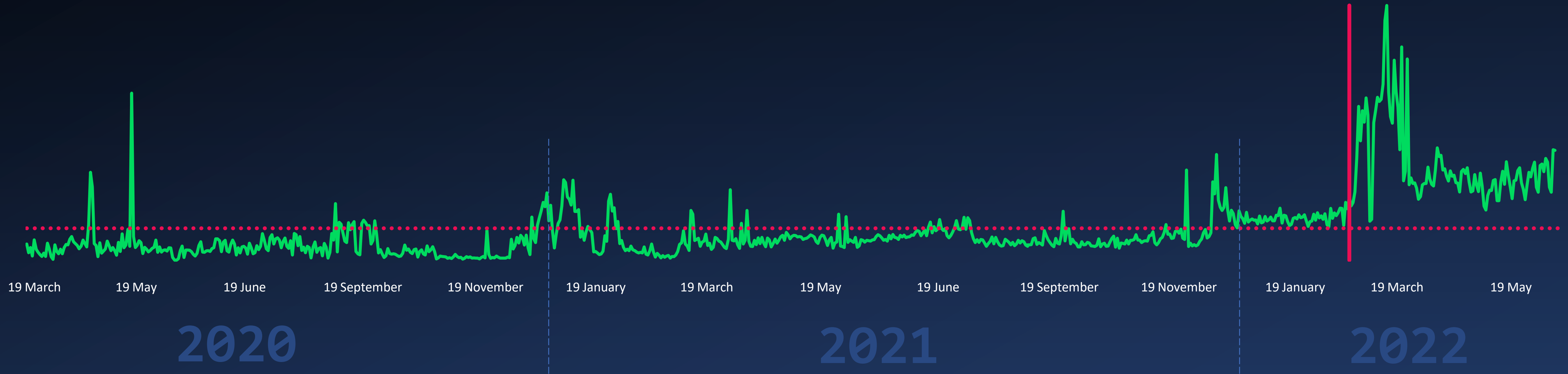
After log-file research, vendor confirmed GPS jamming:
“So, indeed there is a chance to be related to jamming…”

!Do not be afraid of APTs, they are people too and they make mistakes!



Attacker Address	COUNT(Attacke...	Attacker Geo Co...	Attacker Geo Lo...	Target Address	Target Port
95.173.128.80	1144	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1143	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1143	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1142	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1141	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1139	Russian Fe...	Moscow	[redacted]	443
95.173.128.80	1105	Russian Fe...	Moscow	[redacted]	443

ISP	The Federal Guard Service of the Russia Federation
Usage Type	Military
Domain	gov.ru
Country	Russian Federation
City	Moscow, Moskva



Observation: Numbers

- Total amount of incident related events for first 2 month since Day 1 – > 300 000.

  For 2021 – 900 000 for the whole year.
  This year, before Feb 15th – 42 000.

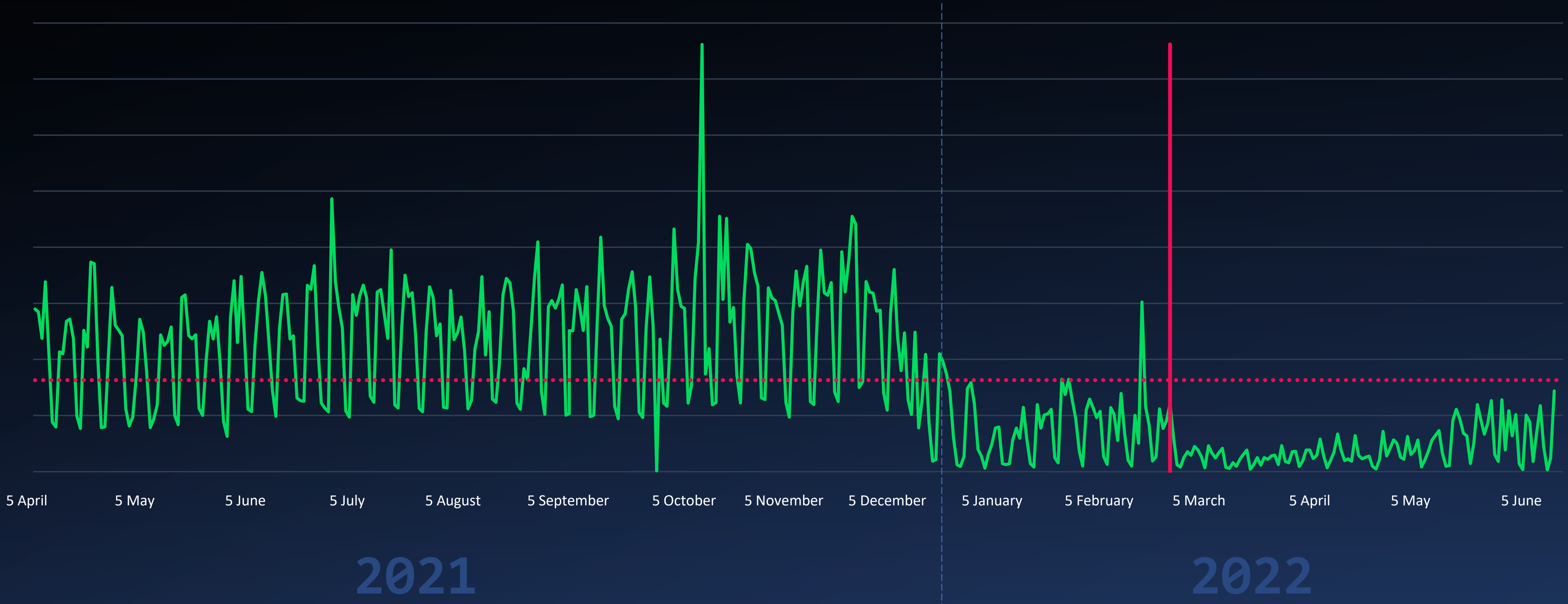
- Total number of DDoS attacks from Day 1 is more than 50.
  For comparison: just 5 attacks were detected for last 3 years before the invasion

- Since Day 1, there are 13 incidents were escalated for sharing through Malware Information Sharing Platform & Threat Sharing “Ukranian Advantage”, total amount for this year so far – 19. The total number for last year – 31.

- The workload of cybersecurity personnel and work hours are doubled since Feb 24th.

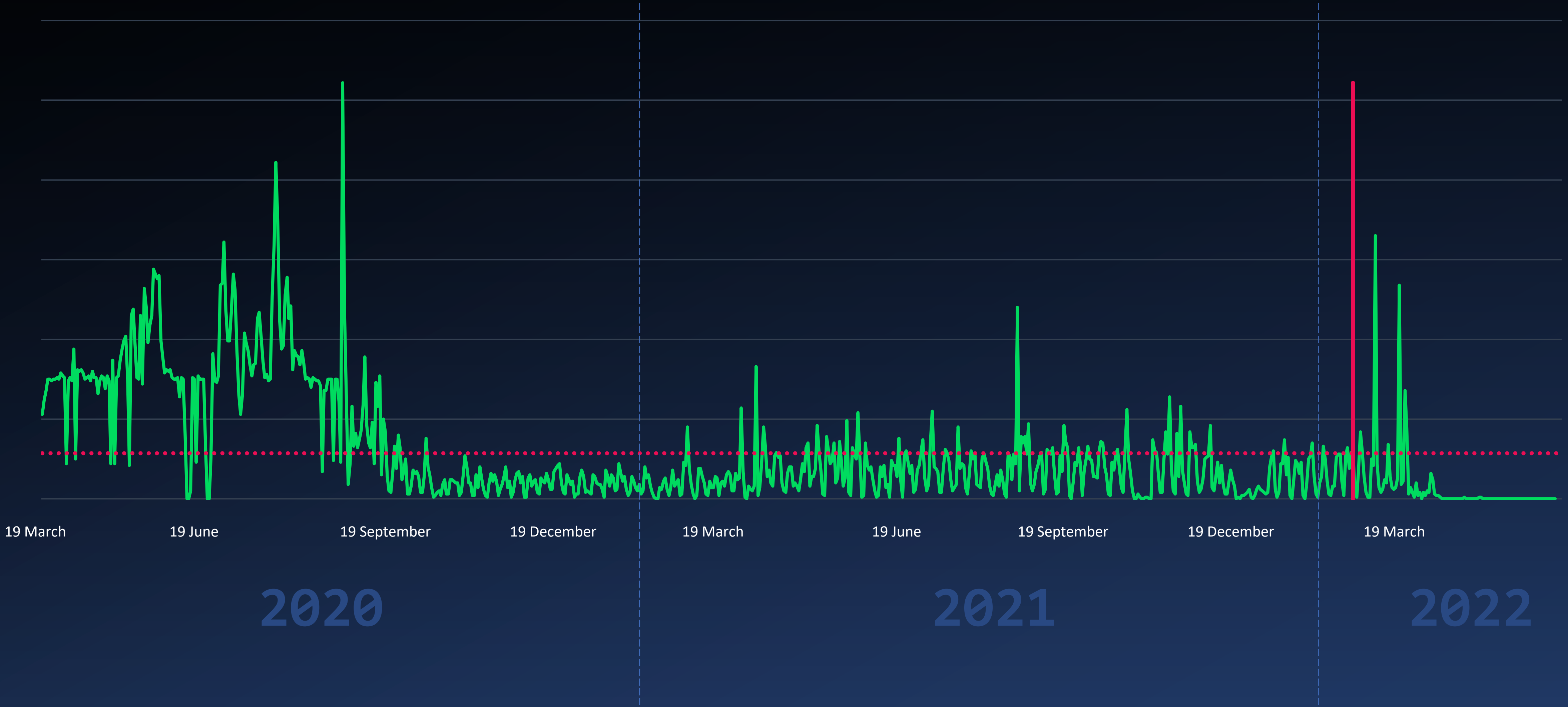
Observation: Statistics

Spam attempts decreased



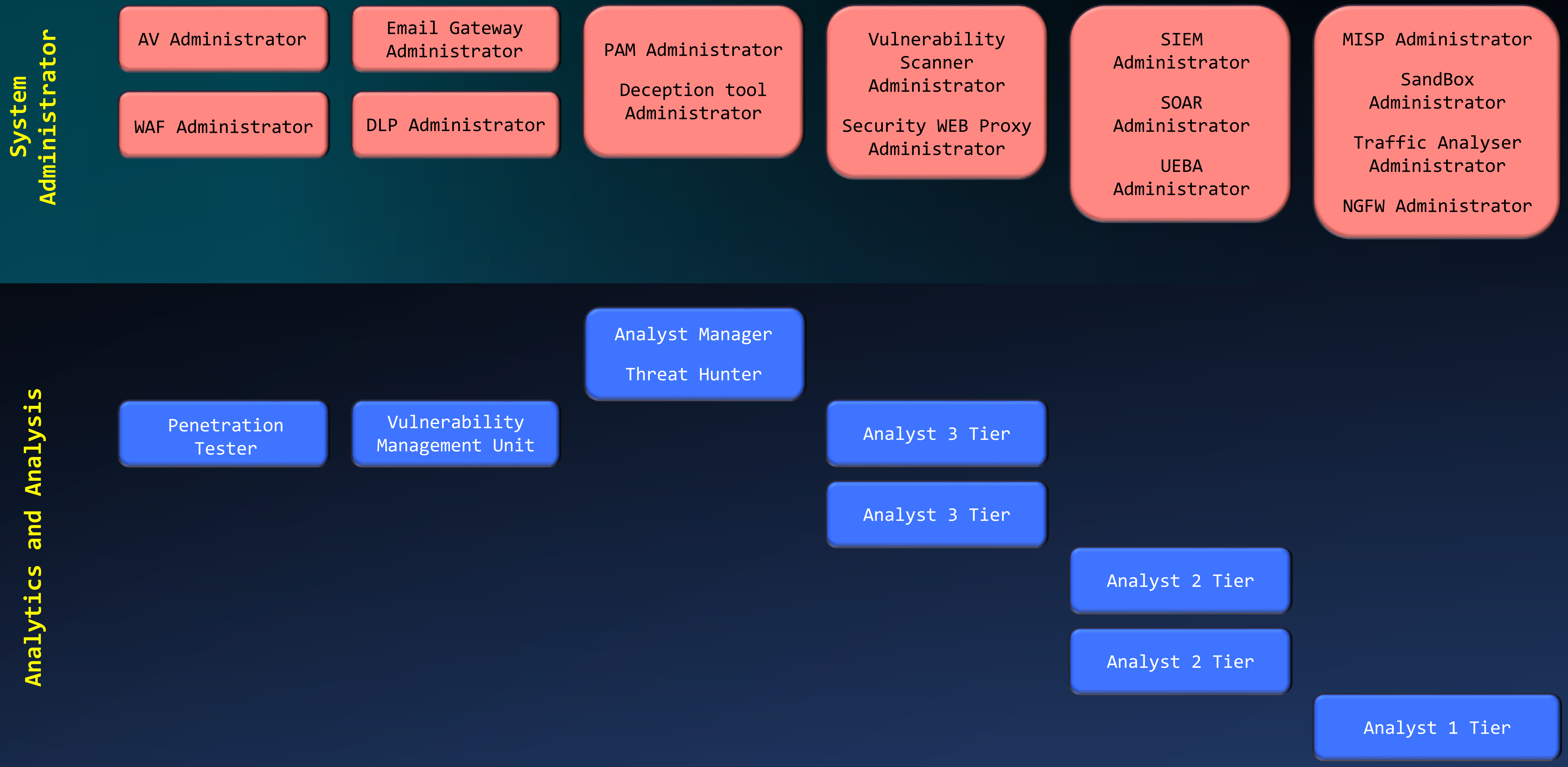
Observation: Statistics

The attempts to send a malware did not stop but amount is vary



How did we manage to resist?

Security operations center



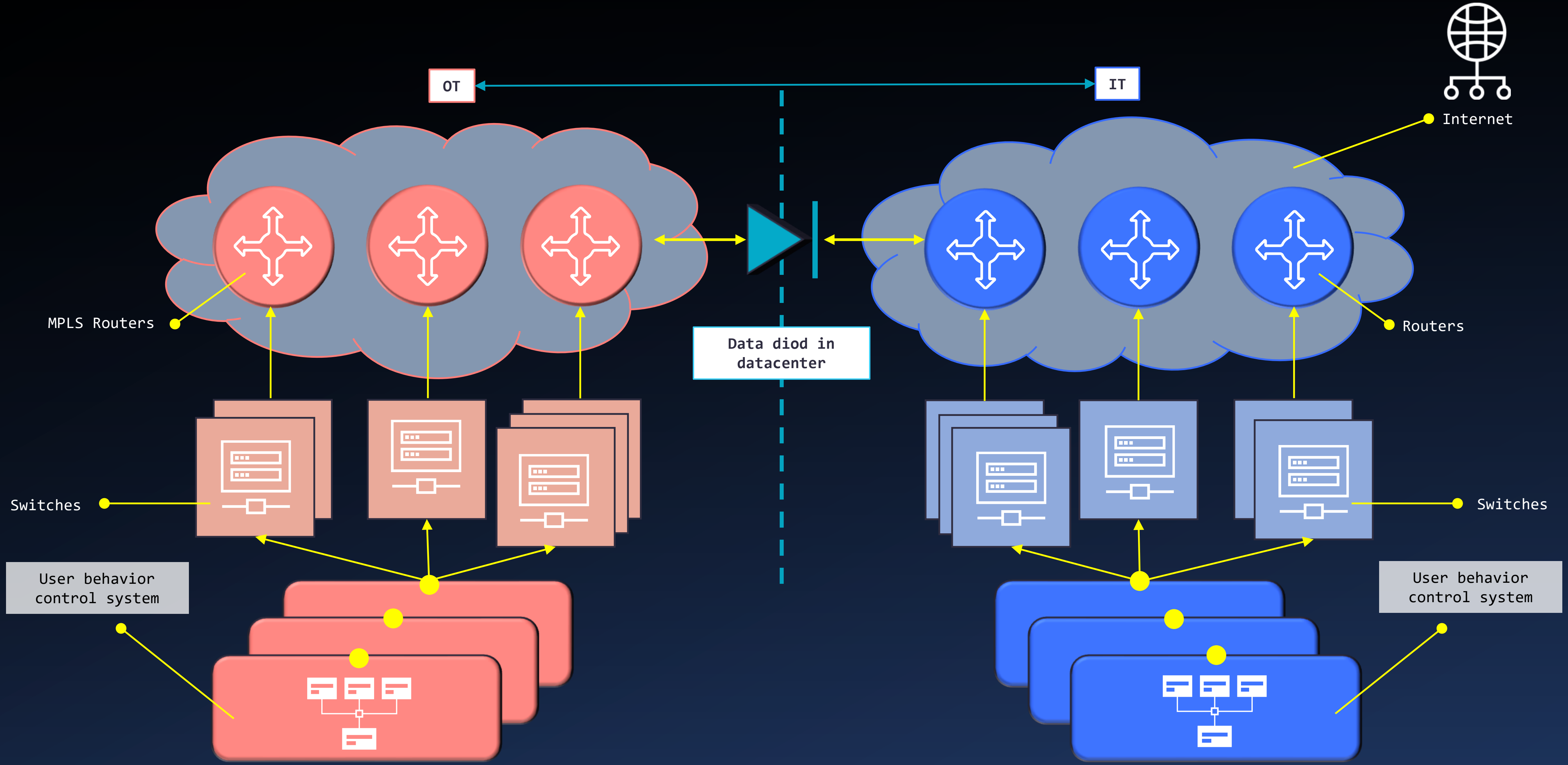
System Administrator

- AV Administrator
- WAF Administrator
- Email Gateway Administrator
- DLP Administrator
- PAM Administrator
Deception tool Administrator
- Vulnerability Scanner Administrator
Security WEB Proxy Administrator
- SIEM Administrator
SOAR Administrator
UEBA Administrator
- MISP Administrator
SandBox Administrator
Traffic Analyser Administrator
NGFW Administrator

Analytics and Analysis

- Penetration Tester
- Vulnerability Management Unit
- Analyst Manager
Threat Hunter
- Analyst 3 Tier
- Analyst 3 Tier
- Analyst 2 Tier
- Analyst 2 Tier
- Analyst 1 Tier

Infrastructure



OT

IT

Internet

MPLS Routers

Routers

Data diod in datacenter

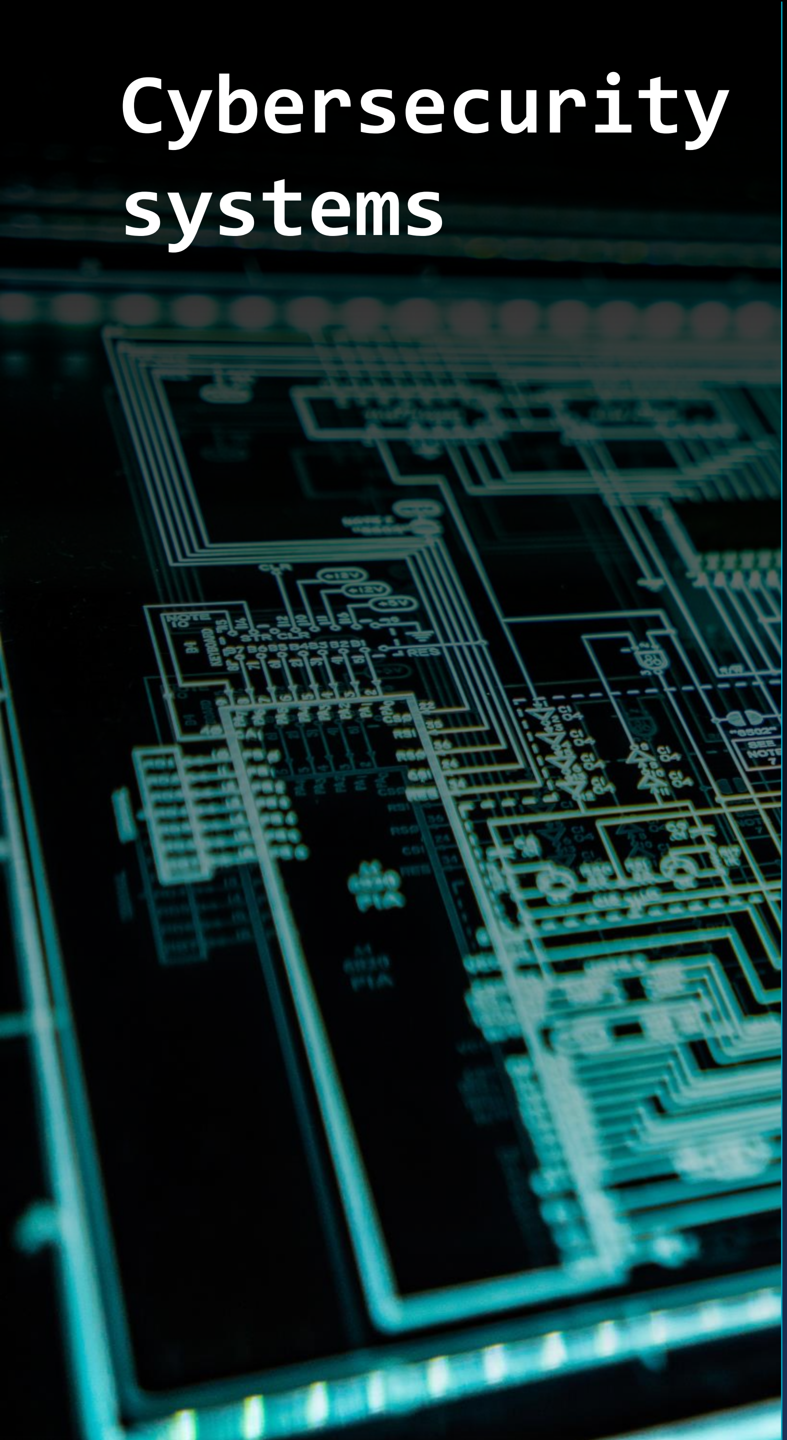
Switches

Switches

User behavior control system

User behavior control system

Cybersecurity systems



PERIMETER	DMZ	INTRANET	SOC
		🔵 NAC	
	🔵 Deception	🔵 PAM	🔵 MISP
🔵 NGFW	🔵 Security WEB Proxy	🔵 Patch Management	🔵 SIEM
🔵 DDoS Protection	🔵 Email Gateway	🔵 Vulnerability Scanner	🔵 UEBA
	🔵 WAF (Premise)	🔵 AV	🔵 SandBox
	🔴 WAF (Premise)	🔵 DLP	🔵 SOAR
		🔵 IDS/IPS	🔵 IDM
		🔴 EDR	

🔵 Acquired systems

🔴 “Lend-lease”

Achievements

Certified by German agency “DQS Holding GmbH” as compliant to ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements»

VIP Customer and referent - Microfocus (CyberRes)

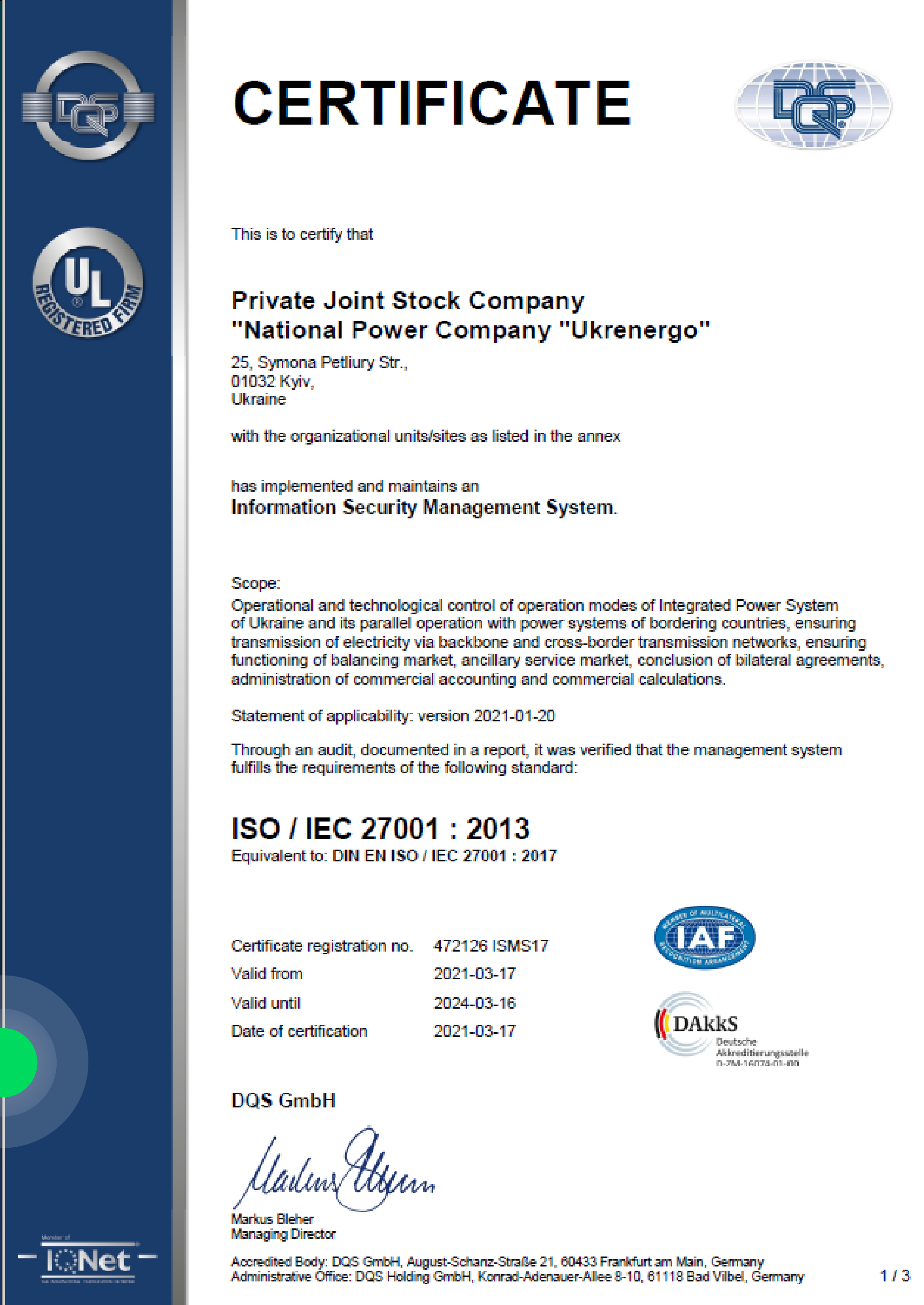
Best installation of Microfocus ArcSight solutions in Ukraine

Good performance on National Hackatons, trainings and competitions

Information sharing with national security agencies and expert cybersecurity teams

https://bit.ly/3O14zXj

https://bit.ly/3xhnq9R



CERTIFICATE

This is to certify that

Private Joint Stock Company
"National Power Company "Ukrenergo"
25, Symona Petliury Str.,
01032 Kyiv,
Ukraine

with the organizational units/sites as listed in the annex

has implemented and maintains an
Information Security Management System.

Scope:
Operational and technological control of operation modes of Integrated Power System of Ukraine and its parallel operation with power systems of bordering countries, ensuring transmission of electricity via backbone and cross-border transmission networks, ensuring functioning of balancing market, ancillary service market, conclusion of bilateral agreements, administration of commercial accounting and commercial calculations.

Statement of applicability: version 2021-01-20

Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:

ISO / IEC 27001 : 2013
Equivalent to: DIN EN ISO / IEC 27001 : 2017

Certificate registration no.	472126 ISMS17
Valid from	2021-03-17
Valid until	2024-03-16
Date of certification	2021-03-17

DQS GmbH

Markus Bleher
Managing Director

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
Administrative Office: DQS Holding GmbH, Konrad-Adenauer-Allee 8-10, 61118 Bad Vilbel, Germany

1 / 3

Lessons learned

- Infrastructure, people, tools and processes has proven it combat readiness

- There is still a lot to work on in terms of cybersecurity in our infrastructure

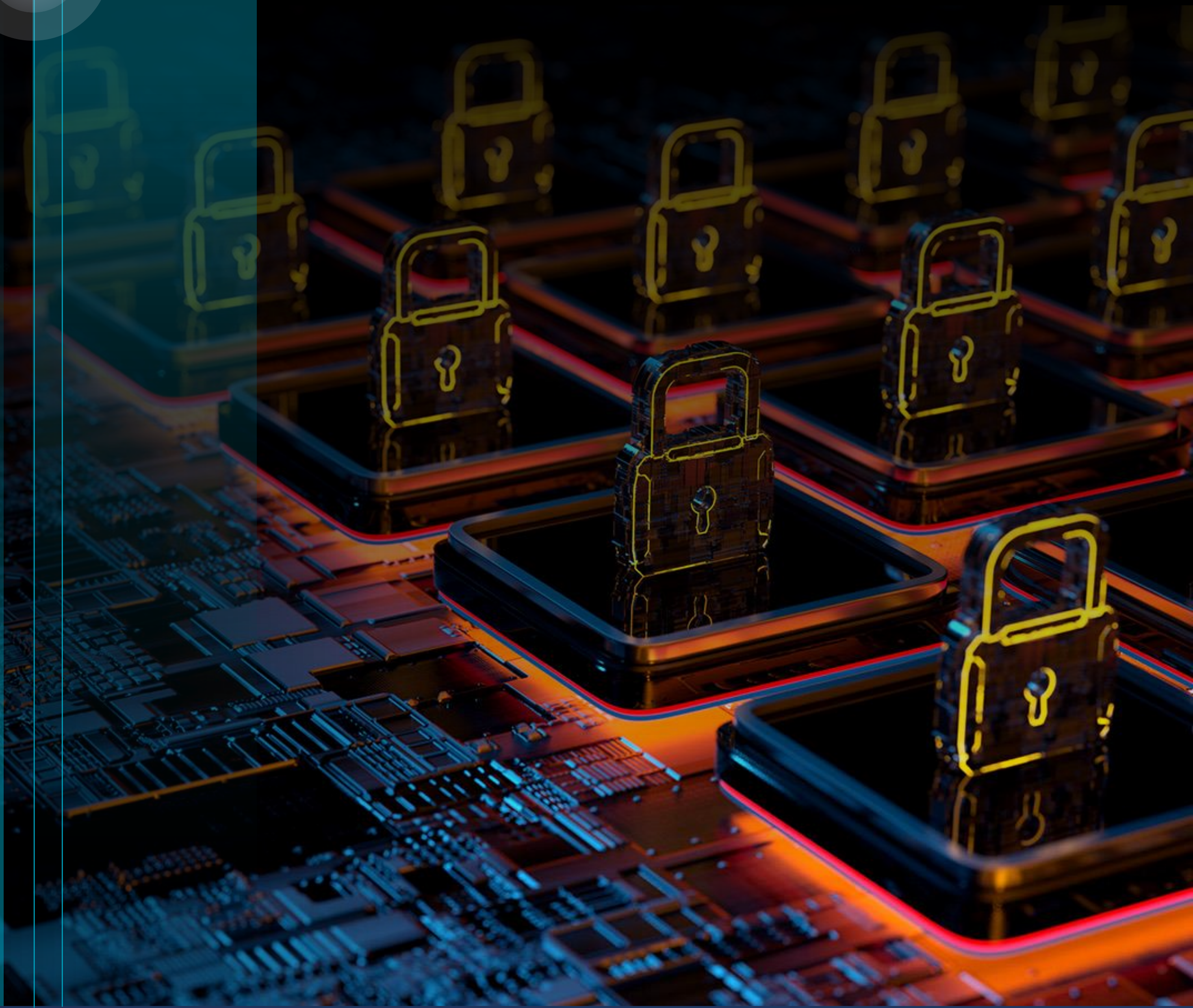
- Our cybersecurity development strategy has proven it’s efficiency so we have to stick to it. Future ICS Security and Data Diodes are very important components

- You got to be ready for any type of targeted attacks, of any power at any time

- Controlled isolation of your resources from outer world can be an option in such difficult conditions and should be considered during business process planning

- Distributed and redundant infrastructure is a key factor of stability

- Every other object in temporary occupied territory or in a war zone has to be considered as lost and zero trust policy has to be applied to it or complete isolation enforced – a new challenge that you should be ready for.



UKRENERGO
National power company

THANK YOU FOR ATTENTION!