Contrastare le minacce evasive con
Optimum Security

Simone Mulattieri
Senior Presales Manager

kaspersky

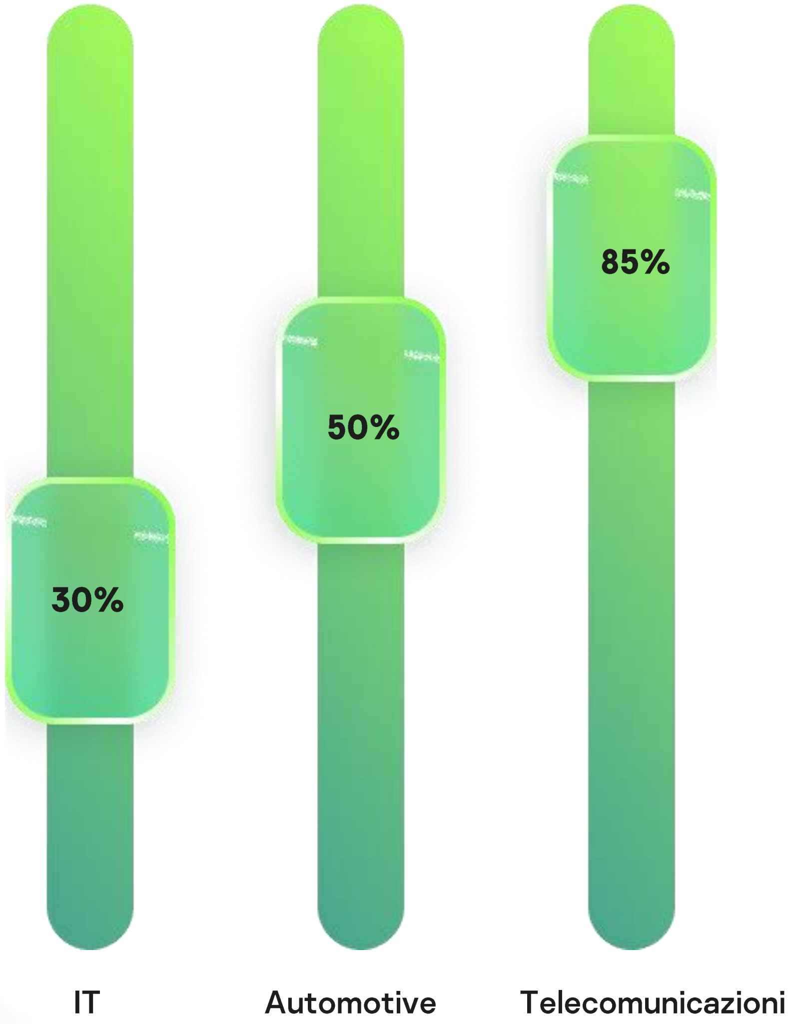
Quali minacce stiamo fronteggiando

Lo stato della cybersecurity nel 2023

kaspersky

Il Cybercrime è una grande business che coinvolge molte persone

Comparato con altri mercati



Il mercato del Cybercrime vale

$1,5T

[1] CSO Online
[2] Yahoo Finance

Ransomware: anche per chi paga il riscatto, non ci sono garanzie

Doppia estorsione

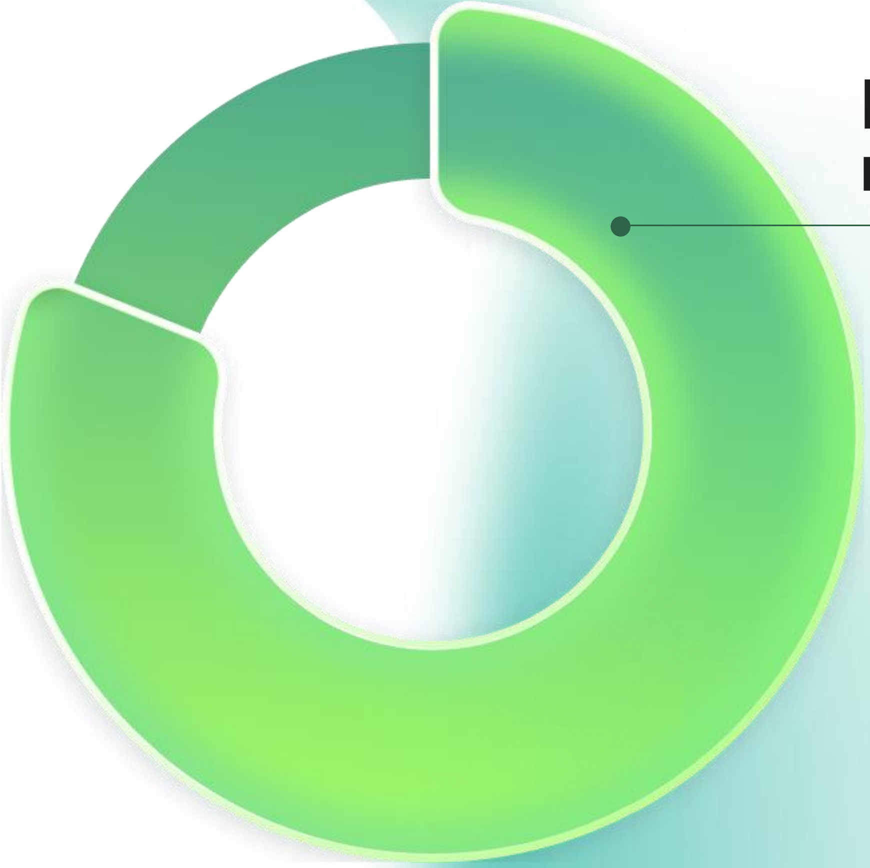
Furto dei dati prima della cifratura, richiesta di un secondo riscatto

20 giorni[2]

Il tempo medio di downtime dopo un attacco ransomware

Nessuna garanzia

Che i dati saranno decifrati e accessibili

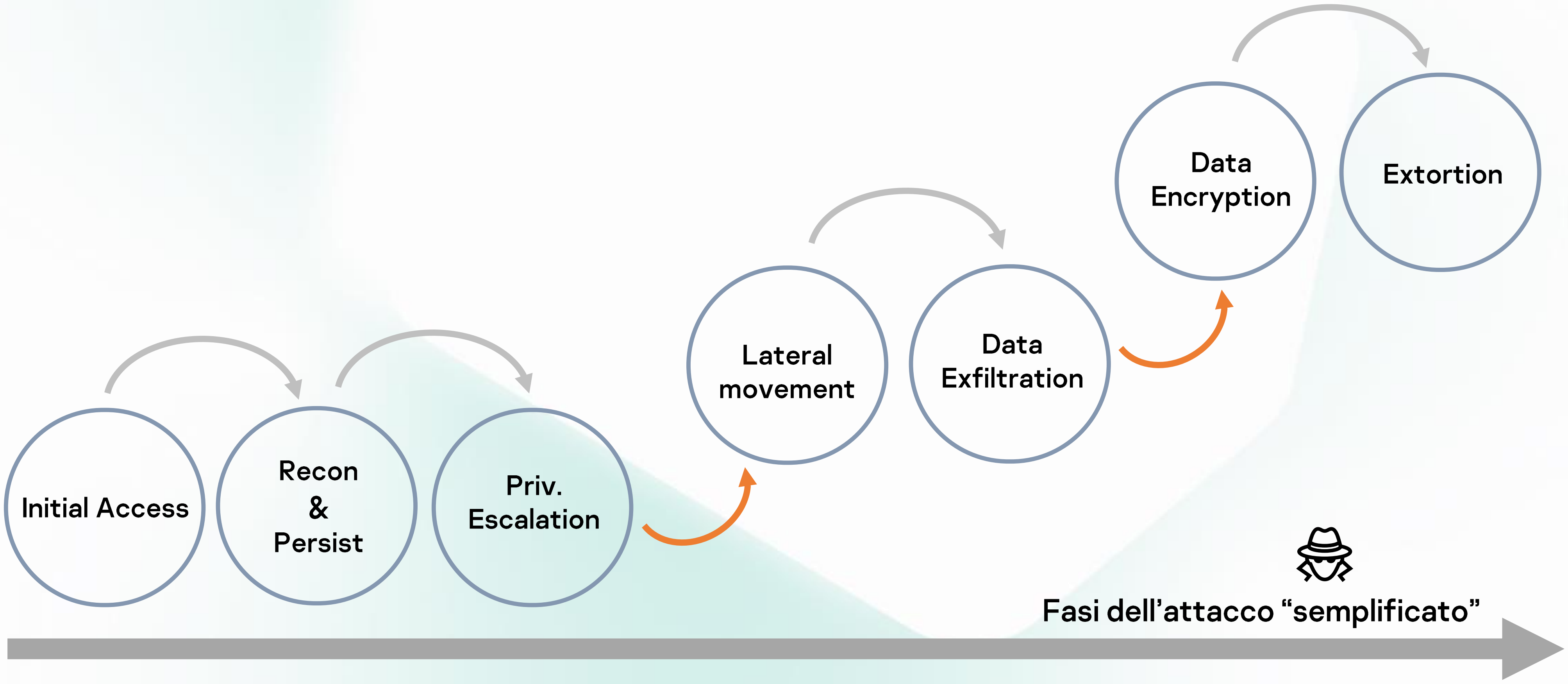


Il 79% paga il riscatto[1]

[1] Kaspersky
[2] Statista

Aumento degli attacchi complessi – statistiche & tipologia

- In media 287 giorni per identificare e mitigare un attacco *
- Crescita del 77% (YoY) degli attacchi complessi *
- L' 80% degli attacchi va a segno grazie a 0-day o malware sconosciuti *



** Gartner Security and Risk Management Summit 2022*

kaspersky

Come Kaspersky ti può aiutare?

kaspersky

Combattere le minacce evasive è possibile

Ridurre la superficie d’attacco

Controllo degli accessi web, dei dispositive e delle applicazioni usate per ridurre le vulnerabilità

Protezione automatica e guidata

Usare metodi multipli di analisi, includendo rilevamenti avanzati basati su Machine Learning e algoritmi di risposta automatizzati e guidati

Formazione

Migliorare la consapevolezza informatica dei dipendenti per ridurre gli errori

Detection avanzata e gestita

Diminuire il gap di competenze specifiche con la protezione gestita

Kaspersky Optimum Security

kaspersky

Ridurre la superficie d’attacco

kaspersky

Riduzione delle superfici di Attacco

System hardening

Controlli granulari per Applicazioni, risorse Web e Dispositivi in uso.

Adaptive Anomaly Control

Algoritmi di ML che adattano automaticamente la protezione sul sistema, in base al comportamento del singolo utente.

Vulnerability and patch management

Rilevamento delle vulnerabilità del Sistema Operativo e delle Applicazioni presenti sul device, catalogandole in base alla loro criticità.

Distribuzione automatizzata delle patch e degli aggiornamenti necessari.

kaspersky

Principali tecnologie di prevenzione

Exploit prevention

Rileva i software che sfruttano le vulnerabilità degli applicativi presenti sui device per svolgere attività dannose.

Remediation engine

Permette di ripristinare tutte le operazioni malevole effettuate dal malware sul SO.

Funzionalità molto efficace contro i ransomware.

Web e Mail protection

Protegge, in entrata e in uscita, i dati web e i messaggi e-mail alla ricerca di eventuali minacce e dall'esecuzione di script pericolosi.

File e Network protection

Motori avanzati di analisi euristica e di emulazione del malware, assieme a tecnologie di prevenzione real-time, aiutano a mantenere alta la difesa del device.

Protezione Automatica e Guidata

Detection & Response Automatica

Behavior detection

Gli algoritmi di ML proprietari rilevano attività malevole sconosciute attraverso il loro comportamento nelle primissime fasi di esecuzione.

Cloud reputation

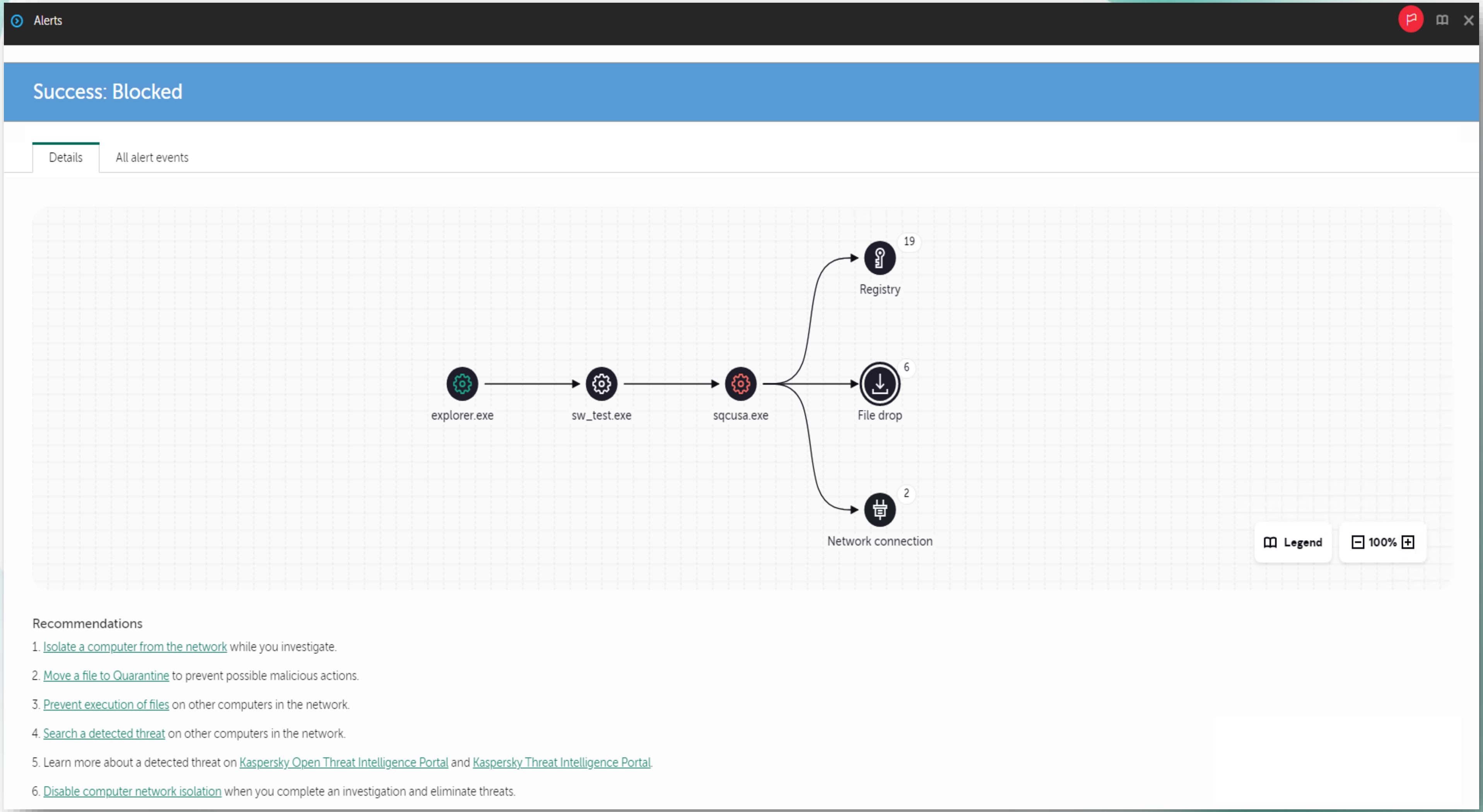
Threat Intelligence del vendor, aggiornata in tempo reale, che aiuta a combattere minacce e malware 0-day.

Cloud sandbox

I file sospetti vengono ulteriormente analizzati in cloud sandbox, attraverso tecnologie evolute di anti evasione, permettendo così di rilevare azioni malevole evolute.

kaspersky

Analisi della "root cause" & Response guidata



Response

- Device Isolation
- Prevent Execution
- Quarantine File
- Kill Process
- Start Process
- Get File
- Delete File
- IoC Scan
- Critical Area Scan

Detection avanzata e gestita

kaspersky

Kaspersky Managed Detection & Response

Proactive threat hunting

Gli esperti di Kaspersky SOC sono in grado di rilevare i più sofisticati attacchi mirati, tramite centinaia di regole di threat hunting frutto della nostra Threat Intelligence e dall'esperienza di oltre 25 nella cybersecurity.

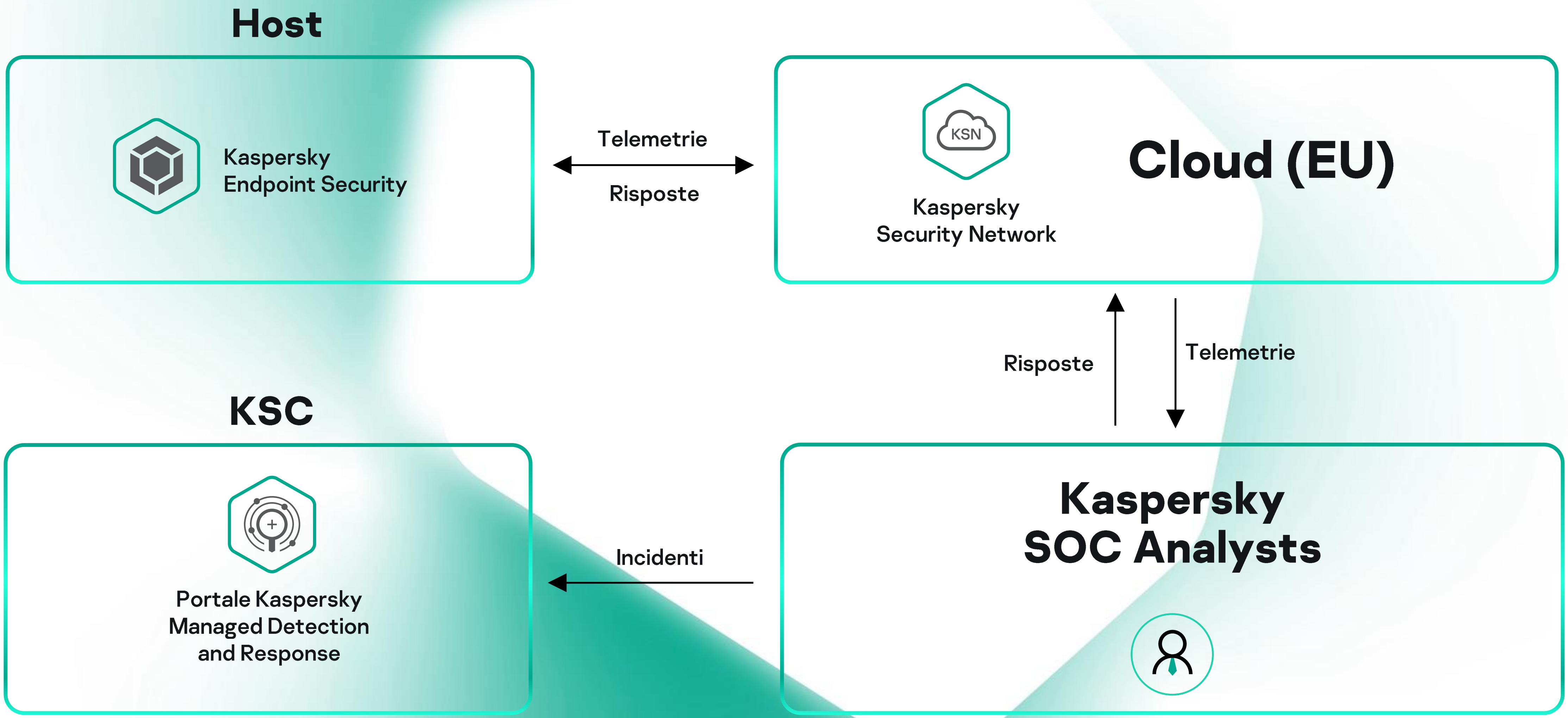
Efficienza

Gli esperti del SOC Kaspersky monitorano le telemetrie dell'infrastruttura dei vostri clienti 24x7. Analizzano anomalie e azioni sospette segnalando solo gli incidenti reali, limitando così i falsi positivi (qualificazione delle telemetrie).

Response & Remediation

Le segnalazioni inviate dal SOC sono affiancate a suggerimenti su come rispondere ai threat rilevati. Ove possibile è supportata anche la funzionalità di risposta automatica all'incidente.

Kaspersky MDR – Architettura



kaspersky

Formazione

kaspersky

Kaspersky Automated Security Awareness Platform (ASAP)

Uno strumento online di facile gestione che sviluppa livello per livello le competenze dei dipendenti in materia di cybersecurity. Piattaforma creato da esperti di cybersecurity leader del settore e sviluppata con concetti di **Multi-Tenancy**.

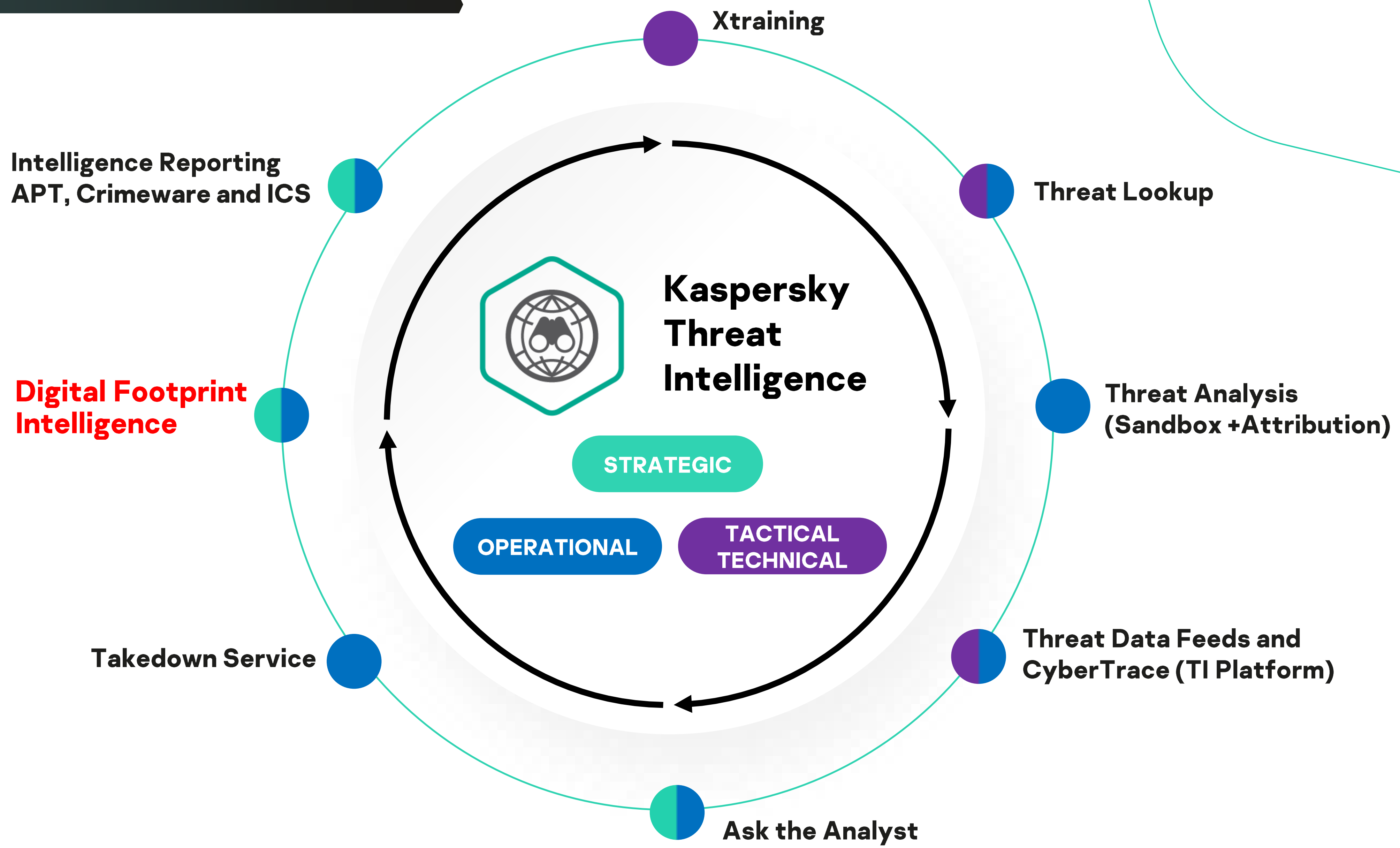
Corso principale
Formazione completa con argomenti suddivisi per livello di complessità

Corso rapido
Formazione audio-video breve ed estremamente coinvolgente

Simulatore di phishing
Assicurati che i dipendenti non siano vittime di attacchi di phishing

Threat Intelligence

kaspersky


Xtraining
Threat Lookup
Threat Analysis (Sandbox +Attribution)
Threat Data Feeds and CyberTrace (TI Platform)
Ask the Analyst
Takedown Service
Digital Footprint Intelligence
Intelligence Reporting APT, Crimeware and ICS
Kaspersky Threat Intelligence
STRATEGIC
OPERATIONAL
TACTICAL TECHNICAL

Grazie!

kaspersky