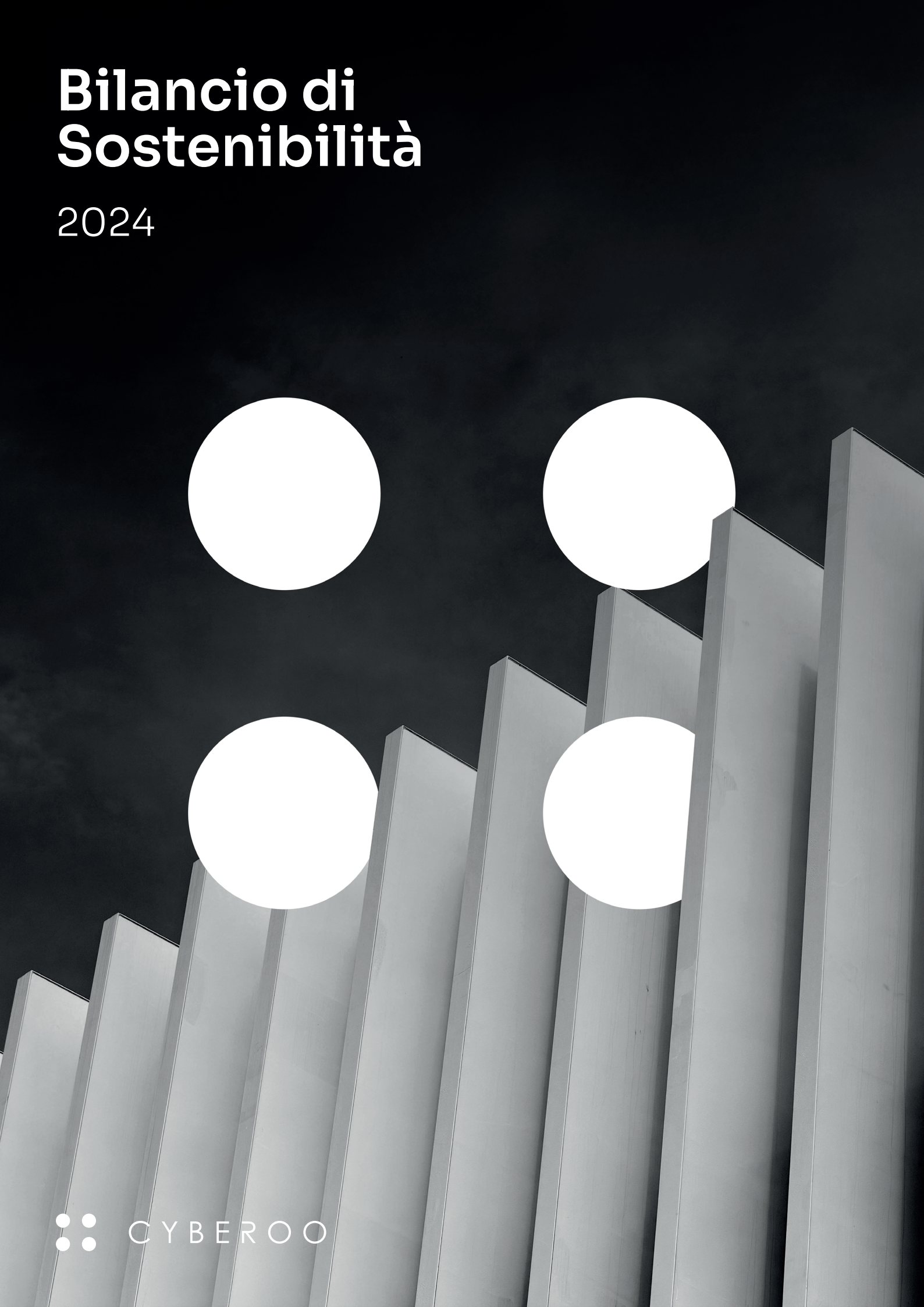
Bilancio di Sostenibilità

2024



CYBEROO

La cybersecurity europea in Europa

Siamo una società italiana specializzata nella difesa della cybersecurity. Vigiliamo sulla sicurezza dei tuoi dati, per lasciarti la libertà di focalizzarti sul tuo business.

CYBEROO

Indice

LETTERA AGLI STAKEHOLDER

“IL 2024 È STATO UN ANNO DI CONSOLIDAMENTO E DI NUOVE CONQUISTE: CON LA PUBBLICAZIONE DEL NOSTRO TERZO BILANCIO DI SOSTENIBILITÀ, CONTINUIAMO A PERSEGUIRE GLI OBIETTIVI DI ECCELLENZA E INNOVAZIONE CHE CI HANNO SEMPRE CONTRADDISTINTO.”

Fabio Leonardi
CEO

Lettera agli stakeholder

Il 2024 per il Gruppo Cyberoo è stato un anno di consolidamento e di nuove conquiste: con la pubblicazione del nostro terzo Bilancio di Sostenibilità, continuiamo a perseguire gli obiettivi di eccellenza e innovazione che ci hanno sempre contraddistinto, affrontando con determinazione le sfide del presente e del futuro. L'esercizio appena concluso è stato ancora caratterizzato dalle conseguenze delle turbolenze geopolitiche internazionali sulle economie mondiali. Tuttavia, il Gruppo Cyberoo, che opera principalmente nel mercato della Cybersecurity, ha saputo reagire nel corso del 2024 arrivando a chiudere l'esercizio con un utile di gruppo di euro 4.376.867.

Siamo molto soddisfatti delle performance ottenute, ma questo aumenta ancora di più la responsabilità che abbiamo verso le persone che lavorano nella nostra organizzazione e verso le comunità e il territorio in cui operiamo.

Siamo consapevoli che la nostra crescita debba essere anche sostenibile e non possa prescindere dall'adottare soluzioni che siano in grado di portare benessere alla società in cui viviamo.

Tutto questo è possibile grazie all'innovazione, da sempre il cuore pulsante attorno al quale ruotano idee, progetti, servizi, design e processi di sviluppo. È in virtù di questa consapevolezza che abbiamo rafforzato i nostri investimenti in ricerca e sviluppo, sviluppando nuovi progetti di cybersecurity che ci hanno consentito di proporre ai nostri clienti soluzioni tecnologiche sicure ed affidabili. Tutto questo conferma la nostra attenzione al cliente e ribadisce la qualità e la sicurezza che contraddistinguono da sempre i nostri prodotti.

La redazione del Bilancio di sostenibilità di Cyberoo è parte di questo percorso e costituisce non solo un'importante opportunità per la rappresentazione dei risultati economici, sociali ed ambientali, ma anche per evidenziare le linee strategiche di medio-lungo periodo e la loro coerenza con uno sviluppo sostenibile.

Il modello di business sostenibile e la creazione e condivisione di valore per gli Stakeholder è da sempre parte del nostro DNA e ci guida nella gestione quotidiana dell'impresa. Crediamo che uno sviluppo realmente sostenibile sia basato sul

benessere delle persone e sull'attenzione all'ambiente, mettendo in condivisione risorse, competenze e sperimentando soluzioni innovative.

Un modello di business sostenibile richiede, infatti, lo sviluppo coerente del tessuto sociale e degli ecosistemi che ci ospitano. Crediamo in una cultura d'impresa che connette e condivide idee e soluzioni attraverso un complesso intreccio di attori e partner che collaborano per la creazione di valore condiviso nel lungo periodo. Abbiamo creato molti prodotti innovativi in questi anni ma le sfide e il miglioramento continuo sono l'essenza del nostro sviluppo. Tutto questo rappresenta il nostro punto di partenza per continuare un percorso nella sostenibilità per la crescita dell'azienda, del territorio e del mondo che ci circonda.

Fabio Leonardi
CEO

Nota Metodologica

Il presente documento rappresenta il terzo Bilancio di sostenibilità del Gruppo Cyberoo (d'ora in poi anche "il Gruppo" o "Cyberoo"). Il documento contiene le informazioni relative ai temi economici, ambientali e sociali, utili ad assicurare la comprensione delle attività svolte da Cyberoo del suo andamento, dei suoi risultati e dell'impatto prodotto dalle stesse.
Il Bilancio di sostenibilità è stato redatto rendicontando una selezione dei "GRI Sustainability Reporting Standards" pubblicati dal Global Reporting Initiative (GRI 2021), come indicato nel GRI Content Index del presente documento, secondo l'opzione di rendicontazione "With reference".
La redazione del presente documento è, al momento, un esercizio di natura volontaria per il Gruppo.
I principi generali applicati per la redazione della Bilancio di sostenibilità sono quelli stabiliti dai GRI Standard: rilevanza, inclusività, contesto di sostenibilità, completezza, equilibrio tra aspetti positivi e negativi, comparabilità, accuratezza, tempestività, affidabilità, chiarezza.

Gli indicatori di performance selezionati sono quelli previsti dagli standard di rendicontazione adottati, rappresentativi degli specifici ambiti di sostenibilità analizzati e coerenti con l'attività svolta da Cyberoo e gli impatti da essa prodotti. La selezione di tali indicatori è stata effettuata sulla base di un'analisi di rilevanza degli stessi, come descritto nel paragrafo "***Analisi di materialità***". Nelle diverse sezioni del Bilancio di sostenibilità, sono segnalate le informazioni quantitative per le quali è stato fatto ricorso a stime.

Il perimetro di rendicontazione dei dati e delle informazioni qualitative e quantitative si riferisce alle performance di Cyberoo S.p.A., Cyberoo51 S.r.l., MFD International S.r.l., Cyberoo Docetz S.r.l. e di Cyberoo PL Sp z.o.o (società di diritto polacco) al 31 dicembre 2024. Eventuali limitazioni di perimetro sono opportunamente segnalate nel testo.

Il Bilancio di sostenibilità è redatto con cadenza annuale. Al fine di permettere il confronto dei dati nel tempo e la valutazione dell'andamento delle attività di Cyberoo sono presentati, a fini comparativi, i dati relativi ai due esercizi precedenti.

Il processo di redazione dell'informativa di sostenibilità ha visto il coinvolgimento dei responsabili delle diverse funzioni del Gruppo.

Il Bilancio di sostenibilità è stato approvato dal Consiglio di Amministrazione di Cyberoo S.p.A. in data 30/06/2025 e non è stato assoggettato a revisione da parte di un revisore indipendente.

Il Bilancio di sostenibilità è pubblicato nel sito istituzionale della Società al seguente indirizzo: www.cyberoo.com.

Per richiedere maggiori informazioni in merito è possibile rivolgersi all'indirizzo: sustainability@cyberoo.com.

Capitolo 1

IDENTITÀ E STRATEGIA

1. Identità e strategia

Il Gruppo Cyberoo opera nel mercato dei servizi e dei prodotti ICT (Information & Communication Technology), ed è specializzato nel fornire alla propria clientela una vasta gamma di servizi e soluzioni tecnologiche a supporto del business delle imprese con focus sulla cybersecurity.

L'attività si rivolge al mercato delle medie imprese con un portfolio di soluzioni enterprise ampio e variegato, sviluppate con l'utilizzo delle più avanzate tecnologie e con una catena del valore unica, sia tra i player nazionali che internazionali.

Il Gruppo, supporta le imprese nella sicurezza, nonché nel miglioramento e nella digitalizzazione dei propri processi organizzativi e di business, al fine di offrire soluzioni e servizi personalizzati ad alto contenuto tecnologico, combinando l'apprendimento artificiale con l'intelligenza umana dei migliori professionisti sul mercato per garantire sicurezza, continuità e resilienza agli investimenti delle imprese clienti.

Il Gruppo realizza una strategia volta alla protezione e al monitoraggio, oltre che alla gestione, del valore delle informazioni di ogni ecosistema IT, con lo scopo di semplificare la complessità aziendale.

I servizi offerti del Gruppo sono declinati in tre linee di business principali: cyber security services, managed services e digital transformation.

Le dimensioni

Il Gruppo Cyberoo ha realizzato ricavi per euro 22 milioni e conta, nelle proprie sedi, di un numero complessivo di 105 dipendenti (al 31 dicembre 2024).

Ricavi per Industry (milioni di euro)	2022		2023		2024	
	Ricavi	%	Ricavi	%	Ricavi	%
Cyberoo S.p.A.	13,98	81,8%	18,17	80,0%	20,98	80,33%
Cyberoo51 S.r.l.	2,11	12,3%	2,64	11,6%	2,94	11,26%
MFD International S.r.l.	0,76	4,4%	0,90	4,0%	0,99	3,79%
Cyberoo Docetz S.r.l.	0,24	1,4%	0,99	4,4%	1,21	4,63%
Cyberoo PL SP. ZO.O.	-	-	-	-	-	-
Totale*	**17,10**	**100%**	**22,70**	**100%**	**26,12**	**100%**

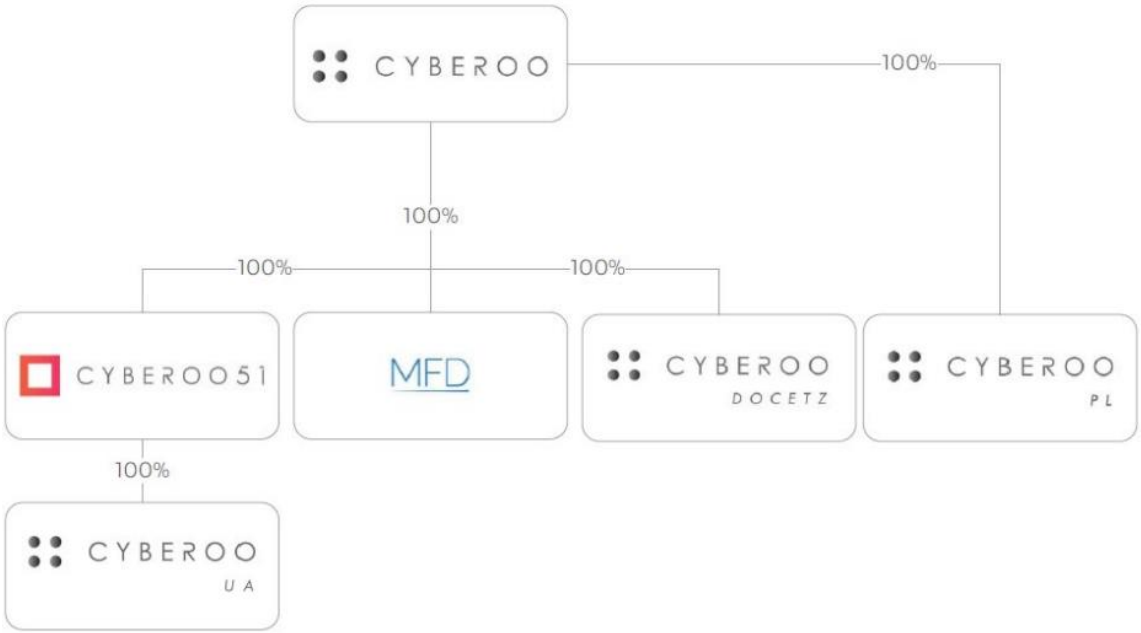
*Importo al lordo delle fatture Intercompany

Ricavi per tipologia di servizio (milioni di euro)	2022		2023		2024	
	Ricavi	%	Ricavi	%	Ricavi	%
Cyber Security & Device Security	11,01	70,8%	15,48	77,4%	17,97	78,7%
Managed Services	4,36	28,0%	4,37	21,8%	4,70	20,6%
Digital Transformation	0,17	1,15%	0,16	0,8%	0,16	0,7%
Totale	**15,5**	**100%**	**20,01**	**100%**	**22,83**	**100%**

Il Gruppo

Il Gruppo, con headquarter a Reggio Emilia e sedi operative in Italia e all'estero, opera nel settore dell'Information Technology è costituito da 6 entità legali.

La struttura del Gruppo al 31 dicembre 2024 è di seguito rappresentata:



Cyberoo S.p.A. detiene una partecipazione pari al 100% del capitale sociale di Cyberoo51 S.r.l. (CYBEROO51), di MFD International S.r.l. (MFD), di Cyberoo Docetz S.r.l. e di Cyberoo PL Sp z.o.o (società di diritto polacco).

Occorre precisare che Cyberoo51 S.r.l. detiene l'intero capitale della società Cyberoo UA LLC (società di diritto ucraino).

Cyberoo51 S.r.l.

CYBEROO51, costituita nel 2014, svolge attività di consulenza nel settore delle tecnologie informatiche offrendo soluzioni software personalizzate e di cloud computing, nonché pianificando la corretta strategia di marketing e l'assistenza nelle scelte di comunicazione delle aziende.

In particolare, CYBEROO51 offre i seguenti servizi: servizi consulenziali e software personalizzati, servizi di digital marketing, software As a Service. CYBEROO51 detiene una partecipazione pari al 100% del capitale sociale di Cyberoo UA, società con sede in Ucraina, a Ternopil, che svolge, per le società appartenenti al Gruppo, servizi in settori quali: *cyber security management, networking management, service desk; backup management, antivirus, antispam, cloud Service, IT consulting*.

MFD International S.r.l.

MFD, costituita nel 2017, svolge servizi di telemarketing e gestione di call center inbound e outbound principalmente rivolti a società facenti parte del Gruppo.

Cyberoo Docetz S.r.l.

Cyberoo Docetz S.r.l. (ex Cyber Division), acquisita per il 100% nel gennaio del 2023 è attiva nel campo della cyber security e, nello specifico, nei segmenti Offensive Security e Incidente Response.

Cyberoo PL z.o.o

Cyberoo PL z.o.o rappresenta il polo polacco per le attività commerciali effettuate nel territorio, parallelamente, essa gestisce il 2° livello dell'i-SOC Cyberoo insieme alle molteplici figure dei cybersecurity specialists.

Storia, evoluzione e crescita

La storia Cyberoo ha inizio nel **2008** con la nascita di **AT Store**, società specializzata nella vendita di device. Nell'agosto dello stesso anno **Sedoc Digital Group**, storica azienda informatica emiliana nata nel 1973, acquisisce il 51% delle quote di AT, ultimandone l'acquisizione nell'aprile 2010. Nel dicembre 2011, AT Store acquisisce un ramo aziendale da Sedoc Digital Group e inizia l'attività di *Printing Management*, nuovo servizio per la gestione e monitoraggio delle stampanti in partnership con HP.

Nel 2015 AT Store diventa un ***Managed Service Provider (MSP)***, ossia un'azienda che fornisce servizi informatici di gestione e monitoraggio, anche a distanza.

Nel 2016 viene aperto il primo Hub in Ucraina per ampliare il focus sui *Managed Security Services*.

Il 2017 è l'anno di svolta. La stampante multifunzione diventa uno strumento per attaccare i dispositivi collegati alla rete locale ed eseguirvi codice malevolo. Dopo l'attacco hacker «Faxploit», la società cambia modello di business e diventa un ***Managed Security Service Solution (MSSP)*** e successivamente di Cyber Security ampliando l'offerta alla gestione, monitoraggio e protezione di tutta l'infrastruttura IT dei clienti, specializzandosi così nella fornitura di servizi di sicurezza informatica.

Nel 2018 è nato CYBEROO Lab: un network di HUB tecnologici proprietari con l'ambizione di creare soluzioni intelligenti e competitive nel mercato internazionale, a supporto della sicurezza e continuità operativa.

Nel 2019 l'azienda cambia nome in **Cyberoo**, lancia sul mercato 3 soluzioni innovative: Cypeer e Cyber Security Intelligence (CSI), che compongono la Cyber Security Suite, e la Titaan Suite, che a sua volta è costituita da tre moduli (Titaan Atlaas, Titaan Croono e Titaan Hyperioon). Il 7 ottobre 2019 Cyberoo viene quotata su Euronext Growth Milan (ex AIM Italia), il mercato di Borsa Italiana riservato alle PMI, risultando la **prima società di cyber security quotata a Piazza Affari**.

A dicembre 2019 Cyberoo ha siglato un accordo con l'Università di Ternopil "Ivan Puluj National Technical University" in Ucraina, volto alla ricerca e sviluppo e alla selezione dei migliori talenti in ambito di cyber security. Cyberoo ha concordato con l'Università un percorso formativo innovativo, con un forte investimento sulle risorse umane coinvolte. Conformemente ai programmi e agli argomenti condivisi

con l'Università, Cyberoo si è resa disponibile allo svolgimento di tirocini e concorsi per borse di studio, con l'obiettivo di selezionare le migliori risorse e garantirsi la progressiva crescita delle competenze specializzate in ambito di cyber security.

Ad aprile 2021 Cyberoo ha avviato anche una collaborazione che la vede partecipare, come membro del Comitato di Indirizzo, al corso di Laurea in "Innovazione e Imprenditorialità Digitale" presso la Facoltà di Economia e Giurisprudenza dell'Università Cattolica del Sacro Cuore, campus di Cremona. Cyberoo punta così a definire insieme all'Università Cattolica nuove linee di ricerca volte al trasferimento tecnologico nell'ambito della sicurezza informatica, attraverso un processo di sensibilizzazione dei giovani e contribuendo alla formazione di risorse altamente specializzate in ambito IT.

In data 27 luglio 2021, Cyberoo finalizza l'acquisizione del 51% di Cyber Division S.r.l., azienda novarese a elevata focalizzazione nelle attività di Vulnerability Assessment, Penetration Test ed Ethical Hacking oltre a quelle di Incident Response.

Il 25 ottobre 2021 Cyberoo viene nominata "Representative Vendor" nella "2021 Gartner Market Guide For MDR Services", la più importante e autorevole ricerca internazionale sui servizi gestiti di sicurezza informatica. Prima e unica azienda italiana a ottenere l'ambito riconoscimento.

Nell'estate 2022 Cyberoo ha annunciato al mercato e ai propri partner il nuovo MDR (Managed Detection & Response) che integra funzioni di Automatic Remediation potenziate e all'avanguardia, avviando così un nuovo corso per la cyber sicurezza aziendale. Un importante investimento per un valore di circa 1,5 milioni di euro.

Cypeer Pure e Cypeer Sonic sono le due configurazioni del nuovo MDR che funziona con ampio ricorso all'intelligenza artificiale e al machine learning, e che segna un ulteriore importante cambio di passo per le attività di Response e Automatic Remediation.

A luglio 2022 Cyberoo riprende il percorso di internazionalizzazione e porta le proprie soluzioni sul mercato tedesco. Lo sbarco in Germania è stato reso possibile grazie al partner distributore ICOS.

A settembre 2022 Cyberoo si riconferma tra i principali player internazionali nel segmento dei servizi di Managed Detection and Response (MDR). Gartner, infatti, ha citato Cyberoo tra le circa 50 principali aziende mondiali specializzate in questo specifico segmento.

Per Gartner quello degli MDR è uno dei settori più dinamici del mercato della cybersecurity. Cresciuti del 48,9% dal 2020 al 2021, i servizi di Managed Detection and Response dovrebbero raggiungere la loro massima diffusione entro i prossimi cinque anni.
Il 17 gennaio 2023 Cyberoo ha avviato Cyberoo Docetz S.r.l. con l'obiettivo di accelerare la crescita strutturale dell'organizzazione e rispondere in modo efficace alle attività in ambito di cyber security e consulenza aziendale.

A febbraio dello stesso anno, il Gruppo viene riconosciuto per la seconda volta come "Representative Vendor" nella prestigiosa "Market Guide For MDR Services 2023" di Gartner.

Il 22 maggio 2023 Cyberoo ha approvato il suo primo Bilancio di Sostenibilità. Il documento, riferito all'esercizio 2022, è stato redatto su base volontaria rendicontando una selezione degli standard internazionali "GRI Sustainability Reporting Standards - 2021", secondo l'opzione di rendicontazione "Referenced". Con questa pubblicazione Cyberoo fa un ulteriore importante passo nel percorso intrapreso di Corporate Social Responsibility.

Il 23 maggio 2023, viene inaugurata in Polonia la nuova sede. Si tratta di un importante i-SOC (intelligence Security Operation Center), nel quale vengono rafforzate le attività i-SOC di secondo livello, con un ampio gruppo di cyber specialist attivi a supporto della struttura operativa di Gruppo H24. Il nuovo modello scalabile garantisce un ulteriore miglioramento del servizio offerto ai clienti e consente a Cyberoo di supportare al meglio la costante crescita della clientela che si affida sempre più ai servizi MDR (Managed Detection and Response) offerti Cyberoo.

Il 29 giugno 2023 Cyberoo comunica di essere entrata a far parte del circuito CERT (Computer Emergency Response Team) del Trusted Introducer, principale riferimento del settore a livello internazionale. L'ingresso nella rete dei CERT riconosciuti da Trusted Introducer è avvenuto al termine di un rigoroso percorso,

durante il quale Cyberoo ha raggiunto gli obiettivi del framework di riferimento "SIM3 (Security Incident Management Maturity Model)" dedicato alle Listed Organization". In qualità di CERT, per Cyberoo si aprono anche nuove importanti opportunità sia con riferimento all'ampliamento della visibilità verso aziende che necessitano di consulenza e supporto in ambito di sicurezza informatica, ma soprattutto alla collaborazione con altri player internazionali per lo scambio di informazioni utili alla definizione delle best practices volte al contrasto dei nuovi cyberthreat per la sicurezza nazionale e internazionale. L'accreditamento ottenuto è subordinato al rispetto di specifici requisiti come l'operatività h24 del proprio SOC (Security Operations Center) e la necessità di aver maturato un'esperienza dimostrabile nella gestione degli incidenti e nella postura di sicurezza dell'infrastruttura.

Il 27 febbraio 2024 si è tenuta a Reggio Emilia la "Partner Conference: Poland Edition" che ha sancito l'inizio di un anno importante anche sul fronte delle relazioni nazionali ed estere con la rete partner di Cyberoo. L'evento ha rappresentato un primo fondamentale incontro tra i team tecnici e commerciali italiani e i referenti dei tre partner polacchi. La partner conference con stampo polacco apre le porte a una serie di eventi ufficiali per il 2024, che vedranno Cyberoo impegnata nella solidificazione dei rapporti con partner, clienti ed investitori.

Il 23 maggio 2024, durante il "Black Club - Partner Conference 2024" (il tradizionale appuntamento che riunisce la rete dei partner aziendali) sono state presentate diverse novità, tra cui Cypeer KEERA, il nuovo servizio integrato in Cypeer che offre un livello aggiuntivo di remediation, e Cypeer POT, una funzione avanzata di reception per rafforzare la sicurezza informatica. È stato inoltre annunciato Cypeer AgentX, un'evoluzione tecnologica per il monitoraggio più dettagliato degli endpoint, e BlackBOX, il primo hardware di Cyberoo che integra i sistemi Cypeer Manager, Cypeer Continuous Scanning e Cypeer Probe. Tra le novità anche VIP Monitoring Ultra, un aggiornamento del modulo di controllo VIP della soluzione CSI, progettato per intercettare prontamente informazioni che possano rivelarsi sensibili per la protezione della sicurezza cyber degli utenti VIP. Novità anche sul fronte dell'AI generativa in relazione ai processi di detection e reportistica degli allarmi rilevati da Cypeer. Il team I-SOC ha infatti istruito il sistema di intelligenza artificiale per redigere autonomamente un'analisi approfondita dell'allarme, che

riporta i passaggi precisi di risoluzione del problema, oltre a dettagli relativi al caso specifico.

Cyberoo ha inoltre completato l'installazione delle proprie apparecchiature all'interno del Data Center Equinix Warsaw WA2 International Business Exchange (IBX) in Polonia, come parte della sua strategia di espansione dell'infrastruttura cloud. L'ordine per la fornitura è stato siglato il 16 maggio 2024, con l'installazione delle macchine avvenuta il 12 giugno 2024.

Il 4 giugno 2024, Cyberoo ha annunciato l'avvio delle attività in Spagna e Portogallo, proseguendo il percorso di sviluppo della propria presenza internazionale dopo l'apertura della sede in Polonia. La strategia di espansione segue il modello già collaudato in Italia e Polonia, che prevede una crescita organica nel Paese grazie alla costruzione di una rete di partner locali e la creazione di una struttura tecnica con specialisti sul territorio.

Parallelamente, l'11 luglio 2024, Cyberoo ha approvato il suo secondo Bilancio di Sostenibilità, che garantisce grande trasparenza su tutto l'operato aziendale ed evidenzia i risultati raggiunti nel 2023.

Il 12 settembre 2024, Cyberoo ha siglato un accordo strategico con Arrow Electronics per la distribuzione esclusiva delle proprie soluzioni sul mercato polacco. L'accordo rappresenta un ulteriore passo avanti nel processo di internazionalizzazione dell'azienda, rafforzando la presenza di Cyberoo in Europa e consolidando il modello di "go to market" già adottato con successo in Italia.

Il 25 settembre 2024 Cyberoo ha poi siglato un importante accordo di distribuzione con Zaltor, tra i principali player nel settore delle soluzioni IT in Spagna e Portogallo. La collaborazione strategica consentirà a Cyberoo una penetrazione strutturata e capillare nel mercato della cyber security della penisola iberica. A dicembre Cyberoo ha poi avviato partnership strategiche per la rivendita dei suoi servizi MDR con Omega Peripherals, importante reseller con sede a Barcellona, specializzato in soluzioni di sicurezza per il mercato corporate e governativo, COS Mantenimiento e Global Digital Consulting, due società del gruppo COS Global Services, rivenditore basato a Madrid, focalizzato su soluzioni avanzate di cybersecurity per le PMI e le grandi imprese. Questi accordi

rappresentano un importante passo nella strategia di espansione dell'azienda nel mercato iberico.

2008

Start up:
Inizia l'attività come distributore di devices con la denominazione di AT Srl.

2011

Print Management:
Nuovo servizio per la gestione e monitoraggio delle stampanti in partnership con HP.

2015

MSP
(Managed Server Provider)

2017

MSP e Cyber security
La stampante multifunzione diventa uno strumento per attaccare i dispositivi collegati alla rete locale ed eseguirvi codice malevolo.
Dopo l'attacco hacker "Faxploit", inizia l'attività di Managed Server Provider e successivamente di Cyber Security ampliando l'offerta alla gestione, monitoraggio, e protezione di tutta l'infrastruttur IT dei clienti.

2019

Nuove soluzioni e IPO
Rilascio sul mercato di nuove soluzioni di Cyber Security e MSP e IPO sul mercato AIM Italia.

Riassetto societario:
Acquisizione delle partecipazioni totalitarie in Life Your Brand S.r.l. (il 20 dicembre 2018 da SEDOC) e MFD International S.r.l. (il 22 febbraio 2019 da Fabio Leonardi, Massimo Bonifati e Davide Cignatta), quest'ultima titolare, a sua volta, dell'intero capitale sociale di DFM Virtual Service LLC (con sede in Ucraina).

Quotazione in borsa
Il 7 ottobre 2019 Cyberoo viene quotata su Euronext Growth Milan (ex AIM Italia), il mercato di Borsa Italiana riservato alle PMI, risultando la prima società di cyber security quotata a Piazza Affari.

2021

Acquisizione di Cyber Division S.r.l.
In data 27 luglio, Cyberoo finalizza l'acquisizione del 51% di Cyber Division S.r.l., azienda novarese a elevata focalizzazione nelle attività di Vulnerability Assessment, Penetration Test ed Ethical Hacking oltre a quelle di Incident Response.

Nomina "Representative Vendor" da Gartner
Cyberoo viene nominata "Representative Vendor" nella "2021 Gartner Market Guide For MDR Services", la più importante e autorevole ricerca internazionale sui servizi gestiti di sicurezza informatica. Prima e unica azienda italiana a ottenere l'ambito riconoscimento.

2022 NEW

Nuove soluzioni e internazionalizzazione
Cypeer Pure e Cypeer Sonic, che fanno ampio uso di IA e machine learning, un importante progresso nelle attività di Response e Automatic Remediation.
A luglio 2022 Cyberoo riprende il percorso di internazionalizzazione e sbarca in Germania grazie ad ICOS.

Tra le 50 principali aziende mondiali specializzate in MDR
A settembre Cyberoo si riconferma tra i principali player internazionali nel segmento dei servizi di Managed Detection and Response (MDR). Gartner, infatti, ha citato Cyberoo tra le circa 50 principali aziende mondiali specializzate in questo specifico segmento.

Cyberoo Docetz
Cyberoo dà vita a Cyberoo Docetz S.r.l. per accelerare la crescita aziendale e dare sempre maggiore risposta alle attività di cyber security e consulenza.

2023

Nomina "Representative Vendor" da Gartner
Cyberoo ottiene da Gartner il secondo riconoscimento come "Representative Vendor" nella "Market Guide For MDR Services 2023".

Nuova sede in Polonia
Nel maggio 2023, Cyberoo inaugura la sua nuova sede nella capitale polacca, dove svolge attività I-SOC di secondo livello, 24/7, e nella quale prenderanno il via, verso la fine dell'anno, le attività commerciali per l'internazionalizzazione aziendale.

Digital Improvements
Successivamente alle attività di R&D impegnate in campo digitale, Cyberoo introduce il nuovo sito web, il Black Button e l'App CYBShield. Le nuove feature digitali sono volte a velocizzare e facilitare la comunicazione tra le aziende e Cyberoo.

Cyberoo è CERT
Cyberoo entra a far parte del circuito CERT (Computer Emergency Response Team) del Trusted Introducer, principale riferimento del settore a livello internazionale.

2024 NEW

Avvio attività commerciali in Spagna e Portogallo
Cyberoo avvia le prime attività commerciali nella penisola iberica.

Nominata "Represenative Vendor" da Gartner
Per il terzo anno Cyberoo rimane l'unica azienda italiana ad essere nominata “Representative Vendor” nella prestigiosa ricerca "Market Guide For MDR Services”.

Nuove soluzioni di cybersecurity
Lancio di Cypeer Keera, Cypeer POT, Cypeer AgentX, BlackBOX, VIP Monitoring Ultra e AI generativa nei processi di detection e reportistica degli allarmi.

Mission e Valori

WE ARE

CYBEROO

1° vendor di Cybersecurity quotato in Borsa Italiana

Oltre 200 risorse altamente qualificate

Oltre 700 clienti Mid Size Enterprise

5 sedi in EMEA

Gartner Market Guide for MDR Services

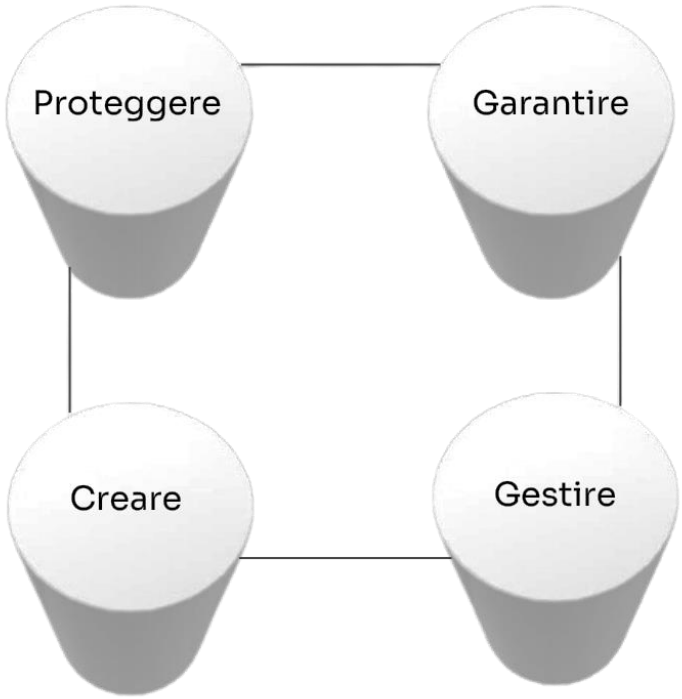
CYBEROO è CERT

Tecnologie proprietarie e certificate

Conforme al GDPR

Mission

Cyberoo si propone di essere “***il faro made in Italy che illumina le zone oscure e poco chiare del cyber spazio***”, una vera e propria guida che accompagni le aziende, le persone e gli enti nel percorso di conoscenza, formazione e difesa oramai imprescindibili per vivere al meglio e in sicurezza le proprie vite nell’ambito del digitale. Un faro che sia però anche polo di ricerca e sviluppo per le più avanzate tecnologie di Detection.



Proteggere, garantire, creare, gestire: sono le quattro "torri di vedetta" di Cyberoo (rappresentate nel logo), indispensabili alla salvaguardia cyber del Business delle aziende clienti.

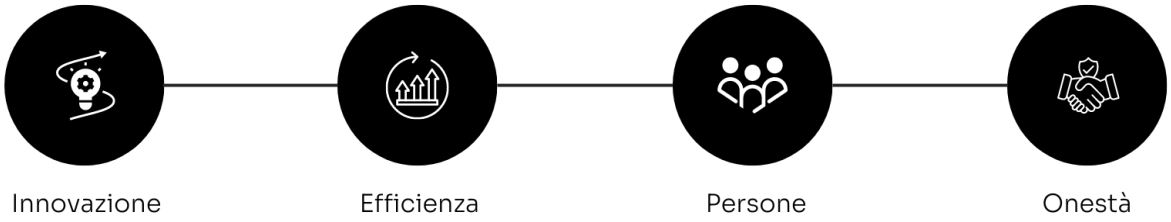
Cyberoo si pone attorno all'attività delle aziende e si colloca come guardiano a tutela delle informazioni e dei dati. Le soluzioni proposte da Cyberoo assolvono a questo scopo mettendo insieme tutte le misure per proteggere i dati da eventi imprevisti, per tutelarne la disponibilità e l'integrità e la riservatezza informatica, garantendo anche un veloce recupero e ripristino in caso di necessità.

Creando nuove soluzioni e algoritmi di intelligenza artificiale, il Gruppo è in grado di monitorare, gestire e proteggere le informazioni dell'ecosistema IT dalle minacce informatiche e dal *cyber crime*, garantendo la sicurezza e le performance dei sistemi.

Valori

Cyberoo è da sempre impegnata a sviluppare e favorire una cultura fondata sulla collaborazione, che contribuisce all'eccellenza dei servizi professionali forniti e alla creazione di un ambiente di lavoro partecipativo.

In questo contesto, i valori a cui il Gruppo si ispira – e dai quali derivano i propri modelli di condotta – per competere efficacemente e lealmente sul mercato, accrescere il valore e sviluppare le competenze e la crescita professionale delle Persone sono:



Innovazione

Promuovere un ambiente che stimoli l'esplorazione e l'identificazione continua di nuove opportunità per progettare, sviluppare e promuovere soluzioni creative, tempestive ed efficaci.

Efficienza

Focalizzarsi sulla produttività e sul miglioramento continuo attraverso soluzioni innovative che incrementino il valore e le performance delle aziende clienti, affrontare rapidamente le sfide di un mercato in evoluzione, garantendo sempre un'elevata qualità del servizio offerto.

Persone

Le persone sono il fattore chiave per il conseguimento degli obiettivi e dei piani aziendali. Per questo motivo Cyberoo tutela il capitale umano, con la promozione del potenziale di ogni singola risorsa e l'incentivazione di competenze individuali e professionali.

Onestà

I dipendenti e i collaboratori di Cyberoo operano con responsabilità, onestà e trasparenza, astenendosi dal perseguire l'utile personale in violazione delle leggi

vigenti. Il Gruppo si impegna a garantire l'integrità nella condotta del business, la migliore qualità di servizio e la massima trasparenza su tempi e aspettative.

Mercato di riferimento

Il Gruppo Cyberoo opera principalmente nel mercato del MDR (Managed Detection and Response), riguardante l'offerta a una clientela business, principalmente in riferimento alla media e grande azienda.
I servizi MDR forniscono ai clienti le moderne funzionalità di Security Operations Center (SOC) erogate da remoto per rilevare, analizzare, indagare e rispondere attivamente alle minacce informatiche. La definizione classica di MDR prevede che i provider di tali servizi installino all'interno dell'ecosistema del cliente le proprie tecnologie proprietarie che coprono endpoint, reti, servizi cloud, tecnologia operativa (OT)/ Internet of Things (IoT) e altre fonti, per raccogliere log, dati e altre informazioni di contesto utili per analizzare la postura di sicurezza del cliente. I dati raccolti da varie fonti vengono analizzati tramite la piattaforma del provider grazie a sistemi di Intelligenza Artificiale e Machine Learning. Infine, i servizi di individuazione della remediation H24 vengono eseguiti da cybersecurity specialists che completano le capacità di monitoraggio e rilevamento in tempo reale.
L'MDR è quindi un provider di servizi gestiti che prevede l'esternalizzazione delle funzioni di gestione della sicurezza informatica di un'azienda cliente. È un metodo strategico destinato a migliorare le operazioni di un'organizzazione e anche a ridurre i costi su attività che non rappresentano il core business dell'azienda che acquisisce il servizio. L'obiettivo, infatti, tramite il servizio è quello di accedere a risorse estremamente preparate sui temi come la cybersecurity e il monitoraggio dell'ecosistema IT sotto diversi punti di vista. L'adozione di servizi gestiti è anche considerata un modo efficace per rimanere aggiornati sulla tecnologia. Gli MDR sono considerati un'alternativa al modello di esternalizzazione su base fissa o on-demand su cui si basa il classico modello di fornitura ICT. Anche da un punto di vista del pricing, l'MDR normalmente propone canoni ricorrenti, che quindi assicura al cliente un costo certo e non legato a monte ore di lavoro connesso a progetti.

In particolare, nel contesto europeo la domanda di Managed Detection and Response (MDR) continua a crescere in modo significativo, con una previsione di crescita annuale del 20% nei prossimi quattro anni, secondo Gartner. In particolare, i mercati di Spagna (+26%) e Polonia (+22%) sono quelli con il maggiore potenziale di espansione. Anche in Italia, il mercato della cybersecurity sta vivendo una forte espansione, con il mercato MDR che cresce del 27% annuo, confermando l'interesse crescente delle aziende italiane nel proteggere i propri sistemi critici. Questo aumento è dovuto alla continua evoluzione delle minacce informatiche e alla necessità di migliorare la resilienza operativa e la risposta agli incidenti. Secondo il report di Gartner, i servizi di Managed Detection and Response (MDR) stanno diventando sempre più essenziali per le organizzazioni che desiderano migliorare la loro capacità di rilevare e rispondere rapidamente alle minacce. Gartner prevede che entro il 2028, il 50% dei risultati ottenuti dai fornitori di servizi MDR sarà incentrato o includerà dettagli sulle esposizioni alle minacce, rispetto al 10% di oggi. Il Global Risk Report del World Economic Forum identifica al quinto posto nella classifica dei rischi più rilevanti per i prossimi due anni quelli legati alla cybersecurity.

In particolare, il "Global Cybersecurity Outlook 2025" offre una panoramica chiara e approfondita sulle sfide e le tendenze emergenti nel mondo della cybersicurezza. Il quadro che ne emerge è quello di un settore in continua evoluzione, in cui le minacce informatiche diventano sempre più sofisticate mentre aziende e governi cercano di rafforzare le proprie difese in un contesto globale sempre più instabile. Uno dei punti chiave riguarda la sicurezza delle catene di approvvigionamento. Sempre più aziende dipendono da fornitori terzi per servizi digitali e infrastrutture IT ma questo introduce nuove vulnerabilità. Più della metà delle grandi organizzazioni (54%) ritiene che la gestione della sicurezza nella supply chain sia una delle sfide più critiche per migliorare la resilienza informatica. Anche le tensioni geopolitiche stanno avendo un impatto significativo. Conflitti e rivalità tra nazioni stanno alimentando lo spionaggio informatico e il furto di proprietà intellettuale, con il 60% delle aziende che ha dovuto ripensare la propria strategia di cybersicurezza per tenere conto di questi rischi. Il 45% dei responsabili della sicurezza teme inoltre che questi fattori possano causare interruzioni operative di rilievo. Un altro elemento di grande rilievo è la diffusione dell'Intelligenza Artificiale (IA). Il 66% delle aziende prevede che l'IA trasformerà il panorama della sicurezza

informatica nel prossimo anno, sia come strumento di difesa che come nuova minaccia. Tuttavia, meno del 40% delle organizzazioni dispone di procedure adeguate a valutare i rischi connessi agli strumenti basati sull'IA prima della loro implementazione. Parallelamente, cresce il pericolo legato agli attacchi di social engineering, come il phishing e il ransomware. Il 72% delle organizzazioni ha segnalato un aumento dei tentativi di attacco, con criminali informatici che sfruttano l'IA generativa per rendere le truffe più sofisticate e difficili da individuare. Dall'analisi emerge un mercato della cybersicurezza sempre più strategico e cruciale per le aziende di ogni settore. La necessità di adottare un approccio più proattivo, investire in tecnologie avanzate e formare nuove competenze è oggi più evidente che mai.

Mercato Europeo

Il 2024 è stato un anno cruciale per il mercato della cybersecurity in Europa, caratterizzato da un incremento significativo degli investimenti, dalla continua evoluzione delle minacce informatiche e dall'introduzione di normative sempre più stringenti. Questi fattori hanno spinto le aziende a rafforzare le proprie strategie di sicurezza digitale, con un impatto positivo sull'intero settore. La spesa in sicurezza rimane quindi una priorità strategica nell'ambito IT per le organizzazioni europee, che devono far fronte a un incremento costante dei cyberattacchi, proteggere gli ambienti cloud e adeguarsi alle nuove normative, come la NIS2 e la DORA. Questo aumento della spesa è stato spinto dalla necessità di affrontare minacce informatiche senza precedenti, derivanti da un'economia criminale in espansione e da un panorama geopolitico turbolento. La crescente digitalizzazione, unita all'aumento degli attacchi informatici, ha sottolineato la necessità di proteggere adeguatamente le infrastrutture critiche e i dati sensibili. Secondo i dati forniti da CONTEXT, il mercato distributivo europeo della cybersecurity ha registrato una crescita del 2% su base annua. In particolare, la protezione delle infrastrutture ha mostrato una crescita robusta del 14%, indicando un focus crescente delle organizzazioni sulla difesa delle proprie infrastrutture critiche. La European Union Agency for Cybersecurity (ENISA) ha pubblicato il "2024 Report on the State of the Cybersecurity in the Union", che fornisce una panoramica dettagliata del panorama della cybersecurity nell'Unione Europea. Il rapporto evidenzia come le minacce informatiche siano in costante evoluzione, con attacchi sempre più sofisticati che

richiedono strategie di difesa avanzate. Inoltre, sottolinea l'importanza di rafforzare le capacità di cybersecurity a livello nazionale ed europeo per affrontare le sfide emergenti. Le aziende hanno investito massicciamente in intelligenza artificiale per la sicurezza informatica e servizi di Managed Detection and Response (MDR) per far fronte alle minacce sempre più sofisticate. Parallelamente, la crescita del cloud computing e dell'Internet of Things (IoT) ha alimentato la domanda di protezioni avanzate contro gli attacchi alle infrastrutture digitali. Si prevede che questo percorso di crescita si tradurrà in un volume di mercato pari a 65,17 miliardi di dollari entro il 2029. Tale crescita dimostra la crescente domanda di soluzioni e servizi di sicurezza informatica in Europa, poiché le organizzazioni si sforzano di proteggere le proprie risorse digitali dalle minacce in continua evoluzione. Il mercato dei servizi di Managed Detection and Response (MDR) ha mostrato una notevole espansione. L'Europa detiene la seconda quota di mercato più grande nel settore della sicurezza informatica, grazie anche alle iniziative intraprese dalla Commissione Europea per rafforzare la lotta contro gli attacchi informatici e al supporto fornito dai fondi UE per la digitalizzazione delle aziende.

L'espansione della cybersecurity si lega all'adozione delle nuove normative europee: il 2 dicembre 2024, il Consiglio dell'Unione Europea ha adottato nuove norme per rafforzare le capacità di cibersicurezza nell'UE, note come "regolamento sulla cibersolidarietà". Questo regolamento istituisce un "sistema di allarme in materia di cibersicurezza" e un meccanismo per le emergenze di cibersicurezza, destinato ad accrescere la preparazione e potenziare le capacità di risposta agli incidenti nell'UE.

Nel contesto delle normative europee, il 2024 ha visto la piena attuazione della Direttiva NIS2, che ha ampliato il numero di settori regolamentati e introdotto sanzioni più severe per le aziende non conformi, favorendo una maggiore attenzione agli investimenti in cybersecurity. L'adeguamento alla NIS2 non rappresenta solo un obbligo normativo, ma anche un'opportunità strategica per le aziende: conformarsi permette di migliorare la sicurezza interna, aumentare la fiducia dei clienti e rafforzare la competitività. Le imprese devono dunque agire rapidamente per garantire la conformità entro i tempi stabiliti. Il 10 dicembre 2024, è entrato in vigore il Cyber Resilience Act, che impone obblighi di sicurezza informatica ai produttori di software e hardware, garantendo che i dispositivi digitali immessi sul mercato dell’UE siano più resilienti agli attacchi informatici.

Contestualmente, il Digital Operational Resilience Act (DORA), adottato nel 2022, mira a garantire che tutte le imprese del settore finanziario nell'UE possiedano le capacità necessarie per resistere, rispondere e riprendersi da tutte le tipologie di interruzioni e minacce legate alle tecnologie dell'informazione e della comunicazione (ICT). Il Digital Operational Resilience Act (DORA) sta rafforzando la sicurezza operativa nel settore finanziario, con impatti significativi su banche, assicurazioni e fintech.

Queste normative stanno ridefinendo il panorama della sicurezza digitale in Europa, imponendo alle imprese standard più elevati di protezione e gestione del rischio informatico. Le imprese che sapranno adattarsi rapidamente alle normative emergenti, integrando soluzioni avanzate di sicurezza e strategie di sicurezza proattive, saranno quelle meglio posizionate per affrontare il futuro digitale, rispondendo così alle sfide di un panorama cyber sempre più complesso.

Le prospettive future per il mercato europeo della cybersecurity rimangono estremamente positive: secondo le previsioni di Statista, il mercato europeo della cybersecurity raggiungerà un fatturato di 49,67 miliardi di dollari entro il 2025, con i servizi di sicurezza che domineranno il mercato con un volume previsto di 26,01 miliardi di dollari. A fronte di questo scenario, il costo del crimine informatico, stimato in 5,5 trilioni di euro nel 2020, è previsto aumentare drasticamente fino a raggiungere i 10,5 trilioni di euro entro il 2025. Questo ulteriore aumento sottolinea l'urgenza di considerare la cybersecurity come una priorità assoluta per le aziende e le istituzioni europee.

Mercato italiano

Nel 2024, il mercato della cybersecurity in Italia ha registrato una crescita continua e significativa, sostenuta dall'aumento costante degli attacchi informatici. Rispetto all'anno precedente, gli incidenti cyber in Italia sono aumentati del 15,2%, posizionandosi sotto la media globale del 27,4%. Nonostante ciò, l'Italia continua a essere uno dei bersagli principali degli attacchi informatici, con una percentuale di incidenti che ha visto una crescita del 65%, molto superiore al tasso globale dell'11,7%. Un elemento rilevante è l'incremento degli attacchi attribuibili al cybercrime, che nel 2024 sono aumentati del 40%, a testimonianza di un panorama di minacce in continua evoluzione. Inoltre, il 39% degli incidenti di alta gravità verificatisi negli ultimi cinque anni si è concentrato nel solo 2024, dimostrando

l'aumento della gravità e dell'impatto degli attacchi sulle organizzazioni italiane. Secondo l'Osservatorio Cybersecurity del Politecnico di Milano, il 73% delle grandi aziende italiane ha affrontato attacchi nel corso dell'ultimo anno, un dato che evidenzia come anche le realtà che si presume abbiano infrastrutture di sicurezza consolidate e investimenti costanti, non siano immuni agli attacchi. Il Rapporto Clusit 2024, inoltre, conferma che il 78% degli attacchi informatici in Italia è attribuibile al cybercrime (in aumento rispetto al 64% del 2023) un dato che riflette l'accessibilità crescente agli strumenti di attacco, molti dei quali disponibili sul dark web come servizi "as-a-Service", che permettono anche ai criminali meno esperti di lanciare attacchi. Gli incidenti classificati come Hacktivism costituiscono il restante 22% e continuano a rappresentare una parte significativa degli attacchi in Italia, anche a causa del prolungarsi del conflitto in Ucraina. Dal 2022 infatti, con l'inizio del conflitto in Ucraina, siamo entrati in una nuova era di guerra cibernetica diffusa, che si è ulteriormente intensificata nel 2024. A questa dinamica si aggiungono le sfide poste dalla diffusione dell'AI generativa, utilizzata come potente strumento dagli attaccanti e dalle crescenti tensioni socioeconomiche e geopolitiche che hanno riacceso forme di antagonismo digitale, principalmente attraverso attacchi DDoS.

Nel contesto globale, l'Italia si posiziona come uno dei principali obiettivi degli attacchi informatici, ricevendo circa il 10,1% degli attacchi mondiali, delineando una chiara incertezza della situazione cyber italiana rispetto agli altri paesi del mondo. Questa crescente minaccia ha determinato un aumento della spesa in cybersecurity, che ha superato i 2 miliardi di euro nel 2024, con un incremento dell'11% rispetto all'anno precedente. Questo dato riflette una crescente consapevolezza delle imprese italiane sull'importanza della protezione dei dati e delle infrastrutture critiche. Tale risultato consolida il trend che ha caratterizzato gli ultimi anni, evidenziando l'importanza sempre maggiore della sicurezza informatica nelle strategie aziendali, sostenuta anche dalle crescenti minacce dovute al fatto che il nostro Paese è uno dei principali obiettivi degli attacchi.

Le previsioni per il periodo 2025-2027 indicano una crescita continua del mercato, con la spesa totale in soluzioni e servizi digitali destinata a superare gli 84,5 miliardi di euro entro il 2025, con incrementi del 4,1% nel 2026 e del 4,2% nel 2027, arrivando a 91,7 miliardi di euro entro la fine del 2027. Una crescita robusta e

continua, stimolata sia dall'aumento delle minacce informatiche che dalle nuove normative.

La regolamentazione di settore

Nel mercato in cui opera, Cyberoo si trova oggi a confrontarsi con il più recente quadro normativo europeo in materia di sicurezza informatica, a partire dalla Direttiva NIS2 (UE 2022/2555).
Per Cyberoo ciò si traduce nella conferma di adozione di un rigoroso sistema di gestione del rischio, che va dall'introduzione di policy interne volte a garantire la prevenzione e il tempestivo rilevamento degli incidenti, fino alla formalizzazione di un modello di governance. Parallelamente, l'azienda ha adeguato le procedure di notifica per segnalare eventuali incidenti, nonché rafforzare i controlli sulla supply chain.
Dal 17 gennaio 2025, poi, è entrata in vigore il Regolamento UE 2022/2554, noto come Digital Operational Resilience Act (DORA) che, pur essendo rivolto principalmente a istituzioni finanziarie e ai loro provider ICT dedicati, impone a Cyberoo – in quanto fornitore di servizi di sicurezza a banche, assicurazioni e intermediari – l'adozione di un solido framework di resilienza operativa digitale.
L'insieme di queste disposizioni normative richiede a Cyberoo un continuo e proattivo aggiornamento delle proprie procedure interne, un rafforzamento degli investimenti in ricerca e sviluppo – soprattutto nelle aree di threat intelligence e dei Security Operations Center – e un costante miglioramento delle competenze del personale tecnico, in un'ottica di servizio sempre più avanzato e capillare a tutela della sicurezza e della resilienza digitale dei clienti.

Normativa in materia di privacy

In data 24 maggio 2016 è entrato in vigore il nuovo Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, in materia di protezione dei dati delle persone fisiche, volto a definire un quadro normativo comune in materia di tutela dei dati personali per tutti gli Stati membri dell'Unione Europea. Esso è direttamente applicabile in tutti i Paesi dell'Unione Europea a partire dal 25 maggio 2018.

In particolare, il GDPR ha introdotto significative modifiche ai processi da adottare per garantire la protezione dei dati personali (tra cui dotarsi di una nuova figura del data protection officer, implementare un efficace modello organizzativo in materia privacy, sottostare a obblighi di comunicazione in caso di particolari violazioni dei dati) aumentando il livello di tutela delle persone fisiche e inasprendo, tra l'altro, le sanzioni applicabili al titolare e all'eventuale responsabile del trattamento dei dati, in caso di violazioni delle previsioni del GDPR. Con riferimento alle violazioni dei dati personali (c.d. data breach), si segnala che il GDPR impone che il titolare del trattamento debba comunicare tali eventuali violazioni all'Autorità nazionale di protezione dei dati.

Intelligenza Artificiale

Considerata la centralità, soprattutto prospettica, dell'ambito dell'intelligenza artificiale per il business di Gruppo Cyberoo, si segnala che in data 21 aprile 2021, la Commissione Europea ha presentato una proposta di Regolamento che definisce in modo organico e strutturato il quadro giuridico in relazione all'Intelligenza Artificiale, riconoscendo innumerevoli vantaggi competitivi che l'Intelligenza Artificiale può fornire da un punto di vista economico, sociale ed ambientale. Allo stesso tempo, ha individuato alcune applicazioni che potrebbero generare rischi e avere effetti negativi sul mercato.

È dunque necessario, secondo la Commissione Europea, definire un quadro normativo che stabilisca regole chiare e condivise volte a disciplinare l'applicabilità dell'AI (Artificial Intelligence), in modo tale da creare le condizioni di fiducia per quel che riguarda l'immissione sul mercato e l'utilizzo degli strumenti di IA nell'Unione Europea.

Per queste ragioni, si sono stabilite regole di trasparenza armonizzate per i sistemi di IA che interagiscono con persone fisiche e per quelli utilizzati per generare o manipolare immagini, audio, video o contenuto.

Il nuovo quadro giuridico destinato all'intelligenza artificiale sarà basato su misure che individuano un rischio chiaramente definito, regole che facilitano l'istituzione di codici di condotta volontari e un sistema di governance a sostegno dell'attuazione del regolamento a livello europeo e nazionale.

Strategia e sostenibilità

Il ruolo di Cyberoo e le linee strategiche di sviluppo

L'impronta Cyberoo ha il suo cardine nella cultura dell'innovazione che permea ogni aspetto del processo di management.

Le finalità di Cyberoo sono coerenti con i principi di un modello di sviluppo sostenibile, rispetto al quale il settore IT viene riconosciuto come strategico secondo tre direttrici:

- Trasformazione digitale quale motore di sviluppo.
- Innovazione che punti su ricerca e sviluppo applicate e favorisca le idee, la condivisione della conoscenza, a sostegno delle filiere produttive.
- Sviluppo sostenibile e inclusivo, dove l'innovazione è al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.

Obiettivi di sviluppo sostenibile

Cyberoo persegue da sempre un modello di sviluppo industriale che fa propri i principi di sostenibilità, trasparenza e qualità, assumendo impegni concreti e adottando specifici assetti gestionali e organizzativi, con **l'obiettivo di creare valore condiviso per tutti i propri stakeholder** e nel rispetto dell'ambiente.

In particolare, Cyberoo fonda il proprio approccio strategico in coerenza con il percorso di sostenibilità intrapreso, che prevede una progressiva integrazione degli obiettivi di sviluppo sostenibile (SDGs – Sustainable Development Goals), parte dell'Agenda 2030 delle Nazioni Unite.

L'attuale contesto ed i megatrend in atto richiedono alle imprese un impegno nel perseguimento di obiettivi economici che possano generare degli impatti positivi, anche in termini ambientali e sociali. L'attuazione di una politica di sviluppo sostenibile da parte delle imprese, quale parte del core business di Gruppo, è infatti una leva per il raggiungimento degli SDGs, alla quale si affiancano progetti ed iniziative specifiche.

In questo contesto, Cyberoo ha effettuato una prima analisi di coerenza del proprio modello di business ed obiettivi strategici rispetto agli SDGs, consentendole di evidenziare alcuni SDGs ritenuti prioritari, rispetto ai quali le attività di business del Gruppo sono in grado di dare un contributo significativo.

I driver del Piano industriale e l'impegno di Cyberoo rispetto agli Obiettivi di sviluppo sostenibile trovano la loro integrazione nelle attività, nei progetti e nelle azioni di gruppo, secondo lo schema di seguito rappresentato.

I driver della strategia di Cyberoo

L'innovazione per Cyberoo è da sempre il cuore pulsante attorno al quale ruotano idee, progetti, servizi, design e processi di sviluppo. L'innovazione è alimentata dalla ricerca che favorisce lo sviluppo delle idee e la condivisione della conoscenza, a sostegno dei diversi settori di mercato. Ma l'innovazione, dove è al servizio delle persone, delle imprese, delle comunità e dei territori, nel rispetto della sostenibilità ambientale, produce anche lo sviluppo sostenibile e inclusivo.
Partendo proprio dal connubio **INNOVAZIONE** unita al **BENESSERE DELLE PERSONE**, Cyberoo ha individuato 6 linee di azione, alla base anche delle politiche e dei sistemi di gestione che regolano i processi e l'operatività della Società coerenti con lo sviluppo sostenibile.

INNOVATION & WELLBEING

Linee di azione	Obiettivi	SDGs
Quality Solutions (Innovation & Digital Transformation)	• Sviluppare progetti per il controllo e l'ottimizzazione della qualità dei servizi • Promuovere la digitalizzazione dei processi e della cybersecurity • Sviluppare l'innovazione dei prodotti	
Environment	• Migliorare l'impatto ambientale dei trasporti e della logistica • Roadmap verso la carbon neutrality	
People	• Migliorare le condizioni di lavoro e il clima aziendale • Potenziare la salute e sicurezza sul lavoro • Migliorare la comunicazione interna verso i dipendenti • Sviluppare il sistema di welfare aziendale • Assicurare il gender balance nei percorsi di carriera e assunzioni • Valorizzare la meritocrazia e assicurare la parità nei percorsi retributivi e di carriera	
Clients	• Sviluppare iniziative per migliorare l'attenzione verso i clienti e la misurazione della loro soddisfazione • Incrementare la sicurezza di prodotto e dei clienti	
Community	• Sviluppare collaborazioni e partnership con il mondo scuola, università, onlus ed enti locali • Sviluppare la cultura delle risorse interne attraverso iniziative di organizzazione e formazione • Sviluppare la formazione su etica e trasparenza	

Analisi di materialità

Il ruolo degli stakeholder

Gli stakeholder sono i soggetti (individui o gruppi) espressione di interessi, aspettative e valutazioni diversi nei confronti di un'impresa, con i quali essa intrattiene relazioni costanti nello svolgimento della propria attività. Il coinvolgimento ed il confronto con gli stakeholder (*stakeholder engagement*) consente non soltanto di comprenderne le esigenze, aspettative e valutazioni, ma anche di definire una migliore strategia e obiettivi di business, valutando il cambiamento, i rischi e le opportunità.

Il sistema di relazioni di Cyberoo con i propri stakeholder prevede strumenti e canali di dialogo differenziati per le diverse categorie di stakeholder, coerenti con il livello di interdipendenza e influenza sull'organizzazione.

Categoria Stakeholder	Attività di engagement (Progetti – Iniziative – Relazioni)
Banche e finanziatori	Assemblea azionisti - Sito internet - Incontri ed eventi periodici
Dipendenti	Dialogo costante con Direzione Risorse umane - Incontri informali / istituzionali - Incontri di formazione - Iniziative di welfare aziendale - Intranet aziendale - Newsletter interna / Piano di comunicazione dedicato; Performance Management
Fornitori & Partner	Incontri commerciali - Definizione e condivisione di standard - Partnership su progetti (prodotti e innovazione)
Clienti	Interazione tramite incontri commerciali / workshop e presentazioni - Incontri progettuali - Social network - Sito web e Altri canali di comunicazione dedicati - Newsletter informative
Pubblica Amministrazione	Enti pubblici nazionali e locali / Autorità nazionali / locali – Enti di controllo e regolatori: incontri / invio e scambio comunicazioni per adempimenti o richieste specifiche
Comunità e territorio - Istituzioni ed Associazioni locali	Incontri con rappresentanti comunità locali - Collaborazione a progetti di open innovazione - formazione e di responsabilità sociale
Media	Interviste - Conferenze stampa - Sito web istituzionale - Comunicati stampa

I temi materiali

Nell'ambito della rendicontazione di natura ESG, l'**analisi di materialità** è volta a identificare gli aspetti ambientali, sociali, economici e di governance considerati rilevanti e significativi per il business del Gruppo Cyberoo e per i suoi stakeholder.

Tali tematiche vengono definite "materiali" in quanto risultano associate agli impatti (positivi o negativi, effettivi o potenziali, di breve o lungo periodo) più significativi che le attività aziendali sono (o potrebbero essere) in grado di generare sull'economia, l'ambiente e le persone, compresi gli impatti sui loro diritti umani.

Non tutti gli aspetti materiali sono di uguale importanza, e l'enfasi all'interno di un report ne riflette la loro priorità relativa. Ai fini della redazione del primo bilancio di sostenibilità, ancorché redatto secondo l'opzione di rendicontazione GRI "*With referenced to*", Cyberoo aveva effettuato, in coerenza con i GRI Standard, un'analisi di materialità.

Al fine di identificare i principali impatti che le attività svolte da Cyberoo generano o potrebbero generare sulla sfera ESG, nel corso del 2022 è stato svolto un processo strutturato che ha permesso di definire nel dettaglio il contesto di riferimento all'interno e all'esterno dell'Organizzazione.

Nel 2024 non sono intervenuti eventi significativamente rilevanti tali da prevedere una revisione dell'analisi di materialità. Per questa ragione il management aziendale del Gruppo ha valutato di considerare come "materiali" gli stessi temi e impatti ESG definiti nell'esercizio 2022.

Lo svolgimento dell'analisi di materialità si è articolata nei seguenti passaggi:

Processo: Fasi	
1	Identificazione e mappatura stakeholder
2	Linee guida del piano industriale e relativi obiettivi
3	Analisi documentale dello scenario di riferimento: normativa settore e megatrend (in particolare politiche EU Green Deal – EU Next Generation Plan e PNRR)

4	Analisi benchmark di settore: Reporting di sostenibilità dei comparables nazionali ed internazionali
5	Stakeholder: approfondimento delle attività di engagement di carattere ricorrente svolte nei confronti delle diverse categorie di stakeholder /Aspettative da analisi contesto
6	Valutazione del management e di alcuni stakeholder (dipendenti, fornitori, investitori, banche e clienti) attraverso un questionario di valutazione
7	Validazione delle tematiche di materialità e del livello di priorità da parte del top management di Cyberoo (Presidente/Amministratore Delegato/Direttore generale)

Gli impatti individuati sono stati clusterizzati in base al reciproco livello di affinità, al fine di ottenere un elenco più limitato di 26 tematiche ESG da sottoporre a valutazione quantitativa da parte dei Vertici Aziendali e da un campione rappresentativo delle principali categorie di stakeholder dell'azienda.

Per la valutazione delle tematiche è stato utilizzato un questionario con il quale è stato richiesto di prioritizzare ciascun tema, secondo il livello di rilevanza.

In particolare, la valutazione circa il livello di "rilevanza" degli impatti ESG connessi a ogni tematica ha tenuto conto dei seguenti elementi:

- **scala**: entità (in senso positivo o negativo, a seconda dei casi) dell'impatto generato direttamente o indirettamente dalle attività aziendali;
- **portata**: diffusione dell'impatto in termini geografici (es: livello locale, nazionale, ecc.), considerando il numero di stakeholder coinvolti, ecc.;
- **carattere di rimediabilità**: misura in cui è possibile mitigare o porre rimedio all'impatto una volta che esso si è verificato (da considerare solo per gli impatti negativi);
- **probabilità**: probabilità con cui tale impatto potrebbe verificarsi nel breve, medio e lungo periodo (da considerare solo per gli impatti potenziali).

Al fine di identificare i temi e gli impatti ESG realmente "materiali" per Cyberoo è stata definita la cosiddetta "**soglia di materialità**", considerando come tali, per ogni macro ambito, il 50% dei temi che hanno ottenuto una prioritizzazione più elevata.

Al termine dell'intero processo, i risultati conseguiti sono stati sottoposti a discussione e validazione da parte del Consiglio di Amministrazione di Cyberoo S.p.A. in data 22/05/2023.

Nella tabella successiva viene data evidenza, per ciascun tema materiale identificato, delle ragioni di rilevanza del tema (impatti generati sull'economia, ambiente e persone), dei KPI relativi che sono stati rendicontati e dei processi di monitoraggio adottati.

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
Governance				
Etica e integrità nella condotta del business	Possibilità di incidere positivamente o negativamente su: • gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera • mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce	GRI 2-27 GRI 205-3 GRI 206-1 GRI 207-1	Processi di verifica dell'allineamento alle normative e agli standard in materia di etica e integrità del business	Codice Etico Modello di Organizzazione, Gestione e Controllo 231/01 Predisposizione e asseverazione con cadenza annuale del Bilancio Finanziario
Tutela del brand e reputazione	Possibilità di incidere positivamente o negativamente su: • sensibilità e consapevolezza della clientela e del mercato sulla sostenibilità • disponibilità di prodotti e servizi con elevate performance ambientali/sociali	GRI 2-6	Processo di aggiornamento e monitoraggio costante dei brand registrati	Adozione di misure volte a rafforzare la reputazione dell'azienda, incrementando l'apprezzamento da parte dei clienti e valorizzando i brand del Gruppo
Anticorruzione e compliance	Possibilità di incidere positivamente o negativamente su: • tutela della legalità in ambiti quali il reimpiego di profitti derivanti da attività illecite, il manifestarsi di episodi di corruzione e concussione,	GRI 205-3 GRI 206-1	Attività di monitoraggio e controllo dell'attività di core business Processi di verifica dell'allineamento alle normative e agli standard in materia di etica e	Codice Etico Modello di Organizzazione, Gestione e Controllo 231/01

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	l'adozione di comportamenti anti-competitivi, ecc.		integrità del business	
Governance trasparente e gestione dei rischi di sostenibilità	Possibilità di incidere positivamente o negativamente su: • tutela della legalità e prevenzione di comportamenti illeciti	GRI 2-27 GRI 205-3 GRI 206-1	Processi di monitoraggio e aggiornamento del sistema di gestione dei rischi con integrazione dei rischi ESG	Codice Etico Modello di Organizzazione, Gestione e Controllo 231/01
Capitale economico-finanziario				
Solidità e resilienza economica	Possibilità di incidere positivamente o negativamente su: • gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera (es: settore di riferimento, distretto geografico, ecc.). • mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce. • grado di attrazione nei confronti degli investitori e dei prestatori di capitale.	GRI 201-1	Sviluppo dell'attività di business	Adozione di una strategia competitiva capace di garantire la salvaguardia ed il possibile miglioramento delle performance economico-finanziarie del Gruppo nel corso del tempo
Creazione e distribuzione della ricchezza generata	Possibilità di incidere positivamente o negativamente su: • gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera • mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce • capacità di retention e attraction e sulla	GRI 201-1 GRI 203-1	Sviluppo e rafforzamento delle relazioni con gli stakeholder e relativa distribuzione della ricchezza generata	Piano Industriale di Gruppo Stakeholder Engagement Adozione di misure in grado di garantire la continuità operativa, la stabilità finanziaria e la redditività del business

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	stabilità occupazionale delle risorse umane			
Capitale Produttivo				
Ricerca e innovazione tecnologica	Possibilità di incidere positivamente o negativamente su: • gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera. • disponibilità nei mercati di prodotti e servizi in grado di soddisfare i bisogni della clientela.	GRI 3-3	Attività di analisi delle richieste di mercato e di R&S	
Qualità, sicurezza ed affidabilità dei servizi	Possibilità di incidere positivamente o negativamente su: • benessere della clientela, in termini di assenza di materiali/sostanze tossiche nei prodotti offerti dall'azienda	GRI 416-2	Controlli periodici di qualità sui prodotti commercializzati	Test a campione sui prodotti/servizi commercializzati Certificazioni di qualità sui prodotti/servizi
Capitale Umano e Relazionale				
Formazione e sviluppo delle carriere	Possibilità di incidere positivamente o negativamente su: • opportunità di ciascun collaboratore di intraprendere un percorso di crescita professionale e di realizzare pienamente il proprio potenziale • disponibilità di percorsi finalizzati al rafforzamento e sviluppo delle competenze e delle skill professionali	GRI 404-1	Sviluppo di piani di formazione obbligatoria e specializzata per la crescita professionale dei dipendenti	Impegno per la formazione e addestramento del personale
Partnership con istituzioni ed imprese	Possibilità di incidere positivamente o negativamente su:	GRI 2-28	Sviluppo di partnership strategiche con imprese, enti locali e	

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	• sviluppo della capacità innovativa, produttiva ed economica del territorio e del mercato in cui la stessa azienda opera		associazioni del settore	
Soddisfazione e gestione delle relazioni con i clienti	Possibilità di contribuire positivamente o negativamente a: • realizzazione e soddisfacimento dei bisogni della clientela in termini di offerta dei prodotti e qualità dei servizi	GRI 418-1	Attività di customer satisfaction Attività di analisi delle richieste del mercato	Gestione della customer satisfaction
Rispetto dei diritti umani e tutela dei lavoratori	Possibilità di incidere positivamente o negativamente su: • tutela dei diritti fondamentali dei membri del personale aziendale e di tutti i collaboratori con cui la Società si interfaccia	GRI 401-1 GRI 406-1	Processi di monitoraggio e segnalazione del mancato rispetto dei diritti umani	Codice Etico Monitoraggio degli episodi di discriminazione
Trasparenza delle informazioni sui servizi	Possibilità di influenzare positivamente o negativamente su: • consapevolezza dei clienti in fase di acquisto • grado di fiducia dei clienti e degli stakeholder nei confronti della Società e della sua reputazione • disponibilità di informazioni sulle caratteristiche dei prodotti e dei servizi offerti	GRI 417-3	Disponibilità per i clienti di informazioni sulle caratteristiche dei prodotti/servizi offerti	Capacità di comunicare con trasparenza le caratteristiche dei prodotti/ servizi immessi nel mercato, evitando il greenwashing.
Capitale Ambientale				
Efficienza energetica	Possibilità di incidere positivamente o negativamente su: • costi energetici attraverso azioni e progetti di efficientamento energetico	GRI 302-1	Monitoraggio dei consumi di energia in ottica di efficientamento energetico	Sottoscrizione contratto per l'acquisto di energia proveniente da sole fonti rinnovabili con

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	• tutela delle comunità locali e del territorio rispetto all'esposizione a eventi atmosferici estremi (es: alluvioni, allagamenti, uragani, desertificazione, ecc.)			certificato di origine
Lotta al cambiamento climatico	Possibilità di incidere positivamente o negativamente su: • tutela degli ecosistemi e salvaguardia della biodiversità • tutela delle comunità locali e del territorio rispetto all'esposizione a eventi atmosferici estremi (es: alluvioni, allagamenti, uragani, desertificazione, ecc.)	GRI 305-1 GRI 305-2	Processo di monitoraggio costante degli impatti sull'ambiente derivante dall'attività di business	Confronto e verifica annuale sui risultati raggiunti sulla riduzione delle emissioni
Gestione dei rifiuti	Possibilità di incidere positivamente o negativamente su: • tutela degli ecosistemi e della biodiversità • prosperità dei principali stakeholder con cui l'Organizzazione interagisce in termini di disponibilità di risorse materiche nei sistemi naturali e facilità di accesso a esse • salute e benessere della clientela, in termini di assenza di materiali / sostanze tossiche nei prodotti offerti dall'azienda	GRI 306-3	Gestione responsabile dello smaltimento dei rifiuti, rispettando le leggi e i regolamenti in vigore	Attenzione alla gestione di fine vita del prodotto Utilizzo di packaging sostenibile Impegno nell'aumentare la quantità di materiali riciclati

Il modello di business

Il Gruppo Cyberoo ha adottato un *business model* caratterizzato da risorse con forti competenze commerciali che presidiano in modo trasversale lo sviluppo del portafoglio clienti, integrate e coadiuvate da business solution specifiche per ogni area di competenza in grado di soddisfare le esigenze della propria clientela.

Oltre a una conoscenza approfondita delle necessità dei clienti, il modello di business del Gruppo si basa su un'elevata **specializzazione tecnica**, avvalendosi di partnership consolidate e di professionisti altamente qualificati e specializzati per il settore di riferimento, che richiede una marcata e specifica professionalità nonché capacità di integrazione di soluzioni tecnologiche complesse.

Analisi e individuazione delle esigenze del cliente

L'attività del Gruppo si articola inizialmente mediante un'accurata analisi delle esigenze del cliente e dei processi aziendali che conducono all'identificazione delle possibili implementazioni di soluzioni a servizio della gestione dei sistemi informativi. In tale fase, il team di specialisti del Gruppo procede a raccogliere **informazioni sulle necessità di business dei clienti analizzando sia i fabbisogni espliciti che latenti**, indipendentemente dalla tecnologia che verrà utilizzata: riveste, infatti, particolare importanza l'analisi degli aspetti organizzativi ai fini dell'individuazione delle lacune tecnologiche.

Comparazione delle soluzioni applicabili

In tale fase, vengono analizzate le principali soluzioni applicabili ai fabbisogni del cliente. In particolare, si procede all'**analisi delle soluzioni personalizzate** grazie all'apporto delle capacità professionali altamente specifiche delle risorse interne ed esterne a Cyberoo.

Progettazione delle soluzioni

Completate le attività di analisi, il Gruppo si occupa di progettare internamente le soluzioni tecnologiche da offrire al cliente, a supporto dell'implementazione dei processi organizzativi e operativi e al fine di garantire altresì una sicurezza integrale del perimetro aziendale.

All'esito dell'individuazione delle soluzioni e dei servizi tecnologici da offrire al cliente, si procede a elaborare l'offerta economica che dovrà essere sottoposta all'approvazione del cliente stesso. In particolare il Gruppo, tenendo conto delle esigenze e caratteristiche del cliente, predispone una soluzione tecnologica strutturata attraverso la combinazione di software e/o hardware prodotti e distribuiti dai propri partner e/o soluzioni tecnologiche sviluppate internamente dal Gruppo e concesse in licenza ai clienti. Al fine di proporre al cliente finale un'offerta adeguata alle sue esigenze, il Gruppo individua e seleziona le singole applicazioni, integrando le stesse in un'**unica soluzione tecnologica customizzata alle esigenze del modello di business del cliente**.

Installazione della soluzione

Una volta individuata la soluzione, il Gruppo svolge le **attività necessarie per l'attivazione e l'installazione della stessa sui sistemi del cliente**, il quale viene assistito e affiancato da risorse specializzate del Gruppo.

Erogazione dei servizi di gestione della soluzione

Il Gruppo offre, infine, al proprio cliente servizi di gestione della soluzione prescelta che comprendono: il **servizio di monitoraggio costante dei possibili malfunzionamenti, manutenzione ordinaria della soluzione, risoluzione di possibili errori procedurali,** nonché **implementazione di aggiornamenti**.

Le caratteristiche distintive di Cyberoo

Cyberoo si contraddistingue nel mercato di riferimento per una marcata "anima tech" che si riflette non solo nell'expertise tecnologica, ma soprattutto nelle proprie risorse umane, con l'obiettivo di realizza per le imprese clienti una strategia globale in grado proteggerle dagli attacchi esterni, monitorare e gestire le informazioni dell'ecosistema IT.

In particolare, il successo di Cyberoo può essere sinteticamente riassunto in determinati *fattori critici di successo* di seguito riportati:

- **Settore in forte crescita:** il Gruppo opera in un settore in continua crescita, contraddistinto da un ampio spettro di opportunità di sviluppo.
- **Personale dotato di competenze professionali specifiche e management con elevato know-how:** il Gruppo nasce dall'aggregazione di figure imprenditoriali con esperienza pluriennale nel settore dell'Information Technology con competenze distintive nella gestione di progetti e soluzioni IT complesse per clienti appartenenti a settori strategici per l'economia italiana. Cyberoo offre un portafoglio completo di soluzioni a valore aggiunto per la clientela grazie all'apporto di figure professionali specializzate e dotate di elevate competenze nel settore di riferimento. Grazie a ciò, ha la capacità di sviluppare ed offrire tempestivamente alla propria clientela soluzioni personalizzabili e servizi integrati a supporto delle principali piattaforme infrastrutturali.
- **Comprovata capacità di M&A:** nel perseguimento della strategia di crescita intrapresa fin dalla sua fondazione dal management per il tramite di operazioni di merger & acquisition, il Gruppo ha maturato una considerevole esperienza nelle attività di selezione di società e aziende target e nell'integrazione delle stesse all'interno del Gruppo.
- **Capacità di offrire soluzioni tecnologiche innovative:** il Gruppo, grazie a un costante investimento nella ricerca e nello sviluppo, è fortemente orientato all'innovazione di servizi e all'offerta di soluzioni proprietarie sviluppate in house ed è in grado di mantenere un'elevata competitività a livello tecnologico.
- **Modello di distribuzione TIER II:** Cyberoo adotta questo modello di distribuzione, basato su una rete indiretta di distributori e partner a valore, che consente una penetrazione capillare del mercato grazie a relazioni consolidate con i clienti finali. Questa scelta strategica permette di massimizzare l'efficienza commerciale, ridurre i costi di acquisizione, aumentare la fidelizzazione e garantire una crescita scalabile, valorizzando le competenze e la presenza locale dei partner. Sedoc Digital Group azionista di riferimento e tra i principali partner commerciali, acquisisce le soluzioni Cyberoo tramite il sistema distributivo nazionale a partire dal 1° luglio 2024. Tale modalità faciliterà la riduzione nel tempo dell'esposizione di Sedoc

verso Cyberoo fino alla completa estinzione del credito scaduto, tramite i piani di rientro già definiti.

Le linee di prodotti e servizi

I servizi offerti da Gruppo Cyberoo sono declinati in tre linee di business principali: ***cyber security services, managed services e digital transformation***.

Cyber security services

Cyberoo affianca ai tradizionali prodotti di security un sistema di gestione degli stessi, volto ad analizzare e controllare gli strumenti e i dati da essi prodotti. In particolare, i servizi ricompresi nell'ambito della cybersecurity sono:

Antispam

Il servizio Antispam prevede la messa a disposizione dei clienti di un'infrastruttura remota, operativa presso un primario fornitore nazionale, ridondata, ovvero articolata tramite un cluster Active-Active in modalità Software-as-a-Service (SaaS) operativo presso due Centri Dati che si trovano sul territorio Italiano, uno di Livello (Tier) IV e l'altro di Livello (Tier) III, in grado di analizzare i messaggi di posta elettronica, al fine di individuare sia i messaggi indesiderati (SPAM), sia eventuali minacce informatiche (virus, malware...). Grazie all'ambiente cloud, i clienti hanno la possibilità di migliorare l'affidabilità della loro soluzione di posta elettronica: in caso di necessità, possono utilizzare la soluzione offerta da Cyberoo per leggere, inviare e inoltrare le email. Inoltre, sulla base delle proprie esigenze, i clienti possono scegliere di attivare il servizio in modalità 24 ore su 24, 7 giorni su 7.

Antivirus

Il servizio antivirus, acquistato da terzi e declinato in tre differenti versioni (base, pro e FSS) prevede la presa in carico, da parte del personale tecnico e specialistico della sicurezza degli endpoint aziendali. All'interno del servizio viene fornito al cliente tutto il software necessario per la messa in sicurezza degli endpoint aziendali.

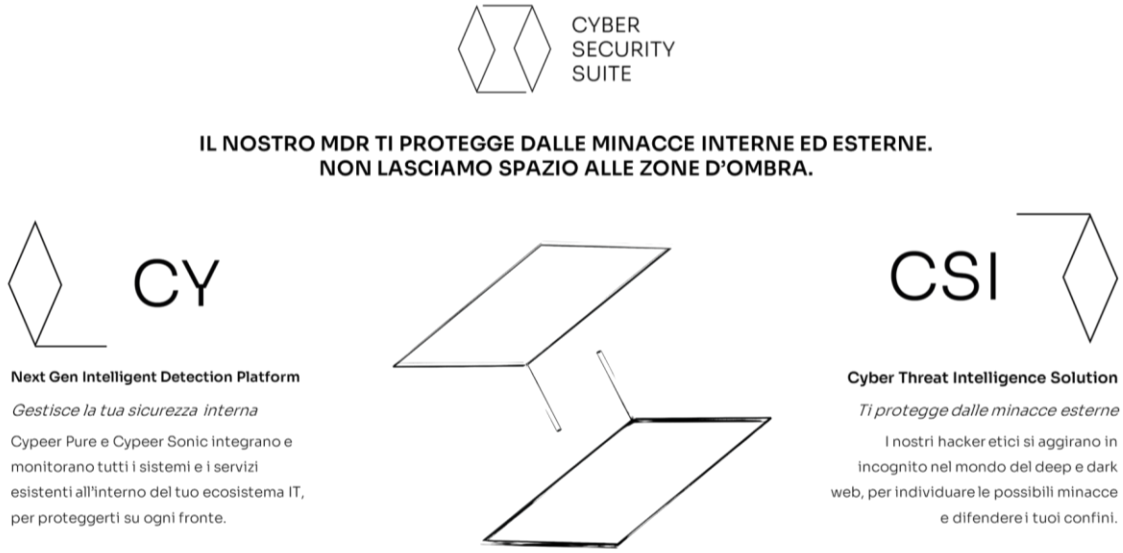
Il servizio antivirus si caratterizza per la semplicità di installazione, per una gestione completa e per il profilo della proattività, in quanto, in caso di segnalazione di una postazione infetta, il personale specialistico procede proattivamente con l'intervento di rimozione della minaccia.

Web security

Il servizio di web security consente alle aziende clienti di definire e applicare regole sull'utilizzo di internet, in modo da impedire che i dipendenti assumano un comportamento illecito che potrebbe anche danneggiare l'immagine dell'azienda. Allo stesso tempo, il software fornito mette in sicurezza l'accesso a internet impedendo gli attacchi cyber e tutelando le persone dall'accesso a siti web compromessi o fraudolenti. Il servizio prevede la registrazione dei siti web visitati dagli utenti del cliente e, ove previsto, il blocco dell'accesso ai siti web. Più in generale, il servizio consente di contrastare le infezioni da malware, di ridurre o calmierare gli effetti del phishing e dei ransomware. Il servizio è, altresì, in grado di regolamentare l'accesso a internet anche sui dispositivi che operano al di fuori della rete aziendale del cliente. Il servizio, caratterizzato da una soluzione basata sul cloud, consente un controllo e una protezione costante della navigazione internet anche in mobilità e una limitazione dell'accesso a internet per determinate categorie (white list e black list) e offre altresì report avanzati per l'analisi della sicurezza aziendale anche a disposizione dei clienti.

Cyber Security Suite

Cyberoo, grazie anche alle proprie competenze e conoscenze in termini di servizi di cyber security e delle differenti tipologie di minacce che si attestano sui clienti, ha sviluppato soluzioni proprietarie innovative di elevata affidabilità. A tal proposito, in aggiunta ai servizi sopra descritti e nell'ambito dei servizi di cyber security, l'Emittente offre servizi relativi a (i) **Cyber Security Intelligence ("CSI")** volti a proteggere i clienti dalle minacce esterne; e (ii) **Cypeer ("CY")**, funzionali alla garanzia della sicurezza interna dell'azienda.



Cyber Security Intelligence (CSI)

Cyber Security Intelligence (CSI) è il servizio di **Threat Intelligence** che, attraverso la raccolta e l'analisi di informazioni presenti nel deep e dark web, permette di avere una visione completa delle minacce esterne che riguardano la presenza sul web dell'azienda.

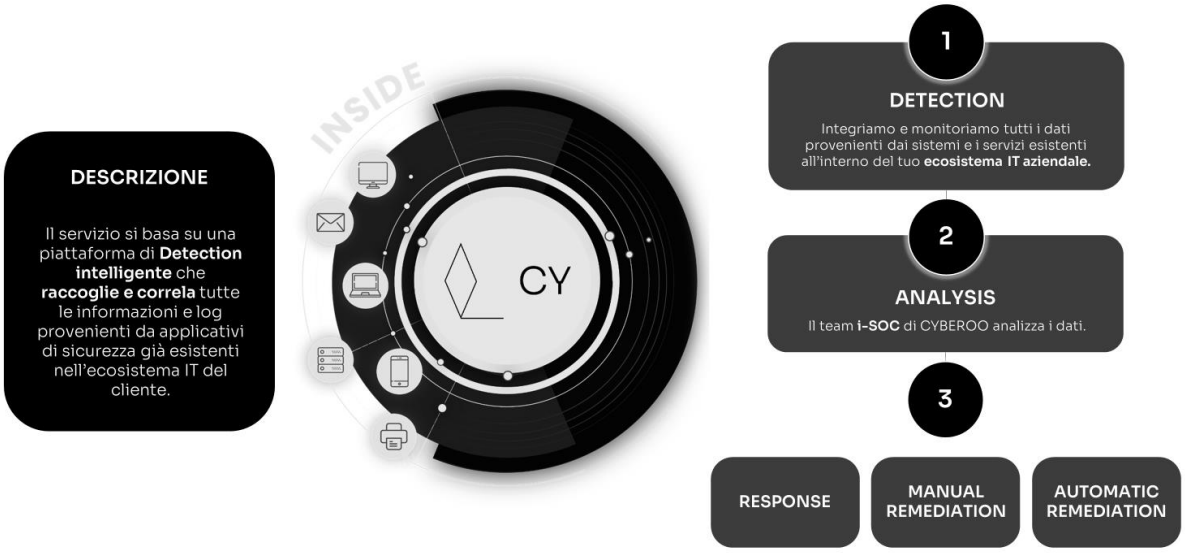
A svolgere il servizio è l'**I-SOC**, che si occupa di:

- verificare gli allarmi e abbattere i falsi positivi, grazie anche all'ausilio di processi automatizzati;
- definire i workaround per identificare un percorso di risoluzione delle problematiche rilevate;
- svolgere attività di OSINT (Open Source Intelligence) quali Data Breach & Data Leakage Identification, Brand Monitoring, Deep & Dark Web Analysis e VIP Users Protection.

CSI permette di accrescere la propria consapevolezza dei rischi e delle minacce dirette e indirette che possono impattare ogni realtà. L'i-SOC attivo H24 notifica infatti in near real-time le minacce individuate e le azioni necessarie volte a mitigare o evitare l'impatto. Grazie a ciò, è possibile prendere provvedimenti sulle proprie soluzioni in modo proattivo, contrastando il verificarsi di incidenti di sicurezza.

Questo servizio vanta la capacità di andare oltre a quelle che possono essere le minacce prettamente tecnologiche, ponendo l'attenzione anche e in particolar modo alle minacce di natura fraudolenta. Le informazioni raccolte ed elaborate da CSI sono secretate e disponibili solo agli utenti/sistemi autorizzati alla loro gestione: ogni accesso alle informazioni è dovutamente registrato e i log sono mantenuti secondo gli standard di sicurezza in materia e la normativa vigente.

Cypeer (CY)



Cypeer è un servizio basato su una piattaforma di detection intelligente, pensato per avere un quadro completo della postura di sicurezza IT dell'azienda da un punto di vista interno, allo scopo di prevenire minacce e attacchi al sistema.

Il servizio permette di aggregare e correlare tutti gli eventi generati dagli apparati di sicurezza già esistenti nell'ecosistema IT, consentendo di avere una visione specifica per ciascuna macchina o soluzione appartenente all'infrastruttura. Eventuali minacce rilevate sono poi prese in esame dall'i-SOC attivo in H24 e segnalate insieme alla remediation proposta per risolvere il problema stesso, grazie a:

- **INTEGRAZIONE CON SOLUZIONI DI SICUREZZA E INFRASTRUTTURA IT**: Cypeer può andare a integrare qualunque servizio di sicurezza, a patto che questo possa condividere le proprie informazioni attraverso log di sistema e simili.
- **CORRELAZIONE DEGLI EVENTI**: per tutte le fonti di dati agganciate a Cypeer, questo effettua attività di identificazione, correlazione e alerting di anomalie o attacchi cyber che vanno oltre alle capacità native dei singoli servizi.
- **DASHBOARD MULTITENANT PER UN ACCESSO COMPLETO AI DATI:** Cypeer dispone di dashboard multitenant per un accesso completo ai casi

in gestione da parte dell'i-SOC, allo scopo di avere una visione istantanea e pregressa della postura di sicurezza dell'ecosistema IT.

- **AUTOMATIC REMEDIATION:** Cypeer può attivare remediation automatiche a fronte di allarmi specifici o di condizioni predefinite.
- **REMEDIATION MANUALE:** Cypeer grazie alle persone che compongono il team di remediation e a un'istanza che non richiede gli accessi di amministratore di sistema sono in grando di intervenire direttamente con Playbook definiti sui sistemi dei clienti laddove non ci sia una catena del soccorso con presenza H24.

È proprio nella remediation che si distinguono *Cypeer Dek* e *Cypeer Sonic* e Cypeer Keera

Cypeer Dek permette ai clienti con limitazioni di budget ad accedere a un eccellente strumento di detection e analisi grazie all'I-SOC e poi implementa la remediation direttamente tramite catena del soccorso identificata sulla base degli schemi MITRE ATT&CK.

In **Cypeer Sonic** oltre agli elementi presenti in Cypeer Dek è possibile implementare automatismi di risposta tramite Playbook. Questo fa sì che l'Automatic Remediation sia senza limiti su tutte le tecnologie che offrono la possibilità di essere utilizzate tramite sistemi automatici (che forniscono API).

Cypeer Keera aggiunge alle funzionalità di Sonic anche la possibilità di avere un servizio di remediation Night & Weekend per effettuare attività di risposta alle minacce supportando una catena del soccorso 8x5, mentre la versione **Keera +** permette le attività di remediation H24.

Incident Response Team

Il Cyber Security Incident Repsonse Team è il servizio di Cyberoo che contrasta gli attacchi informatici critici in modo rapido ed efficace ed è erogato tramite un team di specialisti dell'Offensive Security disponibile 24 ore su 24, 7 giorni su 7, 365 giorni all'anno

Il team diretto da persone esperte nel campo dell'incident response stabilisce le priorità e le azioni da intraprendere e coordina le attività.

Il Cyber Security Incident Response Team interagisce con gli staff di altre unità o dipartimenti interni od esterni all'organizzazione, come ad esempio il management, l'ufficio legale, gli amministratori di rete e di sistema oppure consulenti e società esterne eventualmente chiamate a intervenire nella gestione dell'incidente.

Durante la gestione dell'incidente il Cyber Security Incident Response Team svolge le seguenti attività:

- Risposta iniziale all'incidente
- Investigazione dell'incidente in corso
- Supporto al ripristino dei sistemi compromessi
- Supporto agli adempimenti del GDPR

Incident Response Team Retainer

L'Incident Response Team Retainer Service di Cyberoo è un servizio di consulenza avanzata di pronto intervento al fine di contrastare attacchi informatici critici, contribuendo a proteggere la sicurezza e a supportare la ripresa delle attività aziendali eventualmente compromesse.

Erogato tramite il DFIR (Digital Forensic & Incident Response) team, il servizio è disponibile 24 ore su 24, 7 giorni su 7, 365 giorni all'anno e fornisce una risposta rapida e un supporto specialistico in caso di incidente informatico grave.

L'adozione dell'Incident Response Team Retainer per la risposta agli incidenti consente di beneficiare di una pianificazione e di un supporto per la protezione del business, dell'operatività e della reputazione aziendali.

Virtual Chief Information Security Officer (vCISO)

Il servizio di vCISO (Virtual Chief Information Security Officer) consente alle aziende di beneficiare di un team specializzato di esperti di sicurezza informatica, che in qualità di CISO virtuale, offrono una guida strategica per indirizzare le politiche di cybersecurity aziendale.

Il Team vCISO collabora strettamente con le risorse interne del cliente per sviluppare e implementare piani di sicurezza personalizzati, garantire la conformità alle normative vigenti e gestire la governance del rischio.

Questo servizio è particolarmente vantaggioso per le organizzazioni che richiedono una guida esperta e qualificata, senza dover ricorrere a una figura full-time, consentendo di ottimizzare i costi e di accedere a un supporto specializzato flessibile, che evolve in risposta alle minacce e alle esigenze in continua evoluzione.

Vulnerability Assessment

Il servizio di Vulnerability Assessment rappresenta il processo di definizione, identificazione e classificazione delle vulnerabilità nei sistemi informatici, delle applicazioni e delle infrastrutture di rete. Questo servizio fornisce una valutazione del rischio, migliorando la consapevolezza delle potenziali minacce al proprio ambiente e fornendo il background necessario per rispondere reagire in modo adeguato a tali rischi.

Il Vulnerability Assessment può essere suddiviso in due tipologie:

- **Interno**: si concentra sull'analisi della LAN (Local Area Network) e dei servizi erogati all'interno della rete aziendale. L'analisi della rete interna viene effettuata sull'infrastruttura locale, indicando gli indirizzi IP sui quali effettuare le analisi di vulnerabilità e gli URL esposti in Internet o nella rete interna.
- **Esterno**: si concentra sull'analisi alla rete perimetrale, esaminando le vulnerabilità presenti sulle appliance e sui servizi esposti pubblicamente sulla rete Internet, come i firewall, i server web, le applicazioni web e altri servizi di rete accessibili dall'esterno.

Penetration Test

Il Penetration Test (PT) è un'attività di valutazione tecnologica approfondita ed estremamente specialistica sulla sicurezza di un determinato asset, servizio o infrastruttura, volta a individuare vulnerabilità che potrebbero essere sfruttate durante un attacco da parte di un ente malevolo, sia questo una persona o un software e volta a testare i controlli che dovrebbero proteggere i sistemi IT da tali tentativi.

Risk Assessment

Il Risk Assessment è un'attività di individuazione e analisi dei rischi per comprendere le priorità di intervento e poi produrre azioni strategiche per contenerli o attenuarli.

Consente di fare delle previsioni sul rischio a livello di:

- Infrastruttura
- Network
- Cyber Security
- Compliance Privacy
- Advanced Persistent Threat

Managed services

Cyberoo, nell'esercizio della propria attività, svolge la funzione di ***Managed Security Service Provider (MSSP).*** I servizi ricompresi in tale linea di business sono riferibili a tre categorie principali: (i) *data center management*; (ii) *cloud management*; e (iii) *device management*.

Data center management

Il servizio di *data center management* prevede la gestione dei server, fisici o virtuali, degli apparati di rete (switch, router, firewall e fibre channel switch), nonché delle unità dischi (NAS e SAN) presenti all'interno di un centro dati. In particolare, il servizio prevede una gestione proattiva delle eventuali problematiche che possono verificarsi sia lato hardware sia lato software sui dispositivi gestiti, tramite degli interventi remoti o in locale.

Nell'ambito del servizio, Cyberoo offre altresì il servizio di *back up management*, ideato per garantire ai clienti una gestione completa dell'infrastruttura per il salvataggio dei dati e delle macchine virtuali, sia monitorando, controllando e gestendo l'intero processo di salvataggio dei dati, sia eseguendo le eventuali richieste di ripristino dei dati. Il servizio di back up management si caratterizza per il profilo della scalabilità, in quanto la soluzione realizzata è in grado di gestire sia le piccole imprese sia le imprese medie e grandi: il servizio, infatti, essendo tarato sulla effettiva quantità di dati da proteggere, è indipendente dal numero di dispositivi da salvare.

In aggiunta, Cyberoo ha ideato il servizio di *back up in cloud* al fine di garantire al cliente una maggiore affidabilità della salvaguardia dei dati aziendali e l'integrità degli stessi. Grazie a tale servizio, infatti, è possibile archiviare i dati salvati all'interno di un server sicuro, ospitato presso un centro dati. Il servizio comprende anche il controllo e il monitoraggio proattivo di tutto il processo di copia remota dei dati all'interno dello spazio disco remoto. Il software di backup fornito consente di salvare i dati in locale e poi replicarli in cloud al fine di conservarli, a seconda delle specifiche esigenze del cliente, per una, due o quattro settimane.

Cloud management

Cyberoo mette a disposizione dei propri clienti infrastrutture e applicazioni cloud che garantiscono altissimi livelli di performance grazie alle più avanzate tecnologie disponibili sul mercato. I *cloud services*, oltre a ridurre i costi di infrastruttura, consentono scalabilità e agibilità virtualmente illimitate, nonché un elevato grado di sicurezza e conformità.

In particolare, l'Emittente propone una soluzione Infrastructure as a Service (IaaS), erogabile secondo una duplice modalità:

- *cloud*, dove i dati e i servizi del cliente sono ospitati presso un data center, di proprietà di soggetti terzi, di primaria importanza nazionale (modalità indicata per aziende multi sede);
- *on premise*, dove i dati e i servizi sono ospitati in una infrastruttura locale all'interno della sede del cliente (modalità indicata per aziende di produzione o mono sede).

Device management

Cyberoo effettua la gestione e il monitoraggio utilizzando sistemi basati sull'intelligenza artificiale in grado di rilevare gli eventi di ogni dispositivo distribuito all'interno della rete del cliente, garantendone la massima efficienza operativa.

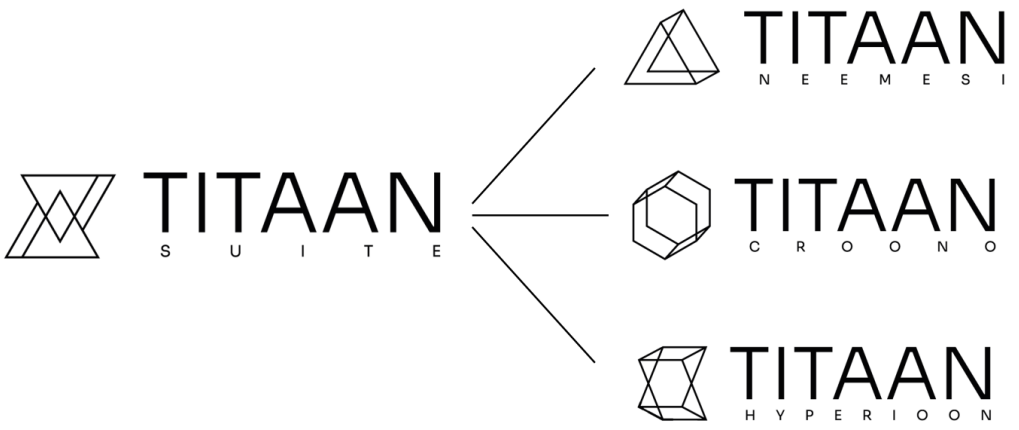
Il servizio di *help desk* (24 ore su 24, 7 giorni su 7) consente di avere un maggiore controllo delle postazioni, di monitorare lo stato hardware e software delle postazioni stesse e la gestione degli aggiornamenti dei sistemi e delle principali applicazioni.

Cyberoo, grazie a una esperienza pluriennale e una profonda conoscenza dei servizi riguardanti la gestione dell'ecosistema IT e del mercato degli strumenti di monitoraggio classici, ha ideato, sviluppato e registrato una soluzione innovativa, denominata **Titaan Suite**, che consente una gestione dei servizi ancora più efficiente utilizzando le conoscenze sull'intelligenza artificiale, deep learning e big data.

Titaan è un "*System behaviour analyser (SaaS)* ", ossia una piattaforma che supera il paradigma dei classici sistemi di monitoraggio basato sulle soglie statiche in quanto è in grado di identificare e prevenire le inefficienze sui sistemi, basandosi dunque non su soglie impostate dall'utente, ma sullo studio del comportamento della macchina stessa. Questo avviene attraverso complessi algoritmi di **Intelligenza Artificiale**, che imparano a identificare puntualmente comportamenti anomali, segnalando solamente reali problematiche e non i cosiddetti "falsi positivi".

Con una *dashboard user-friendly*, Titaan è in grado di prevenire le inefficienze sui sistemi e ridurre i costi. Oltre a identificare il problema, la suite è in grado di farne un'analisi causale, andando a individuare chi e come sta causando un malfunzionamento. È sempre tramite gli algoritmi di IA che Titaan consente di fare un'analisi predittiva fino a 8 settimane sul dimensionamento delle macchine ed eventuali anomalie.

Il servizio Titaan offerto è disponibile in tre differenti versioni: (i) Titaan Neemesi; (ii) Titaan Croono; e (iii) Titaan Hyperioon.



Titaan Neemesi

Titaan Neemesi è il modulo che ha lo scopo di mantenere la compliance all'interno dell'infrastruttura IT.

Nello specifico si compone di cinque application: Admin Log, Log Extra AD, Best Practice Analyzer e Active Directory Report.

Il modulo è stato sviluppato con l'obiettivo di:

- garantire la compliance al GDPR e l'inalterabilità del dato e dei log raccolti grazie alla tecnologia Blockchain;
- identificare eventi che si verificano su Active Directory;
- identificare e fornire le Best practice per il GDPR, procedure di certificazione e compliance;
- evitare cali di prestazioni, scarsa affidabilità, conflitti e problemi di sicurezza;
- identificare problemi specifici su alcuni dei più importanti componenti aziendali, politiche di login, permessi, ruoli, sistemi operativi, unità organizzative.

Titaan Nemesi ha la possibilità di aggiungere anche tre add-on:

- Whistleblowing: consente ai dipendenti di fare segnalazioni anonime a fronte di comportamenti non etici all'interno dell'azienda;
- File Integrity: consente di sapere che cosa accade ai file aziendali, chi ne ha accesso, al fine di proteggere il know how aziendale;
- NIS2: fornisce e consente il monitoraggio e l'analisi dei sicurezza necessarie per supportare la compliance NIS2.

Titaan Croono

Titaan Croono è il modulo che rappresenta **l'inventario degli asset di rete dell'infrastruttura aziendale**. Individua gli apparati di rete e i nodi che sono più carichi a livello di throughput dei dati permettendo di evitare i colli di bottiglia delle prestazioni e di recuperare e redistribuire le risorse hardware in base al carico effettivo. È in grado di disegnare automaticamente la topologia della rete e monitorarne l'hardware. Offre, inoltre, una reportistica omnicomprensiva di tutti gli asset di rete e delle relative informazioni.

Titaan Hyperioon

Titaan Hyperioon è il terzo modulo della Titaan Suite ed è la soluzione di Observability per infrastrutture On-Premise, Hybrid e Cloud.

È il concentratore di ogni informazione inerente a log e metriche di sistema: Hyperioon, infatti, integra e correla dati da oltre 200 fonti, garantendo una gestione immediata delle problematiche. Tramite l'Intelligenza Artificiale, è in grado di individuare deviazioni dal comportamento usuale dell'ecosistema IT e inviare alert proattivi, consentendo così di aumentare la velocità di risoluzione delle problematiche.

Digital transformation

Cyberoo, mediante l'offerta di servizi di digital transformation, ha lo scopo di portare il valore e l'integrazione della tecnologia digitale in tutte le aree di un'azienda, cambiando radicalmente il modo in cui esse operano, apportando valore ai clienti e supportandone il cambiamento culturale.

I servizi di digital transformation comprendono le seguenti soluzioni:

- **CRM (Customer Relationship Management)** è un software manageriale, strategico ed operativo, che pone il cliente al centro della propria azienda e che porta straordinari benefici al proprio business. In particolare, CRM consente di creare un'efficace pianificazione, gestione e monitoraggio di tutte le attività legate ai clienti. Su ogni modulo è possibile impostare dei processi automatizzati per aumentarne l'efficienza, soprattutto se la mole di dati inseriti viene aggiornata frequentemente. Tale software permette altresì di personalizzare le relazioni con i propri contatti, creare comunicazioni ed attività mirate e sviluppare, conseguentemente, l'offerta che meglio soddisfa le particolari esigenze di ciascun interlocutore in tempi rapidi.
- **HRM (Human Resources Management)** è un software ideato al fine di supportare l'attività quotidiana di ciascun dipendente e dell'intera azienda, garantendo risultati immediati ed elevate prestazioni in termini di ottimizzazione. L'applicativo è in grado di gestire in maniera efficiente le presenze in azienda, le entrate/uscite dei dipendenti, le richieste ferie e/o

permessi, i processi di rimborso spese. Inoltre, il software può includere al suo interno dei moduli per l'assegnazione dei compiti di progetto, con conseguente misurazione della performance individuale per dipendente e reportistica sulle performance di lavoro. HRM aiuta altresì gli ospiti a connettersi alla rete wifi aziendale in modo autonomo e consente di creare una sezione dove scambiare documenti fra colleghi.

- **PMS (Product Management System)** è una soluzione che consente alle aziende di organizzare puntualmente i dati dei propri prodotti, accentrandoli in un unico sistema per renderli disponibili e fruibili. Le funzionalità di integrazione con gestionali e software aziendali rendono il PMS uno strumento con un'interfaccia strutturata, che automatizza i processi di gestione, ricerca, estrapolazione, raccolta e pubblicazione su più canali aziendali (website, B2B, B2C) dei dati relativi ai diversi prodotti e servizi commercializzati.
- **C51 CheckIn** è una soluzione ideata per gestire l'accesso e l'accoglienza dei visitatori in reception in modo organizzato e automatizzato, tutelando le esigenze di sicurezza. Allo stesso tempo tale soluzione migliora l'immagine aziendale, contribuendo a garantire l'idea di un'azienda all'avanguardia. Tale applicativo consente quindi di controllare i flussi di accesso in azienda con modalità innovative, (tramite app). Inoltre, mediante tale soluzione, l'ospite ha altresì la possibilità di visionare l'informativa aziendale sulla privacy aziendale, al fine di tutelare la sua sicurezza e la sua permanenza in azienda.
- **C51 Events** è l'applicativo pensato per migliorare e ottimizzare la gestione di eventi in presenza. Disponibile sia per mobile che versione web, aiuta a concentrare tutte le attività necessarie per l'organizzazione in un unico spazio e a rendere perfetto l'evento.
- **C51 Commerce** è la piattaforma proprietaria per siti e-commerce di Cyberoo51 in grado di adattarsi alle specifiche esigenze di ognuno dei suoi clienti, integrando i loro processi aziendali e creando per ognuno un design unico e completamente personalizzato. Consente di gestire i portali di vendita online, sia B2B che B2C, con un sistema multipiattaforma e multilingua che guida l'utente nel suo processo di acquisto.
- **Digital marketing**: comprende tutte le attività di marketing di un'azienda volte a sviluppare la propria rete commerciale, analizzare i trend di mercato,

prevederne l'andamento e creare offerte nel profilo del cliente target, con lo scopo di commercializzare beni o servizi, aumentare clienti e rafforzare il proprio brand (ad esempio: *SEO, social media marketing, web advertising, web marketing, web design, e-commerce*).

- **App mobile**: comprende la progettazione, lo sviluppo, la realizzazione e la manutenzione di applicazioni mobile per dispositivi iOS e Android, utili per la comunicazione interna ed esterna alle aziende, consentendo l'interazione tra gli utenti in qualsiasi luogo e momento in modo semplice.
- **AMY:** un sistema integrato basato sull'Intelligenza Artificiale (IA) progettato per assistere, migliorare ed evolvere il lavoro quotidiano dei dipendenti in ogni settore d'impiego.

Capitolo 2

GOVERNANCE

GOVERNANCE
OVERVIEW

SGI ISO 27001

Sistema di Gestione Integrato per la Qualità
e la Sicurezza delle Informazioni (SGI)

NESSUNA SANZIONE

Nessuna sanzione e/o contenzioso
in essere in materia ambientale,
sociale ed economica

2. Governance

La gestione responsabile d'impresa

Cyberoo crede fermamente che la definizione di specifiche procedure che regolano la gestione dell'impresa orientate alla creazione di valore condiviso sia fondamentale per perseguire la crescita sostenibile della società.

Grazie alla spinta dei vertici del Gruppo nell'adottare strategie sempre più orientate alla sostenibilità, Cyberoo tramite il presente Bilancio di Sostenibilità ha l'obiettivo di implementare l'attività di comunicazione esterna al fine di incentivare una trasparente, puntuale e accurata informazione agli *stakeholder* relativamente agli sviluppi strategici e operativi.

Cyberoo è determinata ad assicurare la massima correttezza nella conduzione dei propri affari e delle relative attività aziendali, anche a tutela della propria immagine e reputazione: per questo motivo nel corso del 2025 è stata prevista l'adozione del Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001.

La governance

Cyberoo adotta il sistema di governo tradizionale costituito dai seguenti organi sociali:

- l'**Assemblea degli Azionisti** (competente a deliberare in ordine alle materie previste dalla legge e dallo Statuto sociale);
- il **Consiglio di Amministrazione** (a cui è affidata la gestione della Società);

L'attività di **revisione legale** dei conti è stata affidata a BDO Italia S.p.A., nominata in data 29/04/2022. Tale incarico è conferito fino all'approvazione del bilancio al 31 dicembre 2024.

All'approvazione del bilancio al 31 dicembre 2024, in occasione dell'assemblea del 28 aprile 2025, sono state rinnovate le cariche dell'intero Consiglio di Amministrazione, del Collegio Sindacale[1] e della Società di Revisione.

[1] È stato nominato Luciano Volta come Sindaco supplente al posto di Mariangela Rossetti.

Il Consiglio ha designato Massimo Bonifati nella carica di Presidente.

Consiglio di Amministrazione	Massimo Bonifati	Fabio Leonardi	Davide Cignatta	Veronica Leonardi	Riccardo Pietro Leonardi	Renzo Bartoli	Alessandro Viotto
Funzione	Presidente	Consigliere	Consigliere	Consigliere	Consigliere	Consigliere indipendente	Consigliere indipendente
Esecutivo / Non esecutivo	Non esecutivo	Esecutivo	Esecutivo	Esecutivo	Non esecutivo	Non esecutivo	Non esecutivo
Altre posizione rivestite nel Gruppo Cyberoo e/o esternamente	-	C.E.O Cyberoo S.p.A.	Sales Director	C.M.O. Cyberoo S.p.A.	-	-	-

Il Consiglio di Amministrazione è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, con la facoltà di compiere tutti gli atti che ritenga opportuni per il raggiungimento dell'oggetto sociale, esclusi quelli che la legge riserva all'Assemblea.

Nel 2024 la società ha rinominato il Responsabile della Protezione dei Dati (RPD o DPO) ai sensi dell'art. 37 del Regolamento UE 2016/679 (GDPR).

Consiglio di Amministrazione – Diversità (genere – classi di età)					
Donne		Uomini		Totale	
Nr	%	Nr	%	Nr	%
4	21%	15	78%	19	100%
Minori di 30 anni		Tra 30 e 50 anni		Maggiori di 50 anni	
Nr	%	Nr	%	Nr	%
-	-	10	53%	9	47%

Il Collegio Sindacale, nominato dall'assemblea del 29 aprile 2022, rimarrà in carica sino all'Assemblea che approverà il bilancio di esercizio al 31 dicembre 2024 ed è composto da 3 membri effettivi e 2 supplementari.

Collegio Sindacale	Gianluca Settepani	Rita Sciaraffa	Alberto Ventura	Mariangela Rossetti	Claudia Peri
Funzione	Presidente	Sindaco effettivo	Sindaco effettivo	Sindaco supplente	Sindaco supplente
Esecutivo / Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo
Altre posizione rivestite nel Gruppo Cyberoo e/o esternamente	-	-	-	-	-

Collegio Sindacale – Diversità (genere – classi di età)					
Donne		Uomini		Totale	
Nr	%	Nr	%	Nr	%
3	60%	2	40%	5	100%
Minori di 30 anni		Tra 30 e 50 anni		Maggiori di 50 anni	
Nr	%	Nr	%	Nr	%
-	-	2	40%	3	60%

Assetto organizzativo

L'assetto organizzativo esprime il sistema di funzioni, poteri, deleghe, processi decisionali e procedure aziendali e fornisce una chiara individuazione dei compiti e delle responsabilità di ciascuno rispetto alle attività aziendali.

La struttura organizzativa del Gruppo Cyberoo è fortemente improntata a fornire una governance della Società, oltre che a definire i principi dell'organizzazione aziendale, della gestione dei processi e delle risorse.

I sistemi di gestione

L'Azienda ha istituito un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni (SGI), inteso come sistema per garantire e migliorare la qualità dei processi aziendali, in conformità ai requisiti della norma **ISO/IEC 27001:2022**.

Il Sistema di Gestione, implementato da Cyberoo, si basa sulla gestione e il governo dei suoi processi primari di business (progettazione, realizzazione ed erogazione dei servizi di cybersecurity e monitoraggio Infrastrutture IT) e sulle relative attività che hanno influenza sulle prestazioni aziendali.

Il Sistema di Gestione (SGI) è costituito dall'insieme di responsabilità, procedure, attività, strutture e risorse predisposte per realizzare la Politica per la Qualità e Sicurezza delle Informazioni nel modo più efficace possibile e per garantire al massimo la sicurezza, integrità e disponibilità delle informazioni, ottenendo al tempo stesso un continuo miglioramento.

Al fine di mettere in atto il SGI, l'Azienda ha:

- identificato e documentato i processi operativi;
- stabilito le sequenze e le interazioni tra i processi;

- individuato gli elementi in ingresso (input), gli elementi in uscita (output) per ogni attività aziendale, le responsabilità e i documenti di riferimento;
- individuato i punti di controllo per ogni processo;
- individuato le interfacce e i requisiti di sicurezza dei fornitori esterni (contenuti in appositi documenti contrattuali o attraverso audit eseguiti da Cyberoo).

In ottica di migliorare sempre di più la qualità dei processi, e dunque dei servizi erogati, Cyberoo ha in previsione per i prossimi anni – essendo una delle attività core aziendali – di ottenere la certificazione secondo lo schema **ISO 27035**, relativo alla gestione degli incidenti informatici. Per raggiungere questo obiettivo, si è avviato un primo assessment ed è già stato disegnato il processo di Gestione degli Incidenti.

.

Capitolo 3

CAPITALE INFRASTRUTTURALE

CAPITALE INFRASTRUTTURALE
OVERVIEW

OLTRE 80

Accordi di partneship su tutto
il territorio nazionale

Gartner®

Global “Representative Vendor 2024”
in Italia dei servizi di cybersecurity

3. Capitale infrastrutturale

Innovazione e digitalizzazione

Cyberoo, attenta all'evoluzione tecnologica e in ottica di miglioramento continuo, sta procedendo con un massiccio lavoro di **ottimizzazione dei processi interni**: partendo dall'analisi dei punti di forza e debolezza di ogni entità aziendale, sono stati disegnati nuovamente i flussi operativi delle varie business unit secondo modello BPM[2], consentendo così di avere ben chiaro il risultato di ogni fase. Sono state aggiornate e condivise le matrici RACI, per esplicare ancor meglio la correlazione delle responsabilità. La Direzione Aziendale, attenta a questi temi, ha deciso inoltre di finanziare la formazione sulla metodologia Lean[3] e Six Sigma[4] nel corso del 2023, così da poter raggiungere risultati ancora migliori – in ambito di ottimizzazione dei processi – riducendo gli "sprechi" interni e, dunque, poter ottenere una maggiore qualità del servizio e del supporto erogato all'esterno. Il 2024, per concludere, è stato l'anno di applicazione di queste nuove metodologie per raggiungere gli obiettivi di qualità ed eccellenza che il gruppo persegue.

I progetti

Cyber Security Suite

La Cyber Security Suite è composta da CSI (Cyber Security Intelligence) e Cypeer.

La Soluzione CSI è composta dalla sinergia di diversi servizi volti a identificare nel web (clear, dark e deep) tutti i segnali che possano far supporre che vi è un'attività propedeutica alla violazione della cyber-sicurezza delle realtà monitorate o che vi è stato un attacco e quali servizi/informazioni sono stati colpiti. CSI sfrutta l'accesso a informazioni pubbliche analizzandole mediante complessi algoritmi di navigazione e di estrapolazione semantica del contenuto di informazioni presenti

[2] BPM: Business Process Modeling

[3] Lean: un sistema di produzione che, riducendo gli sprechi fino a eliminarli, mira alla qualità totale;

[4] Six Sigma: approccio metodologico, rigoroso e fortemente strutturato orientato al miglioramento radicale dei processi in termini di performance e robustezza.

nel web, nel dark e deep web per ottenere una serie di informazioni relative alla sicurezza dall'azienda cliente.

Di seguito vengono descritti sinteticamente i diversi servizi che compongano la soluzione e le funzionalità operative ad essi associati che sono disponibili al termine delle attività implementative della soluzione.

1 – Servizio CSI di Data Breach

Il servizio di Data Breach si pone l'obiettivo di mostrare al cliente una visione completa dello stato di compromissione delle credenziali relative alla propria realtà. Per effettuare questa attività vengono utilizzate conoscenze e servizi che effettuano la raccolta di tutte le credenziali apparse pubblicamente online. Tale raccolta include anche le credenziali non rilasciate pubblicamente, ma vendute o diffuse nei Black Market online dagli autori della compromissione.

2 – Servizio CSI di Domini Malevoli

Gli agenti malevoli che effettuano attacchi a utenti e società, con lo scopo di trarre del profitto con attività illecite, devono preparare l'ambiente necessario affinché il loro attacco vada a buon fine. Questo ambiente deve necessariamente attestarsi pubblicamente in Internet, poiché questa tipologia di attacco viene effettuata completamente da remoto.

Il fattore comune di molteplici tipologie di attacco, ad esempio attacchi come Phishing, Spear Phishing, CEO Fraud, IT Fraud, Malware campaign ecc., consistono nella registrazione di domini web afferenti all'obiettivo dell'attacco. Se l'obiettivo dell'attacco è una società o un'azienda, gli attaccanti con l'intenzione di perpetrare un attacco come quelli di cui sopra, effettueranno molto probabilmente delle registrazioni di dominio con nomi simili a quelli utilizzati legittimamente dalla società. Il servizio si propone di analizzare tutti i domini recentemente registrati a livello mondiale al fine di identificare quelli che potrebbero essere stati registrati per effettuare, di lì a breve, attività malevole ai danni dei Clienti. Questo servizio effettua un'analisi dei domini registrati nelle ultime 24 ore su un notevole numero di Generic Top-Level Domains (gTLD), ossia tutti i domini utilizzabili per la registrazione di domini web (es: .it, .com, .org, .net, .eu, ecc). Il servizio effettua un'analisi della somiglianza dei domini registrati con i domini dei Clienti sotto monitoraggio. Se la somiglianza supera una certa soglia, viene inviata una notifica a MSS che si opererà per analizzare il dominio sospetto e, se le analisi avranno dato

riscontro positivo, attuare le procedure necessarie per implementare attività mitigative prima dell'accadimento dell'attacco.

3 – Servizio CSI di Early Warning

Ogni giorno vengono identificate da parte di ricercatori e società di ricerca nuove vulnerabilità e problematiche che possono impattare sulla postura di sicurezza cyber di qualunque ente, società o azienda. Mantenersi aggiornati sugli ultimi ritrovamenti in materia di cybersecurity non è semplice e, in particolar modo, risulta ancor più ostico scremare tutte le informazioni con lo scopo di identificare solo quelle realmente utili per la propria realtà aziendale. Il servizio sviluppato si pone l'obiettivo di fornire al Cliente evidenza delle ultime notizie in ambito cybersecurity focalizzandosi specificatamente sulla realtà del Cliente. Tale specificità viene concordata con il Cliente stesso nel momento dell'attivazione del servizio e può integrare diverse aree di competenza. L'attività viene eseguita in modo automatico facendo uso di funzionalità atte alla raccolta, categorizzazione e visualizzazione delle informazioni.

4 – Servizio CSI di Deep Analysis

Molte informazioni di forte interesse per l'area di cybersecurity non vengono rese pubblicamente disponibili dato il loro valore di mercato in questo ambito. Informazioni come gravi vulnerabilità di sistemi molto diffusi, informazioni trafugate illegittimamente contenenti dati personali come username e password o le modalità per l'accesso non autorizzato a sistemi privati non vengono rese pubbliche, ma esistono, e possono essere recuperate sotto certe condizioni.

I vantaggi che offre la piattaforma ai propri clienti sono:

- UP TO DATE NUOVE MINACCE: l'I-SOC di Cyberoo è costantemente attivo sull'analisi del deep e dark web allo scopo di scovare informazioni rilevanti per la sicurezza e per rimanere aggiornati sulle più recenti tecniche di hacking;
- ROOT CAUSE ANALYSIS: circoscrive il problema, basandosi sulla correlazione di una o più metriche. Monitora i valori presupposti di quelle metriche, e i valori attuali. Individua chi e come sta causando un mal funzionamento;
- ELIMINAZIONE DEI FALSI POSITIVI: grazie al lavoro di intelligence e correlazione effettuato dai Cyber security specialist, il cliente viene allertato

solo in caso certo di minaccia, eliminando il tempo perso nell'analisi di falsi positivi;

- COMPETITIVITÀ VERSO OGNI BUSINESS: pur avendo una tecnologia all'avanguardia, il nostro modello di mercato ci permette di essere accessibile anche alle realtà più piccole.

Le principali attività R&S svolte nell'ambito del progetto sono riconducibili alle seguenti:

1. analisi dei requisiti/modello e flussi (con Key Users);
2. progettazione dell'architettura e algoritmi;
3. implementazione del codice del programma prototipo (con sviluppo sperimentale);
4. test e prove su versione prototipale Alfa e Beta (con Key Users).

5- Servizio CSI di OSINT Social

All'interno della Cyber Security Suite, la componente CSI è stata potenziata con l'introduzione di **nuovi moduli di raccolta e analisi OSINT** orientati alla profilazione e tracciabilità di soggetti e asset digitali.

Tra i nuovi strumenti integrati:

- **Profilazione cross-platform**: moduli che raccolgono e aggregano automaticamente le tracce digitali associate a un determinato username o dominio, identificando la presenza su social network, piattaforme professionali, repository di codice e marketplace. Questa funzionalità consente una ricostruzione approfondita della footprint digitale del soggetto analizzato.
- **Crawling mirato per info-leak e metadati**: attraverso motori ad hoc, il sistema è in grado di recuperare informazioni pubblicamente accessibili (ma non indicizzate nei motori tradizionali) come indirizzi e-mail, IP correlati, nomi utente e contenuti testuali associabili a potenziali violazioni.
- **Moduli di enrichment automatico**: i dati raccolti vengono incrociati con fonti OSINT e pubblici registri per arricchire le evidenze e attribuire contesto, con l'obiettivo di supportare analisi più accurate e azioni tempestive.

L'integrazione di questi moduli rafforza ulteriormente la capacità investigativa della piattaforma CSI, rendendola uno strumento completo per l'intelligence proattiva e la risposta alle minacce emergenti.

Cypeer rappresenta la Soluzione MDR (Managed Detection and Response). Ad oggi Cypeer è l'unica Soluzione MDR Italiana riconosciuta da Gartner ed inserita nella Gartner Market Guide. La Soluzione Cypeer è in grado di raccogliere e normalizzare tutte le informazioni relative a diverse fonti dato, con lo scopo di identificare minacce o attacchi già presenti impattanti sulla postura cyber di sicurezza del Cliente. Tra le principali caratteristiche, che distinguono inoltre la Soluzione tra quelle di mercato, vi è una approfondita gestione delle informazioni e la capacità di correlazione orizzontale tale per cui il sistema è in grado di elevare le potenzialità e le capacità identificative delle singole soluzioni che rappresentano per Cypeer le fonti dato, nonché fungere da osservatore super partes in grado di correlare eventi relativi a diverse entità. La Soluzione CSI permette di rendere automatizzabile un'attività di per sé complessa e che richiede una capacità di identificazione e reazione specifica per ogni evento. Tramite questa Soluzione il team di Cybersecurity è in grado di fornire al Cliente una visibilità approfondita e gestita di quelle che sono le minacce che potrebbero tramutarsi in impatti per le proprietà di sicurezza di dati e servizi afferenti al Cliente stesso.

Inoltre, la Soluzione prevede un portale di *Case Handling*, il quale, permette al Cliente di avere piena trasparenza delle attività in carico ai vari livelli di SOC che gestiscono la Soluzione. Tramite il portale si palesa la capacità di correlazione degli allarmi basata sulle entità degli stessi. Tali allarmi, vengono quindi raccolti in Case e dai SOC analizzati.

Infine, la Soluzione mette a disposizione una tecnologia di automatic remediation agnostica che è in grado, sulla base di condizioni definite, di eseguire autonomamente attività volte a mitigare o bloccare gli attacchi in corso direttamente sui sistemi coinvolti del cliente.

Per lo sviluppo del progetto sono stati adottati algoritmi e modalità tali per cui risulta possibile alla Intelligenza del sistema identificare automaticamente minacce non altrimenti identificabili, tramite l'implementazione di metodologie proprietarie. L'architettura, le logiche e le modalità di funzionamento delle

soluzioni sono state completamente ideate durante il processo di definizione del progetto e implementazione.

La soluzione è stata completamente sviluppata in "Cloud" garantendo elevati livelli di affidabilità sfruttando sistemi di ridondanza e controllo delle informazioni in essa gestite. Inoltre, tali informazioni sono secretate e disponibili solo agli utenti/sistemi autorizzati alla gestione di queste. Ogni accesso alle informazioni è dovutamente registrato e i log sono mantenuti secondo gli standard di sicurezza in materia. Obiettivo principale del progetto è stato quello di implementare una soluzione che potesse portare su un cliente, di qualunque dimensione e competenze strutturali in ambito IT, un prodotto completamente gestito in h24 dagli specialisti Cyberoo (esternalizzando quindi la competenza).

Titaan

Al momento sul mercato esistono sistemi di monitoraggio che si basano su un paradigma detto "Supervised". I software tradizionali, come Nagios, si affidano a regole e soglie/ threshold. La conseguenza è che questi sistemi non sono in grado di discernere tra picchi di carico abituali (si pensi agli aggiornamenti) e quelli realmente anomali. Il progetto mira allora a sviluppare un sistema di monitoraggio totalmente innovativo basato su logica "unsupervised".

La piattaforma Titaan è un innovativo servizio di monitoraggio in real time dell'infrastruttura informatica di un'azienda, dei suoi servizi e delle sue applicazioni che permetta di garantire la Business continuity all'interno delle infrastrutture aziendali con un approccio "unsupervised" che permetta di superare le limitazioni dei tradizionali sistemi "supervised" I principali contenuti innovativi derivano dall'utilizzo delle tecnologie di Machine Learning e Intelligenza Artificiale che si è scelto di utilizzare perché sono le uniche in grado di lavorare in un vantaggio competitivo rispetto alla concorrenza maniera proattiva e in grado di generare previsioni analizzando in tempo reale elevati volumi di dati (big data). In aggiunta, per ogni macchina sotto monitoraggio, si genera un modello di comportamento tailor-made della macchina, che consente di identificare tutte quelle stranezze che i normali software non sono in grado di riconoscere. Titaan, in maniera disruptive, identifica le anomalie prima che diventino un problema e circoscrive la causa prima che il Team del cliente debba effettuare un'analisi.

A complemento delle funzionalità predittive e real time di Titaan, è stato sviluppato un **modulo avanzato di monitoraggio eventi conforme alla direttiva NIS2**. Il modulo consente un controllo capillare su eventi di sicurezza, processi di sistema e accessi, offrendo visibilità dettagliata sulle attività a livello endpoint, server e infrastruttura di rete.

Questa integrazione rappresenta un'evoluzione nella capacità della piattaforma di anticipare minacce e supportare attività di forensic analysis, garantendo tracciabilità completa degli eventi significativi all'interno dell'ambiente monitorato. Il modulo adotta una struttura di regole dinamiche e un motore di correlazione che consente l'identificazione automatica di pattern sospetti o anomali, minimizzando il tasso di falsi positivi e ottimizzando le attività di response.

La piattaforma permette di ottenere i seguenti vantaggi rispetto alla concorrenza:

- ELIMINAZIONE DEI FALSI POSITIVI: Titaan non utilizza regole o soglie preimpostate, bensì sfrutta le più avanzate tecnologie dell'Intelligenza Artificiale con il risultato di riuscire a intercettare le anomalie certe, che non siano falsi positivi. Ciò riduce significativamente la mole di notifiche giornaliere che i sistemi tradizionali inviano ai responsabili IT e per le quali è stato stimato che, per la maggior parte, si tratta di falsi positivi. Indirizzando il dipartimento IT direttamente verso le reali anomalie dei propri sistemi;
- PROATTIVITÀ: Titaan individua l'inizio del degrado dei sistemi con uno scarto di pochi secondi;
- VISIBILITÀ INTEGRATA IN UN'UNICA DASHBOARD: Titaan riunisce tutti i log e dati di monitoraggio in un unico pannello, per cui i tecnici IT non dovranno continuamente cambiare da un'interfaccia all'altra per avere una visione a 360° sulla propria infrastruttura;
- COMPETITIVITÀ: pur sfruttando tecnologie avanzate nel campo dell'Intelligenza Artificiale, il sistema permette di essere accessibile anche alle realtà medio-piccole;
- MONITORAGGIO IN TEMPO REALE;
- MONITORAGGIO PREDITTIVO: Titaan effettua previsioni fino a 2 mesi permettendo il giusto dimensionamento dei sistemi business critical.

Reos

Reos è un software di time tracking e reportistica pensato per aziende del comparto SMB ed enterprise. Scopo primario del software è aiutare i decisori aziendali a capire quali tipi di software vengono utilizzati in azienda all'interno delle varie Business Unit e con quali modalità di fruizione.

La soluzione monitora il tempo speso dalle risorse in relazione a:

- navigazione web;
- software utilizzati;
- tempo di utilizzo dei device aziendali;
- classificazione automatica del tempo speso.

La soluzione è pensata per ottimizzare fortemente la produttività delle risorse aziendali, sia mentre sono in sede sia mentre sono in telelavoro e/o in regimi di orario flessibile. Il software risponde a tutti i requisiti fondamentali che riguardano i moderni applet di time tracking. L'utente ha la possibilità di vedere la propria reportistica in merito all'utilizzo del tempo, in questo modo può rendersi conto in autonomia di quali abitudini è possibile modificare per migliorare la propria produttività.

Gli elementi di particolare innovazione sono dati dall'utilizzo di due algoritmi di Machine Learning che sono stati utilizzati per specifiche applicazioni e sono risultati più efficienti rispetto a tutti gli algoritmi esistenti sul mercato.

Progetto generalista B2B/B2C

Nell'ambito degli archivi digitali i metadati sono le informazioni di cui bisogna dotare il documento informatico per poterlo correttamente formare, gestire e conservare nel tempo.

Il documento informatico è infatti privo della componente materiale costituita dalla carta ed è memorizzato in sistemi che contengono moltissimi oggetti digitali; per poter essere conservato, reso accessibile nel tempo, e per poter essere correttamente inserito nel suo contesto, deve essere posto in relazione a un insieme di informazioni che lo descrivano a vari livelli. La normativa italiana prevede alcuni metadati minimi che devono essere associati al documento informatico come per esempio: la data di chiusura, l'oggetto, il soggetto produttore, ecc.

Tutti questi elementi servono per attribuire al documento un'identità ben precisa.

Al fine di poter sviluppare un *marketplace* che possa essere adattato a ogni settore, si è pensato di realizzare uno speciale schema di database che racchiude i metadati che sia facilmente adattabile alle esigenze di vari clienti e permetta di realizzare la complessità e l'architettura dei dati attualmente implementati con singole personalizzazioni. Le attività di R&S sono finalizzate alla progettazione e allo sviluppo sperimentale di tabelle multidimensionali di associazione che permettono di associare un insieme definito di metadati a una molteplicità di prodotti

È stata studiata una particolare architettura di dati che permette di velocizzare la risposta alle query di sistema mediante viste che si possono aggiornare rapidamente. In tal modo si ha la flessibilità di una vista e la consistenza e integrità del dato di una tabella. La soluzione proposta è l'unica sul mercato che permetta di personalizzare in modo semplice ed efficiente la struttura dei metadati per ogni tipologia di prodotto in vari settori. La tecnologia che si vuole sviluppare è innovativa per il settore dell'e-commerce business in quanto al momento tutte le piattaforme utilizzano DB relazionali personalizzati per singolo progetto e non hanno una struttura facilmente configurabile dall'utente e valida in varie situazioni applicative. I principali contenuti innovativi sono dati dallo studio e sperimentazione di innovativi algoritmi non esistenti sul mercato, basati su tecnologie di Machine Learning e Intelligenza Artificiale che permettono di analizzare in tempo reale grande quantità di dati e di supportare il decision maker in base alla valutazione dei rischi in real time.

Il valore delle partnership

Cyberoo vende i suoi servizi sul mercato in via indiretta, costruendo e consolidando un importante network di partner a valore aggiunto in Italia e all'estero, che permette di presidiare in modo capillare tutto il territorio italiano e internazionale.

Tale modello di business adottato consente un rapporto *win-win* che permette:

- ai partner, grazie a Gruppo Cyberoo, di riuscire a fornire dei servizi evoluti di cyber security che diversamente farebbero fatica a proporre ai clienti;
- al Gruppo Cyberoo di raggiungere velocemente il cliente finale tramite un rapporto già consolidato tra il partner e l'end-user.

Ad oggi Cyberoo può contare su un contratto di distribuzione nazionale e oltre 80 contratti di partnership a valore aggiunto che permettono di coprire l'intero territorio italiano.

Di seguito, vengono elencati alcuni dei principali partner con cui il Gruppo Cyberoo collabora nella sua attività:

NPO Torino S.r.l.	**Euro Informatica S.p.A.**
Zerouno Informatica S.p.A.	**Cyber-Bee-R1 S.p.A.**
Magnetic Media Network S.p.A.	**WindTre S.p.A.**
NPO Sistemi S.r.l.	**Retelit Digital Service S.p.A.**
Ergon S.r.l.	**Eurosystem S.p.A.**
Vidata S.r.l.	**Reti S.p.A.**

Inoltre, nel corso del 2024 Cyberoo ha ampliato le sue operazioni internazionali con altre sei partnership in Polonia sotto riportate.

- VERNITY SP. Z O.O
- ASCOMP SA.
- SPRINTTECH SP. Z O.O.
- XCOMP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SP. K.
- AIRO S.R.O.

- SEVENET S.A.

L'azienda ha la possibilità di supportare i clienti e i partner con maggior facilità, avendo asset e personale in loco. I clienti ricevono un supporto diretto e da un servizio 24/7 svolto da personale che parla la loro lingua.

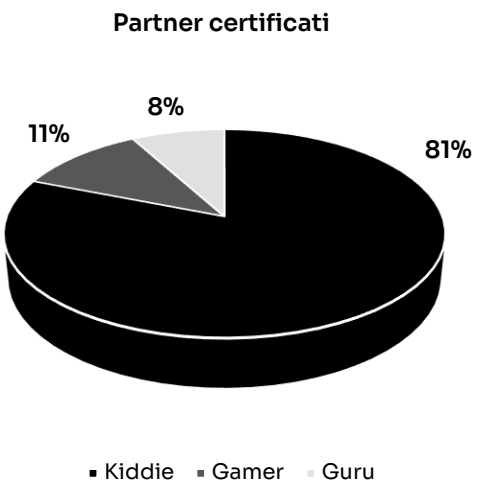
I partner sono inoltre agevolati dalla costruzione di un network e sono in condizione, insieme a Cyberoo, di supportare un maggior numero di aziende nel paese.

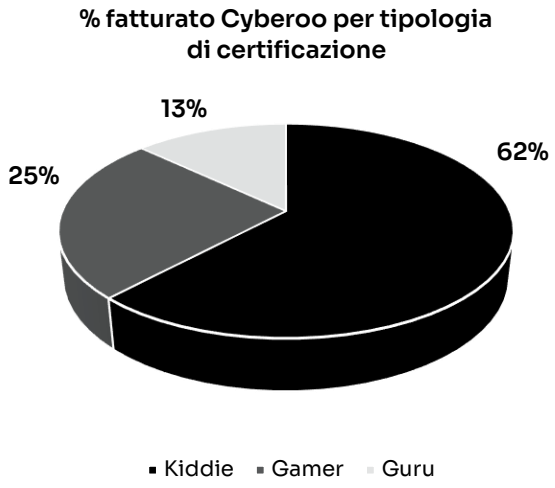
CYBEROO BLACK CLUB – Il Partner Program

Dal 2020, Cyberoo ha istituito il "**Cyberoo Black Club**", un programma di Partnership con alcuni dei più rilevanti brand del settore IT, in Italia e all'estero: è fondamentale per Cyberoo supportare i partner nella buona riuscita delle loro attività commerciali e di rapporto con il cliente e, per questo motivo, mette a disposizione tutte le sue competenze tecniche per la formazione delle risorse del partner e nella realizzazione di attività di marketing congiunte per dare sostegno al brand, alla proposizione di valore e alla generazione di lead sul canale.

Il Black Club è un programma con tre livelli di partnership, definito in base a due valori che devono risultare contemporaneamente soddisfatti, ovvero (i) quantità di fatturato nell'anno precedente e (ii) numero di persone certificate sales, presales e tecniche:

- **KIDDIE**: il livello è quello di iscrizione iniziale e offre ai partner l'accesso a una varietà di risorse, materiali, strumenti e vantaggi di marketing;
- **GAMER**: il livello fornisce ai partner maggiori vantaggi, oltre all'accesso a risorse aggiuntive progettate per aiutarli a sviluppare piani aziendali incentrati sulla crescita e abilità tecnologiche sempre più avanzate;
- **GURU**: il livello è pensato per i partner che hanno una relazione strategica con Cyberoo. I partner che raggiungono questo livello hanno investito fortemente nel portfolio di Cyberoo e hanno contribuito maggiormente alla buona riuscita del Go to Market. Ricevono quindi il massimo livello di benefici.





Premi e riconoscimenti

Grazie alla qualità della Suite proprietaria, nel 2024 Cyberoo è stata riconosciuta per la terza volta consecutiva come Global "Representative Vendor" nella prestigiosa "Market Guide for Managed Detection and Response 2024" di Gartner. La ricerca internazionale sui servizi avanzati di sicurezza informatica più importante e autorevole, ha riconosciuto Cyberoo come parte del ristretto gruppo dei "**Representative Vendor**" delle nuove frontiere della cybersecurity. Con questo riconoscimento, Cyberoo si conferma tra i big internazionali della cybersecurity avanzata, prima e unica italiana tra 14 società europee e 40 nel mondo.

Cyberoo è stata anche nominata "Example MDR Provider" in due ricerche di Gartner dal titolo: Emerging Tech: Security — Leverage Emerging MDR Trends to Grow Your Security Service Revenue ed Emerging Tech: Security — Adoption Growth Insights for Managed Detection and Response. Nel primo report, l'azienda viene nominata tra i fornitori di servizi MDR che riducono falsi positivi, provvedono a convalidare la sicurezza pre-breach e che offrono una copertura estesa al cliente. Nel secondo report, Gartner presenta insights e dati inerenti alla crescita dell'adozione di servizi MDR.

Capitolo 4

CAPITALE RELAZIONALE

CAPITALE RELAZIONALE
OVERVIEW

0

Nessun data breach
nel 2024

65%

fornitori situati in Italia
(di cui il 26% in Emilia-Romagna)

COLLABORAZIONI

Collaborazioni con Università,
scuola ed enti di ricerca

4. Capitale relazionale

La relazione con i clienti

Nel corso degli anni, Cyberoo ha consolidato una rete stabile di relazioni con le principali aziende che propongono soluzioni e attività specialistiche nell'ambito della cybersecurity, sia a livello nazionale che internazionale. Tali aziende svolgono un ruolo chiave nella diffusione delle soluzioni Cyberoo, contribuendo allo sviluppo del business attraverso la loro capacità di presidiare il mercato finale.

Il presidio del partner rappresenta un elemento centrale del modello operativo del Gruppo Cyberoo, che si impegna costantemente per accrescere il valore generato dalla relazione con ciascun cliente.

La capacità di rispondere in modo efficace alle esigenze dei clienti rappresenta un fattore chiave per lo sviluppo sostenibile di Cyberoo ed è determinante per mantenere e rafforzare la fiducia nel rapporto.

Dall'altro lato, i partner scelgono Cyberoo perché garantisce il raggiungimento di tre obiettivi fondamentali:

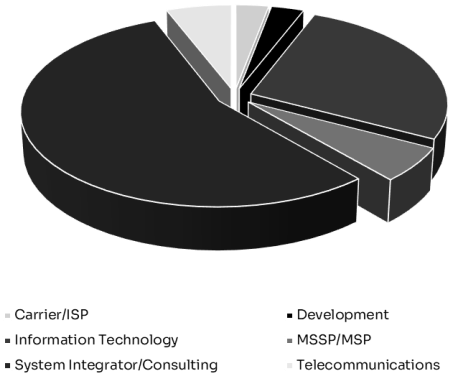
- **Valore**: ampliare il proprio portafoglio di offerta con servizi cybersecurity ad alto valore aggiunto, erogati in modalità H24 tramite un I-SOC altamente specializzato;
- **Fidelizzazione**: l'erogazione di servizi *always on* consente ai partner di seguire il cliente finale in modo proattivo e continuativo, aumentando il grado di fidelizzazione;
- **Ricavi ricorrenti**: i servizi proposti generano benefici economici attraverso ricavi ricorrenti, contribuendo a rafforzare la solidità degli economics aziendali.

La base partner di Cyberoo è costituita da aziende con profili eterogenei, accomunate dalla capacità di interagire con i clienti finali in funzione della loro propensione a indirizzare l'adozione tecnologica, a offrire consulenza o a fornire direttamente servizi. Nei grafici seguenti sono riportati:

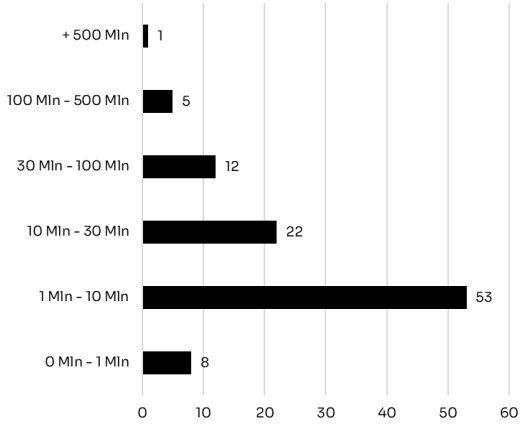
- i partner suddivisi per tipologia di business sviluppato;
- La concentrazione del fatturato per tipologia di partner.

PARTNER ITALIA

Tipologia di business del partner

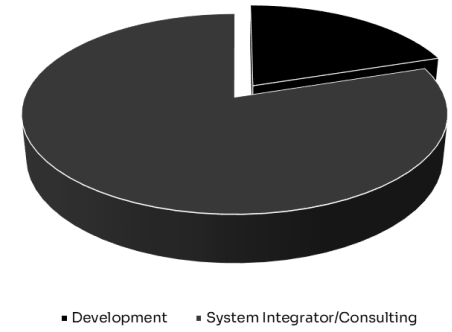


Fatturato del partner

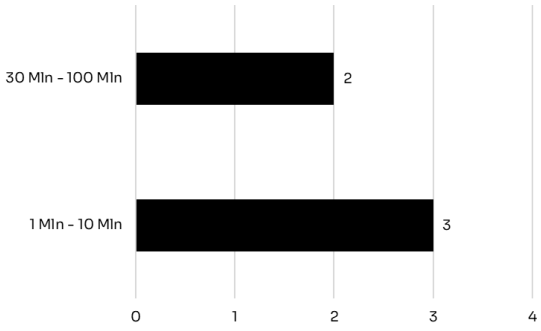


PARTNER POLONIA

Tipologia di business del partner

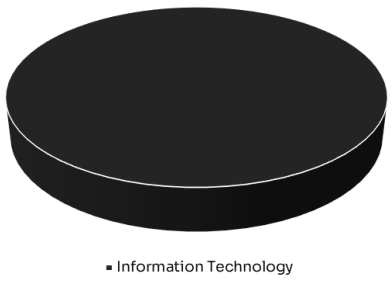


Fatturato del partner

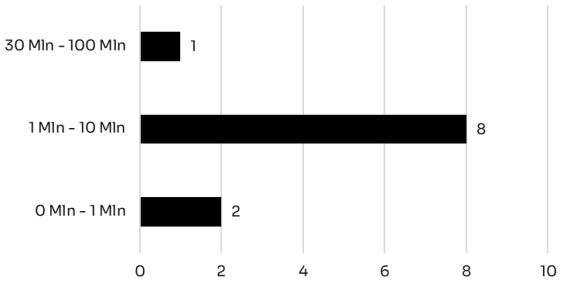


PARTNER SPAGNA

Tipologia di business del partner



Fatturato del partner



Cyberoo stipula con essi **contratti di partnership di durata annuale o pluriennale**.

La gestione delle relazioni con i clienti

I partner possono contare su una struttura composta da risorse altamente qualificate e interamente dedicate allo sviluppo del business. Cyberoo mette a disposizione figure professionali specializzate, ciascuna con un ruolo specifico all'interno del processo di gestione della relazione:

- **Channel Manager**: sviluppa le strategie di canale e attiva le relazioni con nuovi partner;
- **Partner Account Manager**: affianca i partner con l'obiettivo di consolidare e gestire la relazione nel lungo periodo, supportandoli nello sviluppo dell'offerta di cyber security e nelle trattative commerciali con l'end user;
- **Key Account Manager**: sviluppa e mantiene le relazioni con l'end user, generando nuove opportunità commerciali che vengono poi assegnate al partner più idoneo, secondo parametri predefiniti;
- **Business Development Manager**: supporta il partner nelle attività di formazione e certificazione, nell'analisi del mercato di riferimento, nella definizione di piani di sviluppo del business, nelle demo e presentazioni con i clienti e nella gestione delle opportunità;
- **Deal Manager**: figura interna incaricata di supportare il partner nella deal registration e nella relativa approvazione.
- **Inside Sales**: risorse interne dedicate al primo contatto con i prospect, con l'obiettivo di supportare e potenziare l'attività dei Key Account Manager (KAM), sia in ambito commerciale che marketing.

Questa struttura è pienamente operativa e sviluppata nel mercato italiano, dove ogni figura è presente e integrata nei processi di vendita. Nei mercati esteri, come la Polonia, il modello è attualmente più snello: le figure presenti sono principalmente i Key Account Manager, i Partner Account Manager e i Business Development Manager, che svolgono un ruolo centrale nella gestione delle relazioni con partner e clienti e nella crescita del business locale. In Spagna sono già attive anche alcune figure come gli Inside Sales. Trattandosi di mercati di più recente sviluppo, la struttura commerciale non è ancora articolata come in Italia ed è in fase di progressivo rafforzamento, con l'obiettivo di mantenere ovunque standard elevati di supporto e vicinanza ai partner e ai clienti finali.

Processo di on-boarding dei partner

Il reclutamento dei partner avviene sia su base territoriale sia in funzione del modello di sviluppo del business definito per una determinata tipologia di cliente. Una volta identificata l'azienda, condiviso il modello di business e ottenuta la manifestazione di interesse a diventare partner Cyberoo, si avvia il processo strutturato di "**on-boarding del partner**", articolato nelle seguenti fasi:

- firma del contratto di partnership e adesione al Cyberoo Black Club;
- formazione iniziale del personale del partner (Sales, Presales, Tecnici);
- condivisione dello Starter Kit commerciale e tecnico;
- definizione del piano commerciale;
- pianificazione e supporto allo sviluppo del business, attraverso incontri e gestione delle trattative).

Formazione e certificazione

Per garantire ai partner una piena comprensione e autonomia del modello di business e delle soluzioni Cyberoo, vengono organizzati **corsi specifici di certificazione** per le figure commerciali (sales), di prevendita (Presales) e tecniche. Tali corsi, **gratuiti e a cadenza trimestrale**, consentono di trasferire competenze strategiche e operative su temi fondamentali riguardanti la cyber security, le minacce del cyber crime e l'intera offerta dei servizi di Cyberoo (Cyber Security Suite).

Security Advisor Manager

A seguito dell'attivazione delle soluzioni Cyberoo, viene messa a disposizione dei clienti una figura altamente specializzata: il Security Advisor Manager. Questa risorsa ha il compito di valutare il livello di servizio erogato attraverso incontri periodici, generalmente con cadenza trimestrale e preferibilmente svolti on-site. Durante queste Service Review, vengono analizzati:

- lo stato attuale dei servizi attivi;
- le principali segnalazioni ricevute e i potenziali punti di miglioramento;
- le criticità da risolvere per ottimizzare i processi di sicurezza.

Poiché la consapevolezza della propria postura di sicurezza nello scenario contemporaneo diventa essenziale per poter garantire efficacemente i risultati

operativi aziendali, elemento centrale della Service Review è la presentazione di un documento di **Risk Assessment**, volto a fornire una fotografia aggiornata del livello di rischio del cliente, con riferimento a infrastrutture, networking e ambiti cyber. Il documento viene analizzato da un team di specialisti che, domanda per domanda, attribuisce un livello di rischio e fornisce suggerimenti operativi e indicazioni su eventuali vulnerabilità/criticità.

Questo approccio consente a Cyberoo di offrire un servizio altamente personalizzato, in grado di rispondere con efficacia alle esigenze specifiche di ogni cliente e orientato all'eccellenza, garantendo la massima efficienza nelle soluzioni implementate.

Qualità, sicurezza ed affidabilità del servizio

Il monitoraggio costante dei servizi erogati ai clienti consente al Gruppo Cyberoo di perseguire un duplice obiettivo: da un lato, garantire **costantemente un'elevata qualità di erogazione del servizio al cliente**; dall'altro, **ottimizzare i processi interni** aziendale in un'ottica di miglioramento continuo.

Con una particolare attenzione alla qualità e alla soddisfazione del cliente, la Direzione aziendale di Cyberoo, sensibile a questa particolare tematica, ha istituito una struttura dedicata: il **Quality and Customer Relationship Department**, responsabile delle seguenti attività:

- analizzare e comprendere le aspettative e i bisogni di business dei clienti;
- garantire la qualità dei processi/servizi erogati e il raggiungimento degli obiettivi prefissati sin dalla fase progettuale;
- coordinare le interazioni tra tutti gli stakeholder coinvolti, supervisionandone l'operatività;
- elaborare piani di *problem management* e iniziative di *service improvement*;
- organizzare riunioni periodiche con i clienti per la verifica dello stato del servizio, sulla base di KPI e stati di avanzamento del servizio condivisi con il cliente finale;
- redigere report sulle performance di servizio, secondo modalità e frequenza concordate;
- registrare e analizzare i dati relativi ai feedback ricevuti su prodotti e servizi;

- condividere, ove necessario, evoluzioni dei servizi attivi attraverso progetti ad hoc (tempi e attività);
- rafforzare la fidelizzazione dei clienti e dei partner, stimolando al contempo la generazione di nuove opportunità commerciali.

Privacy dei clienti e perdita di dati dei clienti

Nel corso dell'esercizio non sono state ricevute contestazioni o reclami, né da parte dei clienti in materia di privacy, né sono state rilevate violazioni della normativa sulla protezione dei dati personali (GDPR) per i trattamenti effettuati da Cyberoo, sia in qualità di Titolare che di Responsabile del trattamento.

Inoltre, non si sono stati verificati incidenti relativi alla sicurezza delle informazioni, come divulgazione, furto o perdita di dati dei clienti *(data breach).*

Cyberoo, operando nel settore B2B, tratta principalmente dati aziendali (es. numero di dipendenti, settore, tecnologie utilizzate), limitando la raccolta di dati personali a informazioni come e-mail e numero di telefono aziendali. Non vengono trattati dati sensibili relativi a preferenze personali, salute o orientamenti individuali. Le attività di marketing sono rivolte a clienti o prospect che interagiscono volontariamente con il Gruppo e i trattamenti sono sempre chiaramente esplicitati sul sito web. Campagne di telemarketing vengono condotte utilizzando database forniti da operatori specializzati, che garantiscono la conformità alle normative in materia di protezione dei dati.

Attività di marketing

Digital360

Cyberoo collabora attivamente con **Digital360**, partner strategico per le attività di comunicazione e marketing digitale. La collaborazione integra in modo efficace **storytelling, posizionamento SEO, attività social** e azioni mirate sia su canali esterni (portali del network Digital360 – outbound) sia su asset proprietari di Cyberoo (inbound).

L'obiettivo della partnership è quello di valorizzare le competenze e l'expertise nella comunicazione digitale, generando in modo continuativo **opportunità commerciali concrete**.

Ciò avviene attraverso l'impiego di:

- **contenuti editoriali "gated"**, come white paper e approfondimenti tematici,
- **Marketing Automation**, per la gestione efficiente e scalabile dei lead,
- **Contenuti multimediali**, quali vlog e pillar pages di approfondimento.

Tra le attività e gli strumenti digitali prodotti in collaborazione con Digital360, e utilizzati come tool strategici di supporto alla generazione di domanda e al posizionamento del brand, si segnalano:

Attività	Output	Dettaglio
Ottimizzazione SEO dei contenuti	• Audit del sito • Mappatura pagine per redirect • Ottimizzazioni SEO	*Assessment sito, e consegna roadmap interventi. Ottimizzazione in ottica SEO dei contenuti per migliorare il posizionamento sui motori di ricerca*
Creazione contenuti da promuovere sul Network Digital360	• **3** contenuti originali/anno	*Contenuti sulle tematiche concordate (interviste, use case, news, scenari e trend di settore, ecc.) pubblicati sul Network Digital360 e relative riprese social e di NL di testata.*
Contenuti asset Cyberoo corredati di riprese social	• **2** Pillar page • **15** articoli da Blog + **30** post social • **5** articoli passati con rich media • **4** Vlog + pillole video per Linkedin • **1** White paper Deep & Dark web • **1** Review del White paper «Security as a service: il nuovo approccio alla sicurezza informatica che rivoluziona il mercato»	*Contenuti e riprese social sulle tematiche concordate (interviste, use case, news, scenari e trend di settore, ecc.) pubblicati su asset Cyberoo.*
Marketing Automation Technology	• Licenza Hubspot Marketing (+ 6.000 Marketing contact included) • Implementazione workflow e supporto marketing automation	• *Licenza Hubspot PRO* • *Workflow di benvenuto* • *Workflow di marketing automation* • *Workflow nurturing Sales* • *Workflow pagine web* • *Workflow content curation* • *Workflow preparazione evento* • *Workflow follow up evento*

In particolare, nel 2024 le attività di marketing di Cyberoo si sono focalizzate principalmente sui canali **social**, con la diffusione di contenuti corporate attraverso i **profili ufficiali del Network Digital360** (Linkedin, Facebook, Twitter) e su quelli di Cyberoo.

La collaborazione con Digital360, che proseguirà per tutto il 2025 sui canali network di Digital360, ha come obiettivi principali:

- potenziare il posizionamento e la reputation di Cyberoo;
- ampliare la community building di Cyberoo;
- potenziare l'automazione dei processi di lead generation e i processi interni a Cyberoo.

Il sito cyberoo.com ha registrato 185 mila visite nel 2024 (+170% rispetto al 2023). Ottimi risultati anche per i due blog aziendali: il blog dedicato a temi di awareness ha ottenuto 13 mila visite (+200% rispetto al 2023), mentre quello con taglio

maggiormente tecnico, attivo da febbraio 2024, ha superato le 3 mila visite con dati in constante crescita.
La pagina LinkedIn ha raggiunto oltre 1 milione di visualizzazioni (+40% rispetto al 2023), +3 mila follower (il dato più alto di sempre) e 50 mila click su contenuti pubblicati.
Nel mese di maggio 2024, è stato inoltre inaugurato il canale Instagram, con l'obiettivo di rafforzare le attività di employer branding e proporre contenuti di awareness rivolti a un pubblico più giovane, andando oltre la sola base clienti. I reel, formato innovativo e coinvolgente, hanno totalizzato circa 15 mila visualizzazioni.

Marketing Arena

Cyberoo collabora attivamente anche con **Marketing Arena**, in qualità di partner digitale per elaborare una strategia di digital marketing volta ad aumentare la *brand awareness* e la consapevolezza degli utenti sul tema della cybersecurity.

A questo scopo sono state attivate campagne di *digital advertising* su diversi canali, indirizzate verso la promozione di tutti i contenuti digitali per continuare a presidiare i temi di cybersecurity su tutto il mondo Google e Meta.

La collaborazione proseguirà nei mesi a venire con budget da destinare all'advertising online sui diversi canali.

I focus 2024 sono divisi su 4 campagne:

- Campagna Lead generation in piattaforma LinkedIn;
- Campagna Google Search con nuova Key strategy;
- Campagna Organico;
- Campagna Education.

VENTISETTE Digital

Tra il 2022 e il primo semestre del 2023 Cyberoo ha avviato un importante progetto di rifacimento del sito web, con l'obiettivo di comunicare in modo chiaro, immediato ed efficace la nuova *brand identity*, definita da tre pilastri fondamentali:

- garantire una qualità di servizio vicina al mondo luxury;
- affermarsi come punto di riferimento per la cybersecurity in Italia;

- trasmettere un'immagine con un impatto distintivo, riconoscibile e immediato.

Il nuovo sito web è stato concepito come un'esperienza utente coinvolgente, arricchita da uno storytelling originale e da una User Experience fortemente caratterizzante, unici rispetto alla concorrenza. Il sito rappresenta oggi un'eccellenza un riferimento di eccellenza, sia per la qualità del design sia per le soluzioni tecnologiche adottate. A conferma di questo valore, nel 2023 ha ricevuto una Honorable Mention agli Awwwards, prestigioso riconoscimento internazionale che valuta i migliori siti web sulla base di criteri quali UI, UX, sviluppo e accessibilità. Grazie alla sua struttura multilingua, il sito è inoltre accessibile a un pubblico internazionale.

Nel corso del 2023, la collaborazione con VENTISETTE Digital si è estesa anche alla realizzazione grafica del Bilancio Consolidato 2022, introducendo un approccio innovativo attraverso l'utilizzo di immagini generate con DALL·E, al fine di rinnovare l'iconografia aziendale e valorizzare ulteriormente l'identità del brand.

Questo percorso di ridefinizione dell'immagine coordinata è proseguito coerentemente nel tempo, includendo anche la realizzazione dei Bilanci di Sostenibilità, Consolidati e Semestrali degli anni successivi. Anche nel 2024, la collaborazione con VENTISETTE Digital continua attivamente su tutti i progetti legati alla comunicazione istituzionale, con particolare attenzione alla direzione creativa e alla coerenza con il posizionamento del brand.

Il sito web, parte integrante di questa strategia di evoluzione, è tuttora oggetto di aggiornamento continuo. Nel 2024 è stata infatti pubblicata una nuova sezione dedicata alla Sostenibilità, pensata per rendere ancora più trasparenti e accessibili i valori e gli impegni ESG dell'azienda.

Comunicazioni e valori: la campagna "Above The Rest"

Nel 2024 Cyberoo ha lanciato "*Above The Rest*", una campagna di comunicazione manifesto che ha segnato un punto di svolta nella narrazione del brand. Realizzata in collaborazione con Action Agency, Drop Films e Dr Podcast Audio Factory, la campagna ha scelto di mettere al centro le persone, il coraggio, il sacrificio e l'umanità, andando oltre i confini tecnologici tradizionali della comunicazione nel settore cybersecurity.

Il cuore del progetto è un video emozionale che racconta la storia di una mamma vista come un supereroe, metafora della dedizione e della resilienza che contraddistingue le persone Cyberoo: professionisti che ogni giorno proteggono le aziende non solo con l'ausilio della tecnologia, ma con spirito di squadra, passione e senso di responsabilità.

Ad arricchire la campagna, il podcast originale "*Italiani – Above The Rest*", narrato dalla voce autorevole del giornalista sportivo Federico Buffa. Dieci episodi che raccontano le storie straordinarie di italiani visionari e fuoriclasse — come Samantha Cristoforetti, Margherita Hack, Federico Fellini e altri — che incarnano i valori di eccellenza, innovazione e determinazione che ispirano quotidianamente la cultura aziendale di Cyberoo.

Attraverso "*Above The Rest*", Cyberoo ha voluto trasmettere un messaggio forte e coerente con i propri valori ESG: le tecnologie sono fondamentali, ma sono le persone a fare la differenza. La campagna ha contribuito a rafforzare l'identità del brand come realtà umana, autentica e proiettata verso un futuro in cui l'innovazione passa prima di tutto dalle qualità straordinarie dell'essere umano.

Il video della campagna "Above The Rest" ha registrato oltre 3 milioni di impression, più di 80 mila visualizzazioni, il relativo podcast ha già registrato oltre 5 milioni di impression e 70 mila ascolti, anche grazie alla apprezzatissima partecipazione di Federico Buffa.

Gartner

L'attività di collaborazione con Gartner è attiva dal 2020. Gartner è un'azienda che fornisce ai dirigenti e ai loro team informazioni oggettive e concrete. La sua guida esperta e i suoi strumenti consentono di prendere decisioni più rapide e intelligenti e di ottenere prestazioni migliori sulle priorità mission-critical di un'organizzazione.

Tale accordo di consulenza garantisce il supporto autorevole di Gartner non solo nel processo di M&A (Merger & Acquisitions), ma soprattutto nel percorso di crescita e valorizzazione di Cyberoo, sia in termini di prodotto che di strategia commerciale, contribuendo ad aumentare la visibilità e il posizionamento di mercato a livello nazionale e internazionale.

Gartner si occupa di guidare Cyberoo nelle scelte strategiche più delicate di sviluppo, diversificazione e internazionalizzazione della sua offerta al fine di garantire una solida e mirata crescita sul mercato locale e anche fuori dai confini italiani.

L'etica delle relazioni commerciali

In linea con i valori fondamentali descritti nel proprio Codice Etico e consapevole delle diverse esigenze e aspettative dei clienti, Cyberoo impronta tutte le sue relazioni commerciali sul più rigoroso rispetto delle disposizioni legislative vigenti, delle procedure interne e dei principi di **integrità, onestà, correttezza, rispetto, fiducia reciproca, professionalità, trasparenza, indipendenza** ed **equità**.

L'azienda si impegna a garantire la massima qualità dei servizi e delle soluzioni offerte, ponendo particolare attenzione al miglioramento continuo dei propri processi interni. Gli investimenti costanti in **innovazione tecnologica** e **sicurezza** sono essenziali per rispondere alle sfide in continua evoluzione nel settore della cybersecurity, assicurando soluzioni sempre più efficaci e sicure per i clienti.

Cyberoo comunica le informazioni ai propri clienti in modo chiaro e trasparente, basando ogni rapporto su principi di **collaborazione**, **cortesia** ed **efficienza**. Ogni membro del team commerciale si impegna a fornire informazioni **vere**, **complete** e **accurate** circa i servizi offerti, permettendo ai clienti di prendere decisioni consapevoli e razionali.

Inoltre, Cyberoo si impegna a garantire che ogni accordo commerciale sia basato su principi di **lealtà** e **correttezza**. È severamente vietato concedere benefici di qualsiasi natura a partner commerciali che non siano giustificati dal contesto del rapporto. L'azienda promuove una concorrenza leale e sostenibile, evitando pratiche sleali come l'acquisizione di segreti commerciali tramite metodi illeciti o l'assunzione di dipendenti da concorrenti per ottenere informazioni riservate.

Il processo commerciale e la qualità del servizio

Il processo commerciale di Cyberoo si sviluppa attraverso fasi ben definite, ognuna delle quali garantisce un'interazione continua e costruttiva con i clienti:

- **Identificazione e consulenza iniziale**: ogni nuovo cliente viene ascoltato per comprendere le sue specifiche esigenze nel campo della cybersecurity.

L'analisi approfondita delle necessità consente a Cyberoo di proporre soluzioni personalizzate e mirate.

- **Proposta e personalizzazione del servizio**: le soluzioni sono progettate su misura, con la massima trasparenza riguardo ai costi, ai tempi e agli obiettivi da raggiungere, in modo che il cliente possa prendere decisioni informate.
- **Erogazione e monitoraggio del servizio**: una volta implementato il servizio, Cyberoo continua a monitorare l'andamento del progetto per garantire che gli impegni vengano rispettati e che i risultati soddisfino le aspettative.
- **Feedback e ottimizzazione continua**: Cyberoo raccoglie regolarmente il feedback dei clienti per valutare il livello di soddisfazione e identificare eventuali aree di miglioramento, assicurandosi che ogni servizio evolva in base alle necessità reali del cliente.

Il canale di distribuzione

Cyberoo adotta un modello di vendita indiretto di tipo TIER II, basato sulla collaborazione con un distributore e una selezionata di partner qualificati, supportata da una forza commerciale interna dedicata. Questo approccio permette di massimizzare l'efficacia della penetrazione commerciale, creando una situazione vantaggiosa per entrambe le parti: i partner possono proporre ai propri clienti soluzioni di cybersecurity avanzate, mentre Cyberoo beneficia dell'accesso a clienti con cui i partner hanno già instaurato relazioni di fiducia consolidate.

In molti casi, il rapporto diretto con i clienti finali è gestito autonomamente dal partner, senza un contatto diretto con Cyberoo. Tuttavia, Cyberoo interviene quando è essa stessa a generare l'opportunità commerciale, che viene poi affidata al partner più idoneo in base ai criteri condivisi, oppure su richiesta del partner nei casi in cui il cliente sia particolarmente strategico o complesso. In ogni scenario, Cyberoo garantisce un alto livello di supporto tecnico e consulenziale, assicurando la coerenza qualitativa del servizio erogato, come descritto nei punti precedenti.

Fidelizzazione e misurazione della qualità

La fiducia reciproca è la base su cui Cyberoo costruisce le proprie relazioni commerciali, mirando a stabilire partnership durature e di successo. La qualità del servizio e la fidelizzazione dei clienti sono monitorate attraverso l'analisi dei rinnovi

contrattuali, dei progetti consolidati nel tempo e delle relazioni costruite nel corso degli anni.

Cyberoo mantiene un'attenzione costante verso la soddisfazione del cliente grazie anche al ruolo strategico del Security Advisor Manager (SAM), figura che non si limita al monitoraggio della qualità del servizio ma agisce anche come punto di contatto privilegiato per il cliente nel post-vendita. Il SAM supporta la gestione operativa delle attività, raccoglie feedback in modo strutturato e promuove un miglioramento continuo delle soluzioni e del rapporto con il cliente.

La concentrazione dei ricavi su una clientela di riferimento dimostra l'efficacia delle relazioni instaurate e la qualità dei servizi forniti. Cyberoo si impegna a soddisfare le esigenze dei propri clienti attraverso soluzioni innovative e personalizzate, il che ha permesso all'azienda di consolidare la propria posizione come leader nel settore della cybersecurity.

La gestione della supply chain

I fornitori

Il parco fornitori del gruppo Cyberoo è costituito da un ristretto numero di aziende con cui si è stabilito e consolidato nel tempo un rapporto di stretta collaborazione.

Le diverse esigenze commerciali di offrire alla clientela soluzioni al passo con l'innovazione tecnologica richiedono di selezionare eventuali nuovi fornitori, seppur la politica aziendale incoraggi, ove possibile, a mantenere contatti continuativi con i fornitori qualificati.

Tutte le volte che si rende necessario scegliere, valutare e approvare un Fornitore (sia di prodotti che servizi) che possa avere influenza sulla qualità e sicurezza delle informazioni dei prodotti e servizi forniti dal Gruppo Cyberoo, l'Azienda applica una procedura standardizzata, di seguito sintetizzata:

- i prodotti e i servizi affidati ai fornitori devono essere conformi ai requisiti stabiliti in sede di accordo con Gruppo Cyberoo;
- i prodotti e i servizi approvvigionati esternamente devono essere tenuti sotto controllo secondo modalità definite internamente in base alla tipologia di fornitura, tenendo in considerazione l'impatto potenziale sulla capacità di soddisfare con regolarità il cliente;

- la scelta di selezione dei Fornitori devono avvenire seguendo criteri di affidabilità, che consentano di ottenere la massima soddisfazione dei requisiti di qualità e sicurezza delle informazioni del prodotto o servizio acquistato;
- l'affidabilità dei Fornitori deve essere periodicamente controllata;
- i dati di acquisto devono essere gestiti in forma controllata;
- le modalità di comunicazione identificate con i fornitori esterni devono rispondere a requisiti stabiliti.

La selezione e gestione della catena di fornitura

Per i fornitori con cui si intende intraprendere una collaborazione continuativa, una volta superata con esiti positivi l'attività di valutazione iniziale, vengono completate le informazioni commerciali e tecniche relative al fornitore e, per Cyberoo S.p.A., viene compilato il record fornitore sul file *M APS QVF Qualifica e Valutazione Fornitore*, riportando i dati e l'esito delle prime forniture come da Procedura Approvvigionamenti.

Se un fornitore è ritenuto strategico, viene inserito all'interno dei "fornitori in osservazione" per poi essere promosso a fornitore qualificato in occasione di forniture ricorrenti.

Per tutte le altre aziende del gruppo, l'esito positivo corrisponde con la codifica a gestionale, corredata di tutti i documenti integrativi (sla, visure, certificazioni richieste).

Per Cyberoo, come da normativa ISO 27001, l'approvazione formale dei potenziali fornitori viene effettuata a cura dell'Ufficio Acquisti, sulla base dei dati raccolti e assegnando un voto (da 0 a 3) ai seguenti criteri di valutazione:

- qualità del prodotto/ servizio;
- referenze e professionalità;
- rispetto degli impegni;
- collaborazione e disponibilità;
- sistema gestione qualità;
- sistema di gestione di sicurezza delle informazioni (nel caso in cui non fosse stata conseguita alcuna certificazione in tale ambito, Cyberoo si assicura che i fornitori di servizi, considerati i fornitori più critici, gestiscano in

maniera congrua le informazioni, allegando a tutti i contratti con gli stessi una documentazione specifica);

- prezzi e condizioni economiche.

I criteri di valutazione dei fornitori sono i seguenti:

0 = Insufficiente	Si sono riscontrate non conformità/ inconvenienti e scarsa reattività ai problemi
1 = Sufficiente	Si sono riscontrate episodiche non conformità/ inconvenienti con reattività positiva del fornitore
2 = Buono	Non si sono riscontrate non conformità/ inconvenienti significativi
3 = Ottimo	Prestazione eccellente.

Per quanto riguarda la domanda sul Sistema Gestione Sicurezza delle Informazioni del fornitore, particolare rilevanza è data ai fornitori di servizi che gestiscono informazioni sensibili.

Nel gestionale sono indicati esplicitamente i fornitori in possesso della certificazione ISO 27001 e quindi ritenuti idonei in automatico. Per gli altri fornitori di servizi, Cyberoo ha inviato un modulo di autocertificazione delle misure tecniche e organizzative per misurarne la sicurezza. Per i fornitori occasionali (fornitori utilizzati per momentanea indisponibilità dei fornitori abituali o per soddisfare una richiesta di servizio nuovo occasionale inoltrata da parte del cliente), invece, non è richiesta l'attività formalizzata di selezione e valutazione.

Analogamente, per i fornitori con i quali c'è uno stretto rapporto di partnership, non si richiede una formale selezione e valutazione, bensì vengono assoggettati a definizione di specifiche di fornitura (es. capitolati di servizio, condivisione delle procedure operative) e controllo delle forniture, con eventuale rilevazione / registrazione di non conformità.

Per essere qualificato, il fornitore deve ottenere la valutazione almeno "sufficiente" per il criterio "qualità prodotto/ servizio e la valutazione media pesata maggiore o uguale a 55%.

I Fornitori che hanno superato positivamente la fase di valutazione iniziale vengono qualificati: l'evidenza di tale qualifica risulta dalla data di qualifica inserita nel M APS QVF.

Le schede di Valutazione e eventuali certificati o documenti tecnici inviati dai Fornitori sono conservati a cura dell'Ufficio Acquisti, quali riferimenti documentati delle caratteristiche del Fornitore e della sua valutazione.

Tutte le informazioni contenute nell'archivio fornitori sono considerate riservate e non possono essere divulgate senza l'autorizzazione del responsabile.

La filiera sostenibile

Le società del Gruppo Cyberoo gestiscono i fornitori con lealtà, correttezza e professionalità incoraggiando rapporti continuativi e solidi.

Il gruppo Cyberoo ha intrapreso in percorso di sostenibilità aziendale ESG (Environmental, Social and Corporate Governance) in base al quale si richiede una presa di coscienza a tutta la filiera di fornitura.

Il miglioramento degli impatti ambientali, sociali e di governance di Cyberoo richiede consapevolezza e trasparenza delle attività presenti e future per ampliare l'impatto del percorso che è stato intrapreso internamente: Cyberoo considera essenziale misurare gli impatti del proprio ecosistema e stabilire un dialogo collaborativo con i partner, riconoscendo che ognuno è indispensabile per l'altro, in un processo di apprendimento reciproco e di co-evoluzione.

Ad ogni fornitore ritenuto strategico per volume, numero di ordini, impatto e brand Cyberoo ha intenzione di sottoporre il Form Etico che permetterà di conoscere il livello di maturità in merito alle tematiche ESG.

Le macro categorie trattate sono riassumibili in: ***sostenibilità ambientale, etica, rispetto dei diritti e gestione dei fornitori*.**

NUMERO FORNITORI[5]	2022		2023		2024	
	n.	% sul totale	n.	% sul totale	n.	% sul totale
Numero di fornitori LOCALI[6]	164	**31%**	188	**28%**	194	**26%**
Numero di fornitori situati in ITALIA	308	**60%**	418	**64%**	473	**65%**
Numero di fornitori situati in EUROPA	19	**4%**	27	**4%**	38	**5%**
Numero di fornitori situati in AMERICA	12	**2%**	11	**2%**	15	**2%**
Numero di fornitori situati in ASIA	3	**1%**	1	**0%**	1	**0%**
Numero di fornitori situati nel RESTO DEL MONDO	10	**2%**	12	**2%**	11	**2%**
TOTALE FORNITORI	516	**100%**	657	**100%**	732	**100%**

Nonostante si cerchi di dare preferenza ai fornitori locali, sia per prodotti che servizi, la scelta dei fornitori è anche condizionata dalla specificità di brand, caratteristiche e qualità alla base di quanto ordinato.

A parità di condizioni aziendalmente si è deciso di orientarsi su fornitori i più locali possibile.

Nel triennio si osserva una crescita significativa del budget complessivo speso in fornitori, che passa da 5,47 milioni di Euro nel 2022 a 8,53 milioni di Euro nel 2024 (+56%).

L'incidenza dei fornitori locali mostra un trend positivo, aumentando dal 15% nel 2022 al 21% nel 2024, a dimostrazione di un crescente impegno verso il sostegno all'economia del territorio.

I fornitori italiani si confermano il principale canale di approvvigionamento, rappresentando costantemente oltre il 65% della spesa totale, anche se in leggero calo percentuale nel 2024 (dal 69% al 65%), a fronte di un'espansione della spesa in Europa.

La spesa verso fornitori europei è più che triplicata tra il 2022 e il 2024, anche se rimane contenuta (dal 2% al 4%). Gli acquisti da fornitori extraeuropei (America, Asia, resto del mondo) sono stabili o marginali, con quote complessive inferiori al 15%.

[5] I dati del 2022 sono stati aggiornati, poiché dal 2023 si è utilizzata una metodologia differente per l'estrazione del numero dei fornitori.

[6] Per fornitori locali si intende i fornitori provenienti dall'Emilia Romagna.

Budget speso in fornitori	2022		2023		2024	
	€	% sul totale	€	% sul totale	€	% sul totale
Budget speso in fornitori LOCALI	817.000	**15%**	1.107.000	**18%**	1.751.000	**21%**
Budget speso in fornitori situati in ITALIA	3.740.000	**68%**	4.192.000	**69%**	5.565.000	**65%**
Budget speso in fornitori situati in EUROPA	115.000	**2%**	171.000	**3%**	366.073	**4%**
Budget speso in fornitori situati in AMERICA	145.000	**3%**	64.000	**1%**	115.257	**1%**
Budget speso in fornitori situati in ASIA	800	**0%**	100	**0%**	110	**0%**
Budget speso in fornitori situati nel RESTO DEL MONDO	650.000	**12%**	570.000	**9%**	734.000	**9%**
TOTALE FORNITORI	5.467.800	**100%**	6.104.100	**100%**	8.531.440	**100%**

Il monitoraggio della filiera di produzione

Tutti i fornitori del Gruppo sono sottoposti a riesami periodici delle prestazioni, per valutare se i prodotti o servizi forniti hanno rispettato i requisiti di qualità e sicurezza delle informazioni attesi, ponderati e rapportati al volume delle forniture effettuate.

Per Cyberoo S.p.A., le valutazioni periodiche avvengono con frequenza commisurata agli eventuali problemi che si sono presentati nel periodo, seppur indicativamente a intervalli non superiori a 12 mesi (a inizio anno, per l'anno solare precedente, in occasione del Riesame Sistema Qualità e sicurezza delle informazioni da parte della Direzione).

In assenza di prestazioni, il fornitore viene comunque preso in considerazione almeno una volta all'anno per verificare la necessità di mantenerlo tra i fornitori approvati.

Per mantenere lo stato di Fornitore qualificato, il fornitore deve conservare nel tempo la valutazione almeno "sufficiente" per il criterio "qualità prodotto/servizio" e la valutazione media pesata maggiore o uguale al 55%.

Il fornitore in precedenza "qualificato", che nelle successive verifiche di prestazione risultasse "scarso" per 2 volte consecutive, non verrà più considerato fornitore approvato ed evidenziato in quanto tale nell'anagrafica dei fornitori. In

caso di valutazione scarsa viene normalmente attivato un reclamo formale al fornitore con la richiesta di normalizzare la situazione.

L'Ufficio Acquisti, in occasione del monitoraggio, si occupa di verificare se i fornitori approvati sono stati interpellati nell'arco del periodo: qualora non gli fosse richiesto alcun servizio di fornitura per 3 anni, non verrà più considerato approvato e, in caso di successiva necessità di utilizzo, si provvederà a ripetere l'iter di qualificazione.

Gli acquisti possono rispondere sia a esigenze di vendite transazionali, di canoni di servizio, sia di riapprovvigionamento interno.

Le relazioni con il territorio

Cyberoo riconosce l'importanza di sviluppare relazioni solide e sostenibili con il territorio in cui opera, impegnandosi a contribuire attivamente alla crescita sociale, culturale ed economica delle comunità locali e internazionali. La politica di relazioni territoriali dell'azienda si fonda su una costante collaborazione con attori locali, istituzioni e associazioni e realtà accademiche, con l'obiettivo di promuovere iniziative che generino valore condiviso e benessere per la collettività. Nel 2024, Cyberoo ha rafforzato il proprio impegno attraverso diverse attività di stakeholder engagement, inclusi incontri dedicati con gli investitori per la presentazione dei risultati legati alla sostenibilità. Sono stati attivati comitati d'impresa e per la sicurezza e la salute sul lavoro, che hanno favorito un dialogo costruttivo con le comunità locali. Complessivamente, le attività che hanno previsto il coinvolgimento diretto del territorio sono aumentate del 58% rispetto al 2023.

ATTIVITÀ CHE PREVEDONO IL COINVOLGIMENTO DELLE COMUNITÀ LOCALI, VALUTAZIONI D'IMPATTO E PROGRAMMI DI SVILUPPO[7]	2022		2023		2024	
	n.	% sul totale	n.	% sul totale	n.	% sul totale
Incontri organizzati (conferenze, workshop, focus group, ecc..) per divulgare i risultati delle valutazioni d'impatto ambientale e sociale	1	**9%**	2	**11%**	12	**40%**
Attività di stakeholder engagement	10	**91%**	15	**78%**	16	**53%**
Comitati di impresa, comitati per la sicurezza e la salute sul lavoro	-	**0%**	2	**11%**	2	**7%**
TOTALE ATTIVITÀ	**11**	**100%**	**19**	**100%**	**30**	**100%**

Nel 2024, Cyberoo ha consolidato il proprio impegno nel campo della sostenibilità sociale e culturale attraverso iniziative che hanno coinvolto attivamente il territorio e le comunità di riferimento. Le attività si sono sviluppate in ambiti strategici come la valorizzazione del patrimonio culturale, la promozione della formazione digitale e il contrasto alle disuguaglianze, in particolare quelle legate al divario di genere. In collaborazione con organizzazioni no-profit e istituzioni culturali, Cyberoo ha contribuito alla realizzazione di eventi pubblici, percorsi formativi e campagne di sensibilizzazione, favorendo la diffusione della cultura della protezione – sia materiale che digitale – e l'accesso consapevole alle tecnologie.

Parallelamente, sono proseguite e si sono rafforzate le collaborazioni con enti professionali e accademici, finalizzate allo sviluppo di progetti di formazione. Queste sinergie hanno permesso l'attivazione di corsi, webinar, tirocini e iniziative congiunte, generando nuove opportunità di crescita e contribuendo allo sviluppo delle competenze nel settore della cybersecurity.

Attraverso tali attività, Cyberoo conferma la propria volontà di generare valore condiviso, promuovendo uno sviluppo sostenibile e inclusivo, e rafforzando il legame con le comunità e i territori in cui opera.

CRIT

Tra le collaborazioni territoriali consolidate, Cyberoo annovera il proprio ruolo di Fornitore Accreditato del Network CRIT – realtà modenese attiva nello sviluppo di

[7] È importante sottolineare che nella tabella non sono incluse tutte le iniziative a carattere gratuito realizzate in collaborazione con i partner commerciali sul territorio, finalizzate esclusivamente alla divulgazione e sensibilizzazione delle aziende del territorio.

progetti di ricerca, trasferimento tecnologico e analisi tecnico-scientifiche. Questa partnership, avviata nel 2020, ha permesso a Cyberoo di usufruire dei servizi di innovazione collaborativa offerti da CRIT, entrare in contatto con altre realtà innovative italiane e contribuire attivamente all'arricchimento delle competenze del livello di expertise in ambito cybersecurity del network e dei suoi soci, offrendo contenuti formativi specialistici e momenti di confronto ad alto valore aggiunto per le imprese del territorio.

Nel corso degli anni, Cyberoo ha realizzato con CRIT numerose attività di formazione tecnica e divulgazione:

Con CRIT, Cyberoo ha realizzato i seguenti progetti:

- nel 2020, un webinar intitolato "DEEP & DARK WEB: la parte sommersa della rete", un evento formativo volto ad aggiornare le imprese del network CRIT sui pericoli connessi al Deep & Dark Web destinato a una piattaforma interna riservata agli associati. In quella che viene definita "La parte sommersa della rete" è infatti possibile trovare una moltitudine di informazioni sensibili e strategiche offerte in via illegale. Un vero e proprio bottino digitale (costituito da password, informazioni sulla proprietà intellettuale, dati economici e finanziari delle aziende, ecc.), utilizzabile da malintenzionati e criminali informatici per ottenerne profitto o, molto peggio, come principio di un attacco più complesso. Grazie alla competenza dei tecnici qualificati di Cyberoo, i partecipanti al webinar hanno potuto accrescere e qualificare le proprie conoscenze in materia di sicurezza informatica ed attivare efficaci strategie difensive;
- nel 2021, è stata svolta formazione online: un ciclo di 3 webinar da 50 minuti l'uno circa per cui Cyberoo ha messo a disposizione relatori esperti, occupandosi di sviscerare in capitoli i macro-argomenti della Cyber Security fondamentali per accrescere le competenze di ogni dipendente di azienda e manager del network del CRIT. In questa formazione, gli esperti di Cyberoo si sono messi a disposizione per mostrare come andare oltre il semplice firewall o antivirus, guidando i partecipanti nel mondo del Deep e Dark Web e per elevare la sicurezza delle aziende e proteggere l'identità digitale;

- nel 2022 un webinar intitolato “AGE OF CYBERCRIME: Strumenti, metodologie e strategie di difesa”, un evento formativo volto ad aggiornare le imprese del network CRIT (personale tecnico come IT Manager, CISO e CIO) e manager clienti di Cyberoo. In questo webinar, Cyberoo ha messo a disposizione alcuni cyber security specialist e ripercorso l’evoluzione del cyber crime in Italia e le migliori strategie con cui le organizzazioni possono difendersi dagli attacchi informatici. Al webinar si sono iscritte 89 persone a cui sono seguite attività di follow-up tramite newsletter di Cyberoo e del CRIT, con condivisione delle slide di presentazione utilizzate durante l’evento e il video registrato.
- nel 2023 è stato sviluppato un ciclo di tre webinar incentrati su diversi aspetti della sicurezza da una panorami degli attacchi e i limiti dei servizi di Endpoint Protection della protezione della filiera di fornitura fino all’importanza della Cyber Resilience e la gestione del rischio.
- nel 2024 prosegue l’impegno formativo con un ulteriore ciclo di 3 webinar tematici: il primo dedicato all’intelligenza artificiale generativa; il secondo incentrato sull’entrata in vigore della direttiva NIS2; il terzo, previsto a fine anno, focalizzato sugli aggiornamenti e adeguamenti operativi richiesti dalla stessa direttiva.

Questa collaborazione rappresenta un esempio concreto di come Cyberoo, attraverso l’interazione con enti locali altamente qualificati, contribuisca a diffondere una cultura della sicurezza digitale e a sostenere l’evoluzione tecnologica delle imprese del territorio. Le attività svolte hanno coinvolto centinaia di partecipanti, generando un impatto positivo sul piano della formazione, della consapevolezza e dell’adozione di misure di prevenzione informatica.

Collaborazioni con Università, scuola ed enti di ricerca

Unindustria Reggio Emilia - Istituto Scaruffi

Cyberoo, membro attivo del Club Digitale di Unindustria Reggio Emilia, ha consolidato nel 2024 il proprio impegno nella formazione e nella divulgazione delle competenze digitali attraverso la collaborazione con l’Istituto Tecnico Scaruffi-Levi-Tricolore di Reggio Emilia. Il progetto, avviato nel 2022 e proseguito nel 2023,

ha coinvolto anche nel 2024 due classi quinte dell'indirizzo Sistemi Informativi Aziendali, per un totale di 28 studenti, in un percorso formativo mirato ad avvicinare i giovani al mondo del lavoro e dell'impresa, con particolare attenzione alla cybersecurity e, da quest'anno, anche all'intelligenza artificiale.

Durante il percorso, gli studenti hanno partecipato a incontri con professionisti Cyberoo, durante i quali è stata data loro la possibilità di confrontarsi con la realtà aziendale in un percorso di conoscenza che li ha portati a respirare momenti di vita professionale e casi di operatività concreta legata al mondo IT e della cybersecurity, dalle nozioni base ai rischi del deep e dark web fino ai recenti attacchi hacker a danno di multinazionali e istituzioni.

Le attività hanno incluso sessioni teoriche, esercitazioni pratiche e un project work, che ha messo gli studenti alla prova con un caso di attacco hacker: dopo un'analisi OSINT (Open Source Intelligence), i ragazzi hanno valutato l'impatto reputazionale derivante da una fuga di dati e proposto azioni correttive per mitigare il danno all'azienda. Nel 2024 il progetto è stato arricchito con una sezione dedicata all'applicazione dell'IA nella difesa informatica, offrendo agli studenti una visione aggiornata delle nuove frontiere della sicurezza digitale.

Questa iniziativa rappresenta un esempio concreto dell'impegno di Cyberoo per lo sviluppo delle competenze digitali nel territorio e per la creazione di ponti tra il mondo scolastico e quello professionale.

Università Cattolica Del Sacro Cuore

Cyberoo ad aprile del 2021 ha avviato una collaborazione che la vede partecipare, come membro del Comitato di Indirizzo, al corso di laurea in "Innovazione e Imprenditorialità Digitale" presso la facoltà di Economia e Giurisprudenza dell'Università Cattolica del Sacro Cuore, campus di Cremona. La convezione prevede il contributo attivo di Cyberoo nella definizione e realizzazione di lezioni, seminari e project work che valorizzano il percorso accademico dei futuri manager, anche con l'esperienza sul campo mediante stage e tirocini formativi in azienda.

Forte di una qualificata esperienza nei campi della digital transformation e della cyber security, Cyberoo punta a definire insieme all'Università Cattolica nuove linee di ricerca volte al trasferimento tecnologico nell'ambito della sicurezza informatica, attraverso un processo di sensibilizzazione dei giovani e contribuendo alla formazione di risorse altamente specializzate in ambito IT.

La convenzione si inserisce in uno scenario caratterizzato da un "ritardo digitale" che, stando ai dati 2020 della Commissione Europea, vede l'Italia classificarsi agli ultimi posti in Europa per quanto riguarda il livello di digitalizzazione del sistema economico e il conseguente ritardo anche sul fronte delle competenze digitali. Con il nuovo corso di laurea magistrale attivato dalla Cattolica, la sfida è colmare progressivamente questo ritardo ma anche coniugare saperi diversi e competenze tecnico-scientifiche inerenti la digitalizzazione e la cyber security, a conferma della necessità di una formazione sempre più ampia, trasversale.

In aggiunta, insieme all'Università Cattolica del Sacro Cuore, Cyberoo ha realizzato i seguenti progetti:

- per la lezione di Economia digitale, a marzo del 2022, si è approfondito il tema della cybersecurity, attraverso contenuti sul tema della sicurezza, minacce, rischi, necessità e scelte imprenditoriali;
- a novembre 2022, Cyberoo ha partecipato allo "SPEED INTERVIEWS-STAGE DAY Circuito di selezione "colloqui lampo" presso il Campus Santa Monica a Cremona.
- nel 2023 tre studenti del corso di "Innovazione e Imprenditorialità Digitale" sono stati selezionati per uno stage e di cui due sono stati confermati per un contratto di apprendistato.
- nel 2024 due studenti del corso di "Innovazione e Imprenditorialità Digitale" sono stati selezionati per uno stage, di cui uno è stato confermato per un contratto di apprendistato.

FIM CISL

Cyberoo continua a sostenere la formazione sulla sicurezza informatica anche in ambito sindacale. Nel 2023 ha collaborato con il sindacato CISL per formare i propri associati impegnati nelle relazioni sindacali aziendali, con l'obiettivo di accrescere la consapevolezza sui rischi legati alla cybersecurity e sull'importanza di affrontare questi temi anche in chiave di tutela della sicurezza e del benessere dei lavoratori.

Le iniziative si sono concretizzate in due momenti formativi in presenza: il 28 febbraio 2023 a Napoli e il 5 ottobre 2023 a Matera. Entrambi gli incontri hanno fornito ai partecipanti strumenti di base per comprendere i rischi cyber e per avviare un dialogo strutturato all'interno delle aziende sul tema della protezione dei

dati e della resilienza digitale, al fine di tutelare la sicurezza e il benessere dei dipendenti.

Nel 2024 la collaborazione è proseguita con un evento online intitolato "Cybersecurity e protezione dei dati", che ha ulteriormente approfondito il ruolo strategico della sicurezza informatica nella salvaguardia dei diritti digitali e della privacy dei lavoratori. Il webinar ha visto la partecipazione di numerosi rappresentanti sindacali da tutta Italia e ha confermato l'impegno condiviso nel promuovere una cultura della sicurezza sempre più trasversale e integrata.

Adesione a iniziative esterne e Membership

Confindustria – RetIndustria Servizi

Cyberoo prosegue il proprio impegno a supporto della sicurezza digitale delle imprese italiane anche attraverso la collaborazione con Retindustria Servizi, struttura del sistema Confindustria dedicata alla promozione di soluzioni e servizi per le aziende associate. A partire dal 2020, Cyberoo è partner di RetIndustria, il brand che gestisce le convenzioni nazionali di Confindustria e offre ai partner la possibilità di promuovere i propri prodotti e servizi legati all'attività imprenditoriale alle oltre 150.000 aziende associate a Confindustria e alle circa 200 Organizzazioni Confederate (associazioni territoriali, associazioni nazionali di categoria, Confindustrie regionali e Federazioni nazionali di settore).

Nel corso degli anni, questa collaborazione ha dato vita a una serie di iniziative informative e promozionali rivolte esclusivamente al network delle Confindustrie e alle imprese associate sul territorio nazionale. RetIndustria è infatti la rete di partner che garantisce agli associati al sistema Confindustria offerte dedicate, in esclusiva e alle migliori condizioni sul mercato, per risparmiare sui principali prodotti e servizi legati all'attività imprenditoriale. Confindustria Servizi S.p.A. gestisce anche attività complementari alla realizzazione di iniziative editoriali per promuovere la diffusione della cultura d'impresa. Tra le attività principali ci sono la pubblicazione di volumi e riviste, l'invio della newsletter "partner del mese" alle Organizzazioni confederate e la partecipazione a eventi di business networking sul territorio, sia fisicamente che in modalità remota.

Nel corso del 2024 la collaborazione con RetIndustria Servizi è proseguita non solo attraverso l'organizzazione di webinar formativi, ma anche mediante attività di

promozione dedicate alla Cyber Security Suite di Cyberoo. Queste iniziative promozionali, rivolte alle imprese associate, sono state veicolate tramite newsletter periodiche e campagne sui canali social del sistema Confindustria. Inoltre, la promozione Security Plus è continuata anche nel 2024, offrendo alle aziende associate vantaggi economici e supportando la diffusione della cultura della cyber resilience.

Grazie a queste attività integrate, Cyberoo ha potuto rafforzare la propria presenza nel tessuto industriale nazionale e contribuire attivamente alla protezione delle PMI italiane da minacce informatiche sempre più sofisticate. La collaborazione con Confindustria Servizi rappresenta un passo fondamentale nella diffusione delle migliori soluzioni di sicurezza digitale per le aziende italiane, supportandole nella protezione dei dati e nella continuità operativa.

Unindustria Reggio Emilia e Confindustria Piacenza

Sempre a partire dal 2020, Cyberoo è associato a **Unindustria Reggio Emilia**, che in coordinamento con il sistema Confindustria, concorre a tutelare e rappresentare le imprese associate sostenendo le ragioni della libera impresa, del lavoro, dei legittimi interessi e delle aspettative del mondo industriale in tutte le sedi, politiche, istituzionali, economiche e sindacali. Unindustria Reggio Emilia è l'associazione territoriale del sistema Confindustria che rappresenta quasi 1.000 imprese manifatturiere e di servizi della provincia, con circa 50.000 dipendenti.

Nel settembre 2021, è stata annunciata l'apertura del nuovo polo tecnologico di Piacenza, che ha permesso a Cyberoo di presiedere anche il territorio piacentino. In questa occasione, Cyberoo è diventata associata a **Confindustria Piacenza**, che, in conformità ai principi organizzativi generali del sistema Confindustria, persegue i seguenti scopi:

- favorire il progresso dell'industria piacentina, promuovendo la maggiore solidarietà e collaborazione tra le aziende associate;
- assistere, tutelare e rappresentare le medesime in tutti i problemi sindacali, sociali, economici e culturali che direttamente o indirettamente le riguardano;
- promuovere nella provincia, e particolarmente presso gli imprenditori, lo sviluppo sociale, civile ed economico, nonché comportamenti conseguenti nel contesto di una libera società.

Il 7 marzo 2024, Cyberoo ha partecipato attivamente al seminario intitolato "*Break the noise, defend clearly - la Cybersecurity come processo chiaro, agile ed efficiente*", organizzato insieme a Confindustria Piacenza e RICT (Ricerca, Innovazione, Comunicazione, Tecnologia – cluster di aziende per l'introduzione delle nuove tecnologie produttive e della comunicazione nel mondo della manifattura). Questo evento, che ha visto la partecipazione di esperti del settore e le aziende piacentine, ha trattato la cybersecurity approcciata come processo e non più come prodotto e le ragioni per cui i sistemi tradizionali di difesa non bastano più per garantire un livello di protezione sufficiente. È stata inoltre approfondita la cruciale importanza della catena del soccorso nella gestione delle emergenze e di come l'efficacia di un approccio resiliente alla cybersecurity dipenda dalla prontezza e dal coordinamento di tutti gli attori coinvolti.

Clusit

Cyberoo a partire da giugno 2021 è socia del Clusit, associazione che nasce nel 2000 sulla scorta delle esperienze di altre associazioni europee per la sicurezza informatica quali CLUSIB (B), CLUSIF (F), CLUSIS (CH), CLUSIL (L) che costituiscono un punto di riferimento per la sicurezza informatica nei rispettivi paesi da oltre 20 anni, alle quali si è aggiunta CLUSIQ. Il Clusit si pone i seguenti obiettivi:

- diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini;
- partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello comunitario che italiano;
- contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Nel 2022 Cyberoo ha avuto la possibilità di contribuire ai contenuti della pubblicazione Supply Chain Security, dedicata al tema della cyber security nelle catene di fornitura. Negli anni precedenti Cyberoo ha partecipato in qualità di sponsor e speaker agli eventi Security Summit.

FAI - Fondo per l'Ambiente Italiano

L'impegno di Cyberoo nella sostenibilità e nella responsabilità sociale si rinnova anche attraverso importanti collaborazioni con organizzazioni che condividono i medesimi valori di protezione e valorizzazione del patrimonio. Tra queste, la Fondazione FAI – Fondo per l'Ambiente Italiano è un partner strategico con cui Cyberoo ha avviato una collaborazione triennale a partire dal 2022, finalizzata a sostenere la Fondazione in progetti che tutelano il patrimonio artistico, culturale e naturale italiano.

Questa partnership si fonda sulla condivisione di valori comuni legati alla protezione e valorizzazione del patrimonio nazionale, con l'obiettivo di promuovere la sostenibilità e la sicurezza in tutte le sue forme.

Cyberoo, impegnata nella cybersecurity per proteggere il patrimonio digitale delle imprese italiane, e il FAI, ambasciatore della cultura della protezione e valorizzazione dei luoghi dell'arte e della natura, collaborano per garantire un futuro migliore al Paese, ciascuno nel proprio ambito di competenza.

Dal 2022, la partnership con il FAI ha portato alla realizzazione di attività comuni volte a promuovere la cultura della protezione e valorizzazione del patrimonio, con un focus particolare sulla sensibilizzazione della sicurezza informatica, essenziale per la protezione anche del patrimonio digitale delle organizzazioni. L'impegno di Cyberoo si è esteso anche alla formazione: insieme al FAI, sono stati organizzati seminari sul tema della protezione dei dati, in collaborazione con la SDA Bocconi School of Management, con l'obiettivo di sensibilizzare sulle problematiche legate alla sicurezza informatica.

Nel corso degli anni, Cyberoo ha anche contribuito alla cura dei Beni FAI, attraverso iniziative di promozione dei biglietti e attività di sensibilizzazione sul valore del patrimonio culturale.

La rinnovata collaborazione con il FAI nel 2024, che proseguirà fino al 2027, rappresenta un ulteriore passo verso un impegno congiunto per la salvaguardia del patrimonio italiano, sia in ambito artistico e naturale, che digitale, con l'obiettivo di promuovere la sostenibilità e la protezione del Paese in tutte le sue forme.

Computer Emergency Response Team (CERT)

Cyberoo comunica, il 29 giugno 2023, di essere entrata nel circuito CERT (Computer Emergency Response Team) del Trusted Introducer, il principale riferimento del settore a livello internazionale.

In qualità di CERT, per Cyberoo si aprono nuove importanti opportunità. Queste includono sia l'ampliamento della visibilità verso aziende che richiedono consulenza e supporto in ambito di sicurezza informatica, sia per la collaborazione con altri player internazionali per lo scambio di informazioni utili alla definizione delle best practices, volte al contrasto dei nuovi cyberthreat a vantaggio della sicurezza nazionale e internazionale.

Comunicazione interna ed esterna

Comunicazione interna

Cyberoo dedica una particolare attenzione alla comunicazione interna, con l'obiettivo di creare una rete solida di flussi informativi, mirati a diffondere conoscenze, obiettivi aziendali e valori all'interno dell'organizzazione. La comunicazione non si limita a trasferire informazioni, ma punta a creare un ambiente di lavoro collaborativo e trasparente, in cui ogni dipendente sia consapevole del proprio ruolo e degli obiettivi aziendali.

Per garantire un clima aziendale positivo, Cyberoo promuove un ambiente di lavoro in cui la qualità della vita lavorativa è valorizzata. L'azienda mira a costruire una forte identità condivisa tra il brand e i dipendenti, trasformandoli in veri e propri ambasciatori dei suoi valori e servizi. In questo contesto, la comunicazione interna gioca un ruolo fondamentale nel favorire la partecipazione attiva dei dipendenti e nel migliorare la collaborazione, creando un forte senso di appartenenza.

Gli strumenti utilizzati per la comunicazione interna includono canali tradizionali come la posta elettronica e soluzioni moderne come ambienti digitali e collaborativi. Cyberoo utilizza la intranet aziendale (Microsoft SharePoint) per la gestione dei documenti e dei contenuti, rendendo possibile una comunicazione più agile e la condivisione di informazioni in tempo reale. Questo strumento consente una riduzione del numero di e-mail, la possibilità di scambiare file in

cloud e lavorare in modalità wiki su documenti condivisi, ottimizzando così il flusso di lavoro.

Comunicazione agli investitori finanziari

Cyberoo gestisce attivamente la propria comunicazione con gli investitori finanziari attraverso una collaborazione con Reputation Value, un'agenzia di consulenza di Milano specializzata in comunicazione e ufficio stampa. Questa partnership consente a Cyberoo di interagire con i media e di diffondere informazioni chiave su eventi, risultati finanziari, novità aziendali e successi, raggiungendo un pubblico qualificato di lettori e potenziali investitori, con lo scopo di far conoscere la propria storia, professionalità, capacità di innovazione, attività e soluzioni.

L'attività con Reputation Value si concentra sulla creazione di contenuti strategici per veicolare l'immagine dell'azienda attraverso comunicati stampa, interviste e conferenze stampa, garantendo visibilità e consolidamento della reputazione di Cyberoo.

Per quanto riguarda le attività di **Investor Relations** (IR), Cyberoo gestisce la comunicazione finanziaria e istituzionale con investitori e intermediari finanziari come banche e analisti, chi si occupa della dematerializzazione delle azioni e della tenuta del libro soci o dei rapporti con Monte Titoli.

La società mantiene un costante dialogo con gli analisti finanziari, che seguono l'azienda, e organizza annualmente conference call per condividere i risultati finanziari annuali e semestrali così da rispondere alle domande degli investitori, che vengono invitati a partecipare tramite newsletter aziendale.

Durante il 2024, Cyberoo ha partecipato a numerosi eventi rivolti agli investitori, tra cui:

7 febbraio 2024	**European MidCap Event Francoforte**
21 febbraio 2024	**EnVent Winter Conference Milano**
17 aprile 2024	**Mid&Small London**
3,4 e 5 giugno 2024	**Mid&Small Virtual**

5 giugno 2024	**KT&Partners Annual Investors Summit Day**
6 giugno 2024	**European Midcap Event Paris**
17 giugno 2024	**Tech Day**
3 e 4 luglio 2024	**Mid&Small Virtual**
18 ottobre 2024	**Investor Day organizzato da Alantra in sede Cyberoo**
3 dicembre 2024	**Mid&Small Milan**

Questi eventi hanno rappresentato un'importante opportunità per Cyberoo di confrontarsi con investitori e analisti, promuovendo ulteriormente la propria crescita e consolidando la propria presenza sul mercato.

Eventi PR, attività istituzionali ed eventi con partner – Italia ed estero

Nel corso del 2024, Cyberoo ha rafforzato il proprio impegno nella diffusione della cultura della cybersecurity e dell'innovazione tecnologica, partecipando e organizzando numerosi eventi, tra attività PR, incontri istituzionali ed eventi con partner strategici, sia in Italia che all'estero su tutto il territorio nazionale. Le attività di PR hanno coinvolto stakeholder istituzionali, imprese, studenti e operatori del settore, consolidando la *brand awareness* e il posizionamento dell'azienda come punto di riferimento nel panorama italiano della cybersecurity. Cyberoo è intervenuta con speech, workshop e sessioni formative su temi chiave quali: intelligenza artificiale, rischio cyber, normative europee (come NIS2), rischio reputazionale e sicurezza delle infrastrutture digitali.

La collaborazione con i partner strategici ha rappresentato un pilastro fondamentale delle attività aziendali, contribuendo in modo significativo alla formazione, alla divulgazione e allo sviluppo commerciale. In questo ambito, sono stati organizzati oltre 30 eventi congiunti, rafforzando la sinergia con l'ecosistema di riferimento e promuovendo la condivisione di conoscenze e buone pratiche tra imprese e stakeholder.

Cyberoo ha inoltre promosso la propria vocazione internazionale attraverso la realizzazione di iniziative all'estero, con 5 eventi organizzati in Polonia,

confermando l'espansione della propria rete relazionale e la volontà di consolidare la presenza nei mercati internazionali.

Tra gli appuntamenti più significativi, si annoverano:

- **Cyber Crime Conference – Roma, 17–18 aprile 2024:** la 12ª edizione della Cyber Crime Conference organizzato da ICT Security Magazine a Roma, presso l'Auditorium della Tecnica. L'evento ha riunito esperti e aziende leader nel settore della sicurezza informatica, focalizzandosi sull'evoluzione delle minacce e sulle strategie di difesa. Cyberoo ha partecipato attivamente, contribuendo con approfondimenti tecnici sulle minacce informatiche avanzate, sulle soluzioni di difesa adottate dalle imprese, con un focus particolare su Managed Detection and Response (MDR), le ultime tendenze in fatto di cybersecurity connesse alla rapidità con la quale i cyber criminali operano su scala mondiale. Un approccio proattivo, dinamico, quanto necessario, che trae origine dall'imprevedibilità delle minacce informatiche e che oggi obbliga le aziende a dotarsi di soluzioni idonee, non soltanto a fronteggiarle ma anche a permettere ai responsabili IT di posizionarsi sempre un passo avanti rispetto ai cyber criminali.
- **HackInBo – Bologna, 7–8 giugno 2024**: Cyberoo ha rinnovato la propria partecipazione alla Spring Edition di HackInBo 2024, confermandosi partner storico dell'evento, giunto alla sua 23ª edizione. Tenutasi a Bologna il 7 e 8 giugno, HackInBo è la più importante conferenza sulla sicurezza informatica in Italia, punto di riferimento per professionisti IT, sistemisti, appassionati e aziende. Cyberoo ha contribuito con la propria esperienza sul campo, rafforzando la relazione con la community tech e confrontandosi su tematiche emergenti in ambito cyber.
- **Farete – Bologna, 4–5 settembre 2024**: in qualità di Partner RetIndustria, Cyberoo ha partecipato a Farete, l'evento annuale organizzato da Confindustria Emilia, dedicato al networking tra le imprese. I due giorni di eventi sono stati focalizzati su incontri B2B tra le aziende, offrendo a Cyberoo l'opportunità di presentare le proprie soluzioni innovative nel campo della cybersecurity. Con uno stand dedicato, l'azienda ha interagito con oltre 500 imprese, consolidando la propria rete di contatti e promuovendo la sicurezza informatica a livello industriale. Cyberoo ha anche

avuto una visibilità significativa sui materiali di comunicazione della Fiera, inclusi il catalogo espositori cartaceo e web, nonché nel materiale distribuito, come le oltre 2.000 shopper consegnate durante l'evento.

- **ICT Security Forum – Roma, 23–24 ottobre 2024**: il 22° Forum ICT Security si è tenuto a Roma, presso l'Auditorium della Tecnica. L'evento ha trattato temi cruciali come l'Intelligenza Artificiale, il Machine Learning, il Cloud Computing e il Quantum Computing, esplorando come queste tecnologie possano migliorare la resilienza e la sicurezza delle infrastrutture IT. Cyberoo ha contribuito attivamente con approfondimenti sulle soluzioni di Managed Detection and Response (MDR) e sull'importante tema della remediation, rispondendo alle sfide emergenti in un contesto digitale sempre più complesso.
- **Digital360 Awards – Lazise, 26-28 settembre 2024**: Cyberoo ha vinto il primo premio nella categoria "*Information & CyberSecurity*" ai prestigiosi Digital360 Awards e CIOsummIT 2024. L'evento ha visto Cyberoo premiata per il progetto "*La perfetta filiera della cybersecurity: dalla detection alla remediation*", realizzato in collaborazione con NPO Sistemi. Il tema che ha rappresentato il filo conduttore degli appuntamenti 2024 è stato "*The Butterfly Effect, la missione possibile del CIO: mettere ordine nel nuovo caos"*. Il progetto proposto da Cyberoo e NPO Sistemi ha l'obiettivo di proporre al mercato una filiera *always on* di identificazione delle minacce e mitigazione delle stesse con una specifica attività di remediation. La sfida consiste nello sviluppare una capacità di detection orientata alla più ampia visibilità sul perimetro logico delle aziende, ma anche sulla possibilità di attuare una remediation che oggi è ancora in larga scala basata su catene del soccorso frammentate e spesso inefficiente rispetto agli standard richiesti per mitigare anche le minacce più gravi e urgenti. I 140 CIO presenti all'evento hanno valutato i progetti innovativi che fanno ampio uso di Intelligenza Artificiale e coinvolgono lo sviluppo di diverse tecnologie utilizzate in ambito aziendale. Il premio ottenuto conferma l'alto livello di innovazione che Cyberoo porta sul mercato e l'apprezzamento continuo da parte delle aziende italiane, dimostrando la capacità di Cyberoo di rispondere on efficacia alle nuove sfide nel campo della cybersecurity.

- **Advanced Threat Summit – Varsavia, 13-15 novembre 2024**: Cyberoo ha partecipato all'Advanced Threat Summit, uno dei principali eventi di cybersecurity in Polonia. Durante l'evento, Cyberoo ha condotto una tavola rotonda sull'evoluzione delle esigenze aziendali in materia di cybersecurity, affrontando le sfide che i team di sicurezza interni devono superare e analizzando quando l'outsourcing può rappresentare una soluzione vantaggiosa rispetto all'investimento nel proprio team. Questa tavola rotonda ha offerto un'ottima opportunità per scambiare esperienze e acquisire conoscenze sulle strategie efficaci per rafforzare la protezione delle organizzazioni contro le minacce informatiche, confrontandosi con esperti e professionisti del settore.

Le donazioni

Ogni anno nel periodo natalizio Cyberoo devolve un contributo a un ente o associazione che sposi uno dei valori dell'azienda. Nel 2024 in particolare Cyberoo ha confermato il suo impegno verso l**Informatici Senza Frontiere (ISF)**, associazione no-profit che promuove l'inclusione digitale e la formazione, con particolare attenzione al divario digitale di genere. In particolare, Cyberoo ha sostenuto un nuovo percorso formativo per donne tra i 18 e i 50 anni, incentrato sulla gestione dei dati e della sicurezza informatica, con un focus sul linguaggio Python.

Inoltre, Cyberoo è stata coinvolta nel Festival ISF 2025 per il ventennale dell'associazione e ha contribuito all'organizzazione di un webinar sulla cybersecurity il 6 marzo 2025, a sensibilizzare sull'uso responsabile delle nuove tecnologie. Il sostegno a ISF rientra nell'impegno di Cyberoo per favorire la formazione e l'inclusione digitale, contribuendo a colmare il divario di genere nel settore tecnologico.

Capitolo 5

CAPITALE ECONOMICO FINANZIARIO

CAPITALE ECONOMICO FINANZIARIO
OVERVIEW

25 mil. €
valore economico generato
(+14% rispetto al 2023)

17 mil. €
valore economico distribuito
(+19% rispetto al 2023)

EBIT 6,47 mil. €
+6,5% rispetto al 2023

EBITDA 9,72 mil. €
+4,7% rispetto al 2023

5. Capitale economico-finanziario

Andamento della gestione

Il bilancio del Gruppo Cyberoo, relativo all'esercizio 2024, si è chiuso con un utile di 4.376.867 euro rispetto al risultato positivo di 3.963.448 euro realizzato nell'esercizio 2023. I ricavi del Gruppo hanno oltrepassato i 22 milioni di euro, con un incremento del 10% rispetto ai 20 milioni di euro realizzati al 31 dicembre 2023. Positivo è stato anche l'andamento dei principali indicatori economici:

- l'EBITDA del 2024 si è attestato a 9,72 milioni di euro, pari al 42,6% dei ricavi, con un incremento del 4,7% rispetto al 2023.
- l'EBIT del 2024 è stato pari a 6,47 milioni di euro, in crescita del 6,5% rispetto ai 6,08 milioni di euro dell'esercizio precedente.

Il valore economico generato e distribuito

Il prospetto che evidenzia il valore generato e distribuito viene elaborato sulla base del Conto Economico del bilancio di esercizio, con l'obiettivo di dare evidenza del valore economico direttamente generato dal Gruppo Cyberoo e la sua distribuzione agli stakeholder interni ed esterni.

Il **Valore Economico generato** si riferisce al Valore della produzione come da Bilancio di esercizio (Ricavi e Altri ricavi operativi), al netto delle perdite su crediti e integrato dei proventi finanziari. Il **Valore Economico trattenuto**, che per il 2024 è pari a 7,628 milioni euro, è relativo alla differenza tra Valore Economico generato e distribuito e comprende gli ammortamenti dei beni materiali e immateriali oltre alla fiscalità differita.

VALORE AGGIUNTO	2022	2023[8]	2024
Ricavi	17.287.908	21.746.026	24.567.052
Altri proventi	275.268	271.209	444.141

[8] Si segnala che è stato effettuato un restatement rispetto al valore dei ricavi e dei costi operativi 2023.

VALORE AGGIUNTO	2022	2023[8]	2024
Proventi finanziari	9.873	95.252	255.810
Totale valore economico generato	**17.573.049**	**22.112.487**	**25.267.003**
Costi operativi	6.202.565	7.107.418	8.690.517
Remunerazione del personale	4.589.142	5.596.319	6.570.914
Remunerazione dei finanziatori	239.838	489.446	484.680
Remunerazione degli investitori	-	-	-
Remunerazione della Pubblica Amministrazione	1.311.687	1.716.523	1.857.864
Liberalità esterne	49.700	35.250	35.000
Totale valore economico distribuito	**12.392.933**	**14.782.668**	**17.638.975**
Valore economico trattenuto	**5.180.116**	**7.167.531**	**7.628.028**

Gli investimenti

L'attività di **ricerca e sviluppo**, finalizzata allo studio e alla progettazione di nuovi prodotti, rappresenta un elemento fondamentale del modello industriale del Gruppo nonché la principale leva strategica.

Il Gruppo Cyberoo tramite le società Cyberoo S.p.A. e Cyberoo51 S.r.l. realizza attività precompetitive a carattere innovativo, indirizzando i propri sforzi su progetti ritenuti particolarmente innovativi quali attività di studio, analisi, ricerca e sviluppo di soluzioni non esistenti sul mercato della *cyber security*.

I progetti si pongono l'obiettivo di fornire alle società un servizio basato su specifici algoritmi di intelligenza artificiale che permettano di avere una visione quanto più completa delle cyber minacce relative a una specifica azienda, degli attacchi potenziali in termini di confidenzialità, integrità e disponibilità dei dati e dei servizi.

Approccio fiscale

Il Gruppo Cyberoo applica la legislazione fiscale in vigore, assicurando che siano osservati lo spirito e lo scopo che la norma e l'ordinamento prevedono per la materia oggetto di interpretazione. Nei casi in cui la disciplina fiscale alimenti

dubbi interpretativi o difficoltà applicative, viene perseguita una linea interpretativa ragionevole, avvalendosi della consulenza di qualificati professionisti esterni.

La sede fiscale del Gruppo è in Italia, dove vengono corrisposte le imposte.

L'approccio alla fiscalità del Gruppo Cyberoo è improntato alla trasparenza e alla totale aderenza alle normative locali, curando l'ambito della compliance e intercettando tutte le novità normative per ottemperare nelle tempistiche previste.

L'obiettivo del Gruppo, in questo ambito, è assicurare che:

- le dichiarazioni sul reddito e sul valore aggiunto vengano redatte in conformità alla disciplina vigente;
- il calcolo delle imposte avvenga nel rispetto dei principi tributari elaborati dalle norme vigenti e dalle circolari emesse dai vari uffici dell'amministrazione finanziaria;
- le operazioni di compensazione dell'IVA e le richieste di rimborso delle imposte abbia per oggetto crediti fiscali realmente sussistenti, certi e verificabili;
- le dichiarazioni sul valore aggiunto originate da rapporti transfrontalieri vengano depositate nel rispetto delle tempistiche e della disciplina tributaria.

Gli impatti fiscali sono tenuti in debita considerazione nella redazione della pianificazione strategica e operativa aziendale e rappresentano un essenziale elemento di valutazione del conseguente impatto economico-sociale.

La governance del controllo fiscale è demandata alla Direzione Amministrativa e Bilancio che, anche tramite il supporto di consulenti esterni, vigila sulla correttezza delle operazioni e applica la corretta normativa.

Tutte le richieste effettuate al Gruppo Cyberoo dalle autorità fiscali vengono gestite all'interno del corretto flusso informativo con un approccio da parte del Gruppo di totale trasparenza e dialogo costruttivo: i dati fiscali e il loro dettaglio sono regolarmente esposti nel bilancio annuale di esercizio e nella relativa Nota integrativa e quindi messi a disposizione dei soci e di tutti gli stakeholder.

Nel corso del triennio 2022-2024 non sono stati registrati contenziosi o contestazioni di tipo fiscale e, alla data del presente documento, non sono in essere contenziosi di carattere fiscale di rilievo.

Capitolo 6

CAPITALE UMANO

CAPITALE UMANO
OVERVIEW

105
dipendenti (+11,7% rispetto al 2023)

21 %
di dipendenti donne (a fronte del 15% nel settore)

99 %
contratti a tempo indeterminato

97 %
contratti full-time

62 %
dipendenti con età compresa
tra i 30 e i 50 anni

100 %
dei senior manager assunti
dalla comunità locale

0
Nessun infortunio sul lavoro

6. Capitale umano

Le politiche del personale

Il Gruppo Cyberoo considera le **persone** come una risorsa strategica per l'azienda: con il suo operato intende valorizzare il lavoro e le esperienze dei suoi dipendenti, garantendo condizioni di lavoro ottimali, il rispetto dei diritti umani e la trasparenza nel processo di selezione del personale.

Per il Gruppo è fondamentale che ogni dipendente contribuisca alla creazione di valore dell'organizzazione in un ambiente che promuova il benessere, il merito e lo sviluppo delle competenze in linea con i principi dell'azienda.

La gestione del personale è ispirata a principi di correttezza ed imparzialità, evitando favoritismi o discriminazioni, nel rispetto della professionalità e delle competenze del lavoratore. Al contempo, nel perseguimento degli obiettivi della Società, il lavoratore deve operare nella consapevolezza che l'etica rappresenta un interesse di primario rilievo per il Gruppo Cyberoo e che, pertanto, deve sempre conformarsi, nelle sue azioni, al rispetto del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 adottato, al Codice Etico e ai protocolli aziendali.

È proprio l'**Etica** il primo valore che l'Azienda persegue, con l'obiettivo di instaurare e mantenere tra i dipendenti un clima di reciproco rispetto e tutelare la dignità, l'onore e la reputazione di ciascuno.

La **crescita delle persone** è un altro dei valori aziendali cardine, dalla fase di recruiting e per tutta la durata della permanenza aziendale, grazie all'organizzazione di iniziative di formazione inter-aziendale mirate a rafforzare il legame tra Azienda e dipendenti.

I processi di selezione

La **politica di selezione** adottata da Cyberoo nella selezione di persone altamente specializzate su tutto il territorio italiano ha come obiettivo quello di mantenere alti i livelli di competenza e trasversalità, favorendo l'integrazione tra figure tecniche, commerciali e di staff con il duplice scopo di creare occupazione e di valorizzare e sviluppare professionisti sempre più verticali nel settore della cybersecurity.

Anche per il 2024 rimane alta l'attenzione sia nei riguardi delle risorse nel territorio emiliano locale, circa il 60% del totale della forza lavoro, ma anche delle risorse provenienti da altre Regioni, circa il 40%, per tutti i ruoli e livelli presenti in azienda. Al fine di agevolare l'integrazione di quest'ultimi e al fine di favorire la loro presenza in azienda, Cyberoo si mobilita sempre per organizzare riunioni periodiche presso la propria sede, sostenendo o rimborsando sia il costo di trasferta che di alloggio.

La selezione è svolta nel pieno rispetto delle pari opportunità e senza discriminazione alcuna, evitando favoritismi, clientelismo e agevolazioni, ispirando la propria scelta esclusivamente a criteri di professionalità e competenza. Il processo di selezione è, infatti, attento e strutturato e prevede una valutazione delle candidature sulla base di requisiti oggettivi, tramite colloqui tecnici e commerciali per valutarne le competenze e quanto altro necessario per fornire un giudizio obiettivo e colloqui attitudinali volti ad approfondire le motivazioni e i valori della persona. Tale flusso di selezione è condiviso con tutti i responsabili di Area in modo da garantirne l'ingaggio e una maggiore uniformità di valutazione.

Poiché le persone sono il fattore chiave per il raggiungimento degli obiettivi di Cyberoo, il processo di selezione riveste un ruolo fondamentale, in quanto destinato a individuare candidati in possesso delle skill, della professionalità, serietà e preparazione tecnica, corrispondenti ai profili effettivamente necessari alle esigenze della Società e che, al contempo, condividano i principi etici e i valori di onestà e lealtà cui Società si ispira.

Ogni persona coinvolta nel processo di selezione si attiene alle seguenti regole di comportamento:

- imparzialità nel trattamento dei candidati che partecipano all'iter di selezione;
- riservatezza sulle informazioni acquisite durante la selezione;
- indipendenza e astensione dal coinvolgimento in azioni che possano generare un conflitto di interessi e divieto di dar seguito a qualsiasi pressione indebita proveniente da soggetti interni o esterni.

Il candidato neoassunto viene accompagnato durante l'inserimento in azienda tramite un processo di ***on-boarding*** differenziato a seconda del profilo professionale.

Il processo di selezione di figure junior prevede il coinvolgimento di enti di formazione, di Università e di scuole superiori locali attraverso la stipula di convenzioni al fine di ospitare giovani talenti in stage e coinvolgerli in progetti già in essere o "ad hoc". L'iniziativa dell'azienda di offrirsi come ente ospitante rappresenta un'occasione per i giovani studenti di mettere in pratica le conoscenze apprese all'interno di un'organizzazione aziendale e di confrontarsi con un ambiente di lavoro complesso e dinamico; per l'azienda è invece un'opportunità per sviluppare mini-progetti, per addestrare giovani manager – in qualità di tutor - nella gestione di risorse, per conoscere, formare e valutare potenziali collaboratori futuri.

I dipendenti

Il numero di dipendenti è in costante aumento: nel 2024 l'organico ha raggiunto le **105 unità**, registrando una crescita del **40% rispetto al 2022**. Questo trend conferma la solidità e l'evoluzione dell'Azienda, che continua a rafforzare la propria struttura organizzativa sia in termini quantitativi che qualitativi.

Numero dipendenti[9]	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
	19	56	75	21	73	94	23	82	105

Le forme di impiego

Numero dipendenti per tipologia di contratto / per genere	2022			2023			2024		
Numero dipendenti	**Donne**	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**
Contratto a tempo indeterminato	19	56	75	21	73	94	23	81	104
Contratto a tempo determinato	-	-	-	-	-	-	-	1	1
Totale	**19**	**56**	**75**	**21**	**73**	**94**	**23**	**82**	**105**

[9] Con riferimento al GRI 2-7, i dati relativi alla classificazione del personale nelle categorie "Altro" e "Non rivelato" sono pari a zero e, pertanto, non state inserite le colonne relative a queste due categorie in tutte le tabelle del presente capitolo.

Numero dipendenti per tipo di impiego / genere	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Contratto full time	18	55	73	20	71	91	23	79	102
Contratto part time	1	1	2	1	2	3		3	3
Contratto con orario variabile	-	-	-	-	-	-	-	-	-
Totale	**19**	**56**	**75**	**21**	**73**	**94**	**23**	**82**	**105**

Numero dipendenti per tipologia di contratto / per genere	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Stagisti e tirocinanti	-	1	1	1	-	1	-	1	1
CO.CO.CO	-	-	-	-	-	-	-	-	-
Totale	**-**	**1**	**1**	**1**	**-**	**1**	**-**	**1**	**1**

Il personale dipendente di Cyberoo è assunto esclusivamente con regolare contratto di lavoro, in conformità alle leggi e alle normative vigenti al Contratto Collettivo Nazionale del terziario, distribuzione e servizi.

Nel 2024, quasi il 100% dei dipendenti è assunto tramite contratto a tempo indeterminato (a accezione di un solo dipendente con contratto a tempo determinato), a dimostrazione della stabilità e valorizzazione del capitale umano all'interno di Cyberoo. Il part time viene richiesto principalmente per motivi familiari.

Inoltre, nel triennio 2022–2024 si registra un aumento del numero e della percentuale di Senior Manager assunti dalla comunità locale, passati da 2 su 3 nel 2022 a 7 su 7 nel 2024, in linea con una crescente presenza di figure locali nelle sedi operative significative.

Senior manager assunti dalla comunità locale	2022	2023	2024
N. Senior manager presso le sedi operative significative assunti dalla comunità locale[10]	2	2	7
N. totale di Senior manager	3	4	7
% di Senior manager presso le sedi operative significative assunti dalla comunità locale	**67%**	**50%**	**100%**

Diversità

La componente maschile continua a essere preponderante in Azienda, riflettendo una tendenza comune nel settore IT: in Italia, infatti, la percentuale media di donne nel comparto della cybersecurity si attesta attorno al 15%. **Cyberoo, con una presenza femminile del 22% nel 2024**, mantiene una posizione più favorevole rispetto alla media del mercato, confermando l'attenzione al tema della diversità e dell'inclusione.

La totalità delle dipendenti donne ricopre ruoli impiegatizi, con un progressivo incremento del numero di profili femminili in ingresso: **23 donne su un totale di 105 dipendenti** al 31 dicembre 2024. La composizione dell'organico vede inoltre una netta predominanza della categoria degli **impiegati**, che rappresentano il **93% della forza lavoro aziendale**, mentre i **quadri** si attestano al 7%.

Dipendenti per categoria/ genere	2022			2023			2024		
	Donne	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**
Dirigenti	-	-	**-**	-	-	**-**	-	-	**-**
Quadri[11]	-	3	**3**	-	4	**4**	-	7	**7**
Impiegati	19	53	**72**	21	69	**90**	23	75	**98**
Operai	-	-	**-**	-	-	**-**	-	-	**-**
Totale	**19**	**56**	**75**	**21**	**73**	**94**	**23**	**82**	**105**

[10] Per comunità locale si fa riferimento alle Unità Locali della Regione Emilia-Romagna (Reggio Emilia e Piacenza). Mentre per Senior manager si fa riferimento alla categoria al Livello Quadro.

[11] La percentuale di Senior manager (quadri) presso le sedi operative dell'Azienda che sono stati assunti dalla comunità locale è pari al 50%.

Di seguito si riportano le percentuali di dipendenti divise per categoria e genere, rapportati al totale dei dipendenti al 31 dicembre 2022, 2023 e 2024.

Dipendenti per categoria/ Genere %	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Dirigenti	-	-	-	-	-	-	-	-	-
Quadri	-	4%	4%	-	4%	4%	-	7%	7%
Impiegati	25%	71%	96%	22%	74%	96%	22%	71%	93%
Operai	-	-	-	-	-	-	-	-	-
Totale	25%	75%	100%	22%	78%	100%	22%	78%	100%

Anche nel 2024 la distribuzione per fasce d'età conferma la prevalenza di dipendenti nella fascia tra i **30 e i 50 anni**, pari al **69% del totale aziendale**, seguita dal 28% di under 30 e dal 15% di over 50. In particolare, i quadri si collocano quasi esclusivamente nelle fasce più esperte (dai 30 anni in su), mentre la categoria impiegatizia abbraccia tutte le fasce d'età.

Dipendenti per categoria/ fascia d'età	2022				2023				2024			
	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale
Dirigenti	-	-	-	-	-	-	-	-	-	-	-	-
Quadri	-	1	2	3	-	1	3	4		2	5	7
Impiegati	17	47	8	72	27	57	6	90	26	63	9	98
Operai	-	-	-	-	-	-	-	-	-	-	-	-
Totale	17	48	10	75	27	58	9	94	26	65	14	105

Dipendenti per categoria/fascia d'età %	2022				2023				2024			
	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale	Fino a 29 anni	Da 30 a 50 anni	Oltre 50 anni	Totale
Dirigenti	-	-	-	-	-	-	-	-	-	-	-	-
Quadri	-	1%	3%	4%		1%	3%	4%	-	2%	5%	7%
Impiegati	22%	63%	11%	96%	29%	61%	6%	96%	25%	60%	9%	93%
Operai	-	-	-	-	-	-	-	-	-	-	-	-
Totale	22%	64%	14%	100%	29%	62%	9%	100%	28%	69%	15%	100%

L'Azienda è molto sensibile al tema della *diversity* e ha cercato nel corso degli anni di creare opportunità di orientamento e formazione che coinvolgano il più possibile le donne come gli uomini, ad avvicinarsi al settore partecipando a giornate di formazione nelle scuole, eventi in Università, piuttosto che stage formativi.

Turnover

Nel triennio 2022–2024 la popolazione aziendale è cresciuta in modo costante, passando da 75 unità al 31/12/2022 a 94 unità al 31/12/2023, per poi consolidarsi nel 2024 a 105 unità con un andamento più stabile, in linea con la fase di assestamento organizzativo avvenuta durante l'anno.

Nel corso di questi anni, l'Azienda ha privilegiato l'assunzione di personale già qualificato e con elevata esperienza nelle aree core del business, con una prevalenza di profili appartenenti alla fascia d'età tra i 30 e i 50 anni.

Le percentuali di turnover sono state calcolate, in linea con i requisiti del GRI Standard, sulla base del totale dei dipendenti al 31 dicembre di ciascun anno, confrontando i tassi di turnover positivo (assunzioni) con quelli di turnover negativo (cessazioni).

Nel 2024 si è registrato un turnover positivo pari al 27%, a fronte di un turnover negativo del 16%, confermando una dinamica aziendale complessivamente ancora orientata alla crescita, seppur in un contesto meno espansivo rispetto agli anni precedenti. L'Azienda ha comunque continuato a investire nell'inserimento di nuove risorse, mantenendo la capacità di attrarre professionalità coerenti con le esigenze strategiche, soprattutto nelle fasce d'età intermedie e in profili specializzati.

Assunzioni[12]	**2022**			**2023**			**2024**		
	Donne	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**	**Donne**	**Uomini**	**Totale**
Fino a 29 anni	4	6	10	7	9	16	3	6	9
Da 30 a 50 anni	3	16	19	4	16	20	4	10	14
Oltre 50 anni	1	-	1	-	1	1	-	5	5
Totale	**8**	**22**	**30**	**11**	**26**	**37**	**7**	**21**	**28**

[12] All'interno delle tabelle "Assunzioni" e "Cessazioni" sono inclusi, nel triennio di riferimento, anche i tirocinanti e gli stagisti.

Cessazioni	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Fino a 29 anni	2	2	4	-	5	5	-	-	-
Da 30 a 50 anni	2	16	18	6	6	12	6	9	15
Oltre 50 anni	1	3	4	-	1	1	-	2	2
Totale	**5**	**21**	**26**	**6**	**12**	**18**	**6**	**11**	**17**

Tasso di turnover	2022			2023			2024		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Turnover negativo - cessazioni	26%	38%	**35%**	29%	16%	**13%**	26%	13%	**16%**
Turnover positivo - assunzioni	42%	39%	**40%**	52%	36%	**36%**	30%	26%	**27%**

I congedi parentali

Congedi parentali	2022			2023			2024		
	Donna	Uomo	Totale	Donna	Uomo	Totale	Donna	Uomo	Totale
Dipendenti che hanno avuto diritto al congedo parentale	-	-	**-**	4	4	**8**	7	2	**9**
Dipendenti che hanno usufruito del congedo parentale	-	-	**-**	4	4	**8**	7	2	**9**
Dipendenti che sono tornati al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale	-	-	**-**	1	4	**5**	4	2	**6**
Dipendenti che sarebbero dovuti tornare al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale	-	-	**-**	1	4	**5**	4	2	**6**
Dipendenti che sono tornati al lavoro dopo aver usufruito del congedo parentale e che sono ancora dipendenti dell'organizzazione nei 12 mesi successivi al rientro	-	-	**-**	1	3	**4**	4	2	**6**

Nel 2023 e 2024, tutti i dipendenti che hanno usufruito del congedo parentale sono rientrati nei tempi previsti e risultano ancora in forza dopo 12 mesi, segnalando una buona continuità nel reinserimento post-congedo.

Formazione e competenze

L'Azienda per gli anni 2022, 2023 e 2024 ha strutturato dei percorsi di formazione su più livelli e moduli con focus sulla crescita dei propri dipendenti in termini di collaborazione e comunicazione efficace.

Nello specifico sono stati organizzati con la scuola di Formazione e coaching **Creattività** degli incontri formativi sia online che in presenza, così strutturati:

- ***Modello Brainbow***: dedicato a tutta la popolazione aziendale e volto a migliorare la gestione delle relazioni interpersonali sia in campo privato che professionale;
- ***Corsi di Public Speaking***: dedicati alle figure commerciali, per andare a migliorare la loro comunicazione nei confronti di clienti e stakeholder esterni all'Azienda;
- ***Corsi sulla Leadership & Gestione del Feedback***: rivolto alle figure manageriali, che in Azienda hanno la responsabilità della gestione e mentoring di altre risorse, in qualità quindi di team leader.

Accanto ai percorsi trasversali, l'Azienda ha progressivamente ampliato l'offerta formativa anche in ambito specialistico, consolidando il proprio impegno verso una cultura della formazione continua.

Nel 2024, tuttavia, le attività formative hanno subito una contrazione rispetto al passato, a seguito di una riorganizzazione dell'Ufficio Risorse Umane che ha temporaneamente rallentato la pianificazione e l'erogazione dei corsi.

Nonostante questa fase di transizione, sono stati attivati interventi formativi mirati su tematiche strategiche e di attualità, come le nuove normative in ambito **cybersecurity** (NIS2 e DORA), oltre a corsi destinati a profili chiave dell'organizzazione – tra cui un **master in contrattualistica** di impresa per il **Legal Specialist**, percorsi tecnici per **Product Manager** e momenti formativi per l'**Ufficio HR**, con focus su strumenti e metodi per una più efficace ricerca e selezione del personale.

In vista del 2025, è stato strutturato un piano formativo volto a rafforzare le competenze interne attraverso iniziative su tematiche trasversali e tecnico-specialistiche. L'Azienda intende inoltre incentivare modalità di apprendimento flessibili, anche tramite soluzioni e-learning, per garantire maggiore accessibilità e continuità nei percorsi di sviluppo professionale.

Welfare aziendale

Cyberoo, nel porre al centro delle strategie di crescita e sviluppo aziendale le proprie risorse umane, ha rinnovato l'attenzione nei loro confronti attraverso iniziative legate al welfare aziendale: l'iscrizione al **Fondo Est** (Ente Assistenza Sanitaria Integrativa del Commercio, del turismo e dei Servizi e settori Affini). Tale fondo ha l'obiettivo di supportare i bisogni e le necessità dei lavoratori, fornendo prestazioni di assistenza sanitaria integrative a quelle del Sistema Sanitario Nazionale (SSN). Hanno diritto alle prestazioni di assistenza sanitaria garantite da Fondo Est tutti i lavoratori dipendenti a tempo indeterminato e gli apprendisti ed è consentita l'iscrizione di lavoratori dipendenti con contratto a tempo determinato di durata superiore a 3 mesi.

Tra le altre misure, è prevista l'adozione dello ***smart working*** semplificato che ha accelerato il processo di flessibilità del lavoro, attualmente regolamentato da accordo individuale per 3 giorni a settimana, valido per tutti i dipendenti a prescindere dalla funzione lavorativa.

Dal 2024 tutti i 105 dipendenti del Gruppo sono coperti da assicurazione per invalidità e disabilità.

Sarà intenzione del Gruppo consolidare questo modus operandi e continuare a investire nel benessere dei dipendenti.

Salute e sicurezza sul lavoro

Nel rispetto della persona quale elemento indispensabile al raggiungimento degli obiettivi dell'Azienda, Cyberoo si impegna affinché la propria attività, i propri impianti e servizi siano compatibili con l'obiettivo della miglior prevenzione e protezione della sicurezza e della salute dei lavoratori, nell'ottica di minimizzare i rischi derivanti dall'attività lavorativa normale, da situazioni particolari o di emergenza.

La Società si impegna a diffondere e consolidare una cultura della sicurezza, sviluppando la consapevolezza dei rischi e il rispetto della normativa vigente in materia di prevenzione e protezione, e promuovendo comportamenti responsabili da parte di tutti; inoltre, opera per preservare e migliorare, soprattutto con azioni preventive, le condizioni di lavoro, la salute e la sicurezza dei Dipendenti.

Cyberoo si impegna pertanto a:

- eliminare/ridurre al minimo i rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte;
- adottare, per l'esercizio dell'attività produttiva, attrezzature, macchinari e impianti rispondenti ai requisiti essenziali di sicurezza;
- sostituire, per quanto riguarda i prodotti utilizzati, ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
- limitare al minimo il numero dei lavoratori che sono, o che possono essere, esposti ai rischi;
- garantire idonea informazione, formazione, sensibilizzazione e addestramento in materia di sicurezza e di salute a tutti i lavoratori.

Al fine della prevenzione, la Società assicura il rispetto delle leggi e delle normative di settore: per questo motivo viene redatto il **Documento di Valutazione dei Rischi (DVR)**, dove sono stati individuati gli specifici fattori di rischio potenziale relativi a tali ambiti di riferimento operativi e il **Documento di Valutazione dei Rischi Interferenti (DUVRI)**, dove sono stati valutati i "rischi interferenti" in relazione agli appalti. Viene inoltre periodicamente redatto e aggiornato un documento che contiene il piano di lavoro e gli interventi di miglioramento (**Piano di miglioramento**). Sono stati inoltre organizzati per il 2024 i corsi di sicurezza sul lavoro, addetti antincendio e primo soccorso.
Come previsto dal D.Lgs 81/08, è istituito un servizio di sorveglianza sanitaria (medico competente) con lo scopo di controllare lo stato di salute dei dipendenti e di esprimere il giudizio di idoneità alla mansione specifica cui il dipendente è assegnato.
Inoltre, il Gruppo Cyberoo ha nominato come **Responsabile del Servizio di Prevenzione e Protezione (RSPP)** una persona esterna. Tale figura, coordinando il servizio di prevenzione e protezione, si reca in azienda con regolare frequenza e si

occupa della gestione della sicurezza negli ambienti lavorativi e dei rapporti con i diversi enti e organismi di controllo e certificazione e si coordina con le rappresentanze dei lavoratori per la sicurezza e gli Amministratori.

Gli infortuni

Nel corso del 2024, così come nel 2023, non sono stati registrati infortuni mentre nel 2022 è stato registrato un solo infortunio (in itinere).

Infortuni sul lavoro[13]	2022	2023	2024
Mortali	-	-	-
Incidenti gravi	-	-	-
Altri Incidenti[14]	1	-	-
Totale Incidenti registrati	1	-	-
Di cui: Incidenti in itinere	1	-	-
Giorni assenza per infortuni	4	-	-
Totale ore lavorate	125.565	157.638	101.947
Tasso di decessi risultanti da infortuni sul lavoro	**-**	**-**	**-**
Tasso di infortuni sul lavoro con gravi conseguenze (ad esclusione dei decessi)	**-**	**-**	**-**
Tasso di infortuni sul lavoro registrabili	**7,96**	**-**	**-**

[13] Il tasso di infortuni sul lavoro registrabili è stato calcolato come di seguito: numero di infortuni sul lavoro su ore lavorate per 1.000.000.

[14] Incidente inferiore a un mese.

Capitolo 7

CAPITALE AMBIENTALE

CAPITALE AMBIENTALE
OVERVIEW

-65 %
di rifiuti prodotti dal Gruppo

-2,5 %
di riduzioni di Emissioni di CO_2 dirette
e indirette (Scope 1 e Scope 2)

-41 %
di prelievi idrici

Con 24bottles il gruppo ha ridotto di 80 grammi
per dipendente le emissioni di CO_2 in atmosfera

7. Capitale ambientale

Cyberoo, considerando la tutela dell'ambiente essenziale per uno sviluppo sostenibile, si propone di contemperare le esigenze di sviluppo economico e di creazione di valore con il rispetto e la salvaguardia ambientale.

Obiettivo primario della Società è quindi quello di sviluppare le attività di business nell'ottica di un miglioramento delle performance e nel rispetto dell'ambiente.

Responsabilità ambientale

Pur operando nel settore dei servizi che per sua natura non presenta generalmente aree di rischio specifiche rispetto alla sfera ambientale, il Gruppo Cyberoo non si limita ad agire passivamente ma promuove, nelle proprie attività quotidiane, comportamenti virtuosi in merito all'utilizzo razionale delle risorse e alla riduzione dei consumi.

Il management, consapevole del proprio ruolo e dei propri obblighi nei confronti dell'ambiente in cui opera, ha intrapreso un percorso di miglioramento delle proprie prestazioni nell'ottica di sviluppare soluzioni di valore e sostenibili nel rispetto delle normative e capaci di soddisfare le richieste e le aspettative dei propri stakeholder.

Gli obiettivi principali della **Politica ambientale** di Cyberoo vengono di seguito sintetizzati:

- rispettare leggi, norme e regolamenti vigenti relativi al settore e ad altre eventuali prescrizioni sottoscritte dalla Società;
- coinvolgere il personale, garantendo un elevato livello di professionalità, anche nelle tematiche di sostenibilità ambientale;
- scegliere partner e fornitori che dichiarano di agire nell'ottica di un miglioramento continuo delle loro prestazioni ambientali;
- efficacia, efficienza e affidabilità, impiegando tutte le risorse necessarie al fine di garantire il rispetto dei principi di diligenza e correttezza;
- operare riducendo la produzione di rifiuti, prevenendo l'inquinamento e provvedendo allo smaltimento di rifiuti in conformità alla normativa in vigore;

- rinnovare sistematicamente il proprio parco automezzi, consentendo di mantenere basso l'impatto ambientale dei veicoli impiegati;
- divulgare la cultura ambientale tra i propri dipendenti, clienti e fornitori;
- gestire in maniera sostenibile le risorse naturali e l'energia all'interno delle sedi aziendali, riducendo gli sprechi e presidiando il monitoraggio e il controllo degli aspetti ambientali.

Consumi energetici

Il Gruppo Cyberoo crede fermamente nello sviluppo sostenibile e di conseguenza non possono essere ignorati i consumi energetici derivanti dalle soluzioni tecnologiche.

Questo si traduce nel saper scegliere con attenzione fornitori capaci di garantire non solo sostenibilità economica ma anche quella ambientale.

I consumi energetici (e le relative emissioni) di Cyberoo sono relativi a:

- Energia elettrica, prelevata dalla rete e utilizzata per l'infrastruttura tecnologica (server[15]);
- Gas per il riscaldamento della sede centrale;
- Diesel, benzina e GPL per l'alimentazione delle auto aziendali. Relativamente a quest'ultima voce, il Gruppo ha avviato un'attività di monitoraggio continuativo per raccogliere dati quantitativi a supporto delle proprie politiche di mobilità sostenibile. Inoltre, è stata installata una colonnina di ricarica elettrica in una delle sedi del Gruppo.

Nelle successive tabelle sono riportati i consumi energetici relativi al triennio 2022 - 2024.

Nel 2024, il Gruppo Cyberoo ha registrato un **consumo energetico totale pari a 2.652 GJ**, in leggero calo rispetto al 2023 (-2%). Questa riduzione è principalmente dovuta alla diminuzione dell'energia elettrica acquistata, passata da 229 GJ a 167 GJ, grazie a interventi mirati di efficientamento delle infrastrutture IT e alla razionalizzazione degli spazi aziendali. I consumi di carburante per la flotta

[15] I server sono localizzati in centri terzi. Si specifica che essi sono certificati ISO 14001:2015 e ISO 50001:2018

aziendale si mantengono invece sostanzialmente stabili: **2.397 GJ** per il diesel e **88 GJ** per la benzina.

Parallelamente, le **emissioni di gas serra (GHG)** risultano in leggera diminuzione. Il totale delle **emissioni Scope 1 e Scope 2 (market-based)** per l'anno 2024 è pari a **198 tCO_2e**, in calo del 2% rispetto alle **203 tCO_2e del 2023**.

Energia consumata (GJoule)[16]	2022	2023	2024
Energia elettrica			
Energia elettrica acquistata	217	229	167
Di cui da fonti non rinnovabili	*217*	*229*	*167*
Di cui da fonti rinnovabili	-	-	-
Carburanti			
GPL	-	-	-
Diesel	1.708	2.377	2.397
Benzina	64	96	88
Totale	**1.989**	**2.702**	**2.652**

[16] I fattori di conversione impiegati per trasformare i consumi energetici in GJ sono stati derivati dal documento UK Government GHG Conversion Factors for Company Reporting (versione 2024), pubblicato dal Department for Energy Security and Net Zero del Regno Unito (in precedenza veniva invece sviluppato dal c.f. DEFRA). Tale documento, è riconosciuto per la regolarità degli aggiornamenti, l'elevata qualità dei dati e l'ampia copertura delle fonti di energia, motivo per cui è ampiamente adottato anche al di fuori del Regno Unito per ricavare i consumi di energia e le emissioni di ambito 1. I dati relativi all'anno fiscale 2022 sono stimati sulla base dei dati relativi al biennio precedente in quanto non disponibili.

Rispetto alla precedente rendicontazione il consumo di gas è stato considerato all'interno della quota dei consumi derivanti dal teleriscaldamento.

Emissioni

Per dare un contributo indiretto alla compensazione delle emissioni, il Gruppo Cyberoo ha deciso nel corso del 2021 di finanziare interventi specifici di plantumazione: con l'aiuto di **Treedom**, sono stati piantati 100 alberi da frutto in Kenya, Tanzania e Colombia contribuendo così a sottrarre più di 10 tonnellate di CO2 dall'atmosfera (nei primi 10 anni).

Con l'aiuto, invece, di **24bottles** è stata realizzata e fornita una bottiglia per ciascun dipendente con l'obiettivo di ridurre l'utilizzo di bottiglie di plastica monouso, evitando di rilasciare in atmosfera circa 80 grammi di CO2 (per ogni bottiglia di plastica monouso).

Emissioni GHG Scope 1 (tCO2e) – Scope 1[17]	**2022**	**2023**	**2024**
Emissioni dirette			
GPL	-	-	-
Gasolio	128	168	169
Benzina	5	6	6
Emissioni complessive – Totale Scope 1	**133**	**174**	**175**
Emissioni GHG Scope 2 (tCO2e) – Location Based[18]			
Emissioni indirette			
Energia elettrica acquistata	15	19	12
Emissioni Complessive – Totale Scope 2	**15**	**19**	**12**
Totale emissioni Scope 1 + Scope 2	**148**	**193**	**187**
Emissioni GHG Scope 2 (tCO2e) – Market Based[19]			
Emissioni indirette			
Energia elettrica acquistata	27	29	23
Emissioni Complessive – Totale Scope 2	**27**	**29**	**23**
Totale emissioni Scope 1 + Scope 2	**160**	**203**	**198**

[17] I fattori di emissione impiegati per il calcolo delle tCO2e Scope 1 sono tratti dal documento UK Government GHG Conversion Factors for Company Reporting (versione 2024), pubblicato dal Department for Energy Security and Net Zero del Regno Unito (in precedenza veniva invece sviluppato dal c.f. DEFRA). Tale documento, è riconosciuto per la regolarità degli aggiornamenti, l'elevata qualità dei dati e l'ampia copertura delle fonti di energia, motivo per cui è ampiamente adottato anche al di fuori del Regno Unito per ricavare i consumi di energia e le emissioni di ambito 1.

I dati delle emissioni relativi al triennio sono stati rettificati in quanto i consumi di gas sono stati conteggiati all'interno del teleriscaldamento.

[18] La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Location Based per il 2022 e 2023 è *Terna Confronti internazionali 2019*. La fonte dei fattori di emissione utilizzati per il calcolo 2024 è Ispra 2024.

[19] La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Market Based per il 2022 e 2023 è l'*European Residual Mixes "AIB"* ultimo aggiornamento (31.05.2021). La fonte dei fattori di emissione utilizzati per il calcolo 2024 è l'*European Residual Mixes "AIB"* (2023) ultimo aggiornamento al 2024.

Utilizzo responsabile delle risorse naturali

Acqua

L'acqua per le società del Gruppo Cyberoo non è una risorsa critica in quanto non è utilizzata ai fini industriali. La gestione dell'approvvigionamento idrico e dello smaltimento è affidata alla capogruppo per la quasi totalità, la quale adotta specifiche politiche di gestione dei reflui.

Le società si impegnano a monitorare costantemente i propri consumi, per individuare eventuali perdite ed intervenire con tempestività, riducendo al minimo il proprio impatto ambientale in questo senso.

Acqua consumata (in ML)[20]	2022	2023	2024
Risorse idriche di terze parti - fornitori idrici *Di cui: Acqua dolce (≤1.000 mg/l di solidi disciolti totali)*	134	279	164
Totale (in ML)	**134**	**279**	**164**

I **prelievi di acqua** di Cyberoo avvengono dalla rete dell'acquedotto pubblico e riguardano prevalentemente utilizzi di tipo sanitario in quantità modeste.

Nonostante l'incremento avvenuto nel 2023, con un consumo idrico pari a circa 279 mL rispetto ai 134 mL del 2022, nel 2024 il Gruppo Cyberoo ha registrato una riduzione di circa il 41% dei consumi, attestatisi a circa 164 mL.

Rifiuti

Le società del Gruppo Cyberoo adottano tutte le misure necessarie per lo smaltimento dei dispositivi tecnologici che sono comunque la minima parte siccome la gestione dei dispositivi è affidata alla Capogruppo. Per i rifiuti assimilabili a quelli civili, Cyberoo ha introdotto la raccolta differenziata.

[20] I dati del 2022 sono stati aggiornati, poiché dal 2023 si è utilizzata una metodologia differente per l'estrazione dei dati sul prelievo di acqua.

Rifiuti prodotti (in t)[21]	2022	2023	2024[22]
Rifiuti non pericolosi	36,34	16,60	5,53
Rifiuti pericolosi	5,24	3,70	1,54
Totale rifiuti prodotti	**41,58**	**20,30**	**7,07**

Nel 2024, i rifiuti prodotti dal Gruppo Cyberoo sono stati pari a 7,07 tonnellate, di cui circa il 78% sono rifiuti non pericolosi (5,53 tonnellate). Rispetto al 2023, quando i rifiuti prodotti erano 20,30 tonnellate (con l'82% non pericolosi), si registra una diminuzione significativa, confermando la continua ottimizzazione nella gestione e smaltimento dei rifiuti.

[21] I dati relativi ai rifiuti prodotti sono stati rettificati in quanto è stata utilizzata una differente metodologia di calcolo. I dati relativi al triennio fanno riferimento alla capogruppo Sedoc.

[22] Nel 2024 Cyberoo S.p.A. non ha effettuato smaltimenti di rifiuti. Le uniche operazioni sui rifiuti nel gruppo sono state effettuate dalla capogruppo Sedoc, che ha gestito esclusivamente rifiuti destinati al recupero (codice R13).

GRI Content Index

Ove non diversamente indicato, sono stati utilizzati i GRI Standards pubblicati nel 2021.

Statement of use	Gruppo Cyberoo ha redatto la presente informativa non finanziaria con riferimento agli Standard GRI per il periodo 1° gennaio 2024 - 31 dicembre 2024 secondo l'opzione "with reference".
GRI 1	GRI 1: Foundation 2021
GRI Sector Standard(s) applicabile	N/A

GRI SUSTAINABILITY REPORTING STANDARD			RIFERIMENTO CAPITOLO / PARAGRAFO	PAG.	NOTE APPLICAZIONE STANDARD / OMISSIONI
GENERAL DISCLOSURES					
GRI 2: General Disclosures 2021	**2-1**	Dettagli organizzativi	1. Identità e strategia/Il Gruppo	11	
	2-2	Entità incluse nella rendicontazione di sostenibilità dell'organizzazione	Nota Metodologica	7	
	2-3	Periodo di rendicontazione, frequenza e punto di contatto	Nota Metodologica	7	
	2-4	Revisione delle informazioni	Nota Metodologica	7	
	2-5	Assurance esterna	Nota Metodologica	7	Il presente Bilancio di Sostenibilità non è stato oggetto di revisione da parte di un ente terzo

	2-6	Attività, catena del valore e altri rapporti di business	1. Identità e strategia/Il modello di business	41	
	2-7	Dipendenti	6. Capitale umano/I Dipendenti	125	
	2-8	Lavoratori non dipendenti	6. Capitale umano/I Dipendenti	126	
	2-9	Struttura e composizione della governance	2. Governance/La Governance	61	
	2-10	Nomina e selezione del massimo organo di governo	2. Governance/La Governance	61	
	2-11	Presidente del massimo organo di governo	2. Governance/La Governance	61	
	2-14	Ruolo del massimo organo di governo nella rendicontazione di sostenibilità	Nota Metodologica	7	
	2-16	Comunicazione delle criticità	2. Governance/La Governance	61	Non sono state comunicate preoccupazioni critiche al più alto organo di governo in quanto non sono state riscontrate nel periodo di rendicontazione
	2-22	Dichiarazione sulla strategia di sviluppo sostenibile	Lettera agli Stakeholder	5	
	2-25	Processi volti a rimediare agli impatti negativi	1. Identità e strategia/Analisi di materialità	33	Rientra nel management approach dei temi materiali
	2-27	Conformità e leggi e regolamenti	2. Governance/Compliance normativa in ambito ESG		Nel corso del 2024 non si sono verificati eventi che hanno dato origine a sanzioni e/o contenziosi per non conformità a leggi, normative in

					materia ambientale, sociale ed economica.
	2-28	Appartenenza ad associazioni	3. Capitale infrastrutturale/Il valore delle partnership	76	
	2-29	Approccio al coinvolgimento degli stakeholder	1. Identità e strategia/Analisi di materialità	33	
	2-30	Contratti collettivi	6. Capitale umano/I Dipendenti	125	
TEMI MATERIALI					
GRI 3: Temi materiali 2021	**3-1**	Processo di determinazione dei temi materiali	1. Identità e strategia/Analisi di materialità	33	
	3-2	Elenco di temi materiali	1. Identità e strategia/Analisi di materialità	33	
ETICA E INTEGRITÀ NELLA CONDOTTA DEL BUSINESS					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	2. Governance	61	
GRI 205: Anticorruzione 2016	**205-3**	Episodi di corruzione accertati e azioni intraprese	2. Governance		Nessun episodio di corruzione accertato nel corso del presente esercizio
GRI 206: Comportamento anticoncorrenziale 2016	**206-1**	Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche	2. Governance		Non sono state rilevate azioni legali per comportamento anticorrenziale, antitrust e pratiche monopolistiche nel corso del presente esercizio

GRI 207: Imposte 2019	**207-1**	Approccio alla fiscalità	5. Capitale economico-finanziario/Approccio fiscale	118	
ANTICORRUZIONE E COMPLIANCE					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	2. Governance	61	
GRI 205: Anticorruzione 2016	**205-3**	Episodi di corruzione accertati e azioni intraprese	2. Governance		Nessun episodio di corruzione accertato nel corso del presente esercizio
GRI 206: Comportamento anticoncorrenziale 2016	**206-1**	Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche	2. Governance		Non sono state rilevate azioni legali per comportamento anticorrenziale, antitrust e pratiche monopolistiche nel corso del presente esercizio
GOVERNANCE TRASPARENTE E GESTIONE DEI RISCHI DI SOSTENIBILITÀ					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	2. Governance	61	
GRI 206: Comportamento anticoncorrenziale 2016	**206-1**	Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche	2. Governance/Compliance normativa in ambito ESG		Non sono state rilevate azioni legali per comportamento anticorrenziale, antitrust e pratiche monopolistiche nel corso del presente esercizio
TUTELA DEL BRAND E REPUTAZIONE					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	3. Capitale infrastrutturale	67	

CREAZIONE E DISTRIBUZIONE DELLA RICCHEZZA GENERATA					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	5. Capitale economico-finanziario	117	
GRI 201: Performance economiche 2016	**201-1**	Valore economico direttamente generato e distribuito	5. Capitale economico-finanziario/Il valore economico generato e distribuito	117	
SOLIDITÀ E RESILIENZA ECONOMICA					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	5. Capitale economico-finanziario	117	
GRI 201: Performance economiche 2016	**201-1**	Valore economico direttamente generato e distribuito	5. Capitale economico-finanziario/Il valore economico generato e distribuito	117	
GRI 203: Impatti economici indiretti 2016	**203-1**	Investimenti infrastrutturali e servizi finanziati	5. Capitale economico-finanziario/Gli investimenti	118	
RICERCA E INNOVAZIONE TECNOLOGICA					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	3. Capitale infrastrutturale/Innovazione e digitalizzazione	67	
QUALITÀ, SICUREZZA E AFFIDABILITÀ DEI SERVIZI					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	4. Capitale relazionale	81	
GRI 416: Salute e sicurezza dei clienti 2016	**416-2**	Episodi di non conformità riguardanti impatti sulla salute e sulla sicurezza di prodotti e servizi	4. Capitale relazionale/Qualità, sicurezza e affidabilità dei servizi	85	Nel corso del 2024 non si sono verificati casi di non conformità riguardanti impatti sulla salute e sulla sicurezza di prodotti e servizi offerti

LOTTA AL CAMBIAMENTO CLIMATICO					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	7. Capitale ambientale	137	
GRI 305: Emissioni 2016	**305-1**	Emissioni dirette di GHG (Scope 1)	7. Capitale ambientale/Emissioni	140	
	305-2	Emissioni indirette di GHG da consumi energetici (Scope 2)	7. Capitale ambientale/Emissioni	140	
EFFICIENZA ENERGETICA					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	7. Capitale ambientale	137	
GRI 302: Energia 2016	**302-1**	Energia consumata all'interno dell'organizzazione	7. Capitale ambientale/Consumi energetici	138	
GESTIONE DEI RIFIUTI					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	7. Capitale ambientale	137	
GRI 306: Rifiuti 2020	**306-3**	Rifiuti prodotti	7. Capitale ambientale/Utilizzo responsabile delle risorse naturali	141	
RISPETTO DEI DIRITTI UMANI E TUTELA DEI LAVORATORI					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	6. Capitale umano	123	
GRI 401: Occupazione 2016	**401-1**	Assunzioni e turnover	6. Capitale umano/Turnover	129	

GRI 401: Occupazione 2016	**401-2**	Benefit previsti per i dipendenti a tempo pieno, ma non per i dipendenti part-time o con contratto a tempo determinato	6. Capitale umano/Welfare aziendale	132	
GRI 406: Non discriminazione 2016	**406-1**	Episodi di discriminazione e misure correttive adottate	6. Capitale umano/Diversità	127	Nel 2024 non si sono verificati episodi di discriminazione
SODDISFAZIONE E GESTIONE DELLE RELAZIONI CON I CLIENTI					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	4. Capitale relazionale	81	
GRI 418: Privacy dei clienti 2016	**418-1**	Denunce comprovate riguardanti le violazioni della privacy dei clienti e perdita di dati dei clienti	4. Capitale relazionale/Privacy dei clienti e perdita di dati dei clienti	86	
FORMAZIONE E SVILUPPO DELLE CARRIERE					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	6. Capitale umano	123	
GRI 404: Formazione e istruzione 2016	**404-1**	Ore medie di formazione annua per dipendente	6. Capitale umano/Formazione e sviluppo competenze	131	
TRASPARENZA DELLE INFORMAZIONI SUI PRODOTTI					
GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	4. Capitale relazionale	81	
GRI 417: Marketing ed etichettatura 2016	**417-3**	Casi di non conformità riguardanti comunicazioni di marketing	4. Capitale relazionale/Attività di marketing	86	Nel corso del 2024 non si sono verificati casi di non conformità riguardanti comunicazioni di marketing.
PARNERSHIP CON ISTITUZIONI E IMPRESE					

GRI 3: Temi materiali 2021	**3-3**	Gestione dei temi materiali	3. Capitale infrastrutturale/Il valore delle partnership	76	
ALTRI INDICATORI RENDICONTATI					
PRESENZA SUL MERCATO					
GRI 202: Presenza sul mercato 2016	**202-2**	Proporzione di senior manager assunti dalla comunità locale	6. Capitale umano/I Dipendenti	127	
PRATICHE DI APPROVVIGIONAMENTO					
GRI 204: Pratiche di approvvigionamento 2016	**204-1**	Proporzione di spesa verso fornitori locali	4. Capitale relazionale/La gestione della supply chain	93	
ACQUA E SCARICHI IDRICI					
GRI 303: Acqua e scarichi idrici 2018	**303-3**	Prelievo idrico	7. Capitale ambientale/Utilizzo responsabile delle risorse naturali	141	
OCCUPAZIONE					
GRI 401: Occupazione 2016	**401-3**	Congedo parentale	6. Capitale umano/ I congedi parentali	130	
SALUTE E SICUREZZA SUL LAVORO					
GRI 403: Salute e sicurezza sul lavoro 2018	**403-2**	Identificazione dei pericoli, valutazione dei rischi e indagini sugli incidenti	6. Capitale umano/Salute e sicurezza sul lavoro	132	
	403-3	Servizi di medicina del lavoro	6. Capitale umano/Salute e sicurezza sul lavoro	132	

	403-9	Infortuni sul lavoro	6. Capitale umano/Salute e sicurezza sul lavoro	132	
DIVERSITÀ E PARI OPPORTUNITÀ					
GRI 405: Diversità e pari opportunità 2016	**405-1**	Diversità negli organi di governo e tra i dipendenti	2. Governance/La Governance 6. Capitale umano/Diversità	62 127	
COMUNITÀ LOCALI					
GRI 413: Comunità locali 2016	**413-1**	Attività che prevedono il coinvolgimento delle comunità locale, valutazioni d'impatto e programmi di sviluppo	4. Capitale relazionale/Le relazioni con il territorio	99	

HQ / REGGIO EMILIA
VIA BRIGATA REGGIO, 37
42124 REGGIO EMILIA - ITALIA
TEL. 0522.388111

SPACES ISOLA / MILANO
VIA POLA, 11
20124 MILANO - ITALIA

BUREAU / PIACENZA
VIA DAL VERME, 33
29121 PIACENZA - ITALIA

BUREAU / VARSAVIA
RONDO DASZYŃSKIEGO 2B
00-843 VARSAVIA – POLONIA

CYBEROO