CENTRE FOR
CYBER SECURITY
BELGIUM

Centre for Cyber security Belgium Service Catalogue

Sandro MANZO

Lead of the Fusion Centre

CyTRIS (Cyber Threat Research & Intelligence Sharing)

CyTRIS is the CTI department of the CCB

TLP:AMBER+STRICT

Under the authority of the Prime Minister of
Belgium
Wetstraat 16 - 1000 Brussels - Belgium
Contact: https://www.ccb.belgium.be

15 March 2023

WHOAMI

Sandro Manzo

Lead of the Fusion Centre @ CCB/CyTRIS

Education

- Prof. Bachelor Applied Information Technology – DEV
- Prof. Bachelor Applied Information Technology – Cyber Crime Professional

Certifications

- GSEC, GCTI, GCIH ,GDAT
- GOSI ,GREM, GASF, CEH

TLP:AMBER+STRICT

Legal Basis

CENTRE FOR
CYBER SECURITY
BELGIUM

1. Created by Royal Decree 10/10/2014

   Contribute to build a safer and reliable internet

   Create national policy and capabilities with existing actors

   Under the authority of the Prime Minister

2. NIS-law 7 April 2019 & Royal Decree 12 July 2019

   CCB is the national CSIRT and the national authority

   In charge of monitoring and coordinating

   The implementation of the NIS law

Legal Basis CCB

1. Implementation of the Belgian Cyber Security Strategy & Policy
2. Ensuring coordination
3. Adapting the regulatory framework
4. Ensuring crisis management
5. Implementation of standards, guidelines and security standards for public institutions
6. Belgian representation in international cybersecurity forums
7. Security evaluation and certification
8. Informing and raising awareness

Legal Basis CCB-CERT.be/CyTRIS

1. Monitor incidents at the national and international level
2. Provide early warnings, alerts, announcements and dissemination of Intelligence
3. Respond to incidents
4. Provide dynamic risk and incident analysis and situational awareness;
5. Detect, observe and analyze Cyber security problems;
6. Encourage the adoption and use of common or standardized practices
7. Provide cooperative contacts with the private sector and with other administrative departments
8. Participate in the EU CSIRT network

CCB Mission

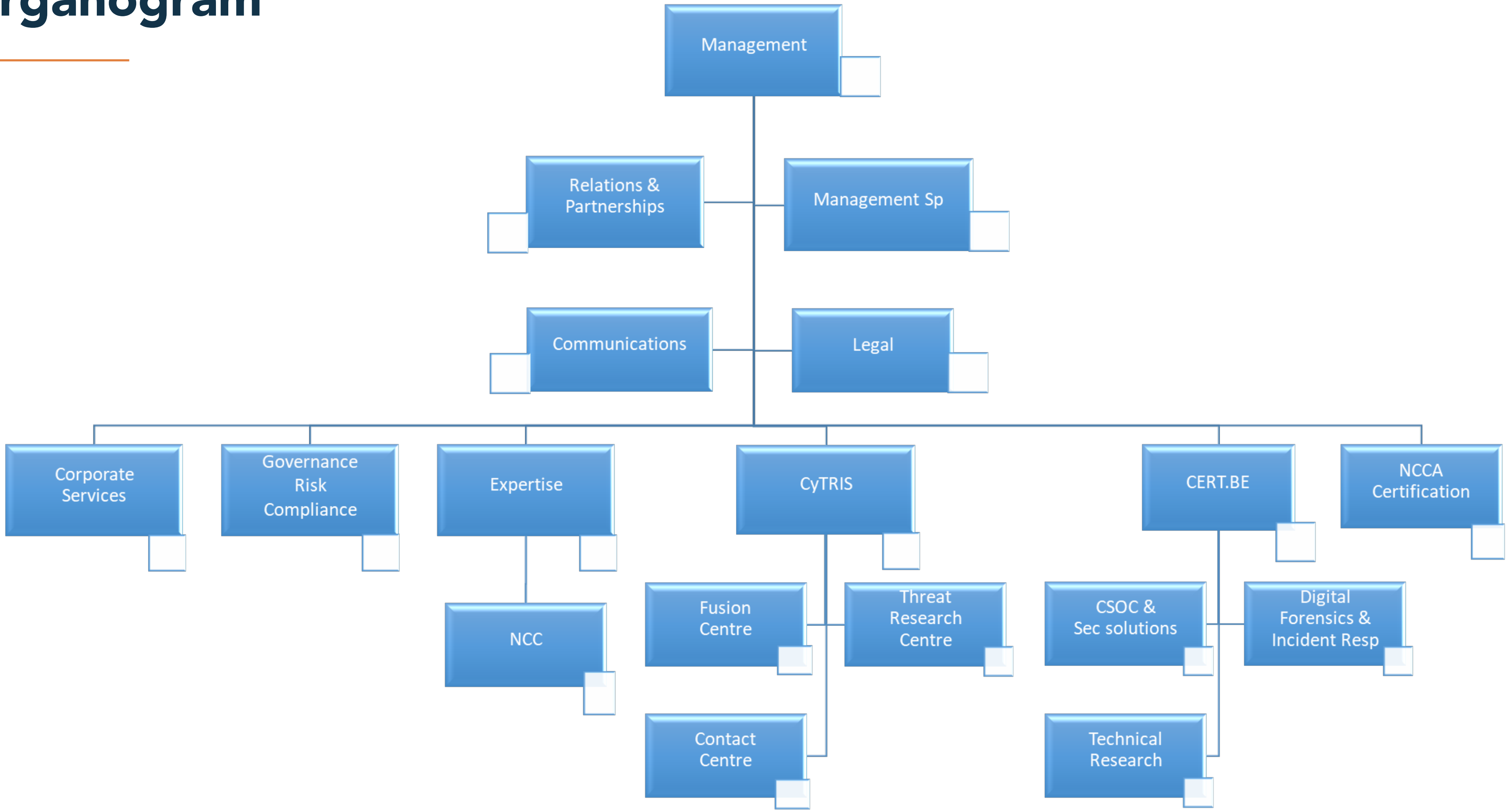
Make Belgium one of the least cyber vulnerable countries in Europe

Understanding Risk/Threat

Sharing Knowledge

Building Trust

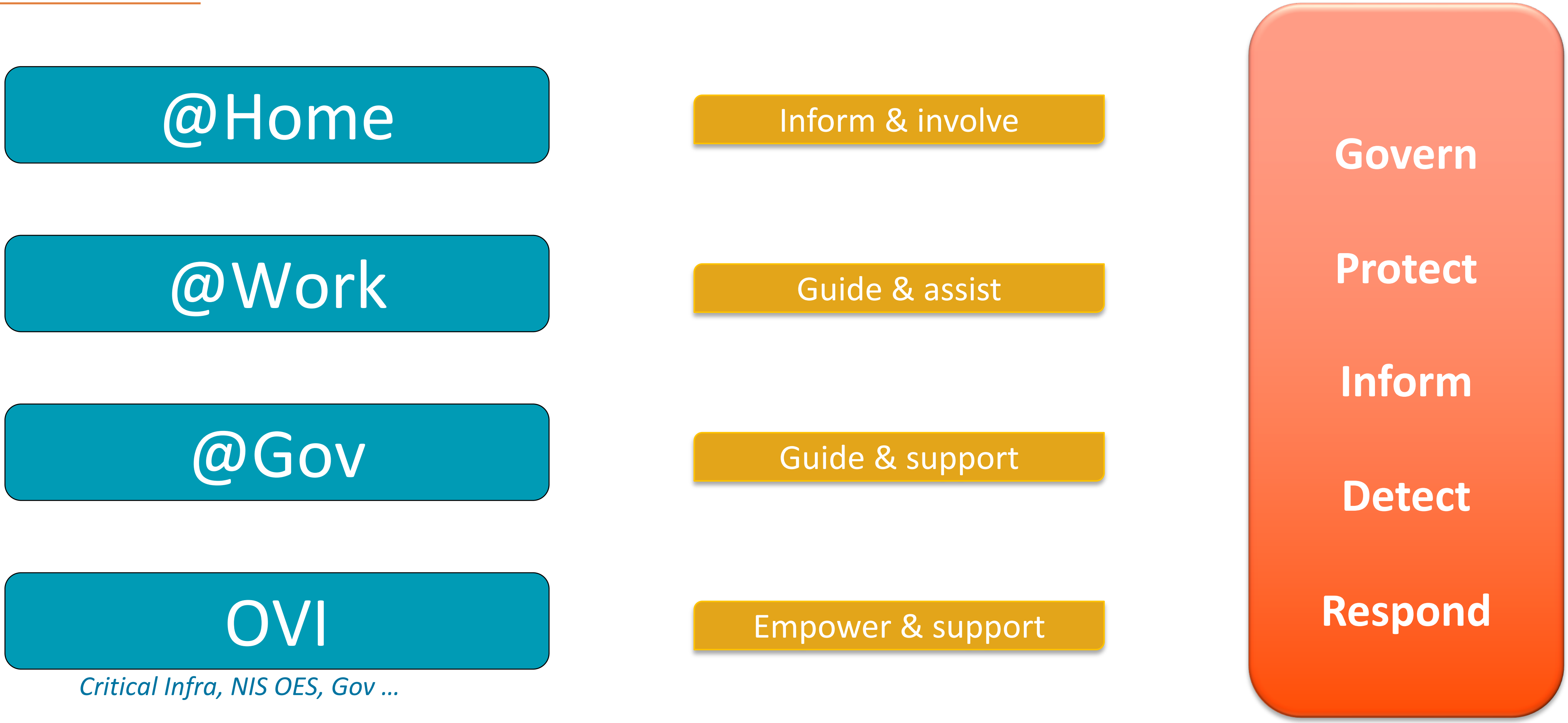
CCB Organogram



CENTRE FOR CYBER SECURITY BELGIUM

TLP:AMBER+STRICT

Mission



@Home

Inform & involve

@Work

Guide & assist

@Gov

Guide & support

OVI

Empower & support

Critical Infra, NIS OES, Gov …

Govern

Protect

Inform

Detect

Respond

The challenge

- Phishing
  - 44% of people think an email is safe when it contains familiar branding/point of contact
  - 33% of people will click links or download malware
  - 41% of cyber attack starts with an phishing email, 95% of ransomware attacks start with phishing
- Malware
  - 92% of malware gets delivered via email.
  - 4.1 million websites host malware at any given time.
- Vulnerabilities
  - Over 25,000 vulnerabilities have been published in 2022.
  - Web application (56%) and mail (28%) servers account for the top two assets being impacted.
  - Unpatched vulnerabilities were involved in 60% of data breaches.
  - Less than 1% of companies have more than 95% visibility into all their assets

References: Proofpoint, IBM, GetAstra

Cyber Crime as a Service Catalogue

Access

- Gaining access to compromised accounts & systems in bulk trough RDP, VPN, Web Shells, Exploitable vulnerabilities

Malware

- Facilitiating distribution of malware with watering-hole attacks, exploitable vulnerabilities

Phishing

- End to end services for cloned sites, hosting, phishing campaigns

OpSec

- Bundled services provided by threat actors to hide C2 beacons, infections to minimize the risk of detection

Scanning

- Offering ready to use lists of organisations that are vulnerable for specific vulnerabilities

Scamming

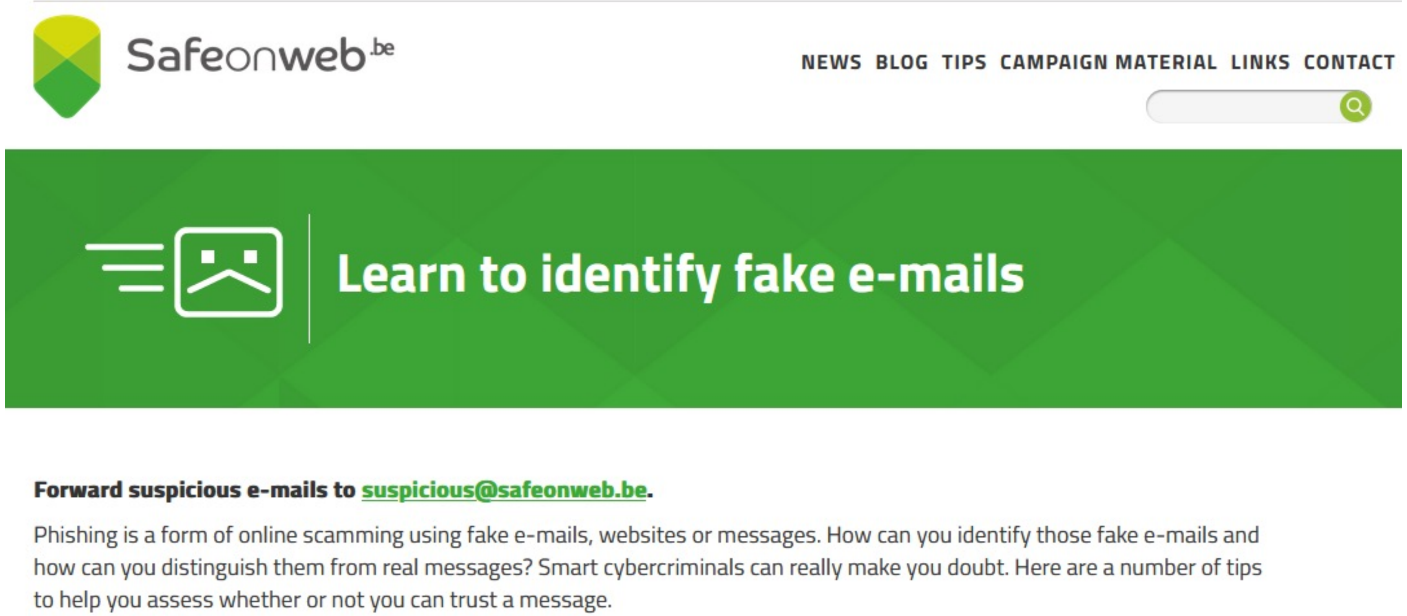
- Delivery of targeted malicious ads, scamming kits , or cryptocurrency scams

CCB's approach: Active Cyber Protection (ACP)

User involvement

Pillar 1 – User Involvement BePhish

- KISS principle
  - User sends suspicious email to one of the 4 e-mailadresses
    - verdacht@safeonweb.be
    - suspicious@safeonweb.be
    - suspect@safeonweb.be
    - verdachtig@safeonweb.be


Safeonweb.be
NEWS BLOG TIPS CAMPAIGN MATERIAL LINKS CONTACT
Learn to identify fake e-mails

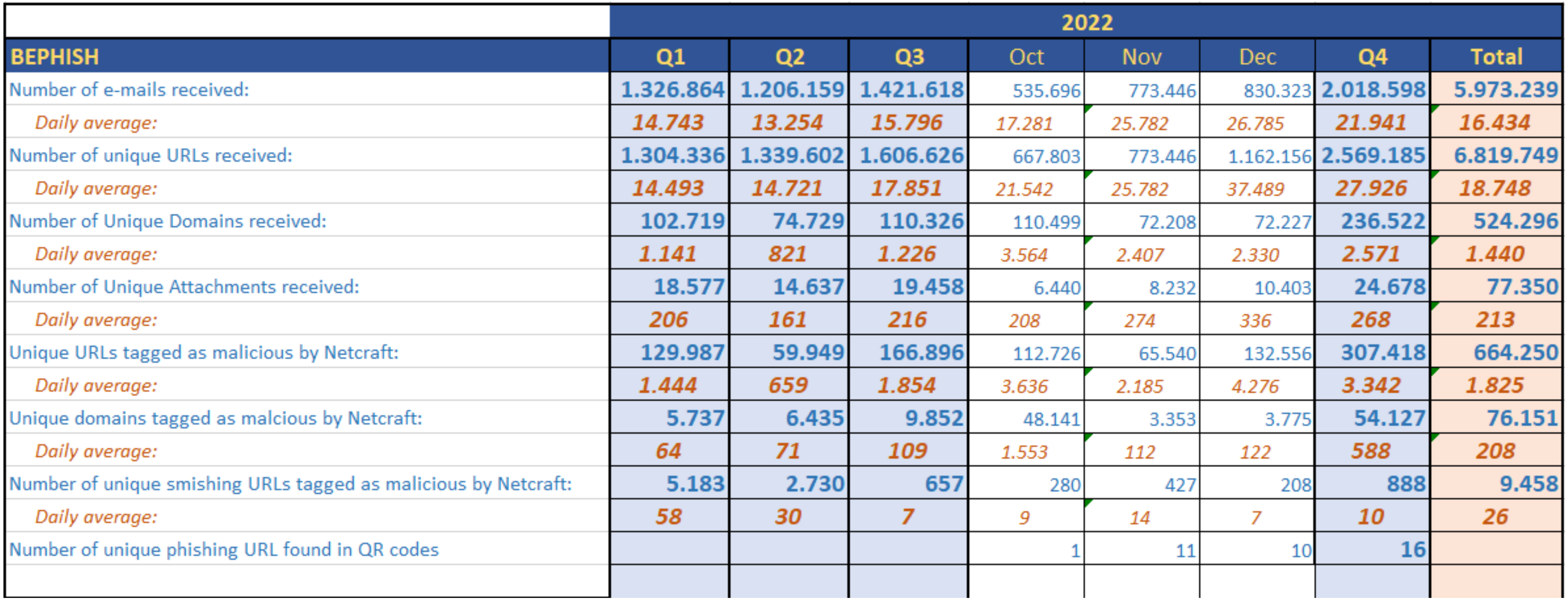
Forward suspicious e-mails to suspicious@safeonweb.be.

Phishing is a form of online scamming using fake e-mails, websites or messages. How can you identify those fake e-mails and how can you distinguish them from real messages? Smart cybercriminals can really make you doubt. Here are a number of tips to help you assess whether or not you can trust a message.

Pillar 1 – User Involvement BePhish

- Collection
  - Suspicious e-mail
  - SMS
  - MMS
- Detection of malicious
  - URLS/Attachments
  - Malware
  - Web shell
  - Credential harvesting pages
- Block
  - 3d party organisations
  - Browser
  - Belgian Anti Phishing Shield

Pillar 1 – User Involvement BePhish Statistics

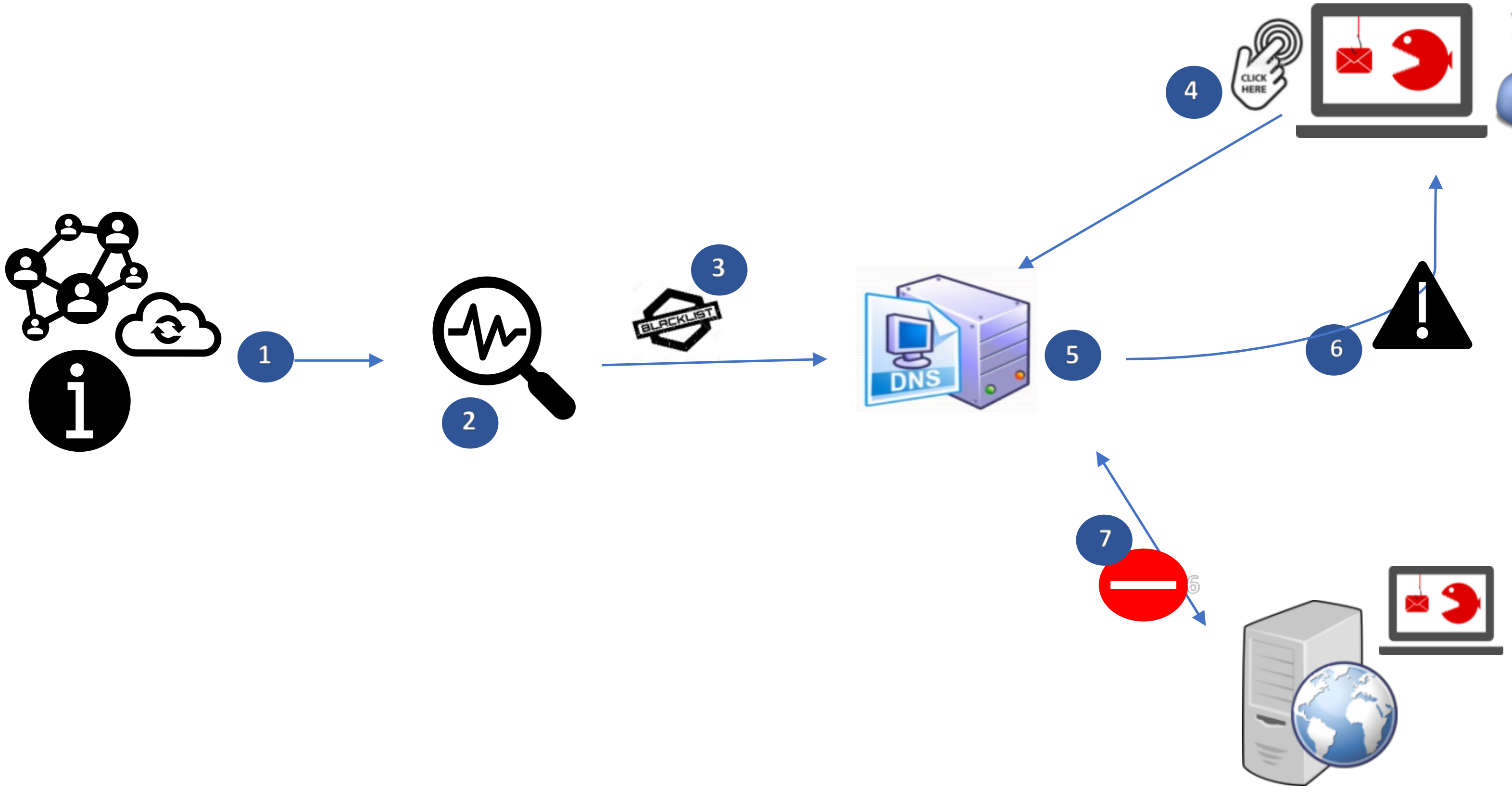


	2022							
BEPHISH	**Q1**	**Q2**	**Q3**	Oct	Nov	Dec	**Q4**	**Total**
Number of e-mails received:	**1.326.864**	**1.206.159**	**1.421.618**	535.696	773.446	830.323	**2.018.598**	**5.973.239**
Daily average:	***14.743***	***13.254***	***15.796***	*17.281*	*25.782*	*26.785*	***21.941***	***16.434***
Number of unique URLs received:	**1.304.336**	**1.339.602**	**1.606.626**	667.803	773.446	1.162.156	**2.569.185**	**6.819.749**
Daily average:	***14.493***	***14.721***	***17.851***	*21.542*	*25.782*	*37.489*	***27.926***	***18.748***
Number of Unique Domains received:	**102.719**	**74.729**	**110.326**	110.499	72.208	72.227	**236.522**	**524.296**
Daily average:	***1.141***	***821***	***1.226***	*3.564*	*2.407*	*2.330*	***2.571***	***1.440***
Number of Unique Attachments received:	**18.577**	**14.637**	**19.458**	6.440	8.232	10.403	**24.678**	**77.350**
Daily average:	***206***	***161***	***216***	*208*	*274*	*336*	***268***	***213***
Unique URLs tagged as malicious by Netcraft:	**129.987**	**59.949**	**166.896**	112.726	65.540	132.556	**307.418**	**664.250**
Daily average:	***1.444***	***659***	***1.854***	*3.636*	*2.185*	*4.276*	***3.342***	***1.825***
Unique domains tagged as malcious by Netcraft:	**5.737**	**6.435**	**9.852**	48.141	3.353	3.775	**54.127**	**76.151**
Daily average:	***64***	***71***	***109***	*1.553*	*112*	*122*	***588***	***208***
Number of unique smishing URLs tagged as malicious by Netcraft:	**5.183**	**2.730**	**657**	280	427	208	**888**	**9.458**
Daily average:	***58***	***30***	***7***	*9*	*14*	*7*	***10***	***26***
Number of unique phishing URL found in QR codes				1	11	10	**16**	

CENTRE FOR
CYBER SECURITY
BELGIUM

TLP:AMBER+STRICT

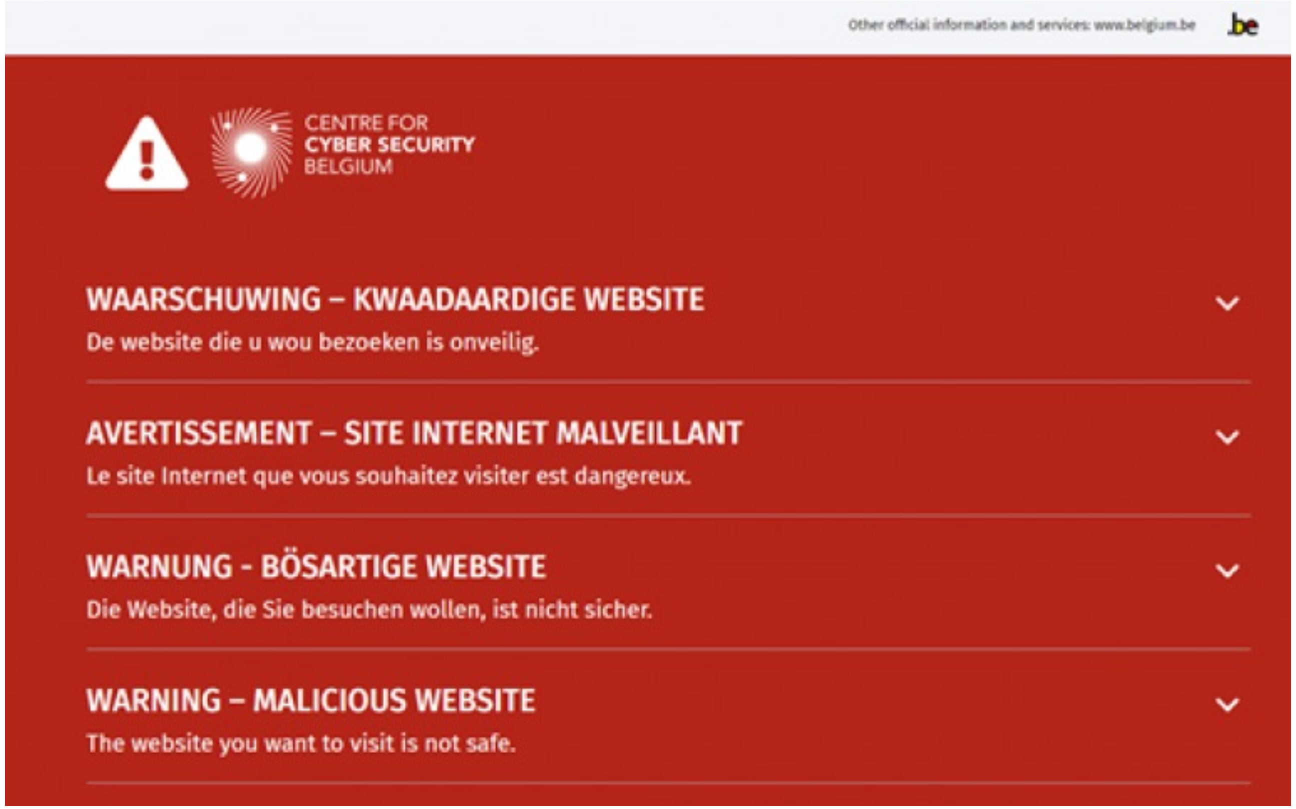
Pillar 2 – Infrastructure segmentation: Belgian Anti Phishing Shield



TLP:AMBER+STRICT

Pillar 2 – Infrastructure segmentation: Belgian Anti Phishing Shield

Belgian Anti-Phishing Shield (BAPS)



Other official information and services: www.belgium.be .be

CENTRE FOR CYBER SECURITY BELGIUM

WAARSCHUWING – KWAADAARDIGE WEBSITE

De website die u wou bezoeken is onveilig.

AVERTISSEMENT – SITE INTERNET MALVEILLANT

Le site Internet que vous souhaitez visiter est dangereux.

WARNUNG - BÖSARTIGE WEBSITE

Die Website, die Sie besuchen wollen, ist nicht sicher.

WARNING – MALICIOUS WEBSITE

The website you want to visit is not safe.

2022

664 000 URLs redirected related to **76 000 malicious web domains**

Pillar 3 - Early Warning System

Pillar 3 - Early Warning System

Goal

- Obtain Organization Information
  - Where?
  - Who?
  - What?
- Cyber Threat Intelligence Requirements
  - Reports, Alerts, Advisories
  - Correlation
- Collaboration
  - Threat Intel Loopback

Benefits

Rapid Response, Early Warning

Actionable Information for each profile

Improvement of Belgium's Cyber Security

Pillar 3 - Early Warning System: Spear Warning?

Active Cyber security

Spear Phishing: Threat actor targets organizations of interest to achieve actions on objectives

Spear Warning: CCB informs vulnerable organizations to prevent the threat actor to achieve its actions on objectives

TLP:AMBER+STRICT

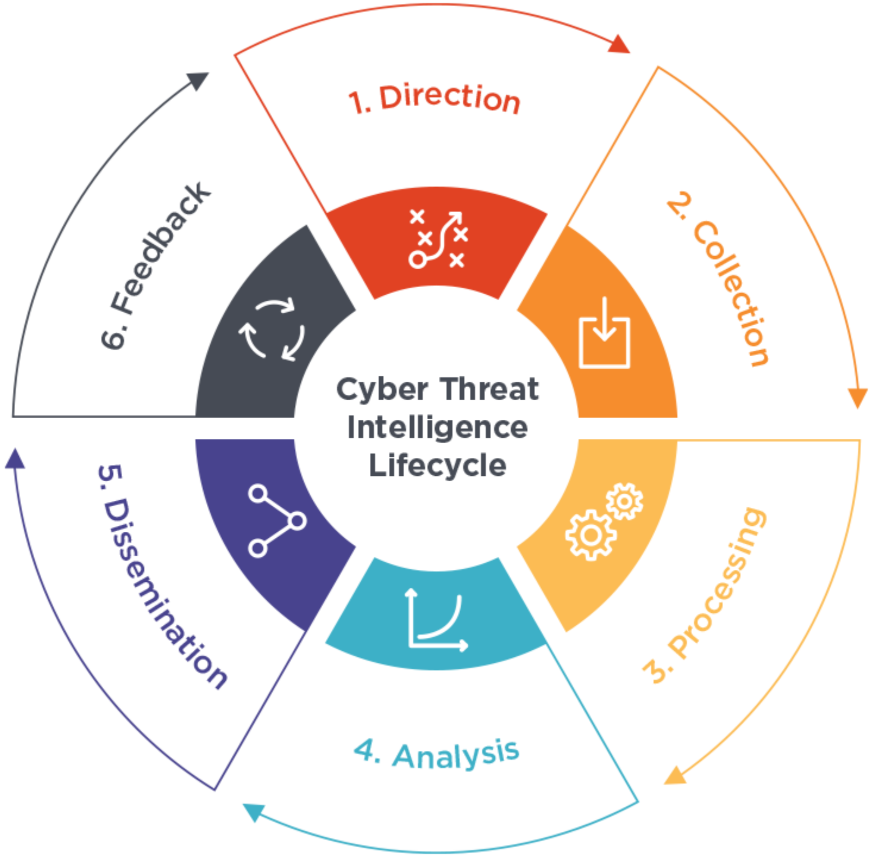
Pillar 3 - Early Warning System Spear Warning Types

- Credential Leak
- Infection
- Vulnerability
- Pre-Ransomware notification
- Compromised assets

Pillar 3 - Early Warning System Spear Warning: Deliverables

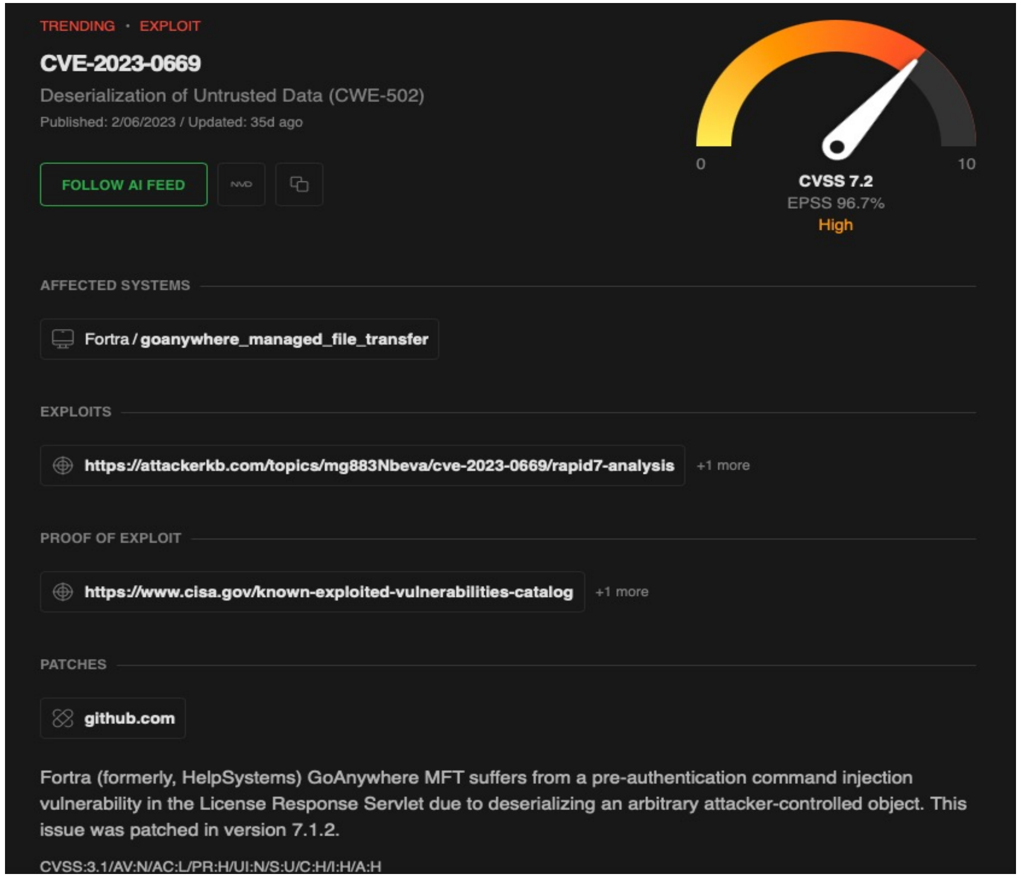
- Email
- Physical Letter (CEO)
- Phone call

Pillar 3 - Early Warning System Spear Warning: CTI driven – Intelligence lifecycle



TLP:AMBER+STRICT

CVE-2023-0669: Fortra Go Anywhere - Collection



TRENDING • EXPLOIT

CVE-2023-0669

Deserialization of Untrusted Data (CWE-502)

Published: 2/06/2023 / Updated: 35d ago

FOLLOW AI FEED

CVSS 7.2
EPSS 96.7%
High

AFFECTED SYSTEMS

Fortra / goanywhere_managed_file_transfer

EXPLOITS

https://attackerkb.com/topics/mg883Nbeva/cve-2023-0669/rapid7-analysis +1 more

PROOF OF EXPLOIT

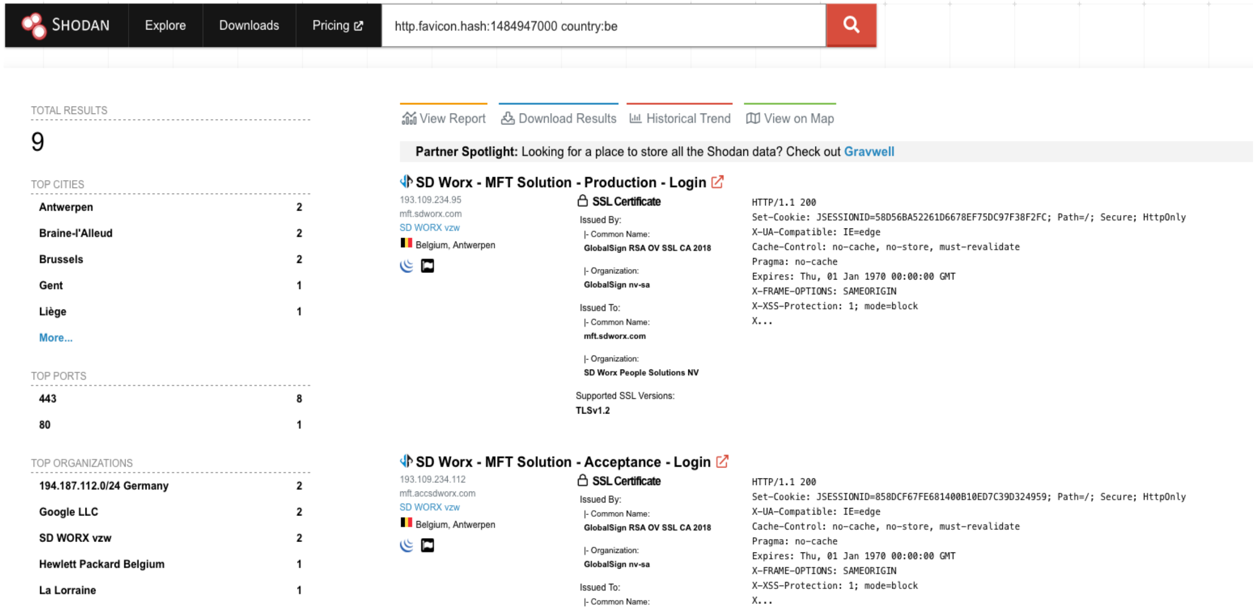
https://www.cisa.gov/known-exploited-vulnerabilities-catalog +1 more

PATCHES

github.com

Fortra (formerly, HelpSystems) GoAnywhere MFT suffers from a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object. This issue was patched in version 7.1.2.

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



```
http.favicon.hash:1484947000 country:be
```

TOTAL RESULTS

9

TOP CITIES

Antwerpen	2
Braine-l'Alleud	2
Brussels	2
Gent	1
Liège	1

More...

TOP PORTS

443	8
80	1

TOP ORGANIZATIONS

194.187.112.0/24 Germany	2
Google LLC	2
SD WORX vzw	2
Hewlett Packard Belgium	1
La Lorraine	1

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

SD Worx - MFT Solution - Production - Login

193.109.234.95
mft.sdworx.com
SD WORX vzw
Belgium, Antwerpen

SSL Certificate

Issued By:
|- Common Name:
GlobalSign RSA OV SSL CA 2018
|- Organization:
GlobalSign nv-sa

Issued To:
|- Common Name:
mft.sdworx.com
|- Organization:
SD Worx People Solutions NV

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=58D56BA52261D6678EF75DC97F38F2FC; Path=/; Secure; HttpOnly
X-UA-Compatible: IE=edge
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X...
```

SD Worx - MFT Solution - Acceptance - Login

193.109.234.112
mft.accsdworx.com
SD WORX vzw
Belgium, Antwerpen

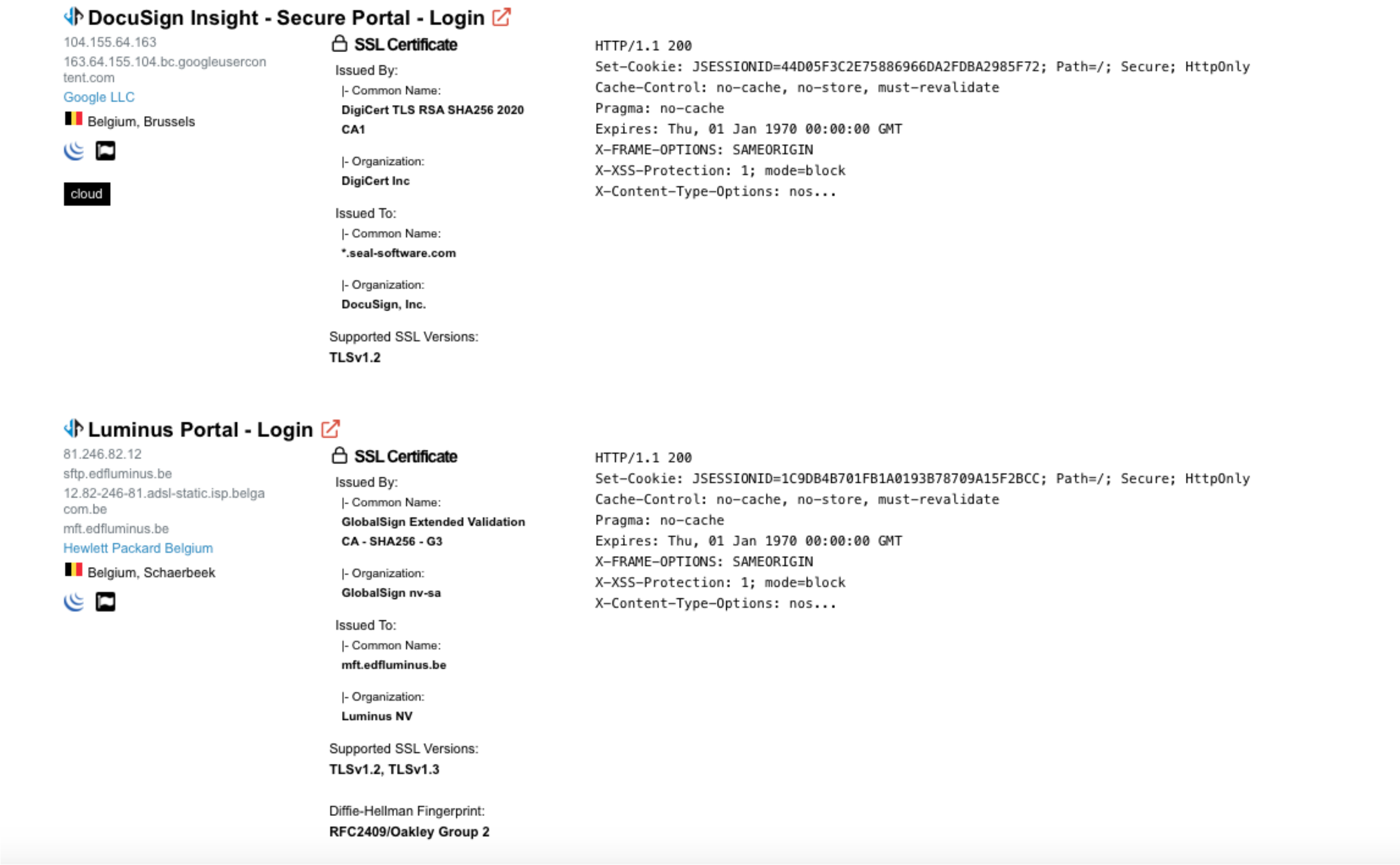
SSL Certificate

Issued By:
|- Common Name:
GlobalSign RSA OV SSL CA 2018
|- Organization:
GlobalSign nv-sa

Issued To:
|- Common Name:

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=858DCF67FE681400B10ED7C39D324959; Path=/; Secure; HttpOnly
X-UA-Compatible: IE=edge
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X...
```

Spear Warning: Processing & Analysis



DocuSign Insight - Secure Portal - Login

104.155.64.163
163.64.155.104.bc.googleusercontent.com
Google LLC
Belgium, Brussels

cloud

SSL Certificate

Issued By:
|- Common Name:
DigiCert TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
***.seal-software.com**
|- Organization:
DocuSign, Inc.

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=44D05F3C2E75886966DA2FDBA2985F72; Path=/; Secure; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nos...
```

Luminus Portal - Login

81.246.82.12
sftp.edfluminus.be
12.82-246-81.adsl-static.isp.belgacom.be
mft.edfluminus.be
Hewlett Packard Belgium
Belgium, Schaerbeek

SSL Certificate

Issued By:
|- Common Name:
GlobalSign Extended Validation CA - SHA256 - G3
|- Organization:
GlobalSign nv-sa

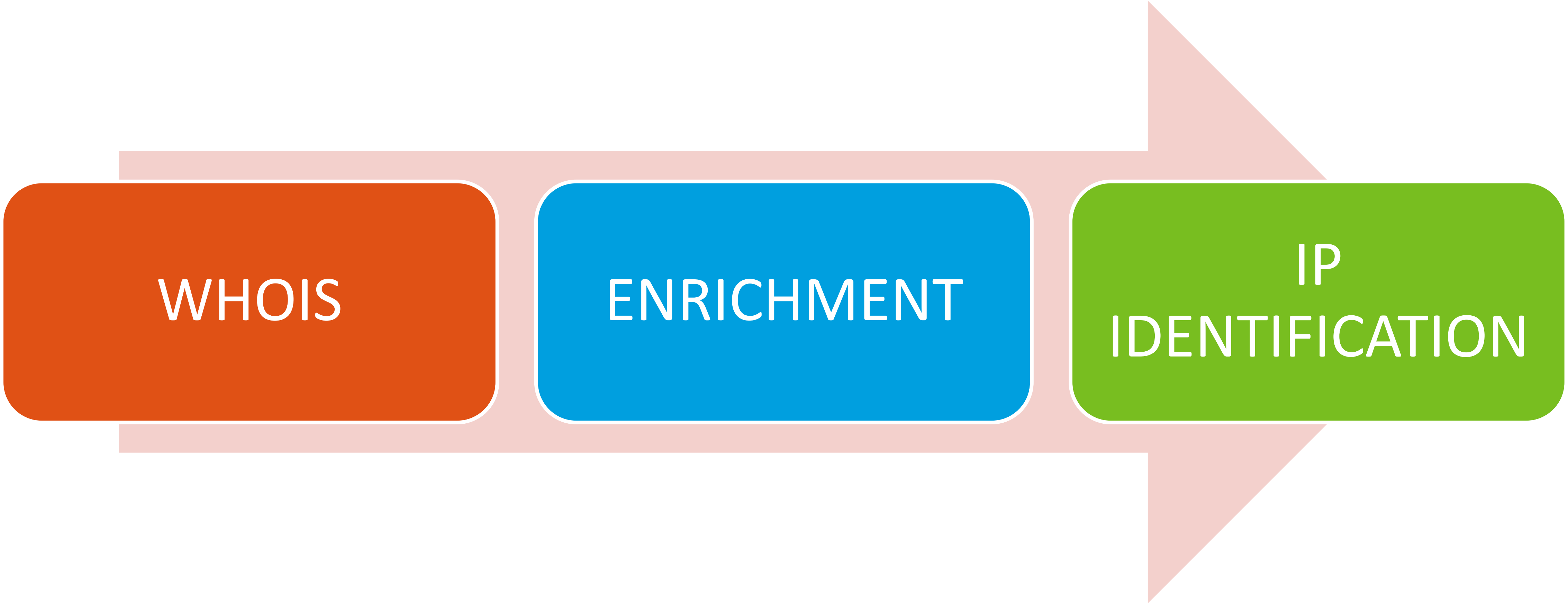
Issued To:
|- Common Name:
mft.edfluminus.be
|- Organization:
Luminus NV

Supported SSL Versions:
TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=1C9DB4B701FB1A0193B78709A15F2BCC; Path=/; Secure; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nos...
```

Spear Warning: IP Identification



WHOIS

ENRICHMENT

IP IDENTIFICATION

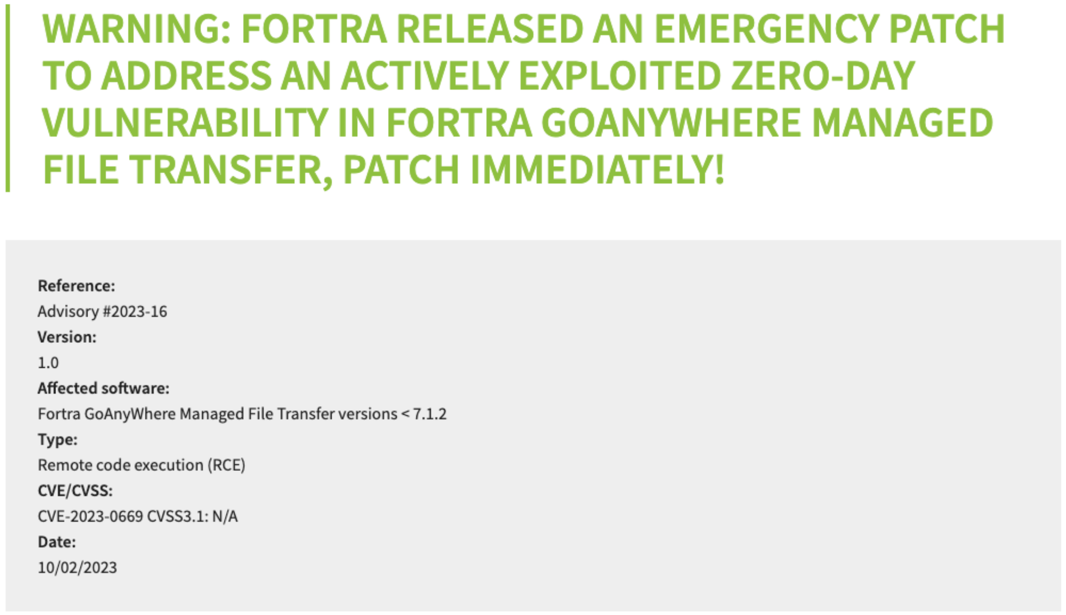
TLP:AMBER+STRICT

Spear Warning: Processing & Analysis

- Risk
- Technical Description
- ✓ Recommended actions

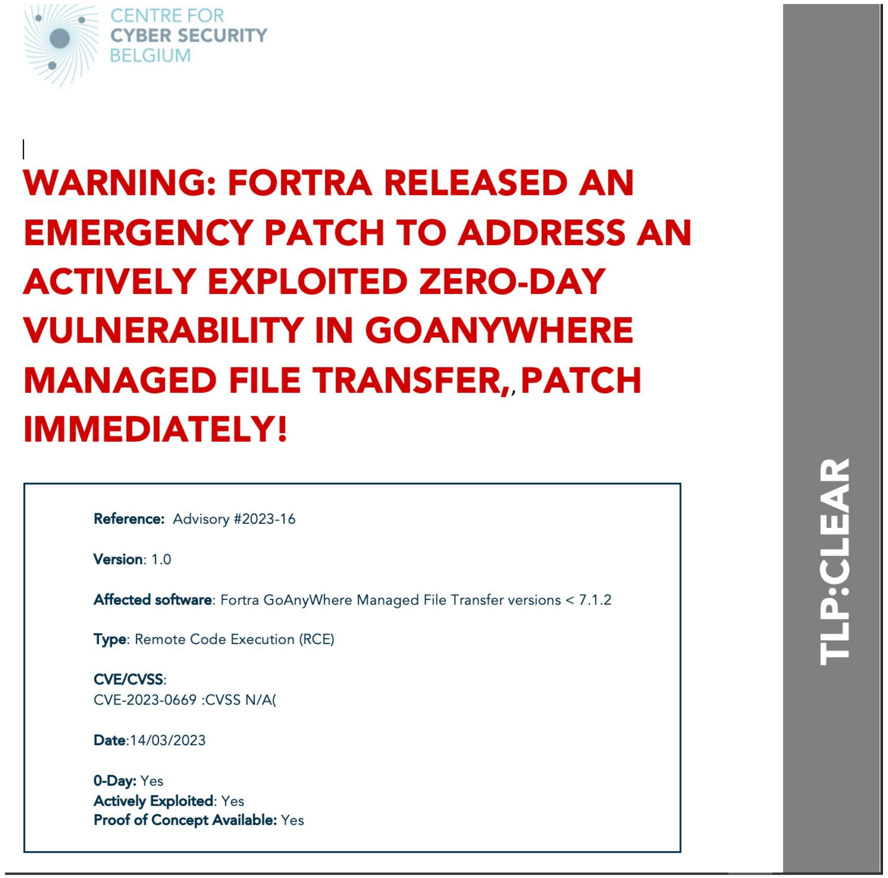
TLP:AMBER+STRICT

Spear Warning: Dissemination - Advisories & CTI reports



WARNING: FORTRA RELEASED AN EMERGENCY PATCH TO ADDRESS AN ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN FORTRA GOANYWHERE MANAGED FILE TRANSFER, PATCH IMMEDIATELY!

Reference:
Advisory #2023-16
Version:
1.0
Affected software:
Fortra GoAnyWhere Managed File Transfer versions < 7.1.2
Type:
Remote code execution (RCE)
CVE/CVSS:
CVE-2023-0669 CVSS3.1: N/A
Date:
10/02/2023



CENTRE FOR
CYBER SECURITY
BELGIUM

WARNING: FORTRA RELEASED AN EMERGENCY PATCH TO ADDRESS AN ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN GOANYWHERE MANAGED FILE TRANSFER,,PATCH IMMEDIATELY!

Reference: Advisory #2023-16

Version: 1.0

Affected software: Fortra GoAnyWhere Managed File Transfer versions < 7.1.2

Type: Remote Code Execution (RCE)

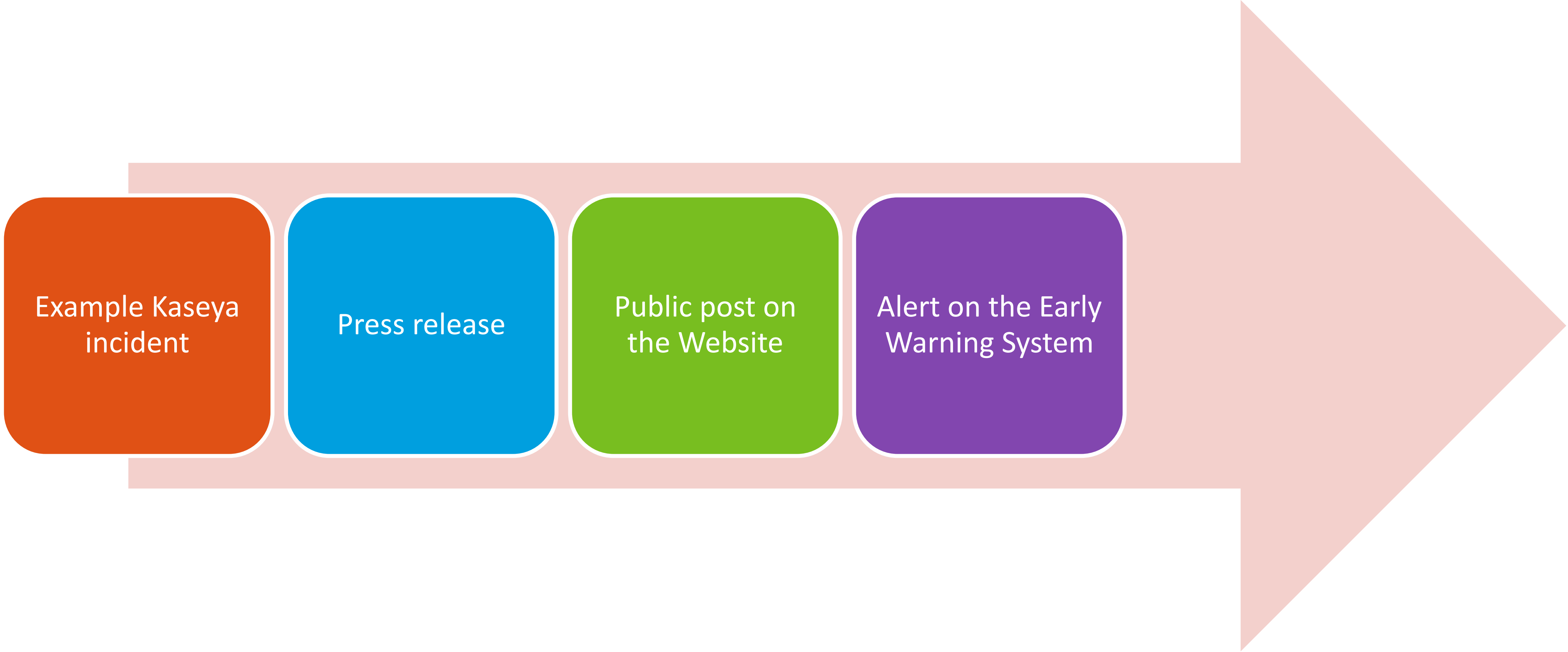
CVE/CVSS:
CVE-2023-0669 :CVSS N/A(

Date:14/03/2023

0-Day: Yes
Actively Exploited: Yes
Proof of Concept Available: Yes

TLP:CLEAR

Spear Warning: 0-Day - Escalation procedure (Use Case Kaseya)



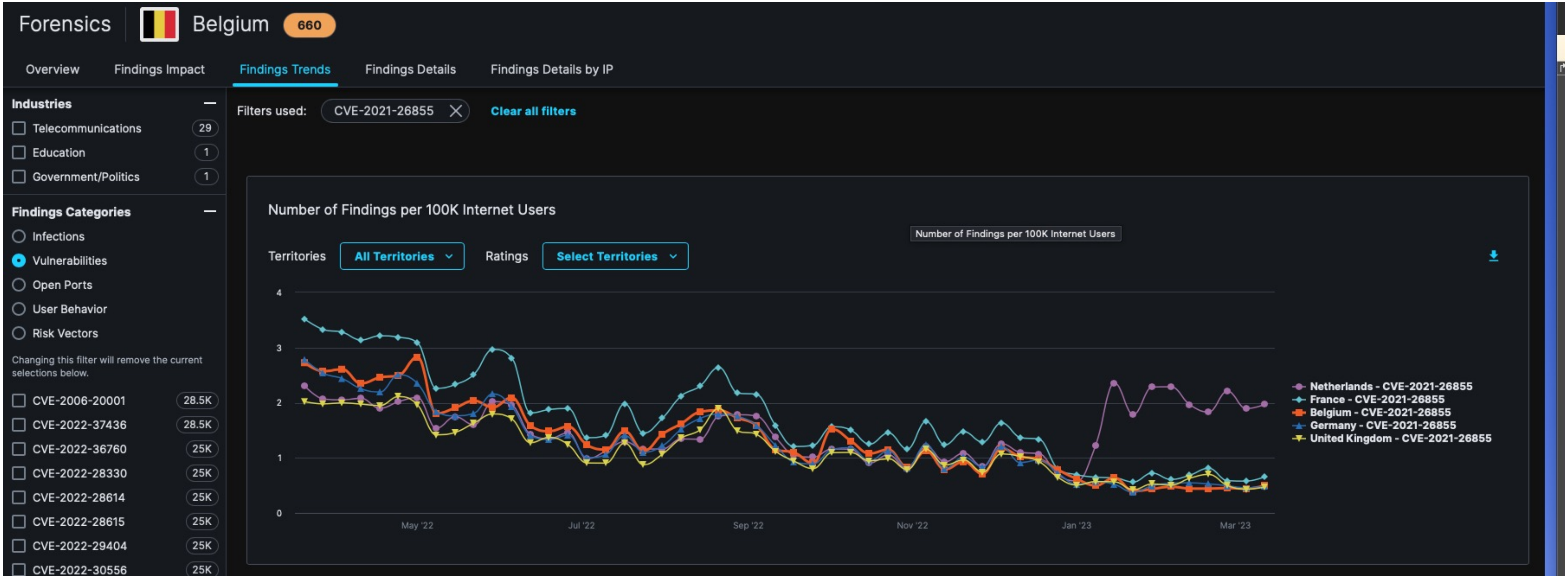
Example Kaseya incident

Press release

Public post on the Website

Alert on the Early Warning System

Spear Warning: Benchmark – (Use Case Hafnium)



Forensics | Belgium 660

Overview | Findings Impact | Findings Trends | Findings Details | Findings Details by IP

Industries

□ Telecommunications	29
□ Education	1
□ Government/Politics	1

Findings Categories

○ Infections
● Vulnerabilities
○ Open Ports
○ User Behavior
○ Risk Vectors

Changing this filter will remove the current selections below.

□ CVE-2006-20001	28.5K
□ CVE-2022-37436	28.5K
□ CVE-2022-36760	25K
□ CVE-2022-28330	25K
□ CVE-2022-28614	25K
□ CVE-2022-28615	25K
□ CVE-2022-29404	25K
□ CVE-2022-30556	25K

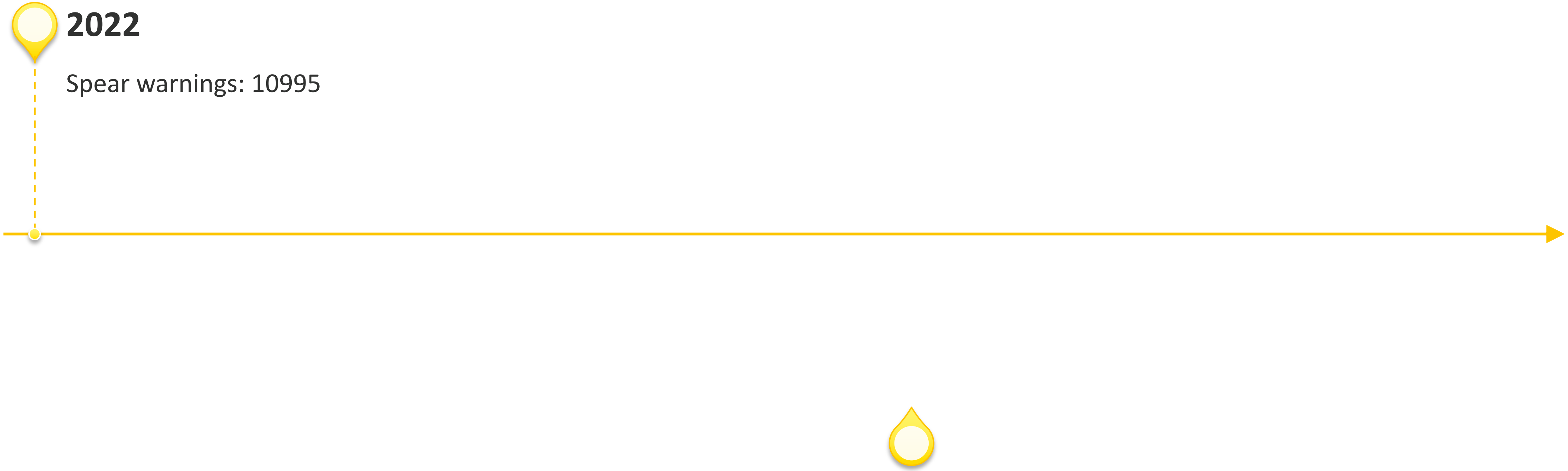
Filters used: CVE-2021-26855 ✕ **Clear all filters**

Number of Findings per 100K Internet Users

Territories: **All Territories** | Ratings: **Select Territories**

TLP:AMBER+STRICT

Spear Warning metrics



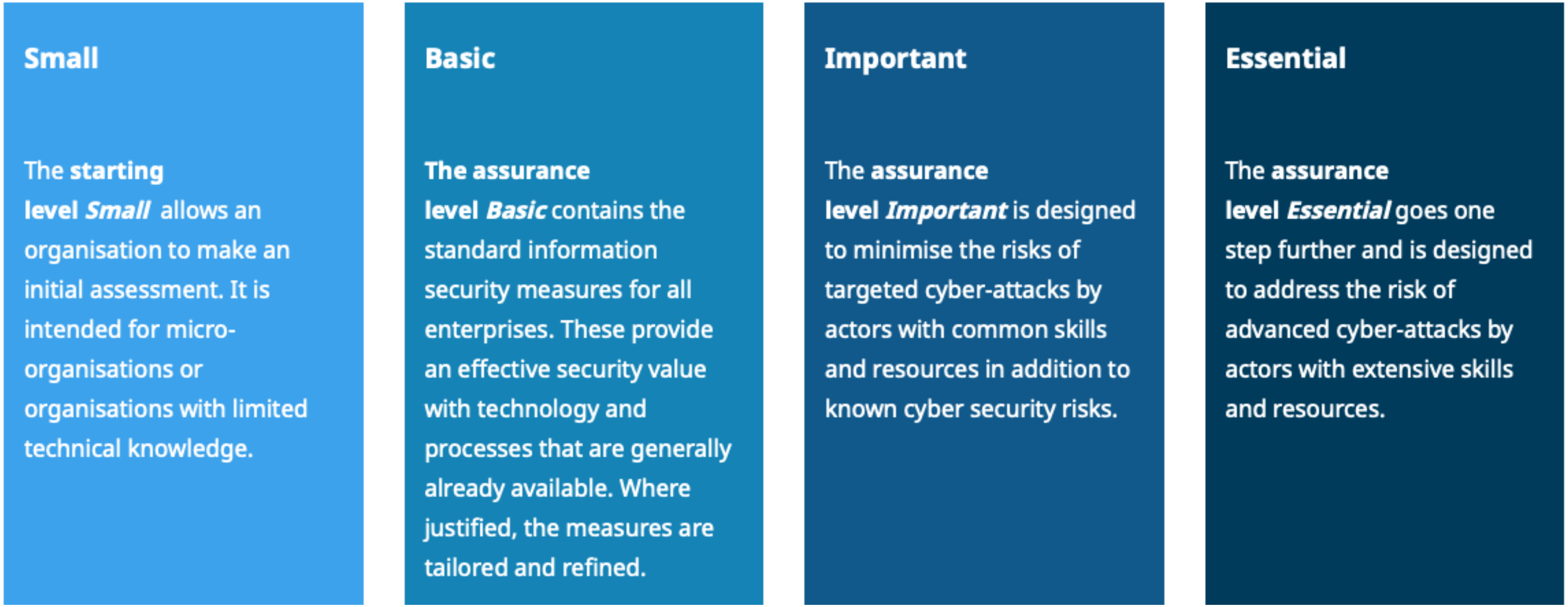
2022

Spear warnings: 10995

Pillar 4 – Cybersecurity Routine – Cyberfundamentals

The **Cyberfundamentals (CyFUN)** framework was released in early 2023 to help all Belgian organisations increase their cyber resilience.

Policy & Guidance: Cyberfundamentals Framework



Small

The **starting level *Small*** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

Basic

The assurance level *Basic* contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

Important

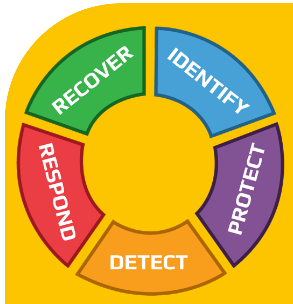
The **assurance level *Important*** is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

Essential

The **assurance level *Essential*** goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources.

Pillar 4 – Cybersecurity Routine

Use of Common standards

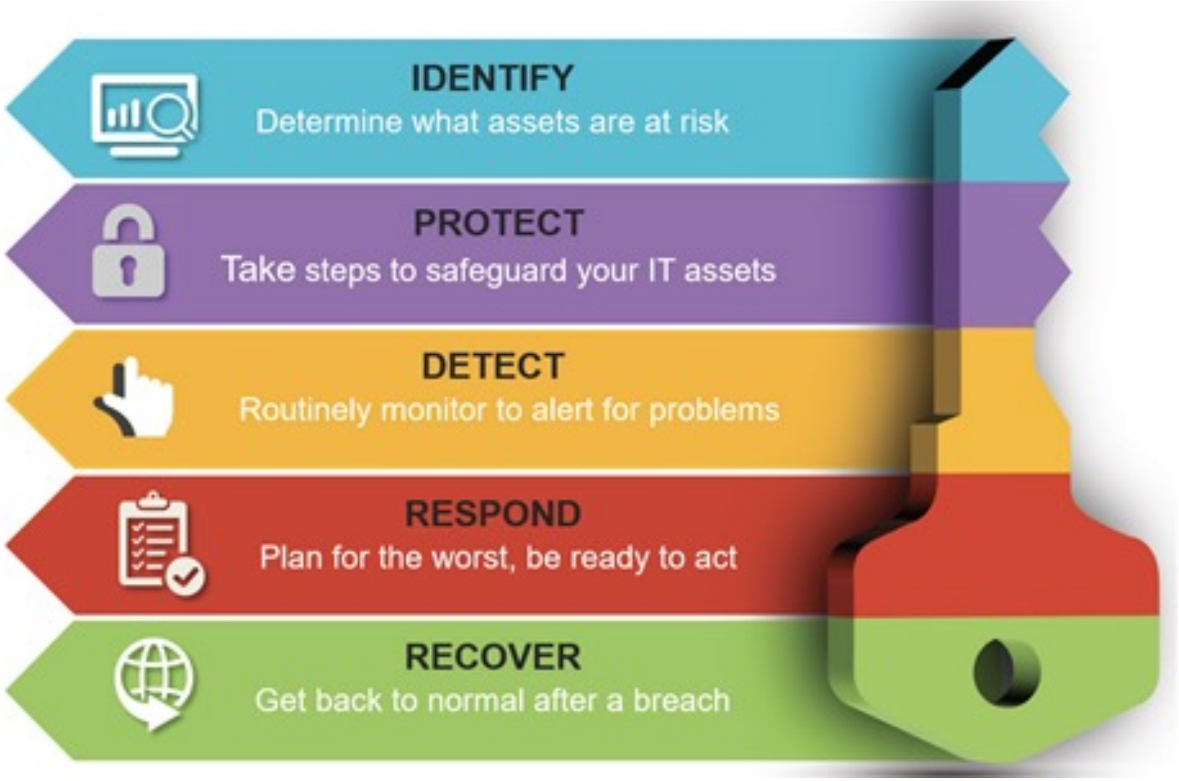


The NIST Cybersecurity Framework

CIS Controls

Information Security Management System
ISO
27001
Certified

IEC 62443
OT standards


IDENTIFY
Determine what assets are at risk
PROTECT
Take steps to safeguard your IT assets
DETECT
Routinely monitor to alert for problems
RESPOND
Plan for the worst, be ready to act
RECOVER
Get back to normal after a breach

Pilar 4: CyberFundamentals Framework

Based on our historical data, retro-fitting was done on successful cyber-attacks using anonymized data.

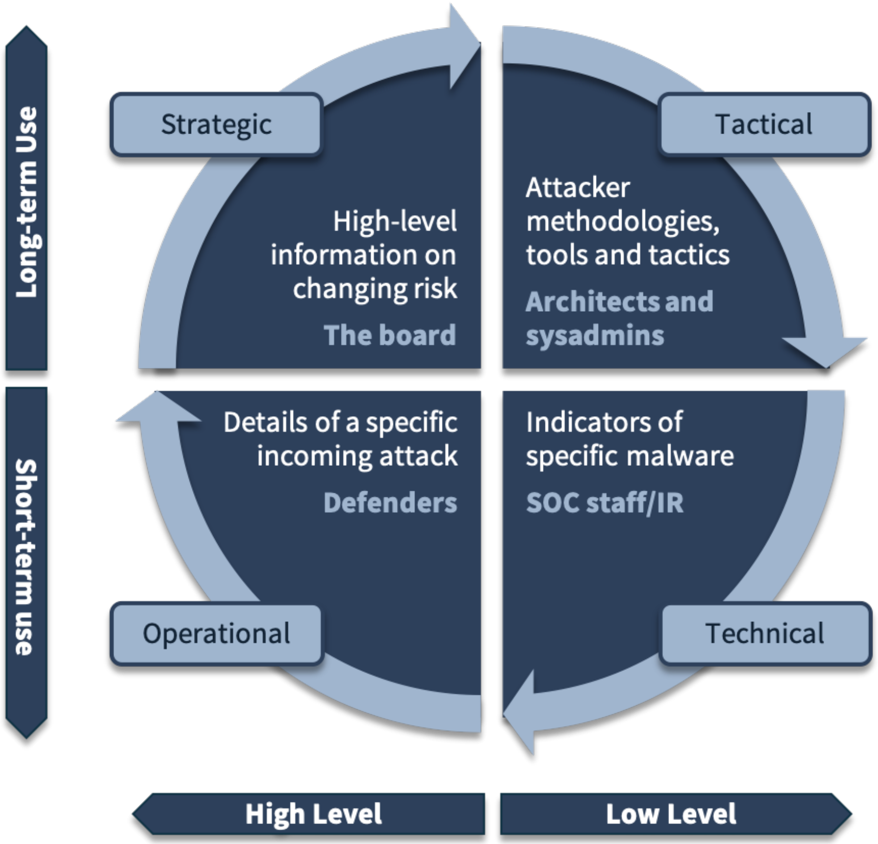
Based on these attacks, key measures were identified at each level to prioritize the countermeasures to protect against the known cyberattacks relevant for the respective assurance level.

Conclusion:

- Measures in assurance level Basic: cover 82% of the attacks,
- Measures in assurance level Important: 94 % of the attacks,
- Measures in assurance level Essential: 100% of the attacks.

https://ccb.belgium.be/en/cyberfundamentals-framework

Pillar 5: Sharing Cyber Threat Intelligence


Long-term Use
Short-term use
Strategic
High-level information on changing risk
The board
Tactical
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Operational
Indicators of specific malware
SOC staff/IR
Technical
High Level
Low Level

TLP:AMBER+STRICT

Sharing Intelligence is key

This Photo by Unknown Author is licensed under CC BY-NC-ND

Coming together = beginning

Keeping together = progress

Working together = success

- Henry Ford

- Share Intelligence in your organisation
- Share intelligence in your community
- Share intelligence with your partners

Thank You

рахмат
danke
謝謝
spas
ngiyabonga
teşekkür ederim
mahalo
tapadh leat
Баярлалаа
mersi
kia ora
barka
welalin
tack
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
gracias
хвала
asante
manana
obrigada
tenki
murakoze
kiitos
dankie
nanni
nandri
dhanyavad
thank you
bedankt
bayarlalaa
gràçie
hvala
maururu
köszönöm
akun
dankon
aciū
enkosi
dziękuję
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chokrane
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
sobodi
dėkuji
obrigado
sukriya
kop khun krap
mèsi
didi madloba
sagolun
ありがとう
arigatô
takk
dakujem
trugarez
najis tuke
tanemirt
grazie
terima kasih
rahmet
kam sah hamnida
rahmat
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
ευχαριστώ
merci