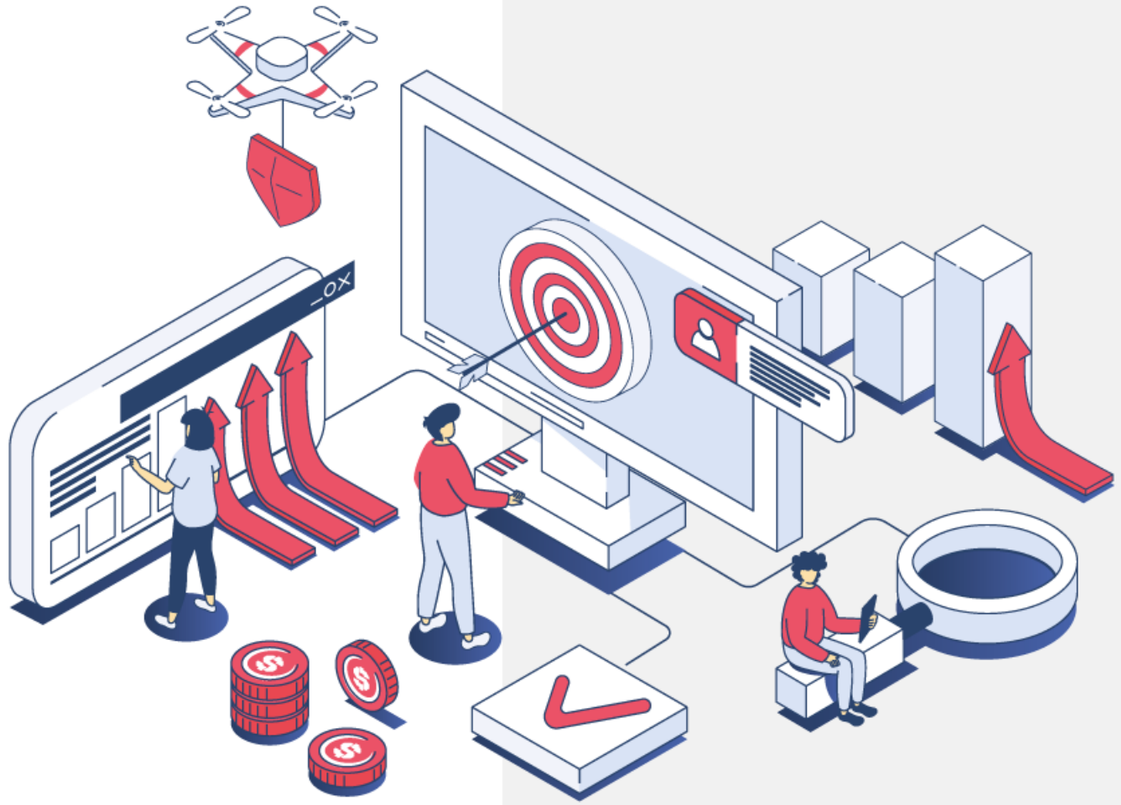
S3K

Cyber Threat

WEEKLY REPORT

\ week 09/03/2026 - 15/03/2026



www.s3kgroup.it

CTI WEEKLY

Aumento delle vulnerabilità critiche

Vulnerabilità gravi in SolarWinds e Ivanti, con impatti significativi per le organizzazioni italiane nei settori energetico e manifatturiero.

Nuove campagne di phishing

Il CERT-AGID ha registrato 103 campagne di phishing, di cui 70 mirate a obiettivi italiani, con incremento delle truffe legate a servizi pubblici e finanziari.

Attacchi ransomware in Italia

Il gruppo LockBit ha rivendicato attacchi a diverse aziende italiane, sottolineando la vulnerabilità delle organizzazioni locali.

Malware emergenti

Scoperto un nuovo trojan Android BeatBanker e un malware generato da IA, Slopoly, utilizzato in attacchi ransomware.

Leak di dati sensibili

Segnalati leak di email italiane e violazioni di dati in servizi come Divine Skins, aumentando il rischio di attacchi mirati.

Patch urgenti necessarie

Microsoft e Veeam hanno rilasciato patch critiche per vulnerabilità RCE, rendendo fondamentale l'aggiornamento tempestivo dei sistemi.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità critiche e delle minacce informatiche. Diverse aziende, tra cui Microsoft e Veeam, hanno rilasciato patch per affrontare vulnerabilità di grave entità, mentre attori malevoli hanno intensificato le loro attività, sfruttando falle nei sistemi di sicurezza.

- **Vulnerabilità critiche in SolarWinds e Ivanti:** Emerse vulnerabilità critiche con impatti significativi sui settori energetico e manifatturiero. Discussioni sui forum underground evidenziano l'urgenza di patchare questi sistemi.
- **Patch di sicurezza Veeam:** Veeam ha rilasciato una patch per vulnerabilità RCE nella piattaforma Backup & Replication, che potrebbero consentire attacchi gravi ai server di backup.
- **Aggiornamenti di sicurezza Microsoft:** Patch Tuesday di marzo ha corretto 84 vulnerabilità, tra cui due zero-day. Le organizzazioni devono aggiornare i sistemi per mitigare i rischi.
- **Attacchi ai cloud tramite vulnerabilità:** Google ha avvertito che gli hacker sfruttano vulnerabilità in software di terze parti per accedere agli ambienti cloud, riducendo il tempo di attacco da settimane a giorni.
- **Minacce ai dispositivi FortiGate:** Nuove campagne mirano a sfruttare i dispositivi FortiGate per compromettere reti e rubare credenziali di account di servizio.
- **Flaws in n8n workflow automation:** Scoperte vulnerabilità critiche in n8n che potrebbero portare a esecuzioni di codice arbitrario e esposizione di credenziali memorizzate.
- **Furti di credenziali tramite VPN fasulle:** Storm-2561 distribuisce client VPN falsi per rubare credenziali aziendali.
- **Vulnerabilità in Chrome:** Google ha rilasciato aggiornamenti di emergenza per due vulnerabilità attivamente sfruttate in Chrome.

La settimana ha evidenziato la continua evoluzione delle minacce informatiche e l'importanza di mantenere aggiornati i sistemi di sicurezza.

Hacker filo-iraniani prendono di mira gli USA: il cyber fronte della guerra

AP News – 12 marzo 2026

Con l'escalation del conflitto Iran-USA iniziato il 28 febbraio 2026, gli hacker filo-iraniani hanno intensificato le operazioni cyber contro obiettivi statunitensi e mediorientali. Il gruppo Handala ha rivendicato un attacco significativo a Stryker, azienda americana di dispositivi medici con sede in Michigan, in risposta ai presunti attacchi USA che hanno causato vittime civili iraniane.

Attacco a Stryker (USA)

Il gruppo Handala ha compromesso i sistemi globali di Stryker, azienda di tecnologia medica. L'obiettivo: distruzione dei dati, non estorsione finanziaria.

Infrastrutture critiche nel mirino

Datacenter regionali, impianti industriali in Israele, una scuola in Arabia Saudita, un aeroporto in Kuwait e telecamere di sorveglianza in Medio Oriente per migliorare il targeting missilistico iraniano.

Russia e Cina: rischio escalation

CrowdStrike ha rilevato un'impennata di attività di hacker russi a supporto di Teheran. Il gruppo Z-Pentest ha rivendicato la compromissione di reti USA, inclusi sistemi CCTV. La Cina mantiene per ora un approccio cauto.

Polonia: attacco a struttura nucleare

Le autorità polacche indagano su un cyberattacco a un impianto di ricerca nucleare con possibili legami all'Iran, sebbene non si escluda che un altro gruppo stia usando il conflitto come copertura.

Obiettivi prioritari identificati

- Appaltatori della difesa USA e vendor governativi
- Aziende che collaborano con Israele
- Infrastrutture critiche: ospedali, porti, impianti idrici, centrali elettriche, ferrovie
- Sistemi con scarsa igiene informatica (patch mancanti, account obsoleti)

Patch immediata dei sistemi, aggiornamento firewall e soluzioni di sicurezza, rimozione account obsoleti. «All the cyber hygiene that you should be doing, it's more critical now than ever.» — Shaun Williams, ex FBI/CIA, SentinelOne

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama dei data leak ha mostrato un'attività intensa, con numerosi incidenti che coinvolgono organizzazioni italiane ed europee. Le informazioni trapelate includono credenziali di accesso, dati personali e dettagli sensibili.

1.4K

Email italiane di alta qualità

Leak di email italiane pubblicate su diversi forum, utilizzabili per attacchi mirati.

105,814

Account Divine Skins compromessi

Violazione del servizio skin per League of Legends con accesso a email, username e cronologia acquisti.

1.2M

Account Baydöner esposti

La catena di ristoranti turca ha subito una violazione con nomi, numeri di telefono e password in chiaro.

49.08MB

Dati italiani in leak

Dati italiani pubblicati su un forum di hacking, rappresentando un rischio per la privacy degli utenti.

In aggiunta, è stato segnalato un breach presso **Starbucks**, dove si è verificato un accesso non autorizzato agli account *Partner Central* di centinaia di dipendenti. La settimana 08/03/2026 – 15/03/2026 ha evidenziato un aumento preoccupante delle violazioni, sottolineando l'importanza di rafforzare le misure di protezione dei dati.

Minacce per Settori Critici: Dettaglio Breach

Settore Gaming & Entertainment

Divine Skins ha subito una violazione con 105.814 account compromessi (email, username, cronologia acquisti). Il breach è stato comunicato tramite Discord.

Settore Ristorazione

Baydöner (catena turca) ha esposto oltre 1,2 milioni di account con nomi, numeri di telefono e password in chiaro. Dati finanziari non compromessi.

Settore Corporate

Starbucks ha rivelato una violazione che ha colpito centinaia di dipendenti con accesso non autorizzato agli account Partner Central, evidenziando la vulnerabilità delle credenziali aziendali.

Dark Web & Monitoraggio

Nel 2025 registrati oltre 6.000 incidenti di violazione a livello globale. Lanciato Betterleaks, scanner open-source per identificare segreti validi in repository git. Leak di 49.08MB di dati italiani su forum di hacking.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un'intensificazione delle attività malevole, con diverse operazioni di law enforcement che hanno portato alla disattivazione di reti di proxy e botnet. Emergono nuove tecniche di attacco con focus su furto di credenziali e dati sensibili.

Principali Incidenti e Minacce

1. **Disruptione della rete SocksEscort:** Autorità statunitensi ed Europol hanno smantellato la rete di proxy SocksEscort, che sfruttava migliaia di router residenziali infettati per nascondere l'identità degli attaccanti.
2. **Malware nei giochi Steam:** L'FBI ha avviato un'indagine su otto giochi malevoli pubblicati su Steam contenenti malware. Gli utenti sono stati invitati a segnalare installazioni sospette.
3. **Nuovo trojan Android BeatBanker:** Si presenta come app governativa o Starlink, infetta i dispositivi e ruba dati bancari. Diffuso principalmente in Brasile.
4. **Tecnica "Zombie ZIP":** Nuova tecnica che consente ai malware di eludere i sistemi di sicurezza nascondendo payload in file ZIP appositamente creati.

Nuovi Malware Identificati

BlackSanta EDR killer

Malware russo mirato ai dipartimenti HR, progettato per disabilitare soluzioni di rilevamento delle minacce.

VENON

Malware bancario in Rust mirato a 33 banche brasiliane, segna un cambiamento rispetto ai malware precedenti del crimine latinoamericano.

ClipXDaemon

Hijacker di criptovalute su Linux che manipola gli indirizzi copiati dagli utenti.

Malicious npm Package

Pacchetto npm malevolo mascherato da installer di OpenClaw, distribuisce un RAT e ruba credenziali da macOS.

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 & Social Engineering

Negli ultimi sette giorni, il CERT-AGID ha segnalato un totale di 103 campagne di phishing, di cui 70 mirate a obiettivi italiani. Si evidenziano attacchi mirati a sottrarre dati personali attraverso truffe legate a servizi pubblici e finanziari.

01

Phishing PagoPA

Con 32 campagne registrate, il phishing legato a multe e pagamenti pubblici ha raggiunto un picco settimanale, colpendo dati bancari e personali degli utenti italiani.

02

Phishing EasyPark

Attacco che sfrutta il marchio EasyPark per richiedere aggiornamenti dei metodi di pagamento, mettendo a rischio dati finanziari e personali.

03

Impersonificazione di funzionari pubblici

Criminali impersonano funzionari di città per rubare pagamenti di permessi di pianificazione e zonizzazione. Metodo replicabile in Europa.

04

Phishing tramite Microsoft Teams

Attacchi mirati a dipendenti di organizzazioni finanziarie e sanitarie per ottenere accesso remoto e installare malware.

05

Nuove tecniche OAuth

Nuovo vettore di attacco sfrutta il codice dispositivo OAuth per rubare token di accesso a Microsoft 365.

06

Attacchi ai browser AI

Ricercatori dimostrano come i browser AI possano essere ingannati in meno di quattro minuti per eseguire attacchi di phishing.

07

VioletRAT in Italia

Campione di malware distribuito in Italia analizzato, rivela servizi Malware-as-a-Service per attacchi informatici a pagamento.

Tecniche Avanzate Emergenti

- Sfruttamento di token OAuth per accesso Microsoft 365
- Manipolazione dei browser basati su AI
- Distribuzione Malware-as-a-Service (VioletRAT)
- Social Engineering via impersonificazione di enti

Target Principali Italiani

- Utenti di servizi di pagamento (PagoPA)
- Clienti EasyPark
- Personale di enti pubblici e municipali
- Settori finanziario e sanitario (Teams)

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama dei ransomware ha visto un incremento significativo delle attività, con diverse organizzazioni colpite e nuove tecniche emergenti. Le gang sfruttano vulnerabilità e utilizzano malware generato da intelligenza artificiale.

Attacchi LockBit in Italia

Il gruppo LockBit ha rivendiato attacchi a diverse aziende italiane, tra cui bassignanicave.it, barberopietro.it e giunti.it, evidenziando la vulnerabilità delle organizzazioni locali.

Malware AI Slopoly

Identificato un nuovo malware presumibilmente generato da IA, utilizzato in attacchi ransomware, consentendo agli attaccanti di rimanere attivi su server compromessi per periodi prolungati.

Inchiesta su England Hockey

Il gruppo AiLock ha elencato England Hockey come vittima sul proprio sito di leak, avviando un'indagine su una potenziale violazione dei dati

Attacchi INC nel Pacifico

Le autorità hanno avvertito di un aumento degli attacchi ransomware INC che prendono di mira le reti in Australia e Nuova Zelanda.

Operazione contro SocksEscort

Un'operazione internazionale ha portato alla chiusura di SocksEscort, botnet che facilitava attacchi ransomware e DDoS.

Nuove vittime

Gruppi come Coinbase Cartel ed Everest hanno rivendicato attacchi a Augenomics e Executive Aviation, segnalando un aumento delle operazioni di estorsione.

Accuse contro negoziatori

Il DOJ USA ha accusato un ex dipendente di DigitalMint di collaborare con BlackCat per negoziare riscatti più elevati.

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto oltre 1.100 segnalazioni IT e 18 difetti critici nei sistemi ICS. Le organizzazioni sono state avvisate di vulnerabilità critiche in prodotti ampiamente utilizzati, con scadenze di patch accelerate.

1	**CVE-2026-3915 – Google Chrome** Vulnerabilità di overflow del buffer che consente esecuzione di codice arbitrario da remoto. Aggiornare Chrome alla versione 146.0.7680.71 o superiore. (CISA)
2	**CVE-2025-26399 – SolarWinds Web Help Desk** CISA ha fissato scadenza al 16 marzo per patchare questa vulnerabilità critica che potrebbe compromettere gravemente la sicurezza delle reti governative e aziendali. (Over Security)
3	**CVE-2026-1603 – Ivanti Endpoint Manager** Sfruttamento attivo segnalato. Le organizzazioni sono esortate a implementare aggiornamenti di sicurezza tempestivi. (CSIRT Italia)
4	**CVE-2026-27944 – Nginx UI** Consente agli attaccanti di scaricare backup di server e dati sensibili. Applicare le patch disponibili. (Over Security)
5	**CVE-2016-20024/20026 – ZKTeco** Vulnerabilità critiche che consentono escalation dei privilegi e RCE nei prodotti ZKTeco. (CVE Monitor)
6	**n8n Zero-Click** Vulnerabilità critica zero-click in n8n che consente compromissioni complete del server senza autenticazione. Inclusa nel catalogo CISA KEV. (Cyberthint)
7	**Microsoft Patch Tuesday** Rilasciati aggiornamenti per 83 vulnerabilità, di cui due con Proof of Concept disponibili. (CSIRT Italia)
8	**CVE-2025-66249 – Apache Livy** Vulnerabilità di path traversal che potrebbe consentire accesso a directory non autorizzate. (Latest CVE 0day exploit)

Vulnerabilità Aggiuntive e Patch

CVE-2026-3915 – Google Chrome

Overflow del buffer con esecuzione di codice remoto. Aggiornare alla versione 146.0.7680.71+. Miliardi di utenti invitati ad aggiornare il browser.

CVE-2026-27944 – Nginx UI

Permette download di backup server e dati sensibili. Patch disponibile da applicare immediatamente.

CVE-2025-26399 – SolarWinds

Vulnerabilità critica nel Web Help Desk con scadenza patch al 16 marzo fissata da CISA. Impatto su reti governative e aziendali.

CVE-2016-20024/20026 – ZKTeco

Escalation dei privilegi e RCE nei sistemi di controllo accessi ZKTeco. Aggiornamento sistemi necessario.

CVE-2026-1603 – Ivanti EPMM

Sfruttamento attivo confermato da CSIRT Italia. Aggiornamenti di sicurezza urgenti richiesti per Ivanti Endpoint Manager.

CVE-2025-66249 – Apache Livy

Path traversal che consente accesso a directory non autorizzate nel framework Apache Livy.

n8n Zero-Click RCE

Compromissione completa del server senza autenticazione. Inclusa nel catalogo CISA KEV. Patch immediata necessaria.

Microsoft Patch Tuesday Marzo

83 vulnerabilità corrette, 2 con PoC pubblico disponibile. Aggiornamento urgente per tutti i sistemi Windows.

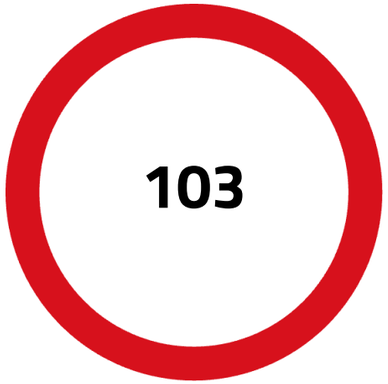
La settimana ha evidenziato un numero significativo di vulnerabilità critiche e PoC pubblici, sottolineando l'importanza di un approccio proattivo alla sicurezza informatica. Le organizzazioni devono aggiornare tempestivamente i propri software e monitorare costantemente le nuove segnalazioni di vulnerabilità.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un aumento allarmante delle vulnerabilità critiche e delle minacce informatiche, con un incremento delle attività malevole che colpiscono sia le infrastrutture IT che i dati sensibili delle organizzazioni. Le vulnerabilità in prodotti ampiamente utilizzati, come SolarWinds e Google Chrome, hanno sollecitato un'urgente necessità di patch, mentre le campagne di phishing e ransomware hanno evidenziato l'evoluzione delle tecniche di attacco, rendendo le organizzazioni italiane ed europee particolarmente vulnerabili.

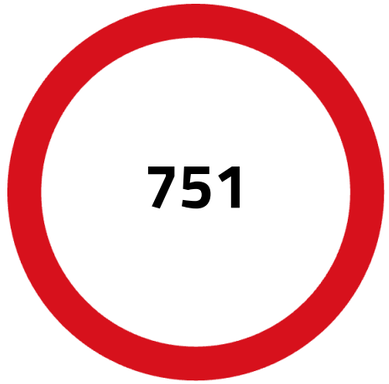
L'emergere di malware sofisticati come BeatBanker e Slopoly (generato da IA) e l'intensificazione delle violazioni di dati, con un numero crescente di credenziali esposte, suggeriscono che il fattore umano continua a rappresentare una vulnerabilità critica. Il CERT-AGID ha registrato 103 campagne di phishing settimanali, di cui 70 mirate all'Italia, con un picco di 32 campagne PagoPA. Rispetto alle settimane precedenti, si osserva una maggiore aggressività da parte degli attaccanti, che sfruttano le vulnerabilità in modo più mirato e tempestivo, aumentando il rischio per le aziende e le istituzioni.

Tendenze chiave: crescente uso dell'IA nella generazione di malware, sfruttamento accelerato delle vulnerabilità (da settimane a giorni), intensificazione degli attacchi alle piattaforme cloud e di comunicazione aziendale (Teams, OAuth), e aumento delle operazioni di law enforcement contro botnet e reti proxy.



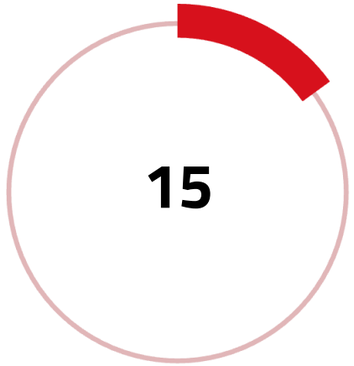
Campagne Malevole

Identificate dal CERT-AGID nella settimana (08/03/2026 – 15/03/2026), di cui 70 dirette a obiettivi italiani



IoC Condivisi

Indicatori di compromissione forniti dal CERT-AGID alle organizzazioni accreditate



Avvisi ICS CISA

Avvisi emessi per sistemi di controllo industriale nei settori energia e produzione critica

Tendenze Emergenti

- Malware generati da IA (es. Slopoly)
- Phishing mirato (focus su PagoPA e settore pubblico)
- Sfruttamento accelerato delle vulnerabilità (zero-day e Patch Tuesday)
- Attacchi a piattaforme di collaborazione (Teams, OAuth)

Settori più Colpiti

- Sanità e Servizi Essenziali
- Settore bancario e finanziario
- Pubblica Amministrazione (servizi digitali)
- Infrastrutture critiche (energia, manifatturiero)

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino un approccio proattivo alla sicurezza informatica. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti.

Priorità immediate:

- Applicare immediatamente le patch critiche per CVE-2026-3915 (Chrome), CVE-2025-26399 (SolarWinds, scadenza 16 marzo), CVE-2026-1603 (Ivanti EPMM) e la vulnerabilità zero-click in n8n.
- Aggiornare tutti i sistemi Windows con le 83 patch del Patch Tuesday di marzo, con priorità alle 2 vulnerabilità con PoC pubblico.
- Verificare e aggiornare i sistemi Veeam Backup & Replication per mitigare le vulnerabilità RCE.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing (103 campagne settimanali, 70 italiane) e delle tecniche di social engineering.
- Implementare l'autenticazione a più fattori per proteggere le credenziali aziendali, in particolare per Microsoft 365 e piattaforme cloud.
- Monitorare attivamente il dark web per rilevare esposizioni di dati aziendali e credenziali.
- Verificare l'integrità dei pacchetti npm e delle librerie di terze parti per prevenire supply chain attacks.
- Proteggere i dispositivi FortiGate e monitorare le reti per attività anomale legate a campagne di credential theft.

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