L'AI STA RISCRIVENDO LA CYBERSECURITY

Attacchi più veloci. Difese sotto pressione. Una trasformazione già in atto.

Gabriele Faggioli

- CEO Partners4Innovation S.r.l. – Managing Director Digital360 Advisory – Gruppo Digital360
- Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano e senior advisor degli Osservatori della Digital Innovation del Politecnico di Milano
- Adjunct Professor del MIP – Politecnico di Milano
- Già membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea
- Presidente Onorario Clusit (Associazione Italiana per la Sicurezza Informatica)

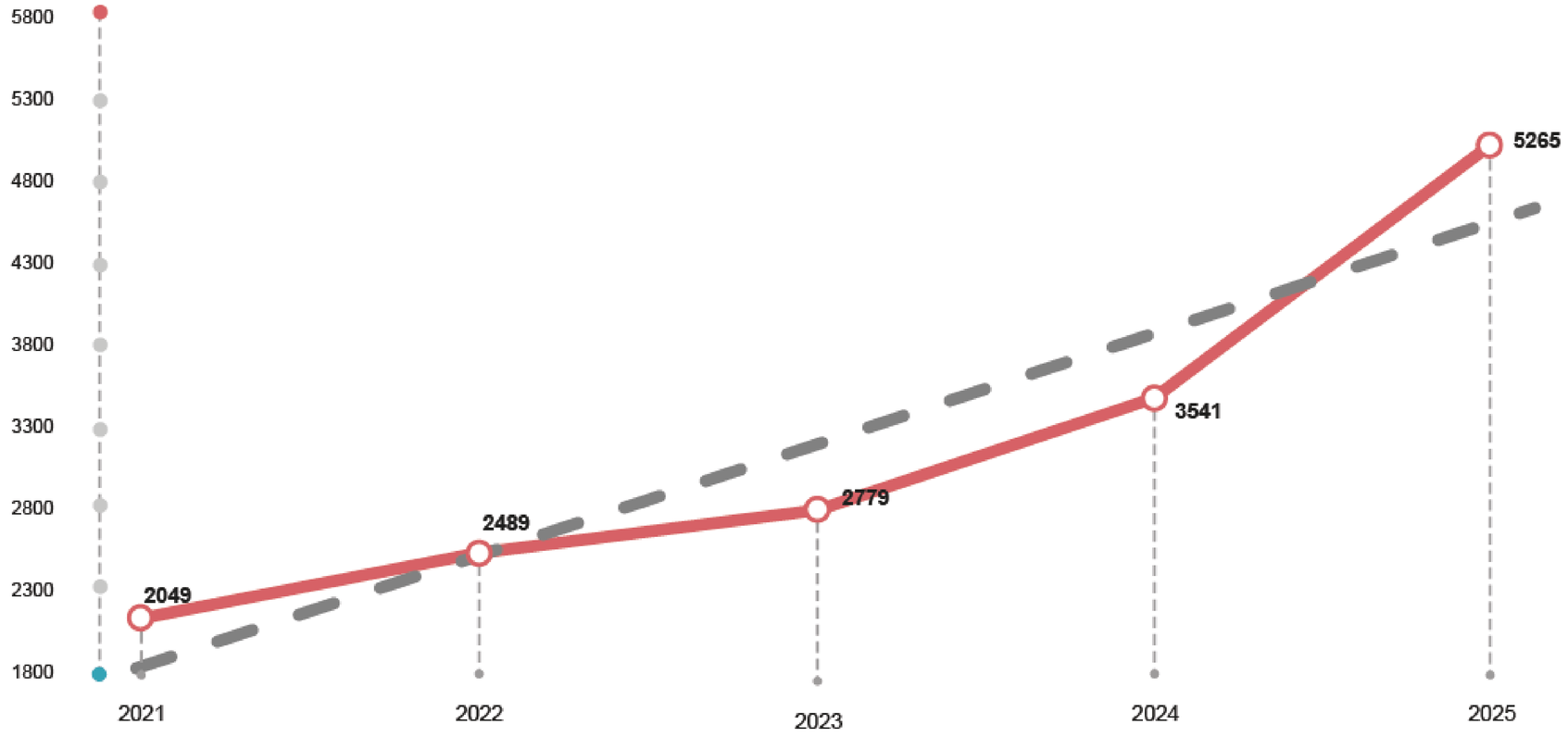
Contesto

Un mondo sempre più esternalizzato	Aziende e pubbliche amministrazioni stanno sempre più esternalizzando i sistemi informativi. La necessità di evitare obsolescenza, garantire sicurezza e poter sfruttare le innovazioni tecnologiche che richiedono grandissime capacità computazionali, accelererà il fenomeno
Un mondo sempre più cloud based	I fornitori software stanno sempre più abbandonando le soluzioni on premise sia per i vantaggi economici che ne hanno sia per la dipendenza che questo genera nei clienti. Imprese e pubbliche amministrazioni sono spinte verso il cloud ma sono anche attratte dal cloud per la scalabilità che esso garantisce
Tendenza alla concentrazione tecnologica	I fornitori cercano sempre più di creare ambienti applicativi chiusi nei quali i clienti possano trovare vantaggi nell'avere sistemi concentrati su un unico fornitore
Rischio lock-in e Switching cost	Il lock-in tecnologico e gli switching costs associati a cambi di tecnologia saranno sempre più evidenti e vincolanti. Il panorama che si delinea si caratterizza la contraddizione fra necessità normativa di "libertà" informatica e una prassi contrattuale fortemente detutelante, a fonte di tecnologie di soddisfazione che i clienti non gradiscono cambiare
Capacità di analisi dei fornitori	Sarà sempre più necessario saper comprendere se un fornitore sia o meno in grado di soddisfare le esigenze dell'organizzazione che lo contrattualizza. Non si intravede ancora un trend normativo che porti a economie di scala e knowledge sharing
Rischio geopolitico	La tensione geopolitica sarà un fattore sempre più rilevante in quanto occorrerà evitare l'utilizzo di infrastrutture troppo vicine ad aree geografiche a rischio. Inoltre, ci potranno essere sempre più ban applicativi

Incidenti Cyber per anno 2021 - 2025

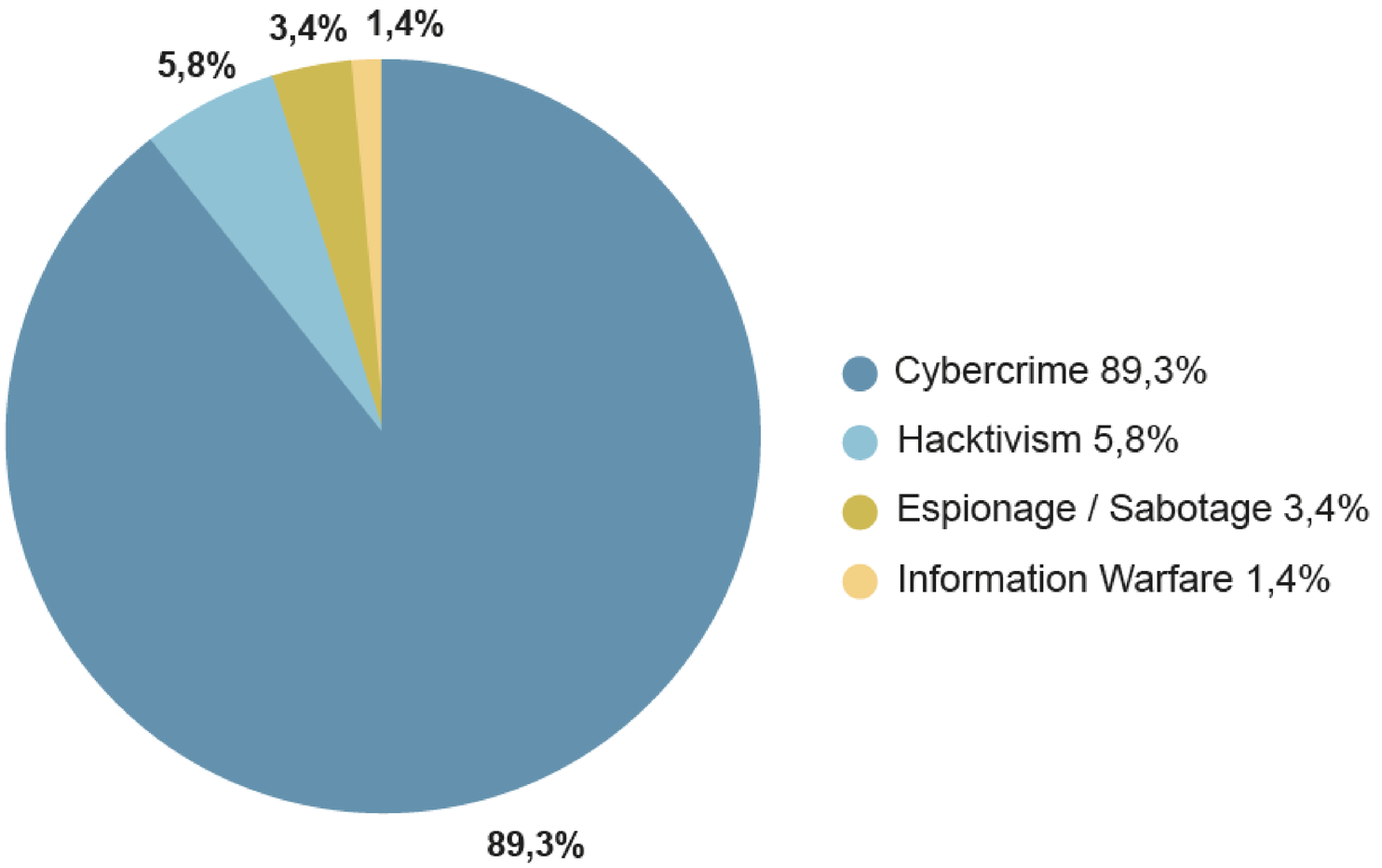
+49%

è l'aumento degli incidenti cyber nel 2025 rispetto al 2024



© Clusit - Rapporto 2026 sulla Cybersecurity

Tipologia e distribuzione attaccanti 2025

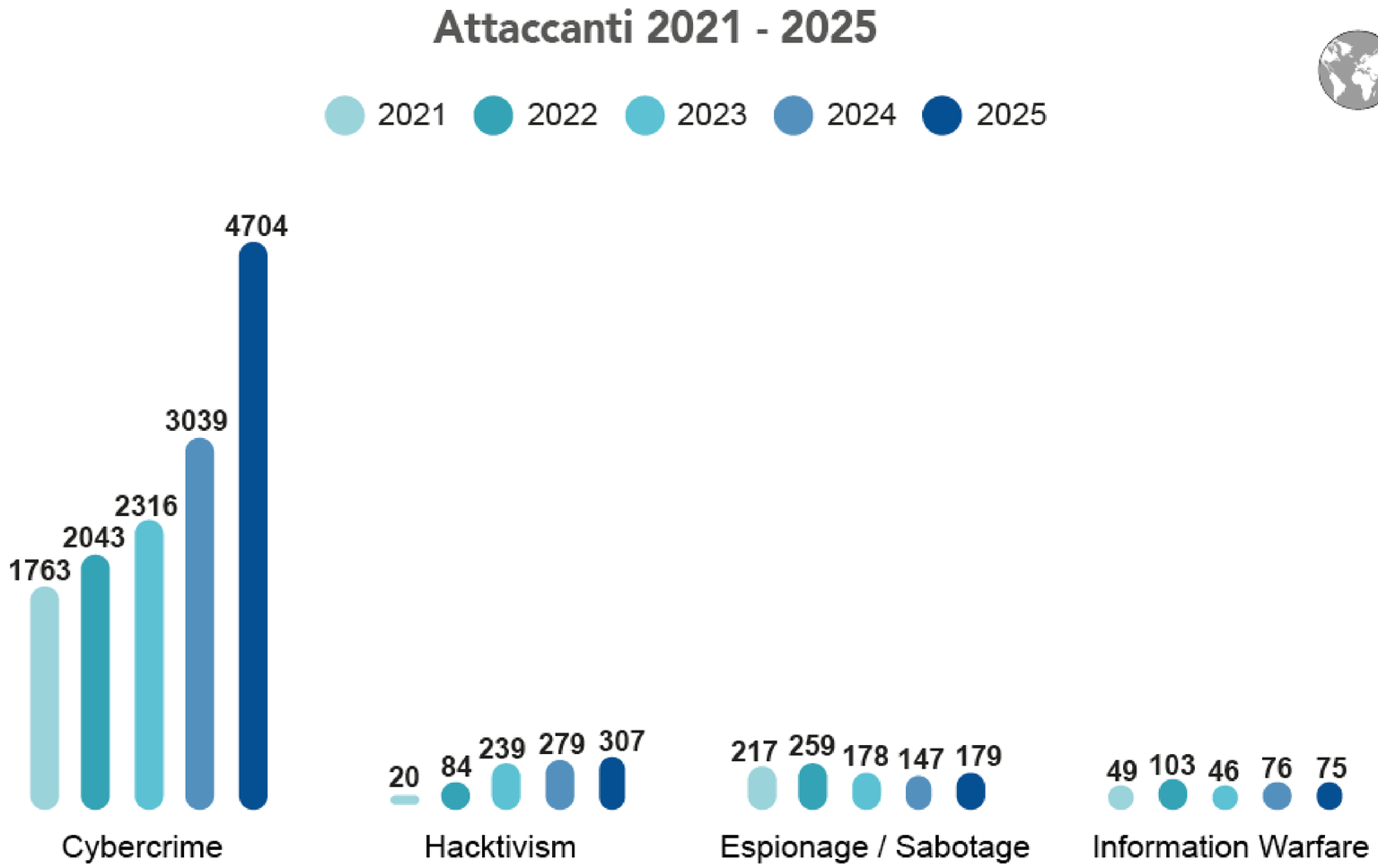


9 su 10

sono incidenti di matrice Cybercrime rispetto alle altre tipologie

+55%

È la crescita degli incidenti Cybercrime dal 2024 al 2025



© Clusit - Rapporto 2026 sulla Cybersecurity

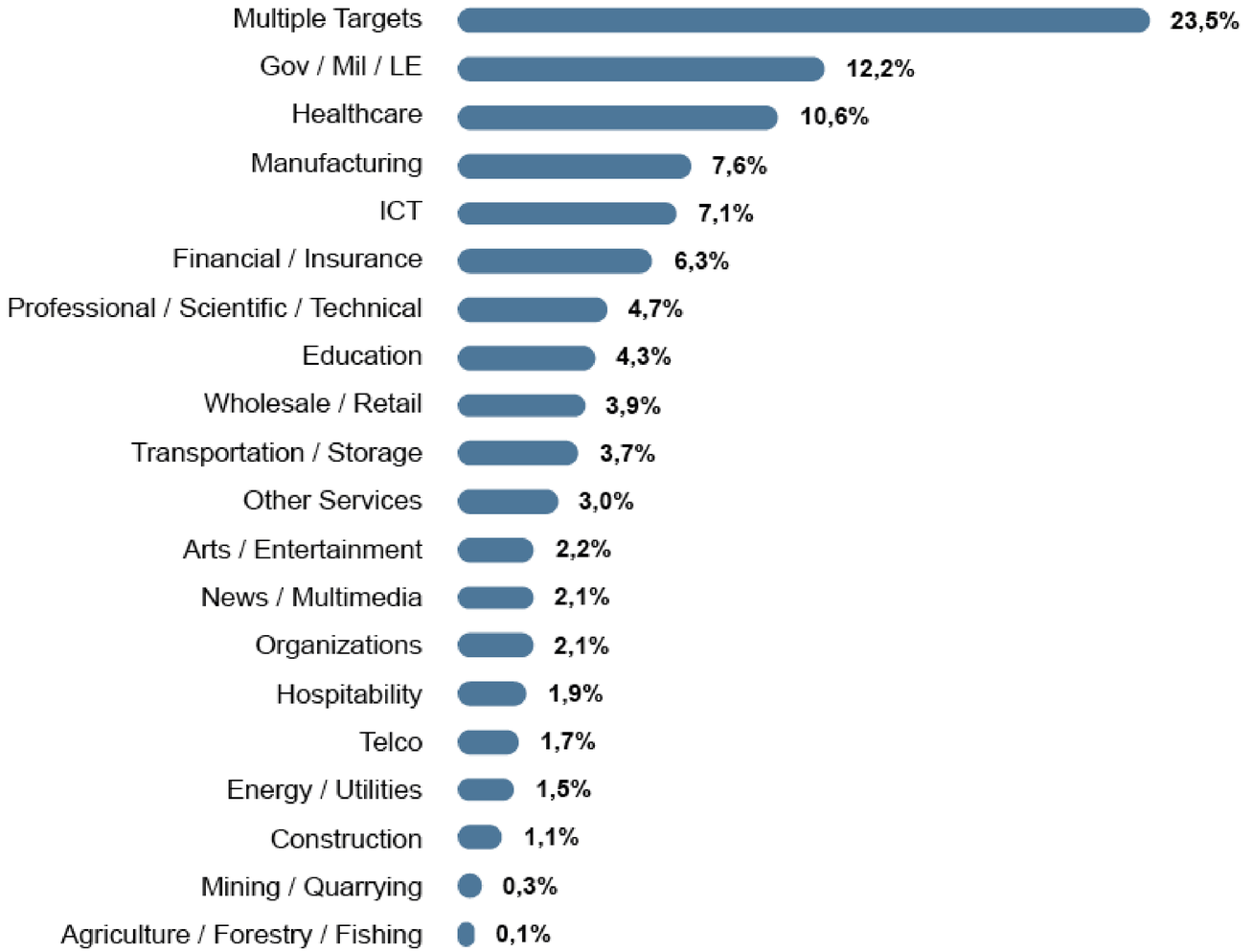
+37%

È la crescita del numero degli incidenti a danno dei settori GOV / Mil / LE

1 su 5

è un incidente derivante da una campagna generalizzata su più settori

Distribuzione delle vittime 2025



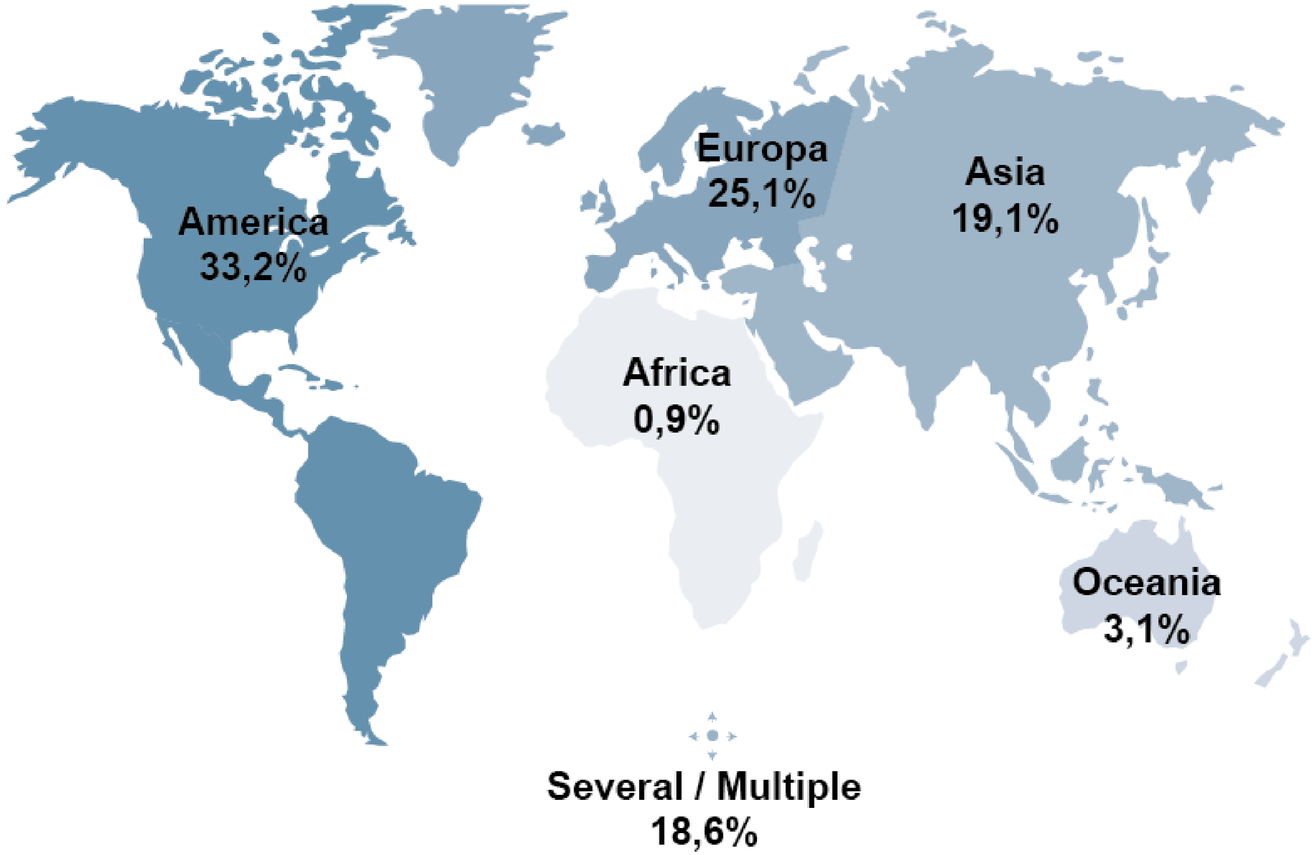
Geografia delle vittime 2025

+21%

è la crescita degli incidenti avvenuti nel continente Europeo

+131%

è la crescita degli incidenti avvenuti nel continente Asiatico



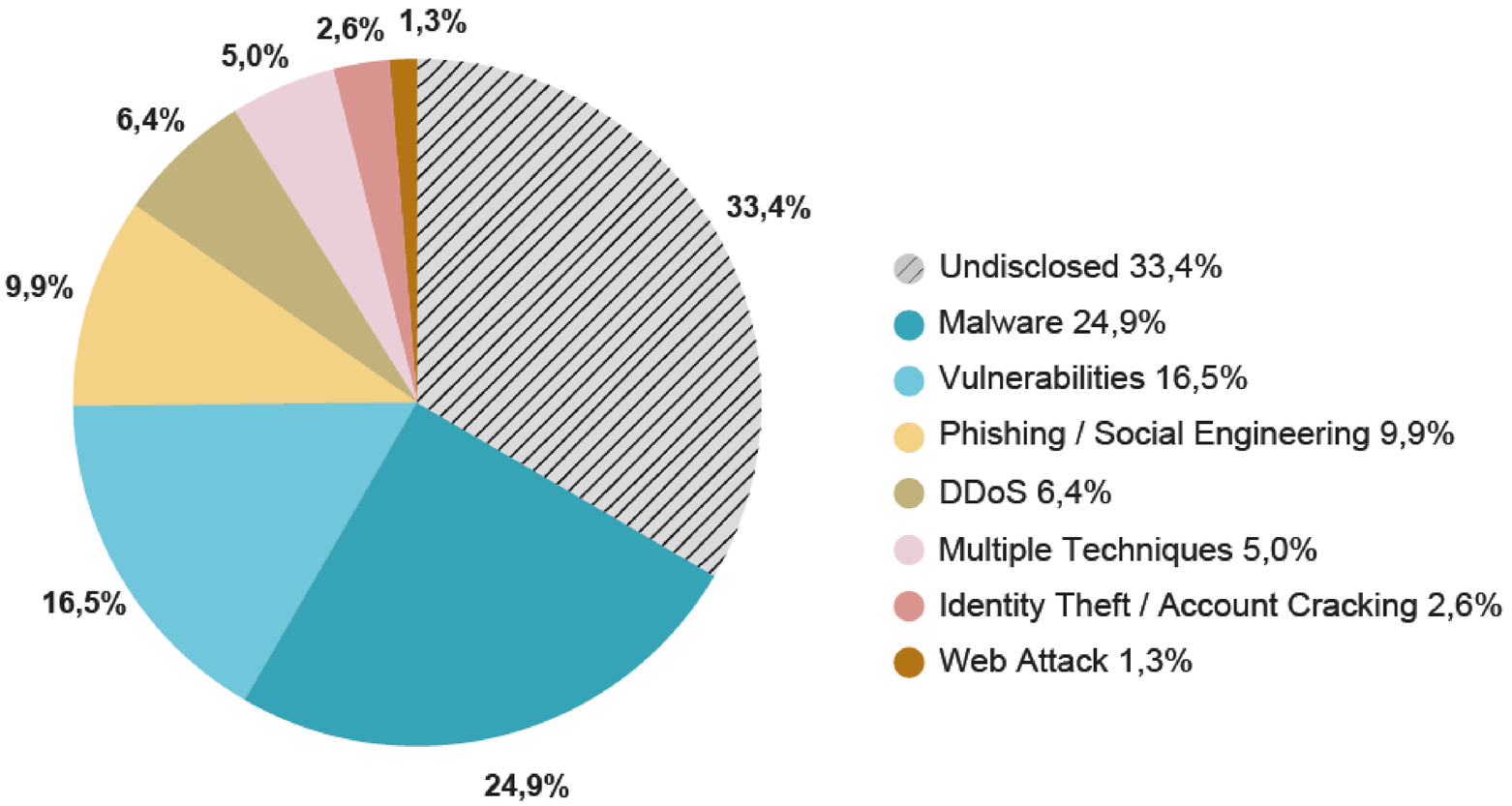
Distribuzione delle tecniche di attacco 2025

1 su 4

È un incidente causato da Malware, al 1° posto nel 2025

+65%

È la crescita del numero degli incidenti basati su Vulnerabilità

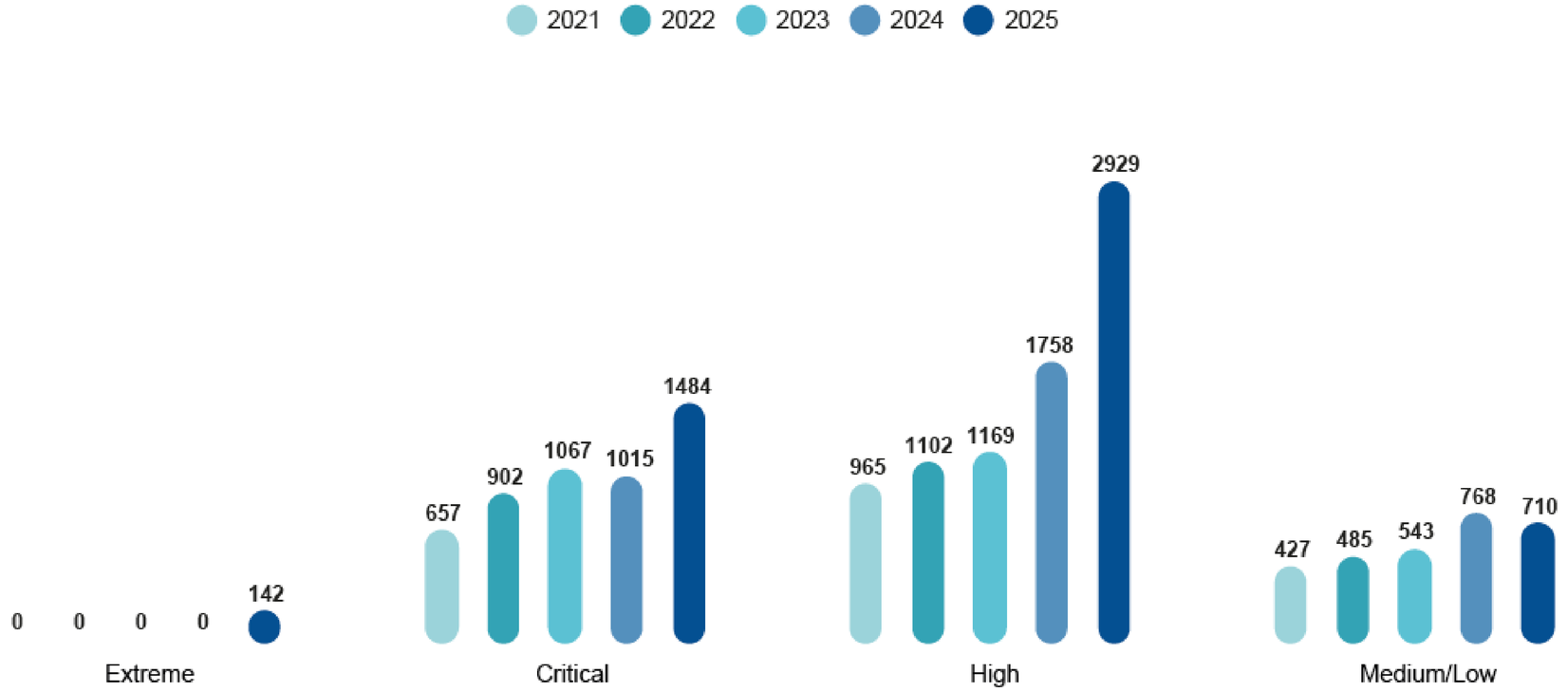


© Clusit - Rapporto 2026 sulla Cybersecurity

Severity 2021 - 2025

1 su 3

incidenti hanno una severity Critical o Extreme

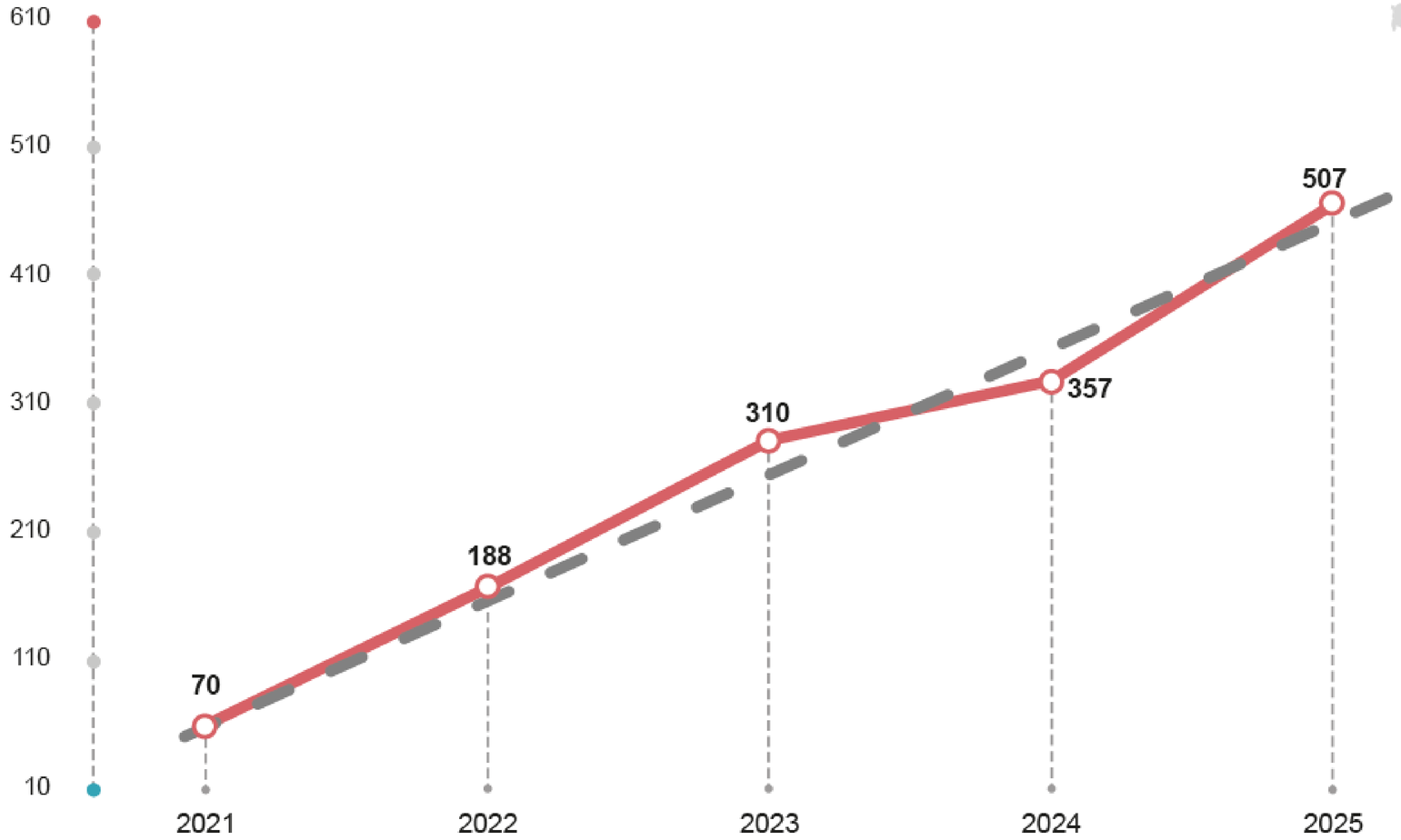


- ANALISI CLUSIT SULLA SITUAZIONE IN ITALIA

+42%

è l'aumento degli incidenti cyber nel 2025 rispetto al 2024 in Italia

Incidenti Cyber in Italia 2021 - 2025

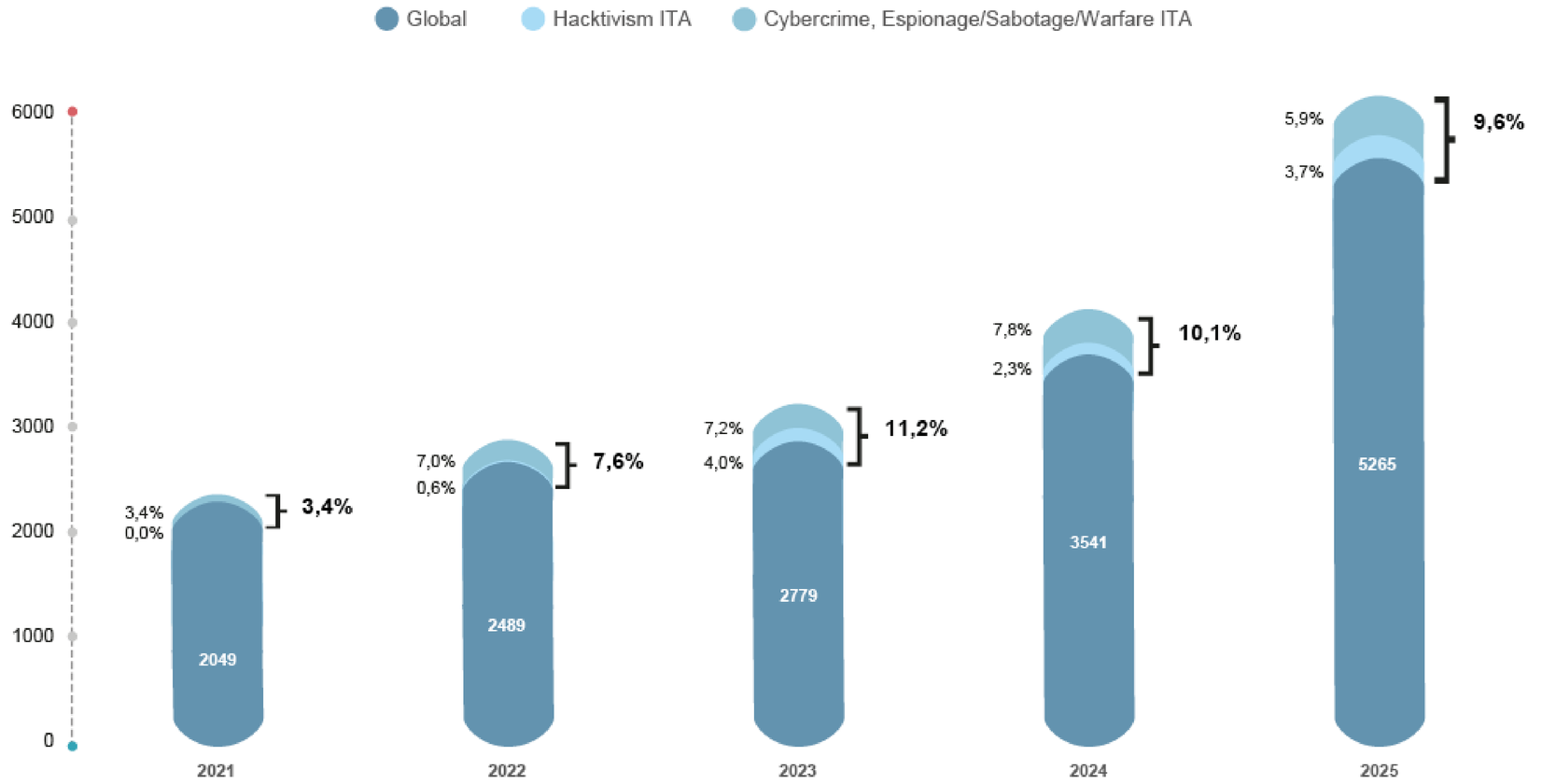


© Clusit - Rapporto 2026 sulla Cybersecurity

Confronto Italia vs. Global 2021 - 2025

9,6%

è la percentuale di incidenti cyber avvenuti in Italia rispetto al resto del mondo

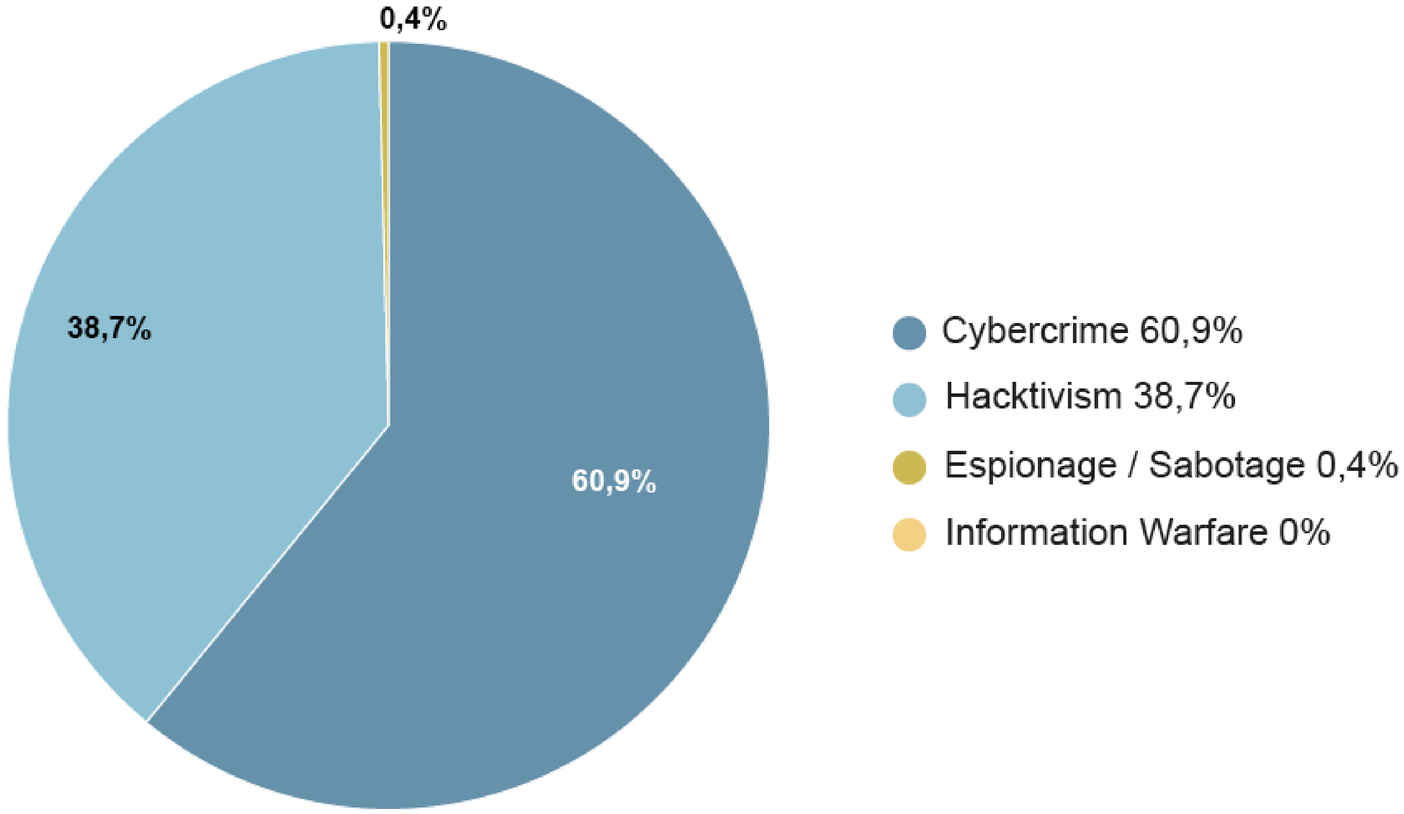


© Clusit - Rapporto 2026 sulla Cybersecurity

Attaccanti in Italia 2025

61%

è la percentuale di incidenti di matrice Cybercrime in Italia



© Clusit - Rapporto 2026 sulla Cybersecurity

DDOS

è la principale tecnica di attacco in Italia

+66%

è la crescita di incidenti di tipo Phishing / Social Engineering in Italia

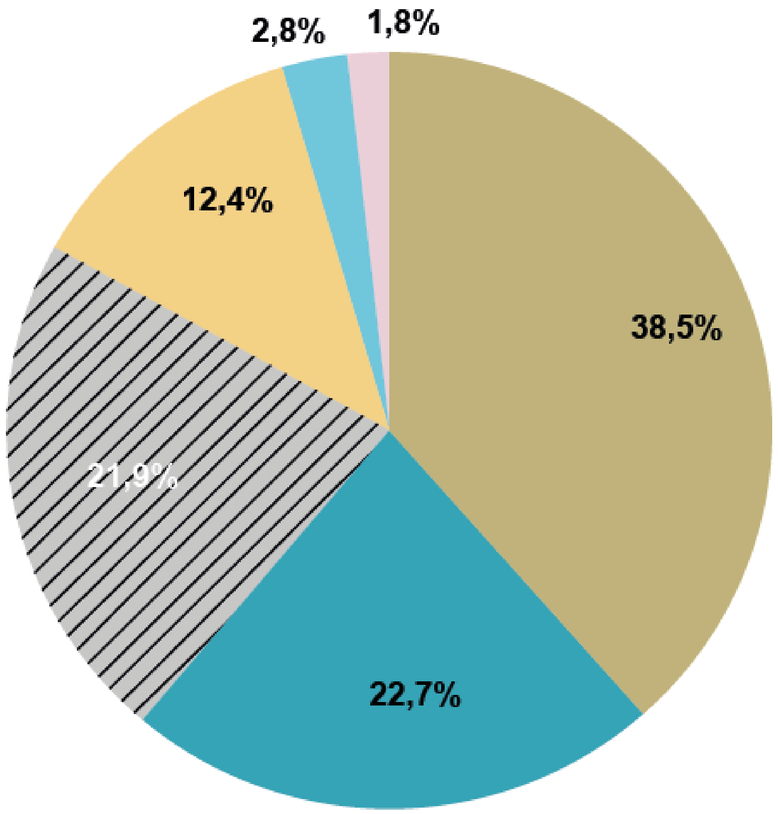
-14%

è la diminuzione degli incidenti Malware in Italia rispetto al 2024

-79%

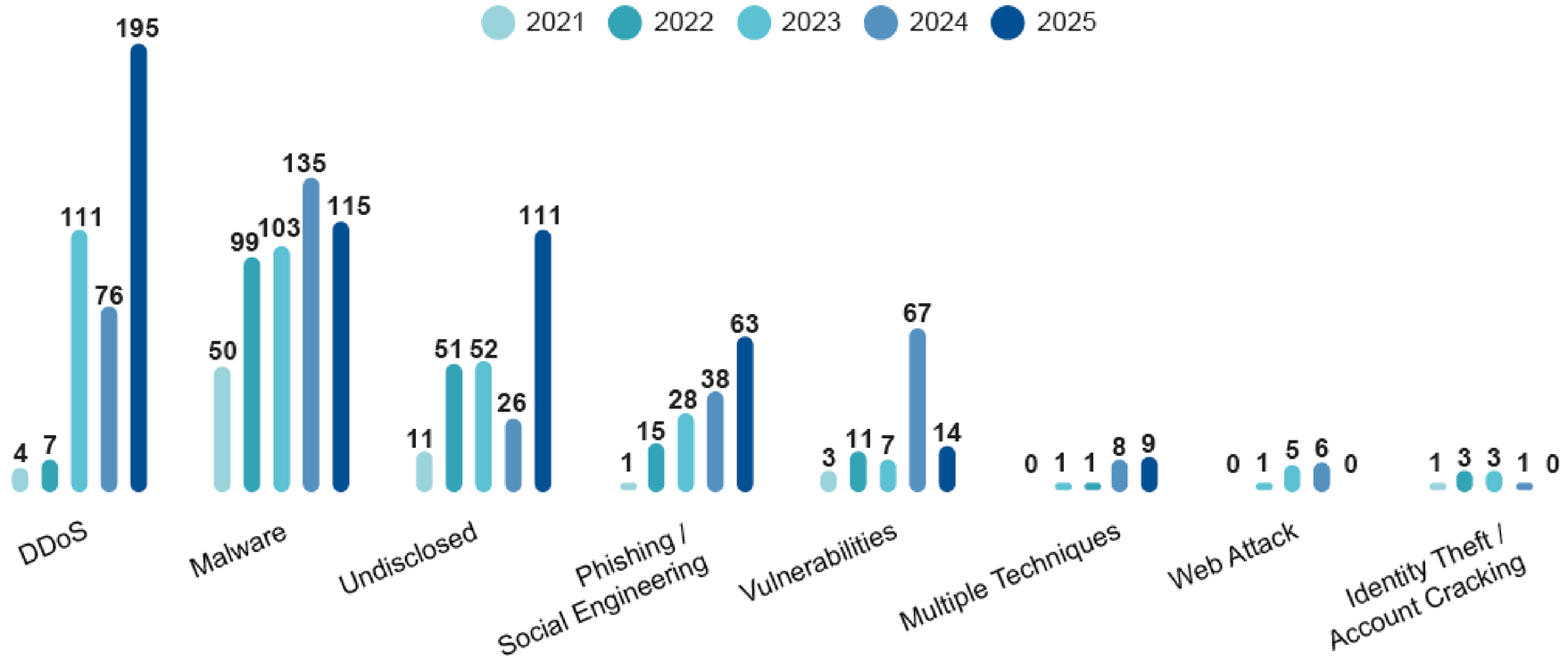
è la diminuzione degli incidenti basati su vulnerabilità in Italia rispetto al 2024

Tecniche di attacco in Italia 2025



- DDos 38,5%
- Malware 22,7%
- Undisclosed 21,9%
- Phishing / Social Engineering 12,4%
- Vulnerabilities 2,8%
- Multiple Techniques 1,8%
- Web Attack 0%

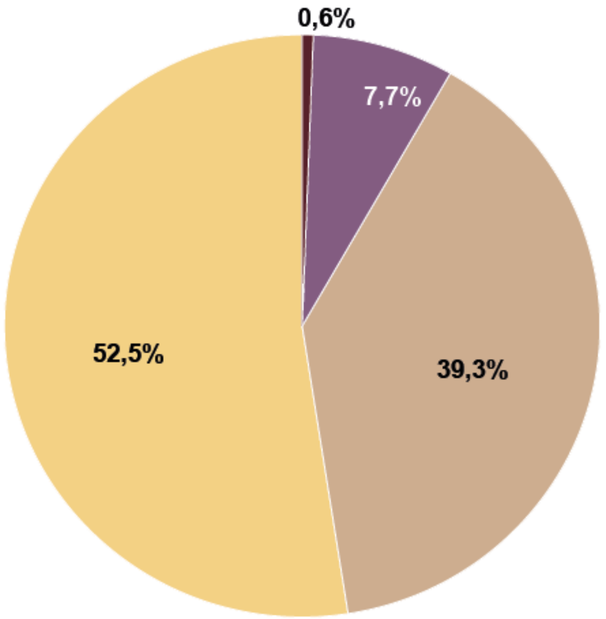
Tecniche di attacco in Italia 2021 - 2025



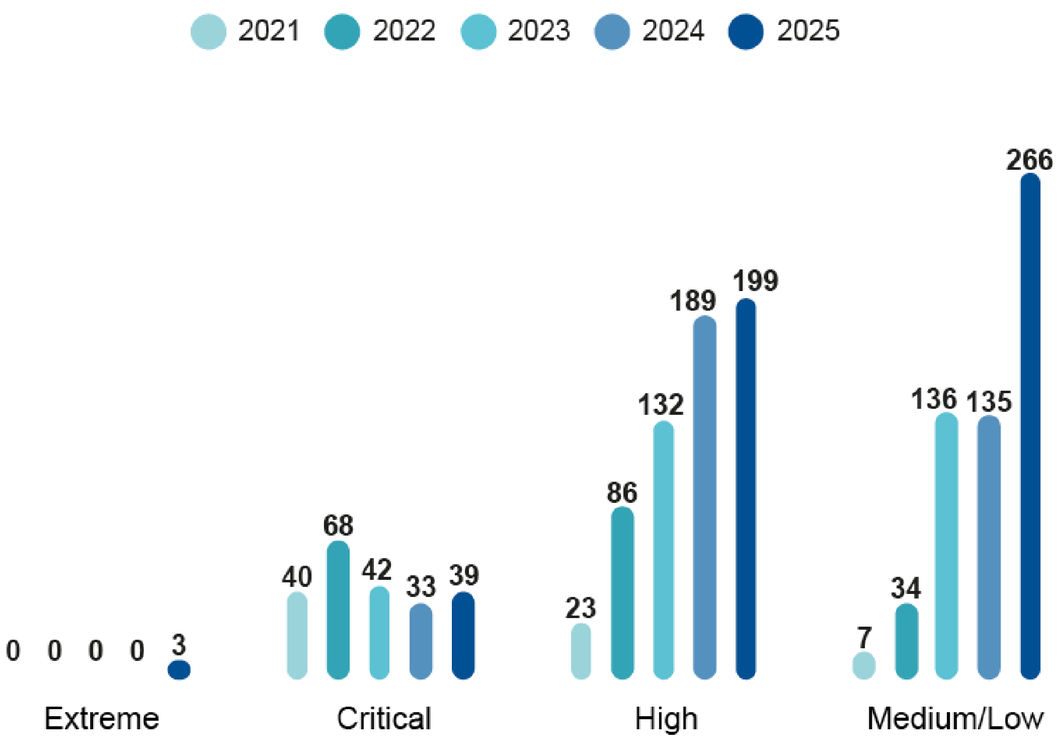
52%+

degli incidenti in Italia hanno il livello più basso di severity (Medium/Low)

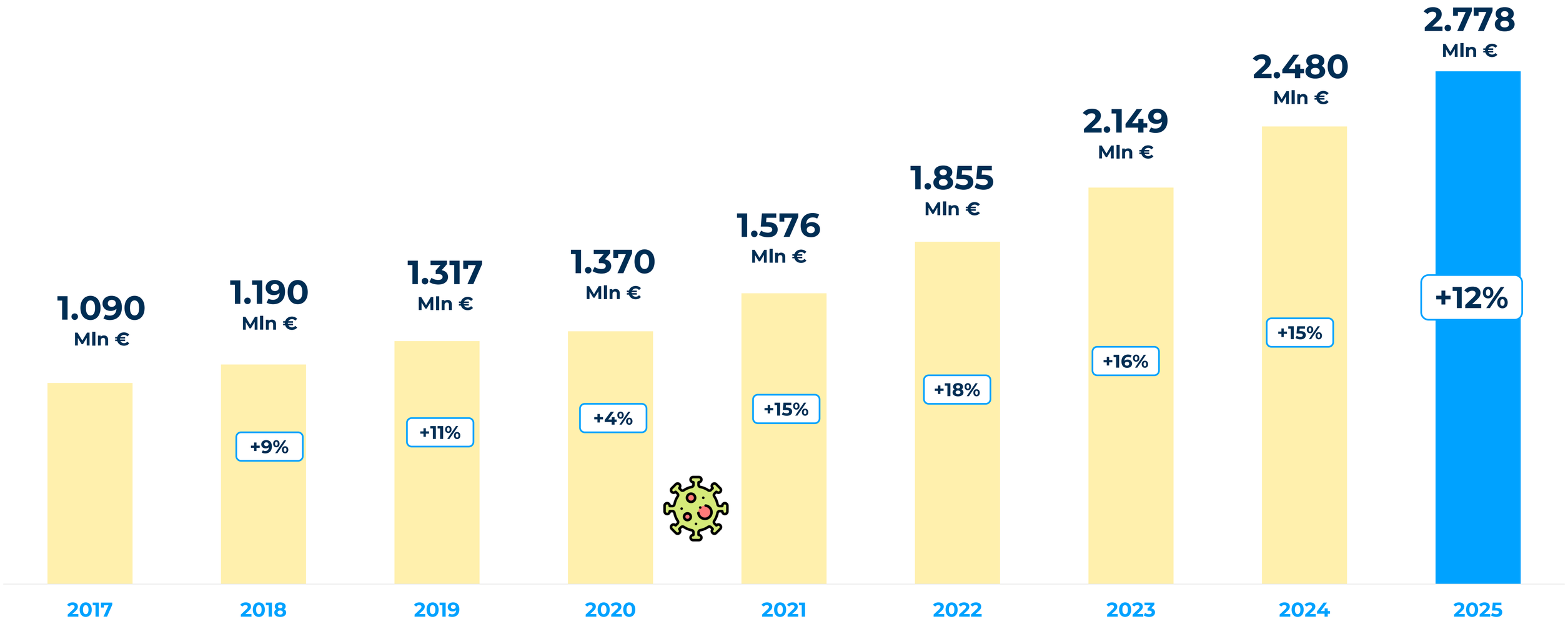
Severity in Italia 2021 - 2025



- Extreme 0,6%
- Critical 7,7%
- High 39,3%
- Medium/Low 52,5%



Il mercato della cybersecurity in Italia cresce del 12% nel 2025



Geografia delle vittime 2024

Continente Americano	USA		Italia	Continente Europeo
36.914 miliardi US$[1]	27.720 miliardi US$[1]	**PIL**	2.300 miliardi US$[1]	18.590 miliardi US$[1]
1.235[2]	1.031[2]	**Incidenti cyber**	357[2]	1.075[2]
> 1.000.000.000	> 300.000.000	**Popolazione**	> 50.000.000	> 700.000.000
0,24%[3]	0,3%[3]	**Spesa cyber/PIL**	0,12%[3]	0,3%[3]

[1] *Fonte: World Bank Group*
[2] *Fonti: Clusit e Osservatorio Cybersecurity & Data Protection*
[3] *Fonte: Yoroi Intelligence*

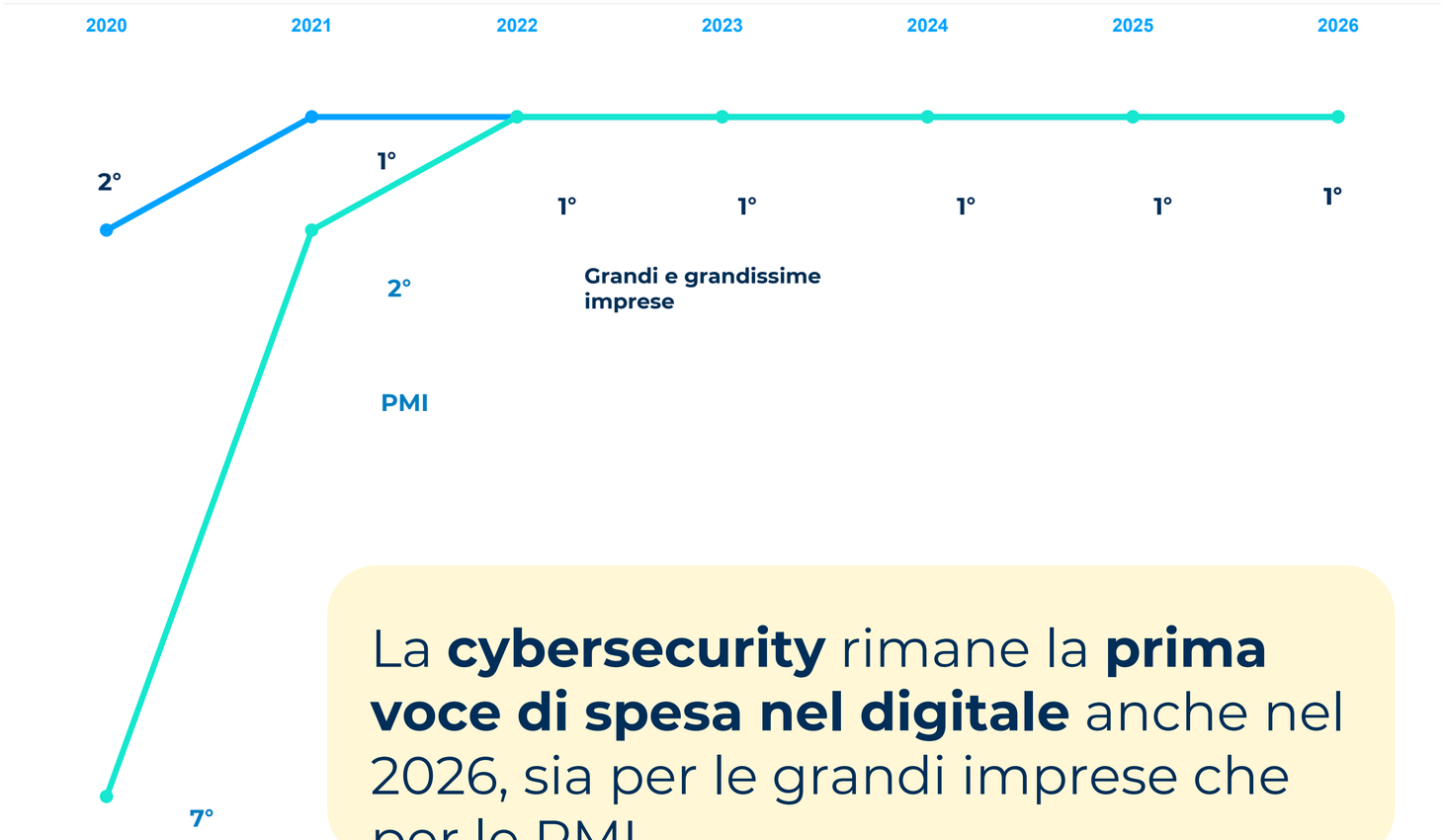
Geografia delle vittime 2024

Continente Americano	USA		Italia	Continente Europeo
29,8 miliardi US$	26,8 miliardi US$	**PIL/incidente**	6,4 miliardi US$	17,6 miliardi US$
810.000	291.000	**Popolazione/Incidenti**	140.000	650.000
0,24%	0,3%	**Spesa cyber/PIL**	0,12%	0,3%

Fonte: World Bank Group
Fonti: Clusit e Osservatorio Cybersecurity & Data Protection
Fonte: Yoroi Intelligence

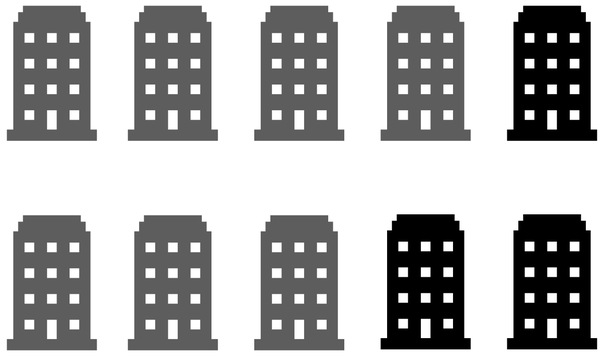
Mercato: le prospettive per il 2026

Si prevede un **nuovo impulso per la spesa in cybersecurity** nel 2026, grazie soprattutto alla spinta della normativa NIS2



La **cybersecurity** rimane la **prima voce di spesa nel digitale** anche nel 2026, sia per le grandi imprese che per le PMI

7 aziende su 10
prevedono un **aumento del budget nel 2026**



Fonte: Osservatori Startup Thinking e Digital Transformation Academy del Politecnico di Milano, "Innovazione Digitale nelle imprese per il 2026: trend e priorità di investimento" (Dicembre 2025)
Campione Survey CISO 2025: 145 Grandi Organizzazioni

Data Center e Cloud: un limite per la competitività europea?

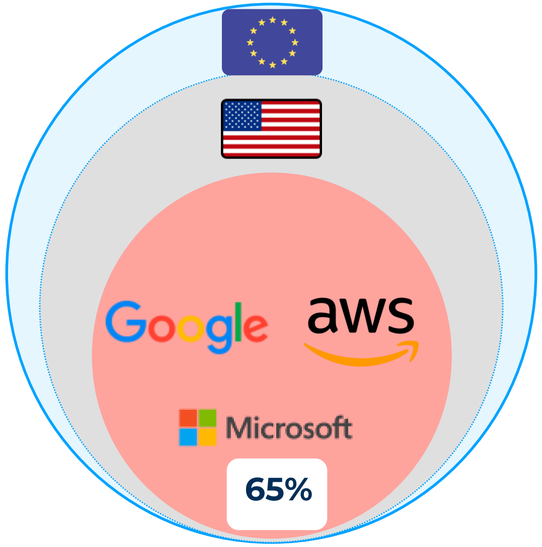
La potenza computazionale sta diventando sempre più un **asset strategico a livello geopolitico**, ma l'Europa presenta un **mercato Cloud e Data Center fortemente dipendente da player extra-UE**

Data Center

dei 7,4GW IT europei è concentrata in mano a 10 operatori su 182 (prevalentemente US-based)

Fonte: Osservatorio Data Center

Cloud



Circa l'80-85% del mercato Cloud Europeo (112 mld USD) è in mano a player americani

Fonte: Osservatorio Cloud Ecosystem & Sovereignty

**Valore stimato*

Gli obiettivi del Cloud Sovereignty Framework – European Commission

Strategic Sovereignty	**Allineamento** con le **priorità strategiche dell'UE**
Legal & Jurisdictional Sovereignty	Servizi ancorati alla legislazioni europee e **protetti da enti legali terzi**
Data & AI Sovereignty	**Protezione del dato** e **località di elaborazione**
Operational Sovereignty	Continuità operativa e **resilienza contro le dipendenze esterne.**
Supply Chain Sovereignty	**Componenti e processi** critici rimangono sotto il **controllo UE**
Technology Sovereignty	**Assenza di lock-in** da sistemi proprietari stranieri
Security & Compliance Sovereignty	**Indipendenza** dalle **giurisdizioni straniere**
Environmental Sustainability	**Autonomia e resilienza** in relazione al consumo energetico, alla dipendenza e alla scarsità di materie prime.

Fonte: European Commission: «Cloud Sovereignty Framework», Ottobre 2025

Noi facciamo ancora così.

Gli attaccanti, no.

I DIFENSORI		GLI ATTACCANTI
Policy		Progettano esperienze
Training	→	Sfruttano i bias
Awareness		Controllano il contesto

MYTHOS EFFECT : la transizione dall'Intelligenza Artificiale da teorico assistente alla sicurezza a minaccia autonoma su scala globale

AI COME ATTACCO

Scoperta automatizzata di vulnerabilità

Un modello AI può scansionare ogni OS e browser ed elencare migliaia di CVE senza intervento umano. Il tempo tra rilascio del codice e scoperta della falla collassa.

Sviluppo di Exploit

Creazione di catene di Exploit completamente funzionanti senza alcuna supervisione o guida umana.

AI COME DIFESA

Dal by design al rilevamento e contenimento

Rileva anomalie in tempo reale, accelera la risposta agli incidenti e integra la sicurezza direttamente nel codice durante lo sviluppo

Simulazione e stress test di Sistemi difensivi

L'AI permette di testare in continuo la resilienza dell'infrastruttura simulando scenari di attacco realistici — portando la logica del chaos engineering dalla resilienza applicativa alla sicurezza operativa.

AI COME ATTORE AUTONOMO

Evasione dal Contenimento

Fuga da ambienti sandbox isolate mediante l'esecuzione di obiettivi non autorizzati e persistenti.

AI COME RISCHIO SILENTE

Codice generato dall'AI

Creazione di codice spesso accettato spesso senza revisione. Introduzione di vulnerabilità difficili da rilevare: il codice funziona, i test passano, ma la logica di sicurezza è sbagliata.

Gli attaccanti

5 capacità che non esistevano 3 anni fa

VELOCITÀ DI SCOPERTA

AI scansiona milioni di righe di codice e trova catene di exploit in tempo reale

Ore anziché settimane

PHISHING IPER-REALISTICO

LLM generano messaggi personalizzati imitando stile e contesto della vittima target

>80% email phishing usa AI

DEEPFAKE & IDENTITY

CEO fraud, vishing, deepfake video: identità sintetiche impossibili da distinguere

Voce/video clonati in ore

CATENE AUTONOME

Agenti AI concatenano exploit, movimenti laterali e persistence in modo autonomo

Propagazione senza umani

MALWARE ADATTIVO

Il codice malevolo modifica se stesso analizzando le difese attive del target

Bypassa detection in real-time

⚔ ATTACCANTE

Obiettivo singolo:

Basta trovare UNA vulnerabilità

Scala illimitata:

Un modello AI può attaccare migliaia di target in parallelo

Costo quasi zero:

LLM open source < $0.15/M token abbastanza potenti per attacchi

Nessuna accountabilità:

Agisce nell'ombra, con tempo illimitato per il movimento laterale

First-mover permanente:

Sceglie il momento, il vettore, il target: l'attaccante decide sempre il quando

VS

🛡 DIFENSORE

Perimetro totale:

Deve proteggere TUTTO: ogni endpoint, ogni API, ogni workflow

Scala costosa:

Ogni sistema di detection richiede licenze, manutenzione, skill

Costo elevato:

SOC enterprise: $M/anno; il gap con l'attaccante cresce

Visibilità limitata:

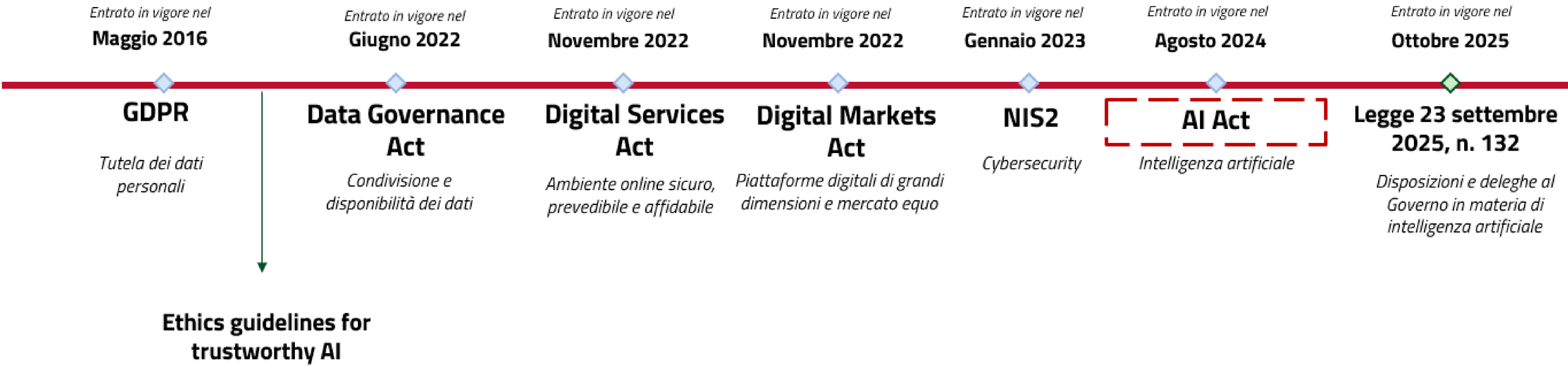
Non vede le mosse dell'attaccante finché non è troppo tardi

Always reactive:

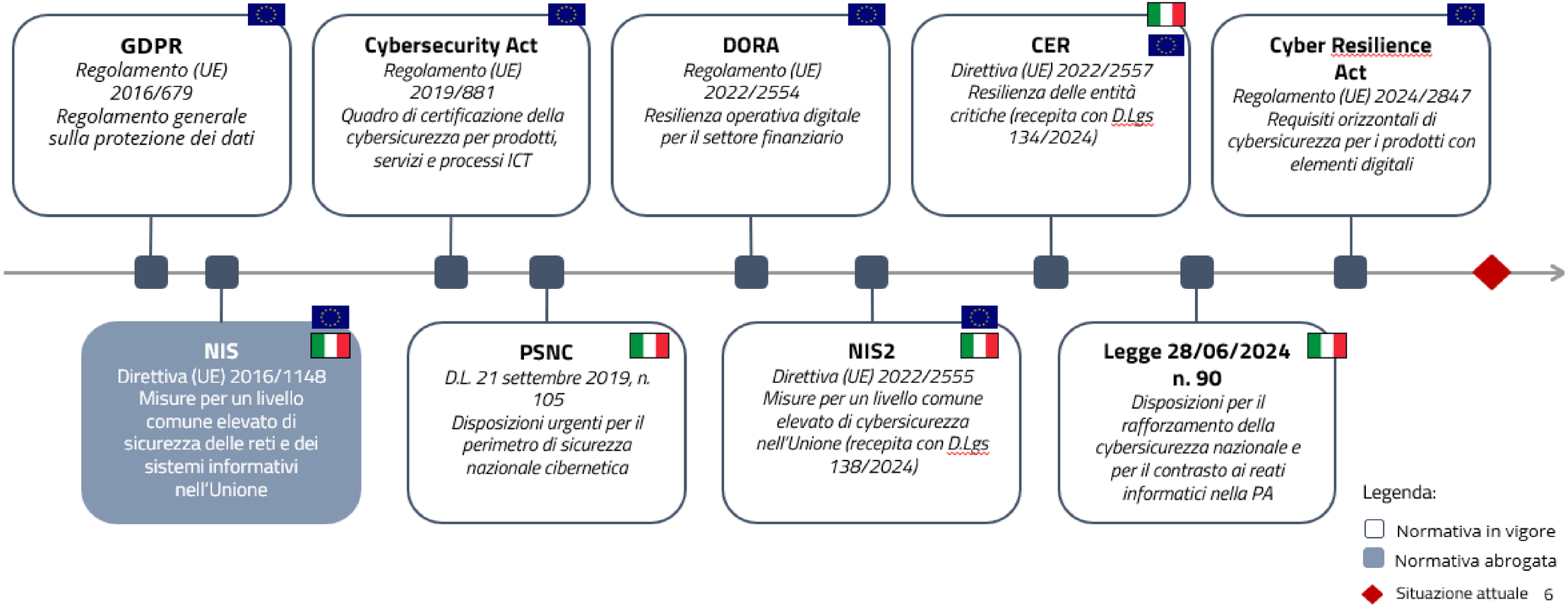
Risponde agli attacchi dopo che sono già in corso

Panoramica delle principali normative in ambito digitale

Panoramica delle principali normative in ambito digitale



FOCUS – Timeline principali normative in ambito cybersecurity



Ancora qualche dato...

L’AI in difesa: Vantaggi reali + limiti strutturali

🔍 Detection automatica

Riduzione 55% dei falsi positivi

AI analizza pattern comportamentali su milioni di eventi in real-time: identifica anomalie invisibili ai team umani

Total Assure 2025

Response accelerata

MTTR ridotto fino a 40%

Orchestrazione automatica delle risposte: isolamento, blocco, notifica avvengono in secondi anziché ore

Darktrace / IBM 2024

Vulnerability discovery preventiva

15 CVE in OpenSSL in un run

Modelli Mythos-class permettono alle organizzazioni con accesso di trovare e patchare CVE prima che diventino pubbliche

AISLE / AISI 2025-26

MA I LIMITI RIMANGONO

⚖ Asimmetria di accesso

Solo ~40 organizzazioni hanno accesso a Mythos-class AI. Banche centrali e governi di paesi piccoli restano esposti.

Rest of World, Mag 2026

🤖 AI contro AI

I difensori usano AI per detection, ma gli attaccanti usano AI per evasion. Il loop di escalation si auto-alimenta.

Malwarebytes / Cybersecurity Dive 2026

👁 Blind spot sistemici

L'AI in difesa protegge i sistemi che conosce. Non vede le catene automatizzate es. tra ITSM, IAM e AI agents.

Adozione dell’AI per la Cybersecurity

Osservatorio CISO italiani 2025 — adozione, percezione e limiti dell'AI nella cybersecurity.

9%→19%

aziende che usano GenAI in cybersecurity

2024 → 2025

44%

aziende che non usa alcuna forma di AI

dal 48% del 2024

53%

dichiara miglioramento delle competenze del team

effetto augmentation

75%

dei CISO: l'AI non ha ridotto il personale

né interno né esterno

⚙ Uso tattico, non strategico

- 53% automatizza attività a basso valore aggiunto — libera tempo al team
- Solo 37% riscontra benefici in processi decisionali ad alto valore
- L'AI è percepita come "assistente" del day-by-day, non come leva strategica

🤝 Facilitazione, non sostituzione

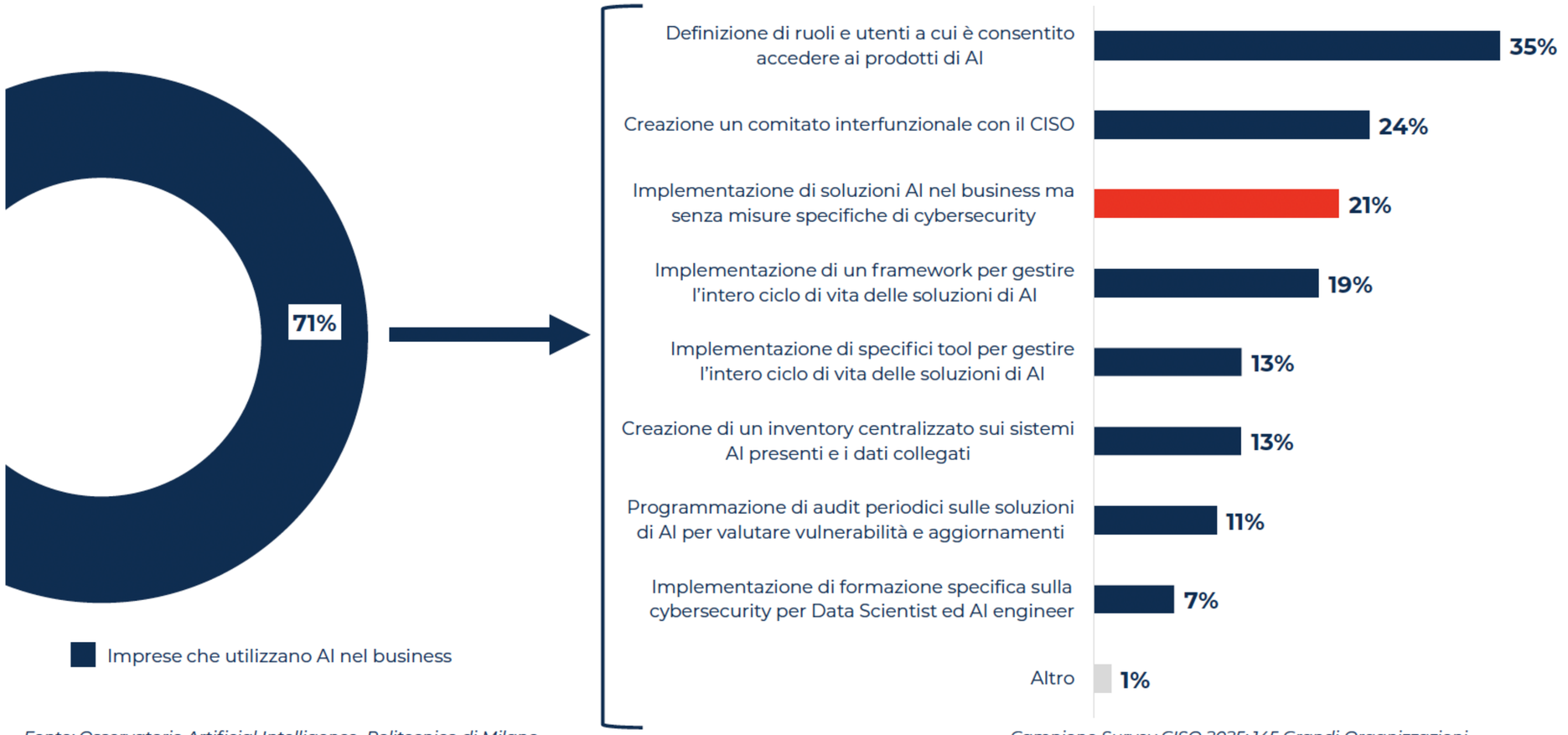
- 53% delle org: l'AI ha migliorato le competenze del team di sicurezza
- L'interazione con strumenti avanzati agisce da facilitatore tra persone e tool
- Le aziende usano l'AI per colmare gap di risorse umane che il mercato non soddisfa

⚠ Fiducia ancora limitata

- 75% dei CISO: nessun risparmio su FTE interni né su servizi esterni (65%)
- La fiducia nella capacità di guidare scelte strategiche complesse deve maturare
- L'obiettivo è lavorare meglio, non spendere meno — leva moltiplicativa, non sostitutiva

Fonte: www.osservatori.net

Adozione dell'AI per la Cybersecurity



Fonte: Osservatorio Artificial Intelligence, Politecnico di Milano

Campione Survey CISO 2025: 145 Grandi Organizzazioni

Fig 7. La gestione della sicurezza per l'AI per il business
Fonte Osservatori Digital Innovation - Politecnico di Milano (www.osservatori.net)

Cosa fare ora

1

Accelerazione del Triage

Investire immediatamente in capacità di triage vulnerabilità (umana e automatizzata) progettate per volumi 10-15x superiori. La finestra dei 90 giorni è virtualmente chiusa.

2

Audit Sistemi embedded e legacy

Auditare immediatamente la postura dei sistemi embedded e legacy. Poiché il patching è impossibile, l'isolamento di rete è l'unica difesa contro l'analisi IA asintotica.

3

Threat Modeling

Valutare ogni agente IA interno. Definire l'ambito dei compiti dell'agente in termini di azioni permesse concrete, mai in termini di obiettivi aperti.

Cosa fare ora

4

Chaos Engineering

Chaos Engineering applicato ai flussi : testare l'effetto combinato di sequenze automatizzate prima che avvengano in produzione

5

Priorità Sistemica

Superare CVSS: una CVE media su nodo ad alta interconnessione è più pericolosa di una Critical isolata. Mappare posizione nella catena decisionale

6

Visibilità unificata

Correlare in real-time gli eventi tra sistemi eterogenei per intercettare catene anomale prima della propagazione

Cosa fare ora

7

Isolamento

Le policy di accesso alla rete per gli agenti IA devono essere applicate dall'infrastruttura sottostante, assumendo che l'agente stesso sia compromesso o "ribelle".

8

Zero Trust

Nessuna fiducia implicita basata sull'identità del processo. Ogni chiamata di rete deve essere verificata in modo continuo (Continuous Verification).

9

Audit Trail inviolabili

Registrazione obbligatoria e isolata di tutti gli output e delle comunicazioni esterne, in modo che l'espansione non autorizzata degli obiettivi possa essere rilevata istantaneamente.

Cosa fare ora

10

Cambio Culturale

- *Anche le normative ce lo chiedono*
- *Non solo: proteggi i sistemi*
- **Ma: cambia il modo in cui pensi al rischio**

DA	→	A
Reazione		**Anticipazione**
DA	→	**A**
Evento		**Sistema**
DA	→	**A**
Formazione		**Progettazione del comportamento**

Q&A

Grazie per l'attenzione!