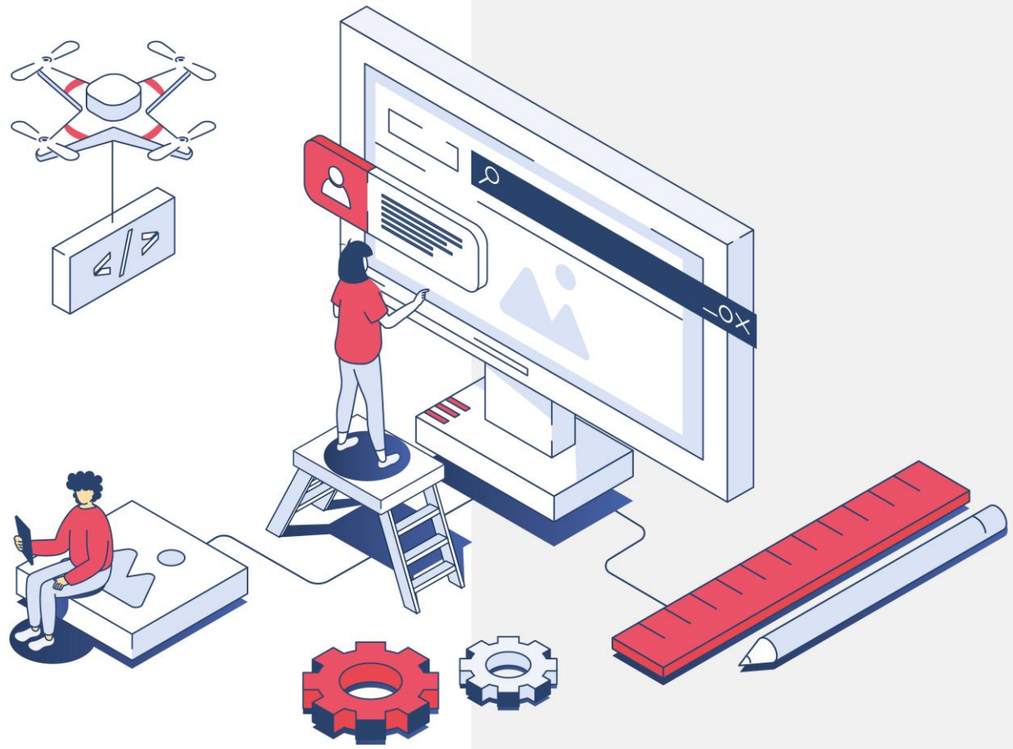
S3K

Cyber Threat

# WEEKLY REPORT

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



www.s3kgroup.it

### Aumento degli attacchi alle infrastrutture italiane

Attacchi mirati, inclusi DDoS e ransomware, hanno colpito istituzioni e infrastrutture critiche in Italia, evidenziando la necessità di misure di sicurezza rafforzate per le Olimpiadi 2026

### Vulnerabilità critiche in software diffusi

Vulnerabilità critiche in piattaforme come n8n e SmarterMail richiedono aggiornamenti urgenti per prevenire potenziali compromissioni

### Incremento dei leak di dati

Diverse fughe di email italiane e accessi non autorizzati a database hanno esposto informazioni sensibili, aumentando il rischio di phishing

- **Attività di phishing in crescita**

  96 campagne di phishing documentate, con focus su istituzioni italiane, utilizzando tecniche sofisticate per rubare dati sensibili

- **Malware su macOS e Linux**

  Nuove campagne di malware come GlassWorm e DKnife hanno colpito sistemi macOS e Linux, evidenziando vulnerabilità delle piattaforme

NEWS CYBER

# Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità e degli attacchi mirati, con un focus particolare sulle infrastrutture italiane e sugli eventi imminenti come le Olimpiadi invernali del 2026. Diverse organizzazioni e istituzioni sono state colpite, evidenziando la necessità di una vigilanza costante e di misure di sicurezza rafforzate.

## Vulnerabilità e Attacchi Critici

- Vulnerabilità critiche in n8n: controllo completo del server possibile
- 1.147 vulnerabilità tracciate, 128 con Proof of Concept
- Attacchi russi alle Olimpiadi invernali italiane
- Cyber attacco alla Galleria degli Uffizi

## Attacchi a Infrastrutture

- Progetto DDoSia di NoName057: controllo sistemi idrici italiani
- Attacchi DDoS ad ANAS e Comune di Parma
- Compromissione infrastruttura Notepad++
- Identità degli agenti AI: nuovo punto cieco nella sicurezza

**Focus Olimpiadi 2026:** Il Ministero degli Esteri italiano ha accusato hacker legati alla Russia di attacchi informatici contro uffici e strutture associate alle Olimpiadi invernali, sottolineando l'importanza della sicurezza informatica in vista dell'evento.

DATA BREACH

# Data Leak & Breach: Scenario Italiano

**2.2K**

### Email Italiane MegaCloud

Accesso a 2.200 email italiane tramite MegaCloud, suggerendo attacco mirato a dati sensibili

**14-18**

### Batch Email Pubblicate

Liste di email italiane pubblicate in batch da 14 a 18, compromettendo la privacy di migliaia di cittadini

**1.4M**

### Breach Betterment

Oltre 1.4 milioni di indirizzi email e dati personali esposti nella violazione della piattaforma di investimento

**96**

### Campagne Phishing

96 campagne di phishing documentate da CERT-AGID, 66 specificamente mirate a obiettivi italiani

La settimana ha evidenziato una crescente vulnerabilità delle informazioni personali e aziendali, con un numero allarmante di dati esposti. Sono state pubblicate diverse liste di email italiane e combo list da provider come Fastweb, Aruba e Libero. Le identità non umane (chiavi API e token) stanno diventando un fattore di rischio significativo nelle violazioni di dati in ambienti cloud.

# Minacce per Eventi e Settori Critici

### Olimpiadi Milano-Cortina 2026

Attacchi DDoS di NoName057 contro l'ecosistema digitale olimpico, colpendo enti locali e strutture ricettive. Necessarie misure di sicurezza rafforzate

### Patrimonio Culturale

Cyber attacco alla Galleria degli Uffizi evidenzia vulnerabilità del patrimonio culturale italiano. Necessarie misure di sicurezza più robuste

### Infrastrutture Pubbliche

NoName057 rivendica controllo di sistemi critici per approvvigionamento idrico. Attacchi DDoS a città italiane e ANAS causano interruzioni

### Piattaforme Software

Compromissione infrastruttura Notepad++ e vulnerabilità in n8n dimostrano rischi per piattaforme di distribuzione software

MALWARE

# Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un incremento significativo delle attività malevole, con attacchi mirati a diverse piattaforme e tecnologie. Le campagne di malware hanno colpito sia sistemi macOS che Linux, mentre le vulnerabilità delle catene di approvvigionamento continuano a rappresentare una minaccia crescente.

## Attacchi Multi-Piattaforma

1. **GlassWorm su macOS:** Malware che sfrutta estensioni compromesse di OpenVSX per rubare password e informazioni sui portafogli di criptovalute
2. **DKnife Toolkit Linux:** Attivo dal 2019, dirottamento traffico router e distribuzione malware in campagne di spionaggio
3. **MoltBot OpenClaw:** Oltre 230 pacchetti malevoli per assistente AI, furto di password tramite compromissione piattaforme di sviluppo

## Campagne Sofisticate

### DDoS Olimpiadi

NoName057 lancia campagna contro ecosistema digitale Milano-Cortina

### Supply Chain eScan

Compromissione infrastruttura antivirus trasformata in veicolo di infezione globale

### Espansione macOS

Malware informatico si espande oltre Windows colpendo macOS via ingegneria sociale

Microsoft ha avvertito che le campagne di malware informatico si stanno rapidamente espandendo oltre Windows, colpendo anche macOS attraverso tecniche di ingegneria sociale. Il toolkit DKnife evidenzia la vulnerabilità degli edge device e la necessità di proteggere le reti locali.

PHISHING

# Phishing & Social Engineering

01

### Phishing Agenzia delle Entrate

Campagna che sfrutta il nome dell'Agenzia delle Entrate per rubare credenziali bancarie tramite finto portale di login

02

### Smishing Autostrade

Messaggi che avvisano di pedaggi non saldati per indurre vittime a fornire dati personali o finanziari

03

### Phishing su Signal

Campagna che utilizza app di messaggistica Signal per rubare informazioni personali tramite procedure di verifica false

04

### Esaurimento spazio cloud

Campagna via email che mira a sottrarre dati carte di credito presentandosi come avviso di esaurimento spazio di archiviazione

05

### Campagna DEAD#VAX

Nuova campagna malware con tecniche avanzate per eludere rilevamento e installare trojan di accesso remoto

### Tecniche Avanzate

- Abuso piattaforme cloud Microsoft e Google
- Kit di phishing sofisticati per bypassare difese aziendali
- AI per email personalizzate e sofisticate
- Aumento truffe via SMS

### Statistiche CERT-AGID

- 96 campagne totali documentate
- 66 campagne mirate a obiettivi italiani
- MEF informato con IoC diramati
- Tecniche di ingegneria sociale in evoluzione

RANSOMWARE

# Operazioni Ransomware Active

Negli ultimi sette giorni, il panorama delle minacce ransomware ha visto un incremento significativo delle attività, con diversi attacchi mirati a organizzazioni in Europa e in particolare in Italia. Le vulnerabilità critiche in SmarterMail e VMware ESXi sono state sfruttate da gruppi di ransomware, evidenziando la necessità di una vigilanza costante.

### LockBit - Target Italia

Attacco rivendicato contro autoservizilocatelli.it con hash identificativo fornito per monitoraggio attività malevole

### Sapienza Università di Roma

Attacco ransomware compromette sistemi di una delle università più grandi d'Europa, causando interruzioni significative

### TheGentlemen - Attacchi Multipli

Attacchi rivendicati contro Silvi-SRL e KlearNowAI, utilizzando hash specifici per identificare le vittime

### BridgePay Interruption

Attacco causa interruzione significativa nei servizi di gateway di pagamento, con impatto potenziale su aziende europee

Un rapporto ha rivelato un aumento del 30% degli attacchi ransomware nel quarto trimestre del 2025. BabLock (Rorschach) condivide caratteristiche con LockBit, suggerendo evoluzione delle tecniche per eludere le difese.

VULNERABILITÀ

# Vulnerabilità Critiche & Patch

1

**CVE-2026-24423**

SmarterMail: Vulnerabilità RCE utilizzata in attacchi ransomware. CISA avverte aggiornamento sistemi urgente. CVSS 9.8

2

**CVE-2026-25052**

n8n: Utenti autenticati possono accedere a file sensibili. Corretta nelle versioni recenti, versioni precedenti a rischio

3

**VMware ESXi Critical**

CISA conferma gruppi ransomware sfruttano vulnerabilità critica precedentemente zero-day. Rischio infrastrutture virtuali

4

**CVE-2026-25763**

OpenProject: Difetto scrittura file arbitrari porta a esecuzione remota codice. Versioni pre-16.6.7 e 17.0.3 vulnerabili

5

**CVE-2026-1499**

WP Duplicate Plugin: Upload arbitrario file per mancanza autorizzazione. Versioni fino a 1.1.8 richiedono aggiornamento urgente

6

**CVE-2025-40551**

SolarWinds Web Help Desk: Vulnerabilità critica CVSS 9.8 attivamente sfruttata. CISA ordina patch immediate agenzie federali

# Vulnerabilità Aggiuntive e Patch

### CVE-2025-11953

React Native Metro: Exploit critico compromette sistemi di sviluppo, distribuendo payload per Windows e Linux

### CVE-2025-14740

Docker Desktop: Vulnerabilità assegnazione permessi errati portano a escalation privilegi. Verifica configurazioni urgente

### CVE-2026-2118

UTT HiPER 810: Vulnerabilità iniezione comandi identificata. CVSS 8.6 richiede attenzione immediata

### CVE-2026-2017

IP-COM W30AP: Overflow dello stack scoperto. CVSS 9.3 richiede aggiornamento firmware per mitigare rischio

### Tracciamento Cyble

1.147 vulnerabilità tracciate nella settimana, 128 con Proof of Concept disponibili richiedono attenzione immediata

### Azione Immediata

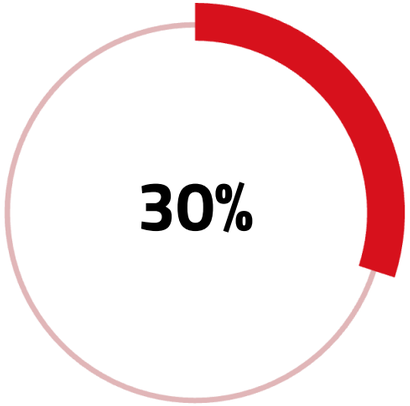
Mantenere aggiornati tutti sistemi, applicare patch tempestivamente, monitorare segnalazioni vulnerabilità attivamente

La settimana ha evidenziato vulnerabilità critiche che richiedono un'azione immediata da parte delle organizzazioni per proteggere i propri sistemi. Le vulnerabilità già attivamente sfruttate in attacchi necessitano priorità assoluta. È essenziale mantenere aggiornati i software e monitorare attivamente le segnalazioni di vulnerabilità per prevenire attacchi informatici.

ANALISI

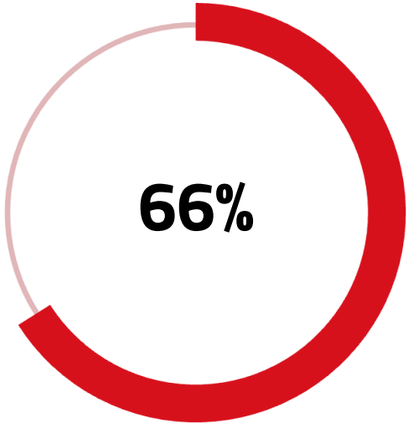
# Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento allarmante di attacchi e vulnerabilità, con focus particolare su infrastrutture critiche e dati sensibili. Le organizzazioni italiane ed europee sono state bersaglio di attacchi mirati, in particolare in vista delle Olimpiadi invernali del 2026. Le vulnerabilità critiche sono state attivamente sfruttate, evidenziando una crescente aggressività da parte dei gruppi di minaccia.



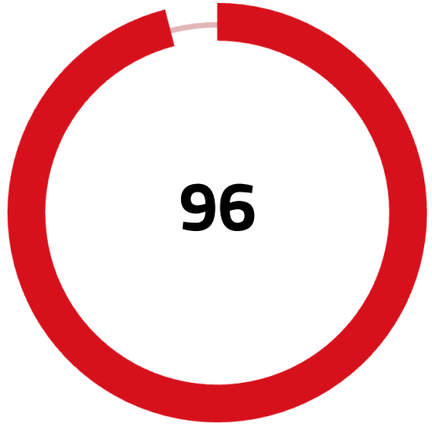

**Incremento Ransomware**

Aumento attacchi ransomware nel Q4 2025




**Phishing Italia**

Campagne phishing specificamente mirate a obiettivi italiani




**Campagne Totali**

Campagne phishing documentate da CERT-AGID

## Tendenze Emergenti

- Attacchi DDoS mirati alle Olimpiadi Milano-Cortina 2026
- Vulnerabilità supply chain (eScan, Notepad++)
- Espansione malware su macOS e Linux
- Identità non umane come fattore di rischio cloud

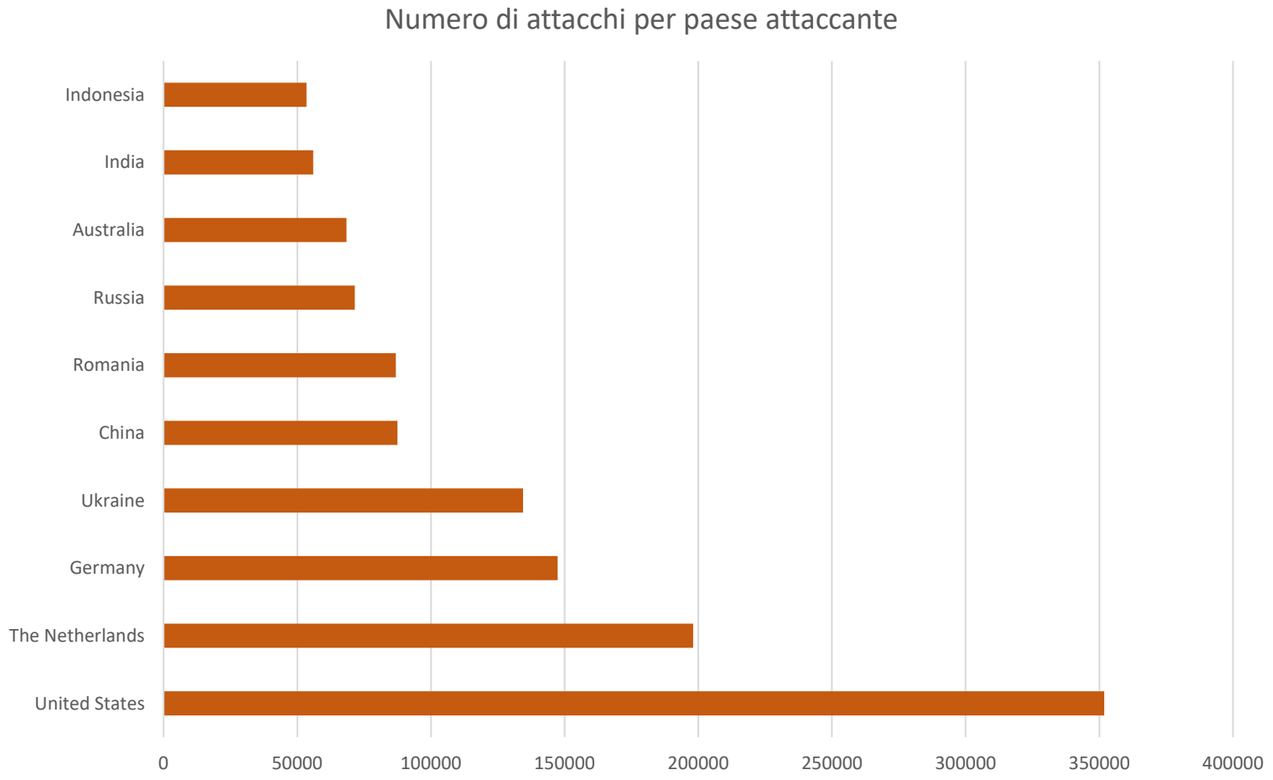
## Settori più Colpiti

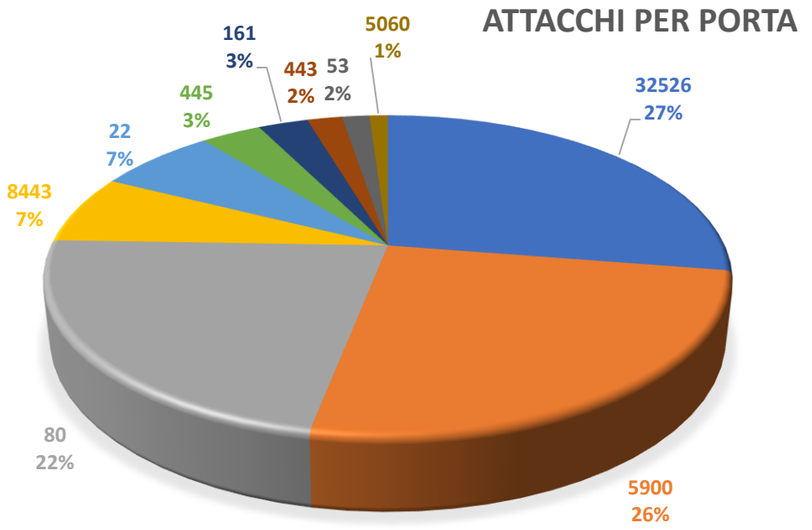
- Infrastrutture critiche: sistemi idrici e ANAS
- Patrimonio culturale: Galleria degli Uffizi
- Istruzione: Sapienza Università di Roma
- Eventi pubblici: ecosistema olimpico

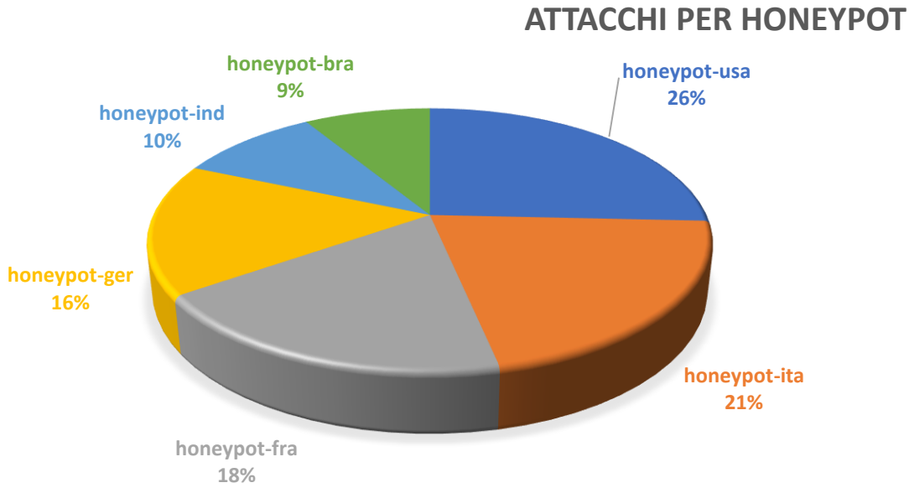
# Honeypot : una panoramica di quanto successo nella  settimana 2/2 – 8/02

ANALISI

# Honeypot : una panoramica di quanto successo nella  settimana 2/2 – 8/02



RACCOMANDAZIONI

# Raccomandazioni Operative Prioritarie

In questo scenario complesso, è fondamentale che le organizzazioni adottino un approccio proattivo e integrato alla sicurezza informatica. Il contesto delle imminenti Olimpiadi invernali del 2026 richiede particolare attenzione. Solo attraverso misure di sicurezza robuste sarà possibile affrontare le sfide attuali e proteggere le proprie infrastrutture e dati sensibili.

01

## Aggiornamento Sistemi

Mantenere aggiornati tutti i sistemi e applicazioni, applicando tempestivamente patch per vulnerabilità critiche in n8n, SmarterMail, VMware ESXi

02

## Formazione Dipendenti

Investire in programmi di formazione per sensibilizzare su rischi di phishing e social engineering, promuovendo cultura della sicurezza

03

## Monitoraggio Minacce

Implementare soluzioni di monitoraggio e rilevamento per identificare tempestivamente attività sospette e leak di dati

04

## Piano Risposta Incidenti

Creare piani di risposta agli incidenti ben definiti per garantire reazione rapida ed efficace in caso di attacco

05

## Protezione Eventi Olimpici

Rafforzare sicurezza per Olimpiadi 2026, coordinamento con CSIRT Italia per protezione da attacchi DDoS e phishing

# Company Profile S3K

**S3K Group (Security of the Third Millennium)** è un **Trusted & Secure Digital Transformation Partner,** che supporta le organizzazioni nel **ridurre i rischi**, **proteggere il valore digitale** e **guidare il cambiamento**.

- ❑ **Core Capabilities**
- ❑ **Cyber Security**
- ❑ **Data Science & Big Data**
- ❑ **Cloud & Application Dev**
- ❑ **Telco & Security Infrastructure**
- ❑ **PLM (Product Lifecycle Management)**
- ❑ **Modelling & Simulation**
- ❑ **Consulting & ERP**
- ❑ **Intellectual Properties e R&D**

**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.

**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