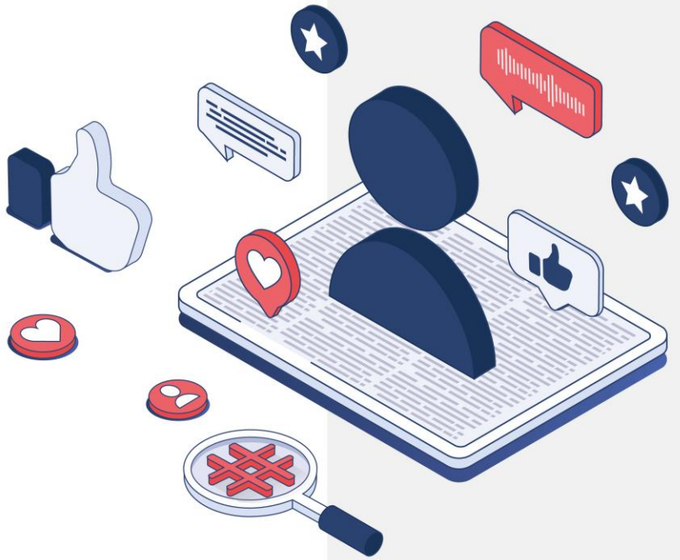
S3K

Cyber Threat

WEEKLY REPORT

\ week 02/03/2026 - 08/03/2026



www.s3kgroup.it

Sommario Settimanale CTI (01/03/2026 – 08/03/2026)

Aumento degli attacchi ransomware

Gruppi come Securotrop e Velvet Tempest hanno colpito settori critici come la sanità e la logistica, richiedendo maggiore vigilanza da parte delle organizzazioni italiane.

Vulnerabilità critiche in software diffusi

Segnalate vulnerabilità critiche in WordPress e dispositivi Qualcomm, evidenziando la necessità di aggiornamenti tempestivi per mitigare i rischi associati.

Campagne di phishing evolute

Nuove tecniche di phishing, tra cui l'abuso del dominio .arpa e campagne mirate ad eventi attuali, evidenziano l'adattamento dei criminali informatici.

- **Chiusura di forum di cybercriminalità**

  Le forze dell'ordine hanno smantellato il forum LeakBase. Le violazioni di LexisNexis e TriZetto continuano a rappresentare una minaccia significativa.

- **Attività malevole in aumento**

  Nuove varianti di malware come VioletRAT e tecniche di social engineering richiedono alle organizzazioni di rafforzare le proprie difese.

- **Implicazioni geopolitiche**

  Le tensioni tra Iran, USA e Israele hanno portato a un aumento delle attività di spionaggio informatico con potenziali spillover in Europa.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della cybersecurity ha visto un incremento significativo delle attività malevole, con un focus particolare su attacchi ransomware e campagne di spionaggio. Le organizzazioni in Italia e in Europa devono prestare attenzione a nuove vulnerabilità e exploit, oltre a monitorare le tensioni geopolitiche che potrebbero influenzare la sicurezza informatica.

Minacce e Attacchi Mirati

- Ransomware INC Ransom: avviso dell'agenzia australiana di cybersicurezza su minacce ad infrastrutture critiche globali
- Attacco ransomware a MAGNETA LOGISTICS in Lituania: vulnerabilità del settore logistico evidenziata
- Vulnerabilità in iOS sfruttate: CISA ha avvertito su tre falle usate in attacchi di spyware e furto di criptovalute
- Nuovi exploit per Erlang e altre piattaforme critiche aziendali segnalati

Spionaggio e Contesto Internazionale

- Conflitto cyber Iran-USA-Israele: attacchi informatici che accompagnano le ostilità nel Medio Oriente
- Campagna di spionaggio attribuita all'India contro agenzie governative di Pakistan, Bangladesh e Sri Lanka
- Celebrazione delle donne nella cybersecurity in occasione della Giornata Internazionale della Donna
- Crescente sofisticazione degli attacchi richiede attenzione costante e rafforzamento delle misure di sicurezza

Attenzione Geopolitica: Le tensioni nel Medio Oriente tra Iran, USA e Israele si sono intensificate con attacchi informatici. Le organizzazioni europee devono considerare il rischio di spillover di tali conflitti nel cyberspazio e prepararsi adeguatamente.

Data Leak & Breach: Scenario Settimanale

3.4M

Pazienti TriZetto

La violazione di TriZetto Provider Solutions ha esposto i dati sensibili di 3,4 milioni di pazienti nel settore sanitario

142K

Membri LeakBase

Il forum LeakBase, smantellato da forze dell'ordine statunitensi ed europee, contava 142.000 membri attivi

1M+

Email KomikoAI

KomikoAI ha subito una violazione che ha compromesso oltre 1 milione di indirizzi email e dati associati

496K

Email Lovora

L'app Lovora ha subito una violazione con esposizione di 496.000 indirizzi email degli utenti

La settimana ha evidenziato un aumento preoccupante delle violazioni di dati, con impatti significativi su utenti e aziende in Italia e in Europa. Oltre ai breach principali, sono state segnalate vendite di liste email italiane raccolte in batch, aumentando il rischio di frodi e furto d'identità per i cittadini italiani.

Minacce per Settori Critici: Dettaglio Breach

Settore Sanitario

TriZetto Provider Solutions ha subito una violazione che ha esposto i dati sensibili di 3,4 milioni di pazienti, evidenziando i gravi rischi nella gestione dei dati sanitari

Servizi Legali e Dati Aziendali

LexisNexis ha confermato una violazione con accesso non autorizzato ad informazioni di clienti e aziende, con potenziali ripercussioni per le organizzazioni che ne utilizzano i servizi

Piattaforme AI e Consumer App

KomikoAI ha compromesso oltre 1 milione di email, mentre Lovora (496K) e Quitbro (23K) evidenziano la vulnerabilità delle applicazioni di consumo

Liste Email Italiane in Vendita

Diverse fonti segnalano la vendita di liste email italiane in batch sui mercati sotterranei, rappresentando un rischio diretto per la privacy e la sicurezza degli utenti italiani

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un'intensificazione delle attività malevole, con nuove varianti di malware e tecniche di attacco innovative. Diverse campagne di malware, tra cui RAT e infostealer, sono emerse evidenziando la continua evoluzione delle minacce informatiche.

Nuovi Malware Identificati

1. **VioletRAT:** Malware pubblicizzato come prodotto commerciale in Italia, con capacità di controllo remoto e raccolta di informazioni. Approfondisci
2. **InstallFix Social Engineering:** Attaccanti usano false guide di installazione per indurre utenti ad eseguire comandi malevoli, sfruttando la fiducia nelle documentazioni online.
3. **Malware via GitHub:** Installer falsi di OpenClaw, promossi da Bing AI, portano all'installazione di malware di furto di informazioni.

Minacce Emergenti

Malware Android Mobile 2025

Statistiche rivelano minacce significative come backdoor preinstallate e trojan bancari, con aumento della sofisticazione degli attacchi mobile.

APT Cinese – Telecomunicazioni

Attore APT cinese ha preso di mira fornitori di telecomunicazioni in Sud America, compromettendo dispositivi Windows e Linux con potenziali implicazioni per reti europee.

RESURGE – Ivanti

La CISA ha avvertito che il malware RESURGE può rimanere dormiente su dispositivi Ivanti, rappresentando una minaccia persistente per le reti aziendali.

Il malware UAT-9244 ha introdotto **nuove varianti** aumentando il rischio per organizzazioni in settori critici incluse le telecomunicazioni. Un attacco malware ha anche compromesso i sistemi IT e le linee telefoniche della contea di Passaic nel New Jersey, dimostrando la vulnerabilità delle infrastrutture pubbliche.

Phishing & Social Engineering

01

Phishing a tema "Festa della Donna"

Campagne diffuse tramite WhatsApp mirate a rubare dati delle carte di credito in occasione della Festa della Donna, inducendo le vittime a condividere informazioni sensibili. 🔗 CSIRT Italia

02

Abuso del dominio .arpa

I criminali informatici sfruttano il dominio speciale ".arpa" e il DNS inverso IPv6 per eludere i controlli di reputazione dei domini, rendendo più difficile la rilevazione delle campagne. 🔗 Bleepingcomputer

03

Spear Phishing contro organizzazioni nazionali

Il CSIRT Italia ha segnalato attacchi di spear phishing mirati a caselle aziendali di enti pubblici, con gli attaccanti che sfruttano email compromesse per propagare le campagne. 🔗 CSIRT Italia

04

Abuso del protocollo OAuth

Nuove campagne di phishing sfruttano il protocollo OAuth per compromettere endpoint aziendali, con focus su organizzazioni governative e del settore pubblico. 🔗 Securityinfo

05

Disattivazione piattaforme phishing-as-a-service

Forze di polizia internazionali hanno smantellato una piattaforma phishing-as-a-service usata per attaccare ospedali e scuole, colpendo centinaia di migliaia di account globali. 🔗 Therecord

Tecniche Avanzate Emergenti

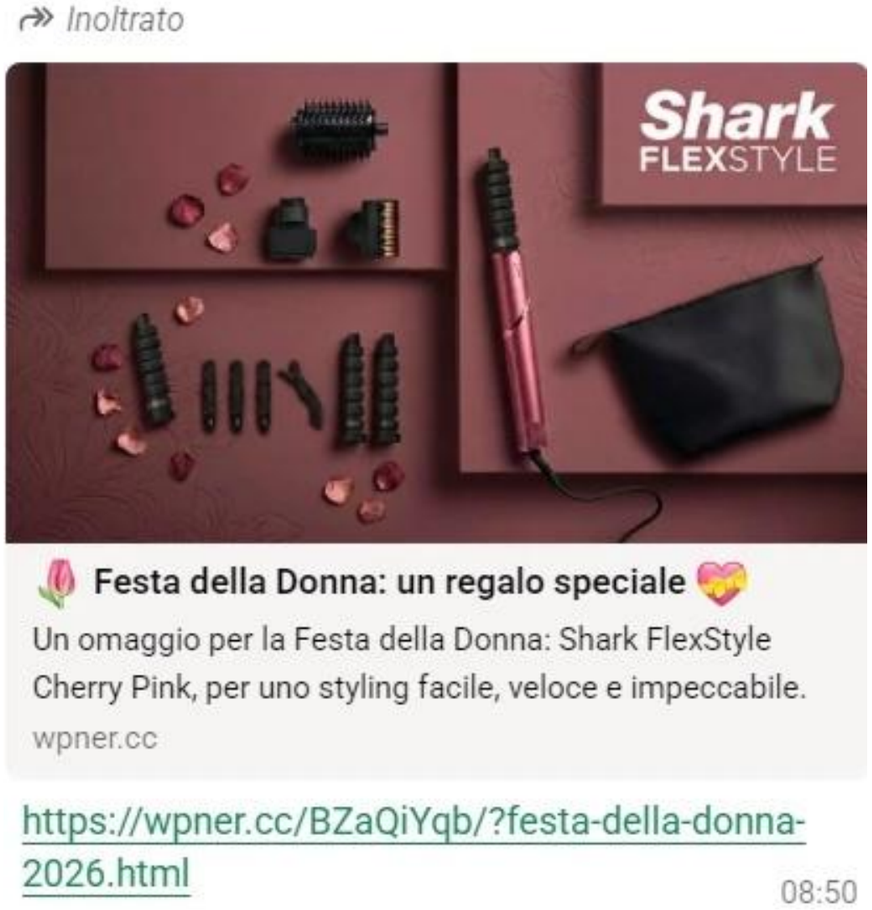
- Abuso del dominio .arpa per eludere controlli reputazione
- Credenziali cPanel compromesse vendute in bulk come infrastruttura phishing plug-and-play
- Phishing su Zoom e Google Meet tramite software legittimo per sorveglianza
- Sfruttamento di OAuth per compromissione endpoint aziendali

Rimborso UE e Responsabilità Bancaria

- L'Avvocato Generale UE ha suggerito rimborso immediato per vittime di transazioni non autorizzate
- Potenziale impatto significativo sulla responsabilità delle istituzioni finanziarie
- Enti pubblici italiani target di spear phishing continuativo
- Risorse per attacchi informatici vendute come servizio in forte crescita

Focus : Phishing a tema “Festa della Donna”

Come segnalato anche dal CSIRT Italia, in concomitanza dell’8 Marzo sono stati rilevati molti casi di mail di phishing aventi come riferimento nell’oggetto proprio questa ricorrenza.
La campagna, diffusa principalmente su WhatsAPP, pubblicizza un presunto kit omaggio rivolto ad un pubblico femminile, ottenibile tramite il versamento via carta di credito di una piccola somma. Per cercare di aumentare la credibilità di tale omaggio nella pagina in cui si indicava l’ottenimento del prodotto veniva riprodotta la grafica di una nota piattaforma di e-commerce. Inoltre la stessa pagina poneva come condizione necessaria per l’ottenimento di tale kit la condivisione di tale link tramite WhatApp.
Qui di fianco uno screenshot del messaggio malevolo (fonte CSIRT Italia), compresa la URL fraudolenta.



Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama dei ransomware ha mostrato un'attività intensa con diversi gruppi che hanno rivendicato violazioni significative in vari settori. Le istituzioni sanitarie e le aziende logistiche si confermano obiettivi privilegiati, con nuove tecniche di attacco che sfruttano strumenti legittimi.

Universal Mailing Service – Securotrop

Il gruppo Securotrop ha rivendicato la violazione di Universal Mailing Service, rubando 490 GB di dati con potenziali impatti sulla privacy e sulla reputazione dell'azienda. 🔗 Link alla notizia

University of Hawaii Cancer Center

Un attacco ransomware ha compromesso i dati di quasi 1,2 milioni di persone, evidenziando i rischi nella gestione di dati sensibili nel settore sanitario. 🔗 Link alla notizia

Velvet Tempest – ClickFix e CastleRAT

Il gruppo Velvet Tempest ha usato tecniche ClickFix per distribuire malware e backdoor, dimostrando l'uso di strumenti legittimi per attacchi complessi. 🔗 Link alla notizia

Play, Worldleaks e Nightspire – Nuove Vittime

Worldleaks ha colpito Sagent Pharmaceuticals, Nightspire ha attaccato MAGNETA Logistics, e Play ha rivendicato attacchi a Southern Concrete Construction e Facilities USA. 🔹 Dettagli

Sviluppi legali: Il leader del gruppo ransomware Phobos, arrestato in Corea del Sud, si è dichiarato colpevole di accuse di hacking. Un attacco brute force ha portato alla scoperta di un'infrastruttura ransomware-as-a-service geo-distribuita. Il University of Mississippi Medical Center ha ripreso le operazioni normali nove giorni dopo l'attacco. 🔗 Link alla notizia

Vulnerabilità Critiche & Patch

1	**CVE-2026-3701 – H3C Magic B1** Buffer overflow con punteggio di gravità 8.7 nel dispositivo H3C Magic B1. Gli attaccanti potrebbero sfruttare questa falla per compromettere il sistema. Dettagli
2	**Vulnerabilità critica in WordPress** Bug nel plugin User Registration & Membership, installato su oltre 60.000 siti, sfruttato per creare account amministrativi. Rischio significativo per le organizzazioni che usano questa piattaforma. Dettagli
3	**CVE-2026-21385 – Qualcomm** Vulnerabilità attivamente sfruttata su vari chipset Qualcomm, con potenziali impatti su esecuzione di codice arbitrario e denial of service. Dettagli
4	**CVE-2026-21902 – Juniper Networks** PoC disponibile per vulnerabilità critica nei prodotti Junos OS. Si raccomanda aggiornamento immediato per mitigare i rischi. Dettagli
5	**CVE-2026-27822 – RustFS Console** PoC identificato per vulnerabilità di esecuzione di codice arbitrario in RustFS Console che potrebbe esporre informazioni sensibili. Dettagli
6	**CVE-2026-30855 – WeKnora** Vulnerabilità critica che consente a utenti non autorizzati di modificare o eliminare dati di tenant in WeKnora. Corretta nella versione 0.3.2. Dettagli

Vulnerabilità Aggiuntive e Patch

Cisco – Aggiornamenti Critici

Cisco ha rilasciato aggiornamenti per risolvere vulnerabilità critiche e alte, inclusa esecuzione di codice remoto e escalation di privilegi. Implementazione urgente raccomandata. Dettagli

Android – Aggiornamento Marzo

Google ha corretto 129 vulnerabilità nel suo aggiornamento di marzo, inclusa una zero-day già attivamente sfruttata. Aggiornamento dei dispositivi Android prioritario. Dettagli

iOS – Tre Vulnerabilità CISA

CISA ha avvertito riguardo a tre vulnerabilità in iOS sfruttate in attacchi di cyber-spionaggio e furto di criptovalute. Aggiornamento immediato necessario.

Erlang – Exploit Critici

Segnalati exploit per vulnerabilità critiche in Erlang e altre piattaforme, aumentando il rischio per le applicazioni aziendali

CSIRT Italia – Avvisi Attivi

Il CSIRT Italia monitora attivamente le vulnerabilità segnalate e fornisce aggiornamenti tramite i propri canali ufficiali

Azione Immediata

Priorità assoluta: WordPress User Registration plugin, Qualcomm chipset, H3C Magic B1. Monitorare attivamente PoC pubblici per RustFS e Juniper.

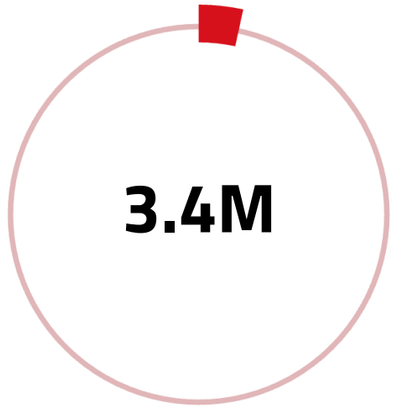
La settimana ha evidenziato un numero significativo di vulnerabilità critiche e PoC pubblici, sottolineando l'importanza di un approccio proattivo alla sicurezza informatica. Le organizzazioni devono aggiornare tempestivamente i propri software, con priorità per WordPress, Qualcomm e i dispositivi iOS, e monitorare le segnalazioni di nuove vulnerabilità attivamente sfruttate.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della cybersecurity ha mostrato un incremento preoccupante delle attività malevole, con un focus su attacchi ransomware, campagne di spionaggio e violazioni di dati. Rispetto alle settimane precedenti, si osserva un aumento delle operazioni di ransomware e un'evoluzione delle tecniche di phishing e social engineering. Le tensioni geopolitiche nel Medio Oriente aggiungono un ulteriore livello di rischio per le organizzazioni europee.

Dati Rubati

Sottratti da Universal Mailing Service dal gruppo ransomware Securotrop in un singolo attacco



Pazienti Esposti

Dati sensibili compromessi nella violazione di TriZetto Provider Solutions nel settore sanitario

Patch Android

Vulnerabilità corrette da Google nell'aggiornamento di marzo, inclusa una zero-day già sfruttata

Tendenze Emergenti

- Ransomware con tecniche ClickFix e strumenti legittimi (Velvet Tempest)
- Phishing adattivo che sfrutta eventi attuali (Festa della Donna)
- Abuso dominio .arpa per eludere controlli di reputazione
- Spionaggio informatico con spillover geopolitico in Europa

Settori più Colpiti

- Sanità: University of Hawaii Cancer Center (1,2M persone), TriZetto (3,4M pazienti)
- Logistica: MAGNETA LOGISTICS (attacco ransomware)
- Servizi legali e dati: LexisNexis (violazione confermata)
- Infrastrutture critiche: INC Ransom, dispositivi Qualcomm e iOS

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino misure proattive. Il contesto in continua evoluzione delle minacce informatiche richiede particolare attenzione. Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente il panorama delle minacce informatiche.

01

Patch Management Urgente

Implementare aggiornamenti immediati per WordPress User Registration plugin, dispositivi Qualcomm, Cisco e Android. Monitorare PoC pubblici per RustFS Console e Juniper Networks.

02

Formazione Anti-Phishing

Sensibilizzare il personale sulle campagne attive a tema Festa della Donna e spear phishing verso enti pubblici. Formare sulle tecniche di abuso del dominio .arpa e OAuth emergenti.

03

Monitoraggio Ransomware e Infrastrutture

Rafforzare piani di risposta con focus su sanità e logistica. Monitorare attività dei gruppi Securotrop, Velvet Tempest, Nightspire e Play. Attenzione alle tecniche ClickFix.

04

Protezione Dati e Privacy

Verificare l'esposizione di dati aziendali a seguito delle violazioni di LexisNexis e TriZetto. Monitorare la circolazione di liste email italiane nei mercati sotterranei.

05

Collaborazione con CSIRT Italia e ACN

Coordinare con CSIRT Italia per ricevere aggiornamenti sulle campagne di spear phishing contro organizzazioni nazionali e sugli avvisi relativi a vulnerabilità attivamente sfruttate.

Framework di Implementazione

1

Valutazione Rischio

Mappatura superfici di attacco con focus su WordPress, Qualcomm, Cisco e iOS. Identificare asset esposti a vulnerabilità attivamente sfruttate e potenziali impatti geopolitici.

2

Prioritizzazione

Focus su vulnerabilità con sfruttamento attivo confermato. Protezione contro ransomware di gruppi Securotrop, Velvet Tempest e Play. Attenzione a campagne phishing su enti pubblici e Festa della Donna.

3

Implementazione

Roll-out patch urgenti per WordPress, Android, Cisco e iOS. Distribuire IoC da CSIRT Italia. Formazione su phishing .arpa, abuso OAuth e tecniche ClickFix di Velvet Tempest.

4

Verifica

Testing efficacia difese contro VioletRAT e malware mobile. Verifica resilienza contro tecniche InstallFix social engineering e varianti APT cinesi nelle telecomunicazioni.

5

Miglioramento Continuo

Revisione basata su intelligence aggiornata e lesson learned da breach TriZetto, LexisNexis e KomikoAI. Monitoraggio evoluzione delle implicazioni geopolitiche Iran-USA-Israele nel cyberspazio.

Coordinamento Nazionale: Per minacce che coinvolgono infrastrutture italiane critiche o dati di cittadini (campagne spear phishing, liste email italiane in vendita, vulnerabilità iOS e Android), coordinare risposta con CSIRT Italia e ACN per massimizzare l'efficacia delle contromisure e la condivisione di intelligence.

01/03 – 08/03

Periodo di Copertura
Monitoraggio settimanale delle minacce CTI

7

Giorni Copertura
Monitoraggio continuativo minacce

24/7

Sorveglianza
Monitoraggio indicatori di compromissione

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