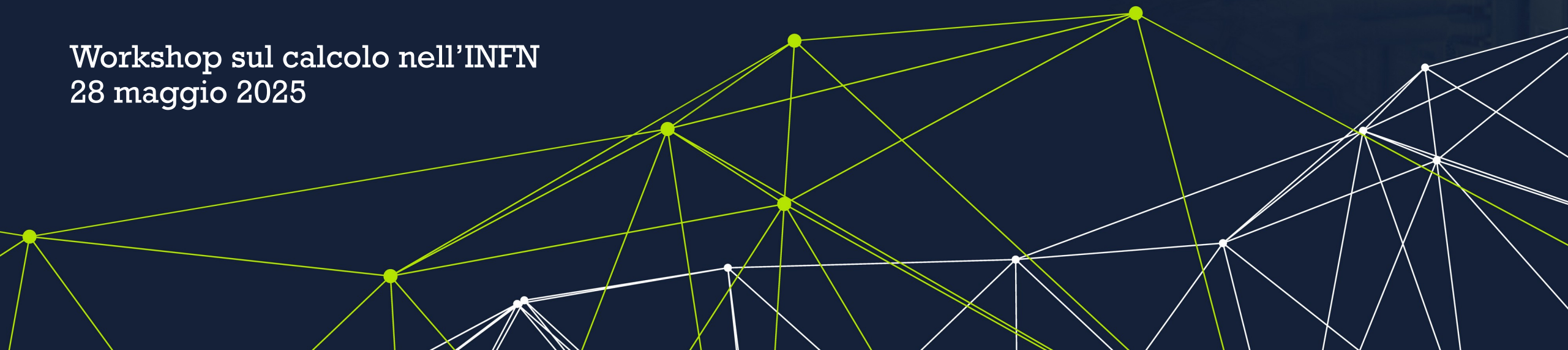
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

NIS2 & friends: un'altra corsa verso la prossima sconfitta?

Leonardo Lanzi – Responsabile di GARR-CERT

Workshop sul calcolo nell'INFN
28 maggio 2025



Presentazioni

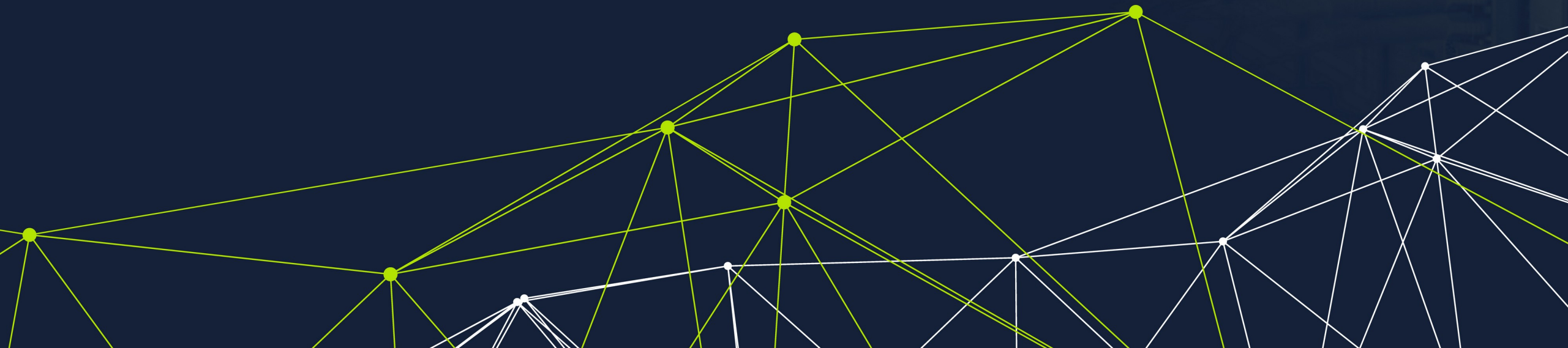
- 2018 – Responsabile di GARR-CERT
- …
- 2012 – PhD Informatica
- …
- 1999 – Dipartimento di Fisica – UniFI
- …
- 1995 – Laurea in Fisica

Agenda

- /var/log/ – linea del tempo
- compliance == sicurezza ?
- (in)cauto ottimismo

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

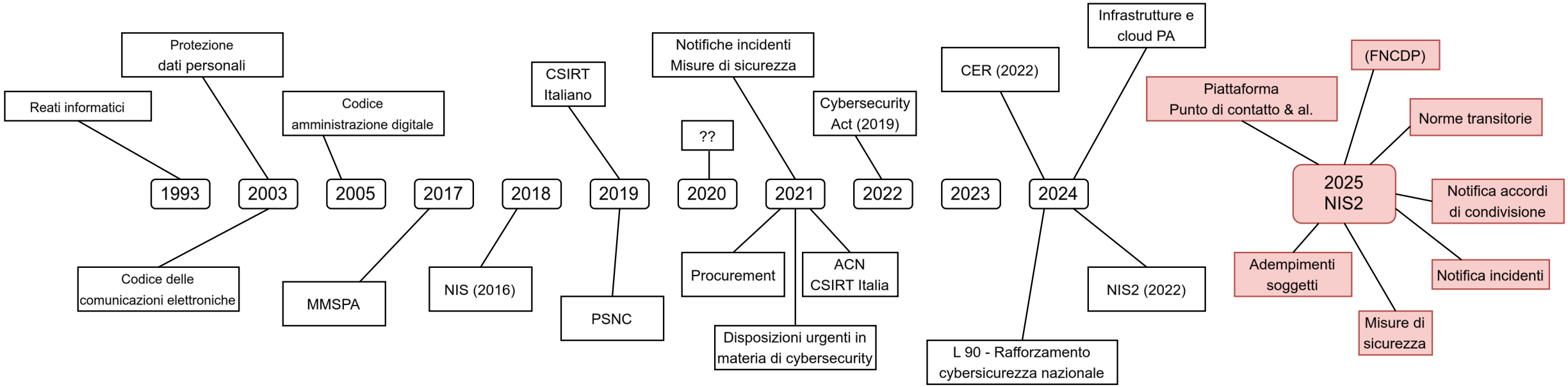
/var/log/ linea del tempo



Per chi preferisce /var/log/

- 23/12/1993, L 547 reati informatici
- 01/08/2003, D.lgs 259 Codice delle comunicazioni elettroniche
- 30/06/2003, D.lgs 196 protezione dati personali
- 07/03/2005, D.lgs 82 – CAD
- 18/04/2017, MMSPA
- 18/05/2018, D.lgs 65 (Direttiva UE 2016/1148) NIS
- 08/08/2019, DPCM CSIRT Italiano
- 21/09/2019, DL 105 PSNC (→ L 133)
- 05/02/2021, DPR 54 Procurement
- 14/04/2021, DPCM 81 Notifiche incidenti e misure di sicurezza
- 14/06/2021, DL 82 Disposizioni urgenti in materia di cybersicurezza (→ L 109) ACN + CSIRT Italia
- 03/08/2022, D.lgs 123 (Regolamento 2019/881) Cybersecurity Act
- 28/06/2024, L 90 Disposizioni per PA centrali
- 01/08/2024, Regolamento infrastrutture e cloud PA (ACN+DTD)
- 04/09/2024, D.lgs 134 (Direttiva UE 2022/2557) CER Resilienza dei soggetti critici
- 04/09/2024, D.lgs 138 (Direttiva 2022/2555) NIS2

Se invece piace la linea del tempo



NIS, 6/7/2016 → D.lgs 18/5/2018, n. 65

Direttiva UE 2016/1148, *Network and Information Security*.

… *misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*.

- Target:
  - Operatori di Servizi Essenziali → "Infrastrutture critiche"
  - Fornitori di Servizi Digitali
- Varie richieste: strategia nazionale (obiettivi, priorità, politiche), misure di sicurezza, segnalazione incidenti.. ma molto discrezionale.
- Sostituita da NIS2 in ottobre 2024 **(prevista già da fine 2015)**.

Avanti veloce

Direttiva EU NIS2 – 14/12/2022

Sempre *relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*.

Sostituisce la NIS (2016/1148).

Nell'estate 2024 compare questa

Essenziali	Importanti
Soglia	
> 250 impiegati	50-250 impiegati
> 50 M€ fatturato	10-50 M€ fatturato
> 43 M€ bilancio	< 43 M€ bilancio
Settori ad alta criticità	**Altri settori critici**
Energia	Servizi postali
Salute	Servizi di trasporto
Trasporto	Gestione rifiuti
Banche	Prodotti chimici
Mercati finanziari	Cibo
Acqua potabile	Industria tech/eng
Infrastrutture digitali	Servizi digitali
Gestione servizi ICT	**Ricerca!**
Spazio	
Pubblica amministrazione	

Direttiva NIS2 (2022/2555)

→ Diventa D.lgs. 138/2024, in vigore dal 16/10/2024

C'è un'area dedicata sul sito di ACN –
Autorità nazionale competente: **acn.gov.it/portale/nis**

- Identificazione (auto- o esercitata da **autorità di settore NIS**):
  18 settori (11 altamente critici e 7 critici),
  oltre 80 tipologie di soggetti, **essenziali** o **importanti**. Quanti saranno?

  → A novembre 2024, durante una presentazione a Sapienza, ACN stima "da alcune migliaia a qualche decina di migliaia"
- 10 tipologie di misure di sicurezza di base, con approccio multi-rischio, e proporzionali al rischio
- Articolazione del processo di notifica degli incidenti
- Rafforzamento dei poteri di esecuzione, ispettivi e sanzionatori
- Nuovi strumenti di collaborazione a livello transnazionale

NIS2, se sono già nel *perimetro*

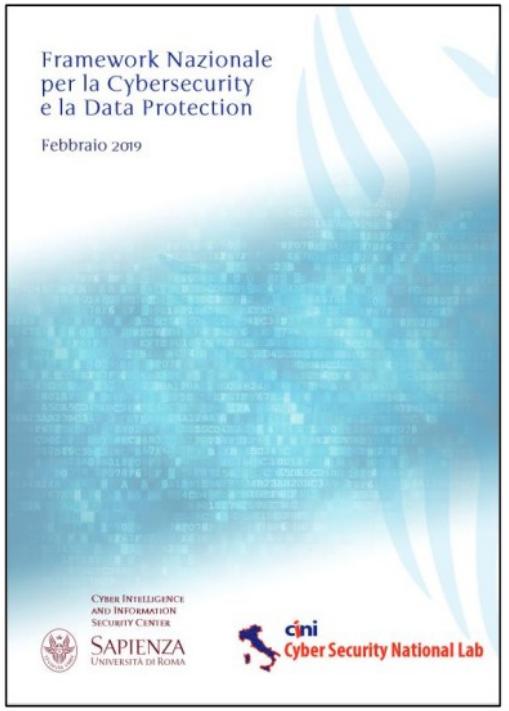
- Le organizzazioni già comprese nel PSNC devono armonizzare i loro obblighi con quelli introdotti dalla Direttiva NIS2.
- Gli obblighi di gestione del rischio e di notifica degli incidenti previsti dal PSNC sono considerati almeno equivalenti a quelli della NIS2, quindi non c'è duplicazione di adempimenti per beni e servizi già coperti dal PSNC.
- Per i restanti sistemi informativi, reti e servizi, dovranno essere adottati i nuovi obblighi che verranno introdotti dalla NIS2.
- PS: in realtà per il PSNC c'erano già indicazioni per i "beni contigui" e per tutte le restanti risorse, ma visto che erano lì a scrivere...

NIS2 – Organi di amministrazione e direttivi

- La **gestione della sicurezza** diventa funzione attiva e strategica dell'organizzazione, quindi di **competenza degli organi di amministrazione e direttivi**
  - Approvano le modalità di implementazione delle misure di sicurezza
  - Sovrintendono all'implementazione degli obblighi
  - Sono responsabili delle eventuali violazioni
  - Sono **tenuti a seguire una formazione in materia di cybersicurezza**
  - Promuovono la formazione dei propri dipendenti

NIS2 – 10 ambiti di applicazione delle misure di sicurezza

- Politiche di analisi dei rischi e di sicurezza dei sistemi informativi
- Gestione degli incidenti
- Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi
- Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con i diretti fornitori o i fornitori di servizi
- Sicurezza dell'acquisizione, dello sviluppo e della manutenzione […], compresa la gestione e la divulgazione delle vulnerabilità
- Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza
- Pratiche di igiene informatica di base e formazione in materia di cybersicurezza
- Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
- Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti
- Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti



(fonte ACN)

NIS2 – Incidenti di sicurezza

Notifica/Report degli incidenti **significativi** a CSIRT Italia

- Early warning
  → entro 24 ore
- Notifica ufficiale (accertamento, valutazione, severità, impatto, IoC)
  → entro 72 ore
- Report intermedi
  su richiesta di CSIRT Italia o altre autorità competenti
- Report finale
  → entro un mese, o entro un mese dalla conclusione dell'incidente.

NIS2 – Timeline

~~Recepimento~~

Prima fase

- → febbraio 2025
  censimento e registrazione dei soggetti
- → marzo 2025
  adozione dell'elenco dei soggetti
- → aprile 2025
  notifica ai soggetti
- → aprile 2025
  elaborazione e adozione obblighi di base
- …

Seconda fase

- gennaio 2026 →
  obbligo di notifica di base
- → aprile 2026
  adozione del modello di categorizzazione di attività e servizi
- → aprile 2026
  elab. e adozione degli obblighi a lungo termine
- → ottobre 2026
  completa implementazione delle misure di sicurezza di base

Terza fase

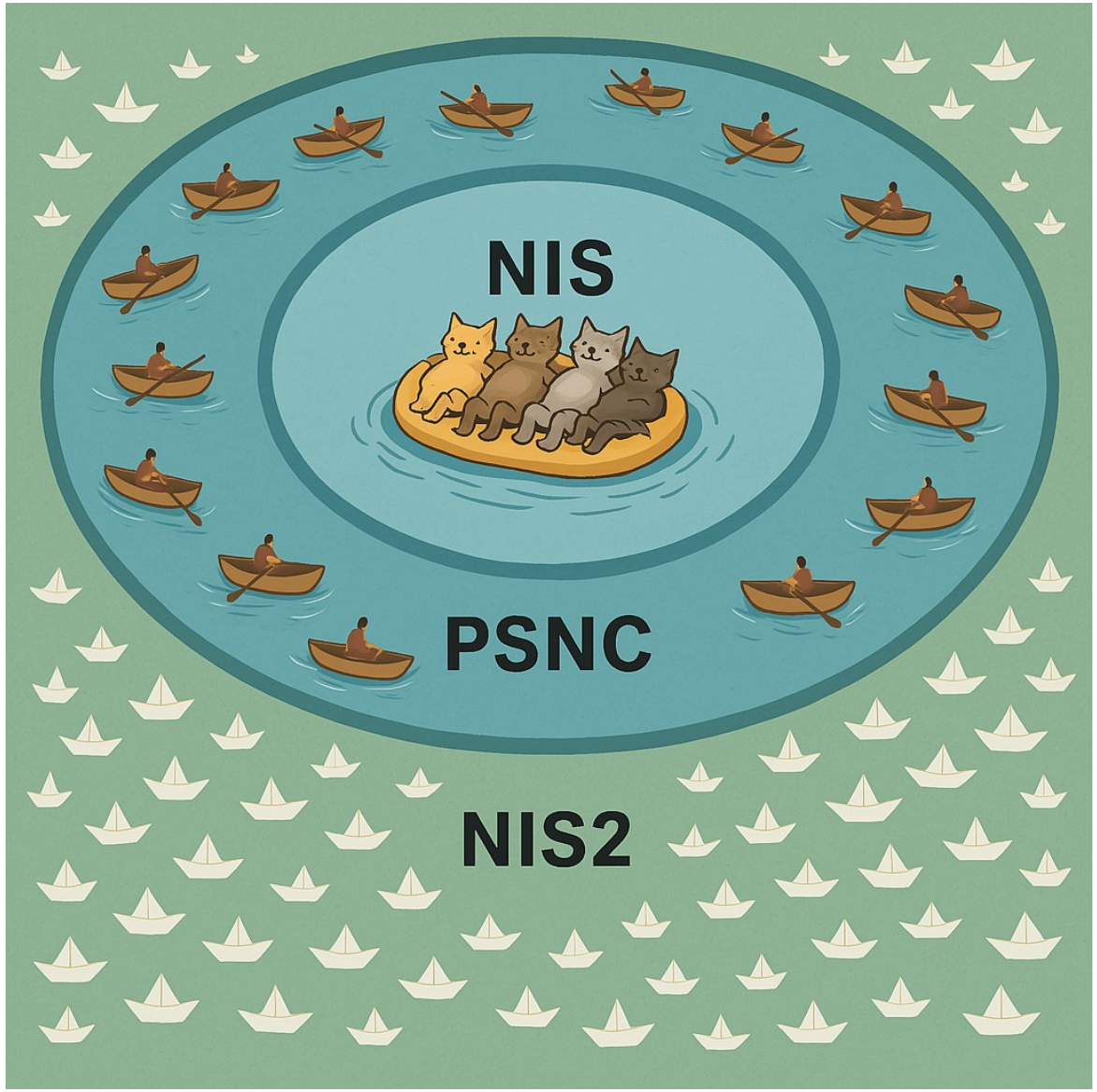
- aprile 2026 →
  categorizzazione delle attività e dei servizi
  Implementazione degli obblighi a lungo termine

In pratica..

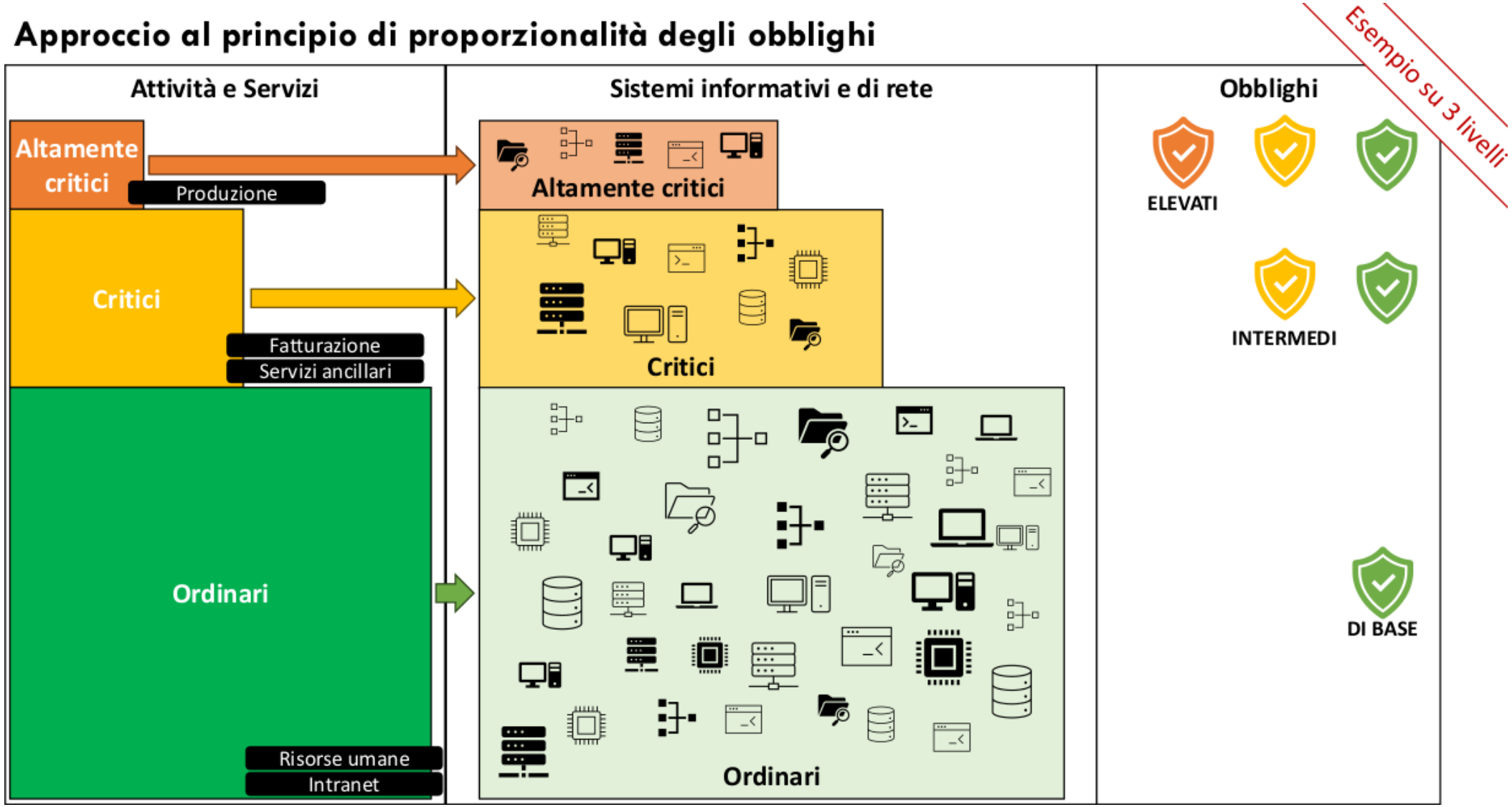
.. il perimetro si allarga.

Quanto?

- PSNC: “alcune decine”
- NIS2 (da sito ACN, maggio):
  oltre 20’000 soggetti,
  di cui oltre 5000
  essenziali



[si allarga anche] all'interno dell'organizzazione



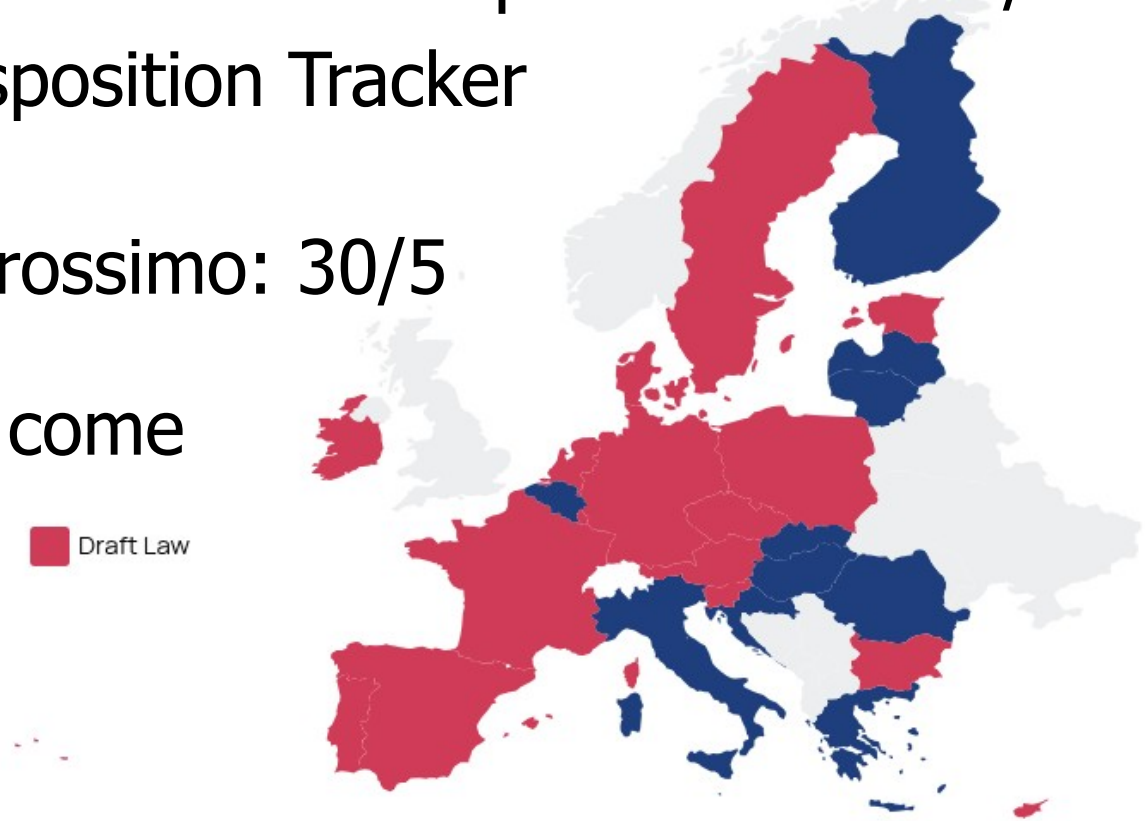
A proposito del “livello comune…”

La European CyberSecurity Organization
ecs-org.eu/activities/nis2-directive-transposition-tracker/
ha il NIS2 Directive Transposition Tracker

Ultimo agg. fine aprile, prossimo: 30/5

Ognuno va avanti un po’ come vuole.

Cliccare per credere.



NIS2 – seconda fase – determinazioni ACN

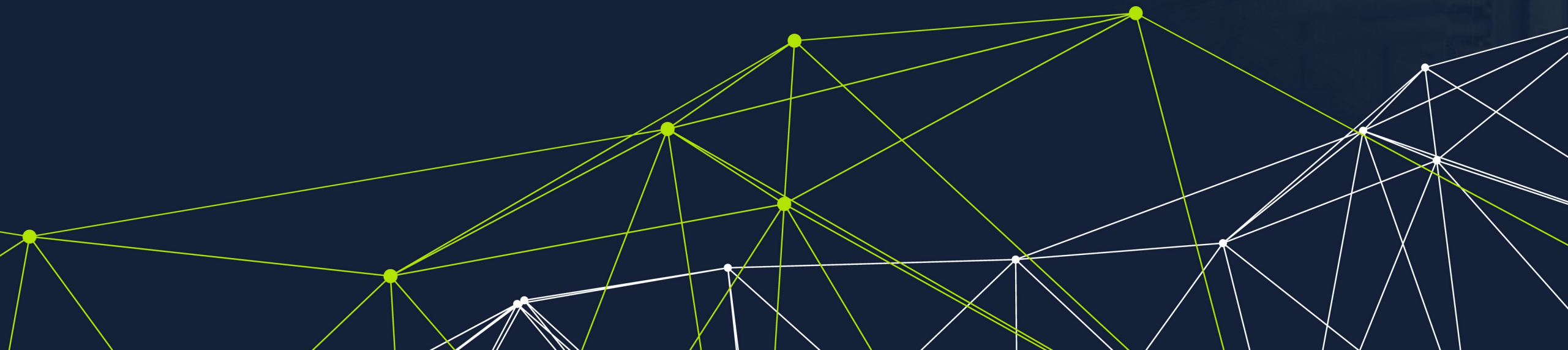
Dal 15 aprile, aggiornamento informazioni (da fare poi ogni anno) **entro il 31 maggio**.

- piattaforma NIS
- punto unico di contatto → e sostituto
- segnalazione componenti degli organi di amministrazione e direttivi
- indirizzi IP (pubblici e statici) e nomi di dominio, in uso o nella disponibilità del soggetto
- notifica degli accordi di condivisione sulla sicurezza informatica [ISAC]
- specifiche di base per adempimento obblighi soggetti essenziali e importanti.. e vari allegati, in particolare
  - soggetti importanti: 37 misure / 87 requisiti
  - soggetti essenziali: 43 misure / 116 requisiti
  - notifica degli incidenti "significativi", risp. 3 e 4 tipologie per importanti/essenziali.

- Update del Framework Nazionale per la Cybersecurity e la Data Protection Edizione 2025 (v. 2.1) – aggiornato a CSF NIST 2.0

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

.. & friends



Legge 28 giugno 2024, n. 90

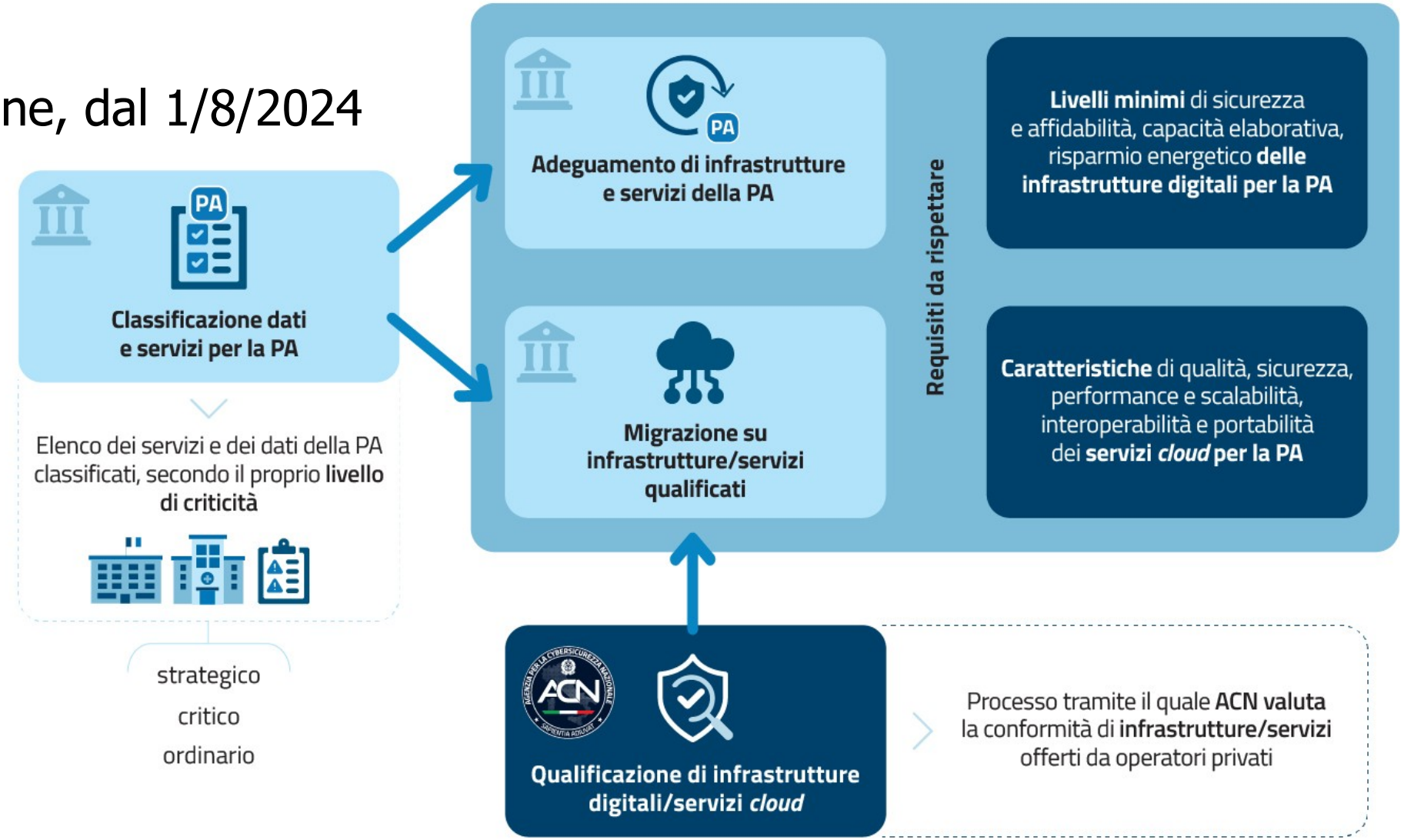
Disposizioni in materia di rafforzamento della cybersicurezza nazionale
(e dei reati informatici)

- Obbligo di notifica degli incidenti informatici
- Sanzioni per il mancato rispetto della normativa
- Requisiti di cybersecurity per i contratti pubblici
- Rafforzamento della resilienza delle PA e referente unico per la cybersicurezza (funzione di punto di contatto unico, v. NIS2)
- Coerente con NIS2 (dove non lo era, tagliata)

"Ispirata" da PSNC e NIS2 – mancavano solo 68 giorni al 4/9/2024 :((

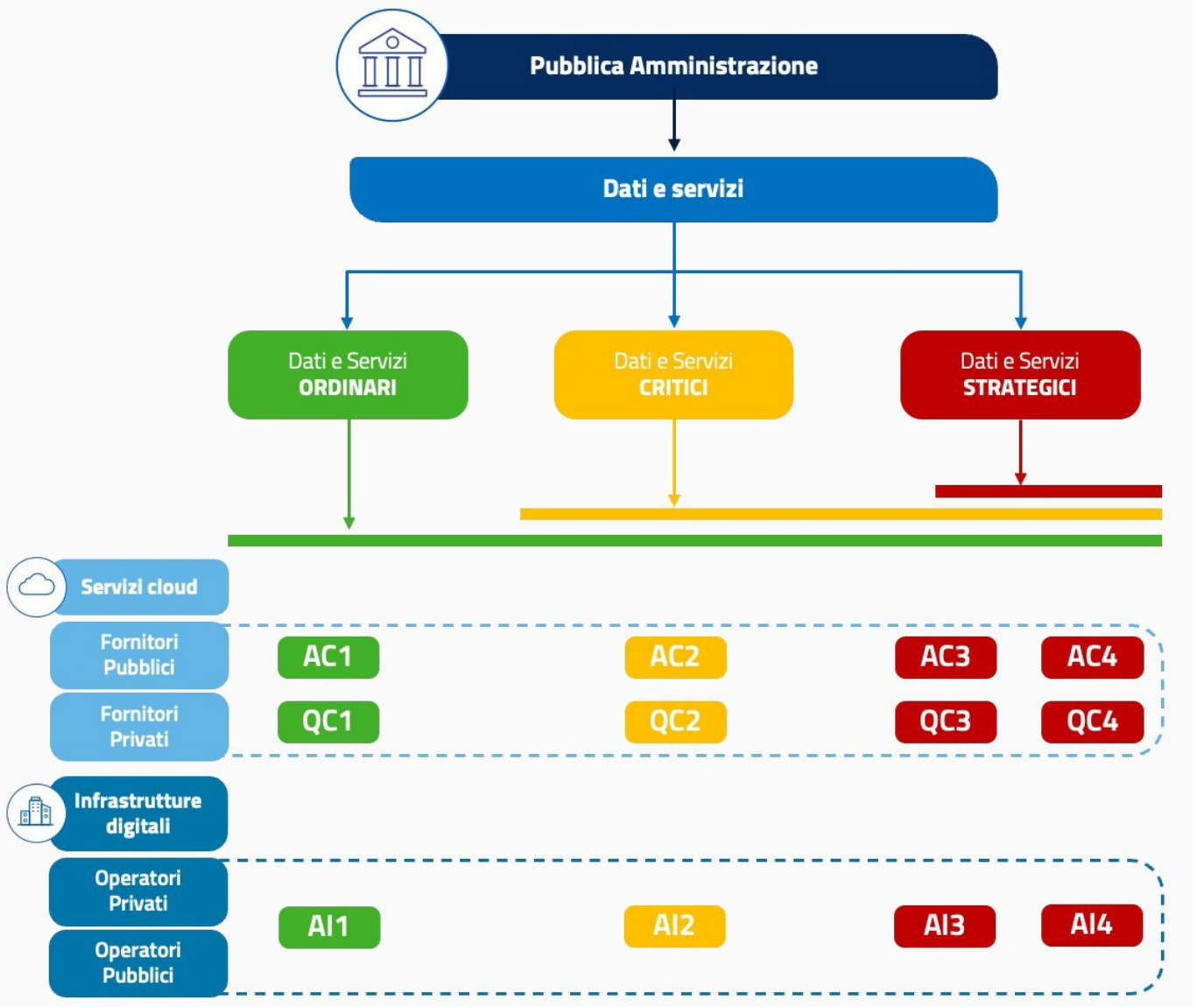
Regolamento Cloud per la PA – ACN+ · D

88 pagine, dal 1/8/2024



Regolamento Cloud per la PA – ACN+ · D

dal 1/8/2024



DPCM 30 aprile 2025

Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale. (25A02717)

Dubbi:

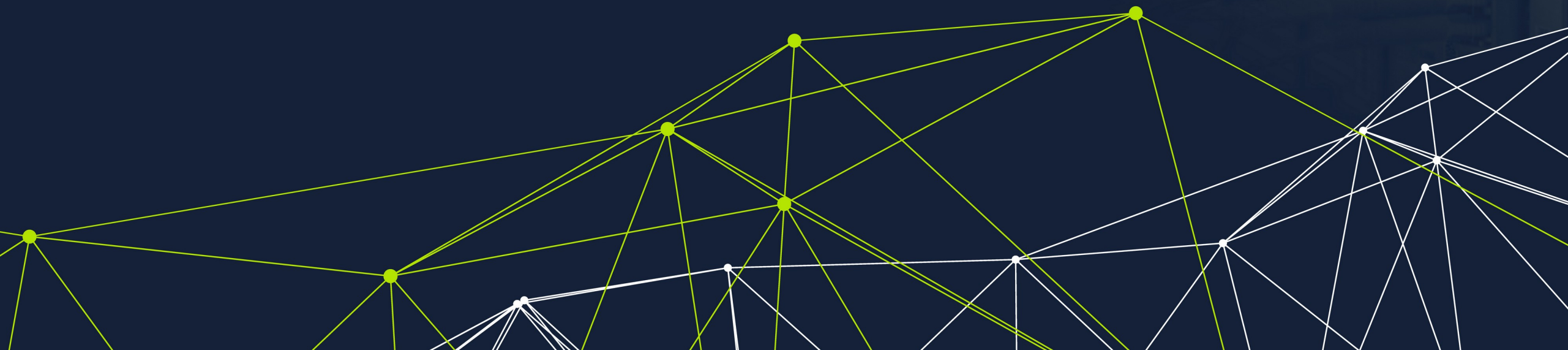
- 3/11 (pagine) di "visto..", tra questi la L. 90, che per il suo art. 1 co. 7 a) **non** si applica ai soggetti PSNC. Ma allora perché parla di "sicurezza nazionale"?
- Se cita la L.90, e gli "interessi strategici", si applica alle PA centrali?

Contenuti:

- elementi essenziali di cybersicurezza per beni e servizi informatici
- criteri di premialità per tecnologie di cybersicurezza italiane, paesi EU, NATO, paesi terzi in un "elenco dei buoni"
- Allegati per i dettagli
- Elenco dei buoni: Australia, Corea del Sud, Giappone, Israele, Nuova Zelanda, Svizzera

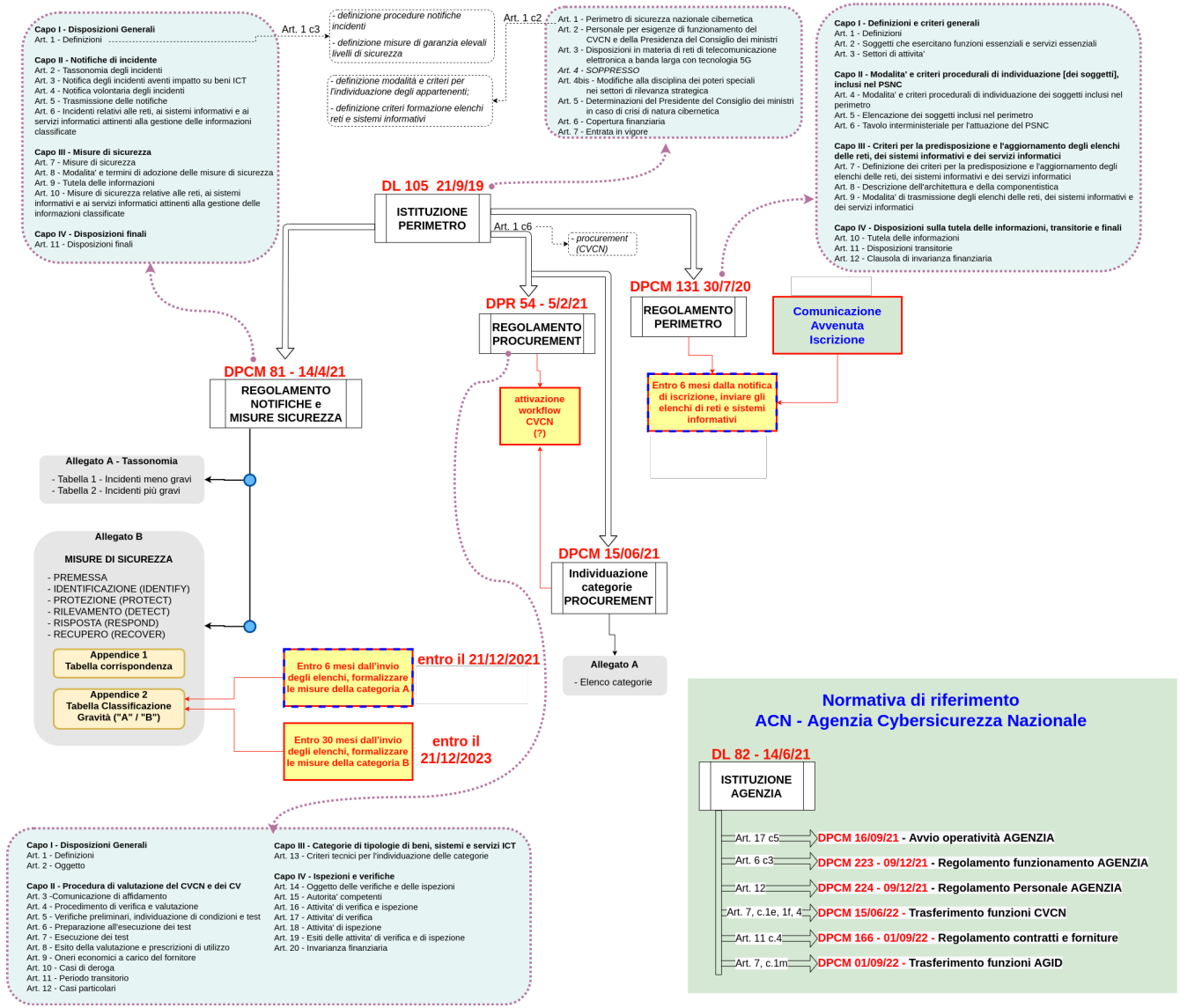
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

compliance == sicurezza ?



NIS2.. Legge 90.. Regolamento Cloud ..

Mi fai un disegnino come questo?



Per ora come va?

19/5/2025

PEC da Just4Cyber → ACN

Oggetto:

Richiesta di urgenti chiarimenti in merito all'**individuazione dei soggetti responsabili** ai sensi degli artt. 7, co. 4, lett. c) e 38, co. 5 del D.lgs. 138/2024 per la registrazione ed il censimento da effettuare **entro il 31 maggio 2025** per le Pubbliche Amministrazioni e altri enti pubblici

Per ora come va?

Cosa chiedono?

- **Chi sono i soggetti responsabili** da censire entro il 31/5/2025?
  - art. 7 co. 4 lett. c) del D.lgs. 138/2024 rinvia all'art. 38, che però cita solo i soggetti essenziali
  - non possiamo riferirci alla Direttiva EU (norma non direttamente applicabile)
  - non rinvia all'art. 23 dove c'è "organi amministrativi e direttivi", che però sta nelle FAQ sul sito di ACN.
  - "Nelle more", vi preghiamo di pubblicare altre FAQ

FAQ???????

Per ora come va?

Ci sono altri casi strani

- Di quasi 100 università, di cui 61 statali, pare che solo 20 siano state incluse nel perimetro NIS.
  I criteri di inclusione non sono stati pubblicati dall'autorità di settore (**quasi** sempre il MUR).

- Nel CDA di un ateneo ci sono anche due rappresentanti degli studenti.
  - Li registriamo sul portale ACN?
  - Vengono sanzionati in caso di inadempienza?

→ qualche ateneo ha mandato PEC con richiesta di chiarimenti.
Update 23/5/25:

- Il coordinamento dei direttori IT sta convergendo per proporre Rettore e DG.
- CODAU di aggiungere direttori IT (e vice)

Va?

20/5/2025

ACN pubblica la
FAQ ODA.10: Nell'elencazione dei componenti degli organi di amministrazione e direttivi e' necessario indicare la PEC personale?

Risposta:
Non è richiesta, per quanto auspicabile, l'indicazione dell'indirizzo PEC individuale e/o nominativo dei componenti degli organi di amministrazione e direttivi che vengono elencati. E anche sufficiente indicare un indirizzo PEC funzionale dell'organizzazione (come il domicilio digitale) o, qualora non disponibile, un indirizzo PEO aziendale.

Update 23/5/25 (sito ACN):

I soggetti NIS, che hanno richiesto supporto per la finalizzazione dell'aggiornamento annuale dei dati, potranno concludere tale procedura entro il 31 luglio.

Misure NIS2/Italia – ambiti politiche (da xlsx ACN)

- gestione del rischio
- ruoli e responsabilità
- affidabilità delle risorse umane
- conformità e audit di sicurezza
- gestione dei rischi per la sicurezza informatica della supply chain
- gestione degli asset
- gestione delle vulnerabilità
- continuità operativa, ripristino in caso di disastro e gestione delle crisi
- gestione dell'autenticazione, delle identità digitali e del controllo accessi
- sicurezza fisica
- formazione del personale e consapevolezza
- sicurezza dei datisviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- protezione delle reti e delle comunicazioni
- monitoraggio degli eventi di sicurezza
- risposta agli incidenti e ripristino

“Sistemi rilevanti” (ACN)

FAQ MSB.7: In alcuni requisiti delle misure di sicurezza è presente la dicitura “per almeno i sistemi informativi e di rete **rilevanti**”. Che cosa si intende?

In linea di principio, le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto NIS (per la definizione di “sistema informativo e di rete” si faccia riferimento all’articolo 1, comma 1, lettera p) del decreto NIS). Ove, tuttavia, la disposizione di un requisito, o di parte di esso, contiene la dicitura in questione, il soggetto NIS ha la facoltà di limitare l’ambito di applicazione della disposizione ai sistemi informativi e di rete la cui compromissione comporterebbe un **impatto significativo** sulla **confidenzialità**, **integrità** e **disponibilità** delle attività e servizi per i quali il soggetto NIS rientra nell’ambito di applicazione del decreto NIS.

Incidenti significativi

Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4 (E)	Il soggetto NIS ha evidenza, anche sulla base dei parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

DE.CM (DEtect.Continuous Monitoring)-01: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi
Suddivisa in 5 punti (+ 2 di compliance GV.PO-01).

Regolamento di Esecuzione (UE) 2024/2690 del 17/10/2024

34 pagine per spiegare requisiti tecnici e metodologici per gestione rischi di cibersicurezza e ulteriore specificazione dei **casi in cui un incidente è considerato significativo** per [.. tutta una serie di servizi forniti], negli artt. 3, 4 (incidenti ricorrenti), da 5 a 14 i dettagli per i vari tipi di servizi.

Trovato!!!!!!!!

Dal Reg. di Esecuzione (UE) 2024/2690 del 17/10/2024

art. 3

1) [..]criteri:

a) l'incidente ha causato o è in grado di causare al soggetto pertinente una perdita finanziaria diretta superiore a 500'000 EUR o, se tale importo è inferiore, al 5 % del suo fatturato totale annuo dell'esercizio precedente;

b) l'incidente ha causato o è in grado di causare l'esfiltrazione di segreti commerciali, quali definiti all'articolo 2, punto 1), della direttiva (UE) 2016/943, del soggetto pertinente;

c) l'incidente ha causato o è in grado di causare il decesso di una persona fisica;

d) l'incidente ha causato o è in grado di causare danni considerevoli alla salute di una persona fisica;

e) si è verificato un accesso non autorizzato ai sistemi informativi e di rete, che si sospetta essere malevolo ed è in grado di causare gravi perturbazioni operative;

f) l'incidente soddisfa i criteri di cui all'articolo 4;

g) l'incidente soddisfa uno o più criteri di cui agli articoli da 5 a 14.

2) Le interruzioni programmate del servizio e le conseguenze previste delle operazioni di manutenzione programmata effettuate dai soggetti pertinenti o per loro conto non sono considerate incidenti significativi.

3) [...] istruzioni per calcolare il numero di utenti interessati…

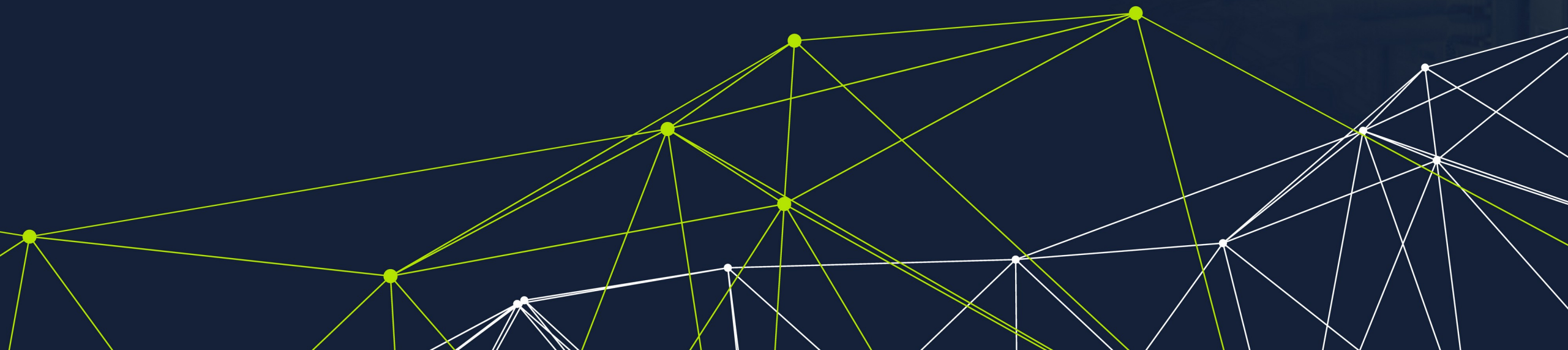
still?

Dubbi vari dalla comunità

1) Bruceremo tutte le energie a scrivere carta?
2) Possiamo pagare qualcuno/qualcosa che fa tutta questa roba al posto nostro?
   - Esistono decine, forse centinaia di "soluzioni integrate" di consulenze+software, ma la responsabilità non si trasferisce/delega
3) Esiste una certificazione NIS2?
   - 20/5/25: compare la Prassi di Riferimento UNI/PdR 174 (ISO27001+NIST2) v. grosso ente di accreditamento e punto 2)
4) Se per fornire un servizio strategico sono già in regola con la normativa, perché devo / come posso affidarlo ad altri?
5) La sicurezza non è un costo, è un investimento
   - Forse se hai tempo per pianificare, ma così se va bene è un delirio
   - Posso scambiare qualche tonnellata di hardware PNRR? e andare al punto 2)
   - OK, posso investire. Ma – anche per la cybersecurity – non trovo nessuno.
6) … il resto solo a voce.

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Stato attuale



OK ma… in pratica?

Sempre (quasi) la stessa storia:

- Identificare (Identify)
- Proteggere (Protect)
- Rilevare (Detect)
- Rispondere (Respond)
- Recuperare (Recover)

e dal 2024, GOVERN che lega il tutto.

C’è poco tempo (ottobre 2026) per occuparsi delle 37|43 misure, con i loro 87|116 requisiti
Si trovano su ACN → NIS → misure di sicurezza di base (pdf e xlsx)

Da dove partiamo

- Abbiamo migrato servizi (soprattutto dati) essenziali su cloud di superpotenze tecnologiche
  - che succede in caso di incidenti (a.k.a. chi riesce a avere/leggere/usare i log)?
  - già dal 2020 compaiono fake tenant Microsoft
  - 2022-23: esempi live di break del 2FA
  - mix letale di auth su cloud / AD locale: evidenze di vulnerabilita' / escalation di privilegi.
  - 2024: Sparisce la mail su Google per alcuni atenei, e ricompaiono tutte le mail cancellate anni prima
- E se chiudono i DB? rischio danni da efficienza (DOGE e simili)
  - 2024: si blocca NVD (NIST), non si sa perché
  - 15 e 16 aprile 2025: annuncio chiusura e rispettivamente riapertura di CVE (MITRE)

Dati Shadowserver Foundation per AS 137

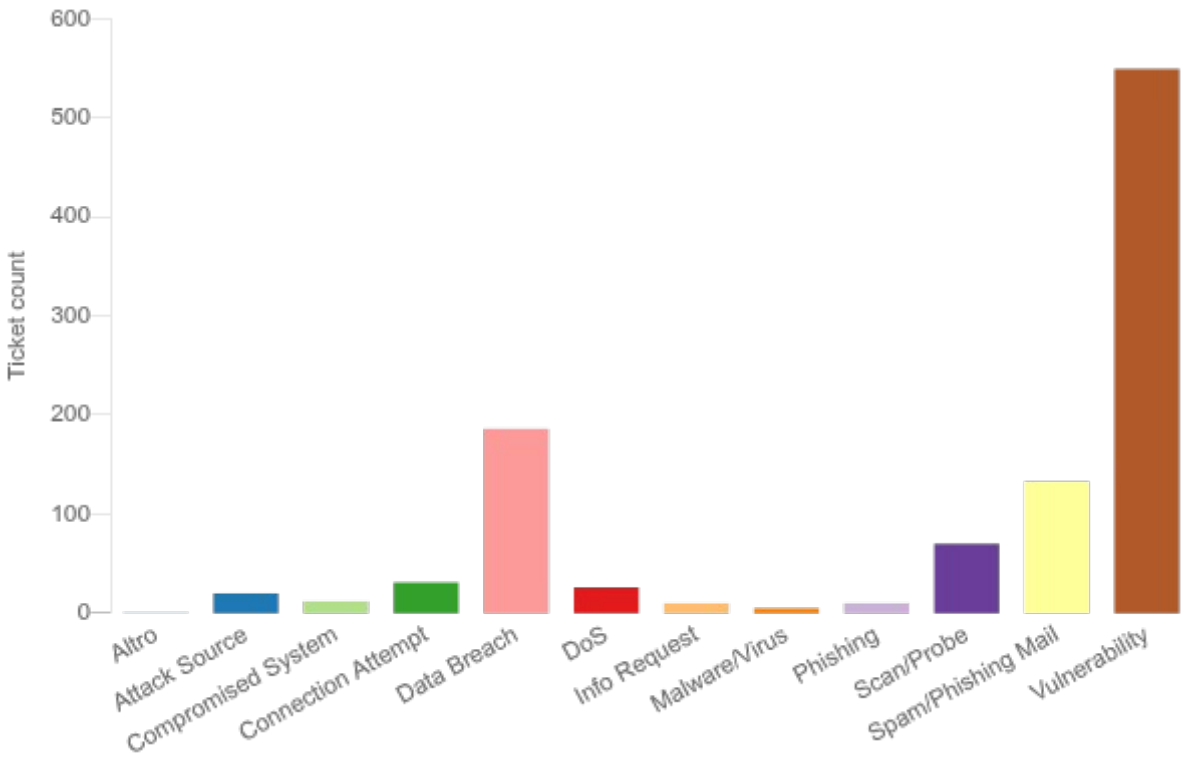
Scansioni IPv4 e IPv6, per 130 tipologie (database) diverse di vulnerabilità, oltre a special report su sistemi compromessi; circa 80 database/giorno.

Ogni record: un IP con un problema.

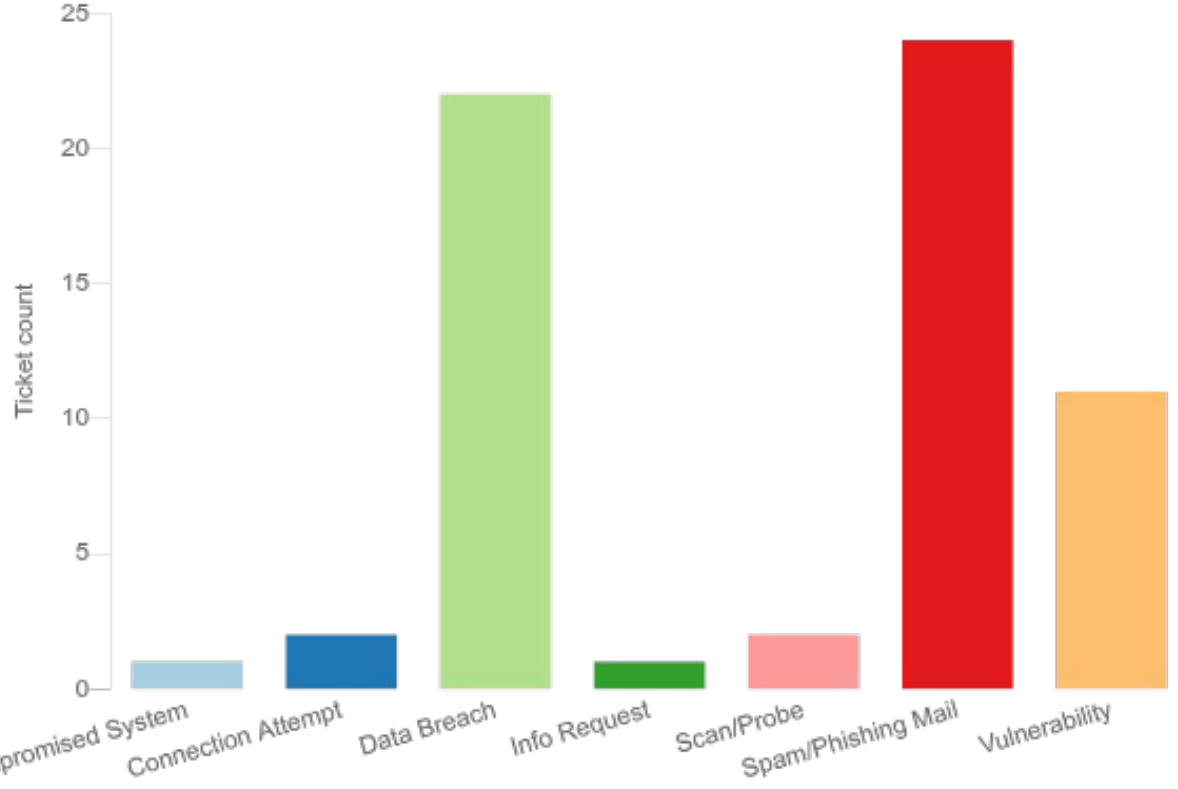
	n. record	critical	high
2024	37’663’358	222’269	620’196
20/5/25	17’307’776	123’995	559’138

Incidenti (*) 2024 – GARR [1054] / INFN [63]

GARR



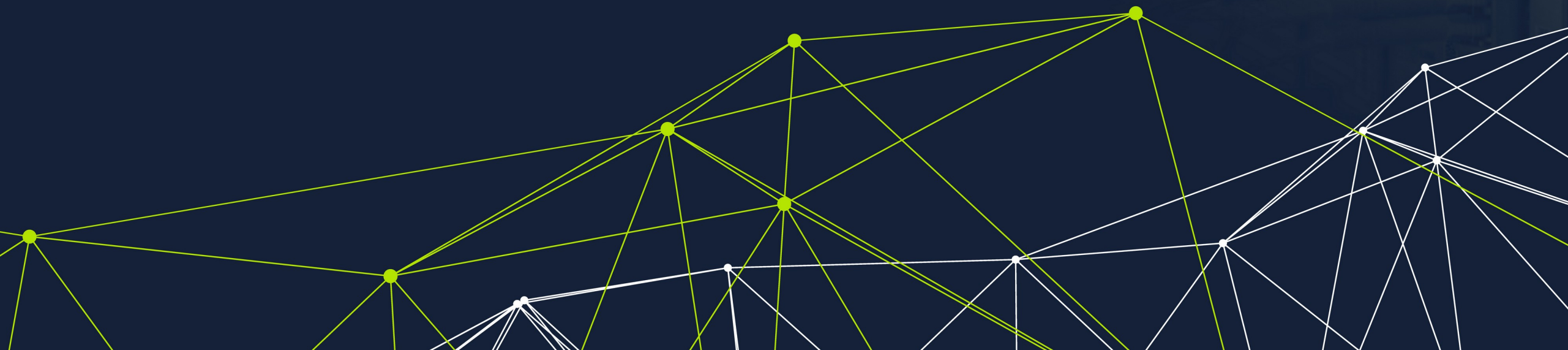
INFN



(*) senza piracy

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

(in)cauto ottimismo



Interesse della comunità GARR per la cybersecurity

- Qualche ente interessato da sempre
- Svolta post-CoViD, per vari motivi
  - attacchi subiti / temuti
  - cambio del management / policy / incarichi specifici
  - nuovi obblighi normativi
- L. 90 + elenco ISTAT PA Centrali
  - CODIGER
    - 2024: Summer School, giornata a tema
    - 2025:
      - test di fattibilità di “formazione coordinata”
      - questionario sul tema al tavolo ICT
- 2025: CODAU
  - Tavolo cybersecurity (molto esteso) con varie proposte
  - maggio – sondaggio agli atenei: situazione attuale + misure NIS2

Argomenti ..

- Vulnerability assessment GARR / INFN
- Strumenti open / condivisi / distribuiti per
  - Risk assessment
  - CTI
  - IoC
- Gestione incidenti / Come si fa uno CSIRT / Distributed Accountability
- AI/ML: PoC / casi d'uso intelligente
- Sicurezza per la ricerca
- ...
- ah già: NIS2!!

ma argomenti ... per cosa?

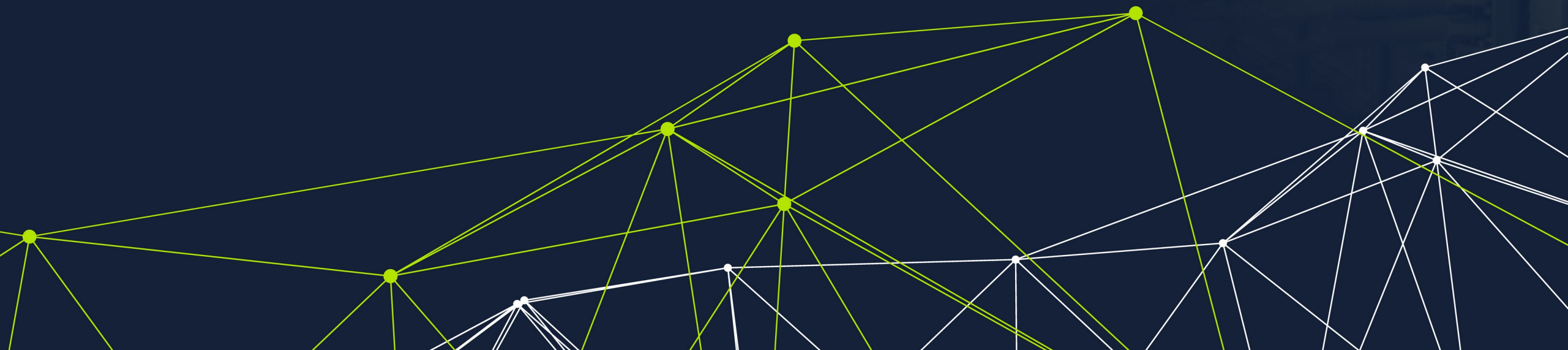
GARR Security Days 2025

Workshop **solo** a tema sicurezza

- 6-7 ottobre
- Roma
- molto probabilmente, c/o ISTAT

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

C’è qualcosa *già pronto*?



Risk assessment

MONARC (Method for an Optimised aNAlysis of Risks)
A tool and a method allowing an optimized, precise and repeatable risk assessment.

- monarc.lu
- github.com/monarc-project
- MOSP: objects.monarc.lu, istanza per creare/condividere oggetti JSON, quali vulnerabilità, minacce, cybersecurity standard
  - objects.monarc.lu/object/view/5146
    draft del FNCDP 2.0 (7/2/2021)

    → Servirebbe qualcuno che lavora sulla NIS2/Italia

Cyber Threat Intelligence

AIL (Analysis Information Leak framework)

- ail-project.org
- github.com/ail-project/[..]
  - ail-training

MISP Threat Sharing

- ~ 2011 Nasce come Malware Information Sharing Project (Belgisch Defensie)
- .. poi passa alla NATO
- Adottato da CERT-EU, CIRCL, ...
- 2013 Lead Developer (Andras Iklody) NATO → CIRCL
- Diventa una delle principali attività di sviluppo del CIRCL

- misp-project.org

C'è stato anche un corso organizzato da GARR a febbraio 2019, tenuto dal suddetto lead developer.

OSINT su Ransomware

RansomLook.io

- .. tracking ransomware-related posts and activities.
- github.com/RansomLook/RansomLook
- API, CLI, ecc..

E se spengono il DB delle vulnerabilità ...

GCVE: Global CVE Allocation – gcve.eu

Interesse → Richieste ~ “Sarebbe bello avere..”

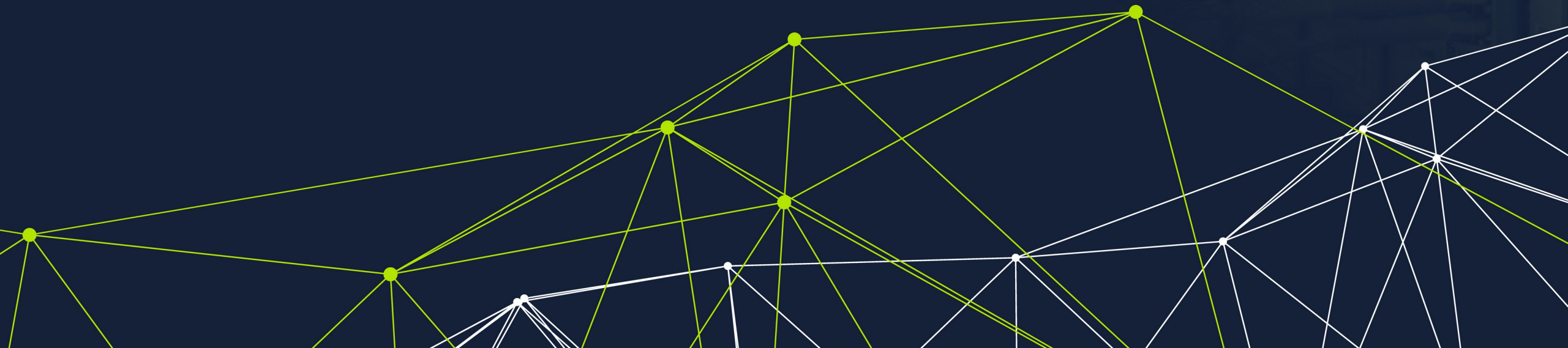
Dati sperimentali

- Richieste da CODIGER, CODAU, altri.. di partecipazione di GARR, in particolare GARR-CERT, alle attività future o già in corso
- Le organizzazioni interessate sono rappresentate nell’organo di indirizzo di GARR – CTS – dove è già stato istituito un gruppo di lavoro sulla cybersecurity. Sync al CTS inizio luglio.
- GARR-CERT ha 1691 contatti distinti [al 27/5/2025] per la gestione degli incidenti di sicurezza.. difficile possa “scalare” sulle singole richieste.

→ Serve una distribuzione del carico di lavoro nella comunità, da inquadrare nelle attività (prossime) future

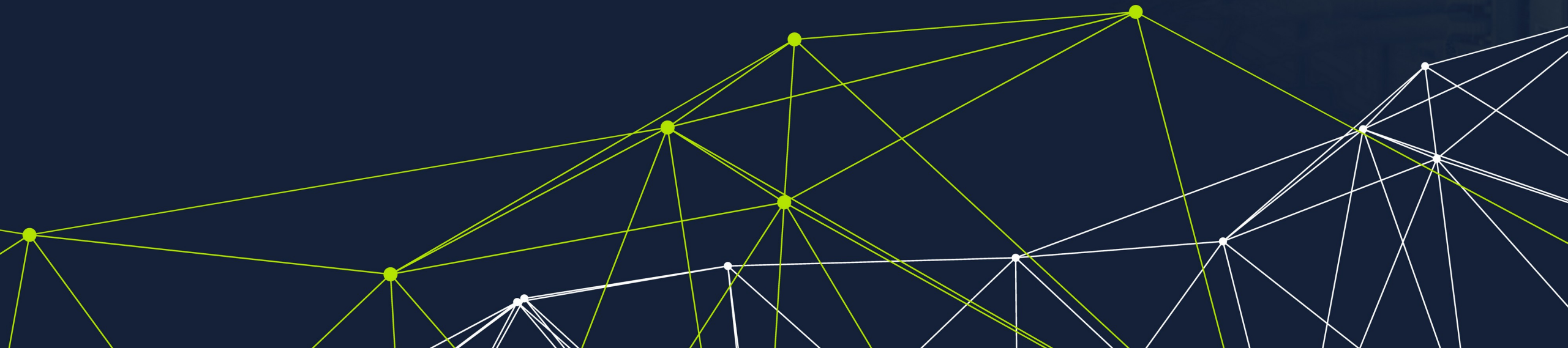
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Domande?



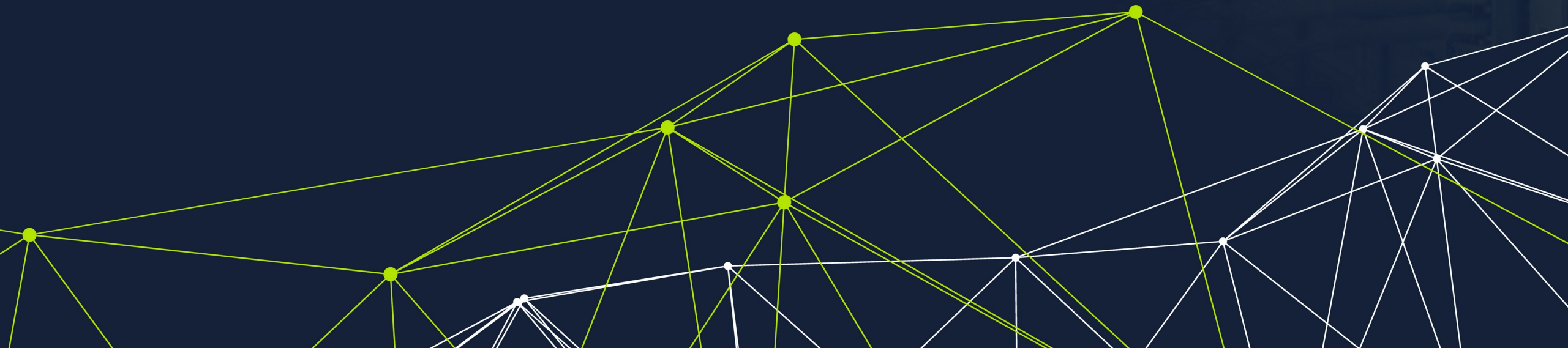
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Grazie a tutti!



Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Riferimenti



Riferimenti (oltre a quelli riportati direttamente)

- I riferimenti normativi sono ripresi generalmente da www.normattiva.it, con eventuali approfondimenti disponibili sui siti web dei rispettivi enti che li hanno emanati (o assimilabili), v. acn.gov.it
- www.just4cyber.eu
- Tassonomia per notifica incidenti e *beni contigui*
  acn.gov.it/portale/documents/d/guest/acn_guida_notifica_incidenti_clear
- Slide ACN presentazione NIS2 a Sapienza – Università di Roma, 27/11/2024
  www.acn.gov.it/portale/documents/20119/37358/ACN-LanuovadirettivaNIS-Sapienza-20241127.pdf
- Framework Nazionale per la Cybersecurity e la Data Protection, ultimo update 2.1, maggio 2025
  cybersecurityframework.it
- NIST CSF 2.0 (febbraio 2024)
  nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- Regolamento di Esecuzione (UE) 2024/2690, 17/10/2024
  eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32024R2690
- acn.gov.it/portale/cloud/regolamento-cloud-per-la-pa
- aggiornamenti NIS scadenza posticipata al 31 luglio
  www.acn.gov.it/portale/w/nis-slitta-al-31-luglio-il-termine-per-gli-aggiornamenti
- Appunti su NIS2 di un volontario
  supporto-nis2.unich.it/index.html
- DPCM 30 aprile 2025
  www.gazzettaufficiale.it/eli/id/2025/05/05/25A02717/sg
- Alcune foto da unsplash.com
- en.wikipedia.org/wiki/CLOUD_Act