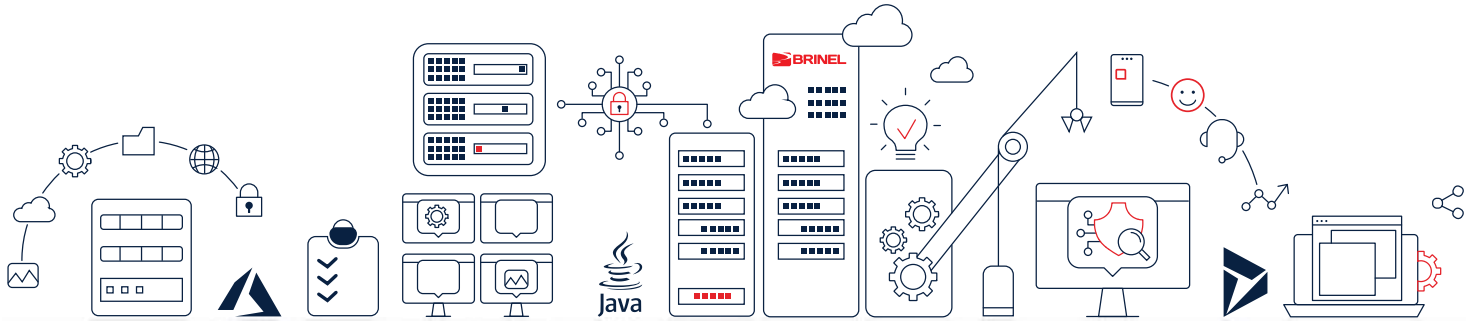
# GET NIS2 READY WITH




# CYBERSECURITY READINESS JOURNEY



**14 MAI 2024, JW MARRIOTT, BUCURESTI**

# AGENDA

| ORA | PREZENTARE | |
|---|---|---|
| 15:00 - 15:30 | **Welcome coffee** | |
| 15:30 - 15:45 | Keynote BRINEL | Bogdan Mustata – Sales Manager **\| BRINEL** |
| 15:45 - 16:15 | Overview NIS2 | Radu Stanescu, Auditor de NIS2 **\| Sandline** |
| 16:15 - 16:45 | Fortinet AI Driven Security Operations for NIS2 compliance | Andrei Peretianu, SecOps Business Development Manager SEE **\| Fortinet** |
| 16:45 – 17:00 | **Coffee Break** | |
| 17:00 – 17:45 | Bounce forward with Radical Resilience | Dan Popa, Regional Manager SEE **\| Veeam Software** |
| | How Veeam can help with NIS2 Directive | Cornel Popescu, Senior Systems Engineer **\| Veeam Software** |
| 17:45 – 18:15 | Employee a CyberSec Asset – Demo Fortra Terranova Security | Bogdan Maracine, Senior System Engineer **\| BRINEL** |
| 18:15 - 20:00 | **Dinner & Networking** | |

# BRINEL PARTE A iQANTO, GROUPE SNEF

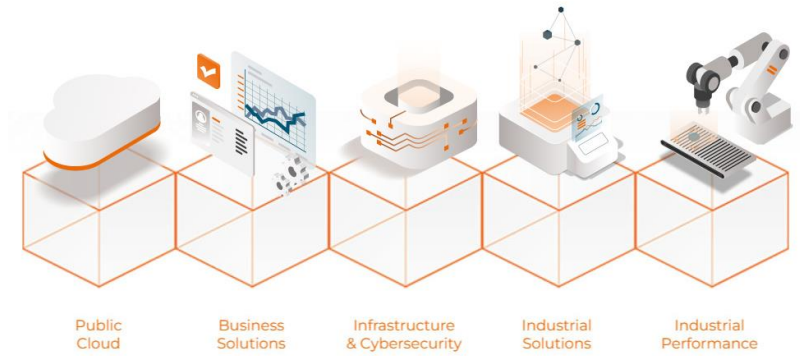
## Despre **iQanto**:

Născut din fuziunea companiilor din **Grupul Snef**, inclusiv **BRINEL**, **iQanto** reunește expertiza digitală și robotică a aproape 900 de colaboratori într-un lanț valoric integrat și extins, centrat pe transformarea digitală.: Data Science, UX/UI, IT, Cloud, Cybersecurity, Automation, Internet of Things, Robotics, and Collaborative Robotics (Cobotics).

- Europe
- Africa
- Australia
- Brazil
- United States

**1,6**
Billion euros in turnover

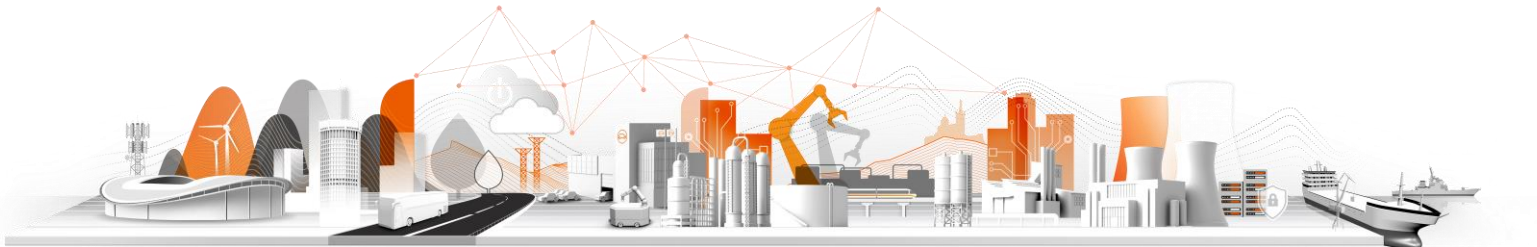
**12.500**
Collaborators




## Despre **Groupe Snef**

Având capacitatea de a interveni de la inceputul si pana la finalul ciclului de viață al instalațiilor dvs., ne-am construit grupul în jurul unui spectru larg de abilități tehnice. Suntem ingineri/proiectanți, integratori, întreținători și operatori de soluții multi-tehnice în domeniile energiei, mecanicii și tehnologiei digitale. Ne reinventăm continuu, susținând revoluția digitală, internetul obiectelor, datele mari, securitatea cibernetică, industria 4.0, inteligența artificială și realitatea mixtă.

Din 2018, BRINEL face parte din Grupul SNEF.



# ABOUT **BRINEL**

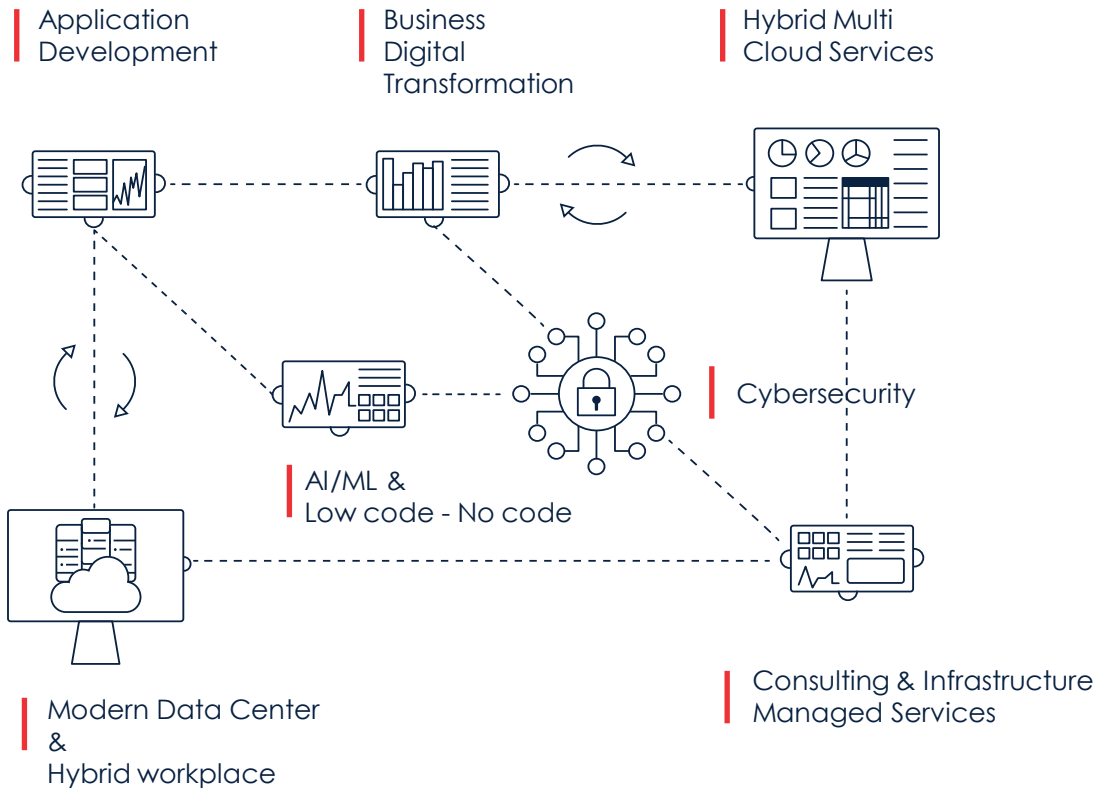

**200**
PROFESSIONALS

**500+**
CLIENTS

**32**
YEARS OF EXPERIENCE

**Brinel** face ca transformarea digitală să fie un proces fara intreruperi si accesibil companiilor din era Cloud și AI, oferind suport în fiecare etapă a proiectului: servicii de consiliere, proiectare, implementare și management.

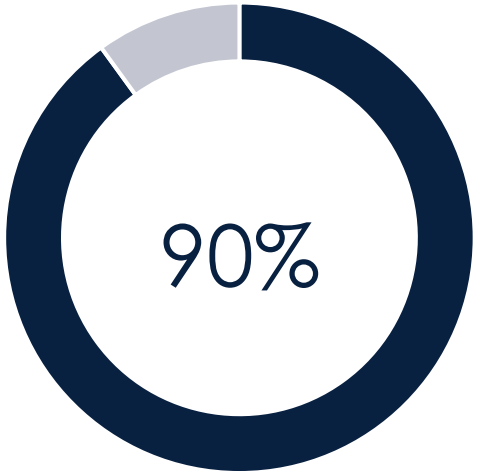
Oferim soluții si servicii IT avansate: **soluții moderne și durabile de centre de date**, **medii de lucru digitale**, **servicii în cloud**, **modernizarea aplicațiilor** folosind tehnologii open-source sau soluții low-code/fără cod, **AI/ML**, transformarea afacerii folosind **ERP**, soluții de **securitate cibernetică**, consultanta si servicii de administrare. Oferim soluții personalizate clienților nostri, indiferent de stadiul acestora în procesul de digitalizare. În plus, propriile noastre aplicații dezvoltate (**BRINEL Digital Tools**), îmbunătățesc interacțiunea cu echipele interne, clienții si partenerii.



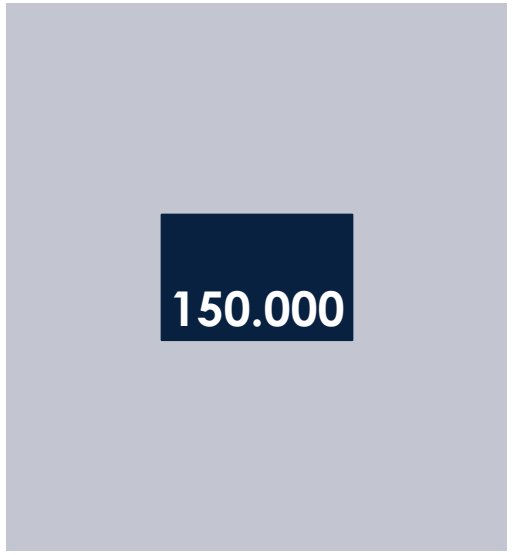
# Context de securitate cibernetică

$10.5 trillion

Costul criminalității cibernetice este estimat să atingă 10,5 trilioane de dolari anual până în 2025.

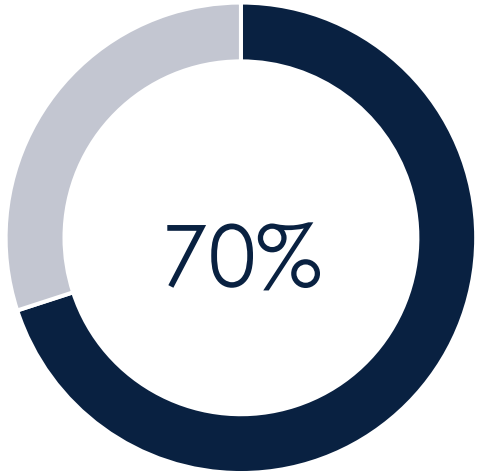



80-90% din toate compromisurile de „succes" ransomware provin din dispozitive negestionate




156,000 pe zi

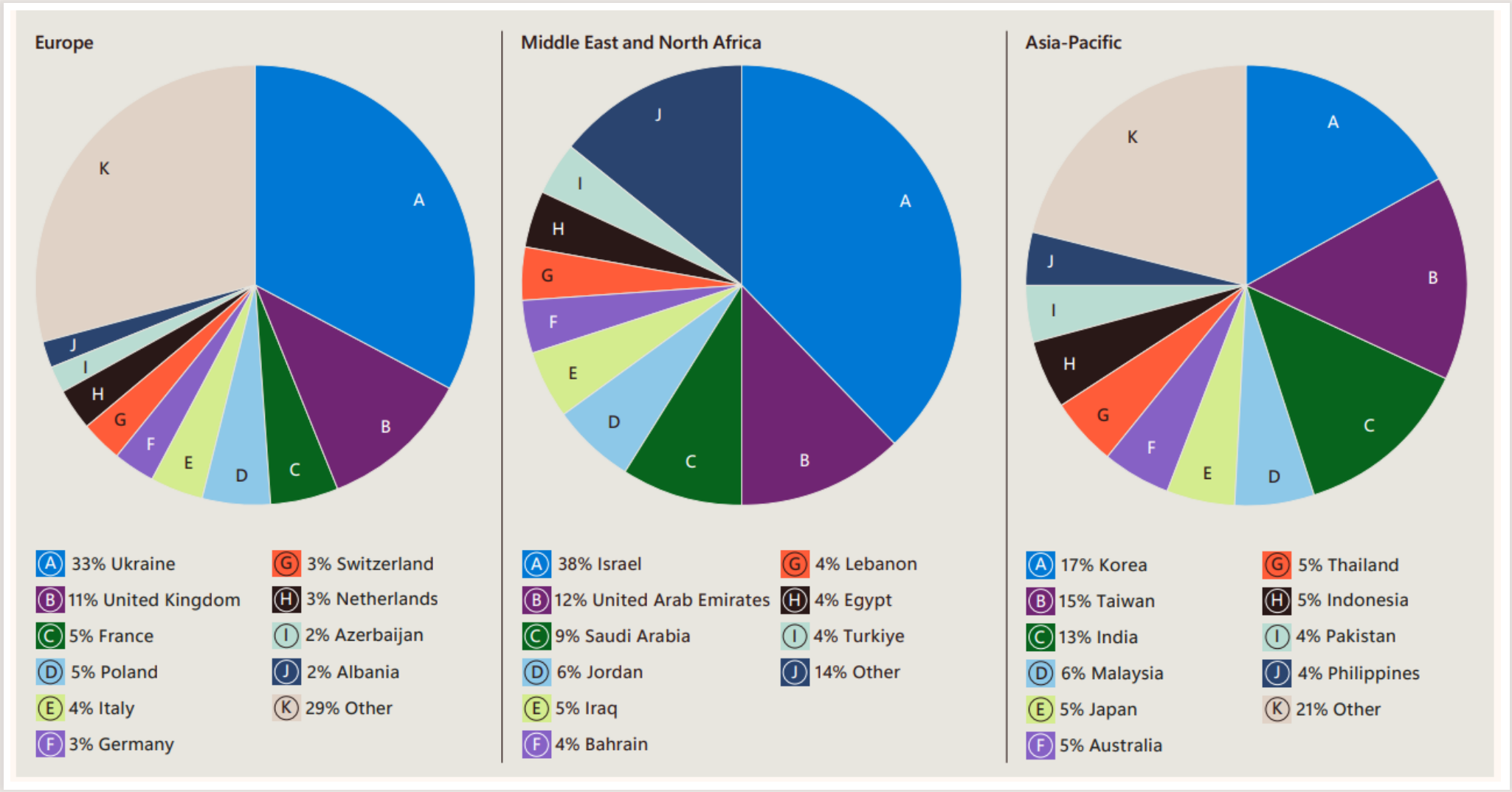
Încercări de compromitere a e-mailurilor de afaceri




70% dintre organizatii se confruntă cu ransomware operat de utilizatori aveau mai puțin de 500 de angajați

Source: Microsoft Digital Defense Report 2023

# Regiunile cele mai atacate cibernetic




Source: Microsoft Threat Intelligence events data

Source: Microsoft Digital Defense Report 2023

# Microsoft Defense Report

## 65 trillion
signals synthesized daily

That is over 750 million signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

## 10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

## 4,000
identity attacks blocked per second

4,000 identity authentication threats blocked per second.

## 300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

## 100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

## 15,000+
partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

## 135 million
managed devices

135 million managed devices providing security and threat landscape insights.

All data is based on Microsoft fiscal year 2023 unless otherwise indicated.

BRINEL

# 5 REGULI DE SECURITATE CIBERNETICA

99%

Igiena de bază de securitate protejează împotriva a 99% din atacuri.

Source: Microsoft Digital Defense Report 2023

## 1. Activeaza Multi factor authentication (MFA)

Protejează împotriva parolelor de utilizator compromise și oferă un nivel suplimentar de protectie al identității

## 2. Aplica principiile Zero Trust

Verificați în mod explicit | Utilizați accesul cu cel mai mic privilegiu | Presupune încălcarea.

## 3. Utilizeaza XDR

Utilizați software de detectare extinsa, răspuns și antimalware pentru a detecta și bloca automat atacurile.

## 4. Fiti cu actualizarile la zi

Asigurați-vă că toate sistemele sunt menținute la zi, inclusiv firmware-ul, sistemul de operare și aplicațiile

## 5. Protejati-va datele

Cunoasteti-va datele importante, unde sunt localizate și dacă sunt implementate mecanismele de protectie adecvate

# Ce este NIS2?

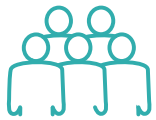
# NIS2

**N**etwork and **I**nformation **S**ecurity **D**irective

**Obiective:** atingerea unui **nivel comun ridicat de securitate cibernetică** în Uniunea Europeană prin

- ❑ Gestionarea riscului de Securitate
- ❑ Protejarea împotriva atacurilor cibernetice
- ❑ Detectarea incidentelor de securitate cibernetică
- ❑ Minimizarea impactului incidentelor de securitate cibernetică

## 1 Directiva | 4 Masuri



**CSIRT Team** - **C**omputer **S**ecurity **I**ncident **R**esponse **T**eams autoritatea națională responsabilă cu strategia națională de securitate cibernetică și gestionarea crizelor

Măsuri de **gestionare a riscurilor de securitate cibernetică** și obligații de **raportare**

**Reguli și obligații** privind partajarea informațiilor de securitate cibernetică

**Obligații de supraveghere și de sanctionare**

Source: Directive - 2022/2555 - EN - EUR-Lex (europa.eu)

BRINEL

# Cine este afectat?

Entitati **Esentiale** = companii cu peste 250 de angajați sau 50 de milioane de euro cifră de afaceri anuală

Entitati **Importante**= companii cu mai mult de 50 de angajați (nu mai mult de 250) sau mai mult de 10 milioane de euro cifra de afaceri

Indiferent de dimensiunea lor, prezenta directivă se aplică și la:

Sectoare foarte critice

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health sector
- Drinking water
- Wastewater
- Digital Infrastructure
- IT service management
- Public administration
- Space

Sectoare critice

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing of medical devices
- Digital providers
- Research organizations

Source: Directive - 2022/2555 - EN - EUR-Lex (europa.eu)

# Care sunt penalitățile?

Amenzi administrative

## Entitati Esentiale

**>10M € sau 2%** din totalul cifrei de afaceri anuale la nivel mondial

## Entitati Importante

**>1.7M € sau 1.4%** din totalul cifrei de afaceri anuale la nivel mondial

Masuri de sanctionare

**Suspendarea** temporara a **activitatii** companiei

**Interzice** exercitarea temporară a **funcțiilor manageriale**

**Directorii sunt răspunzători** pentru încălcarea obligațiilor lor de a asigura conformitatea

**Inspectii** On-site
**Supraveghere** Off-site
**Audituri de securitate** regulate și direcționate
**Audituri Ad hoc**

Source: Directive - 2022/2555 - EN - EUR-Lex (europa.eu)

# Ce trebuie sa faca companiile?

## Implementarea măsurilor de management al riscului de securitate cibernetică

| | | | |
|---|---|---|---|
| Gestionarea Riscului | Politici de securitate | Gestionarea incidentelor (prevenirea, detectarea & raspunsul la incidente) | Continuitatea afacerii și gestionarea crizelor |
| Securitatea lanțului de aprovizionare ia în considerare vulnerabilitățile furnizorilor | Gestionarea vulnerabilităților și comunicarea lor | Evaluări regulate pentru a determina eficacitatea măsurilor de gestionare a riscului de securitate cibernetică (de exemplu, reflectarea stadiului actual al tehnicii – postura de securitate) | |
| Utilizarea criptografiei și a criptării unde este justificat | Igienă de bază de securitate cibernetică si instruirea angajatilor | Utilizarea MFA sau autentificarea continuă | |

## Raportarea incidentelor catre autoritati - *obligatorie*

Raportare incidentelor cu impact semnificativ* asupra furnizării serviciilor

| | | |
|---|---|---|
| In 24 ore | in 72 ore<br>un raport detaliat | Intr-o luna<br>Raport final<br>Raport de progres |

**=Un incident este semnificativ dacă a cauzat sau este capabil să provoace perturbări operaționale grave ale serviciilor sau o pierdere financiară pentru entitatea în cauză sau dacă a afectat sau este capabil să afecteze alte persoane fizice sau juridice, provocând daune considerabile materiale sau non-materiale*

| | | |
|---|---|---|
| Computer Security Incident Response Team (CSIRT) | Autoritatea competenta | Beneficiarii serviciilor |

BRINEL

# BRINEL - PREGĂTIRE PENTRU SECURITATE CIBERNETICĂ

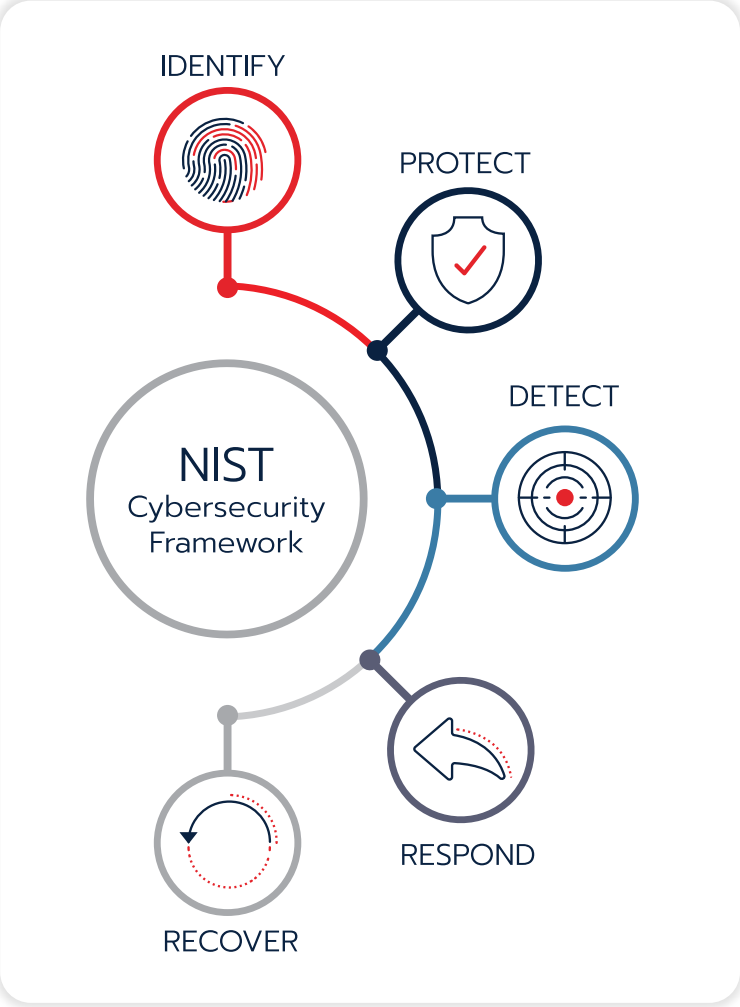
## Plan personalizat pentru securizarea datelor

01 **CLOUD & INFRA SECURITY**
Fortificarea ecosistemului digital, protejarea datelor sensibile, păstrarea continuității operaționale.

02 **PLATFORM & APP SECURITY**
Asigurarea securității robuste a platformei și a aplicațiilor, protejarea infrastructurii digitale și a aplicațiilor software.

03 **DATA SECURITY & GOVERNANCE**
Asigurarea confidențialitatii, integritatii și conformitatii activelor de date, promovând o cultură a încrederii, inovației și luării deciziilor responsabile bazate pe date.

04 **IDENTITY & ACCESS MANAGEMENT**
Oferă acces fără întreruperi, dar sigur, la resurse, sporind productivitatea, minimizând riscurile, verificarea vigilentă a identității utilizatorilor și controale complete ale accesului.




FORTINET veeam FORTRA

BRINEL

# Thank you!


## CONTACT

**Headquarters Cluj-Napoca**
4 Nicolae Titulescu Blvd

**cluj**@brinel.ro

www.**brinel**.com

**Bucharest Office**
U CENTER 2, 2nd floor
206-218 Serban Voda Route

**bucuresti**@brinel.ro

**Bogdan Mustata**
**Sales Director - Bucharest**

Bogdan.mustata@brinel.ro
+40722 741 617

Follow us on: