ODCEC m@ster

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

DIGITALIZZAZIONE DEGLI STUDI

CYBERSECURITY

Francesco Carraro
Mattia Campagner

15 01 2025

Indice

- La Sicurezza non è più un'opzione
  - Overview, andamento degli attacchi e focus sull' Italia
- Le Minacce ai danni degli Studi
  - Overview degli attacchi
  - Phishing
- Come difendersi
  - Analizzare i propri rischi e costruire una strategia aderente di sicurezza
  - Regole auree di protezione della sicurezza
  - Monitoring e Threat Intelligence
- Compliance e normative

La Sicurezza
non è più un'opzione

Overview, andamento degli attacchi
e focus sull' Italia

Alcuni attacchi storici

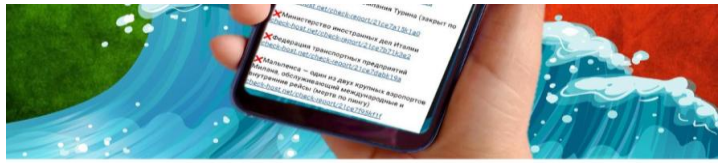
Yahoo (2014): 3 miliardi di account violati, 41 class-action subite

WannaCry (2017): ransomware ha infettato 230.000 computer in 150 paesi

Equifax (2017): furto dei dati personali di 147 milioni di persone

Solarwinds (2020): attacco alla "supply chain" in cui un software di monitoraggio è stato compromesso per distribuire il malware a migliaia di clienti

Quotidianità degli attacchi



Italia Sotto Attacco di NoName057(16). Gli Hacker: “l’Italia dovrebbe pensare alla propria Sicurezza cibernetica”

Redazione RHC : 11 Gennaio 2025 12:15

Santo Stefano con DDoS! Carabinieri, MISE, Marina colpiti dagli attacchi di NoName057(16)

Redazione RHC -27/12/2024

Il Lungo Down dei server del Vaticano, il misterioso crash e i sospetti DDoS

Redazione RHC -02/12/2024

Gli Hacker Criminali di BASHE rivendicano un Attacco Informatico allo Stadio San Siro

Francesco Demarcus -02/12/2024

Attacco Informatico ad InfoCert: Si tratta di un altro attacco in Supply Chain

Redazione RHC -29/12/2024

Source: sito RedHotCyber – Aggiornamento 13/01/2025

Alcune statistiche aggiornate…

Nel mondo, 9 attacchi importanti al giorno

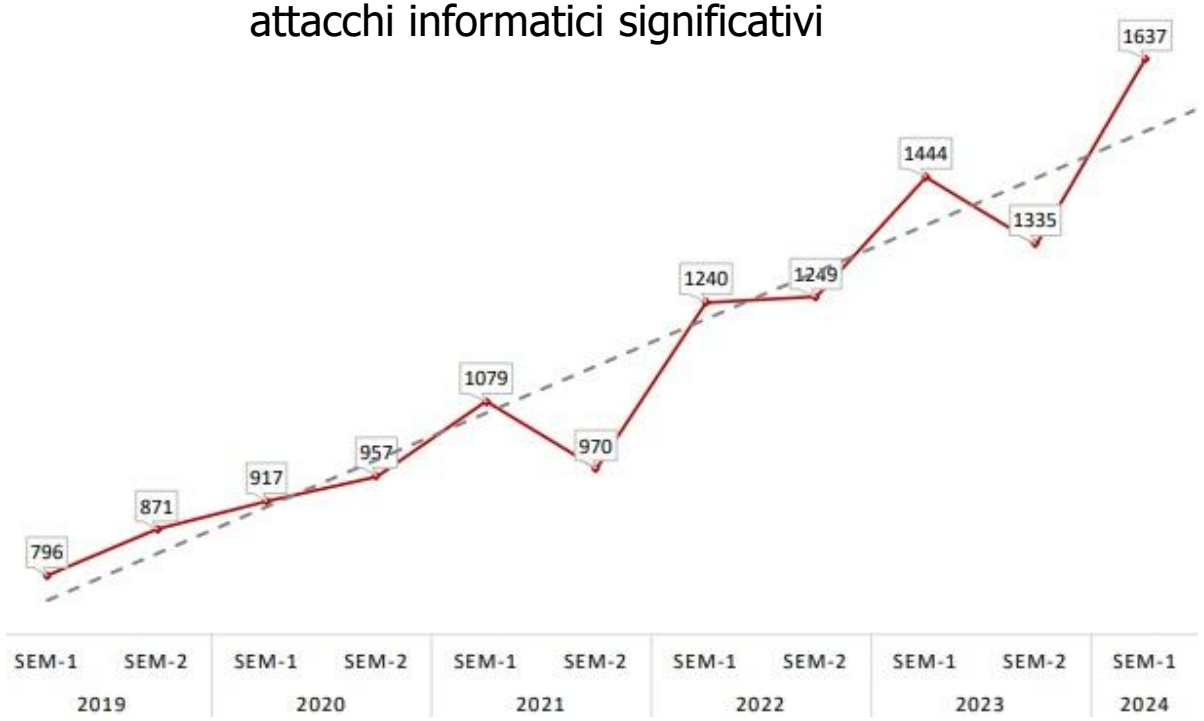
In Italia, 11% degli incidenti rilevati a livello globale nel 2023

In Italia, 71% degli incidenti è di matrice Cybercrime

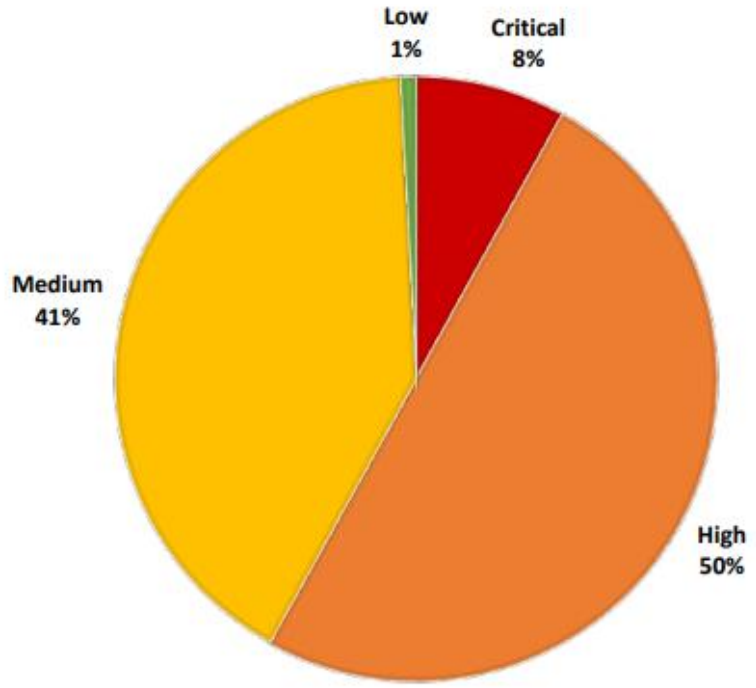
Source: Rapporto Clusit 2024 sulla Sicurezza ICT in Italia – Aggiornamento giugno 2024

Trend degli attacchi e impatti

Trend in crescita mondiale degli attacchi informatici significativi



In Italia, presenza di attacchi di alto/critico impatto

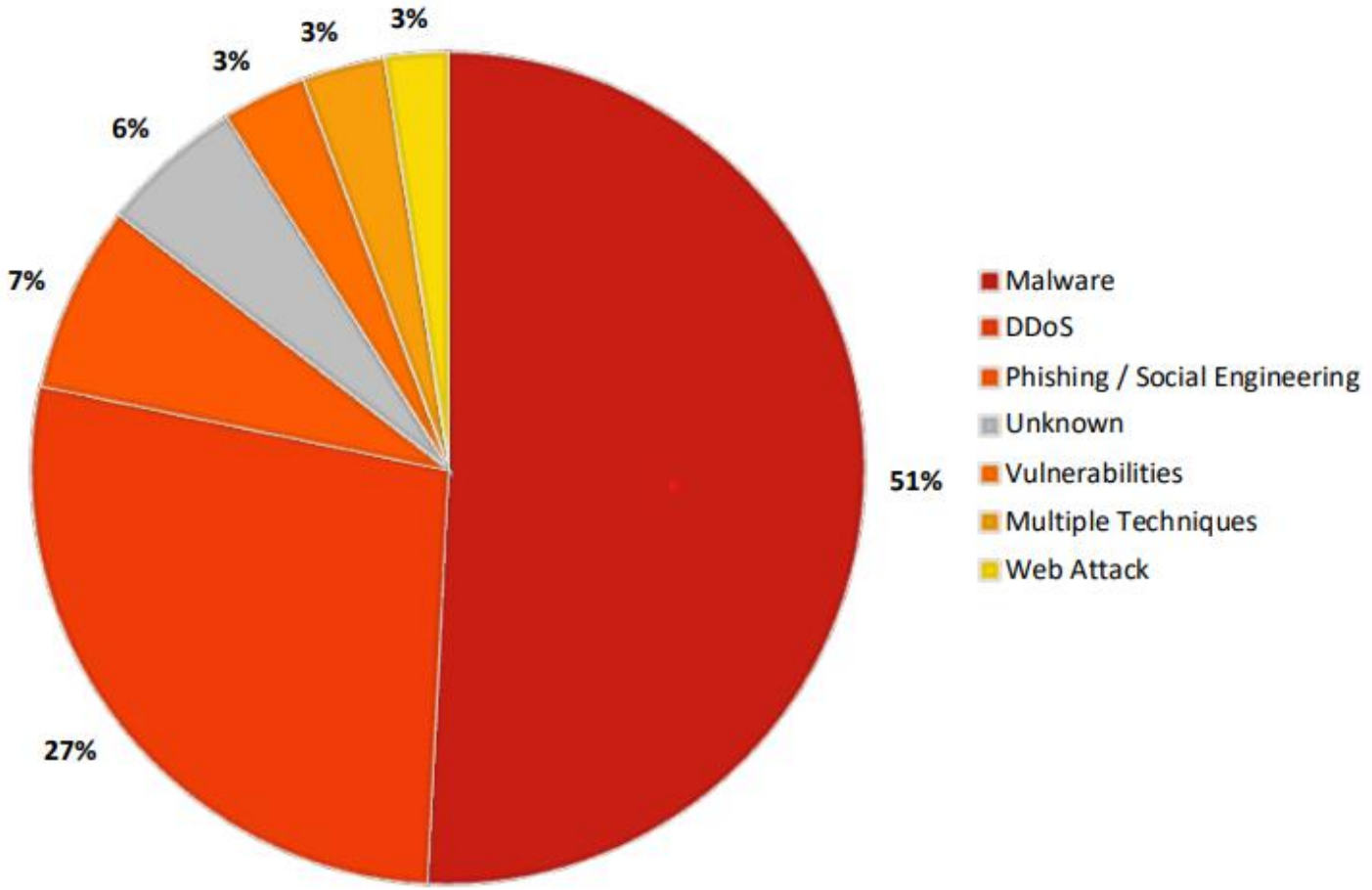


Source: Rapporto Clusit 2024 sulla Sicurezza ICT in Italia – Aggiornamento giugno 2024

Le Minacce ai danni degli Studi

Overview degli attacchi

Tecniche di attacco

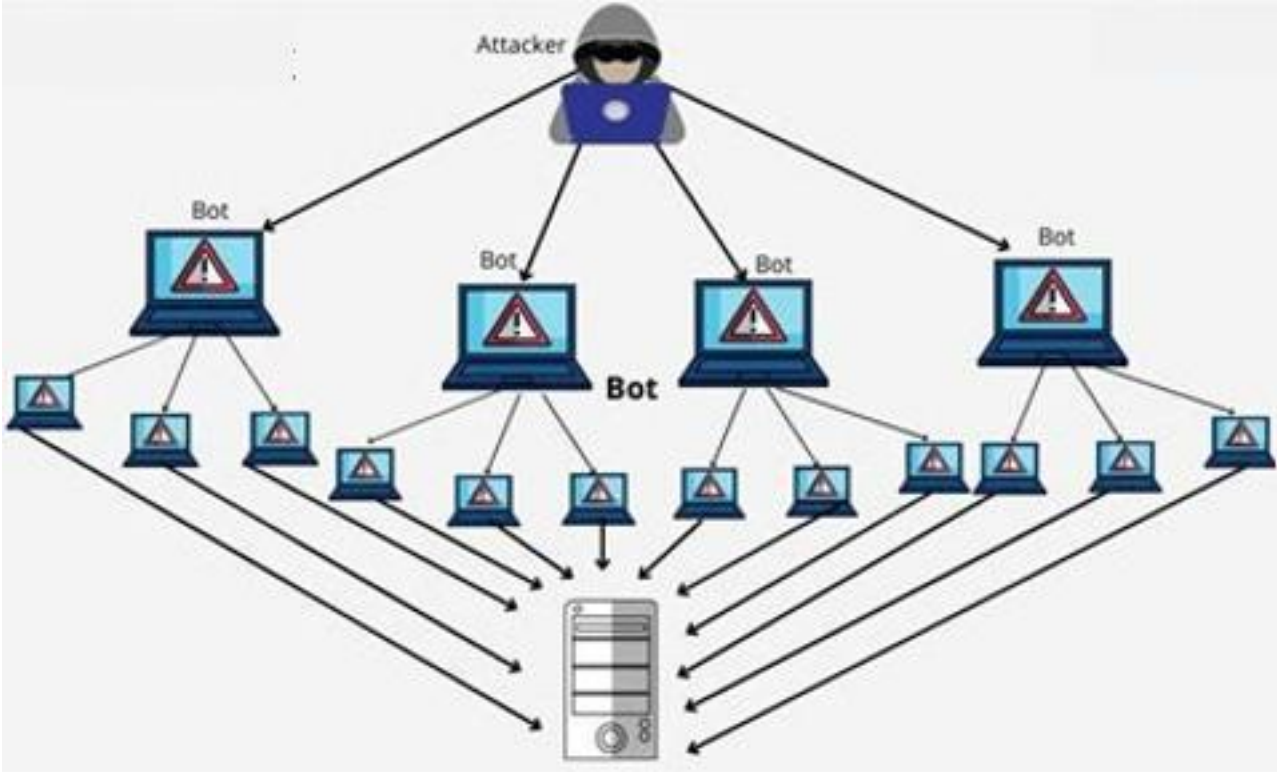


Source: Rapporto Clusit 2024 sulla Sicurezza ICT in Italia – Aggiornamento giugno 2024

MALWARE

Abbreviativo di malicious software, è disegnato per danneggiare o controllare in modo non autorizzato un sistema informatico: può compromettere i dati, danneggiare i dispositivi, interrompere le operazioni. Si diffonde tramite phishing, siti web compromessi o dispositivi USB infetti

DDOS



MAN IN THE MIDDLE

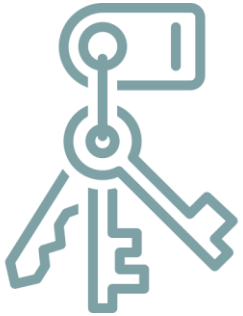
MINACCE ALLA PASSWORD

Brute Force

Keylogger

Password Dictionary

Password Spraying



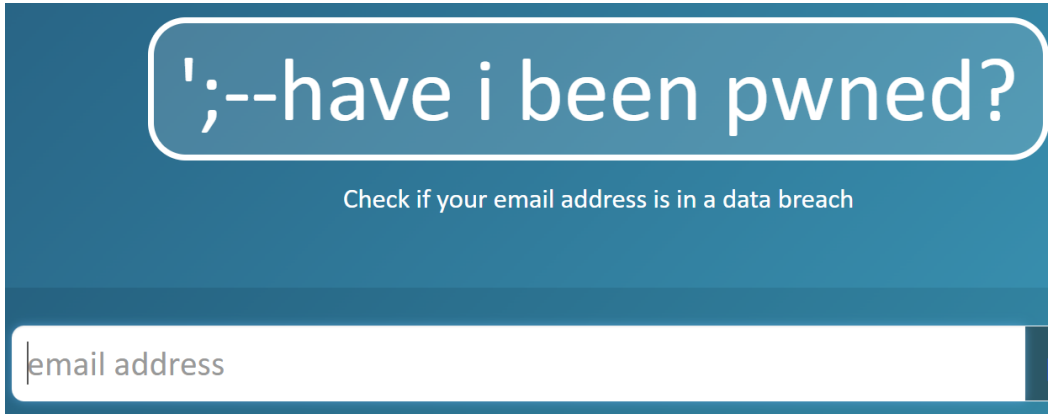
Credential Stuffing

ODCEC m@ster

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

PASSWORD CHECK



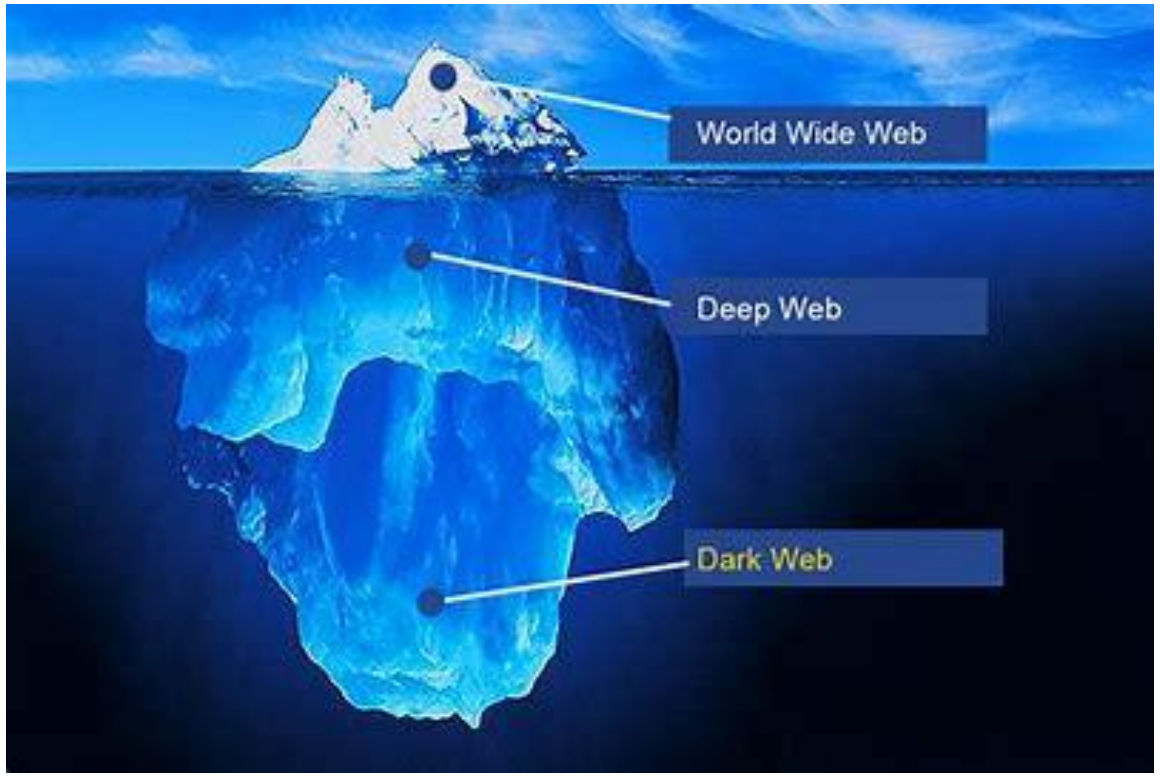
Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

Oh no — pwned!

Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)

LE INFORMAZIONI SUL WEB

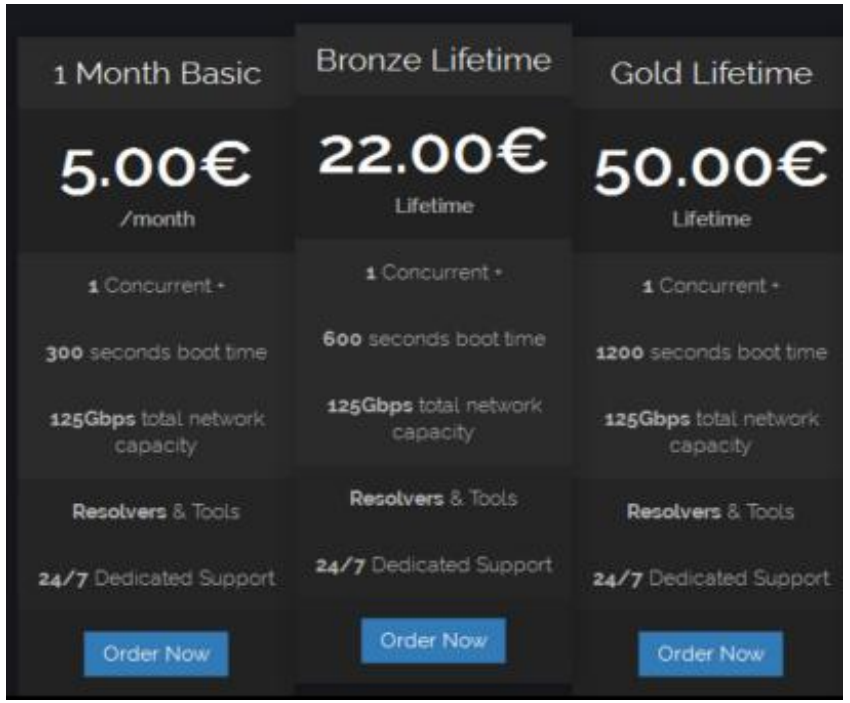


TIPOLOGIA DI ATTACCANTI

	MOTIVAZIONI	CONSEGUENZE	CARATTERISTICHE
 GOVERNI	Vantaggi economici, politici e militari	- Perdita di vantaggi competitivi - Distruzione di infrastrutture	- Budget elevato - Attacchi strutturati - Interessati a nascondere le reali motivazioni
 CRIMINALI	Guadagnare e collezionare informazioni per future frodi	- Perdite finanziarie - Perdita di fiducia dai clienti - Costi di gestione del danno	- Possono essere più criminali connessi in una rete - Interessati a coprire le loro tracce
 ATTIVISTI	Influenzare politica e spronare cambiamenti sociali	- Pressione politica - Diffusione di idee	- Budget ridotto per gli attacchi - Interessati alla paternità dell'attacco

HACKER AS A SERVICE

CREDIT CARD DATA WITH CVV NUMBERS	
U.S.	$5 - $12
U.K.	$15 - $20
Canada	$10 - $20
Australia	$5 - $25
EU	$14 - $30



esemplificativo

RISCHI

- Estorsione
- Frode
- Spionaggio industriale
- Furto dati
- Furto identità

esemplificativo

Le Minacce ai danni degli Studi

Phishing

Cosa è il phishing

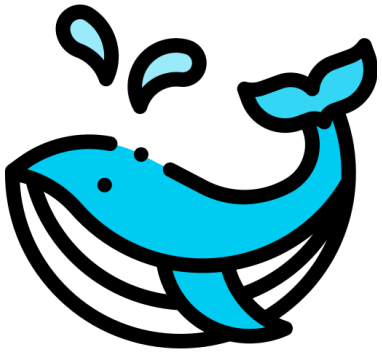
Tecnica fraudolenta per convincere la vittima a fornire propri dati personali o eseguire azioni (codici, password, carta di credito, ecc) con falsi pretesti

E' una modalità di social engineering, tesa alla manipolazione psicologica della vittima per indurla a fidarsi dell'aggressore con il fine di sottrarre informazioni o effettuare azioni specifiche

Differenziazione di phishing per destinatario

SPEAR Phishing

l'attaccante studia la vittima e personalizza il messaggio in modo più convincente, approfittando dei punti deboli della vittima



WHALE Phishing

il target è una persona con un ruolo apicale all'interno di un'azienda

BEC (Business Email Compromise)

l'attaccante compromette, ovvero recupera le credenziali di una casella di posta elettronica (es. di un fornitore) e invia le email, con propri contenuti, alla lista dei contatti presente nella rubrica

LATERAL Phishing

l'attaccante compromette o simula il mittente di una casella di posta elettronica, al fine di inviare richieste ai colleghi della vittima

Differenziazione di phishing per canale di comunicazione sfruttato

SMISHING (SMS phishing)

l'attaccante simula la comunicazione SMS di istituzioni autorevoli (es. banca, Ag.Entrate) per attivare la truffa

VISHING (Voice phishing)

truffa telefonica per indurre il malcapitato a cedere credenziali e dati importanti

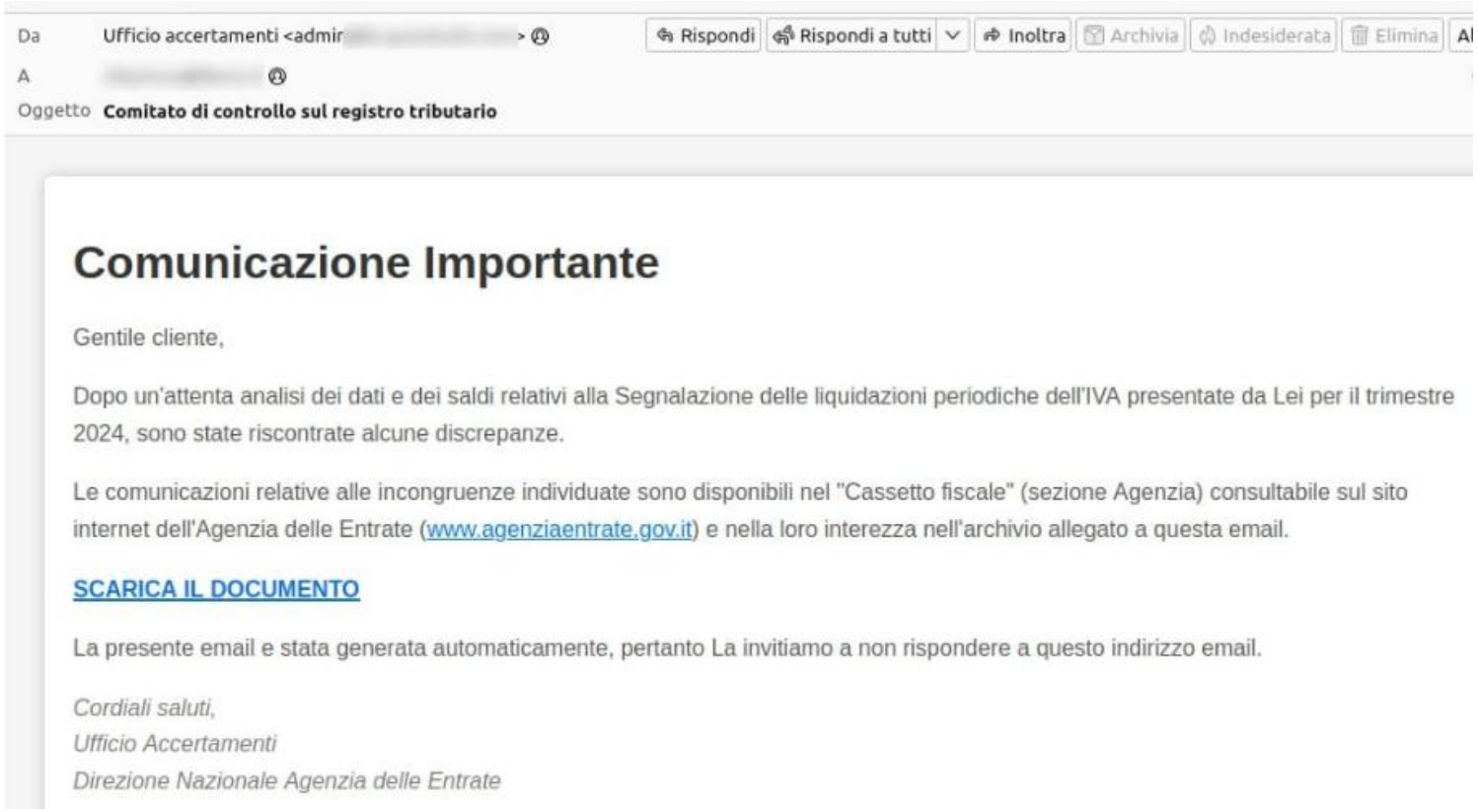
PHARMING

la vittima è invitata a entrare a sua insaputa su un sito malevolo graficamente molto simile all'originale e inserisce dati delicati (es. carta di credito)

QHISHING (QR phishing)

la vittima è incuriosita e inquadra il QR Code, scansionando un codice malevolo

Esempi di phishing



Da Ufficio accertamenti <admir[illegible]>

A [illegible]

Oggetto **Comitato di controllo sul registro tributario**

Rispondi | Rispondi a tutti | Inoltra | Archivia | Indesiderata | Elimina

Comunicazione Importante

Gentile cliente,

Dopo un'attenta analisi dei dati e dei saldi relativi alla Segnalazione delle liquidazioni periodiche dell'IVA presentate da Lei per il trimestre 2024, sono state riscontrate alcune discrepanze.

Le comunicazioni relative alle incongruenze individuate sono disponibili nel "Cassetto fiscale" (sezione Agenzia) consultabile sul sito internet dell'Agenzia delle Entrate (www.agenziaentrate.gov.it) e nella loro interezza nell'archivio allegato a questa email.

SCARICA IL DOCUMENTO

La presente email e stata generata automaticamente, pertanto La invitiamo a non rispondere a questo indirizzo email.

Cordiali saluti,
Ufficio Accertamenti
Direzione Nazionale Agenzia delle Entrate

Da: Dipartimento Investigazione Criminale <Ing.Buero.Wolff@t-online.de>
Inviato: giovedì 11 maggio 2023 03:50
A: polizia.dipartimento.criminale@gov.it
Oggetto: INVESTIGAZIONE CRIMINALE - FASCICOLO N°0896789/18P965-2023IT

è stato presentato un reclamo nei vostri confronti; attendiamo la vostra risposta dopo aver letto

Da: AgenziaEntrate Riscossione <noreply@www.agenziaentrate.gov.it>
Data: 31/01/23 00:28 (GMT+01:00)
A: [redacted]i.it>
Oggetto: Avviso Raccomandata #AR110J4060W

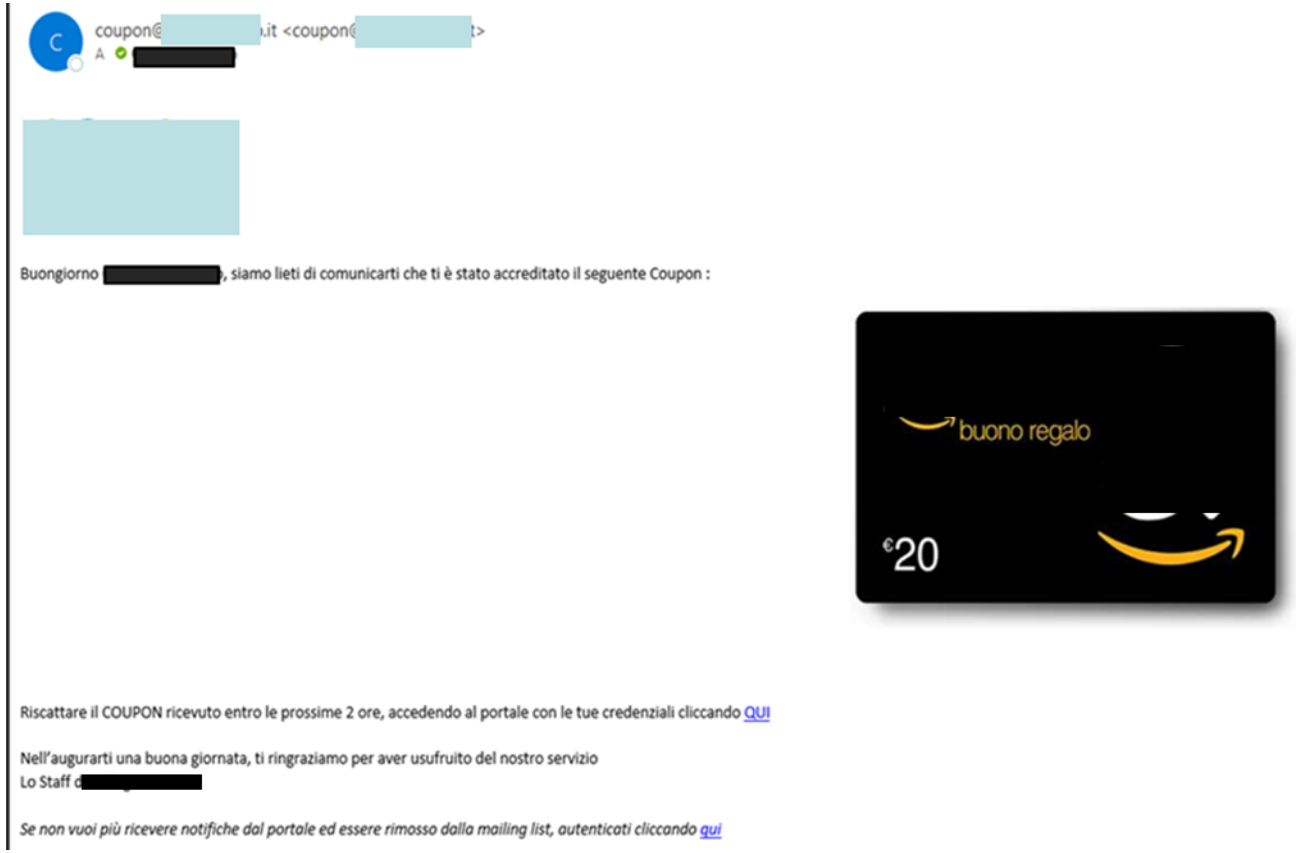
Gentile contribuente,
Agenzia delle Entrate-Riscossione La informa che è disponibile una nuova notifica per [redacted]i.it con le seguenti informazioni:

- Ente emittente: Agenzia delle Entrate
- Titolare: [redacted]i.it
- Soggetto: Notifica amministrativa
- Protocollo n.: AR110J4060W

Può accedere alla notifica su https://www.agenziaentrateriscossione.gov.it/it/, disponibile per 24 ore.

https://holdandfold.us/?c=itb8lzgfuawvsys5uyxzvbmvaz3j1chbvcgvsbgvncmluas5pda==zh3s
Fare clic o toccare per aprire il collegamento


Messaggio di testo • SMS
oggi 06:40
INPS: Per proseguire con l'erogazione di 280a, sul tuo conto controlla i dettagli: https://


coupon@ .it <coupon@ t>
A [redacted]
Buongiorno [redacted], siamo lieti di comunicarti che ti è stato accreditato il seguente Coupon :
buono regalo
€20
Riscattare il COUPON ricevuto entro le prossime 2 ore, accedendo al portale con le tue credenziali cliccando QUI
Nell'augurarti una buona giornata, ti ringraziamo per aver usufruito del nostro servizio
Lo Staff d[redacted]
Se non vuoi più ricevere notifiche dal portale ed essere rimosso dalla mailing list, autenticati cliccando qui

Come riconoscere il phishing

Mittente sospetto

Il mittente presenta un nome non coerente con l'indirizzo email, es. "da: Mario Rossi <info[illegible]@[illegible].it>".

Intestazione generica

Utilizzo di intestazioni come "Caro cliente" oppure utilizzo del nome email "Gentile mario.rossi".

Link ingannevoli

I link presentano incoerenza rispetto al dominio di destinazione (passare il mouse sopra al link senza cliccare per visualizzare la destinazione).

Contenuto sospetto

Contenuto non inerente alle attività svolte nell'ambito lavorativo o personale.

Errori grammaticali

L'oggetto e il testo dell'email presentano errori grammaticali.

Allegati sospetti

Invio di file compressi ".zip" contenenti file Office, PDF di piccole dimensioni. I file di Office potrebbero chiedere attivazioni di macro malevole.

Carattere di urgenza

La presenza di un carattere di urgenza spesso legata a temi di carattere amministrativo, legali, ecc. con scadenze ravvicinate.

Stile sospetto

Utilizzo di vocaboli non appropriati o non consoni al mittente.

Cos’è un Ransomware

Il ransomware è un tipo di **malware** che cifra i dati di un dispositivo o blocca l'accesso al sistema, richiedendo un riscatto (solitamente in criptovaluta) per ripristinare l'accesso.

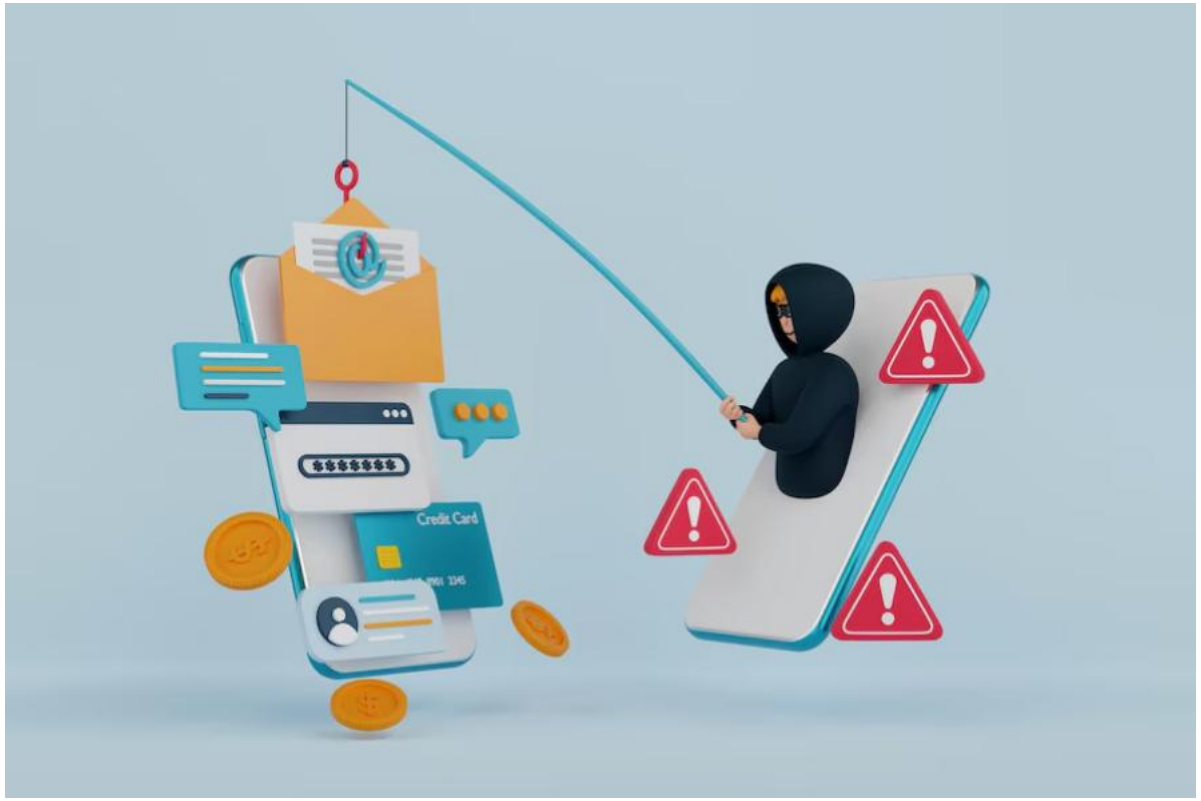
- **Cifratura dei dati**: I file vengono criptati, rendendoli inaccessibili all'utente.
- **Richiesta di riscatto**: Gli aggressori chiedono un pagamento per fornire la chiave di decrittazione.
- **Minacce aggiuntive**: In alcuni casi, i dati possono essere minacciati di divulgazione se il riscatto non viene pagato (es. doppia estorsione).

Modalità di diffusione

Email di phishing: Allegati o link dannosi

Siti web malevoli: Download automatico di malware

Vulnerabilità di sistema: Sfruttamento di falle di sicurezza non corrette

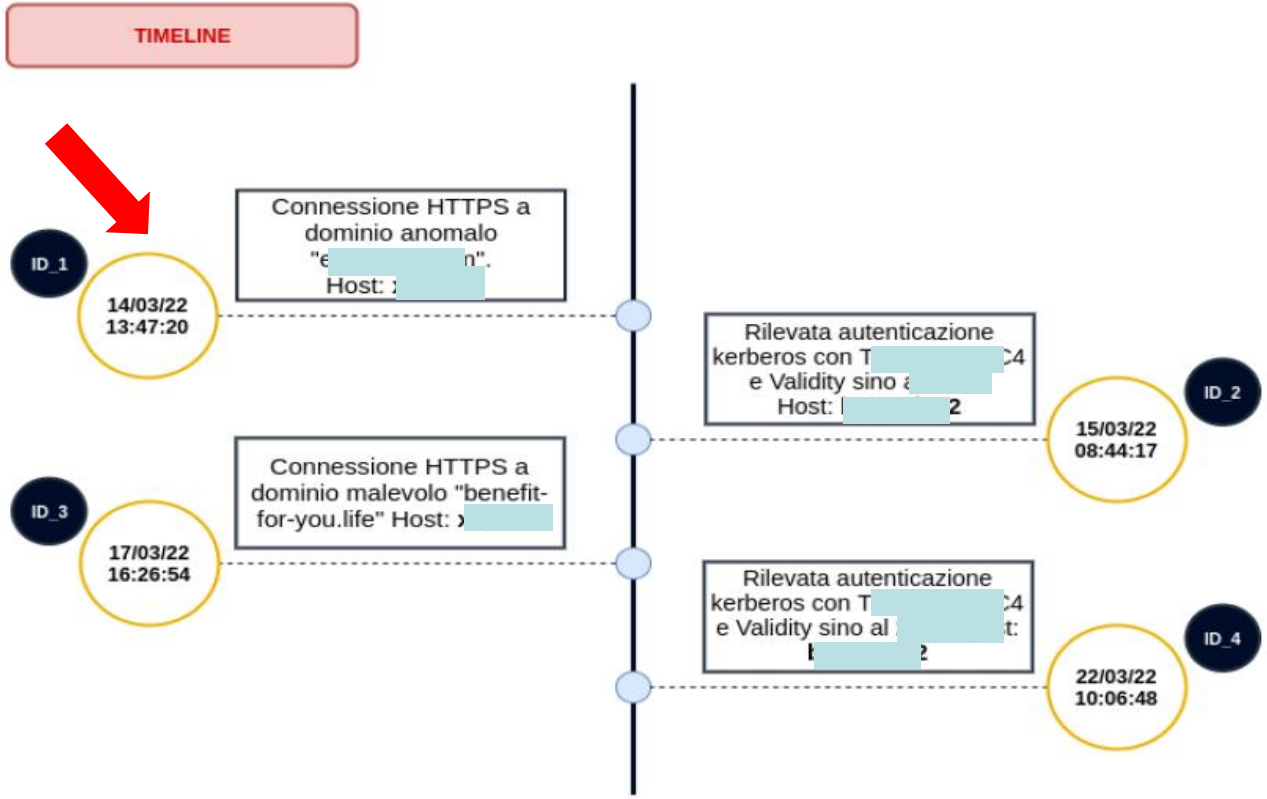


Casi concreti – Wizard Spider

Detecion attacco: 15/04/2022

Gruppo Criminale: Wizard Spider

Tipologia di attacco: Human Operated Ransomware Attack – attacco svolto principalmente da un team di soggetti che operano con un elevato numero di operazioni manuali per ottenere il controllo dell'infrastruttura ed ottenere gli obiettivi prefissati. In caso di mancato pagamento del riscatto, gli attaccanti procedono alla pubblicazione dei dati sensibili

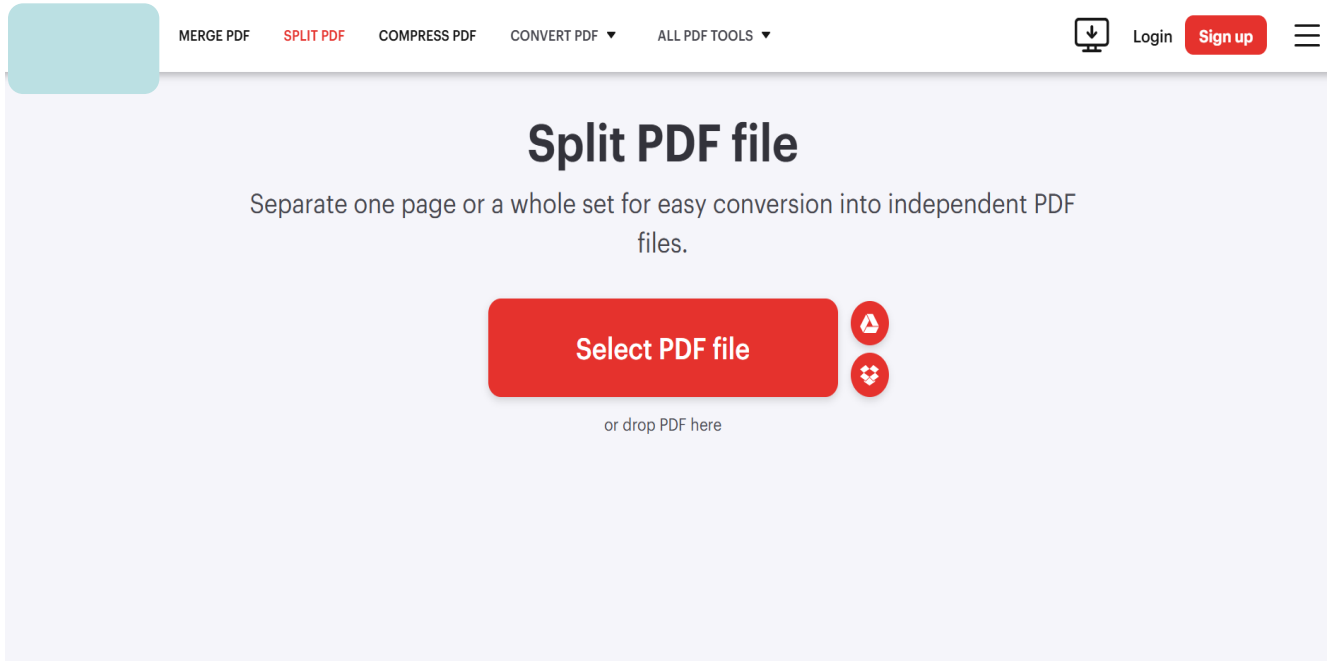


Cloud Security

IaaS infrastruttura IT virtualizzata attraverso Internet (server, storage…)

PaaS piattaforma per sviluppare, testare e distribuire applicazioni

SaaS applicazioni software fornite attraverso Internet.

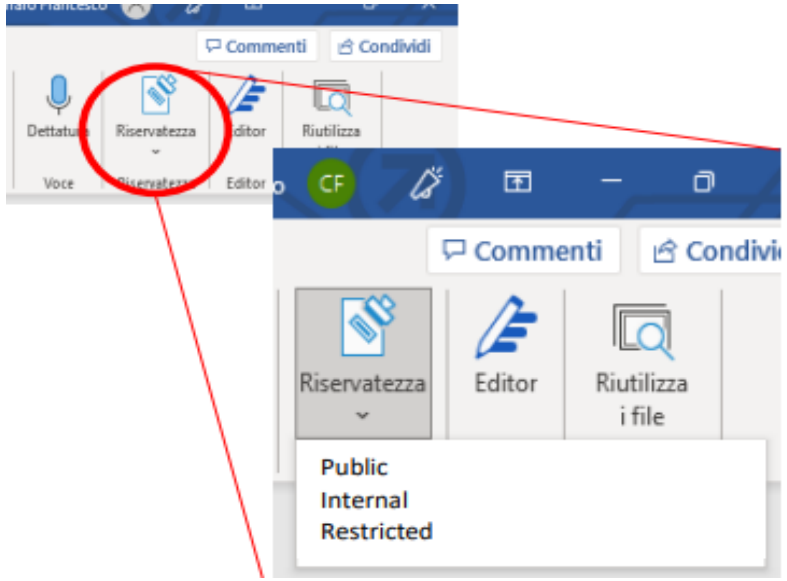


Classificazione delle informazioni

Associare ad ogni documento il proprio livello di confidenzialità:

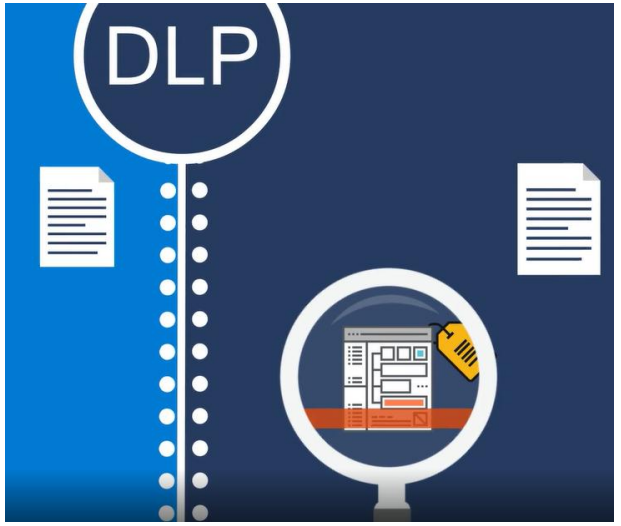
- Dati di dominio pubblico
- Dati ad uso interno
- Dati confidenziali

Controllo delle informazioni in uscita



Gli strumenti Office consentono di personalizzare i criteri di confidenzialità

Le soluzioni Data Loss Prevention consentono di controllare e limitare l'uscita di documenti elettronici

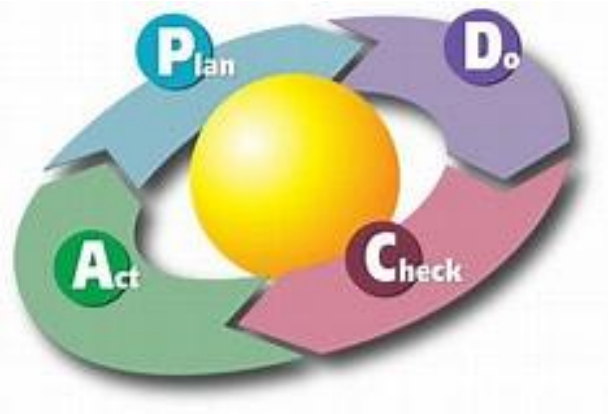


Come difendersi

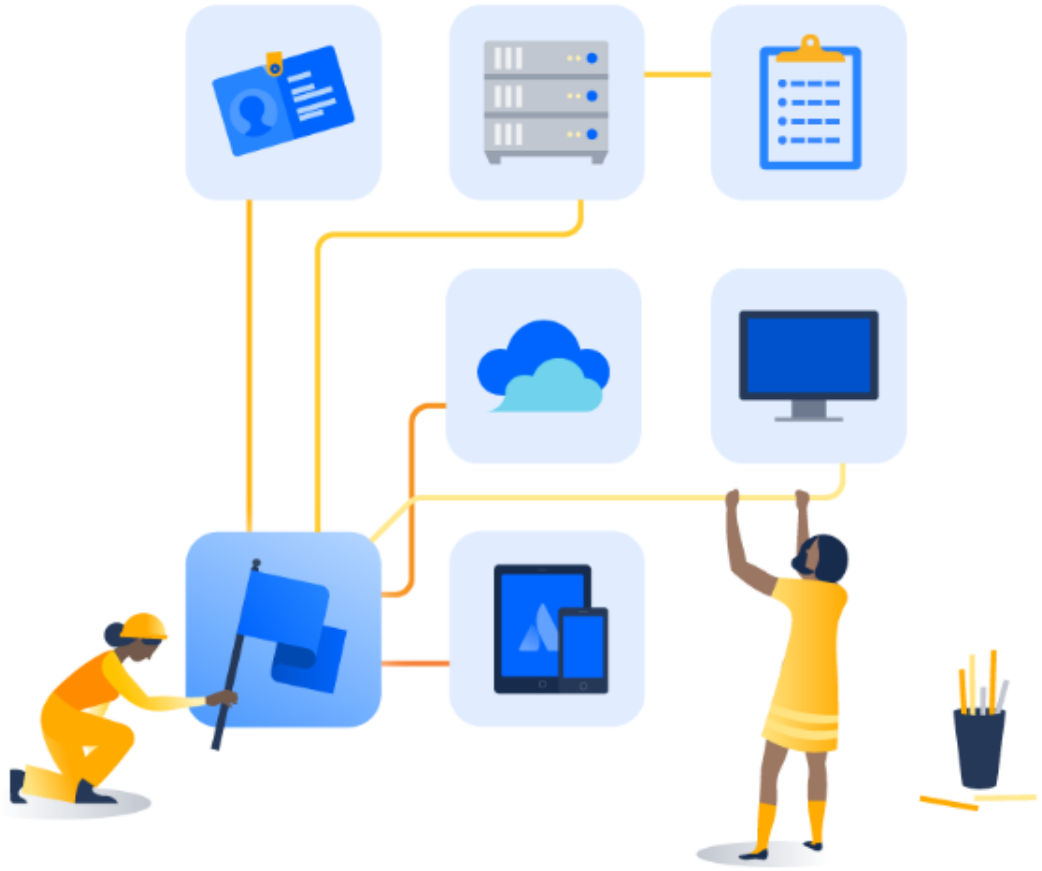
Analizzare i propri rischi e
costruire una strategia aderente di sicurezza

APPROCCIO STRUTTURATO ALLA SICUREZZA

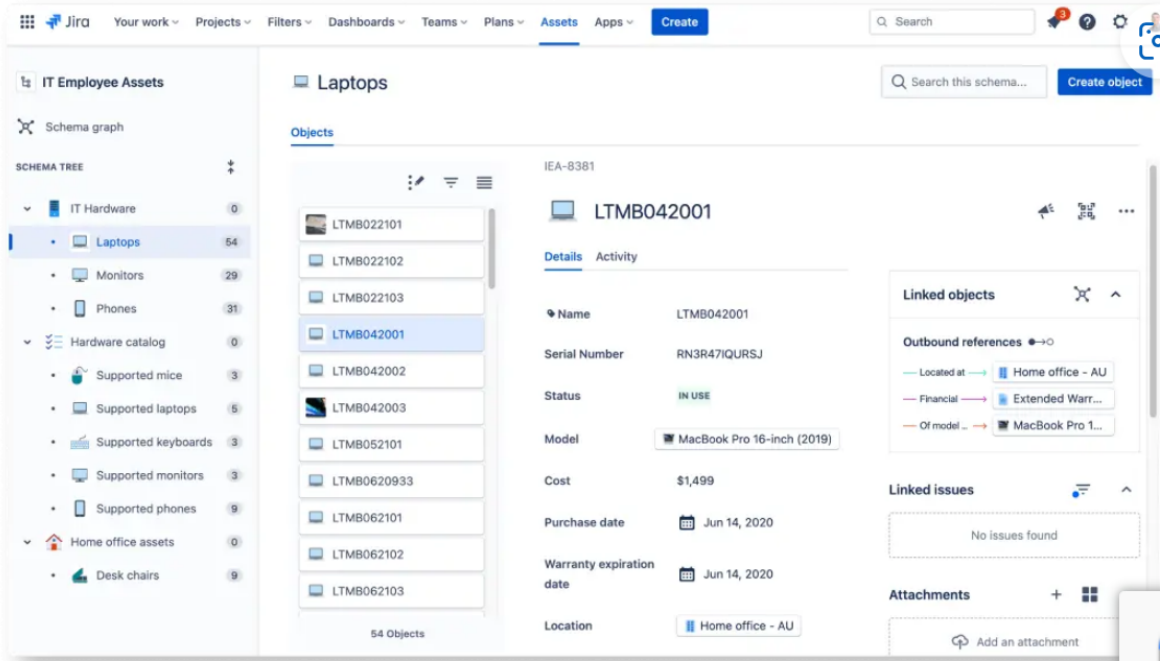
- Identificazione degli asset IT
- Analisi dei rischi di sicurezza
- Disegno della strategia di sicurezza
  - Governance
  - Controlli
  - Indicatori
- Monitoraggio della sicurezza
- Verifica rispetto al livello atteso
- Action Plan



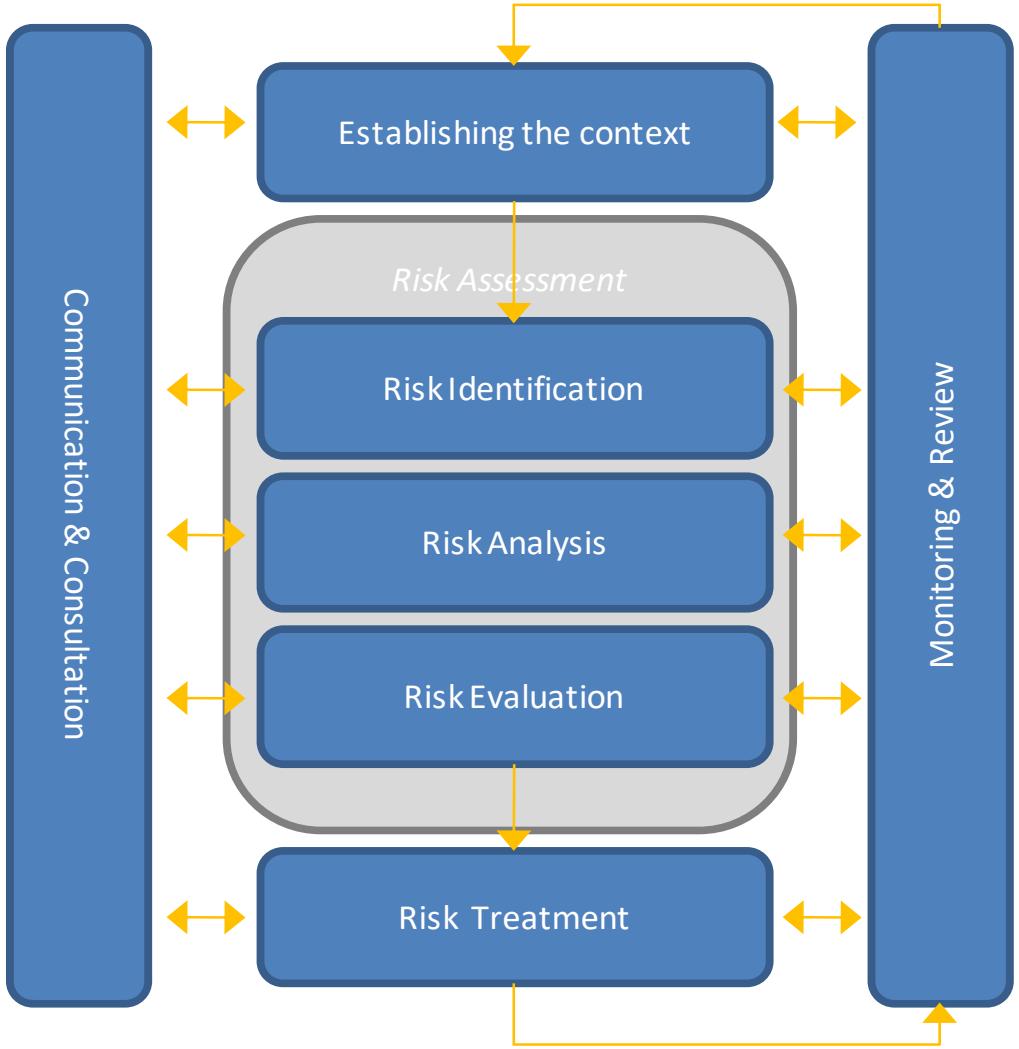
IDENTIFICAZIONE DEGLI ASSET



esemplificativo



PROCESSO DI GESTIONE DEL RISCHIO



PROCESSO DI GESTIONE DEL RISCHIO

Rischio Inerente: È il livello di rischio a cui un'organizzazione è esposta prima di implementare qualsiasi controllo o contromisura. Rappresenta il rischio "puro" associato a un'attività o processo senza tenere conto delle azioni di mitigazione.

$$Ri=P*I$$

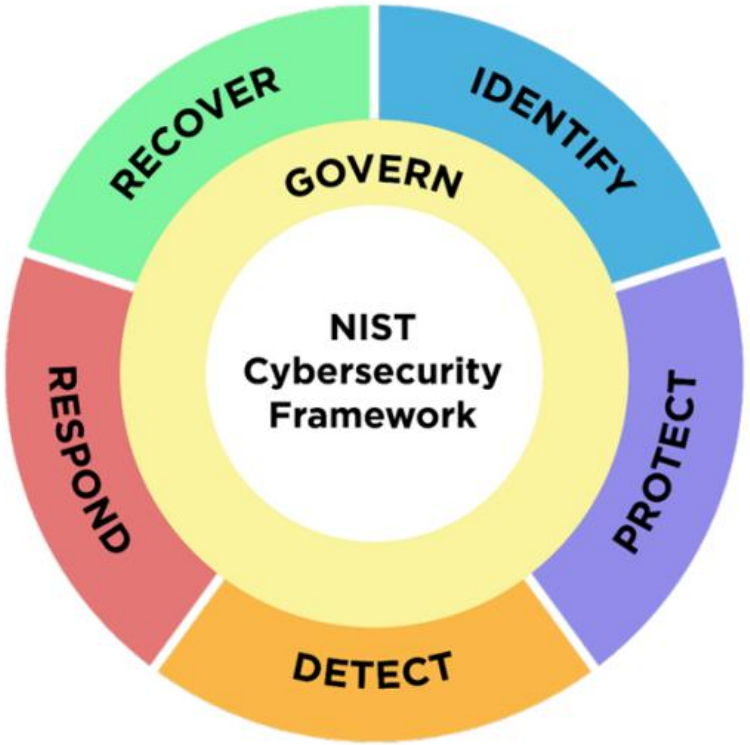
Rischio Residuo: È il livello di rischio che rimane dopo che sono stati implementati i controlli e le contromisure. È il rischio che l'organizzazione continua a dover gestire nonostante le misure di mitigazione adottate.

$$Rr=Ri-C$$

P= Probabilità
I=Impatto
C= Controlli di mitiigazione

NIST
National Institute of Standards and Technology

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



International Organization for Standardization
ISO
27001:2022

ISO/IEC 27002:2022 contiene **93 controlli** suddivisi in 4 domini:

- Organizzativo – 37 controlli
- Persone – 8 controlli
- Fisici – 14 controlli
- Tecnologici – 34 controlli

Come difendersi

Regole auree di
protezione della sicurezza

email e messaggi

- diffida di messaggi da mittenti sconosciuti e verifica l'indirizzo reale del mittente
- verifica bene i messaggi che ti chiedono di reagire con urgenza e rifletti prima di agire
- controlla i link contenuti nei messaggi prima di cliccare
- imposta la funzione antispam per filtrare comunicazioni indesiderate
- verifica e cancella periodicamente le cartelle di posta elettronica di scarto (eliminate, indesiderate)

PC

- non collegare dispositivi esterni (es. chiavette usb) se non sei certo della loro provenienza
- non usare WiFi pubblici (stazioni, parchi) per accedere alla posta o ad altre applicazioni delicate
- tieni il PC in ambiente sicuro (evita di lasciarlo nell'auto) e chiudi la sessione quando ti assenti
- fai regolarmente il backup su un dispositivo esterno e conservalo in luogo sicuro
- installa e aggiorna frequentemente l'antivirus

smartphone

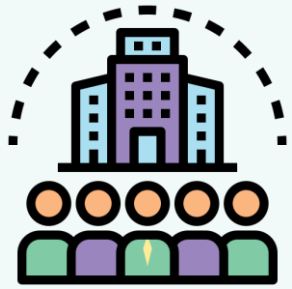
- installa le app solo da Store ufficiali (Play-store, Apple-store)
- tieni aggiornate le app e il sistema operativo
- rimuovi le app non più utilizzate
- elimina dati e applicazioni obsolete e inutili

password

- usa password sicure (lunghe, con caratteri alfanumerici e speciali) e cambiale spesso
- non usare parole identificabili (riferimenti personali, date di nascita, etc)
- non usare le stesse password per servizi e siti diversi
- non condividerle con nessuno e salvale con strumenti sicuri (password manager)
- abilita l'autenticazione forte o MFA per tutti i servizi che lo consentono

browser

- usa un browser conosciuto e aggiornato (Chrome, Edge, Firefox)
- digita correttamente il nome del sito che vuoi visitare, fai attenzione ai banner e ai link
- cancella frequentemente i cookies del browser, su PC e su smartphone
- non salvare password nel browser



Utilizzo di account aziendale

Utilizzare un account aziendale per lo svolgimento delle attività professionali per garantire una comunicazione chiara e professionale, salvaguardare la sicurezza dei dati e promuovere un'immagine coesa e affidabile della propria azienda

Comunicazione di dati sensibili

Per garantire la massima sicurezza e proteggere le informazioni sensibili come l'IBAN o altri dati critici, evitare l'utilizzo della posta elettronica e preferire canali di comunicazione più sicuri ed affidabili (SMS, Chat Teams, …)

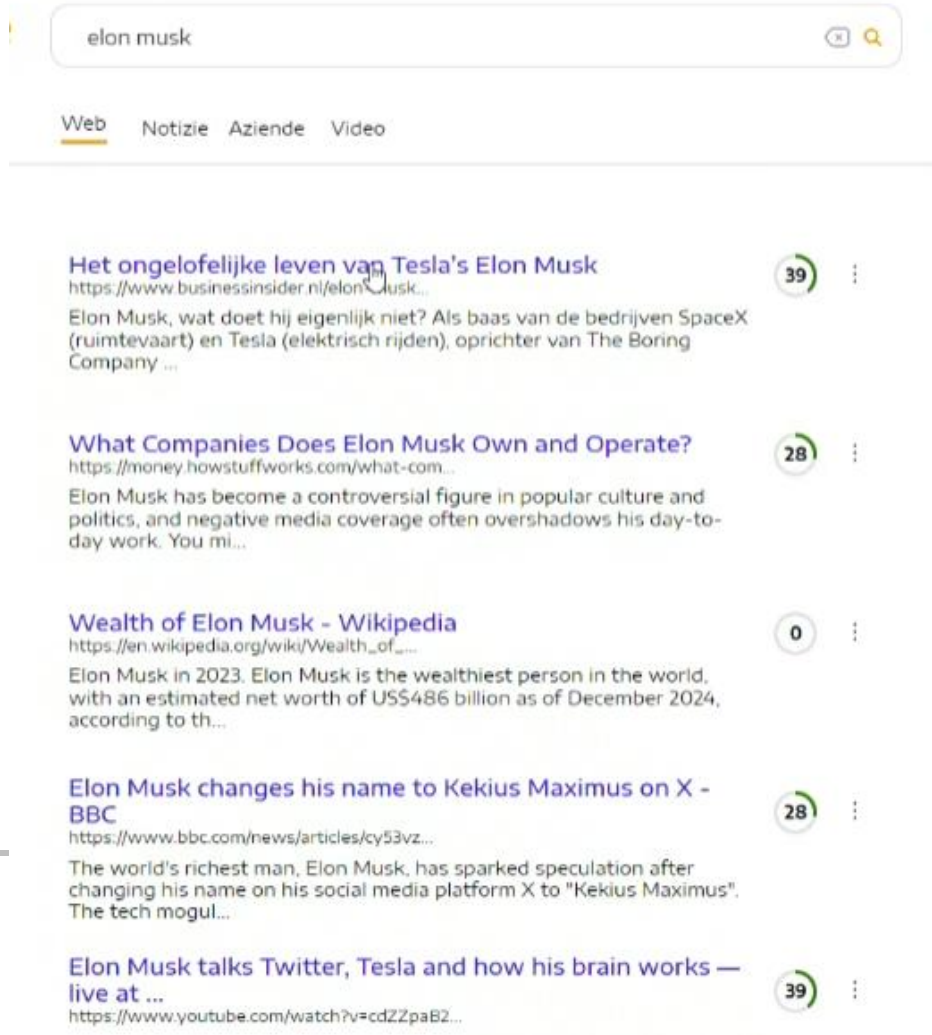
VPN

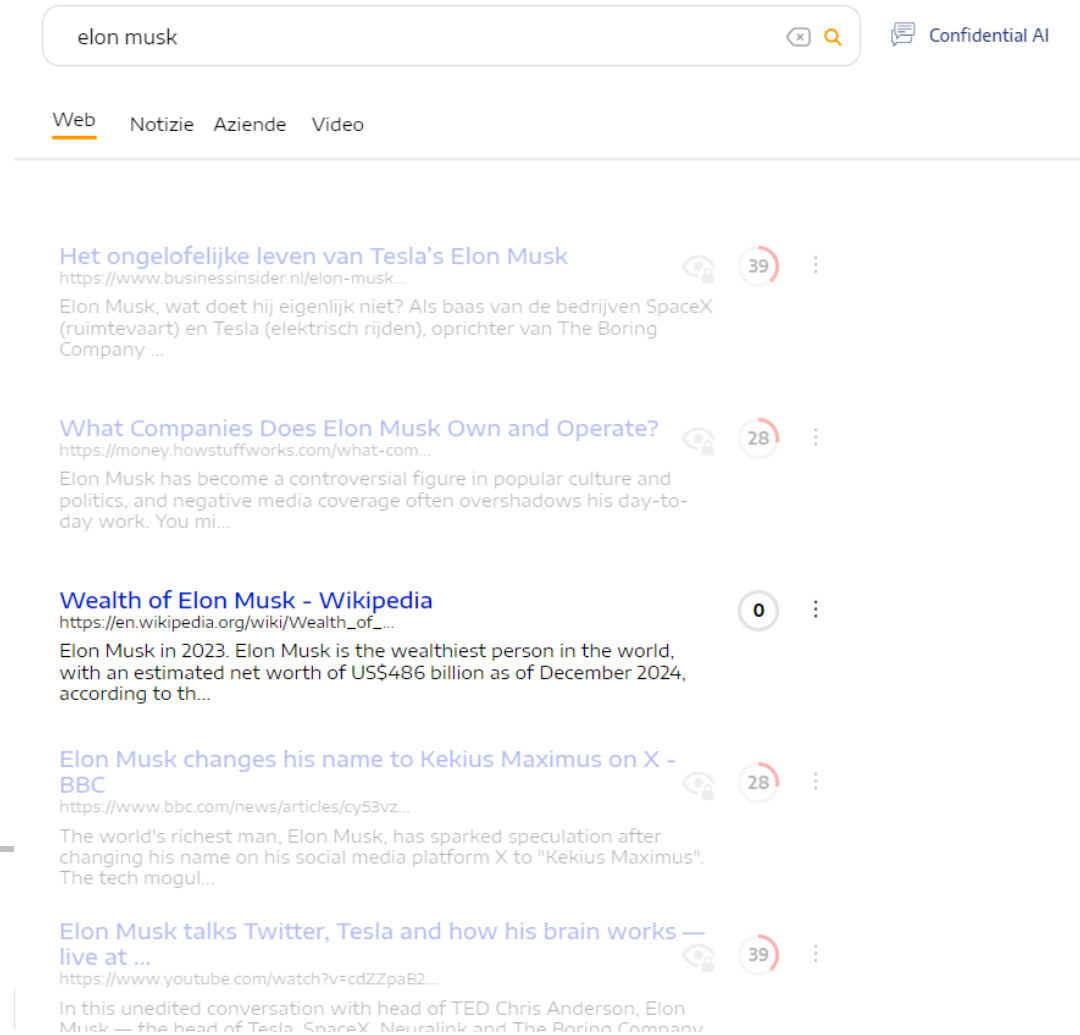
garantisce una connessione sicura, specialmente quando si accede a reti pubbliche o non fidate. La VPN cripta il traffico internet, proteggendo i dati sensibili da potenziali attacchi informatici. Questo strumento è fondamentale non solo per salvaguardare le informazioni aziendali, ma anche per mantenere la privacy online.

Crittografia

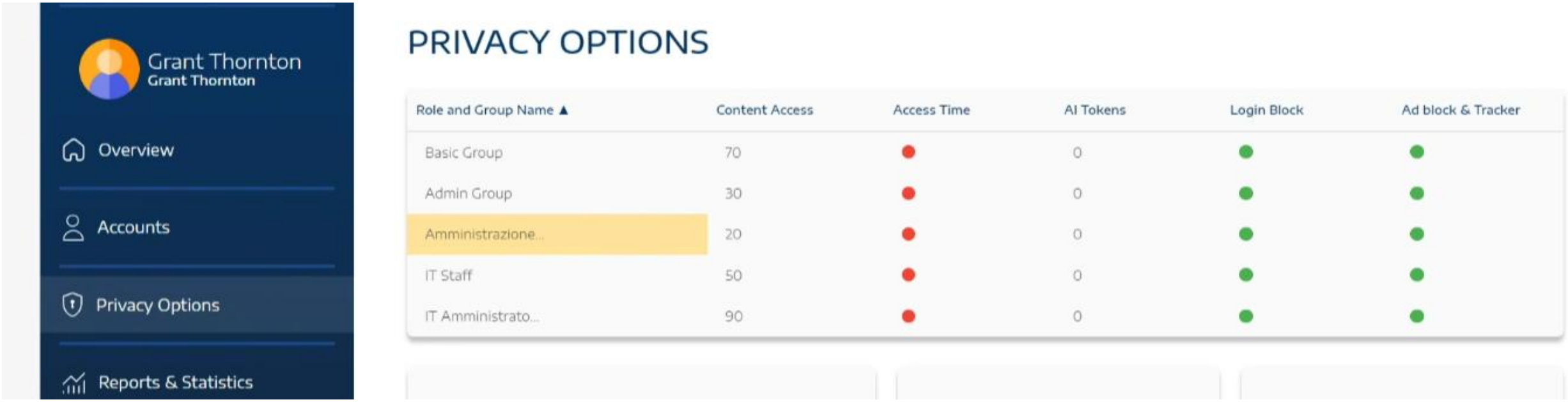
La crittografia rappresenta un pilastro fondamentale nella protezione delle informazioni digitali. Attraverso l'utilizzo di avanzati algoritmi, essa consente di salvaguardare la riservatezza e l'integrità dei dati, garantendo che solo le persone autorizzate possano accedere a informazioni sensibili

Strumenti per la navigazione sicura

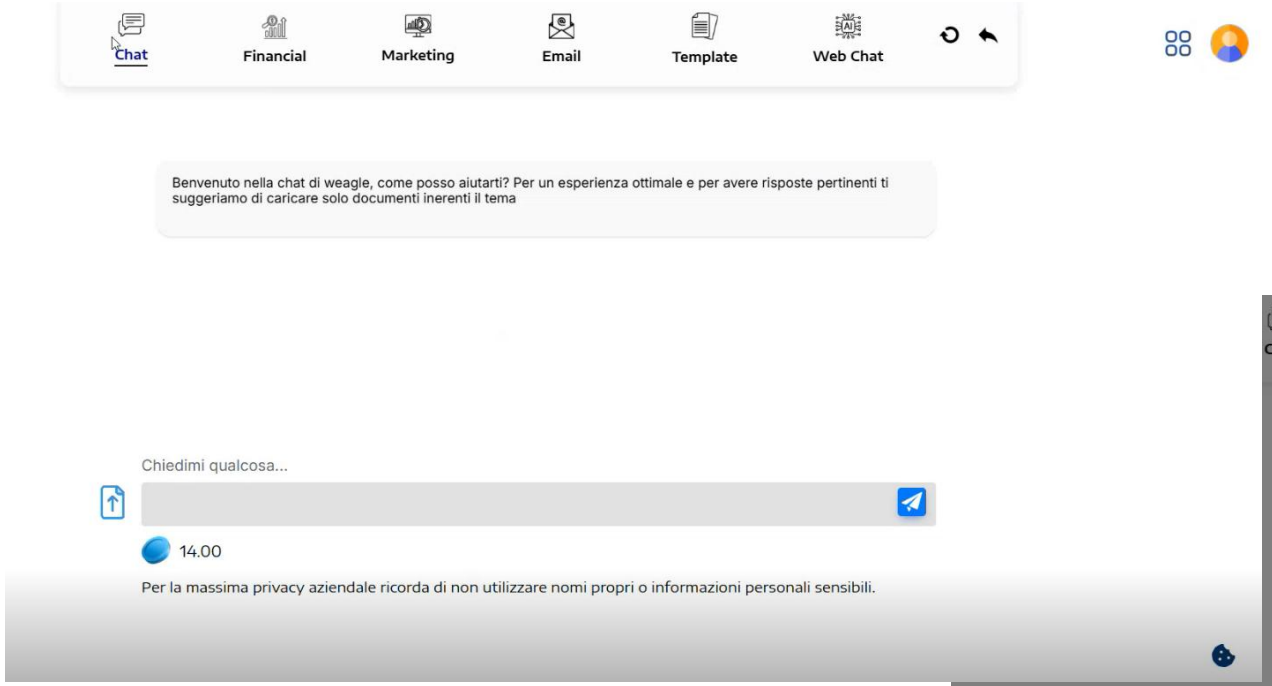


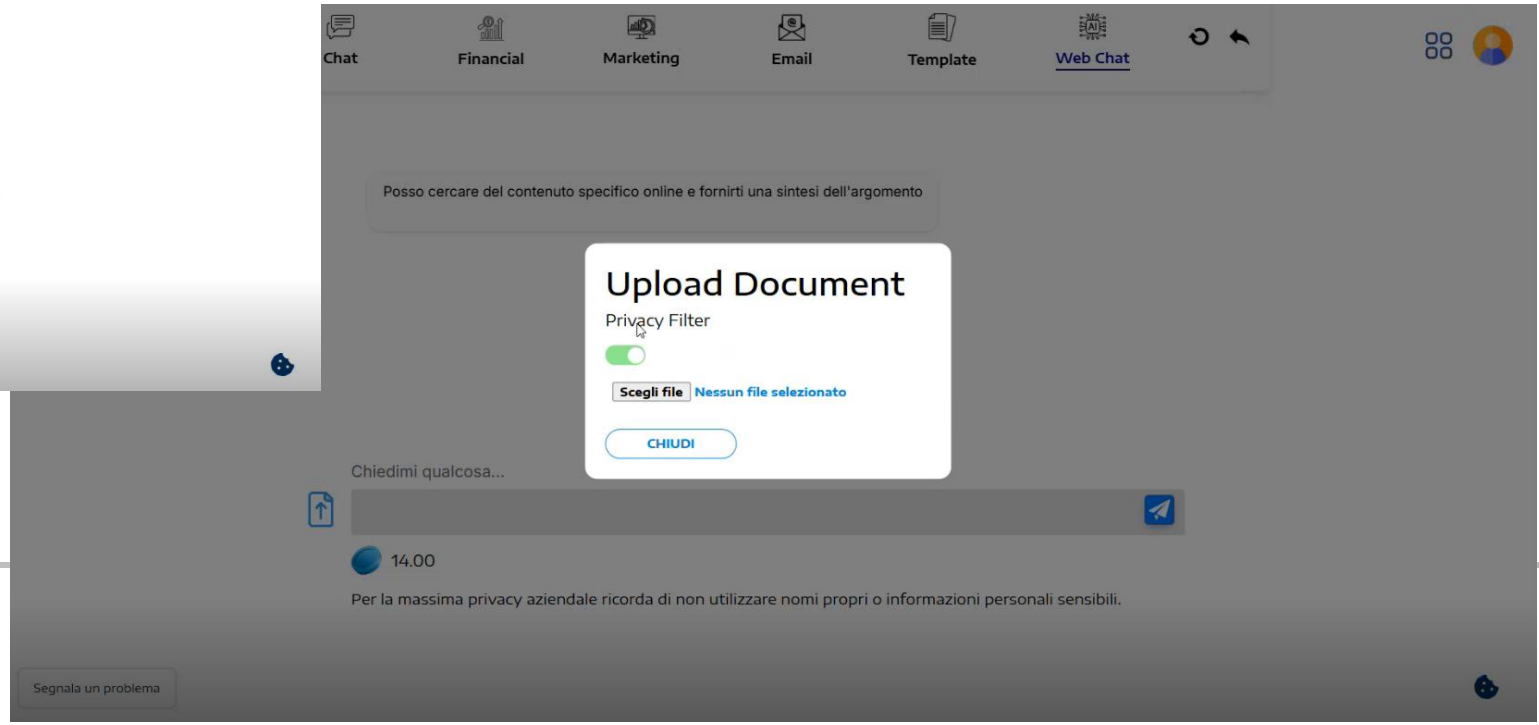


Assegnazione Profili in base ai ruoli



AI Chatbot

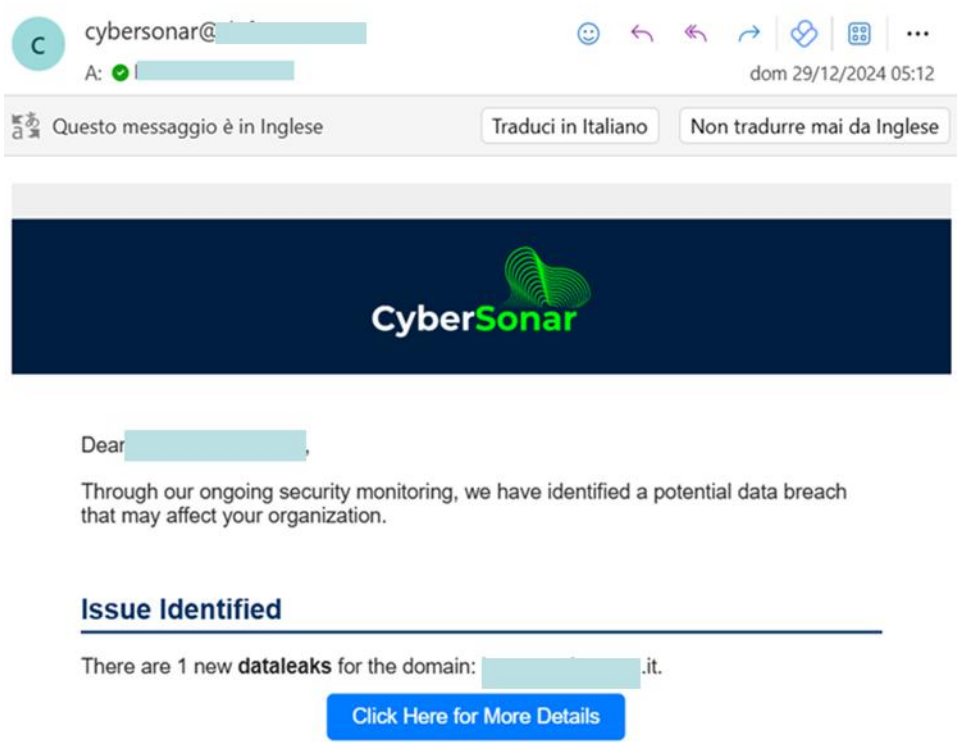

Chat
Financial
Marketing
Email
Template
Web Chat
Benvenuto nella chat di weagle, come posso aiutarti? Per un esperienza ottimale e per avere risposte pertinenti ti suggeriamo di caricare solo documenti inerenti il tema
Chiedimi qualcosa...
14.00
Per la massima privacy aziendale ricorda di non utilizzare nomi propri o informazioni personali sensibili.

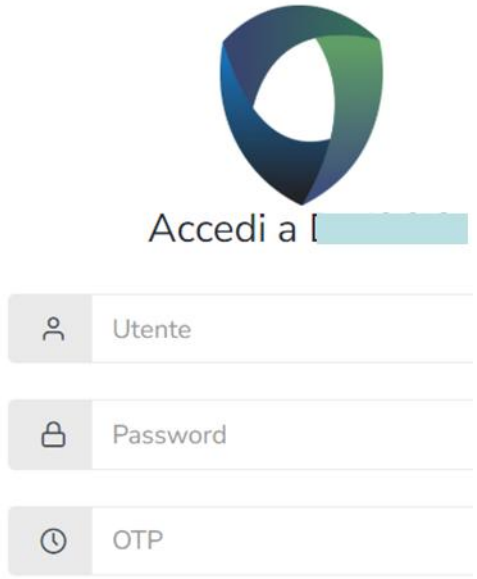

Chat
Financial
Marketing
Email
Template
Web Chat
Posso cercare del contenuto specifico online e fornirti una sintesi dell'argomento
Upload Document
Privacy Filter
Scegli file
Nessun file selezionato
CHIUDI
Chiedimi qualcosa...
14.00
Per la massima privacy aziendale ricorda di non utilizzare nomi propri o informazioni personali sensibili.
Segnala un problema

Come difendersi

Monitoring e
Threat Intelligence

DEMO


cybersonar@
A:
dom 29/12/2024 05:12
Questo messaggio è in Inglese
Traduci in Italiano
Non tradurre mai da Inglese
CyberSonar
Dear
Through our ongoing security monitoring, we have identified a potential data breach that may affect your organization.
Issue Identified
There are 1 new dataleaks for the domain: .it.
Click Here for More Details


Accedi a
Utente
Password
OTP

CISOaaS

L’obiettivo del CISO as a Service è quello di proteggere le informazioni aziendali e garantire la sicurezza informatica dell’azienda. Quali sono le attività principali del team?

Gestione dei rischi di sicurezza

Sviluppo e implementazione politiche di sicurezza

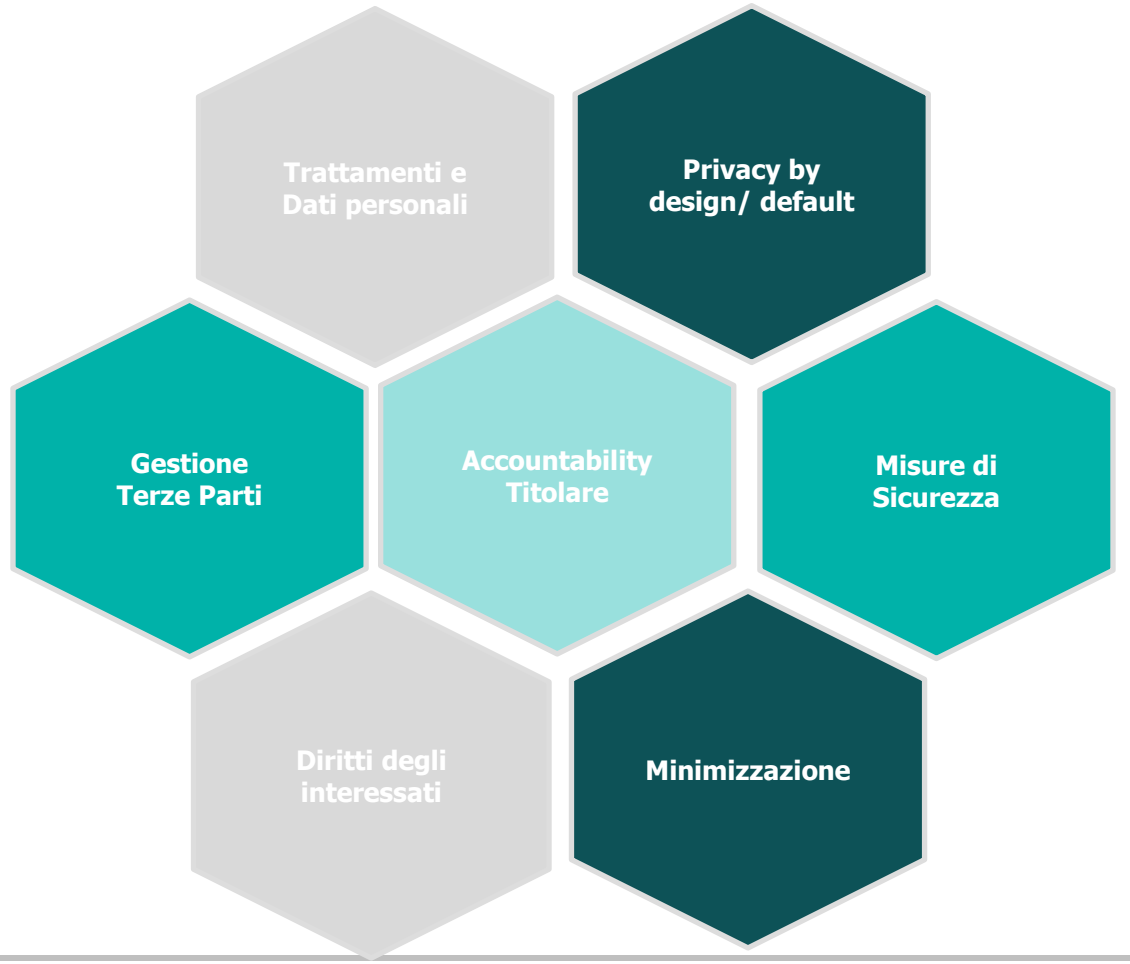
Compliance e normative

Formazione e Awareness

Monitoraggio e risposta degli incidenti di sicurezza

Compliance e normative

GDPR


Trattamenti e Dati personali
Privacy by design/ default
Gestione Terze Parti
Accountability Titolare
Misure di Sicurezza
Diritti degli interessati
Minimizzazione

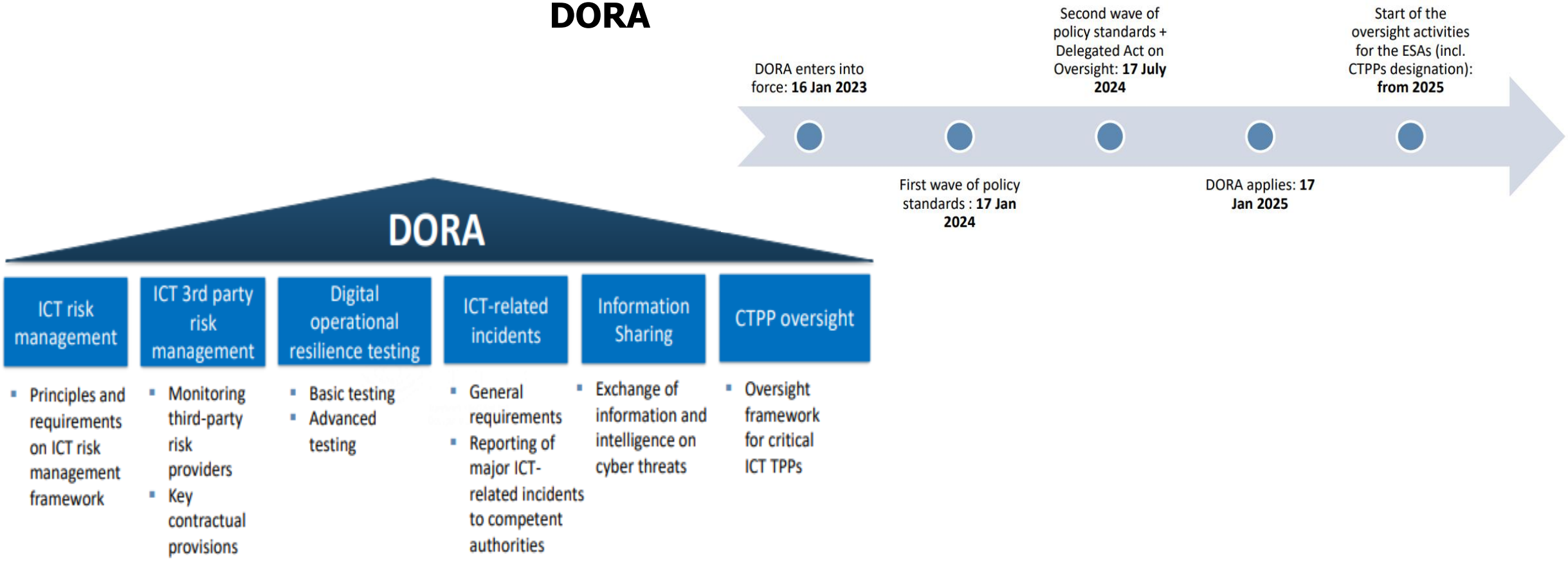
PERIMETRO DI SICUREZZA NAZIONALE

Nel 2019 è stato definito il Perimetro di sicurezza cibernetica nazionale, al fine di delineare un livello adeguato di sicurezza delle reti, dei sistemi e dei servizi informatici **degli operatori pubblici e privati**, da cui dipendono servizi essenziali per lo Stato

ACN è stata istituita con gli obiettivi di:

- **tutelare gli interessi nazionali** nel campo della cybersicurezza
- **prevenire e mitigare** gli attacchi cyber
- favorire il raggiungimento dell'autonomia tecnologica
- attuare la *Strategia Nazionale di Cybersicurezza*, entro il 2026

DORA


DORA enters into force: 16 Jan 2023
First wave of policy standards : 17 Jan 2024
Second wave of policy standards + Delegated Act on Oversight: 17 July 2024
DORA applies: 17 Jan 2025
Start of the oversight activities for the ESAs (incl. CTPPs designation): from 2025
DORA
ICT risk management
Principles and requirements on ICT risk management framework
ICT 3rd party risk management
Monitoring third-party risk providers
Key contractual provisions
Digital operational resilience testing
Basic testing
Advanced testing
ICT-related incidents
General requirements
Reporting of major ICT-related incidents to competent authorities
Information Sharing
Exchange of information and intelligence on cyber threats
CTPP oversight
Oversight framework for critical ICT TPPs

NIS2

DIRETTIVA NIS 2
Energia
Acqua potabile, acque reflue
Infrastrutture digitali
Settore sanitario
Settore bancario, infrastrutture dei mercati finanziari
Trasporto, spazio (parziale), servizi postali e di corriere
Produzione, trasformazione e distribuzione di alimenti
Gestione dei rifiuti
Gestione dei servizi TIC (business-to-business)
Pubblica amministrazione
Fabbricazione, produzione e distribuzione di sostanze chimiche
Industria manifatturiera
Fornitori di servizi digitali
Ricerca

- Resilienza e **capacità collettiva di rispondere a incidenti** su vasta scala
- **Cooperazione** tra autorità nazionali
- **Estensione** del perimetro dei **soggetti** coinvolti

28/02/2025 — **Registrazione sulla piattaforma ACN:** Entro il 28 febbraio 2025 per tutti gli altri soggetti che rientrano nell'ambito di applicazione del decreto

15/04/2025 — **Notifica ACN ai soggetti NIS2:** Costituzione dell'elenco dei soggetti NIS2 e notifica agli stessi della loro inclusione

31/01/2026 — **Obblighi notifica incidente:** Entro gennaio 2026, adempimento agli obblighi di base in materia di notifica di incidente

31/10/2026 — **Implementazione requisiti minimi:** Entro ottobre 2026, adempimento agli obblighi di base in materia di sicurezza informatica

NIS2 – MISURE DI SICUREZZA

- Politiche sull'analisi del rischio e sulla sicurezza dei sistemi informativi
- Gestione degli incidenti
- Continuità operative e gestione della crisi
- Supply chain security
- Sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi
- Politiche e procedure per valutare l'efficacia delle misure di gestione del rischio informatico
- Politiche di formazione sulla Cybersecurity
- Politiche e procedure sull'uso di crittografia e cifratura
- Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione degli asset
- MFA, autenticazione continua e comunicazioni sicure

Riferimenti

Francesco Carraro
Manager – CyberSecurity Governance
francesco.carraro@bgt.it.gt.com

Mattia Campagner
Manager – CyberSecurity Governance
mattia.campagner@bgt.it.gt.com

Gianluca Montinaro
Sales Manager
gianluca.montinaro@bgt.it.gt.com