Информзащита
Системный интегратор

INFORMZASCHITA

www.infosec.ru

INFORMZASCHITA – group of companies

Информзащита
Системный интегратор

Информзащита
Сервисный центр

Информзащита
Учебный центр

>25 years

On Russia and CIS market

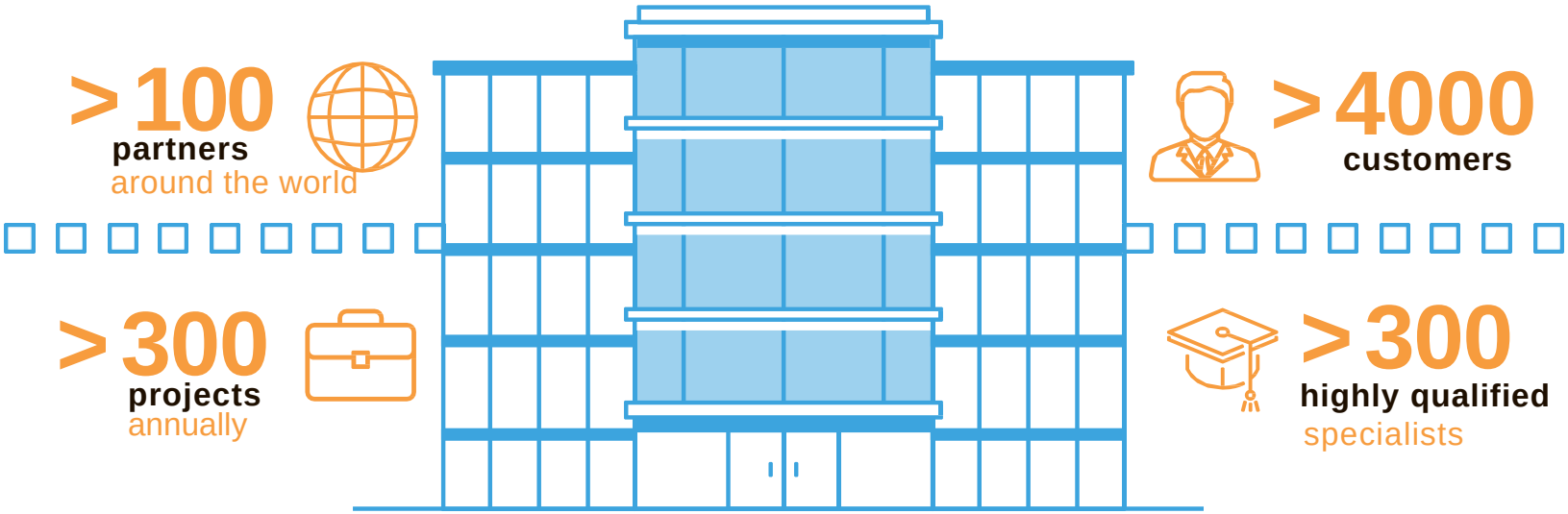
INFORMZASCHITA

25 years on CIS market

TOP-3 Russian CIS-companies

leader

among Russian
information security integrators



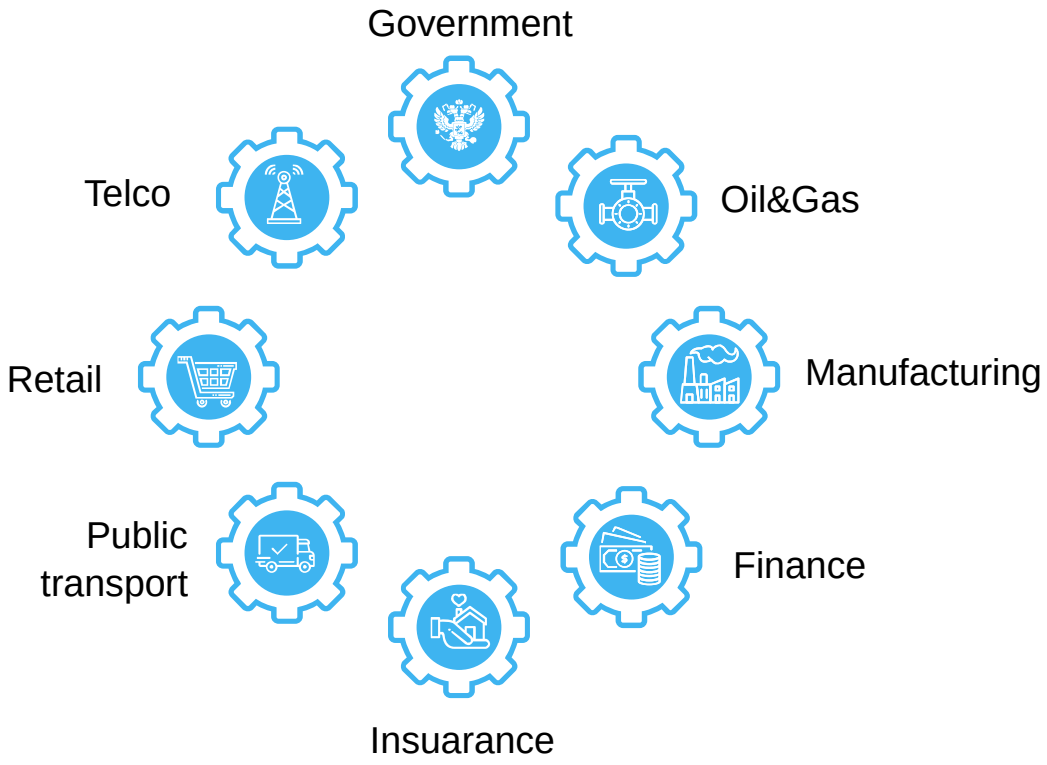
> 100
partners
around the world

> 4000
customers

> 300
projects
annually

> 300
highly qualified
specialists

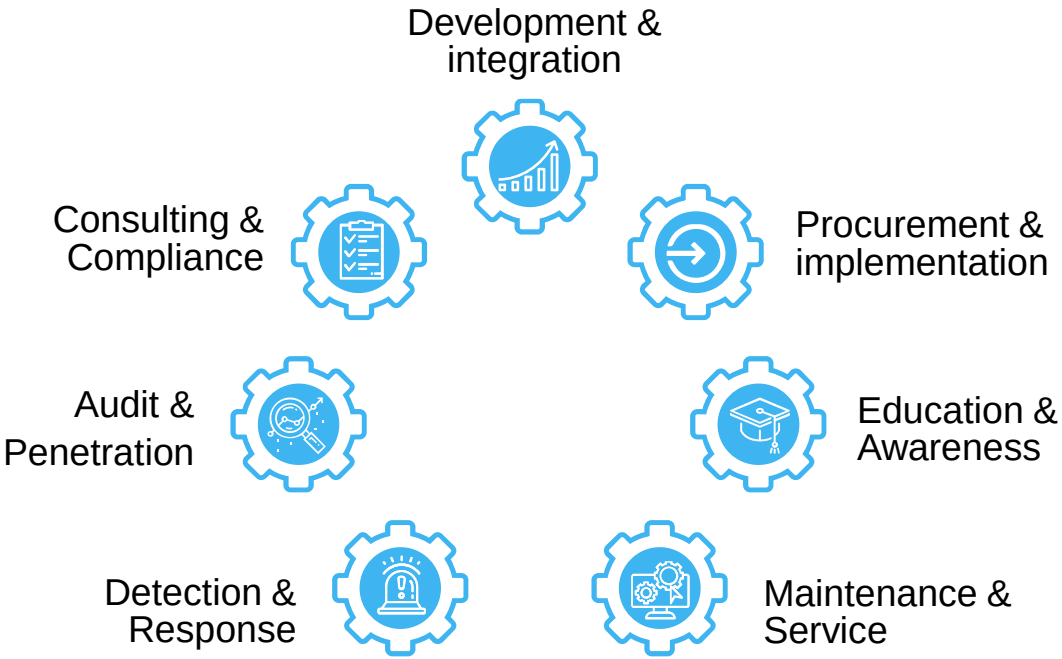
Industry knowledge



Deep knowledge of industry specific business & IT & ICS processes

Our customers

Our offerings



Full set of services for whole Cybersecurity lifecycle

Traditional & MSSP
On premise & Cloud Based

IZ:SOC

MSSP Security Operation Center

- Log handling & storage
- Computer security incident detection & response
- Forensics
- Threat intelligence
- Red team
- Vulnerabilities detection
- IT asset management

IZ:vSOC
Azure Sentinel

Microsoft

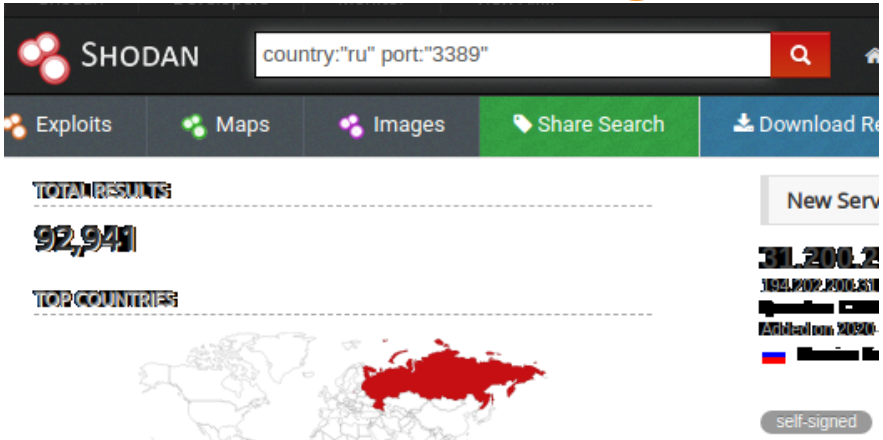
IZ:SOC
IBM qRadar

IBM Silver Business Partner™
Expert
Security Operations & Response

On-site & off-site

- **24x7x365**
- **Dedicated penetration testers team**
- **Automated & Manual tests**
- **Real attack emulation**

Forced teleworking



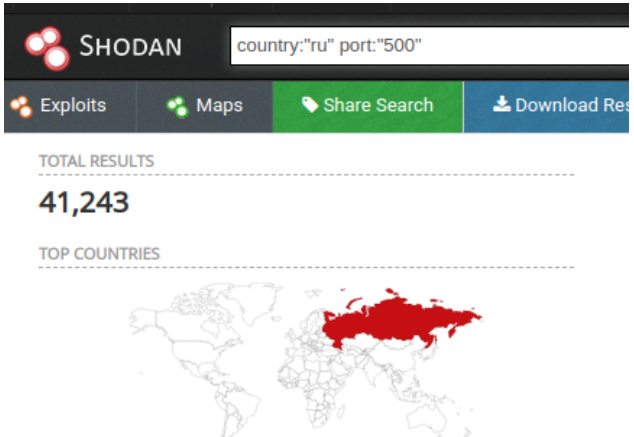
Russian Federation	92,941

TOP CITIES

Moscow	12,998
Saint Petersburg	4,208
Novosibirsk	1,434
Yekaterinburg	1,270
Krasnoyarsk	166

TOP ORGANIZATIONS

Rostelecom	6,609
RUCloud	3,823
OOO Network of data-centers Selectel	3,079
Hosting technology LTD	3,016
JSC Mediasoft ekspert	1,988



Russian Federation	41,243

TOP CITIES

Moscow	8,111
Saint Petersburg	2,878
Yekaterinburg	784
Novosibirsk	628
Nizhniy Novgorod	201

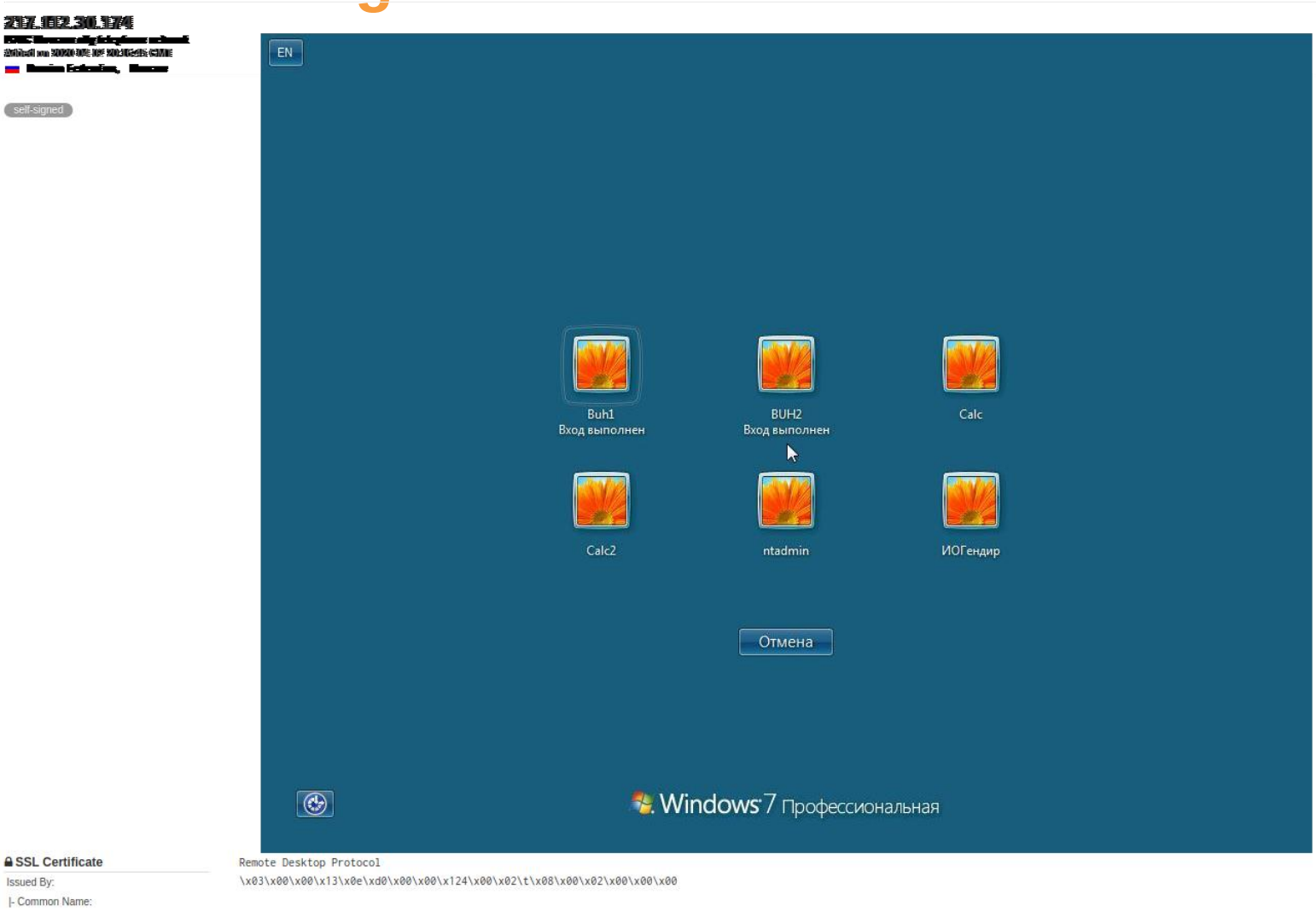
TOP ORGANIZATIONS

Rostelecom	5,167
Interproekt Ltd.	1,691
VimpelCom	1,260
MTS PJSC	611
PJSC MegaFon	483

TOP OPERATING SYSTEMS

Windows 8	412
Windows Server 2008 R2	101
windows	11

Forced teleworking



Forced teleworking

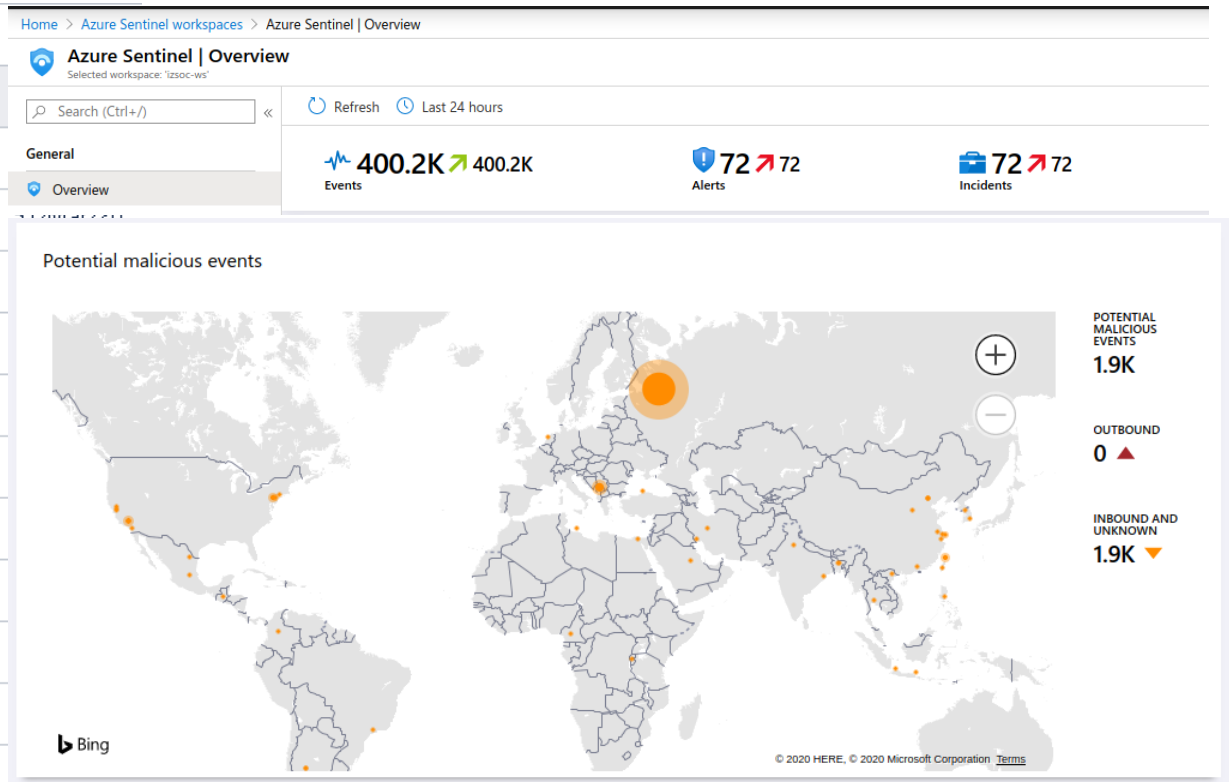
T	Key	Summary	Created
!	TI-45	Обнаружено новое соединение с адресом 104.198.14.52 в списке TI	02/Apr/20 10:44
!	TI-44	Обнаружено новое соединение с адресом 31.31.205.163 в списке TI	02/Apr/20 8:32
!	TI-43	Обнаружено новое соединение с адресом 104.27.131.168 в списке TI	02/Apr/20 7:29
!	TI-42	Обнаружено новое соединение с адресом 104.28.6.46 в списке TI	02/Apr/20 6:09
!	TI-41	Обнаружено новое соединение с адресом 37.140.192.62 в списке TI	02/Apr/20 6:04
!	TI-40	Обнаружено новое соединение с адресом 192.0.78.25 в списке TI	02/Apr/20 3:33
!	TI-36	Обнаружено новое соединение с адресом 216.58.207.206 в списке TI	
!	TI-35	Обнаружено новое соединение с адресом 157.230.120.63 в списке TI	
!	TI-29	Обнаружено новое соединение с адресом 198.185.159.144 в списке TI	
!	TI-28	Обнаружено новое соединение с адресом 195.22.26.248 в списке TI	
!	TI-27	Обнаружено новое соединение с адресом 184.168.131.241 в списке TI	
!	TI-26	Обнаружено новое соединение с адресом 198.185.159.145 в списке TI	
!	TI-25	Обнаружено новое соединение с адресом 67.199.248.10 в списке TI	
!	TI-24	Обнаружено новое соединение с адресом 64.70.19.203 в списке TI	
!	TI-23	Обнаружено новое соединение с адресом 194.87.92.113 в списке TI	
!	TI-22	Обнаружено новое соединение с адресом 104.24.117.35 в списке TI	
!	TI-21	Обнаружено новое соединение с адресом 104.28.25.55 в списке TI	
!	TI-20	Обнаружено новое соединение с адресом 104.28.25.55 в списке TI	02/Apr/20 12:33
!	TI-19	Обнаружено новое соединение с адресом 104.18.43.69 в списке TI	02/Apr/20 12:19
!	TI-18	Обнаружено новое соединение с адресом 104.27.137.80 в списке TI	02/Apr/20 12:16

```
iho@vm-app-03:~/test$ wc dt-covid-19-threat.list.csv
  68766   68766 1432018 dt-covid-19-threat.list.csv
iho@vm-app-03:~/test$ tail dt-covid-19-threat.list.csv
corona-news.com
thecoronavirusdisease.com
coronabeeroutbreak.com
watishetcoronavirus.nl
corona-vaccine.net
coronavirus-in.space
chinesecoronavirus.nl
wuhankuanlu.net
ecoromania.site
coronadelmarchamber.com
iho@vm-app-03:~/test$
```

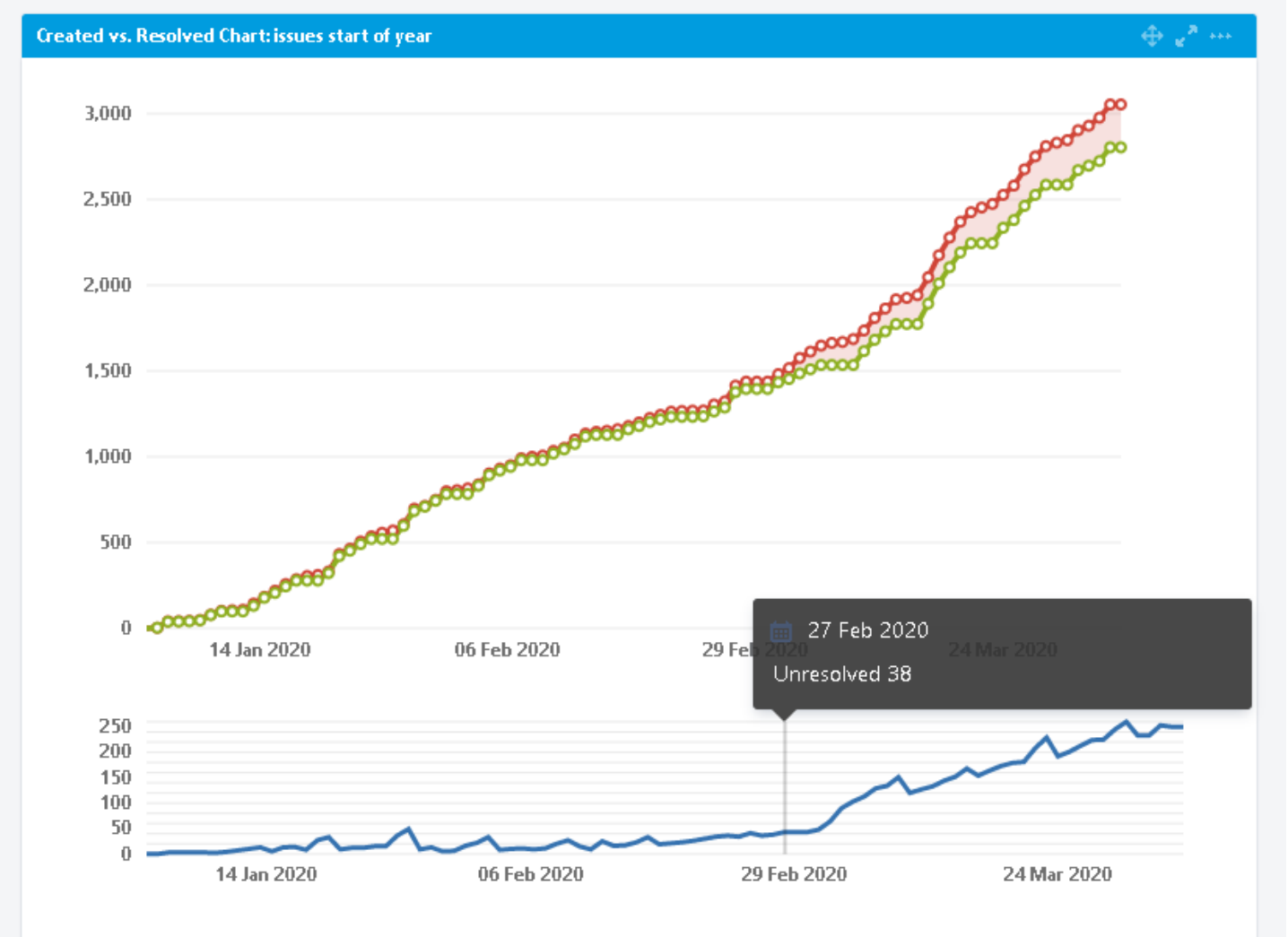
is part of Micros

Forced teleworking

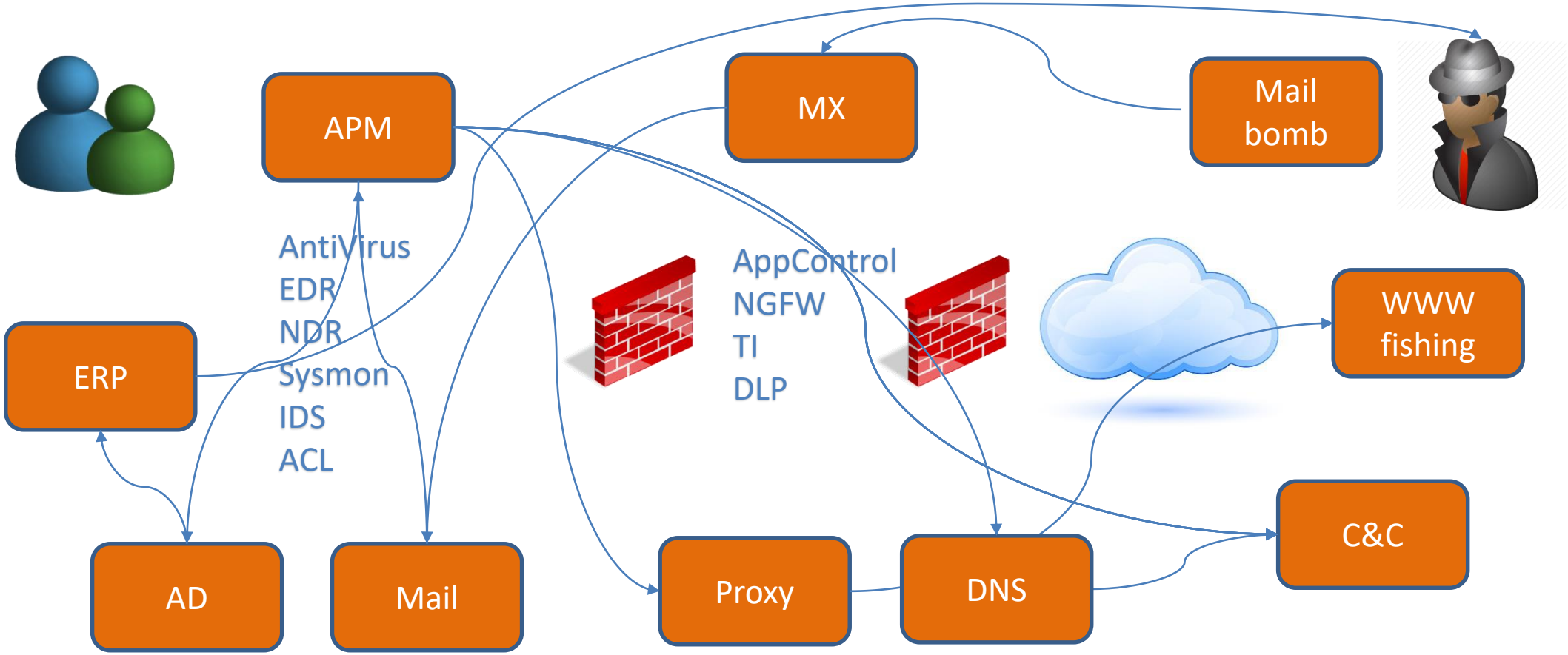
Обнаружен DNS запрос к C&C серверам	
Обнаружен DNS запрос к C&C серверам	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Запуск новой службы ранее не замеченной в организации	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Запуск новой службы ранее не замеченной в организации	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	
Обнаружен вирус на хосте	
Обнаружен вирус на хосте	
Обнаружен DNS запрос к C&C серверам	
Обнаружен вирус на хосте	30/Mar/20
Обнаружено вредоносное ПО в нерабочее время	30/Mar/20
Обнаружен DNS запрос к URL, содержащим вредоносное ПО	30/Mar/20



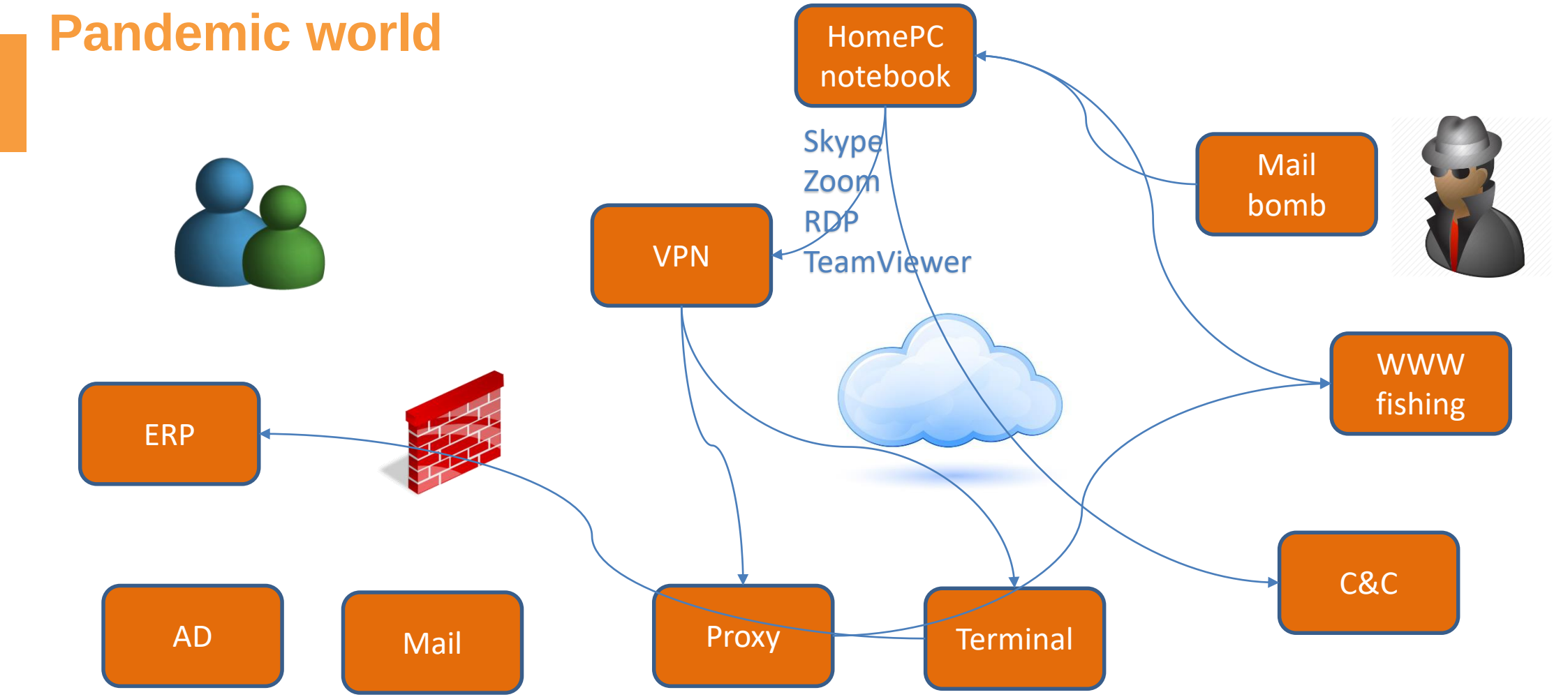
Forced teleworking



Good old days



Pandemic world



Recommendations

- Sprint became marathon
- Finish emergency plan
- Take a breath
- CyberSecurity, CyberSecurity, CyberSecurity …
- Adopt countermeasures and protective gear
- Monitor threats and vulnerabilities
- Ask professional advice
- Use professional services

Информзащита
Системный интегратор

Cyber Security 24x7x365

IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Fraud management
antifraud@infosec.ru

Press office
pr@infosec.ru

System integrator

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Service

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru