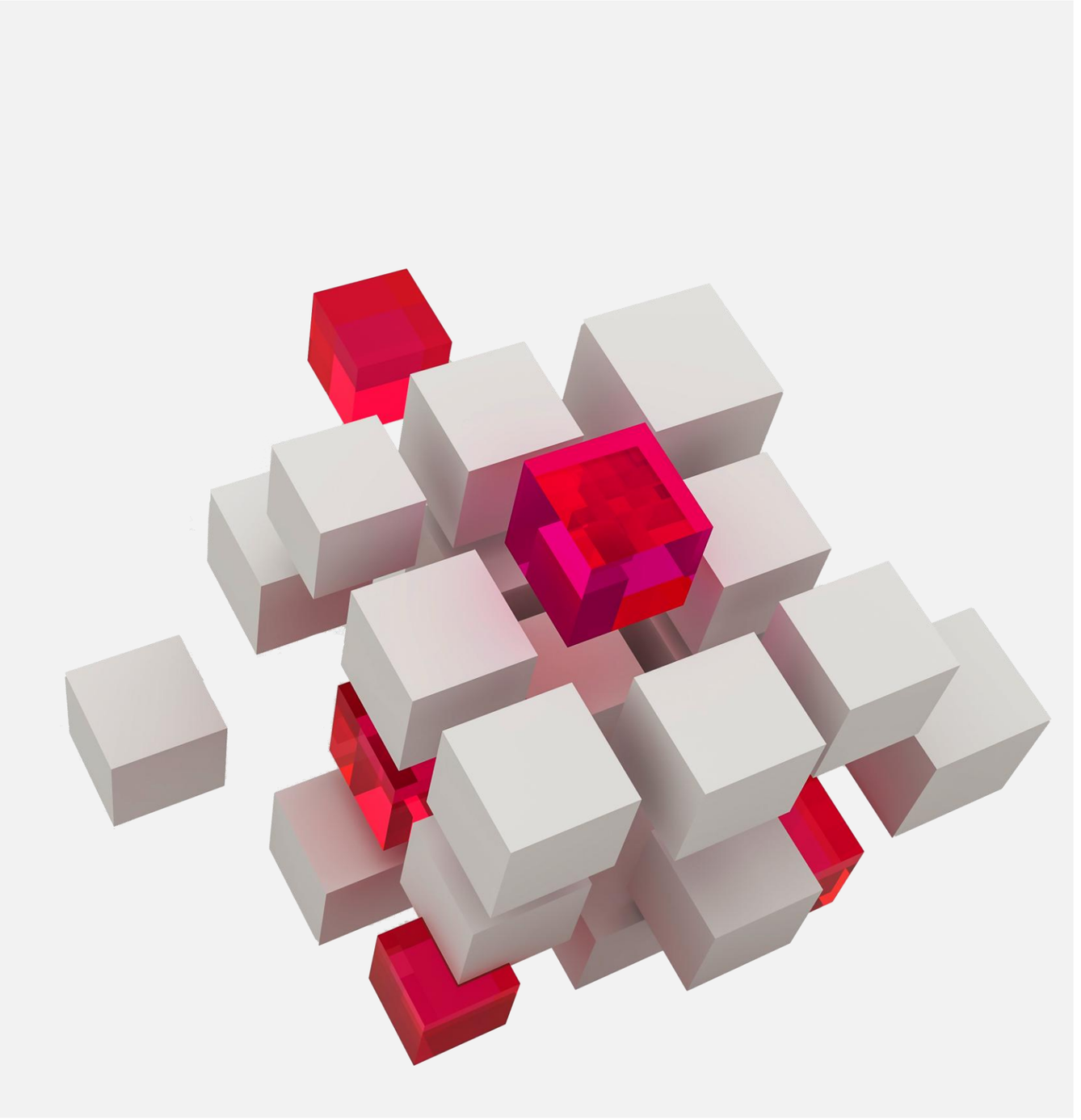
S3K

CTI WEEKLY

Bollettino Settimanale di Cyber Threat Intelligence

Periodo: 28 dicembre 2025 – 4 gennaio 2026

Analisi completa delle minacce informatiche rilevate nel panorama italiano ed europeo. Questo bollettino fornisce una panoramica dettagliata degli attacchi ransomware, data leak, vulnerabilità critiche e campagne di phishing che hanno caratterizzato la settimana, con raccomandazioni specifiche per la protezione delle organizzazioni.



www.s3kgroup.it

Panorama delle Minacce: Una Settimana ad Alta Criticità

6

Aree di minaccia principali

Ransomware, data leak, vulnerabilità critiche, phishing, malware e social engineering

90K+

Dispositivi compromessi

Dalla botnet RondoDox attraverso vulnerabilità IoT

1.4M

Utenti italiani esposti

Nel leak di immobiliare.it con dati sensibili

La settimana ha evidenziato un'escalation coordinata delle attività malevole, con gruppi ransomware altamente attivi e violazioni di dati che interessano direttamente il territorio italiano. L'intensità degli attacchi suggerisce una strategia pianificata da parte degli attori delle minacce.

Attacchi Ransomware: Operazioni Coordinate e Globali

I gruppi ransomware hanno dimostrato una capacità operativa sofisticata, colpendo simultaneamente organizzazioni in diversi continenti. La diversificazione settoriale degli attacchi indica una strategia opportunistica che sfrutta vulnerabilità trasversali.

Gruppo Direwolf

Attacchi multipli in Argentina, Spagna e Turchia

- **Laurenzano Logistics**
- **Hydrodiseño**
- **Varimed Medikal**

Gruppo Qilin

Operazioni diversificate in Asia, Europa e America

- **CSV Group (Italia)**
- **Sönmezler Metal**
- **Farmacia San Pablo**

Altri Attori

Lockbit5, Dragonforce ed Everest attivi

- **Settore sanitario**
- **Costruzioni**
- **Automotive**

Impatto sul Territorio Italiano: CSV Group nel Mirino

Attacco a CSV Group

Il gruppo ransomware Qilin ha rivendicato un attacco significativo contro CSV Group, un'azienda italiana, evidenziando l'escalation delle minacce dirette verso organizzazioni nazionali. L'attacco rappresenta un chiaro segnale dell'interesse crescente dei cybercriminali verso il tessuto imprenditoriale italiano.

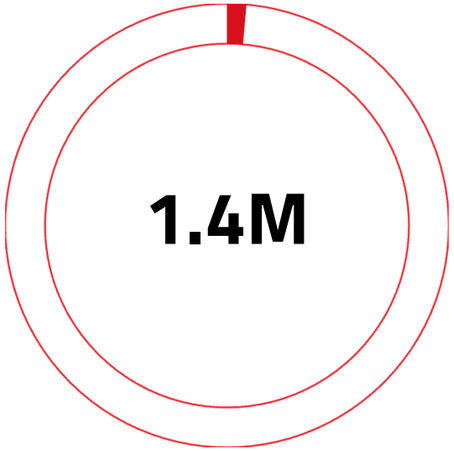
Implicazioni operative: Potenziali interruzioni dei servizi, compromissione dei dati aziendali e rischio di richieste di riscatto elevate. Le aziende del settore devono intensificare immediatamente i controlli di sicurezza.

Urgenza Elevata

Le organizzazioni italiane devono considerare questo attacco come un indicatore di rischio diretto e implementare misure preventive immediate.

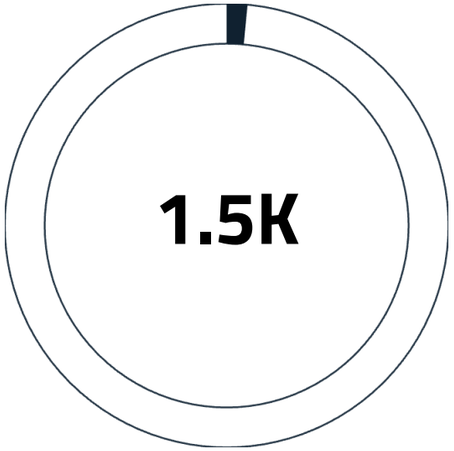
Data Leak: Violazioni Massive di Dati Italiani

La settimana ha registrato esposizioni critiche di dati che coinvolgono milioni di utenti italiani, con conseguenze potenzialmente devastanti per la privacy e la sicurezza finanziaria.



Immobiliare.it

PII, numeri di telefono ed email di agenti immobiliari compromessi



Email italiane

Accessi non autorizzati con potenziale compromissione delle comunicazioni

Combo dati

Pacchetti di informazioni sensibili in vendita su forum underground

---

DAZN Italia e Altri Servizi Compromessi

I leak di DAZN Italia, con scadenze programmate per gennaio e febbraio 2026, suggeriscono attacchi pianificati e coordinati. La compromissione di piattaforme di streaming e servizi online evidenzia vulnerabilità sistemiche nelle infrastrutture digitali.

Servizi e Siti Web Italiani Sotto Attacco

Piattaforme di Intrattenimento

NowTV.it – Credenziali di accesso compromesse con rischio di accesso non autorizzato agli account utente

Servizi Professionali

Fotografiaparisirosario.it – Database potenzialmente esposti con informazioni di clienti e transazioni

Settore Sanitario

Pentadiet.it – Leak del database con implicazioni per la privacy dei dati sanitari sensibili

Documenti Fraudolenti

Mercato nero di documenti falsi di alta qualità, inclusi passaporti e certificati utilizzabili per frodi di identità

Malware e Infrastrutture: Minacce in Evoluzione

RondoDox Botnet

Vulnerabilità sfruttata: React2Shell (CVSS 10.0)

Impatto: 90.300+ dispositivi IoT e server web compromessi

La botnet rappresenta una minaccia critica per le infrastrutture connesse, evidenziando l'urgenza di applicare patch di sicurezza alle applicazioni vulnerabili.

GlassWorm su macOS

Vettore di attacco: Estensioni Visual Studio Code trojanizzate

Obiettivo: Furto di portafogli di criptovaluta

Attacchi sofisticati mirati agli sviluppatori attraverso strumenti di lavoro quotidiani, ampliando la superficie di attacco.

Settore Finanziario

60 istituzioni bancarie globali colpite da malware Android che drena i conti

Botnet Kimwolf

Attività malevola nelle reti locali, richiede monitoraggio infrastrutturale

AI-Enabled Malware

Malware adattivo che modifica il comportamento in tempo reale

Supply Chain Attack

EmEditor compromesso per distribuire infostealer

Phishing e Social Engineering: Tecniche Avanzate

Le campagne di phishing hanno raggiunto livelli di sofisticazione allarmanti, sfruttando servizi cloud legittimi e tecniche multi-stadio per eludere i sistemi di rilevamento tradizionali.

Abuso Google Cloud

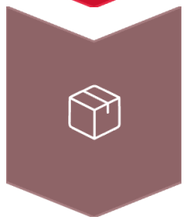
Impersonificazione di email legittime attraverso infrastrutture Google per campagne di furto credenziali su larga scala

SMS Spoofing

Servizi di invio SMS falsificati per distribuire messaggi malevoli a volumi elevati, compromettendo la fiducia degli utenti

WordPress Targeting

Email fraudolente per il rinnovo domini che rubano informazioni di pagamento e codici OTP



Servizi Consegna

Pagine di phishing che imitano Evri e altri corrieri per raccogliere dati personali

Vettori di Attacco Emergenti

Pacchetti npm Malevoli

Librerie JavaScript compromesse utilizzate come infrastruttura di phishing per il furto di credenziali. Le organizzazioni che utilizzano npm devono implementare controlli rigorosi sulle dipendenze.

Gaming Exploits

Cheat per Apex Legends e Fortnite contenenti funzionalità di spoofing e raccolta dati. Rappresentano un rischio spesso sottovalutato ma significativo.

Call ID Spoofing

Strumenti avanzati per falsificare chiamate e ID caller, utilizzati in attacchi di social engineering sofisticati contro dipendenti aziendali.

Vulnerabilità Critiche: Urgenza Massima

Otto vulnerabilità ad alto impatto richiedono attenzione immediata, con potenziali conseguenze devastanti per le organizzazioni che tardano nell'applicazione delle patch.

1

n8n RCE (CVE-2025-68613)

CVSS Score: Critico

Esecuzione codice remoto in n8n <1.120.4. Attaccanti autenticati possono compromettere l'intera istanza della piattaforma di automazione.

2

MongoBleed (CVE-2025-14847)

CVSS Score: Critico

Perdita di memoria non autenticata in MongoDB. Exploit PoC disponibili pubblicamente, esposizione di dati sensibili imminente.

3

Ksenia Security (CVE-2025-15111)

CVSS Score: Alto

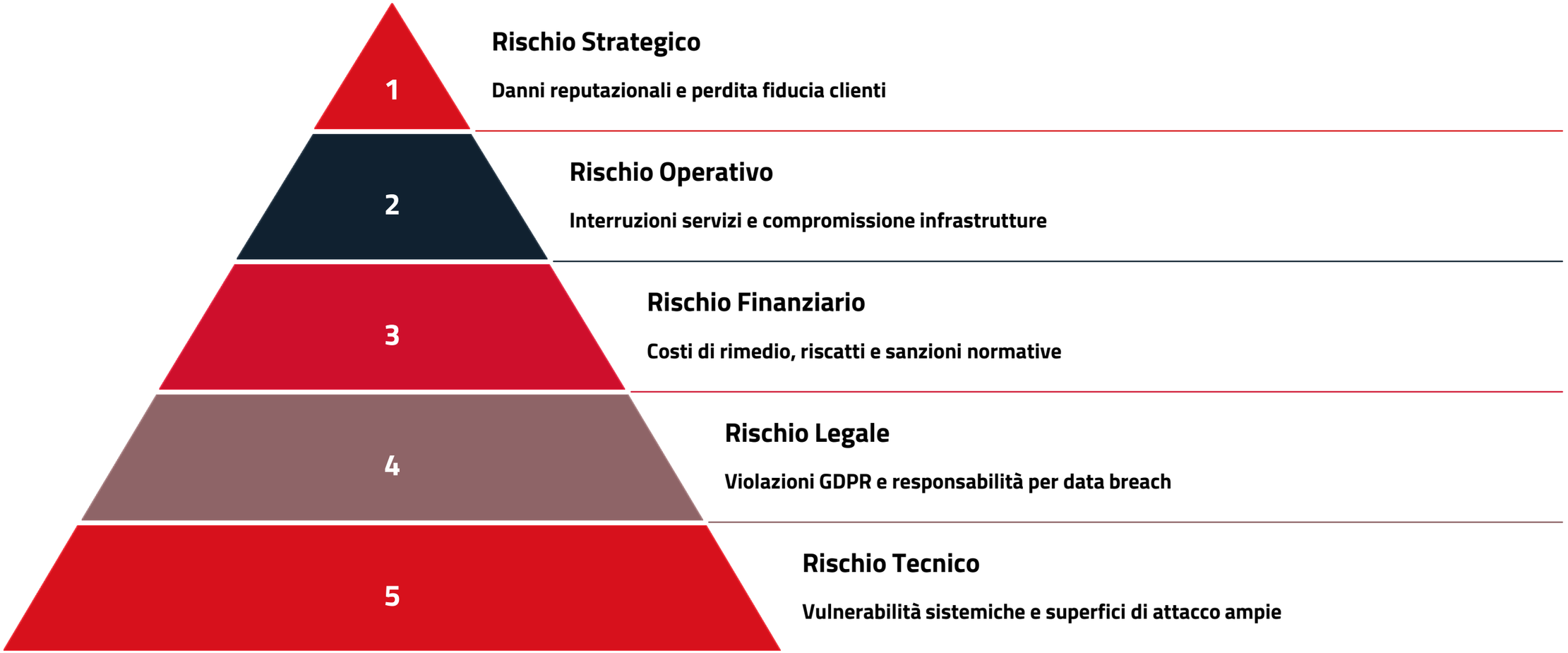
Credenziali predefinite deboli consentono accesso amministrativo non autorizzato ai sistemi di automazione domestica v1.6.

Ulteriori Vulnerabilità Critiche da Monitorare

CVE	Sistema	Impatto
CVE-2025-22777	GiveWP	Deserializzazione non sicura consente iniezione di oggetti PHP
CVE-2025-64120	Nuvation Energy	Iniezione comandi OS su controller multi-stack
CVE-2025-15113	Ksenia Lares	RCE tramite caricamento file non protetti
CVE-2025-66824	TrueConf	XSS consente esecuzione codice arbitrario
CVE-2025-15421	Yonyou KSOA	SQL Injection per compromissione database

Azione richiesta: Le organizzazioni devono implementare immediatamente le patch disponibili e condurre scansioni per identificare sistemi vulnerabili nella propria infrastruttura.

Analisi del Rischio: Impatto sulle Organizzazioni Italiane



La convergenza di queste minacce crea uno scenario di rischio elevato per le organizzazioni italiane. La compromissione di CSV Group e i massicci data leak dimostrano che gli attori delle minacce stanno attivamente prendendo di mira il territorio nazionale con strategie coordinate.

Raccomandazioni Immediate: Piano d'Azione

Patch Management Accelerato

Implementare immediatamente le patch per CVE-2025-68613, CVE-2025-14847 e altre vulnerabilità critiche. Prioritizzare i sistemi esposti pubblicamente e le applicazioni mission-critical.

Resilienza Ransomware

Verificare l'efficacia dei backup offline, testare le procedure di ripristino e implementare segmentazione di rete per limitare la propagazione laterale degli attacchi.

Monitoraggio Proattivo

Intensificare il monitoraggio delle infrastrutture IoT, implementare detection per botnet RondoDox e GlassWorm, analizzare traffico anomalo verso servizi cloud.

Formazione Continua

Condurre simulazioni di phishing focalizzate su Google Cloud spoofing e SMS fraudolenti. Sensibilizzare il personale sulle tecniche di social engineering emergenti.

Strategie di Difesa a Lungo Termine

Architettura di Sicurezza

Zero Trust: Implementare modello zero-trust con autenticazione continua e micro-segmentazione

EDR/XDR: Deploy di soluzioni di detection avanzate per identificare comportamenti anomali

SIEM: Centralizzare i log e correlare eventi per rilevamento tempestivo

Threat Intelligence: Integrare feed CTI per anticipare minacce emergenti

Processi Operativi

Incident Response: Aggiornare playbook con scenari ransomware e data leak

Vulnerability Management: Ciclo continuo di scansione, prioritizzazione e remediation

Access Management: Rivedere privilegi, implementare MFA su tutti i sistemi critici

Supply Chain: Audit di sicurezza su fornitori e partner tecnologici

Focus Italia: Considerare la compliance GDPR e NIS2 come parte integrante della strategia di sicurezza, non come mero adempimento normativo.

Conclusioni e Prossimi Passi

La settimana analizzata rappresenta un punto di svolta nel panorama delle minacce informatiche rivolte all'Italia. L'intensità e la coordinazione degli attacchi, uniti alla sofisticazione delle tecniche impiegate, richiedono un cambio di paradigma nella gestione della sicurezza informatica.

Urgenza

Le organizzazioni italiane sono nel mirino diretto di attori delle minacce globali. Il tempo di reazione è critico.

Investimento

La sicurezza informatica deve essere trattata come investimento strategico, non come centro di costo.

Collaborazione

Condivisione di intelligence tra organizzazioni e autorità è fondamentale per la difesa collettiva.

Prossimi Passi Raccomandati

1. Condurre assessment di sicurezza immediato focalizzato sulle vulnerabilità critiche identificate
2. Implementare un piano di risposta agli incidenti testato e aggiornato con scenari realistici
3. Stabilire un programma di threat intelligence per monitoraggio continuo del panorama delle minacce
4. Pianificare investimenti in tecnologie di detection e response di nuova generazione
5. Rafforzare la cultura della sicurezza attraverso programmi di awareness mirati e continui

La cybersecurity non è più un problema tecnico, ma una priorità strategica di business che richiede attenzione e risorse adeguate da parte del management.

Company Profile S3K

Tutto il nostro essere è racchiuso nella nostra VISION: “Rendere il mondo digitale un luogo accessibile, sicuro e sostenibile, al servizio della conoscenza”

COME LO FACCIAMO:

Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.

Abbiamo un presidio esteso sul territorio con circa 550 dipendenti distribuiti tra le sedi di Roma, Milano, Torino, Padova, Firenze, Palermo e Catania. L’ambizione e la prospettiva vedono un ulteriore e progressivo rafforzamento sia sul territorio nazionale che internazionale dove già operiamo con successo e con Clienti di primaria rilevanza.

CON QUALI LEVE OPERIAMO:

Le nostre competenze principali: Data Analytics & Big Data, CyberSecurity, Application Development, Infrastructure Management, Cloud & Managed Security Services.

Più caratteristiche sono poi le nostre competenze verticali, nel novero delle quali particolare attenzione va al PLM, Modelling & Simulation (la società di S3K, Fabaris, è l'unica azienda italiana che sa utilizzare il sistema di modellazione e simulazione jtls (joint theatre level simulation) utilizzato dalla Nato)) e Digital Transaction Management, Business Operation Systems.

40 partnership strategiche, 215 certificazioni professionali, un’esperienza complessiva che sfiora i 150 anni uomo, ed oltre 500 clienti attivi.

CHI SIAMO:

Un FULL SERVICE PARTNER DELLA DIGITAL & SECURITY TRANSFORMATION. Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.

S3K nasce nel dicembre 2021 come fusione di importanti realtà già operanti su questi mercati in seguito all’ingresso di un importante Private Equity internazionale (HLD).

LA NOSTRA MISSION:

“Guidiamo i Clienti nei loro processi di cambiamento, riducendo complessità e rischi attraverso competenze multidisciplinari, nel pieno rispetto dei nostri valori fondamentali e delle nostre persone”.

I NOSTRI VALORI:

Affidabilità; Integrità; Rispetto; Valorizzazione delle Persone; Passione; Innovazione.

CONTATTI:

contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

DISCLAIMER

CLASSIFICAZIONE DOCUMENTO

2.0 TLP:CLEAR = Divulgazione illimitata

Classificazione Traffic Light Protocol (TLP): sistema di contrassegni che definisce la misura in cui i destinatari possono condividere informazioni potenzialmente sensibili pubblicato formalmente da Forum of Incident Response and Security Teams (FIRST) nella versione TLP 1.0 nell'agosto 2016 e successivamente aggiornato alla versione TLP 2.0 nell'agosto 2022. Secondo FIRST, lo scopo di TLP è “facilitare una maggiore condivisione di informazioni potenzialmente sensibili e collaborazione più efficace”. La versione 2.0 migliora TLP chiarendo ulteriormente le restrizioni di condivisione.

S3K

Cyber security

RISK REPORT

S3K

Via del Serafico, 200 - 00142 | Roma (RM)

C.S.iv. € 10.050.000,00 - C.F. e P.IVA: 15379561002

ISO 14001 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

ISO 45001 BUREAU VERITAS Certification