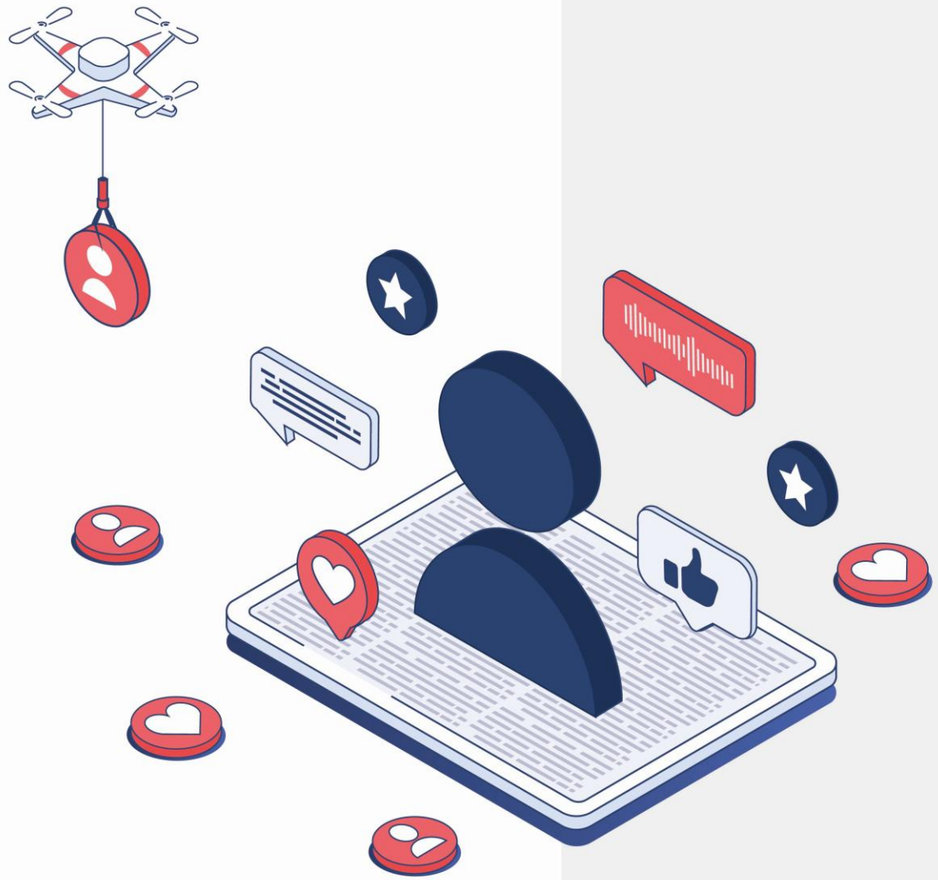
S3K

Cyber Threat

WEEKLY REPORT

\ week 16/02/2026 - 22/02/2026



www.s3kgroup.it

Sommario

Aumento delle vulnerabilità critiche

Scoperte vulnerabilità significative in SolarWinds e Ivanti, con impatti diretti su settori critici come energia e sanità, richiedendo monitoraggio attento da parte delle organizzazioni italiane

Attacchi ransomware in crescita

Diverse organizzazioni, tra cui il University of Mississippi Medical Center, hanno subito attacchi ransomware, evidenziando la vulnerabilità del settore sanitario

Campagne di phishing mirate

Emerse campagne di phishing, tra cui una a tema Intesa Sanpaolo, che sfruttano tecniche di ingegneria sociale per rubare credenziali, colpendo in particolare gli utenti italiani

- **Nuove varianti di malware**

  Malware come Arkanix Stealer e PromptSpy, che utilizzano intelligenza artificiale, sono stati identificati, aumentando la complessità delle minacce per le organizzazioni

- **Data breach significativi**

  Incidenti come il leak di waluta.it e la violazione della French National Bank Authority hanno esposto dati sensibili, sottolineando la vulnerabilità dei sistemi

- **Patch urgenti necessarie**

  Vulnerabilità critiche in prodotti come Google Chrome e Dell RecoverPoint richiedono aggiornamenti immediati per prevenire potenziali attacchi

NEWS CYBER

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un incremento significativo delle vulnerabilità e degli attacchi informatici, con particolare attenzione a settori critici come l'energia e la sanità. Diverse vulnerabilità di alto profilo sono state scoperte in software ampiamente utilizzati, mentre attacchi mirati hanno colpito istituzioni e aziende in tutto il mondo. La situazione richiede un monitoraggio attento e una pronta risposta da parte delle organizzazioni italiane ed europee.

Vulnerabilità e Infrastrutture

- Vulnerabilità critiche in SolarWinds e Ivanti EPMM discusse in forum underground; CISA emette 15 avvisi ICS
- Flaws in estensioni VSCode scaricate oltre 128 milioni di volte: furto file locali ed esecuzione remota
- Hacker cinesi sfruttano zero-day critico di Dell in attacchi avviati a metà 2024
- Sfruttamento zero-day in Ivanti EPMM: web shell già installate sui server

Attacchi e Minacce Emergenti

- Cyberattacco al University of Mississippi Medical Center: chiusura cliniche e cancellazione interventi chirurgici
- Campagna di social engineering Graphalgo mira a sviluppatori crypto e blockchain
- Notepad++ implementa meccanismo di "doppio blocco" per aggiornamenti dopo compromissioni supply chain
- Spyware Predator su iOS: nasconde indicatori di registrazione, audio e video segreti

Focus Settimana: La settimana ha evidenziato una crescente complessità e pericolosità delle minacce informatiche, con vulnerabilità critiche e attacchi mirati che colpiscono settori vitali. È fondamentale che le organizzazioni italiane ed europee rimangano vigili e pronte a rispondere a queste sfide in continua evoluzione.

DATA BREACH

Data Leak & Breach: Scenario della Settimana

1.2M

Conti French National Bank

Un attacco ha compromesso 1,2 milioni di conti bancari, con l'esposizione di credenziali sensibili presso la French National Bank Authority

12M

Account CarGurus

Il marketplace automobilistico ha subito una violazione che ha coinvolto oltre 12 milioni di account, con dati personali e finanziari esposti

1M

Clienti Figure Technology

Un attacco ha colpito quasi un milione di clienti di Figure Technology con furto di dati personali, evidenziando i rischi delle fintech

6M

Mesi Esposizione PayPal

Un errore software ha esposto informazioni personali di utenti PayPal per sei mesi, mettendo in luce le sfide della gestione della sicurezza online

La settimana ha evidenziato un aumento preoccupante delle violazioni di dati, con impatti significativi su utenti e aziende in Italia e in Europa. Sono emersi inoltre un leak di waluta.it, diverse liste email premium italiane pubblicate in batch, un database di documenti identificativi italiani in vendita e un leak del Forex Crypto Database italiano. È fondamentale che le organizzazioni adottino misure proattive per proteggere le informazioni sensibili e mitigare i rischi associati a questi eventi.

Minacce per Settori Critici

Settore Bancario

La French National Bank Authority ha subito un attacco con 1,2 milioni di conti bancari compromessi, evidenziando la vulnerabilità delle istituzioni finanziarie europee

Automotive & Marketplace

CarGurus ha subito una violazione con oltre 12 milioni di account coinvolti, con dati personali e finanziari esposti, evidenziando il rischio per utenti e aziende partner

Fintech

Figure Technology colpita da attacco con quasi un milione di clienti coinvolti, sottolineando i rischi associati alle fintech e la necessità di proteggere le informazioni sensibili

Pagamenti Online

Un errore software PayPal ha esposto dati personali di utenti per sei mesi, mettendo in luce le sfide legate alla gestione della sicurezza nei servizi online

MALWARE

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un incremento significativo di attività malevole, con nuove varianti di malware e tecniche di attacco che sfruttano l'intelligenza artificiale e metodi di social engineering. Le organizzazioni italiane ed europee devono prestare particolare attenzione a queste minacce, poiché i criminali informatici stanno affinando le loro strategie per colpire obiettivi sempre più complessi e diversificati.

Campagne Principali

1. **Arkanix Stealer:** Nuovo infostealer sviluppato con AI, promosso su forum dark web, attivo per diversi mesi e mirante a una vasta gamma di dati. Approfondisci
2. **PromptSpy (Android):** Primo malware Android noto a utilizzare AI generativa per adattare la sua persistenza su diversi dispositivi, passo avanti nella sofisticazione mobile. Approfondisci
3. **Massiv – Trojan bancario:** Distribuito attivamente in Europa meridionale mascherato da app IPTV, progettato per compromettere i dati bancari degli utenti. Approfondisci

Minacce Emergenti

ClickFix – Nuova Variante

Utilizza DNS e Google Ads per distribuire payload malevoli, trasformando gli utenti in vettori di infezione

Keenadu Backdoor Android

Integrata nel firmware di vari dispositivi Android, consente controllo totale delle applicazioni installate

Furto Segreti OpenClaw

Infostealer rileva e ruba file associati all'assistente AI OpenClaw, evoluzione nelle tecniche di furto informazioni

Un'analisi di 90.000 dump di credenziali ha rivelato che gli infostealers stanno sempre più legando le credenziali rubate a identità reali, aumentando il rischio per le aziende. La scansione continua di Active Directory è suggerita come misura per interrompere questo ciclo. Approfondisci

PHISHING

Phishing & Social Engineering

01

Phishing a tema Intesa Sanpaolo

Il CSIRT IT ha segnalato una campagna via email mirata a rubare credenziali bancarie e dati delle carte di pagamento degli utenti Intesa Sanpaolo. Approfondisci

02

Phishing 'Starkiller'

Nuovo servizio di phishing che replica pagine di login reali, agendo da intermediario tra utente e sito legittimo per raccogliere credenziali e codici MFA. Leggi di più

03

Campagne CERT-AgID della Settimana

Identificate 98 campagne malevole, di cui 60 dirette a obiettivi italiani. Inclusa campagna smishing INPS per rubare dati personali. Forniti 751 IoC alle organizzazioni accreditate

04

Attacchi Vishing su Microsoft Entra

Attacchi combinati phishing e vishing contro account Microsoft Entra, colpendo settori tecnologici e finanziari tramite flusso OAuth 2.0. Ulteriori dettagli

05

Phishing 'Esaurimento Spazio Cloud'

Il CSIRT IT ha rilevato una campagna email che inganna le vittime promettendo aumento dello spazio di archiviazione, mirando a rubare dati delle carte di credito. Scopri di più

Tecniche Avanzate Emergenti

- Phishing adattivo con tecniche semplici ma efficaci combinate
- Smishing a tema INPS: richiesta documenti personali e informazioni lavorative
- Spoofing di domini mittente e aggiro dei controlli di sicurezza
- Campagna Graphalgo: social engineering su sviluppatori crypto

Problemi di Sicurezza

- 98 campagne malevole identificate in una settimana, 60 su target italiani
- Attacchi vishing che sfruttano il flusso di autorizzazione OAuth 2.0
- Phishing adattivo in crescita: difficile da riconoscere per le vittime
- Aumento uso piattaforme SaaS legittime per eludere controlli

RANSOMWARE

Operazioni Ransomware Active

Negli ultimi sette giorni, il panorama degli attacchi ransomware ha mostrato un'attività intensa e preoccupante, con diverse organizzazioni colpite in vari settori. Le vulnerabilità di sicurezza continuano a essere sfruttate rapidamente dai gruppi di cybercriminali, evidenziando la necessità di una vigilanza costante e di misure di protezione adeguate. Le notizie di attacchi recenti rivelano un'evoluzione nelle tecniche di estorsione e una crescente sofisticazione degli attaccanti.

Chiusura Cliniche Mississippi

Il University of Mississippi Medical Center ha chiuso tutte le sue cliniche a causa di un attacco ransomware, dimostrando come il settore sanitario sia obiettivo privilegiato. 🔗 Bleepingcomputer

Vulnerabilità BeyondTrust Sfruttata

La CISA ha avvertito che la vulnerabilità CVE-2026-1731 in BeyondTrust Remote Support è attivamente sfruttata in attacchi ransomware. 🔗 Bleepingcomputer

Cheyenne e Arapaho Tribes – Oklahoma

Dopo un attacco che ha chiuso scuole e sistemi critici, i criminali informatici stanno estorcendo il governo delle tribù Cheyenne e Arapaho. 🔗 Therecord

Attacco a Advantest

La società giapponese Advantest ha subito un attacco ransomware che potrebbe aver compromesso dati di clienti e dipendenti. 🔗 Bleepingcomputer

Il gruppo ransomware **Tengu** ha rivendicato attacchi contro femar.it, mentre **Qilin** ha colpito Bluefish Dental & Orthodontics. Il gruppo **Play** ha rivendicato attacchi contro PenLink e Young & Associates Consulting Engineers. In Polonia, la polizia ha arrestato un sospetto legato al gruppo **Phobos**, sequestrando dispositivi con credenziali rubate. 🔗 Bleepingcomputer

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1

CVE-2026-22769

Dell RecoverPoint per Virtual Machines: vulnerabilità zero-day critica sfruttata da gruppo hacker cinese, consente accesso non autorizzato al sistema operativo sottostante. Aggiornamento immediato raccomandato

2

CVE-2026-2441

Google Chrome: vulnerabilità critica confermata come attivamente sfruttata. Gli utenti sono invitati a installare la patch immediatamente per evitare potenziali attacchi

3

CVE-2026-1340 / CVE-2026-1281

Ivanti: due vulnerabilità critiche, una delle quali di tipo zero-day. Potrebbero consentire a un attaccante remoto di eseguire codice arbitrario sui sistemi interessati

4

CVE-2026-25926

Notepad++: rilasciato un PoC per vulnerabilità che potrebbe consentire l'esecuzione di codice arbitrario. Rischio elevato per versioni non aggiornate

5

CVE-2026-26000

XWiki Platform: PoC reso pubblico per vulnerabilità che potrebbe consentire attacchi di redirezione URL e manomissione. Monitoraggio attento consigliato

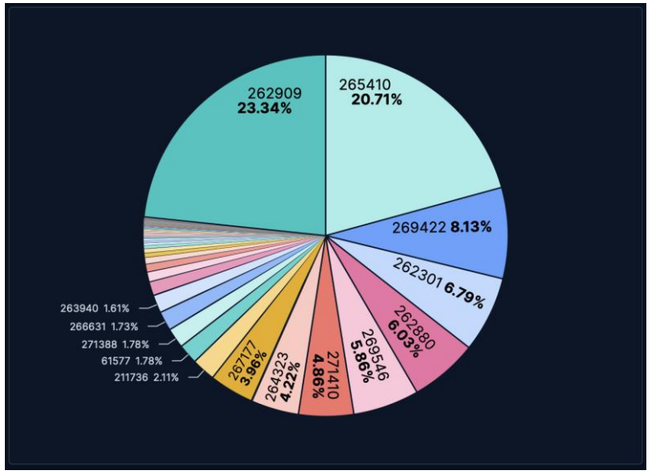
6

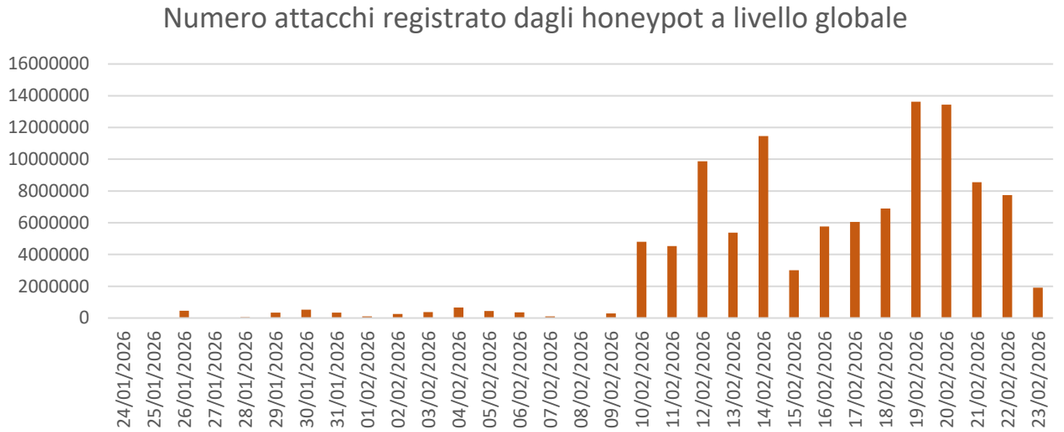
CVE-2026-27112

Kargo: vulnerabilità di bypass dell'autenticazione tramite payload YAML malformati. Gli amministratori sono avvisati di applicare le patch necessarie

Approfondimenti sulla CVE-2026-22769

Traffico in crescita su porte 80/8080/443/8443 L'aumento degli alert nelle ultime due settimane non è di per sé anomalo, ma la progressività e la concentrazione su un arco temporale correlato alla disclosure suggerisce scanning sistematico verso asset web esposti. È traffico di interesse, non comprova compromissione. **Concentrazione ASN brasiliana (ASN 262909 / ASN 265410)** Il dato >40% su due ASN specifici è un indicatore infrastrutturale forte. Questi ASN sono ricorrentemente associati a infrastrutture di scanning-as-a-service e a proxy/VPS utilizzati da attori opportunistici. La concentrazione suggerisce riutilizzo deliberato della stessa infrastruttura.**Evoluzione della minaccia: UNC6201 → rilascio pubblico exploit → mass exploitation** La progressione attributiva è rilevante: UNC6201 (tracciato da Mandiant/GTIG) opera tipicamente in fasi di reconnaissance e initial access prima che il vettore diventi pubblico. Dopo il rilascio del PoC, la soglia di ingresso si abbassa drasticamente e il numero di attori operativi cresce in modo non lineare.





Il quadro descritto è coerente con una campagna post-disclosure strutturata, probabilmente riferita a una vulnerabilità critica su infrastrutture Dell con exploit pubblicamente disponibile. La progressione su 4 settimane riflette la dinamica classica: initial scanning da attori avanzati (UNC6201), seguita da mass exploitation dopo rilascio del PoC. **In sintesi** il segnale è reale e la finestra temporale è critica. La combinazione di exploit pubblico, attore tracciato (UNC6201), concentrazione infrastrutturale e crescita progressiva del traffico configura un rischio elevato e immediato per chi ha asset Dell vulnerabili esposti. La priorità è ridurre la superficie prima che lo scanning si converta in exploitation confermata.

Vulnerabilità Aggiuntive e Patch

CVE-2026-27206

Zumba Json Serializer: vulnerabilità di iniezione oggetti PHP che potrebbe consentire attacchi di deserializzazione. Aggiornare alla versione corretta

CVE-2026-26010

OpenMetadata: PoC disponibile per vulnerabilità che potrebbe consentire accesso non autorizzato a informazioni sensibili e l'elevazione dei privilegi

SmarterMail – Exploit Underground

Canali Telegram underground condividono exploit e credenziali rubate per SmarterMail (CVE-2026-24423 e CVE-2026-23760), usate in attacchi ransomware

CISA – 15 Avvisi ICS

CISA ha emesso 15 avvisi riguardanti sistemi di controllo industriale, con impatti sui settori dell'energia e della produzione critica

Sfruttamento SolarWinds

Vulnerabilità in SolarWinds discusse in forum underground con impatti significativi su settori energia e produzione critica. Vigilanza costante necessaria

Azione Immediata

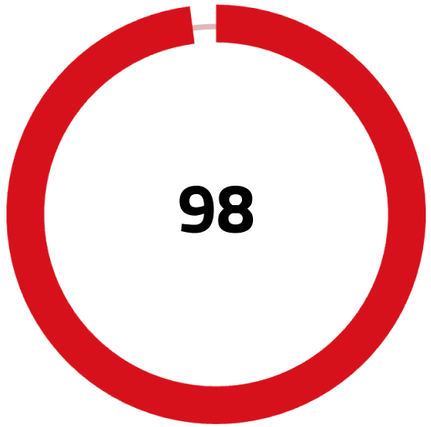
Mantenere aggiornati tutti i sistemi, applicare patch tempestivamente per Chrome, Dell RecoverPoint e Ivanti, monitorare segnalazioni vulnerabilità attivamente

La settimana ha evidenziato un numero significativo di vulnerabilità critiche e PoC pubblici, sottolineando l'importanza di un approccio proattivo alla sicurezza informatica. Le organizzazioni devono rimanere vigili e attuare tempestivamente le patch per proteggere i propri sistemi da potenziali exploit, con priorità assoluta a Dell RecoverPoint, Google Chrome e Ivanti.

ANALISI

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un incremento allarmante delle vulnerabilità e degli attacchi, con un focus particolare su settori critici come l'energia, la sanità e le istituzioni finanziarie. Le vulnerabilità zero-day in Dell RecoverPoint e Google Chrome sono state attivamente sfruttate, mentre campagne di phishing e social engineering hanno preso piede con attacchi mirati. Rispetto alle settimane precedenti, si osserva un aumento della complessità e della diversificazione delle tecniche di attacco, con l'uso crescente di AI nei malware.

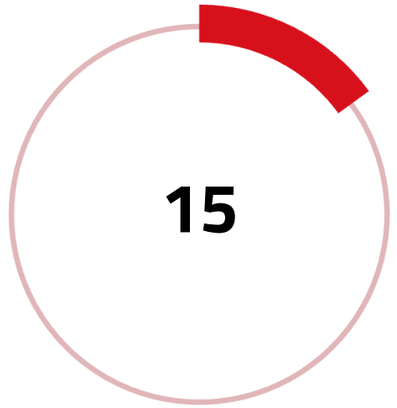


Campagne Malevole

Campagne malevole identificate dal CERT-AgID nella settimana, di cui 60 su target italiani

IoC Condivisi

Indicatori di compromissione forniti alle organizzazioni accreditate dal CERT-AgID



Avvisi ICS CISA

Avvisi emessi da CISA riguardanti sistemi di controllo industriale critici

Tendenze Emergenti

- Malware basati su AI: Arkanix Stealer e PromptSpy segnano nuova era
- Ransomware che colpisce settore sanitario con impatti devastanti
- Campagne phishing italiane mirate: Intesa Sanpaolo, INPS, spazio cloud
- Zero-day attivamente sfruttati in Dell RecoverPoint da attori statali cinesi

Settori più Colpiti

- Sanità: University of Mississippi Medical Center chiuso da ransomware
- Bancario: French National Bank Authority, 1,2M conti compromessi
- Fintech: Figure Technology, quasi 1M clienti colpiti
- Infrastrutture critiche: energia e produzione colpite da vulnerabilità ICS

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per mitigare i rischi associati alle minacce della settimana, è fondamentale che le organizzazioni adottino un approccio proattivo alla sicurezza informatica. Il contesto in continua evoluzione richiede particolare attenzione. Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente il panorama delle minacce informatiche in continua evoluzione.

01

Patch Management Urgente

Implementare patch management rigoroso con priorità assoluta a Google Chrome, Dell RecoverPoint e Ivanti EPMM, assicurando che tutte le vulnerabilità note siano risolte tempestivamente

02

Formazione Continua Anti-Phishing

Investire in formazione continua del personale sulle tecniche di phishing e social engineering, con focus specifico su campagne a tema Intesa Sanpaolo, INPS e spazio cloud

03

Monitoraggio Infrastrutture

Monitorare costantemente le proprie infrastrutture per rilevare attività sospette, con attenzione ai nuovi malware AI-based (Arkanix Stealer, PromptSpy) e dark web leak italiani

04

Piano Risposta Incidenti Ransomware

Rafforzare piani di risposta agli incidenti per garantire reazione rapida in caso di attacco ransomware, con particolare attenzione al settore sanitario e alle infrastrutture critiche

05

Collaborazione con Autorità

Collaborare con CSIRT Italia, ACN e CERT-AgID, condividendo informazioni sulle minacce per migliorare la resilienza collettiva contro le cyber minacce italiane ed europee

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).

CONTATTI:
contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

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