TIG | EVENTS

CSA Cyber Security @ngels

TIGSURVEY
Cyber Risk Management 2024

Ezio Viola, Co-Founder, TIG

29 Febbraio 2024

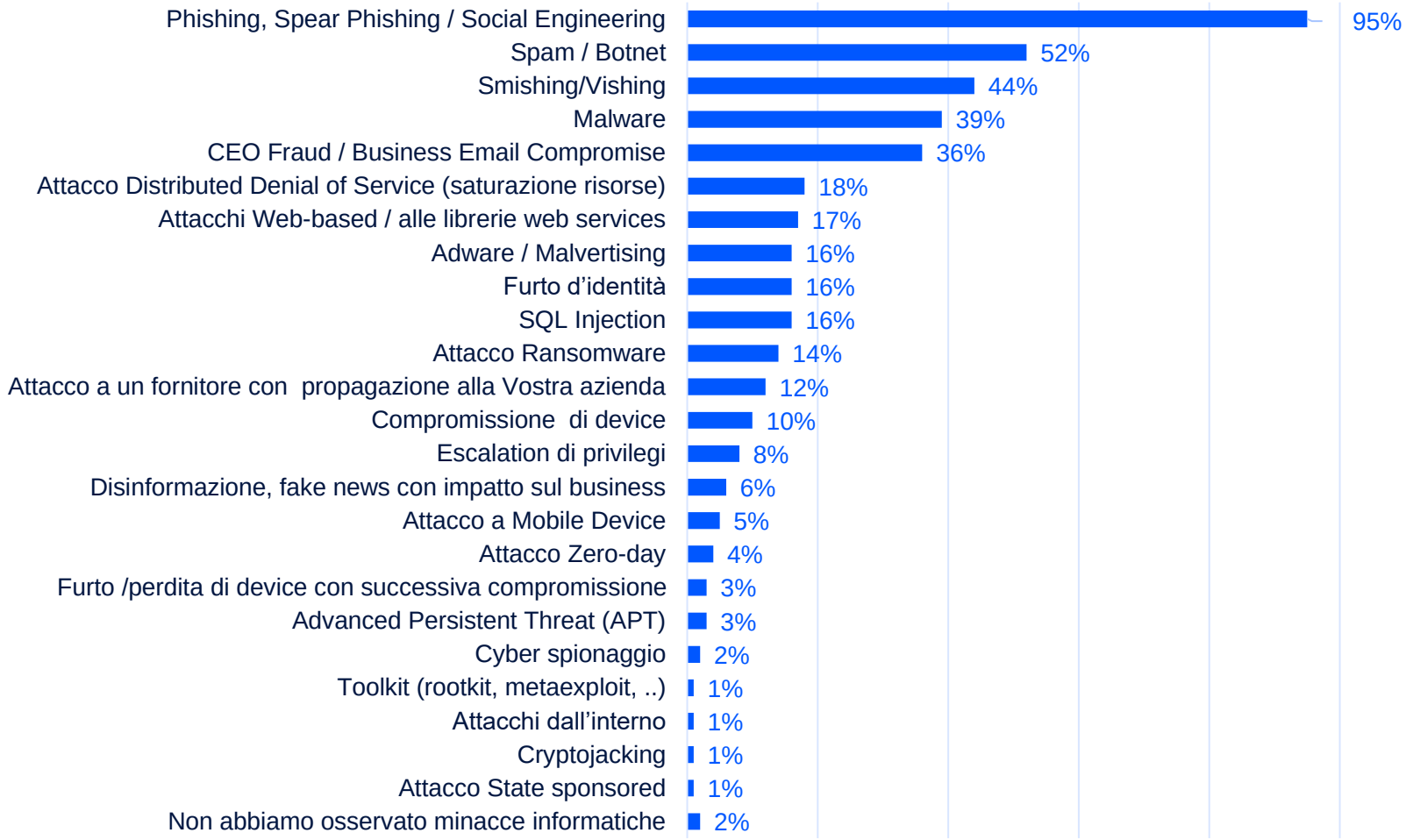
Image: Freepik

I TREND DEL CYBER RISK MANAGEMENT NEL 2024

GLI ATTACCHI CYBER SONO OSSERVATI IN GRAN NUMERO.

- Tutte le aziende (il 95% secondo la survey) ha osservato nel 2023 attacchi di phishing; il 52% spam / botnet; il 44% smishing/vishing; il 39% malware e il 36% CEO Fraud / Business email compromise.
- In media le aziende osservano 4,2 diverse tipologie di minacce nel corso di un anno.

Domanda. Nel corso degli ultimi 12 mesi, quali dei seguenti tentativi di attacco / tecniche di attacco avete rilevato nella Vostra azienda?



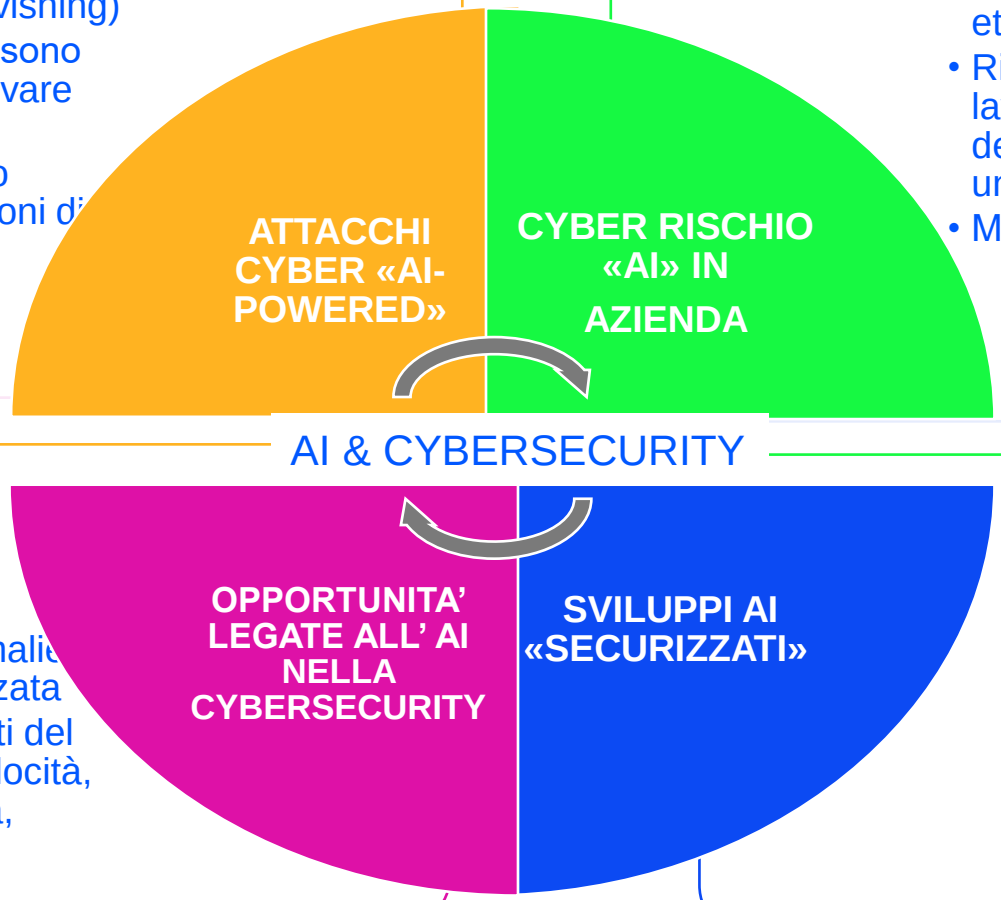
FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024, N = 166 RESPONSABILI CYBERSECURITY E CIO / IT MANAGER

RISCHI E OPPORTUNITÀ DELL'AI IN CYBERSECURITY

RISCHI

OPPORTUNITA'

- La GenAI può migliorare significativamente l'efficacia e la portata degli attacchi di ingegneria sociale (phishing, smishing, vishing)
- Gli attacchi basati sull'AI possono apprendere dalle difese e trovare nuovi modi per aggirarle
- Gli attacchi targeted possono aggirare le tradizionali soluzioni di sicurezza informatica



- Compliance - integrazione della privacy nei sistemi di intelligenza artificiale
- Necessario prevedere linee guida etiche per l'IA
- Rischio di perdere posti di lavoro/competenze a causa dell'automazione dell'IA – rischio di un'eccessiva dipendenza dall'IA
- Malfunzionamento dell'AI - allucinazioni

- Superamento limiti di soluzioni tradizionali – capacità di riconoscimento pattern e anomalie analisi comportamentale avanzata
- Supporto al lavoro degli analisti del SOC, preventivo e reattivo (velocità, efficienza, base di conoscenza, democratizzazione del dato)

- Dare priorità alle tecniche di mitigazione dei rischi cyber per i sistemi di IA
- Rafforzare le misure di sicurezza dei sistemi di IA
- Reporting di compliance automatizzato

I RESPONSABILI DELLA SICUREZZA INFORMATICA SONO CONSAPEVOLI CHE L'UTILIZZO DELL'AI PUÒ COMPORTARE NUMEROSI RISCHI DI CYBERSECURITY

Domanda. Con riferimento all'utilizzo sempre più ampio, in azienda e fuori, di soluzioni basate su intelligenza artificiale, quali sono, secondo Lei, i principali rischi da considerare?

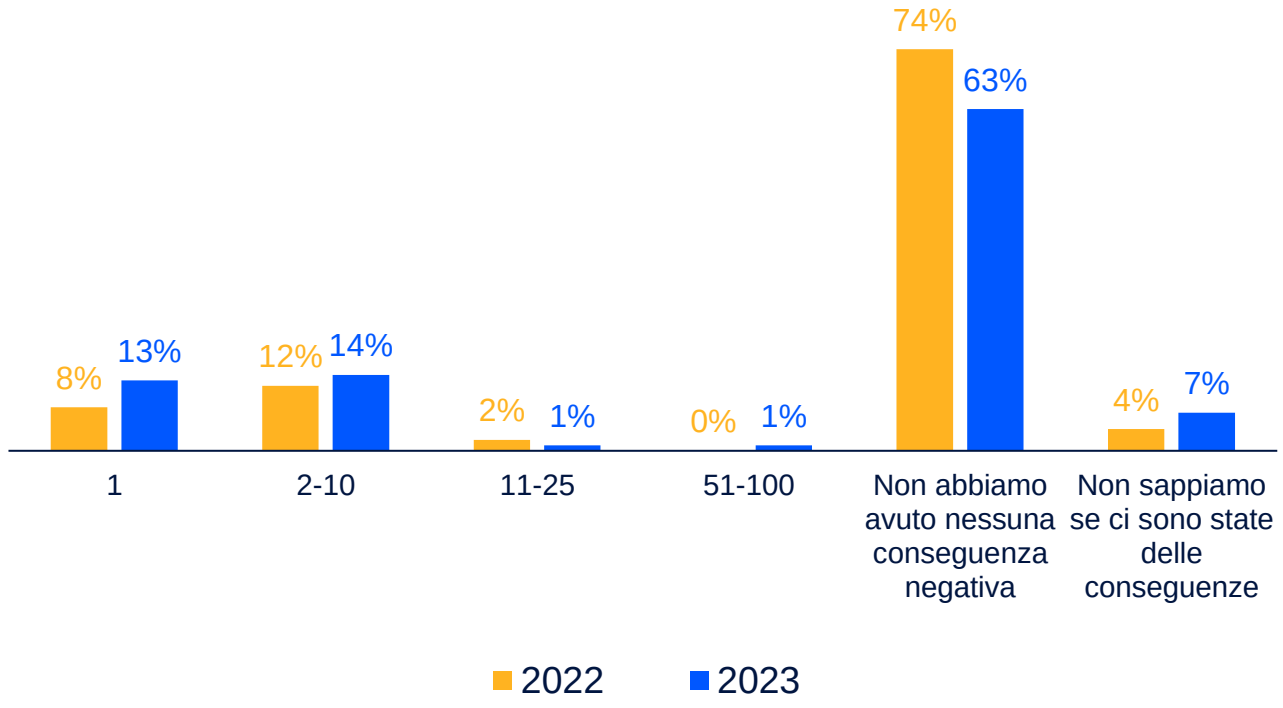
- 52% Rischio di non compliance (es. privacy)
- 52% Attacchi con falsi audio e video (es. deepfake)
- 47% Risultati non corretti, scarsa supervisione
- 46% Comportamenti imprevisti
- 36% Vulnerabilità dei modelli AI
- 33% Adversarial Machine Learning
- 23% Decisioni discriminatorie
- 8% Non saprei

FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

PARLIAMO DI INCIDENTI DI CYBERSECURITY CON IMPATTI SERI

- Le aziende sono costantemente sotto attacco cyber e spesso hanno esperienza di eventi con minore danno. Parlando però di incidenti seri, che hanno avuto conseguenza per l'azienda (mancata operatività, data breach), nel 2023 il **30% delle aziende dichiara di averne avuto esperienza almeno una volta, nel 14% delle aziende anche in più occasioni**: un numero in forte crescita rispetto al 22% dell'anno precedente.
- La situazione risulta più complessa per le grandi organizzazioni, dove il numero di chi ha avuto incidenti arriva al 37%.
- Il 23% delle grandi organizzazioni inoltre ha avuto più incidenti (in numero compreso tra 2 e 10). Segnale importante che gli incidenti avvengono ed è importante gestirli in modo efficace.

Domanda. Quanti incidenti informatici subiti hanno avuto nel 2023 conseguenze in termini di data breach o indisponibilità/danni a sistemi e servizi ICT?

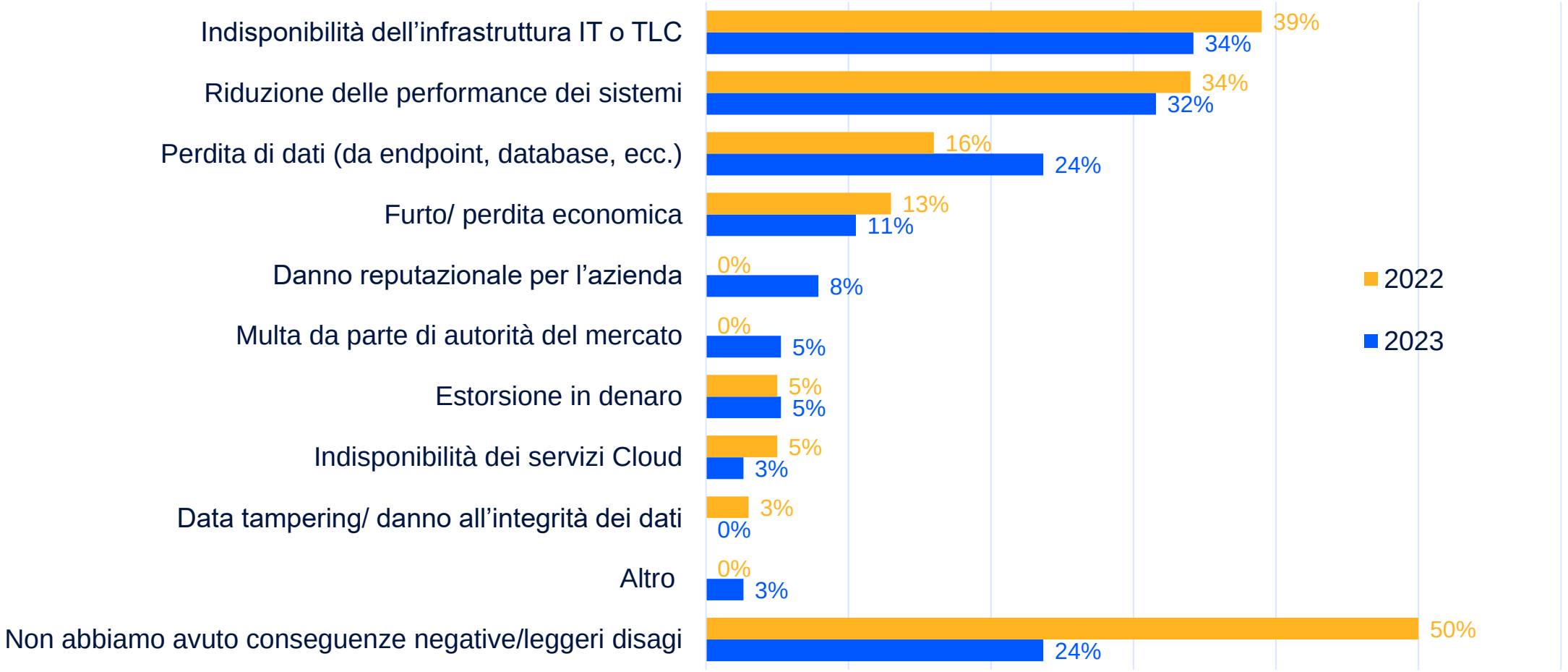


FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

NEL 2023 SI DIMEZZA IL NUMERO DI CHI HA SUBITO SOLO LIEVI CONSEGUENZE, QUINDI IL DANNO COMPLESSIVO È MAGGIORE

THE INNOVATION GROUP

Domanda. Quali sono state nel 2023 le conseguenze degli incidenti cyber?



FONTE: CYBER RISK MANAGEMENT SURVEY 2024, GENNAIO 2024. RISPONDENTI: CHI HA SUBITO INCIDENTI CON CONSEGUENZE.

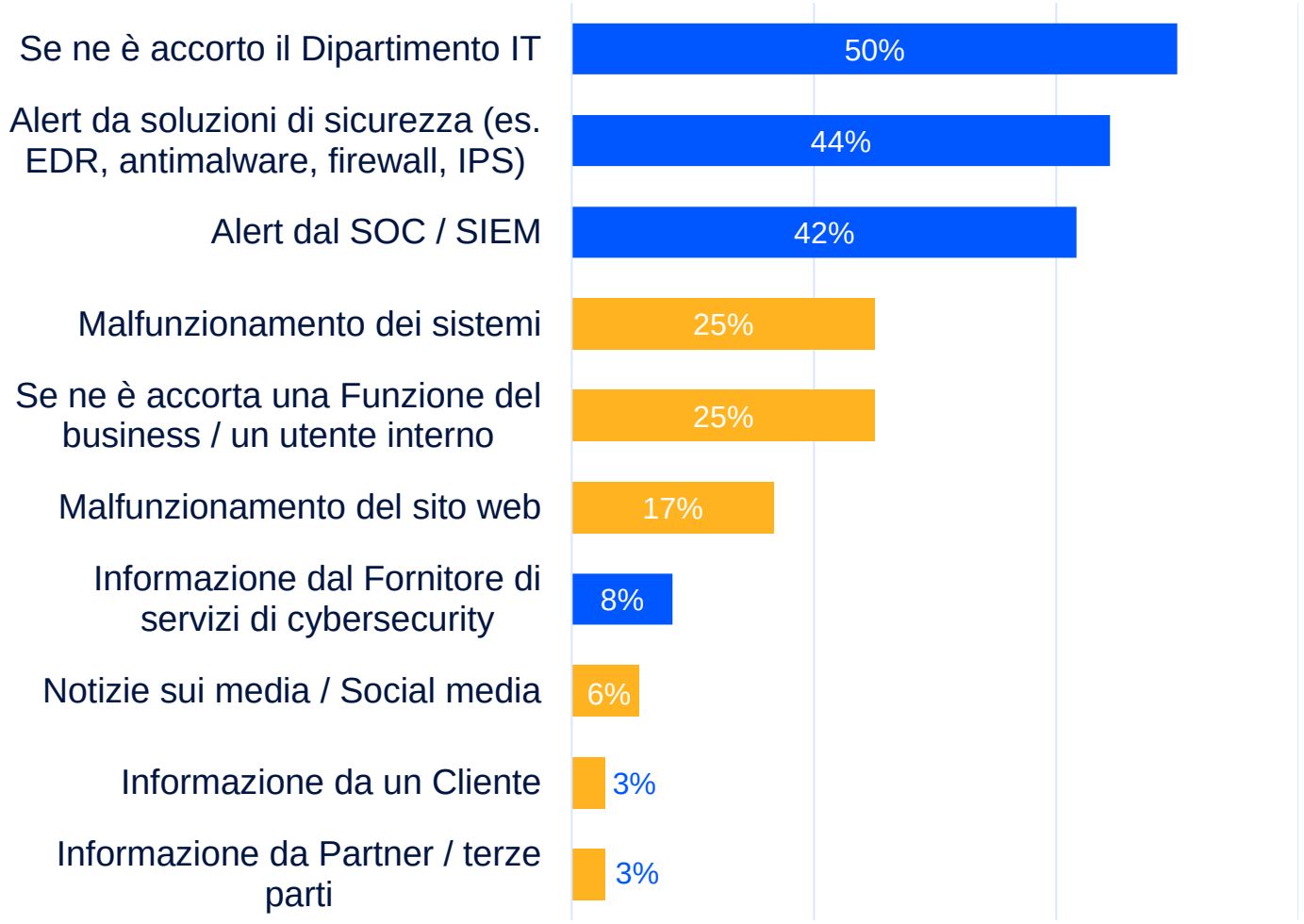
CSA Cyber Security @ngels

TIG EVENTS

COME CI SI ACCORGE DI AVER SUBITO UN INCIDENTE CYBER?

- Come viene a conoscenza l'azienda di un incidente di cybersecurity? Nella maggior parte dei casi, il processo è quello che ci si aspetta (se ne accorge il dipartimento IT – 50%-, arriva un alert dai sistemi di sicurezza – 44%- o dal SOC/SIEM – 42%), non mancano però altre situazioni che possono essere invece fonte di maggiori problemi per chi gestisce i rischi cyber.
- Ad esempio, un **25% di aziende afferma di aver individuato un incidente a partire da un malfunzionamento**: sempre un **25% ha ricevuto l'alert da un utente o da una funzione del business.**
- In pochi casi, per fortuna, la scoperta è stata fatta da altri (clienti, partner, fornitori di cybersecurity o media).

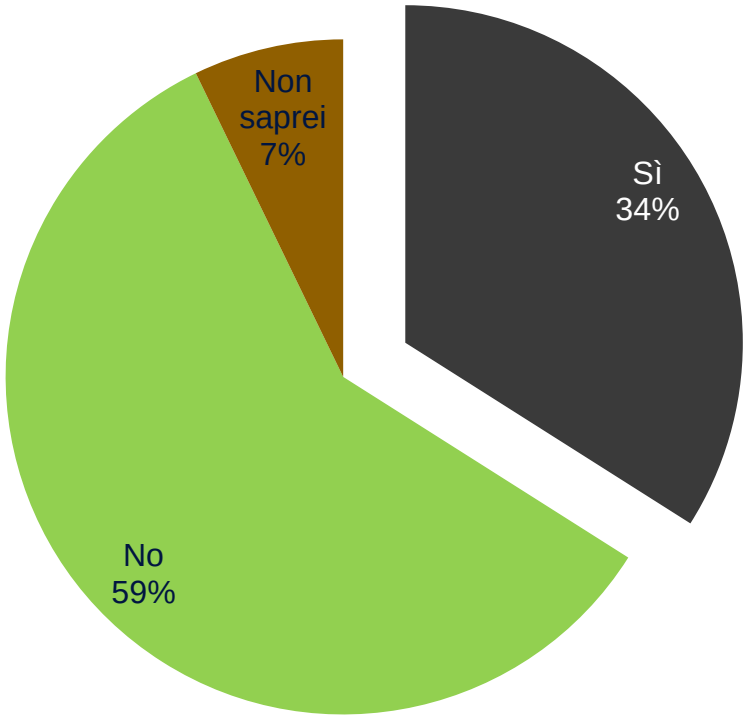
Domanda. Con riferimento agli incidenti subiti nel 2023, come ve ne siete accorti?



FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

UNA QUOTA SIGNIFICATIVA DI AZIENDE (IL 34%) AFFERMA DI AVER SUBITO UN ATTACCO RANSOMWARE: NEL CASO DI AZIENDE DI GRANDE DIMENSIONE, QUESTA QUOTA SALE AL 38%

Domanda. La Sua azienda ha sofferto in passato di un attacco ransomware?



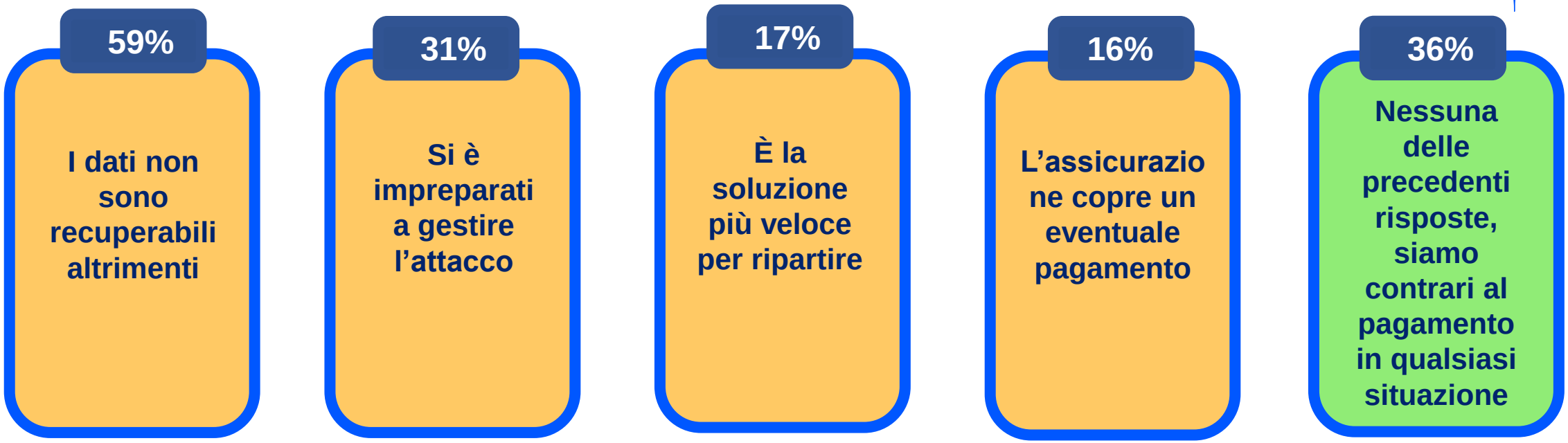
Small	30%
Medium	30%
Large	38%

FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

IL 59% DELLE AZIENDE DICHIARA CHE È DISPOSTA A PAGARE IL RISCATTO SE NON È POSSIBILE RECUPERARE I DATI IN ALTRO MODO

Small	30%
Medium	31%
Large	42%

Domanda. Quali delle seguenti considerazioni possono spingere a PAGARE il riscatto agli attaccanti?



FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

I TREND DEL CYBER RISK MANAGEMENT NEL 2024

CYBER INSURANCE, QUANTO E' DIFFUSA?

Un punto importante di una strategia di gestione dei rischi cyber è la presenza di una copertura assicurativa cyber: l'adozione di questa può infatti influenzare gli approcci e portare all'adozione di best practices di cybersecurity (come richiedono gli stessi assicuratori). Ad oggi, il **54% delle aziende afferma di avere una copertura assicurativa**. Il 30% si è occupato internamente della sottoscrizione della stessa, un ulteriore 24% lo ha fatto con il supporto di specialisti esterni. Un 12% di aziende la richiede anche, come clausola di sicurezza, nei contratti con i fornitori.

COMPLIANCE EUROPEA ALLE PORTE.

Manca poco tempo all'entrata in vigore di molte nuove norme europee. L'arrivo del regolamento europeo DORA (Digital Operational Resilience Act), la cui applicazione è prevista entro il 17 gennaio 2025, e della direttiva NIS2, entro il 17 ottobre 2024, introducono importanti responsabilità per il Board delle aziende: se un'impresa non rispetterà la NIS2, ad esempio, potrà subire una sospensione delle autorizzazioni, delle concessioni, il CEO potrà essere sospeso dal suo ruolo. E con la NIS2, i settori impattati che rientrano nel perimetro cibernetico saranno molti di più, comprenderanno l'industria, l'agroalimentare, il chimico e il farmaceutico, che in Italia pesano molto. Le aziende si stanno preparando? Il percorso verso la conformità alle nuove norme europee è in divenire: **solo un 7% delle aziende è già conforme, il 37% sta iniziando a muovere i primi passi**. Quasi un quarto delle aziende non sa quali azioni intraprendere per essere conformi.

FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

IL PERCORSO VERSO LA CONFORMITÀ ALLE NUOVE NORME UE È IN DIVENIRE: UN 7% DELLE AZIENDE AFFERMA DI ESSERE CONFORME

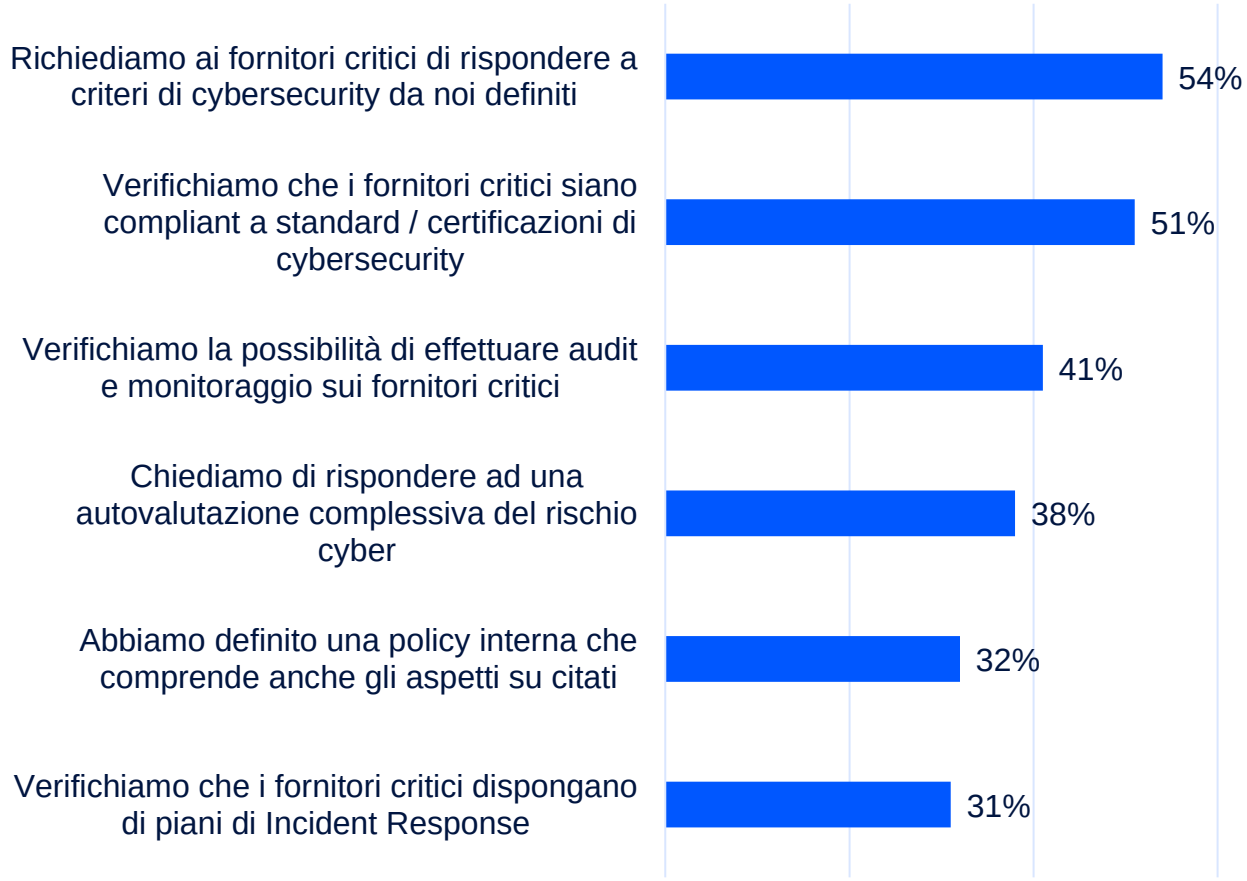
Domanda. Da fine 2024 entreranno in vigore le nuove norme europee (DORA, NIS2) che richiedono più elevati livelli di cyber resilienza, come il controllo della sicurezza dei fornitori e una migliore gestione degli incidenti informatici. Qual è la situazion

FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

METTERE IN SICUREZZA LA SUPPLY CHAIN

- Le aziende in genere rivolgono molte azioni e misure di cybersecurity al proprio interno, ma trascurano i fornitore/le terze parti, a cui spesso sono strettamente collegati in catene del valore digitali. Dall'indagine risulta che solo un'azienda su 2 (il 54%) ha all'interno del proprio programma di cyber risk management, attività specifiche per controllare la sicurezza della supply chain.
- Ad oggi, la maggior parte degli sforzi vanno da un lato nei controlli preliminari sulla sicurezza dei fornitori (verifiche, ad esempio, su certificazioni e misure di sicurezza presenti presso il fornitore), e nelle clausole contrattuali (in cui spesso viene richiesta l'adozione di misure e processi standard di sicurezza). **Con riferimento alle attività preliminari, l'80% delle aziende ha qualche procedura in atto, mentre nel 73% delle aziende la sicurezza entra nei contratti,** soprattutto l'adozione di standard e le attività periodiche VM/VA/PT.

Domanda. Con riferimento alla sicurezza delle terze parti quali sono in generale le attività e le verifiche preliminari nella selezione dei fornitori svolte dalla vostra azienda?



FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

PER LA CYBER RESILIENZA ORGANIZZATIVA SERVE UNO SFORZO COMUNE E COORDINATO

- **Solo un 44% delle aziende si è posto il tema di collaborare attivamente con tutte le aree di business potenzialmente coinvolte**, in modo da aumentare il controllo.
- Per i responsabili della cybersecurity, la cyber resilienza si ottiene oggi con la **formazione (81% degli intervistati),** la **tempestività della risposta (73%), test e simulazioni (63%)** per verificare il livello di preparazione, **visibilità estesa (55%) e threat intelligence (53%).** Sono queste secondo i più le parole chiave di una efficace strategia per incrementare la cyber resilienza.

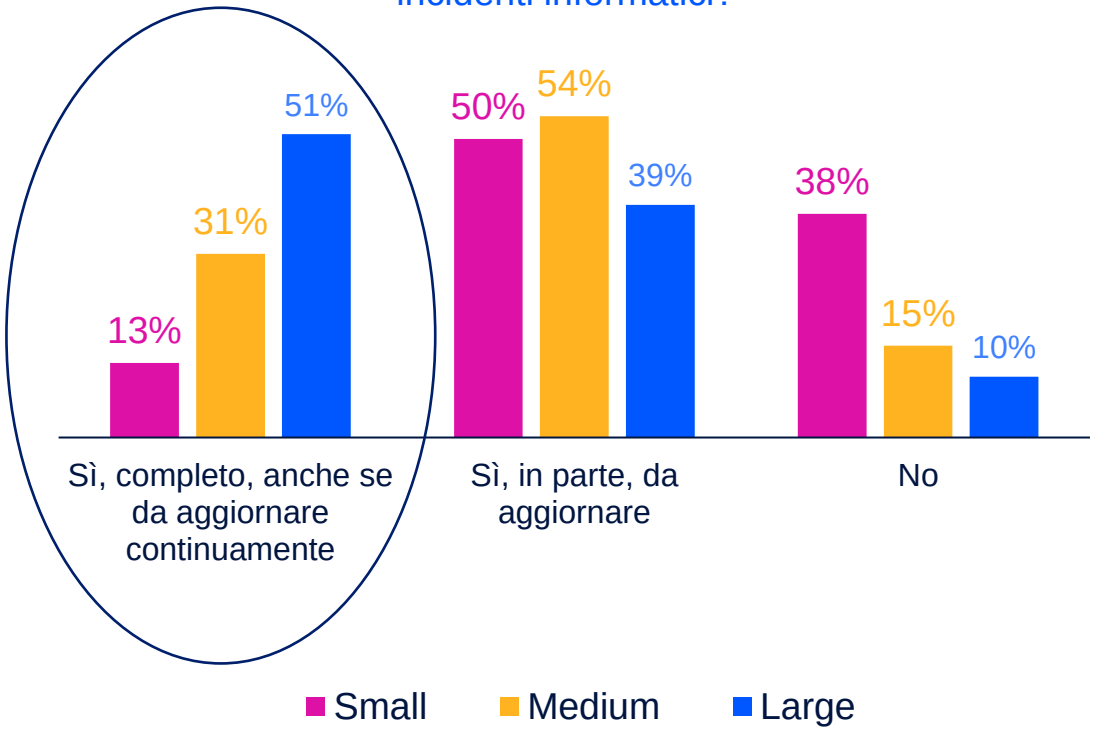
Domanda. Quali delle seguenti attività ritenete più efficaci per incrementare la Cyber Resilienza della vostra organizzazione?

FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

I TREND DEL CYBER RISK MANAGEMENT NEL 2024

- PER LA CYBER RESILIENZA SERVE LA PREPARAZIONE, UN PIANO COMPLETO PER IL RILEVAMENTO E LA RISPOSTA.
- Il piano per il rilevamento e la risposta è una condizione importante per la cyber resilienza, ma oggi è poco presente nelle aziende di minore dimensione (nello small business, è presente nel 63% delle aziende, ma per la maggior parte dei casi, non è completo).

Domanda. Avete un piano di rilevamento e risposta per incidenti informatici?

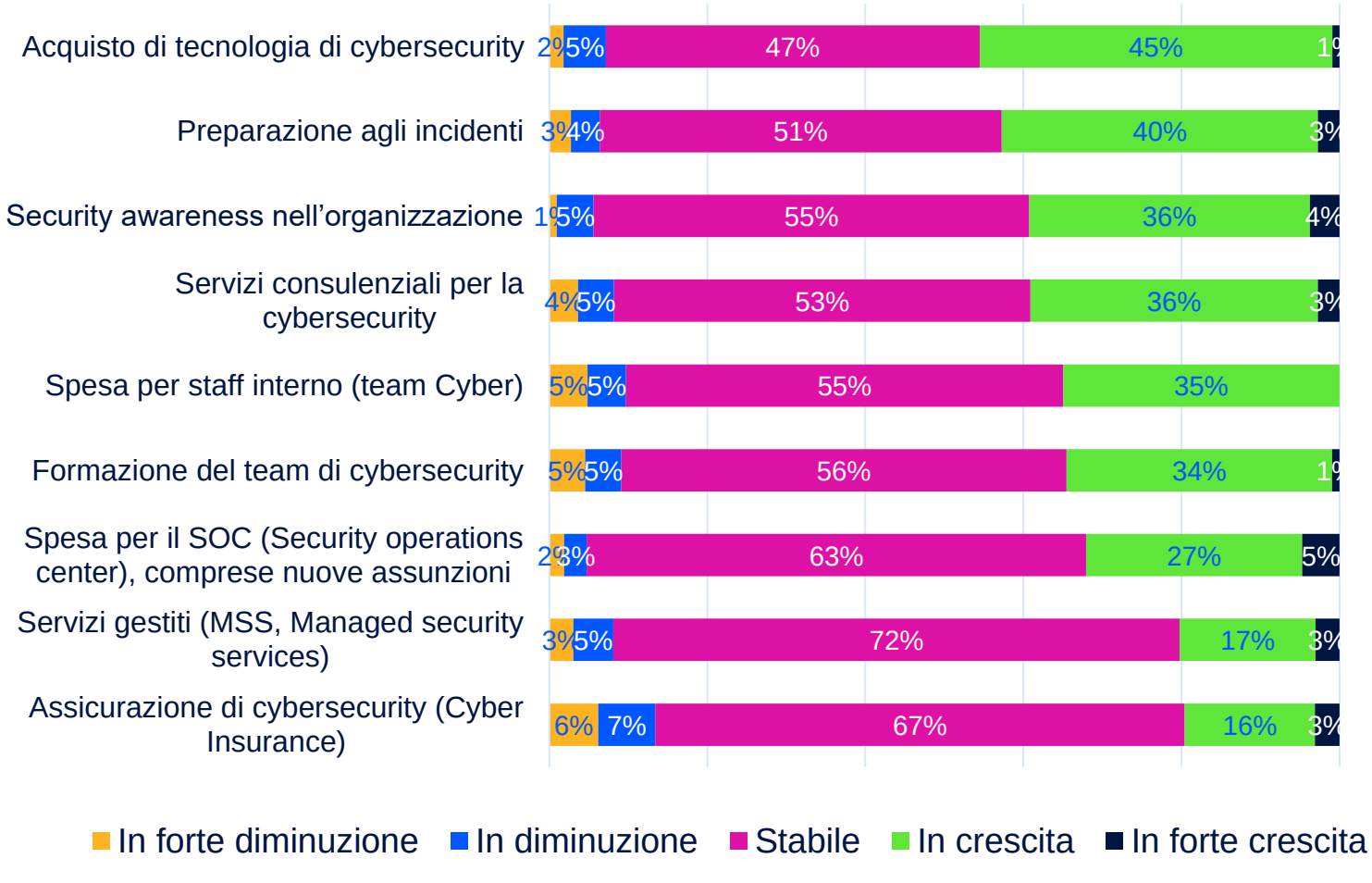


FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

GLI INVESTIMENTI IN SOLUZIONI E SERVIZI PER LA CYBERSECURITY SONO IN CONTINUA CRESCITA

- Secondo la rilevazione di quest'anno, la spesa media è stata nel 2023 pari **all'8,3% rispetto al budget ICT**, in previsione dovrebbe diventare il 9% entro il 2024. Si registra quindi una crescita, visto che il valore medio della spesa per la cybersecurity era un 7,2% nel 2023.
- Al primo posto vanno gli acquisti in soluzioni tecnologiche; la spesa per la preparazione agli incidenti; acquisti legati a formazione e consulenza di cybersecurity; la spesa per lo staff interno e per il SOC (Security Operation Center).
- Le soluzioni per la cybersecurity che registrano tassi di crescita a due cifre sono quelle che caratterizzando una **postura di cybersecurity più avanzata, automatizzata, in linea con i nuovi paradigmi IT (cloud, big data, AI, IoT).**

Domanda. Gli investimenti di cybersecurity cresceranno o diminuiranno nel 2024?

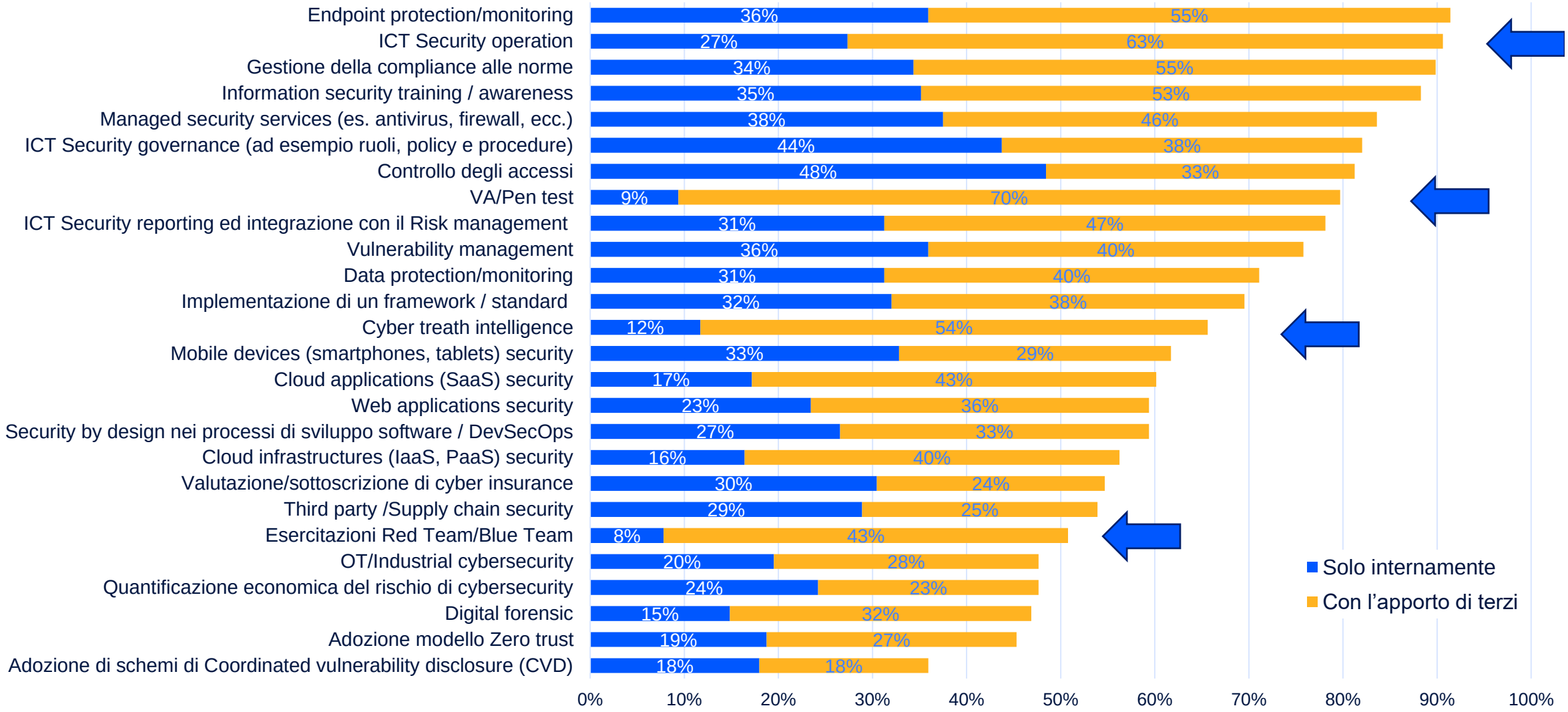


FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

In generale, prevale il ricorso a terzi per più aspetti del piano di cyber risk management: alcuni ambiti sono completamente esternalizzati in molte realtà

THE INNOVATION GROUP

Domanda. Quali sono le attività che avete svolto nel 2023 con riferimento alla sicurezza informatica?



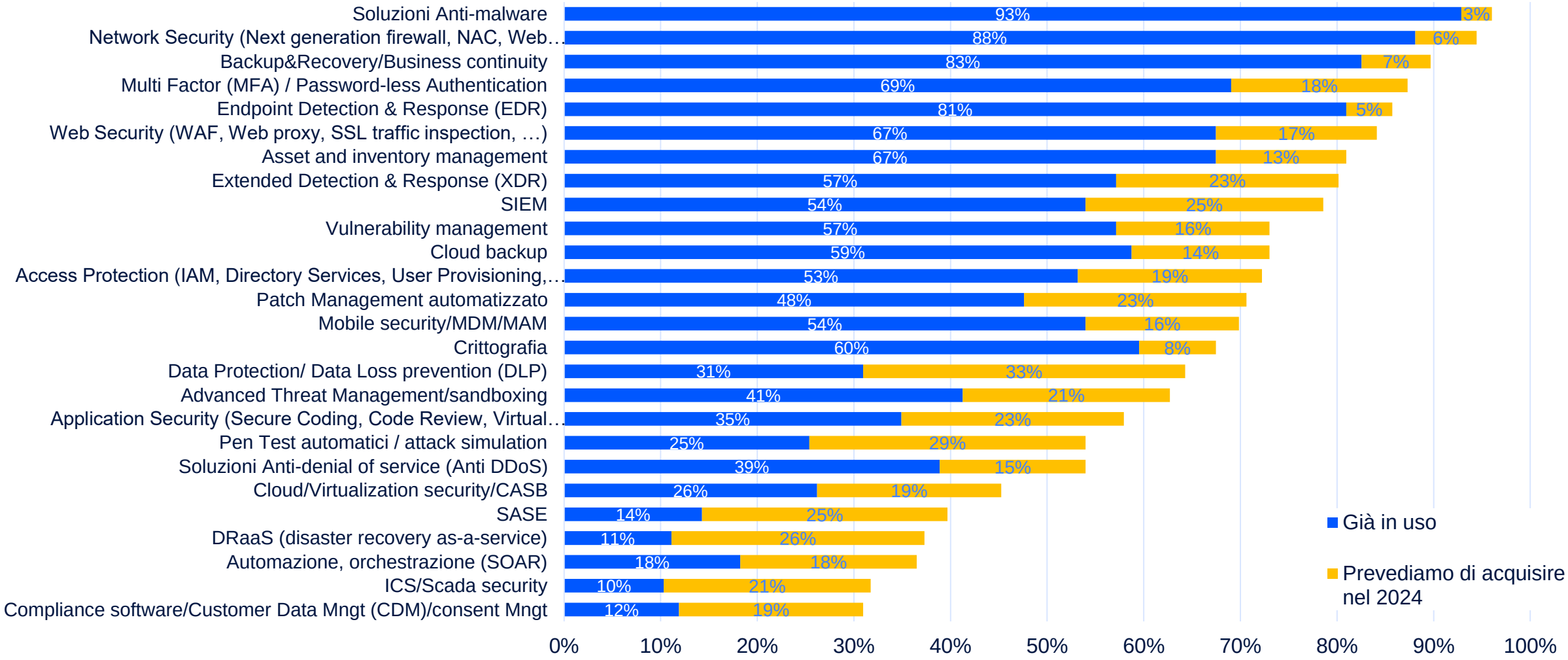
FONTE: CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024. IN MEDIA, 17 ATTIVITA' SVOLTE

CSA Cyber Security Angels

TIG EVENTS

L'adozione di tecnologie di cybersecurity è molto ampia (in media, 17 soluzioni adottate) con margini di crescita elevati per alcune

Domanda. Quali tecnologie/soluzioni di cybersecurity utilizzate già/ andrete a dotarvi nel 2024?



FONTE: CYBER RISK MANAGEMENT SURVEY, GENNAIO 2024. IN MEDIA, 17 SOLUZIONI TECNOLOGICHE ADOTTATE

TIG | THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

The Innovation Group

Fondata nel 2009, The Innovation Group (TIG) è una società di servizi di consulenza e di ricerca di mercato indipendente, specializzata nello studio delle evoluzioni del mercato digitale e nei processi d'innovazione abilitati dalle tecnologie e dalla conoscenza.
TIG si rivolge ad aziende e organizzazioni dell'economia digitale che desiderano sviluppare strategie di crescita attraverso programmi e iniziative di go-to-market.
Vengono pertanto sviluppate analisi, ricerche, approfondimenti sul digitale per il mercato italiano. Per fare questo, si mettono a disposizione piattaforme integrate di servizi e contenuti per facilitare scambi e relazioni con clienti, influencer, stakeholder ed ecosistemi.

www.tig.it
info@tig.it
+39 02.49988.1

Viale Palermo, 5
20121, Milano

Viale Cassala, 36
20143, Milano

FACTORY EVENTS MEDIA

CSA Cyber Security @ngels

CSA - Cyber Security Angels

CSA - Cyber Security Angels - è un gruppo di persone d'Azienda solitamente ICT & Security Manager, costituito per creare una rete di conoscenze dirette al fine di far fronte comune alle problematiche nascenti sul fronte della Cyber Security.
Un incidente cyber o un problema di governance non deve essere causa di frustrazione, ma un'occasione per potersi confrontare tra colleghi competenti, non solo per trovare una soluzione, ma anche per allertare e aiutare altri colleghi a fare prevenzione.
L'approccio migliore per affrontare questi problemi è lavorare in squadra sul campo affidandosi non solo ai report di un fornitore o a soluzioni proposte da un vendor.

Obiettivi della community fra le sole aziende è la Security by Sharing che vuol dire:

- Aumentare la resilienza scambiando le informazioni su nuovi tipi di attacco.
- Avere dei suggerimenti su come proteggersi meglio svincolato da logiche di prodotto.
- Possibilità di scambiarsi informazioni sugli incidenti, sulla qualità dei prodotti, degli integratori e dei servizi.
- Neutralità al di fuori del network dei Vendor, Integratori e Consulenti con la garanzia della discrezione, anonimato e riservatezza.
- Chi crede che la cybersecurity italiana non sia un tabù ha la possibilità di conoscere in modo anonimo nuove startup nel bacino nazionale che propongono soluzioni e servizi innovativi.
- C'è la possibilità di verificare le referenze e i livelli di servizio per arrivare fino ad una piattaforma di ranking di chi si occupa di Cybersecurity.
- Canale di comunicazione condiviso su base etica per chiedere suggerimenti sui problemi e su come risolverli.

CYBER SECURITY ANGELS
moderatore@cybersecurityangels.it
https://cybersecurityangels.it