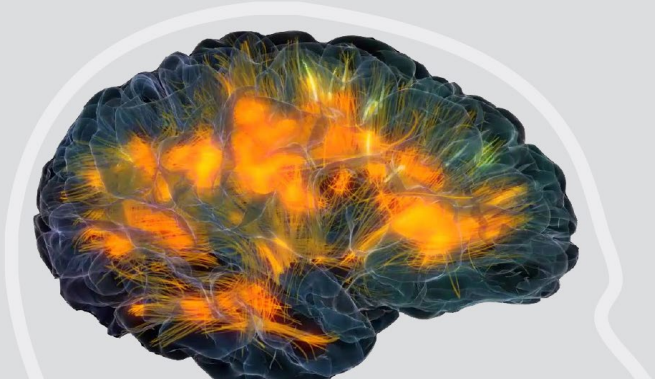
ESET TECHNOLOGY ALLIANCE

GREYCORTEX

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ



GREYCORTEX MENDEL

Моніторинг

Усі мережеві комунікації, пристрої з деталями інвентаризації та поведінка користувачів

Виявлення

Від неправильної конфігурації, проблем із продуктивністю або порушень політик до невиявлених шкідливих програм, програм-вимагачів та дій хакерів, які можуть обійти існуючі засоби безпеки

Реакція

Швидке розпізнавання атак, розслідування та управління інцидентами

+

Моніторинг SCADA/ICS

Моніторинг продуктивності додатків

Інвентаризація активів

KIWI.COM · Česká pošta · meopta EUROPEAN OPTICS | SINCE 1933 · Czech Republic Ministry of Transport · Sąd Apelacyjny w Warszawie · Grupa Żywiec · [redacted] · VD

Network Detection and Response / NDR

Штучний інтелект, машинне навчання, аналіз даних та більш традиційні методи виявлення

GREYCORTEX

ЯК ПРАЦЮЄ ВАШ ЗАХИСТ?

Кіберзлочинність, хакери, програми вимагачі та інші невідомі шкідливі програми

Брандмауери, захист на кінцевих точках

Політики безпеки, відповідність вимогам регуляторів, кращі практики

Захист **BYOD та IoT**

Зашифрований трафік

Network Security Monitoring

Швидко розгортається, простий в управлінні та економічно вигідний

GREYCORTEX

ЩО ВІДБУВАЄТЬСЯ В МЕРЕЖІ?

Неправильні конфігурації
та зміни конфігурації мережі

Продуктивність
програм, пристроїв та мережі

Контроль за поведінкою
працівників та підрядників

Хто з ким взаємодіяв,
з якого приводу, як?

Нові пристрої –
легітимні та ні

Network Visibility & Forensics

Повна прозорість та деталізація всієї мережі

GREYCORTEX

ЩО ВИ ОТРИМУЄТЕ

Виявлення

того, що залишиється прихованим

Можливість вчасно відреагувати

для запобігання втратам

Покращення

стабільності
та захисту мережі

Звіти

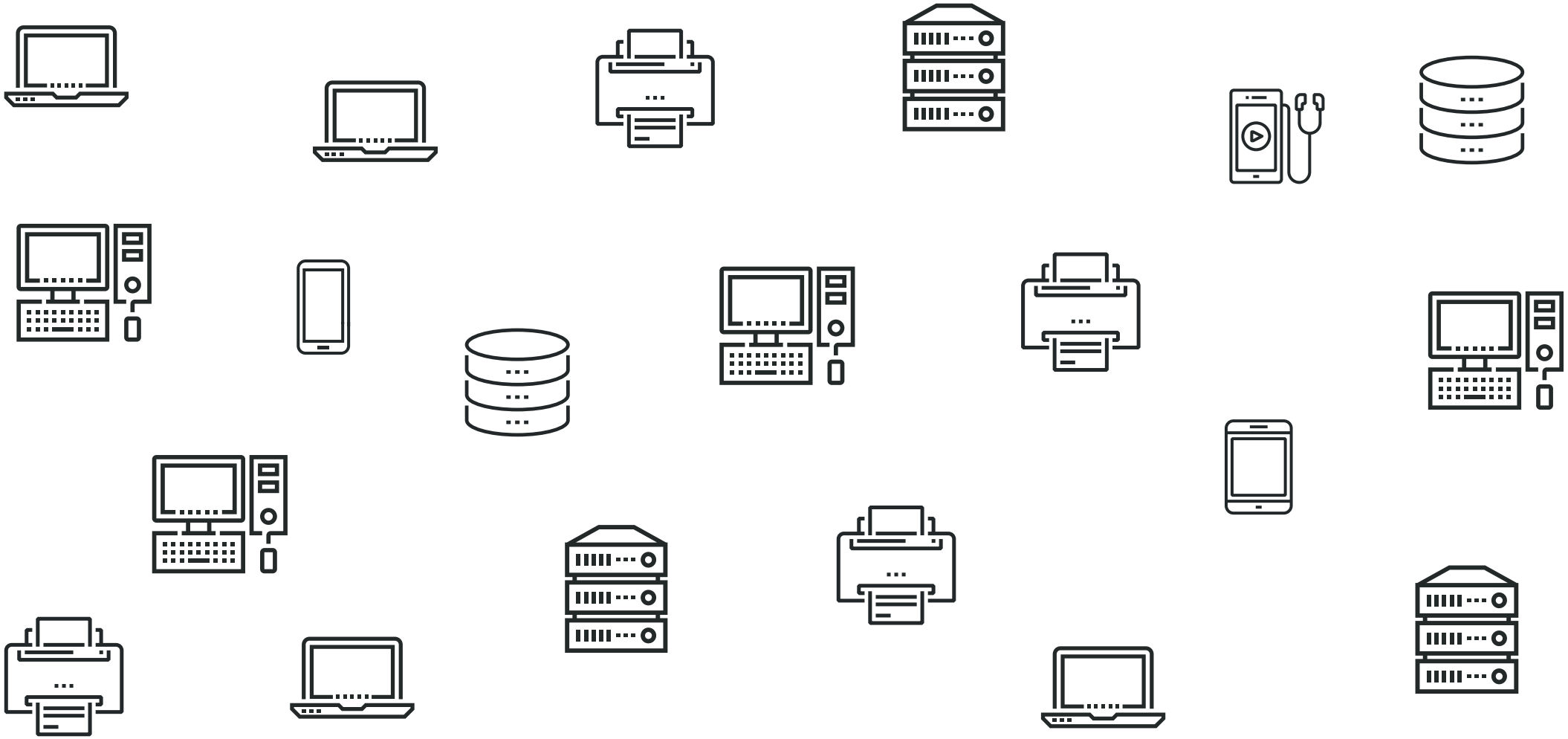
та фіксацію всіх інцидентів та подій

Безперебійне ведення бізнесу

МОНІТОРИНГ + ВИЯВЛЕННЯ + РЕАГУВАННЯ

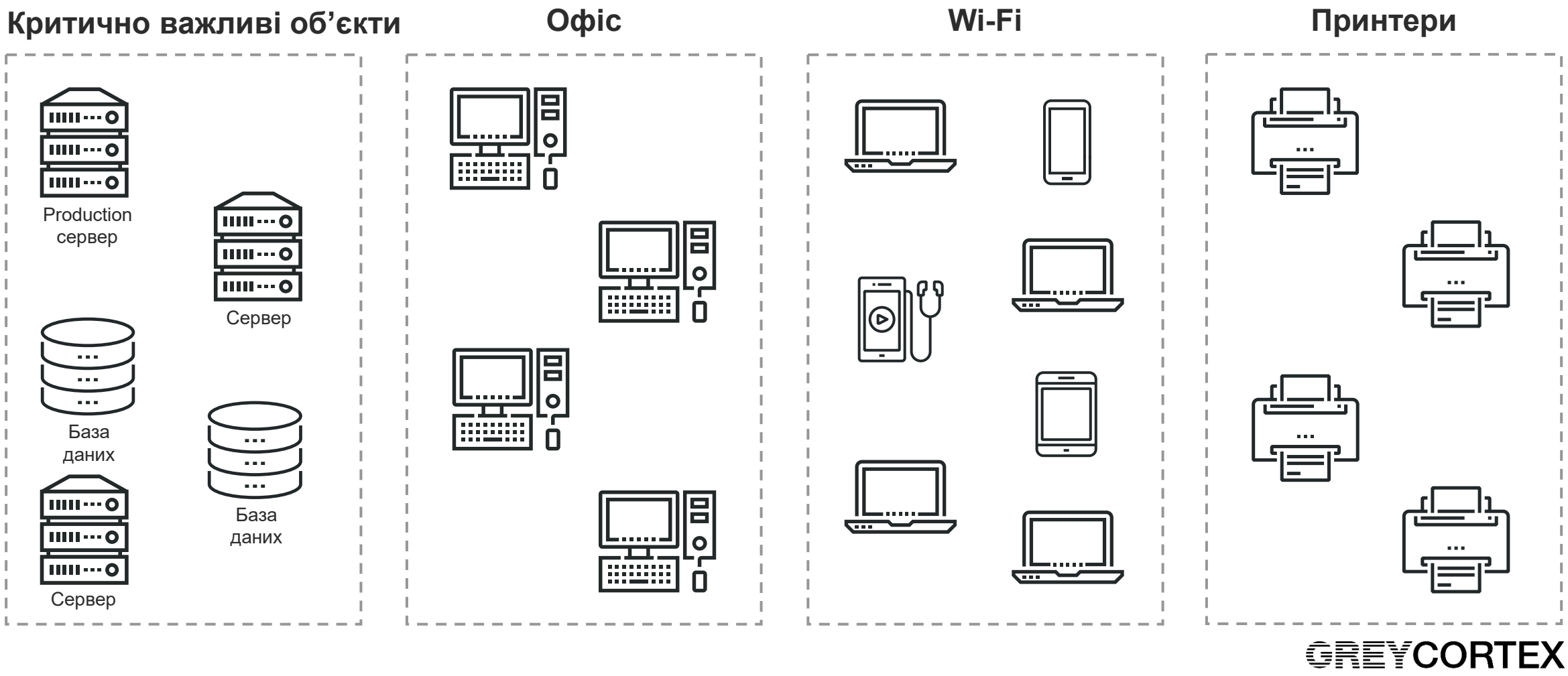
GREYCORTEX

МОНІТОРИНГ



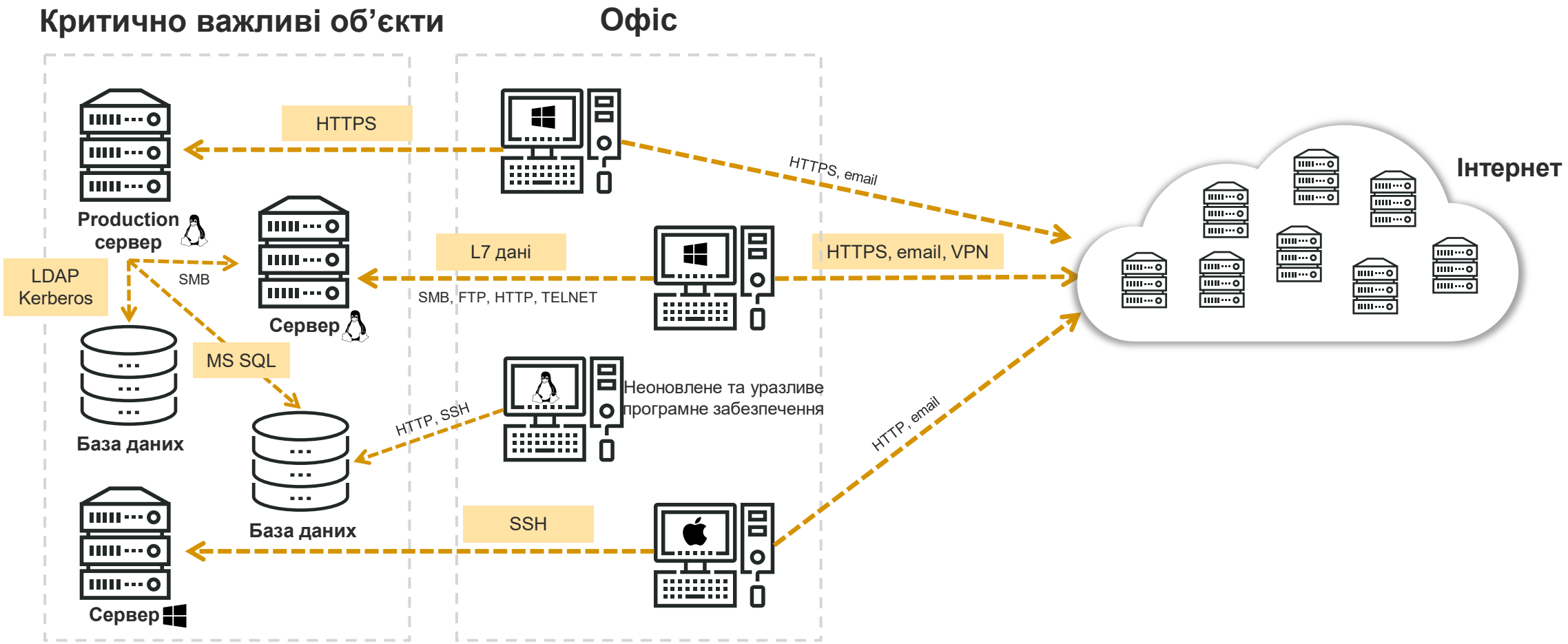
GREYCORTEX

МОНІТОРИНГ



GREYCORTEX

МОНІТОРИНГ



GREYCORTEX

МОНІТОРИНГ МЕРЕЖІ

НАДЗВИЧАЙНА ВИДИМІСТЬ

Фільтрація та відображення будь-яких даних у режимі реального часу

Хто з ким взаємодіяв, як та коли…

Безпека + оперативні події та інциденти з повним контекстом

Простий аналіз першопричин

Швидке виявлення загроз

Усунення проблем в мережі

КРАЩІ АНАЛІТИЧНІ МЕТОДИ

Унікальне сховище для бази даних

Повна та послідовна фільтрація та візуалізація даних

Фільтрація окремих підмереж, хостів, пристроїв та додатків у мережі

Широкі варіанти аналізу поведінки користувачів, пристроїв тощо

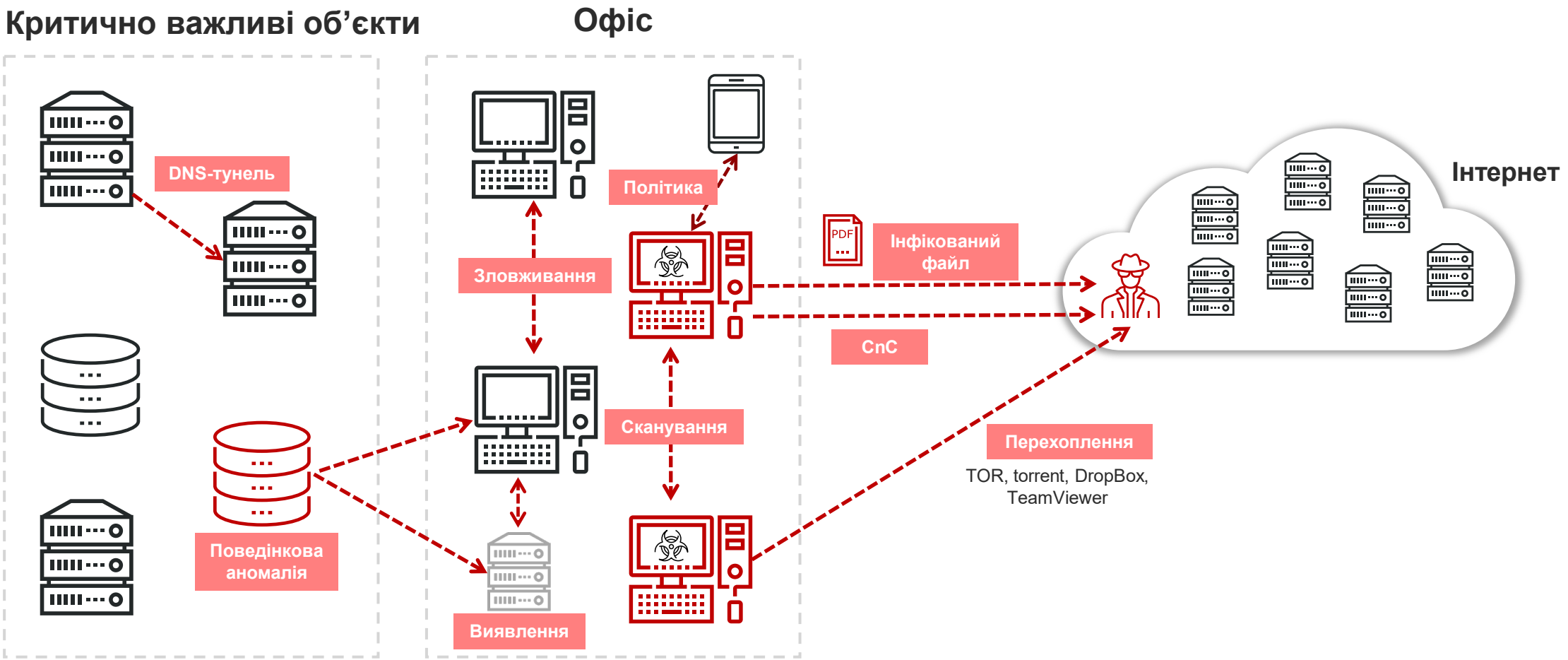
Унікальний набір метрик мережі

Двонаправлені потоки з 60 – 900 параметрами

Детальна видимість від L2 до L7 для десятків протоколів

GREYCORTEX

ВИЯВЛЕННЯ



GREYCORTEX

ШВИДКЕ ВИЯВЛЕННЯ

ІНЦИДЕНТИ БЕЗПЕКИ

Інфіковані пристрої, шкідливі програми, трояни, спроби витоку даних, атаки…

ПОРУШЕННЯ ПОЛІТИК

ISO27000, PCI DSS, GDPR, внутрішні політики…

АНОМАЛІЇ

Нетипова передача даних та поведінка користувачів, проблеми з продуктивністю мережі та додатків, дивні з'єднання загалом

МЕТОДИ ВИЯВЛЕННЯ

Найдосконаліше поведінкове виявлення
(за допомогою машинного навчання тощо)

Унікальні алгоритми виявлення
(зокрема й машинної поведінки)

Потужне виявлення на основі сигнатур з DPI
(понад 45 000 сигнатур з оновленнями щогодини)

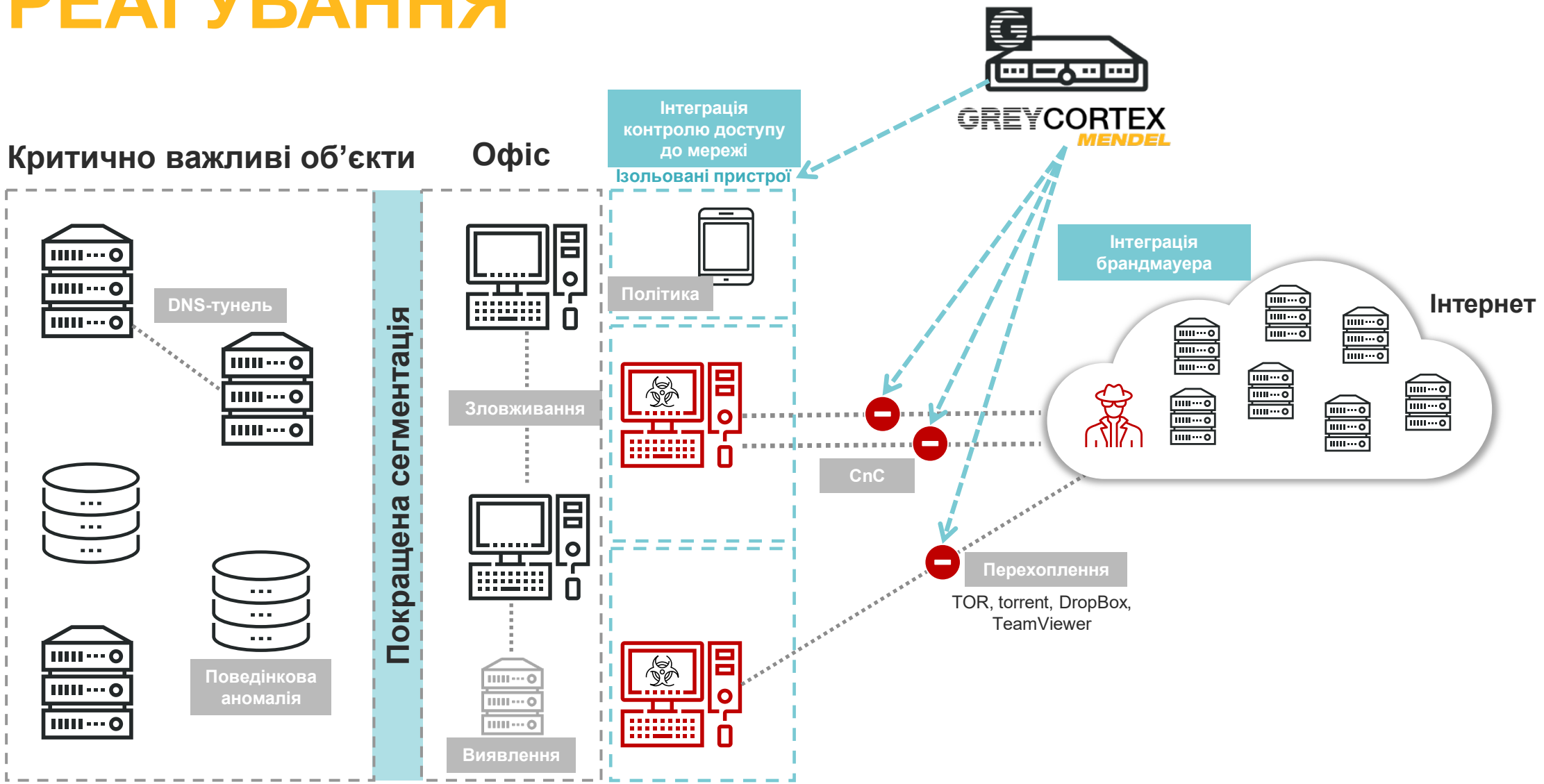
Співставлення подій

L7 аналіз

Аналіз зашифрованого трафіку

GREYCORTEX

РЕАГУВАННЯ



GREYCORTEX

ШВИДКЕ РЕАГУВАННЯ

ПЕРЕШКОДЖАННЯ АТАКАМ

Реагування на атаки в один клік

Завдяки інтеграції з іншою інфраструктурою безпеки

Розслідування інцидентів

Розслідування займає хвилини, а не години

Історію даних за місяці чи роки можна легко проаналізувати

Управління інцидентами

Інтегрований інструмент управління безпекою та взаємодією

ІНТЕГРАЦІЯ

Брандмауер

Fortinet, Palo Alto, Mikrotik, Juniper, Cisco…

SIEM та управління

QRadar, Splunk, Logrythm, Arksight…

Інша інфраструктруа

Консолі управління безпекою робочих станцій, контроль доступу до мережі, Active directory, веб-проксі

GREYCORTEX


Збереження історії
Від 60 до 180 днів за замовчуванням
Резервне копіювання
Від кількох місяців до років
Оновлення
Щогодинні оновлення нових правил виявлення
Ваші дані
Конфіденційність
Усі дані зберігаються локально, а не в хмарі
Нові функції
Важливі оновлення 3 рази на рік

GREYCORTEX

ЯК ЦЕ ПРАЦЮЄ

GREYCORTEX

Date | Time range

May 2019

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Detection methods:

Subnet:

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

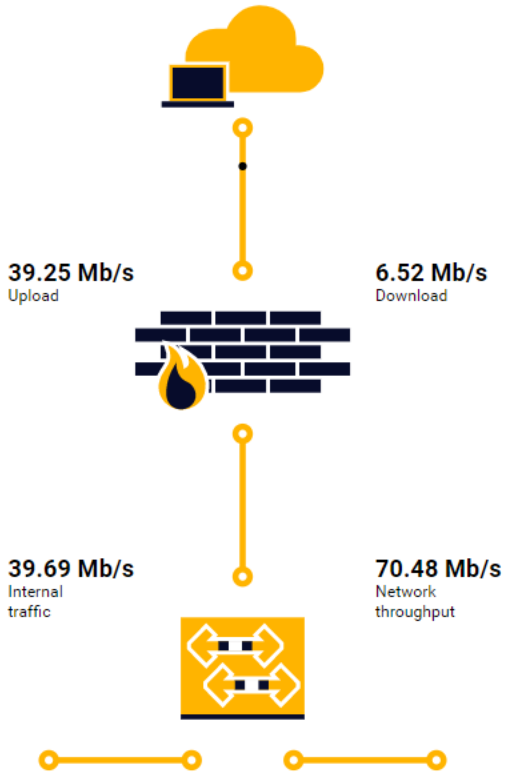
Event:

Severity:

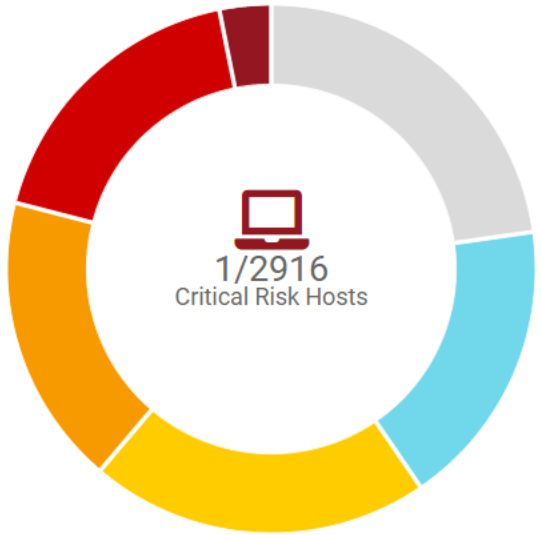
Filter

Clear | Filter Manager

Monitored Network Overview (custom)



Host Risk Overview (custom)



Map of Top Countries by Traffic

Top Hosts by Risk (custom)

Risk	Host	Events
Critical	skadi (10.22.10.124)	57.8 k
High	anhur (10.22.10.107)	24.5 k
High	eddisontollett (fd00:dead:beef:e811:0:48a7:0:3f)	17.6 k
High	siarnaq (10.22.8.124)	8.7 k
High	crios (10.22.10.246)	5.7 k
High	edmure (fd00:dead:beef:e811:0:48a7:0:1129)	5.1 k
High	sepa (fd00:dead:beef:e811:0:48a7:0:9dc4)	3.8 k

Top Users by Events

Risk	User	Events
High	Michelle Harris (mharris_6574)	1
Medium	Ashley Henry (ahenry_2097)	2
Medium	Eric Vega (evega_3527)	1
Medium	Jonathan Waller (jwaller_5446)	1
Medium	Tonya Hess (thess_5365)	1

GREYCORTEX MENDEL

Dashboard | Network | Events | Incidents | Status Monitor

Overview | Performance | Cyber Law | HTTP Dashboard | **Security**

Date | Time range

May 2019

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Detection methods:

Subnet:

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

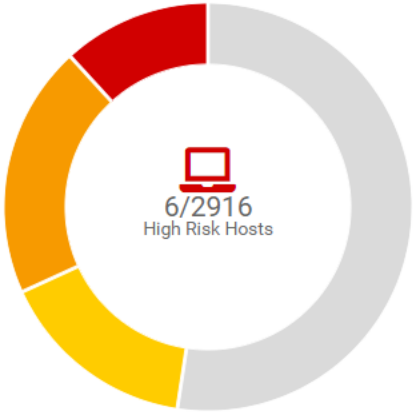
Event:

Severity:

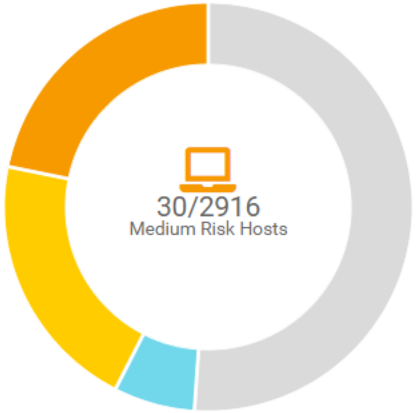
Filter

Clear | Filter Manager

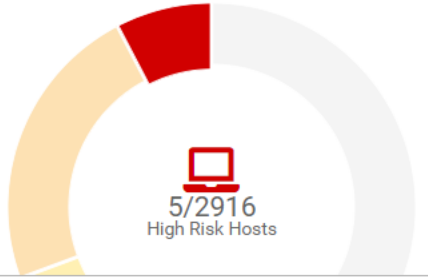
Malware and C&C (custom)



Information (custom)



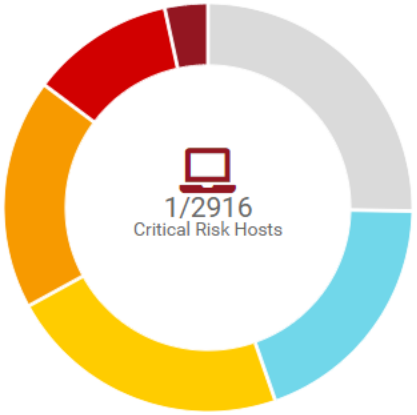
Exploitation (custom)



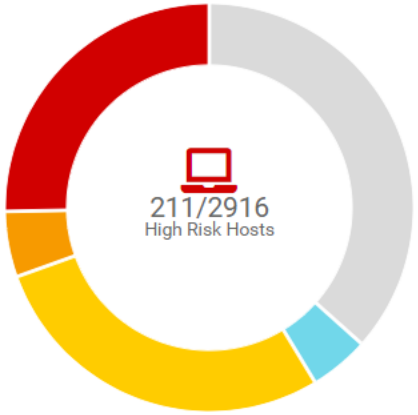
Top events

- shellcode: Hex Obfuscated JavaScript Heap Spray 41414141
- brute-force: Potential DNS Brute-Force attempt
- info: Session Traversal Utilities for NAT (STUN Binding Response)

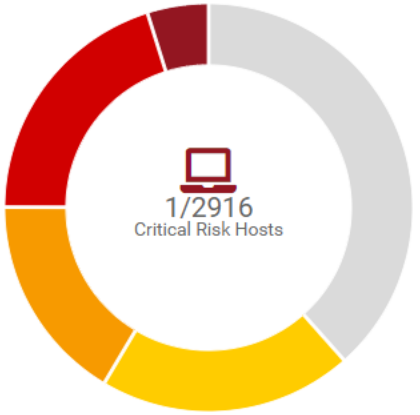
Anomaly (custom)



Reconnaissance (custom)



Policy Violation (custom)



Date | Time range

May 2019

S M T W T F S
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1

Attributes

Predefined filters:

Detection methods:

Subnet:

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

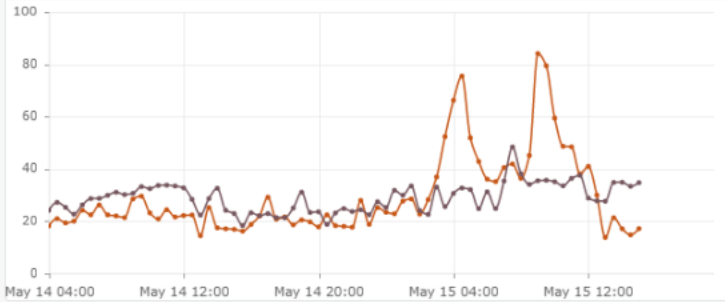
Event:

Severity:

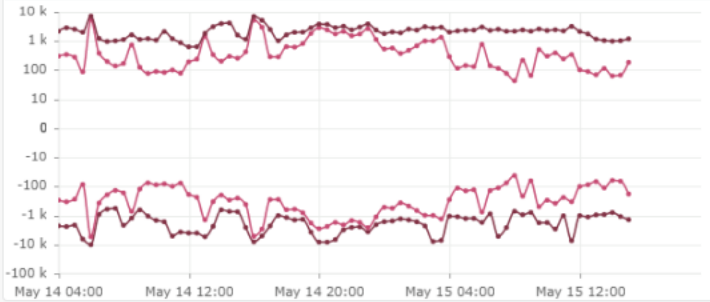
Filter

Clear | Filter Manager

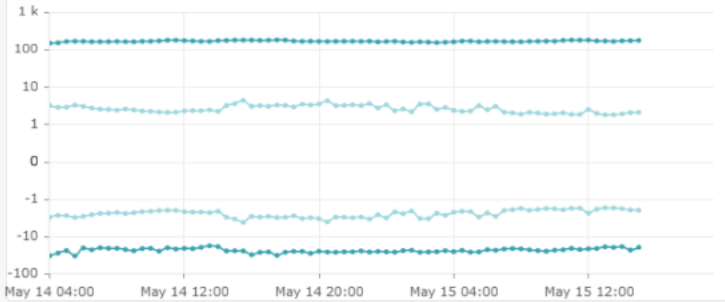
Data Transfer Time



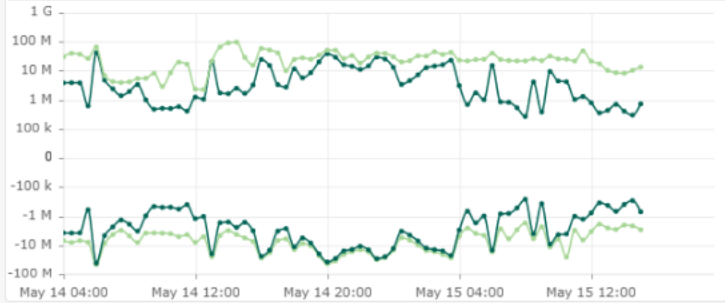
Packets Transfer



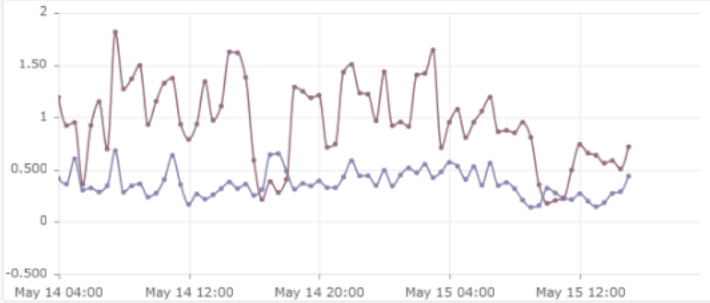
Flows Transfer



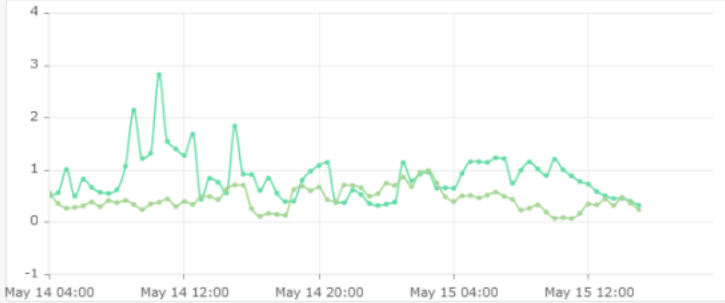
Data Throughput



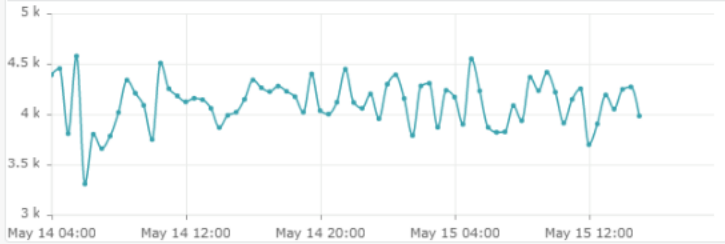
Round Trip Time



Application Response Time



Number of Monitored Hosts



Top Hosts by Traffic

Host	Traffic
seasmoke.greycortex.com (10.22.14.27)	110.77 G
harvest.greycortex.com (fd00:dead:beef:e811:0:48a7:0:3e8)	97.93 G
edmure.greycortex.com (fd00:dead:beef:e811:0:48a7:0:1129)	47.71 G
eurus.greycortex.com (10.22.176.33)	33.66 G
bellerophon.greycortex.com (10.22.10.242)	24.07 G
fd00:dead:beef:4ff0:c97:f0a1:4d8a:fc47	15.08 G
fd00:dead:beef:4f3:c27b:2eed:45b:cb16	14.35 G
kuhn.greycortex.com (10.22.15.195)	10.99 G
buto.greycortex.com (10.22.176.147)	10.0 G
aristotle.greycortex.com (10.22.15.229)	9.86 G

Top Countries by Traffic

Country	Flows	Traffic
France	141.17 k	113.9 G
Czech Republic	153.1 k	97.5 G
Netherlands	56.18 k	58.1 G
Russian Federation	111.39 k	39.8 G
Ireland	105.81 k	13.1 G
United States	696.53 k	12.2 G
United Kingdom	56.44 k	10.0 G
Germany	83.91 k	7.2 G
Poland	24.26 k	6.9 G
Slovakia	19.95 k	4.7 G

Top Services by Traffic

Service	Type	Traffic
HTTPS (443)	LOCAL	134.42 G
Rsync (873)	LOCAL	120.49 G
RTSP (554)	LOCAL	113.36 G
HTTPS (443)	REMOTE	78.03 G
NDL-AAS (3128)	LOCAL	44.93 G
NDL-AAS (3128)	REMOTE	44.92 G
HTTP (80)	REMOTE	28.05 G

Top Hosts by Traffic at Mail Services

Host	Service	Traffic
larissa.greycortex.com (10.22.176.107)	IMAP (143)	3.98 G
larissa.greycortex.com (10.22.176.107)	IMAPS (993)	397.28 M
khons.greycortex.com (10.22.8.224)	IMAPS (993)	294.6 M
fd00:dead:beef:e8d:39d7:4972:9aa3:fb8	IMAPS (993)	81.62 M

Top Hosts by Traffic at Web Services

Host	Service	Traffic
eurus.greycortex.com (10.22.176.33)	HTTPS (443)	28.99 G
kuhn.greycortex.com (10.22.15.195)	HTTPS (443)	10.99 G
buto.greycortex.com (10.22.176.147)	HTTP (80)	10.0 G
aristotle.greycortex.com (10.22.15.229)	HTTPS (443)	9.86 G

Date | Time range

May 2019

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Detection methods:

Subnet: 10.22.176.0/23

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

Event:

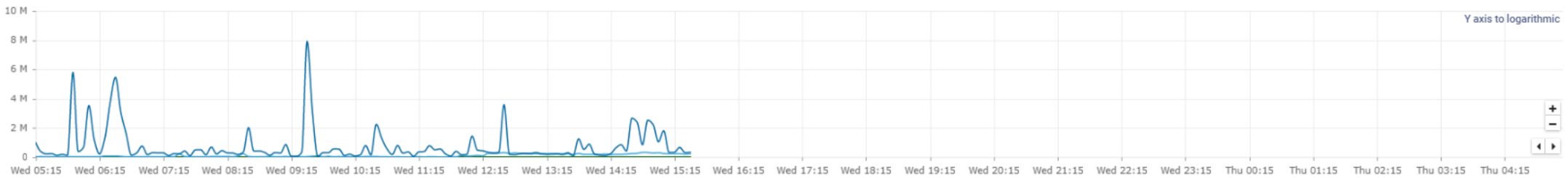
Severity:

Filter

Clear | Filter Manager

Metrics

Flows IN | Flows OUT | Packets IN | Packets OUT | Data IN | Data OUT



Sum | Current value | Model

Manage columns

Sensor	Address	Name	Flows IN	Flows OUT	Packets IN	Packets OUT	Data IN [B]	Data OUT [B]
demo	10.22.177.255	sward.greycortex.com	34	2	54		4.9 k	
demo	10.22.177.254	mholloway.greycortex.com					3.0 k	
demo	10.22.177.253	jpineda.greycortex.com					2.72 k	
demo	10.22.177.252						3.78 k	
demo	10.22.177.251	kek.greycortex.com					12.5 k	10.26 k
demo	10.22.177.250	jedwards.greycortex.com					6.65 k	
demo	10.22.177.249	sevans.greycortex.com					4.63 k	
demo	10.22.177.248	scampbell.greycortex.com					5.09 k	
demo	10.22.177.247	ablackwell.greycortex.com					3.52 k	
demo	10.22.177.246	lwilcox.greycortex.com					4.32 k	
demo	10.22.177.245	sriggs.greycortex.com					6.54 k	
demo	10.22.177.244	lcampbell.greycortex.com					3.21 k	
demo	10.22.177.243	rortega.greycortex.com					6.31 k	
demo	10.22.177.242	hhester.greycortex.com					6.14 k	
demo	10.22.177.241	jjones.greycortex.com					4.62 k	
demo	10.22.177.240	ewalker.greycortex.com					5.79 k	
demo	10.22.177.239	tsimpson.greycortex.com					5.93 k	
demo	10.22.177.238	aether.greycortex.com					4.51 k	
demo	10.22.177.237	khall.greycortex.com					7.45 k	
demo	10.22.177.236	shenry.greycortex.com					5.38 k	
demo	10.22.177.235	codonnell.greycortex.com					3.94 k	
demo	10.22.177.234	kglass.greycortex.com					3.35 k	
demo	10.22.177.233	jchaney.greycortex.com					6.16 k	
demo	10.22.177.232	zrivas.greycortex.com					3.96 k	
demo	10.22.177.231	janderson.greycortex.com					3.85 k	
demo	10.22.177.230	dgutierrez.greycortex.com					4.18 k	
demo	10.22.177.229	rclayton.greycortex.com					3.88 k	
demo	10.22.177.228	shines.greycortex.com					3.53 k	
demo	10.22.177.227	trystramdelyens.greycortex.com					33.58 k	85.41 k
demo	10.22.177.226	jgutierrez.greycortex.com					5.35 k	
demo	10.22.177.225	ahudson.greycortex.com					11.58 k	74.72 k
demo	10.22.177.224	ccruz.greycortex.com	40	4	49		4.12 k	
demo	10.22.177.223	kpatton.greycortex.com	53		64		5.29 k	

Double click to open in services

Host Information

IP: 10.22.177.255 Whois

Hostname: sward.greycortex.com

Subnet: Users (10.22.176.0/23)

Sensor: demo

MAC: 00:04:96:1d:4e:30

Description: None

3rd party info

google.com
ipvoid.com
robtex.com
scumware.org
virustotal.com

Active directory user

Sara Ward (sward_114)

Sara Ward (sward_114)
sara.ward@greycortex.com
GreyCortex s.r.o

Address 1: 5033 Green Underpass Suite 943 Harmonton, ME 09830

Country: Finland

Mobile: (778)957-1759x6522

Job Title: Engineer, building services

To filter | Services | Settings | Close

Date | Time range

May 2019

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Detection methods:

Subnet:

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

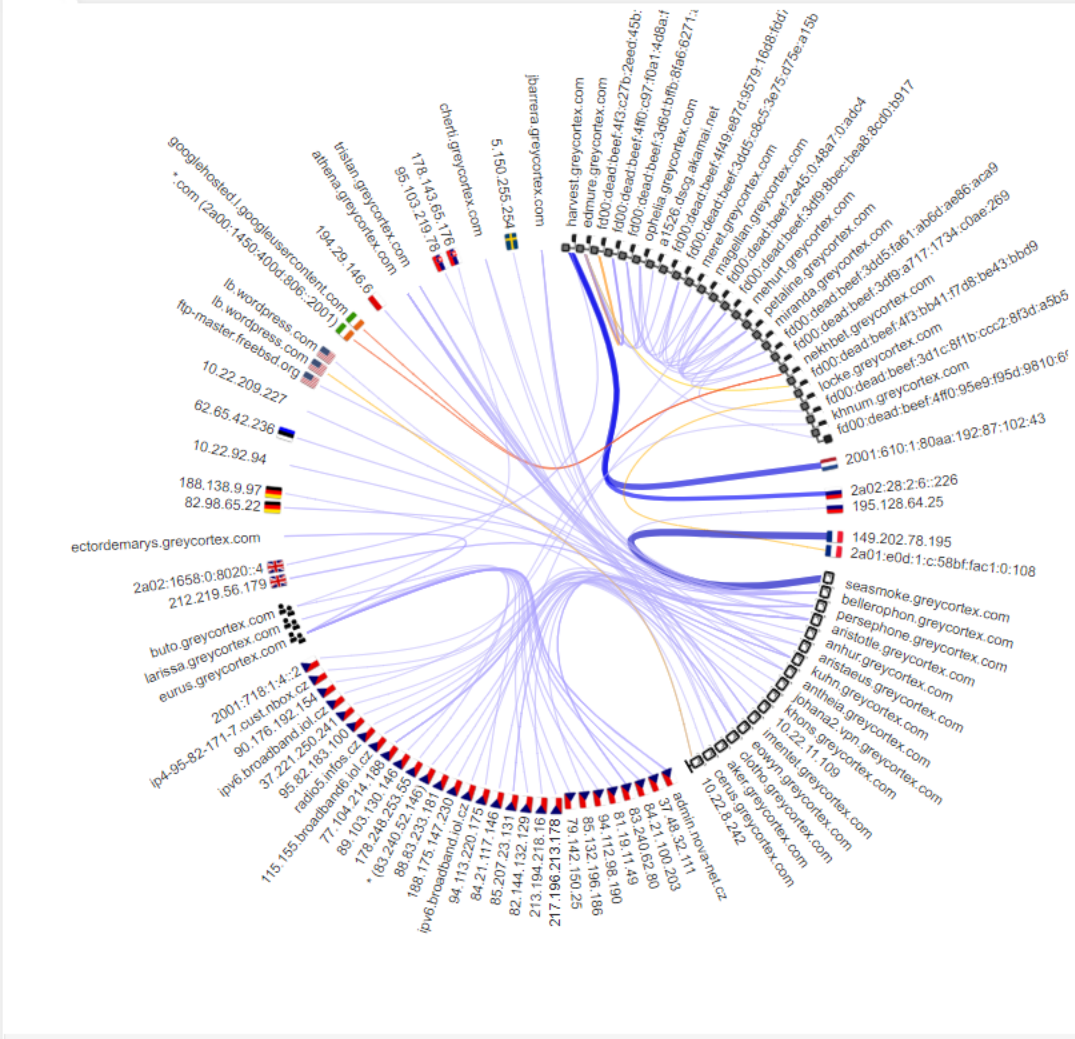
Event:

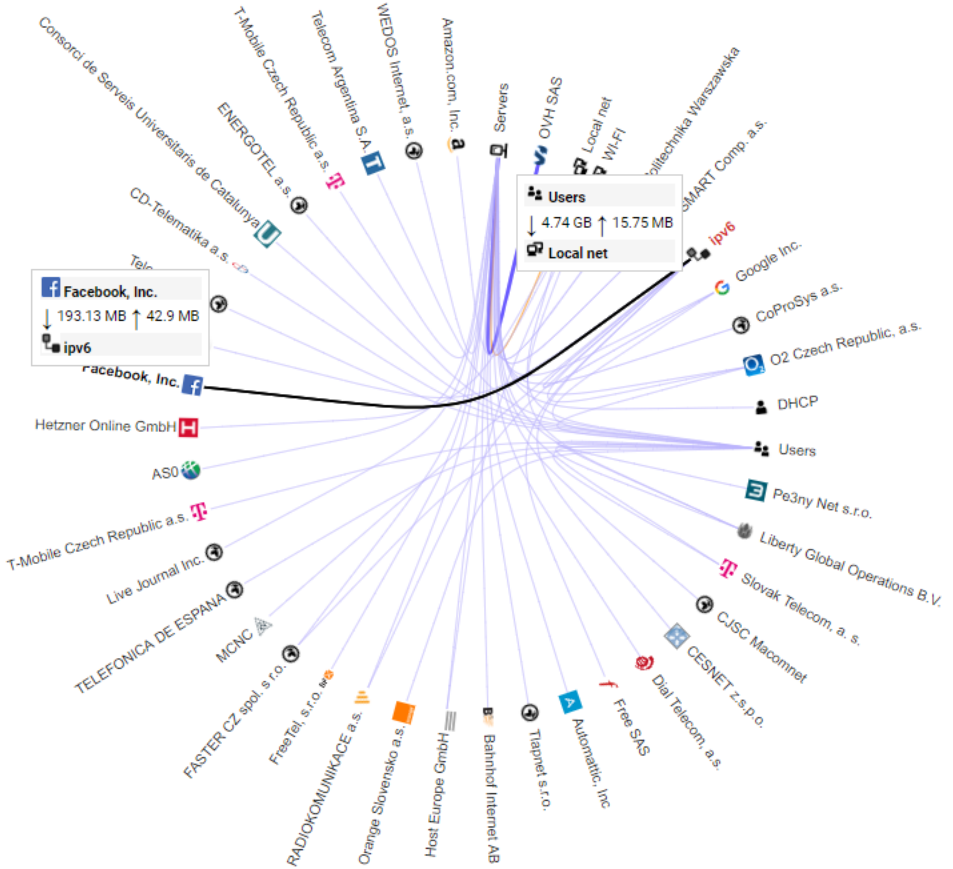
Severity:

Filter

Clear | Filter Manager

Chart | Hosts | Subnets





1 (153+) 50 1 2 3 4

1 (51+) 50 1 2

Date | Time range

May 2019

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

Attributes

Predefined filters:

Detection methods:

Subnet:

Host:

Service:

Service Type:

Protocol:

Traffic:

Country:

Event: trojan

Severity:

Filter

Clear | Filter Manager

Chart | Map

Events

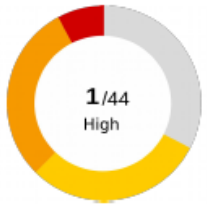
Manage columns

		Name	Src Hosts	Dst Hosts	Events	Date
+	7	trojan: Suspicious User-Agent (MyAgent)	1	1	3	Tue 01:32 – 14:15
+	7	trojan: DNS Reply Sinkhole - Anubis - 195.22.26.192/26	1	1	1	Tue 05:57 – 05:58
+	6	trojan: Single char EXE direct download likely trojan (multiple families)	1	1	2	Tue 01:11 – 07:12
+	6	trojan: MS Terminal Server Single Character Login, possible Morto inbound	1	1	2	Tue 23:50 – 23:51
+	5	trojan: MS Terminal Server Single Character Login, possible Morto inbound	6	4	57	Tue 01:54 – 17:06
+	5	trojan: Linux.Mirai Login Attempt (xc3511)	2	2	2	Tue 08:57 – 12:43
+	5	trojan: Possible Linux.Mirai Login Attempt (1111111)	2	2	2	Tue 09:01 – 09:51
+	5	trojan: Possible Linux.Mirai Login Attempt (7ujMko0admin)	5	5	8	Tue 01:38 – 09:51
+	5	trojan: Possible Linux.Mirai Login Attempt (7ujMko0vizxv)	4	4	4	Tue 05:22 – 17:11
+	5	trojan: Possible Linux.Mirai Login Attempt (888888)	3	2	6	Tue 05:24 – 09:35
+	5	trojan: Possible Linux.Mirai Login Attempt (dreambox)	4	2	4	Tue 08:46 – 19:43
+	5	trojan: Possible Linux.Mirai Login Attempt (ikwb)	1	2	2	Tue 08:46 – 08:48
+	5	trojan: Possible Linux.Mirai Login Attempt (realtek)	3	2	3	Tue 05:21 – 17:10
+	5	trojan: Possible Linux.Mirai Login Attempt (service)	2	2	3	Tue 07:17 – 17:14
+	5	trojan: Possible Linux.Mirai Login Attempt (ubnt)	2	3	6	Tue 05:24 – 09:52
+	5	trojan: Possible Linux.Mirai Login Attempt (vizxv)	4	3	4	Tue 01:37 – 17:12
+	4	trojan: IRC Nick change on non-standard port	1	2	14.0 k	Mon 23:59 – Tue 23:59
+	3	trojan: DNS Reply Sinkhole - Anubis - 195.22.26.192/26	1	1	1	Tue 01:08 – 01:09
+	2	trojan: MS Terminal Server Single Character Login, possible Morto inbound	4	1	104	Tue 01:19 – 23:53
+	2	trojan: Linux.Mirai Login Attempt (xc3511)	3	2	3	Tue 05:20 – 09:48
+	2	trojan: Possible Linux.Mirai Login Attempt (7ujMko0admin)	3	3	4	Tue 08:47 – 17:12
+	2	trojan: Possible Linux.Mirai Login Attempt (7ujMko0vizxv)	1	1	1	Tue 09:49 – 09:50
+	2	trojan: Possible Linux.Mirai Login Attempt (888888)	2	1	4	Tue 08:49 – 09:02

SECURITY REPORT

These graph visualize the number of security events per each of displayed icategories showing the most frequent occurrences with its severity. It can be used to understand the overall levels of threats found in the network over the report period.

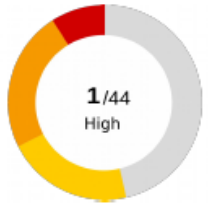
Anomaly



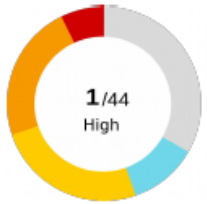
Policy Violation

Malware and CnC

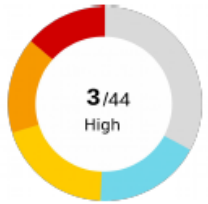
Reconnaissance



Information



Exploitation



GREYCORTEX

CATEGORY: INFORMATION

High

Host: 172.16.42.54
Subnet: floor2 (172.16.42.0/24)

- 7 Domain: Blocked Domain Detected
- 3 Domain: Domain containing Malicious Files Detected
- 1 Policy: GNU/Linux APT User-Agent Outbound likely related to pa...

Medium

Host: 172.16.42.52
Subnet: floor2 (172.16.42.0/24)

- 5 Blacklist: Tor blacklist
- 3 Domain: Domain containing Malicious Files Detected
- 1 Policy: GNU/Linux APT User-Agent Outbound likely related to pa...

Medium

Host: 172.16.42.62
Subnet: floor2 (172.16.42.0/24)

- 5 Blacklist: General blacklist
- 5 Blacklist: Tor blacklist
- 3 Domain: Domain containing Malicious Files Detected

Low

Host: 172.16.42.64
Subnet: floor2 (172.16.42.0/24)

- 4 Domain: Unwanted Domain Detected

Low

Host: 172.16.42.51
Subnet: floor2 (172.16.42.0/24)

- 2 Periodic: SSDP Permanent Multicast Communication

GREYCORTEX

INCIDENT SUMMARY

The Incident Summary displays incidents reported by MENDEL users, and the status of their resolution. Every incident has an assigned risk from the most critical (e.g. company network compromised) to informational (e.g. new device discovered).

RISK	REPORTED	ANALYZED	RESOLVED
CRITICAL	1	0	1
HIGH	0	0	2
MEDIUM	1	3	11
LOW	15	42	121
INFO	0	0	0
TOTAL	17	45	135

AVERAGE RESOLUTION TIME: 21 minutes

GREYCORTEX

GREYCORTEX

3

1. RAT: Machine Communication in Japan

Risk: Critical **Sensor:** Test

Labels: Security

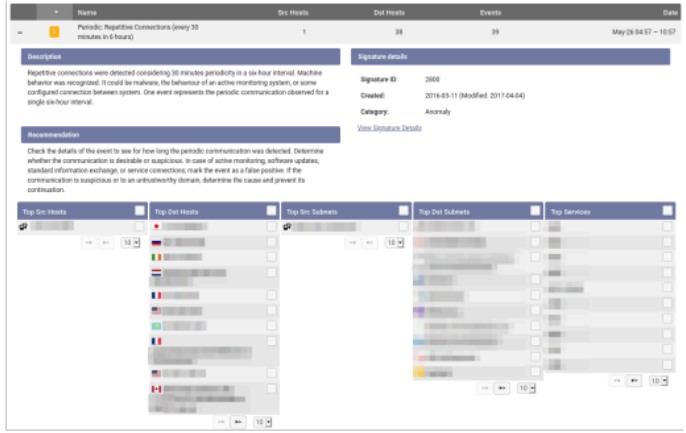
Link: https://mendel.greycortex.com/incidents.xhtml?id=1

Source IP:

- xxx

Finding

This device was detected communicating to Japan and to other atypical countries. Furthermor e, these communications used torrent communications. The device is among others connected to the IP reputation services by TOR.



GREYCORTEX

5

2. Outgoing Portscan on UDP Port 1

Risk: Medium **Sensor:** mendel

Labels: Security

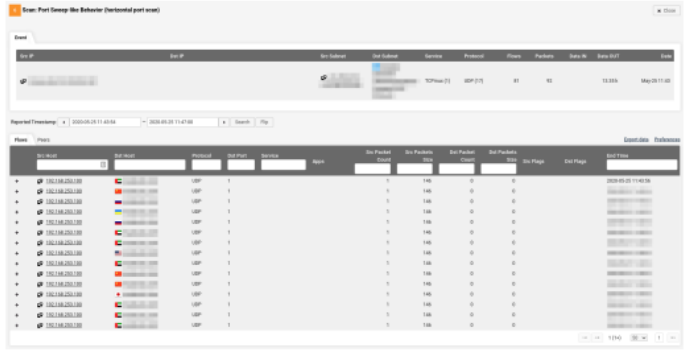
Link: https://mendel.greycortex.com/incidents.xhtml?id=2

Source IP:

- xxx

Findings

The device made several port scans to external addresses to the internet in various countries. It may be a legitimate outdated P2P application or evidence of the presence of malware that tries to contact the parent botnet.



Risk

There is a risk of infection as a device with malware that can cause data loss or damage to reputation. It is especially common in port scanning that the public IP address of the network gets blacklisted it will be seen as hostile.

Recommendation

We recommend an analysis to determine what is causing the activity. The appropriate solution is then to re-install the device.

GREYCORTEX

6

3. Anomalous Amounts of Communication Partners to SMB

Risk: Low **Sensor:** Test

Link: https://mendel.greycortex.com/incidents.xhtml?id=3

Source IP:

xxx

Findings

The device connects to a large number of other stations in the MS Samba protocol on port X, which carries large amounts of data. Such behavior was identified by the NBA engine as an anomaly, because this device communicates with too many communication partners compared to modeled communications.
It may be an audit tool, or anomalous user behavior, or malware.

Risk

If it is not an audit tool, it may be a type of malware (ransomware) which encrypts user connected disks or strange user activity.

Recommendations

Analyze the equipment and check the cause of the behavior.

GREYCORTEX

GREYCORTEX

Dashboard | Sensor Overview | Performance | Security | Network | Events

Map of sensors

Top events

S	Sensor	Name	Hosts	Events
9	moscow	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	4	7
6	paris	blacklist: Tor blacklist	6	12
6	london	blacklist: BotCC blacklist	2	10
6	london	blacklist: Tor blacklist	2	2
6	vienna	blacklist: Tor blacklist	2	2
6	sanmarino	blacklist: Tor blacklist	2	2
6	zagreb	blacklist: Tor blacklist	2	2
5	london	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	159	573
5	london	p2p: BitTorrent transfer	6	57
5	london	p2p: BitTorrent DHT ping request	16	33
5	sanmarino	Periodic: Possible Malware Check-in on HTTP/S	12	32
5	monaco	p2p: BitTorrent DHT ping request	16	31
5	astana	Periodic: Possible Malware Check-in on HTTP/S	16	28
5	monaco	Periodic: Possible Malware Check-in on HTTP/S	11	22
5	monaco	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	6	20
5	sanmarino	p2p: BitTorrent DHT ping request	11	20
5	paris	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	11	19
5	rome	Periodic: Possible Malware Check-in on HTTP/S	15	19
5	zagreb	Periodic: Possible Malware Check-in on HTTP/S	6	17
5	astana	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	8	16

Top sensors

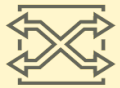
S	Sensor	Events
9	moscow	7
6	london	799
6	vienna	142
6	paris	84
6	sanmarino	69
6	zagreb	25
5	astana	610
5	monaco	401
5	madrid	233
5	rome	41
5	bern	15
5	reykjavik	15
5	tallinn	13
5	stockholm	5
5	helsinki	2

АРХІТЕКТУРА + РОЗГОРТАННЯ

GREYCORTEX

АРХІТЕКТУРА

Трафік мережі



Віддзеркалені дані

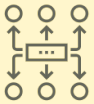
NetFlow

Захоплення пакетів

Моніторинг

Ідентифікація користувача

Дані про обладнання (назви хостів, ОС)



Додатки та метадані

Геолокація IP

Контекст мережі

Методи виявлення

Виявлення

Threat Intelligence

Розслідування та пошук загроз

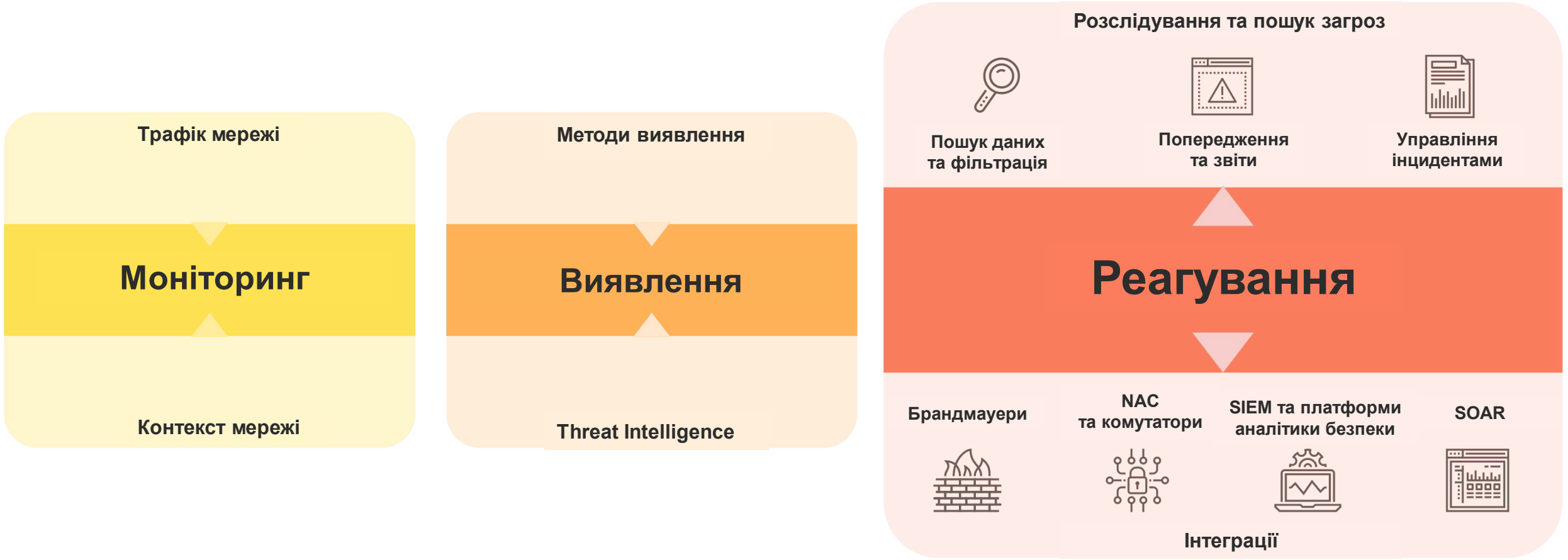
Реагування

Інтеграції

GREYCORTEX

АРХІТЕКТУРА

АРХІТЕКТУРА



GREYCORTEX

РОЗГОРТАННЯ

All-in-one appliance

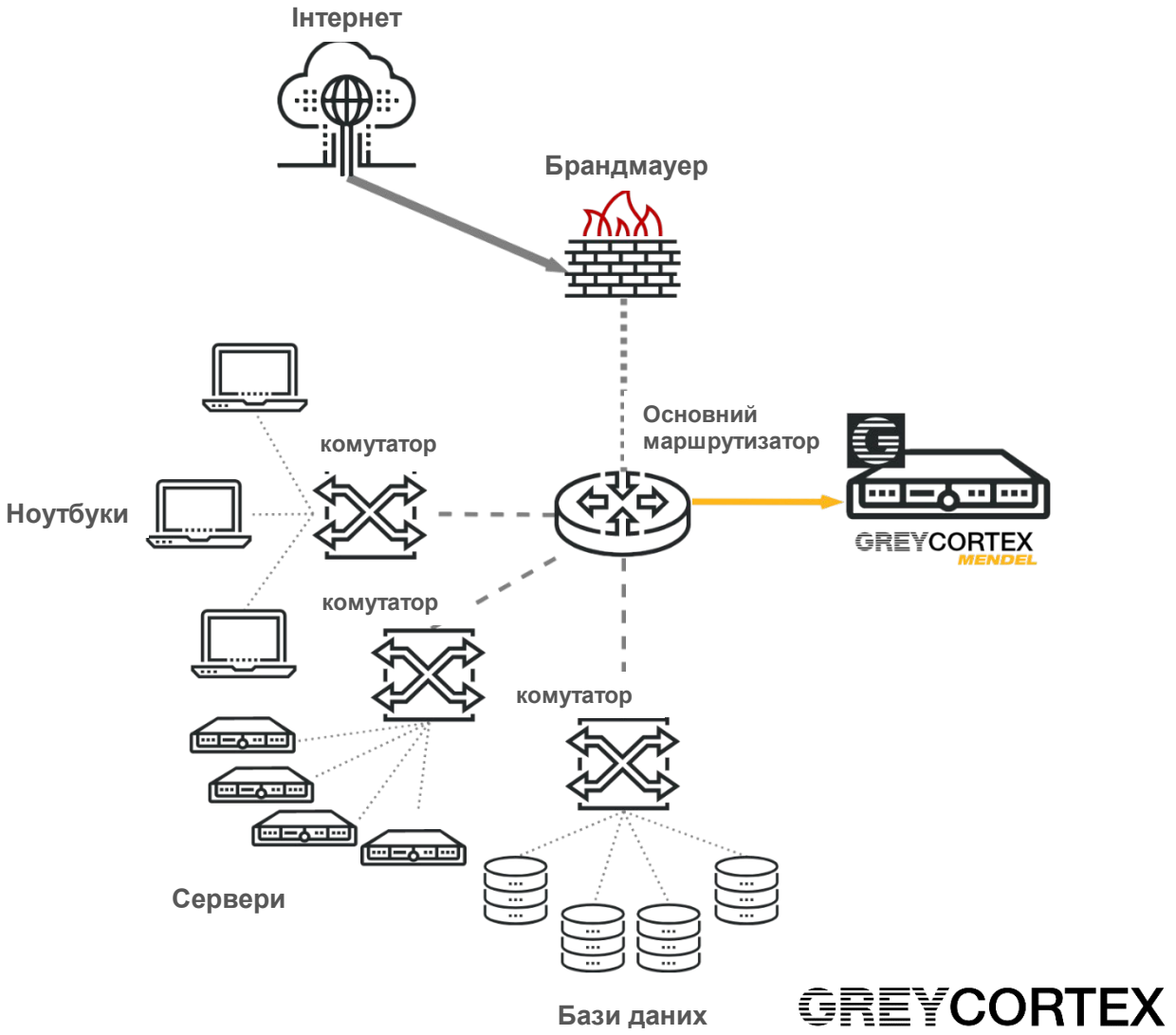
Швидке розгортання та миттєві результати

Від 200 Мб/с до 10 Гб/с

1GE або 10GE інтерфейси для моніторингу

Від 500 до 30 000 хостів у мережі

Virtual appliances до 1Гб/с



GREYCORTEX

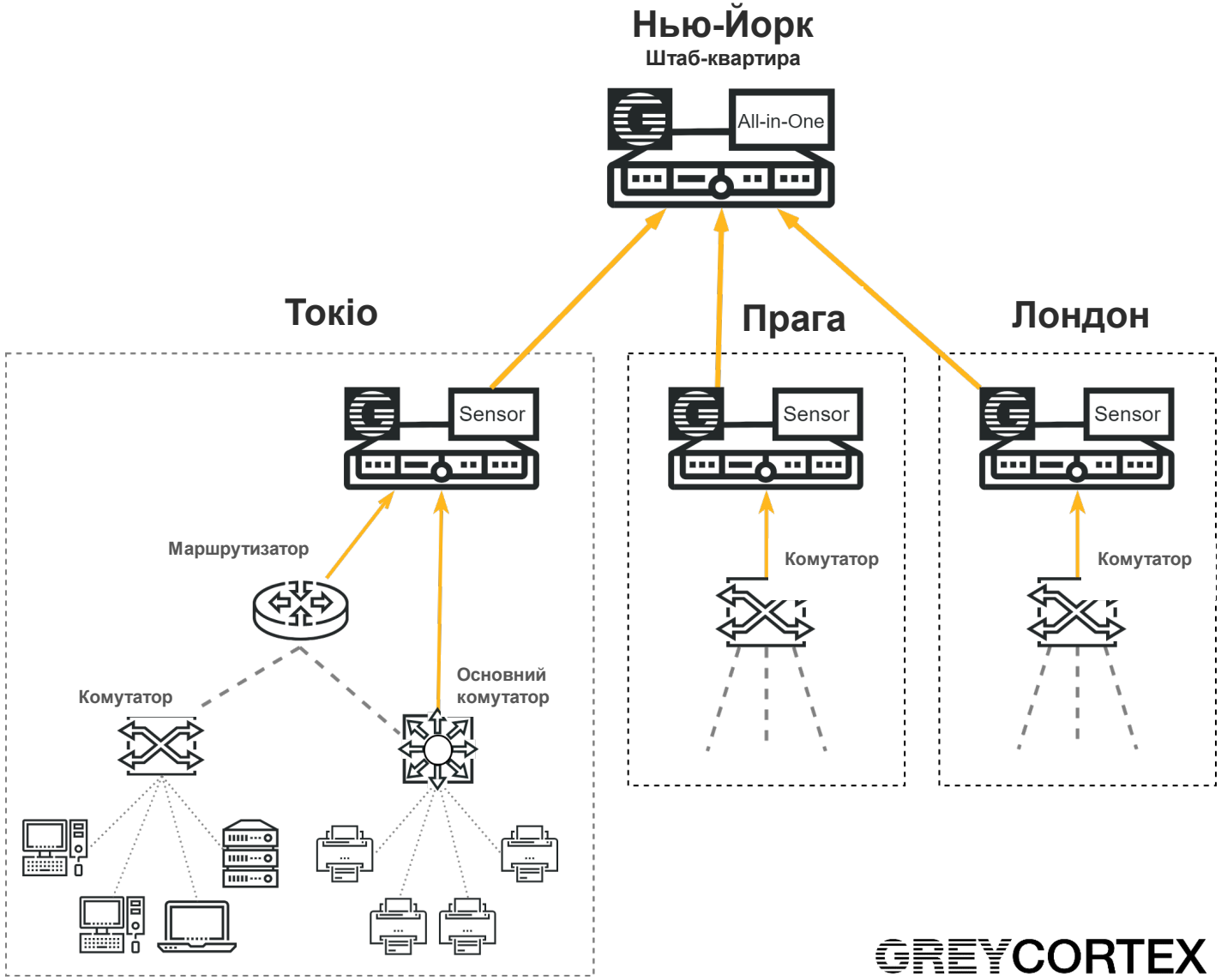
РОЗГОРТАННЯ

All-in-one appliance
(сенсор + колектор) у головному офісі

Сенсори встановлені у філіалах

1 колектор може керувати
до 40 сенсорами та 60 000
відслідковуваних хостів

Кілька колекторів можна об'єднати
у CEM (central event management)



GREYCORTEX

ПЕРЕВАГИ РІШЕННЯ

Широкі та глибокі можливості виявлення

- Поведінки (200+ поведінкових шаблонів + понад 45 тисяч сигнатур)
- Аномалій через моделювання очікуваної поведінки
- Машинної поведінки (RAT, командні сервери ботнетів)
- Співставлення вищезазначеного

Унікальний огляд мережі

- Зручна та ефективна фільтрація та звітування

Зручність використання

- Створено з думкою про управління безпекою

Об'єднання IT-спеціалістів та OT/SCADA інженерів

- Єдиний інструмент для моніторингу IT та OT/SCADA

GREYCORTEX

TECHNOLOGY ALLIANCE

ESET TECHNOLOGY ALLIANCE

ВИНИКЛИ ЗАПИТАННЯ?

БАЖАЄТЕ ЗАМОВИТИ ДЕМО-ВЕРСІЮ?

ЗВЕРТАЙТЕСЯ!

Сергій Кадет
s.kadet@eset.ua
+380 67 824 54 14