Workshop on cybersecurity assurance practices
23 May 2023, Geneva

Cybersecurity Assurance Practices at Member State Level

Speaker: Francisco Fonseca
VP National Cybersecurity

BITSIGHT

What are Cybersecurity Assurance Practices?

“Cybersecurity assurance practices can take many forms, they can be industry lead self-regulation, guidelines issued to consumers or industry from national and international bodies, or national and international regulations imposed on manufacturers. All these combine to form updated best practices to ensure the protection of our electronic devices.”

“Cyber Security Assurance Practices refer to a set of methodologies, processes, and controls designed to ensure the confidentiality, integrity, and availability of an organization's information systems and data. These practices are aimed at minimizing the risks associated with cyber threats and maintaining a secure computing environment.”

“Cyber Security Assurance Practices are a set of activities that are designed to ensure that an organization's systems, networks, and data are protected against cyber threats. These practices are used to validate the security of an organization's information technology (IT) infrastructure, to identify potential vulnerabilities, and to implement measures to mitigate risks.”

Sources: OpenAI ChatGPT, Access Partnership, Contribution numbered SG2RGQ/48-E;

What?

What are Cybersecurity Assurance Practices?

“Cybersecurity assura
industry from nationa
combine to form upd

issued to consumers or
acturers. All these

“Cyber Security Assur
integrity, and availabi
associated with cyber

ure the confidentiality,
imizing the risks

“Cyber Security Assur
data are protected ag
technology (IT) infras

ystems, networks, and
s information
ks.”

What?

Umbrella term: Regulations / guidelines / methodologies / processes / controls / activities

Can be **proposed** or **imposed** (by National or International Bodies)

Sources: OpenAI ChatGPT, Access Partnership, Contribution numbered SG2RGQ/48-E;

Goal?

Their **Goal** is to **ensure:**

- the **protection** of our electronic devices
- individual system components can adequately **protect** themselves from attacks
- that an organization's systems, networks, and data are **protected** against cyber threats
- the confidentiality, integrity, and availability of an organization's information systems and data
- validate the security of an organization's information technology (IT) infrastructure

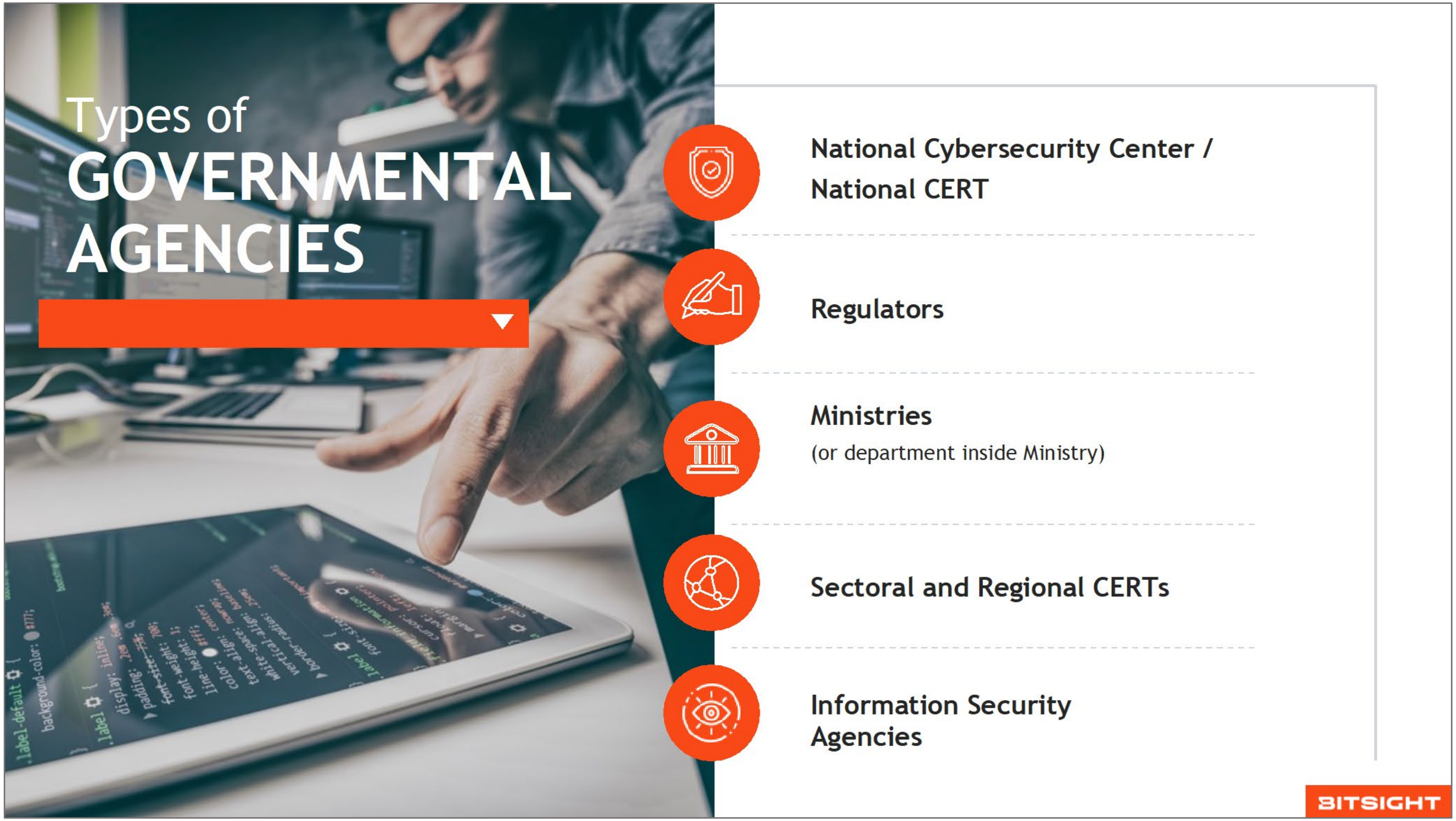
and…

- **identification** potential **vulnerabilities** and **cyber threats**
- minimize / mitigate the **risks**

Sources: OpenAI ChatGPT, Access Partnership, Contribution numbered SG2RGQ/48-E;

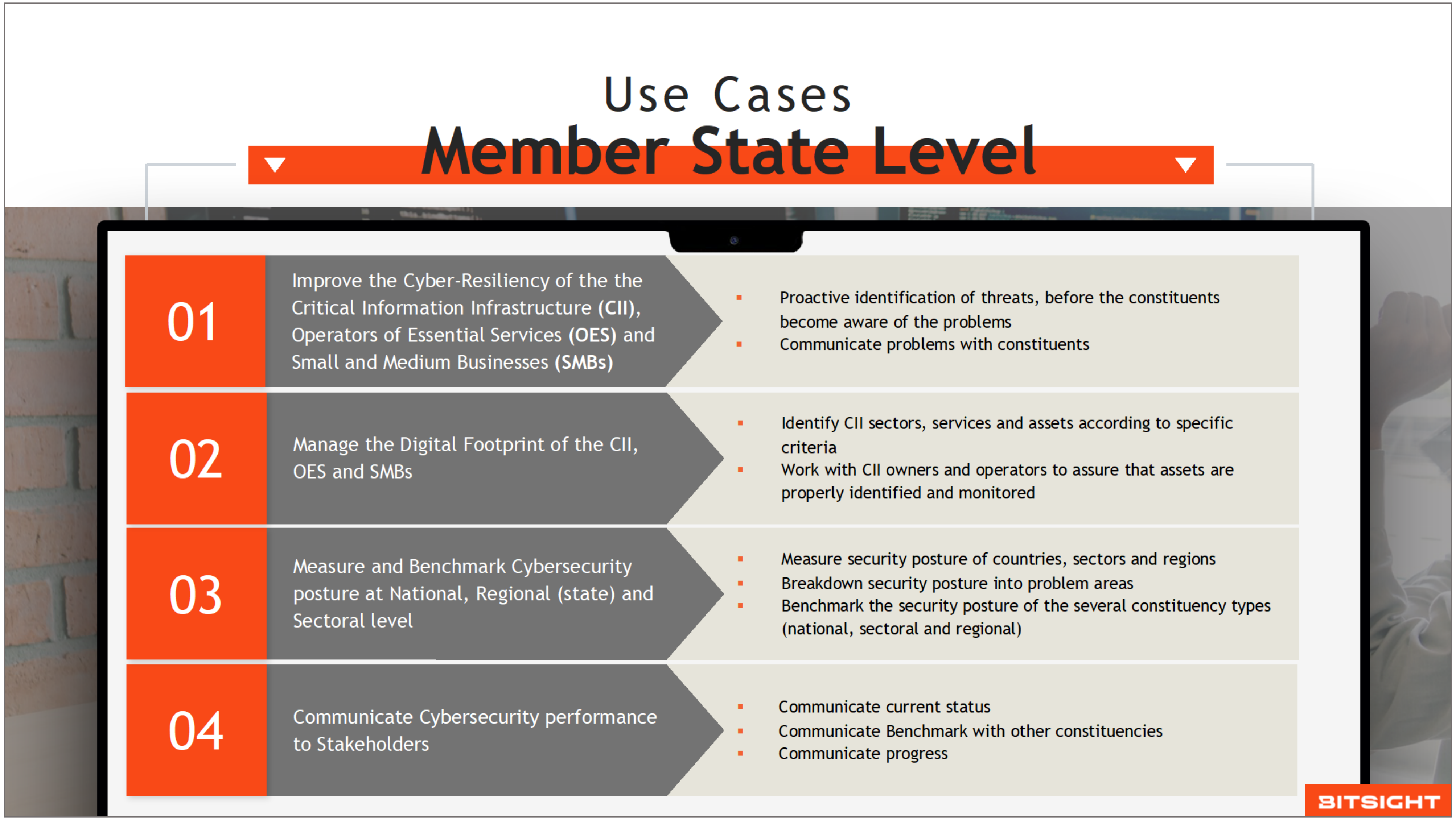
What are Cybersecurity Assurance Practices?

- **Are:** Regulations / guidelines / methodologies / processes / controls / set of activities
- **Can be: proposed** (Industry lead) or **imposed** (by National or International Bodies)
- **Their goal** is to ensure **protection** (devices, systems, networks and data) and **identification** of **vulnerabilities** and **threats**
- **So that risks** can be **mitigated**
- They are **dynamic,** not just a one-time effort



Types of GOVERNMENTAL AGENCIES

- National Cybersecurity Center / National CERT
- Regulators
- Ministries
  (or department inside Ministry)
- Sectoral and Regional CERTs
- Information Security Agencies



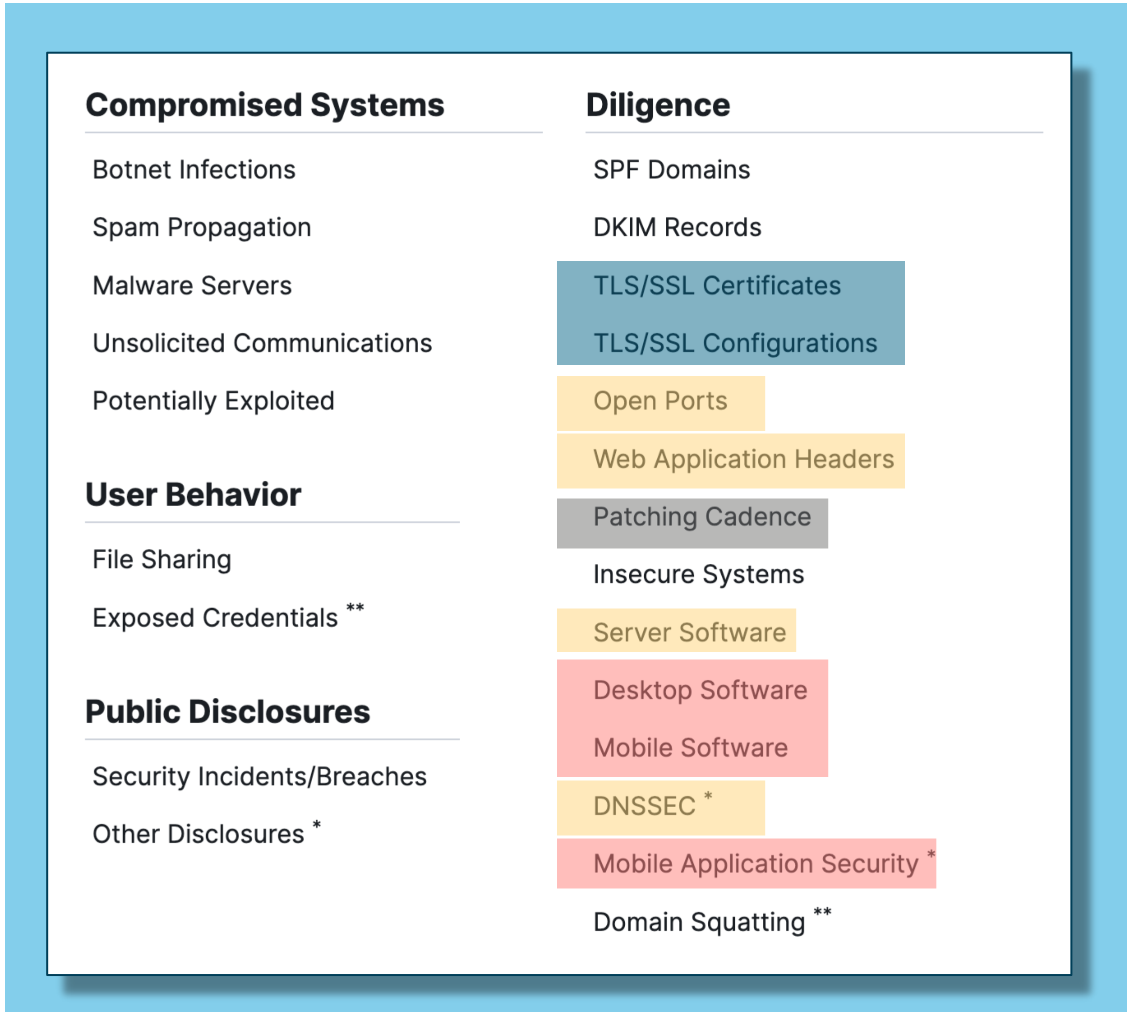
Use Cases
Member State Level

01	Improve the Cyber-Resiliency of the the Critical Information Infrastructure **(CII)**, Operators of Essential Services **(OES)** and Small and Medium Businesses **(SMBs)**	▪ Proactive identification of threats, before the constituents become aware of the problems ▪ Communicate problems with constituents
02	Manage the Digital Footprint of the CII, OES and SMBs	▪ Identify CII sectors, services and assets according to specific criteria ▪ Work with CII owners and operators to assure that assets are properly identified and monitored
03	Measure and Benchmark Cybersecurity posture at National, Regional (state) and Sectoral level	▪ Measure security posture of countries, sectors and regions ▪ Breakdown security posture into problem areas ▪ Benchmark the security posture of the several constituency types (national, sectoral and regional)
04	Communicate Cybersecurity performance to Stakeholders	▪ Communicate current status ▪ Communicate Benchmark with other constituencies ▪ Communicate progress

BITSIGHT

Identify	• Risk assessment • Regular audits and compliance • Security policies and procedures
Protect	• Security awareness training • Vulnerability management • Network security • Endpoint security • Data protection and encryption • Access control
Detect	• Security Continuous Monitoring
Respond	
Recover	

Risk Assessment



Compromised Systems

- Botnet Infections
- Spam Propagation
- Malware Servers
- Unsolicited Communications
- Potentially Exploited

User Behavior

- File Sharing
- Exposed Credentials **

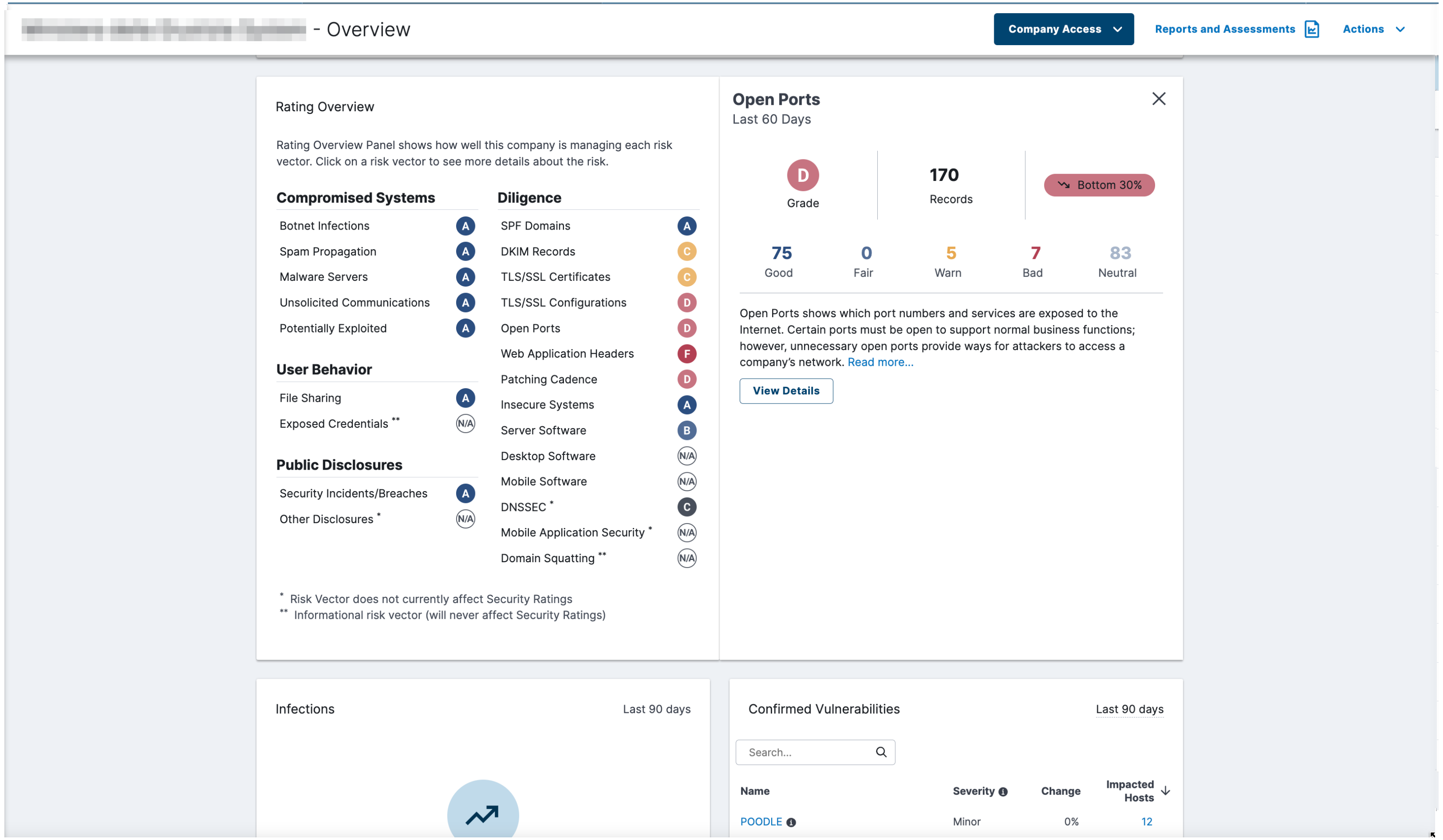
Public Disclosures

- Security Incidents/Breaches
- Other Disclosures *

Diligence

- SPF Domains
- DKIM Records
- TLS/SSL Certificates
- TLS/SSL Configurations
- Open Ports
- Web Application Headers
- Patching Cadence
- Insecure Systems
- Server Software
- Desktop Software
- Mobile Software
- DNSSEC *
- Mobile Application Security *
- Domain Squatting **

Risk Assessment



[redacted] - Overview

Rating Overview

Rating Overview Panel shows how well this company is managing each risk vector. Click on a risk vector to see more details about the risk.

Compromised Systems	
Botnet Infections	A
Spam Propagation	A
Malware Servers	A
Unsolicited Communications	A
Potentially Exploited	A

User Behavior	
File Sharing	A
Exposed Credentials **	N/A

Public Disclosures	
Security Incidents/Breaches	A
Other Disclosures *	N/A

Diligence	
SPF Domains	A
DKIM Records	C
TLS/SSL Certificates	C
TLS/SSL Configurations	D
Open Ports	D
Web Application Headers	F
Patching Cadence	D
Insecure Systems	A
Server Software	B
Desktop Software	N/A
Mobile Software	N/A
DNSSEC *	C
Mobile Application Security *	N/A
Domain Squatting **	N/A

* Risk Vector does not currently affect Security Ratings
** Informational risk vector (will never affect Security Ratings)

Open Ports
Last 60 Days

D Grade | 170 Records | Bottom 30%

75	0	5	7	83
Good	Fair	Warn	Bad	Neutral

Open Ports shows which port numbers and services are exposed to the Internet. Certain ports must be open to support normal business functions; however, unnecessary open ports provide ways for attackers to access a company's network. Read more...

View Details

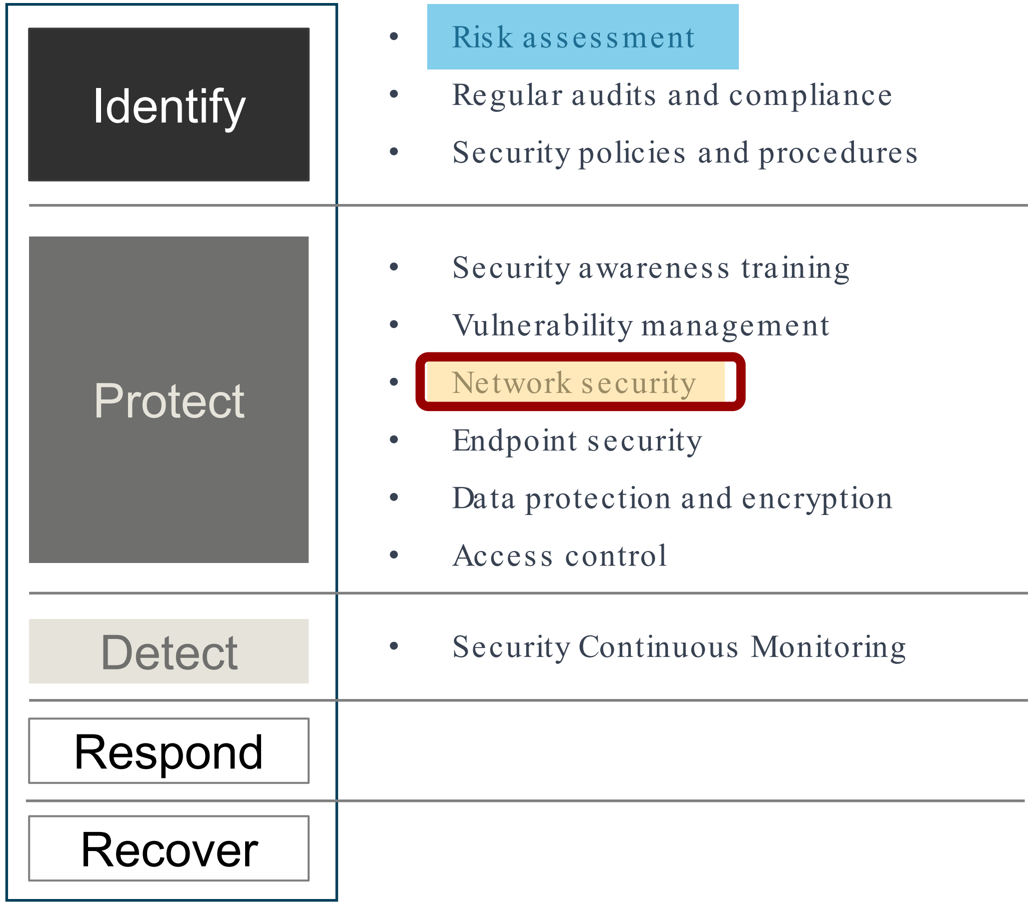
Infections Last 90 days

Confirmed Vulnerabilities Last 90 days

Search...

Name	Severity	Change	Impacted Hosts
POODLE	Minor	0%	12

Assessing Risks in the Critical Information Infrastructure of a Member State



Identify

- Risk assessment
- Regular audits and compliance
- Security policies and procedures

Protect

- Security awareness training
- Vulnerability management
- Network security
- Endpoint security
- Data protection and encryption
- Access control

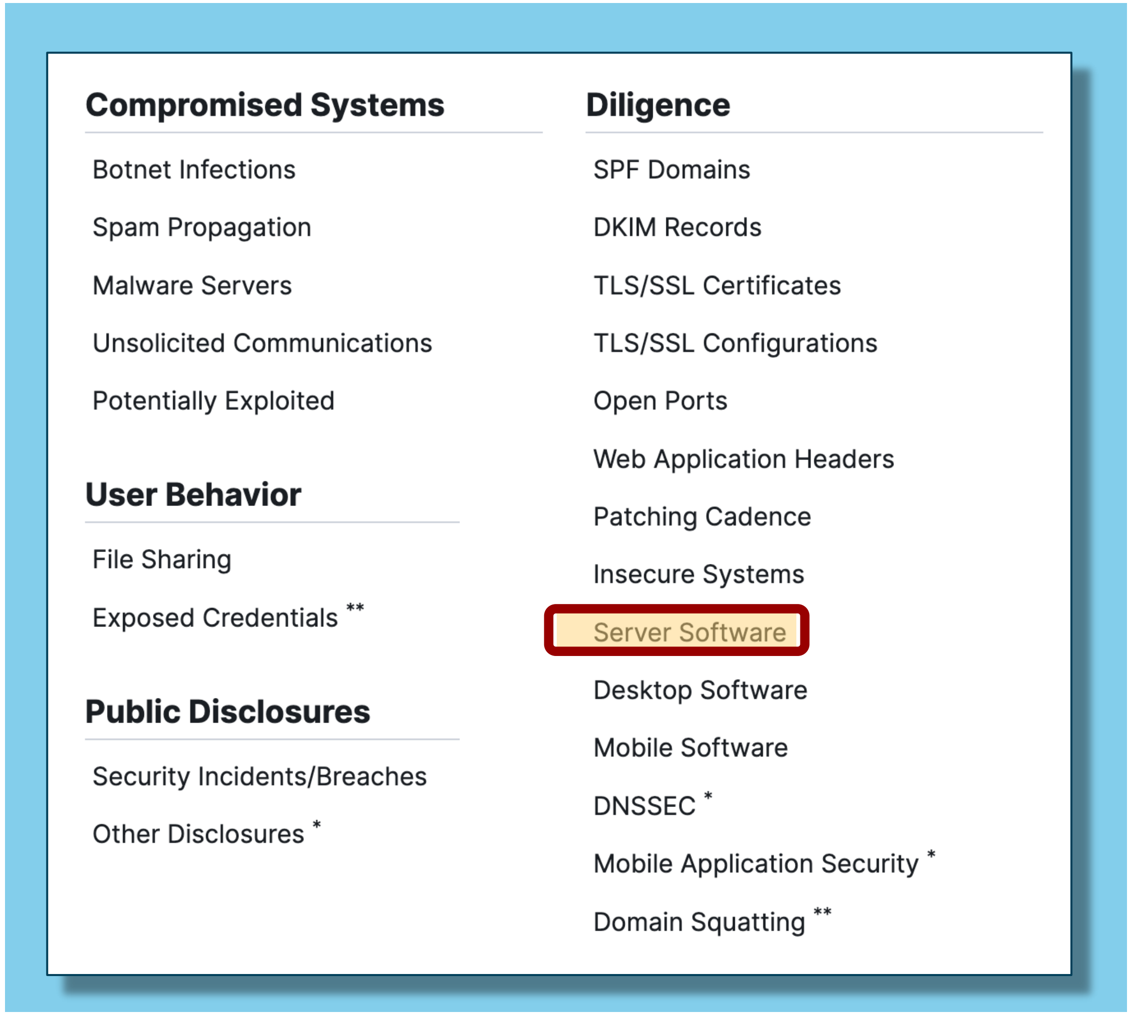
Detect

- Security Continuous Monitoring

Respond

Recover

Risk Assessment



Compromised Systems

Botnet Infections

Spam Propagation

Malware Servers

Unsolicited Communications

Potentially Exploited

User Behavior

File Sharing

Exposed Credentials **

Public Disclosures

Security Incidents/Breaches

Other Disclosures *

Diligence

SPF Domains

DKIM Records

TLS/SSL Certificates

TLS/SSL Configurations

Open Ports

Web Application Headers

Patching Cadence

Insecure Systems

Server Software

Desktop Software

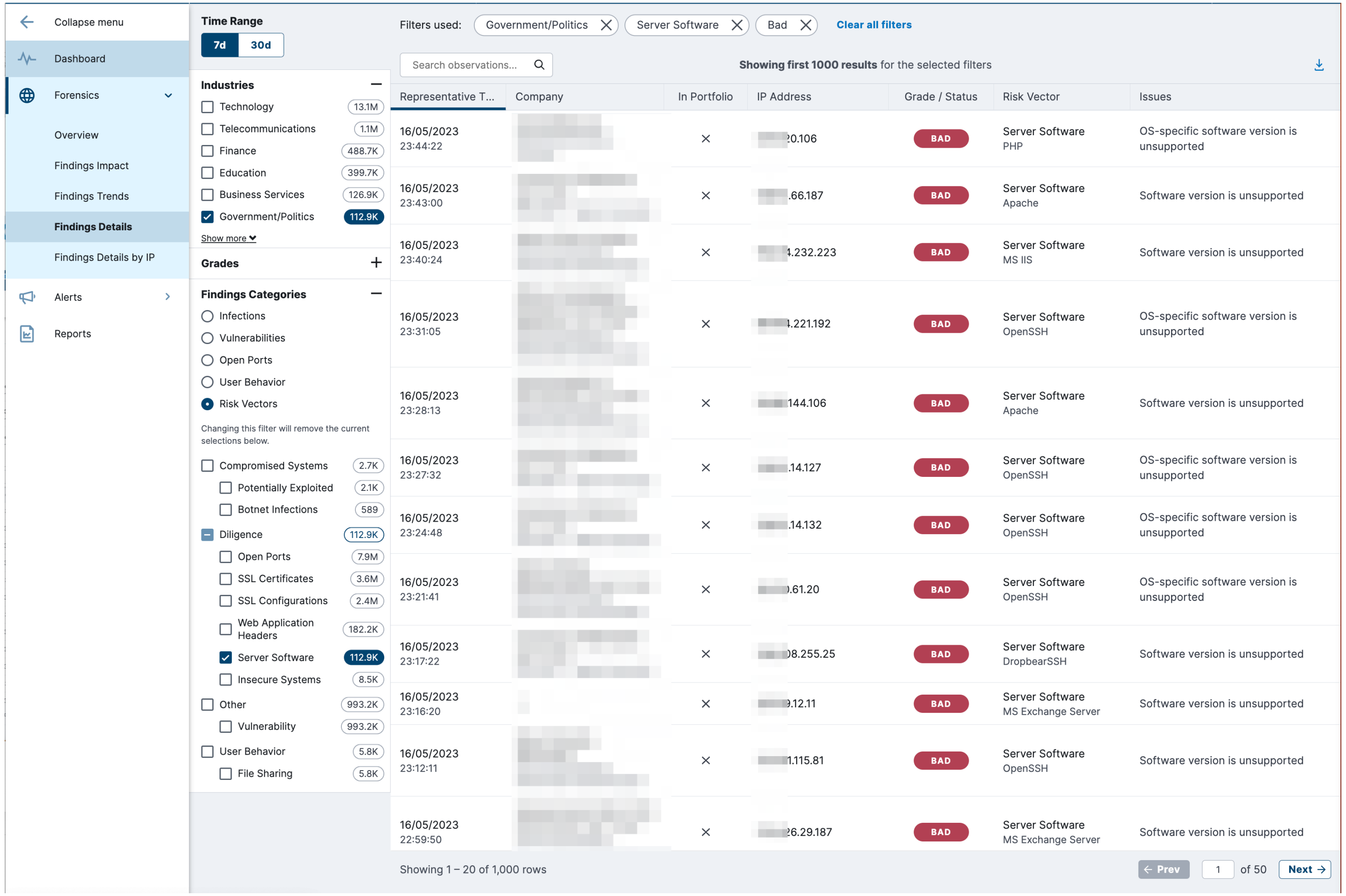
Mobile Software

DNSSEC *

Mobile Application Security *

Domain Squatting **

Risk Assessment at National Level – Server Software



Collapse menu
Dashboard
Forensics
Overview
Findings Impact
Findings Trends
Findings Details
Findings Details by IP
Alerts
Reports

Time Range
7d | 30d

Industries

- □ Technology 13.1M
- □ Telecommunications 1.1M
- □ Finance 488.7K
- □ Education 399.7K
- □ Business Services 126.9K
- ☑ Government/Politics 112.9K

Show more

Grades +

Findings Categories

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

Changing this filter will remove the current selections below.

- □ Compromised Systems 2.7K
  - □ Potentially Exploited 2.1K
  - □ Botnet Infections 589
- ⊟ Diligence 112.9K
  - □ Open Ports 7.9M
  - □ SSL Certificates 3.6M
  - □ SSL Configurations 2.4M
  - □ Web Application Headers 182.2K
  - ☑ Server Software 112.9K
  - □ Insecure Systems 8.5K
- □ Other 993.2K
  - □ Vulnerability 993.2K
- □ User Behavior 5.8K
  - □ File Sharing 5.8K

Filters used: Government/Politics ✕ | Server Software ✕ | Bad ✕ | Clear all filters

Search observations...

Showing first 1000 results for the selected filters

Representative T...	Company	In Portfolio	IP Address	Grade / Status	Risk Vector	Issues
16/05/2023 23:44:22	[redacted]	×	[redacted]20.106	BAD	Server Software PHP	OS-specific software version is unsupported
16/05/2023 23:43:00	[redacted]	×	[redacted].66.187	BAD	Server Software Apache	Software version is unsupported
16/05/2023 23:40:24	[redacted]	×	[redacted]4.232.223	BAD	Server Software MS IIS	Software version is unsupported
16/05/2023 23:31:05	[redacted]	×	[redacted]4.221.192	BAD	Server Software OpenSSH	OS-specific software version is unsupported
16/05/2023 23:28:13	[redacted]	×	[redacted]144.106	BAD	Server Software Apache	Software version is unsupported
16/05/2023 23:27:32	[redacted]	×	[redacted].14.127	BAD	Server Software OpenSSH	OS-specific software version is unsupported
16/05/2023 23:24:48	[redacted]	×	[redacted].14.132	BAD	Server Software OpenSSH	OS-specific software version is unsupported
16/05/2023 23:21:41	[redacted]	×	[redacted].61.20	BAD	Server Software OpenSSH	OS-specific software version is unsupported
16/05/2023 23:17:22	[redacted]	×	[redacted]08.255.25	BAD	Server Software DropbearSSH	Software version is unsupported
16/05/2023 23:16:20	[redacted]	×	[redacted]9.12.11	BAD	Server Software MS Exchange Server	Software version is unsupported
16/05/2023 23:12:11	[redacted]	×	[redacted]1.115.81	BAD	Server Software OpenSSH	Software version is unsupported
16/05/2023 22:59:50	[redacted]	×	[redacted]26.29.187	BAD	Server Software MS Exchange Server	Software version is unsupported

Showing 1 – 20 of 1,000 rows

← Prev | 1 | of 50 | Next →

Identifying unsupported software in all the IP addresses of a Member State

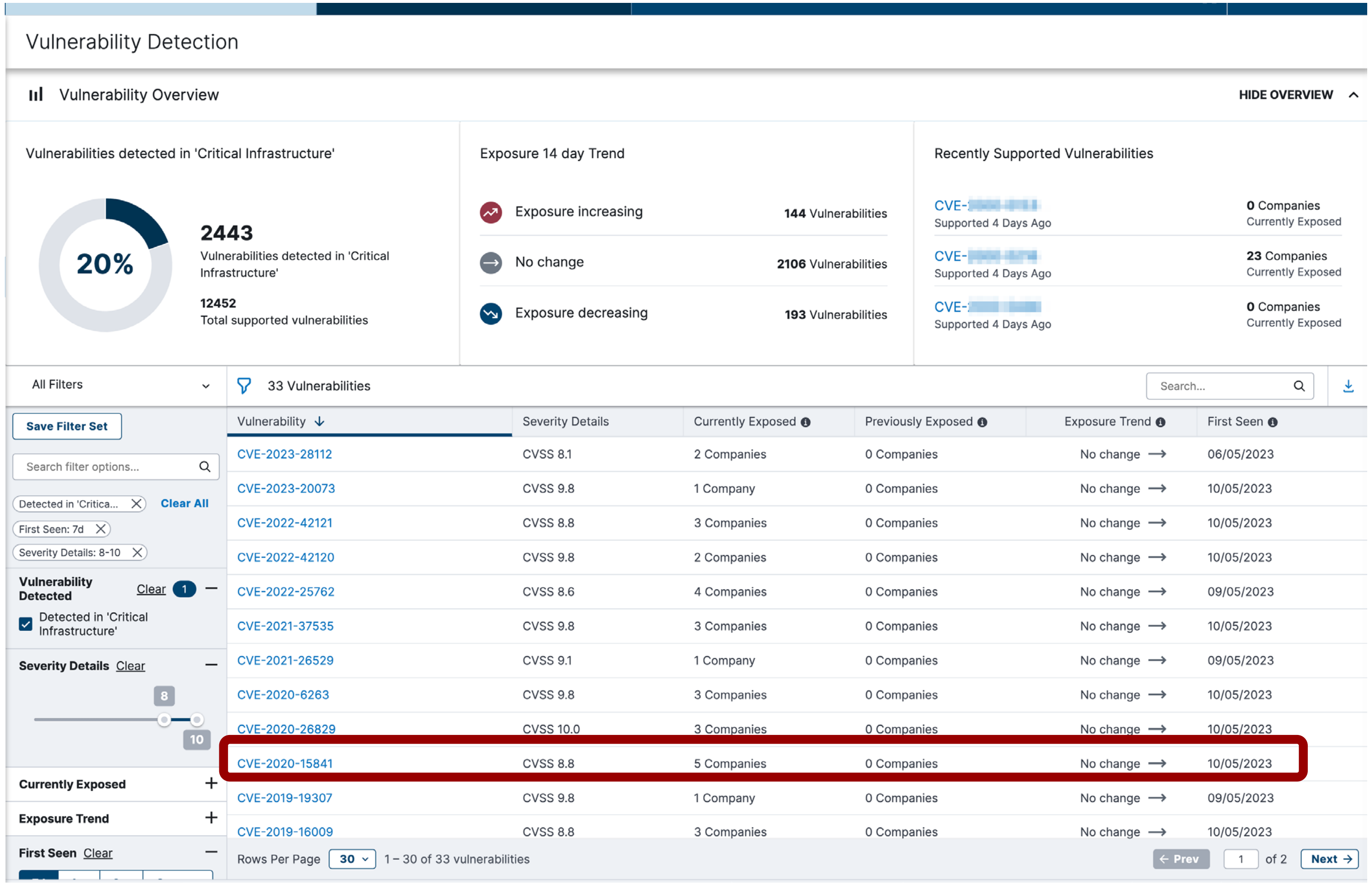
Identify	- Risk assessment - Regular audits and compliance - Security policies and procedures
Protect	- Security awareness training - Vulnerability management - Network security - Endpoint security - Data protection and encryption - Access control
Detect	- Security Continuous Monitoring
Respond	
Recover	

Ramsonware

Ransomware typically infiltrates organizations through a variety of methods, but the following are the most common:

- Phishing Emails
- Exploit Kits (vulnerabilities / non-updated software)
- Remote Desktop Protocol (RDP)
- Malicious Websites or Ads (Malvertising)

Identifying Vulnerabilities in the CII of a Member State



Vulnerability Detection

Vulnerability Overview

HIDE OVERVIEW

Vulnerabilities detected in 'Critical Infrastructure'

20%

2443
Vulnerabilities detected in 'Critical Infrastructure'

12452
Total supported vulnerabilities

Exposure 14 day Trend

Exposure increasing	**144** Vulnerabilities
No change	**2106** Vulnerabilities
Exposure decreasing	**193** Vulnerabilities

Recently Supported Vulnerabilities

CVE-[redacted] Supported 4 Days Ago	**0** Companies Currently Exposed
CVE-[redacted] Supported 4 Days Ago	**23** Companies Currently Exposed
CVE-[redacted] Supported 4 Days Ago	**0** Companies Currently Exposed

All Filters

Save Filter Set

Search filter options...

Detected in 'Critica... ✕ Clear All

First Seen: 7d ✕

Severity Details: 8-10 ✕

Vulnerability Detected Clear 1

☑ Detected in 'Critical Infrastructure'

Severity Details Clear

8 – 10

Currently Exposed +

Exposure Trend +

First Seen Clear

33 Vulnerabilities

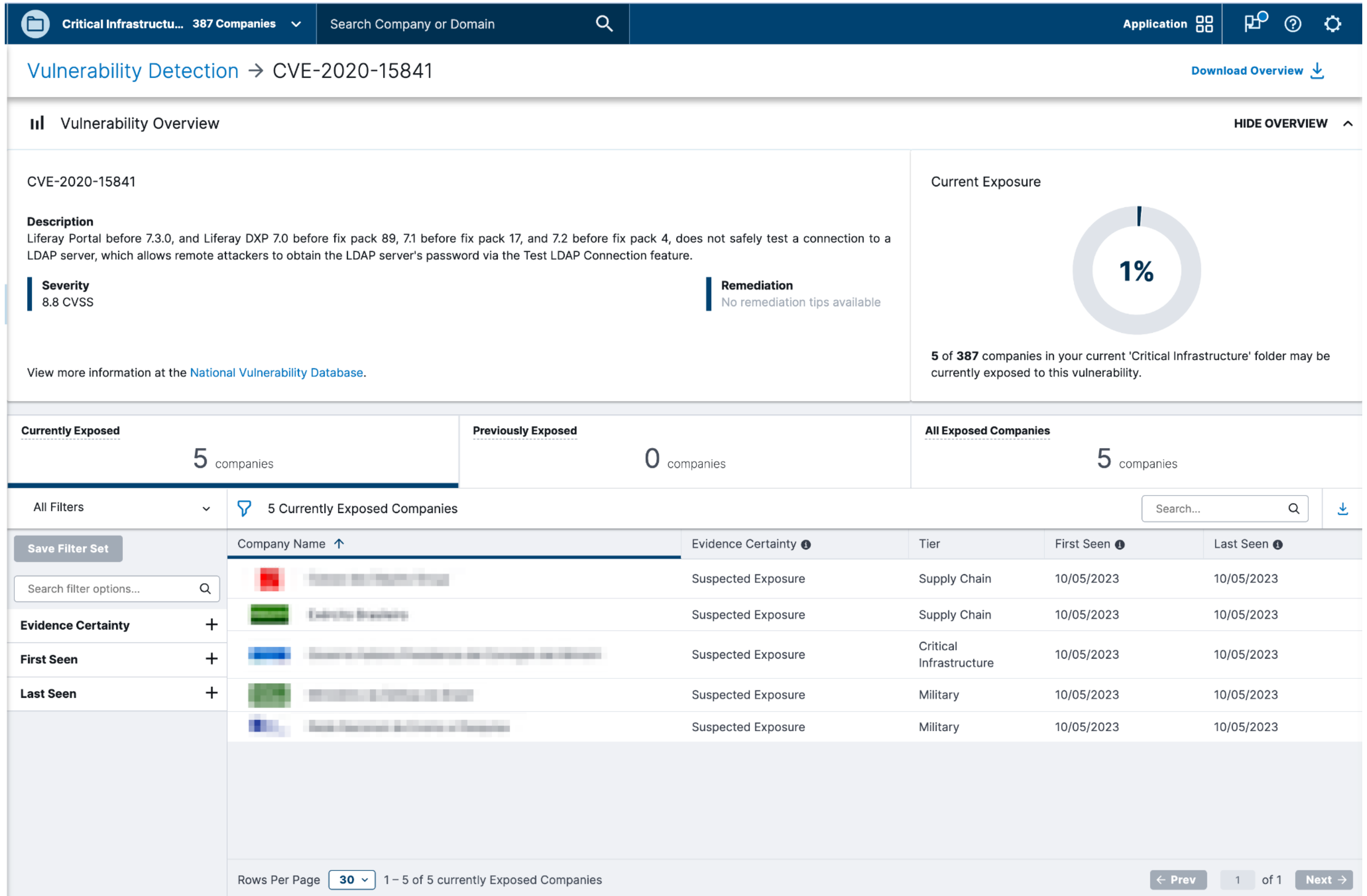
Search...

Vulnerability	Severity Details	Currently Exposed	Previously Exposed	Exposure Trend	First Seen
CVE-2023-28112	CVSS 8.1	2 Companies	0 Companies	No change →	06/05/2023
CVE-2023-20073	CVSS 9.8	1 Company	0 Companies	No change →	10/05/2023
CVE-2022-42121	CVSS 8.8	3 Companies	0 Companies	No change →	10/05/2023
CVE-2022-42120	CVSS 9.8	2 Companies	0 Companies	No change →	10/05/2023
CVE-2022-25762	CVSS 8.6	4 Companies	0 Companies	No change →	09/05/2023
CVE-2021-37535	CVSS 9.8	3 Companies	0 Companies	No change →	10/05/2023
CVE-2021-26529	CVSS 9.1	1 Company	0 Companies	No change →	09/05/2023
CVE-2020-6263	CVSS 9.8	3 Companies	0 Companies	No change →	10/05/2023
CVE-2020-26829	CVSS 10.0	3 Companies	0 Companies	No change →	10/05/2023
CVE-2020-15841	CVSS 8.8	5 Companies	0 Companies	No change →	10/05/2023
CVE-2019-19307	CVSS 9.8	1 Company	0 Companies	No change →	09/05/2023
CVE-2019-16009	CVSS 8.8	3 Companies	0 Companies	No change →	10/05/2023

Rows Per Page 30 1 – 30 of 33 vulnerabilities

← Prev 1 of 2 Next →

Identifying Vulnerabilities in the CII of a Member State



Vulnerability Detection → CVE-2020-15841

Vulnerability Overview

CVE-2020-15841

Description
Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 89, 7.1 before fix pack 17, and 7.2 before fix pack 4, does not safely test a connection to a LDAP server, which allows remote attackers to obtain the LDAP server's password via the Test LDAP Connection feature.

Severity
8.8 CVSS

Remediation
No remediation tips available

View more information at the National Vulnerability Database.

Current Exposure

5 of **387** companies in your current 'Critical Infrastructure' folder may be currently exposed to this vulnerability.

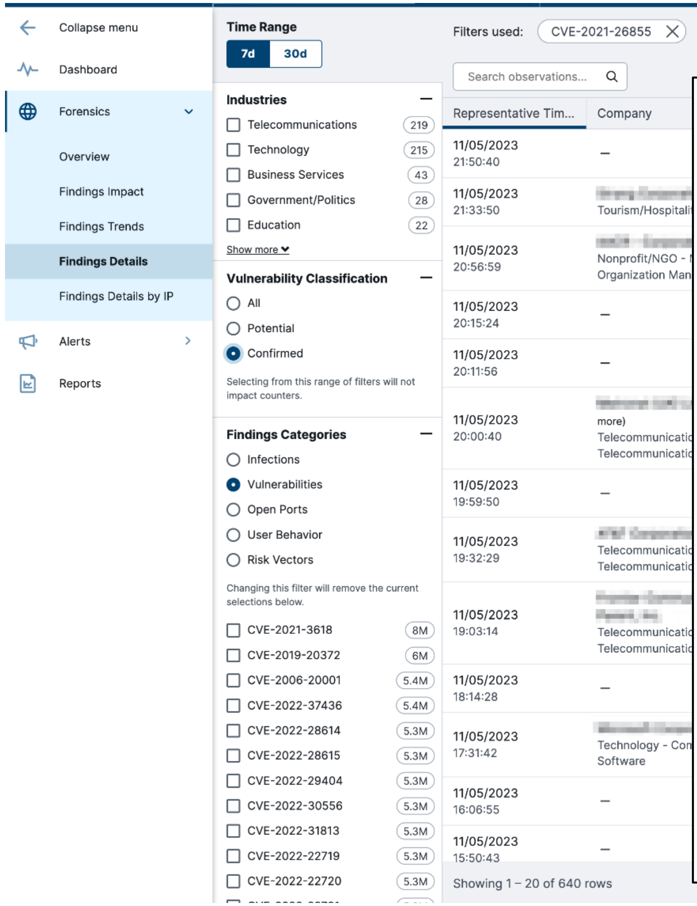
Currently Exposed	Previously Exposed	All Exposed Companies
5 companies	0 companies	5 companies

5 Currently Exposed Companies

Company Name ↑	Evidence Certainty	Tier	First Seen	Last Seen
[redacted]	Suspected Exposure	Supply Chain	10/05/2023	10/05/2023
[redacted]	Suspected Exposure	Supply Chain	10/05/2023	10/05/2023
[redacted]	Suspected Exposure	Critical Infrastructure	10/05/2023	10/05/2023
[redacted]	Suspected Exposure	Military	10/05/2023	10/05/2023
[redacted]	Suspected Exposure	Military	10/05/2023	10/05/2023

Rows Per Page 30 1 – 5 of 5 currently Exposed Companies

Identifying Vulnerabilities in a Member State (All IP addresses)



Time Range: 7d | 30d

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

Search observations...

Industries

- □ Telecommunications 219
- □ Technology 215
- □ Business Services 43
- □ Government/Politics 28
- □ Education 22

Show more

Vulnerability Classification

- ○ All
- ○ Potential
- ● Confirmed

Selecting from this range of filters will not impact counters.

Findings Categories

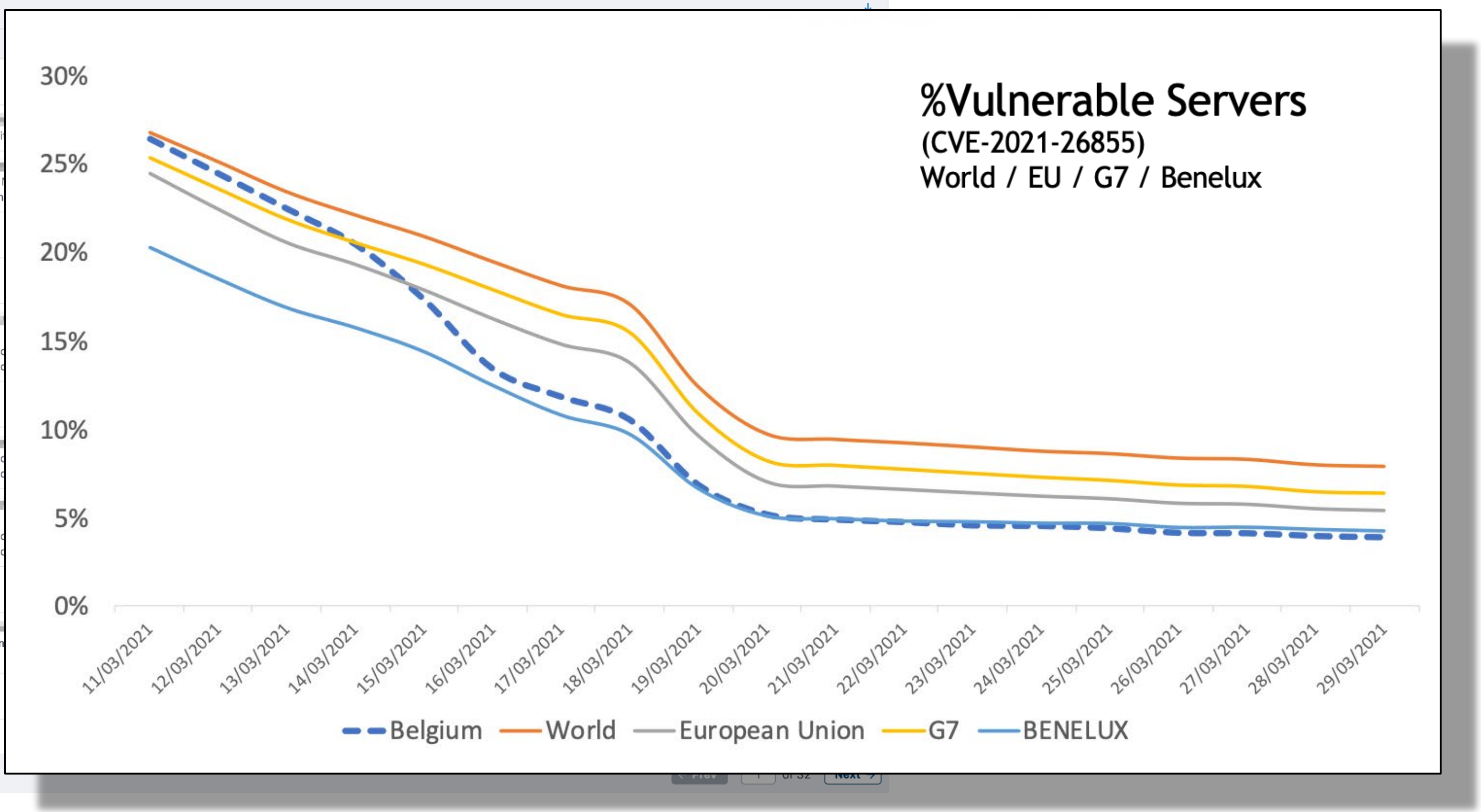
- ○ Infections
- ● Vulnerabilities
- ○ Open Ports
- ○ User Behavior
- ○ Risk Vectors

Changing this filter will remove the current selections below.

- □ CVE-2021-3618 8M
- □ CVE-2019-20372 6M
- □ CVE-2006-20001 5.4M
- □ CVE-2022-37436 5.4M
- □ CVE-2022-28614 5.3M
- □ CVE-2022-28615 5.3M
- □ CVE-2022-29404 5.3M
- □ CVE-2022-30556 5.3M
- □ CVE-2022-31813 5.3M
- □ CVE-2022-22719 5.3M
- □ CVE-2022-22720 5.3M

Representative Tim...	Company
11/05/2023 21:50:40	–
11/05/2023 21:33:50	[redacted] Tourism/Hospitali
11/05/2023 20:56:59	[redacted] Nonprofit/NGO - I Organization Man
11/05/2023 20:15:24	–
11/05/2023 20:11:56	–
11/05/2023 20:00:40	[redacted] more) Telecommunicatio Telecommunicatio
11/05/2023 19:59:50	–
11/05/2023 19:32:29	[redacted] Telecommunicatio Telecommunicatio
11/05/2023 19:03:14	[redacted] Telecommunicatio Telecommunicatio
11/05/2023 18:14:28	–
11/05/2023 17:31:42	[redacted] Technology - Con Software
11/05/2023 16:06:55	–
11/05/2023 15:50:43	–

Showing 1 – 20 of 640 rows


%Vulnerable Servers
(CVE-2021-26855)
World / EU / G7 / Benelux

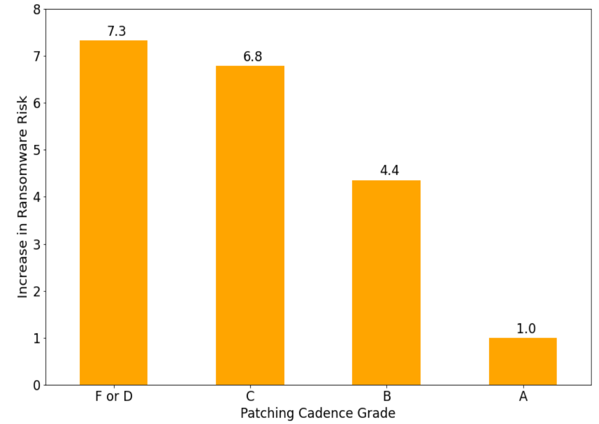
Assure Patching Vulnerabilities and up-to-date Software

Marsh McLennan in a study in October 2022 sought to **quantify** the **relationship** between **data analytics** and Marsh McLennan's **cybersecurity incident data** (2018-2021). After comparing the security performance data of thousands of organizations that experienced cybersecurity incidents against those that did not, Marsh McLennan found that:

1. **Patching Cadence** was most strongly correlated to cybersecurity incidents (risk vector, which measures the rate at which organizations remediate important vulnerabilities)
2. Followed by **updated desktop** and **mobile software** and observed **exploited devices**

With trusted, proven, objective analytics regulators and government officials can make more informed policy decisions and perform better cybersecurity oversight.

Many of these results are consistent with earlier BitSight analyses (e.g. poor performance in the Patching Cadence risk vector was known to be highly correlated with ransomware incidents)



https://www.bitsight.com/blog/ransomware-prevention

Sources: https://www.bitsight.com/blog/new-study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity-incidents

Thank you!

Speaker: Francisco Fonseca
VP National Cybersecurity

BITSIGHT