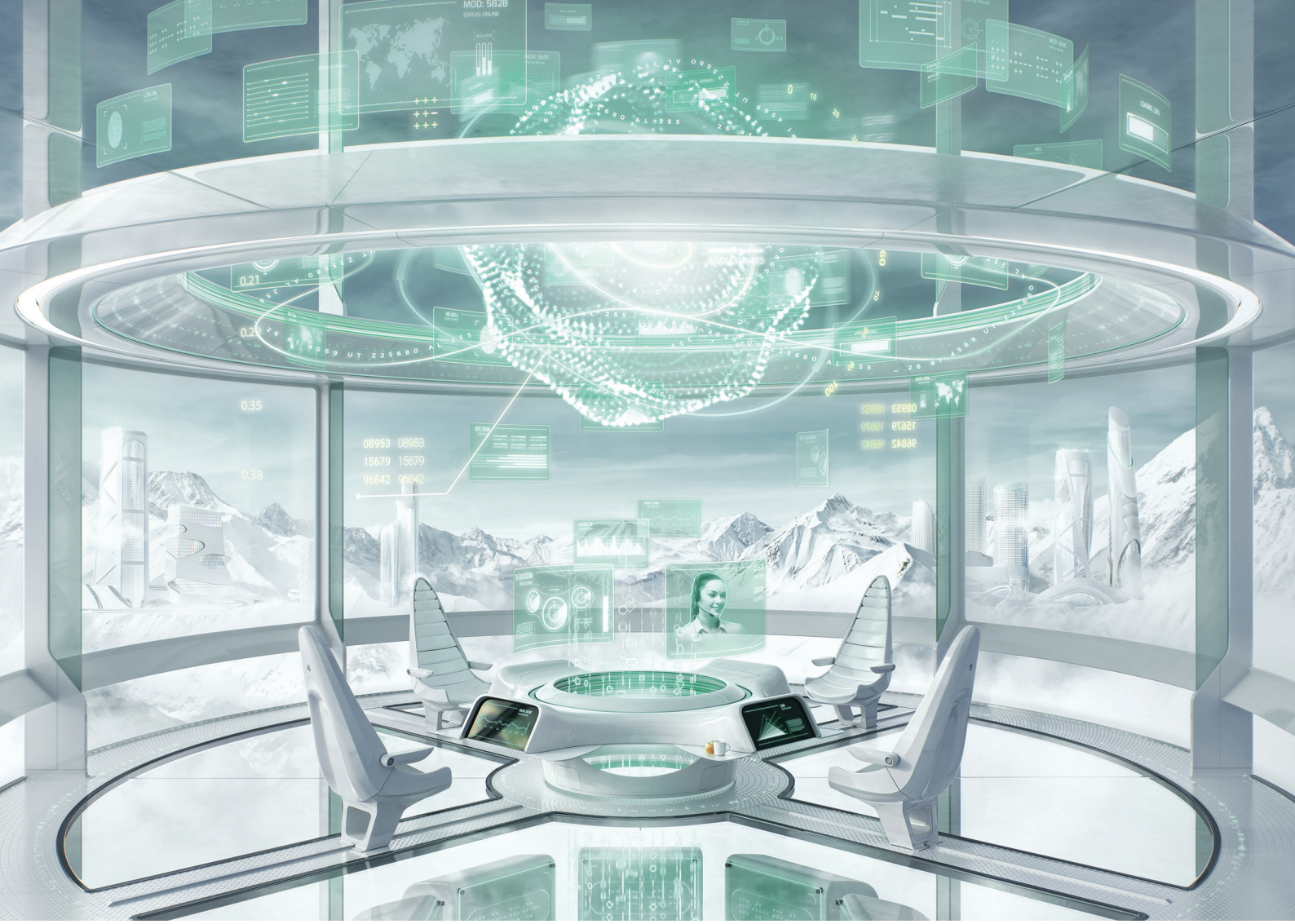


Efficienza e semplicità di gestione per le aziende di ogni dimensione

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky BRING ON THE FUTURE

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

Più dell'80% degli incidenti informatici è causato da errori umani, che si traducono a livello aziendale in milioni di euro spesi per ripristinare i sistemi interessati. Tuttavia, l'efficacia dei programmi di formazione tradizionali destinati a prevenire questi problemi è limitata e di solito non riesce a motivare il comportamento desiderato.

Errori umani come principale rischio informatico

$1.057.000
per azienda Enterprise
Impatto finanziario medio dei data breach causati dall'uso inappropriato delle risorse IT da parte dei dipendenti*

$98.000
per PMI
Impatto finanziario medio dei data breach causati dall'uso inappropriato delle risorse IT da parte dei dipendenti*

Il 52%
delle aziende
ritiene che le negligenze dei dipendenti rappresentino la principale minaccia per la Cybersecurity aziendale**

Il 30%
dei dipendenti
ammette di condividere con i colleghi dati di accesso e password utilizzati sul proprio PC durante l'attività lavorativa***

Il 23%
delle organizzazioni
non applica alcuna regola o criterio di Cybersecurity relativamente all'archiviazione dei dati aziendali***

Fattori da considerare per un approccio efficiente a un programma formativo di Security Awareness

Nonostante le aziende siano pronte a implementare i programmi di Security Awareness, non molte sono soddisfatte dei processi e risultati. Le piccole e medie imprese, invece, che di solito non hanno esperienza e risorse dedicate, sono particolarmente interessate.

Scarsa efficacia per gli utenti:

Percepito come un'attività faticosa, noiosa e di secondaria importanza.

Si tratta solo di cose da "non fare", anziché di istruzioni su "come fare" qualcosa

Le conoscenze acquisite non si conservano

Effort eccessivo per l'amministratore

Maggior carico amministrativo:

Come creare un programma e definire gli obiettivi?

Come gestire gli incarichi in termini di formazione?

Come controllare i progressi realizzati?

Come coinvolgere pienamente le persone nel programma formativo?

* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky, 2019

** Ricerca: "The cost of a data breach", Kaspersky, primavera 2018.

*** "Sorting out a Digital Clutter", Kaspersky, 2019.

Efficienza e semplicità di gestione del programma formativo per aziende di ogni dimensione

Kaspersky introduce la piattaforma Automated Security Awareness, che costituisce il focus principale del portfolio formativo Kaspersky Security Awareness.

La piattaforma è uno strumento online per la formazione dei dipendenti sulle tematiche relative alla sicurezza informatica nell'arco di un anno. Il processo di implementazione e gestione della piattaforma non richiede risorse e configurazioni specifiche ed è in grado di offrire all'organizzazione una guida integrata per ogni step del percorso verso una strategia aziendale improntata alla Cybersecurity.

Come valutare un programma di Security Awareness

Uno dei criteri più importanti nella scelta di un simile programma formativo è rappresentato dal grado di efficienza di quest'ultimo. Con ASAP, il concetto di efficienza è profondamente integrato nei contenuti e nelle modalità di gestione del programma. La piattaforma si basa su un modello formativo suddiviso in 350 micro-lezioni sulla Cybersecurity, pratiche ed essenziali: tutti i dipendenti dovrebbero acquisire queste competenze indispensabili. Senza di esse, per inesperienza o negligenza, i dipendenti possono involontariamente danneggiare l'azienda.

Massima efficienza della formazione

Completa e sistematica	– Contenuti ben strutturati – Moduli interattivi, costante rafforzamento, conduzione di test, attacchi di phishing simulati, per garantire l'applicazione delle competenze acquisite Il materiale formativo e la struttura dello stesso sono organizzati in modo tale da rispecchiare le specificità della memoria umana, la nostra capacità di assorbire e conservare le informazioni.
Pratica e coinvolgente	– Pertinente alle attività lavorative quotidiane dei dipendenti – Le competenze fornite si possono utilizzare immediatamente Gli esempi concreti, relativi a situazioni ed eventi reali in cui i dipendenti si riconoscono pienamente, contribuiscono al coinvolgimento dell'utente e aiutano al contempo a memorizzare le informazioni in modo efficace.
Approccio positivo	– Imprime una decisa spinta proattiva verso l'adozione di comportamenti sicuri – Spiega "perché" e "in che modo" agire, in maniera semplice Troppe regole e restrizioni possono causare malcontento, mentre spiegazioni e strategie di convincimento perfettamente allineate al modo in cui pensano le persone contribuiscono con naturalezza all'adozione e alla modifica di determinati comportamenti.

Facilità di gestione

Facile da gestire	La gestione dell'apprendimento completamente automatizzata permette a ogni dipendente di ottenere un livello di competenze appropriato ai rischi del proprio ruolo, senza alcun intervento da parte dell'amministratore della piattaforma.
Facile da controllare	Dashboard "all-in-one" e report pratici.
Semplici ed efficaci modalità di coinvolgimento	La piattaforma invia in automatico inviti ed e-mail motivazionali, così come i report settimanali per utenti e amministratori.

Gestione della piattaforma ASAP: semplicità attraverso la completa automazione

Avvio del programma in 4 semplici step

Upload utenti

Suddivisione degli utenti in base al profilo di rischio e impostazione del livello target di competenza per ciascun gruppo di dipendenti

Questo è l'unico step in cui l'amministratore deve prendere decisioni

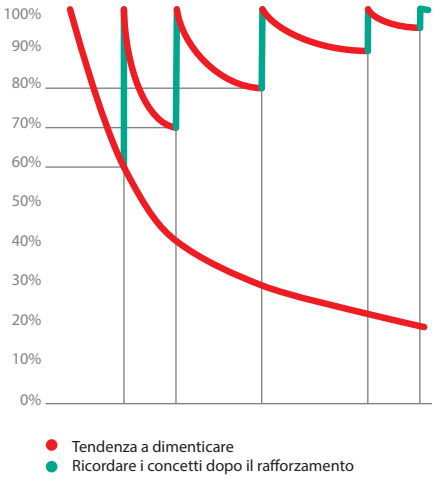
Avvio del programma di formazione

La piattaforma crea un programma formativo per ciascun gruppo, sulla base del ritmo di apprendimento e del livello target; fornisce inoltre report e suggerimenti pratici

Gestione automatizzata dell'apprendimento grazie ad ASAP

La Curva dell'oblio di Ebbinghaus

Rafforzamento ripetuto per la creazione efficiente di competenze.



Personalizzazione dell'apprendimento secondo le capacità individuali di ogni dipendente

- La piattaforma verifica automaticamente l'apprendimento e il superamento dei test sulle nozioni di base da parte dell'utente, prima di proseguire con il livello successivo
- I responsabili non devono perdere tempo con l'analisi dei progressi individuali e le configurazioni manuali

Benefit derivanti da percorsi di apprendimento specifici per ogni profilo professionale

Utilizzo di regole automatizzate per assegnare il livello di formazione finale desiderato ai singoli dipendenti. Il livello target è strettamente correlato al rischio rappresentato dallo specifico ruolo svolto dall'utente per l'azienda. Maggiore è il rischio, più elevato dovrebbe essere il livello di formazione finale. Ad esempio, utenti del reparto IT o contabilità tipicamente rappresentano un rischio più elevato rispetto a quello attribuibile agli altri dipendenti.

Massima flessibilità nell'apprendimento

- La formazione si svolge in maniera flessibile, pur conservando i tipici vantaggi di un prodotto che automatizza il processo di apprendimento
- Per ogni gruppo di utenti si possono selezionare:
  - Gli argomenti oggetto di apprendimento da parte degli utenti di ciascun gruppo (saltando quelli che saranno trattati in seguito).
  - Il livello target desiderato per gli utenti relativamente a ogni specifico argomento. I dipendenti non sprecheranno tempo di lavoro nell'apprendimento di argomenti non pertinenti al loro ruolo.

Possibilità di ottenere report pratici in qualsiasi momento

- Dashboard contenenti tutte le informazioni necessarie alla valutazione dei progressi
- Suggerimenti su come migliorare i risultati
- Download dei report dalla pagina principale con un semplice clic e configurazione della frequenza di ricezione dei report tramite e-mail

Metodologia di apprendimento in ASAP

Apprendimento incrementale continuo

- Dall'argomento più semplice a quello più complesso, modulo dopo modulo, livello per livello: aumento progressivo delle conoscenze
- Estensione e applicazione a nuovi contesti delle conoscenze precedentemente acquisite

Numerosi elementi formativi per lo sviluppo della consapevolezza

- Ogni livello comprende: modulo interattivo, rafforzamento, assessment (test e attacco di phishing simulato, ove applicabile)
- Tutti gli elementi formativi supportano la specifica competenza oggetto di apprendimento in ogni singola unità; in tal modo gli utenti acquisiscono una perfetta padronanza delle varie competenze, le quali divengono parte effettiva dell'apprendimento incentrato sullo sviluppo del nuovo modello comportamentale desiderato
- "Curva dell'oblio" di Ebbinghaus: metodologie di apprendimento basate sulle caratteristiche peculiari della memoria umana
- La ripetizione dei concetti crea abitudini comportamentali sicure e impedisce di dimenticare quanto appreso in precedenza
- Rafforzamento incluso in ogni singolo modulo

Apprendimento modulare

- "Curva dell'oblio" di Ebbinghaus: metodologie di apprendimento basate sulle caratteristiche peculiari della memoria umana
- La ripetizione dei concetti crea abitudini comportamentali sicure e impedisce di dimenticare quanto appreso in precedenza
- Rafforzamento incluso in ogni singolo modulo

Argomenti della formazione

Ciascun modulo comprende diversi livelli, in cui vengono spiegate nel dettaglio le competenze specifiche in materia di sicurezza IT.
I livelli vengono definiti in base al grado di difficoltà che deve essere gestito in materia di sicurezza: il Livello 1 è generalmente sufficiente a fornire protezione dagli attacchi più semplici e generici, mentre per una protezione da attacchi più sofisticati e mirati è necessario studiare i livelli successivi.

- Password e account
- E-mail
- Navigazione in Internet
- Social network e servizi di messaggistica
- Team di PC Security
- Dispositivi mobili
- Dati riservati*
- GDPR*

* Sarà aggiunto nel 1° trimestre 2020

Esempio: competenze apprese nel modulo "Navigazione in Internet"

Base Per prevenire attacchi generici e semplici da individuare	**Principiante** Per prevenire attacchi di massa su un profilo specifico	**Intermedio** Per prevenire attacchi di media complessità	**Avanzato** Per prevenire attacchi mirati
13 competenze, tra cui: – Come configurare il PC (aggiornamenti, antivirus) – Come evitare siti web chiaramente dannosi (che chiedono di aggiornare il software, ottimizzare le performance del PC, inviare SMS, installare lettori e così via) – Come riconoscere file eseguibili dai siti web	**20 competenze, tra cui:** – Come effettuare la registrazione/accesso solo su siti attendibili – Come evitare link numerici – Come inserire informazioni sensibili solo su siti attendibili – Come riconoscere gli indicatori di un sito web dannoso	**14 competenze, tra cui:** – Come riconoscere link malevoli – Come riconoscere file e download dannosi – Come riconoscere software dannosi	**13 competenze, tra cui:** – Come riconoscere link malevoli complessi (compresi quelli creati ad hoc, molto simili a domini relativi a siti web leciti, link con reindirizzamenti) – Come evitare siti Black SEO – Come effettuare il logout al termine delle sessioni di lavoro – Configurazione avanzata del PC (disattivare Java, adblock, noscript e così via)
	+ rafforzamento delle competenze di base	+ rafforzamento delle competenze precedenti	+ rafforzamento delle competenze precedenti

Argomenti chiave trattati nel modulo: Link, Download, Installazioni software, Registrazione e accesso, Pagamenti, SSL

Lingue

Al mese di luglio 2019 la piattaforma (sia interfaccia utente, sia interfaccia amministratore) risulta disponibile nelle seguenti lingue:

- Arabo
- Olandese
- Inglese
- Francese
- Tedesco
- Italiano
- Portoghese
- Russo
- Spagnolo

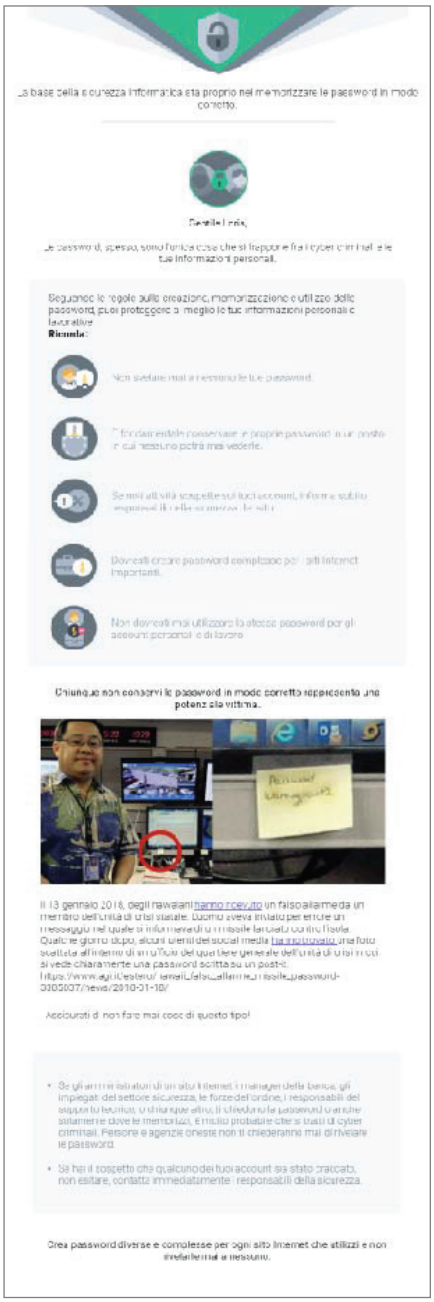
Efficienza della formazione: contenuti ben strutturati e bilanciati, basati su eventi e situazioni reali

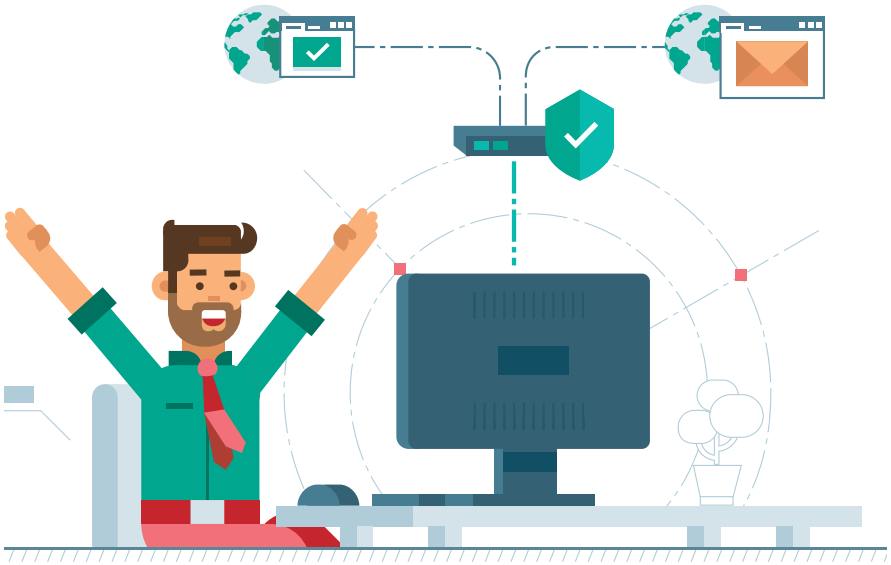
I principi di apprendimento implementati attraverso la piattaforma ASAP si basano sulla particolare metodologia che tiene conto delle specificità della natura umana, della nostra capacità di percepire e assorbire le informazioni. Il contenuto è ricco di esempi e casi concreti, atti a evidenziare l'importanza della Cybersecurity per ogni singolo dipendente. La piattaforma è incentrata sulle competenze di formazione, non solo sulla parte teorica: gli esercizi pratici e i task legati al dipendente sono al centro di ogni modulo.

I moduli combinano diversi tipi di esercizi, per mantenere alto l'interesse degli utenti, per allertarli e motivarli nell'apprendimento di un comportamento sicuro.

Lo stile e i testi non sono solo tradotti nelle diverse lingue, ma vengono adattati perché riflettano le culture locali.

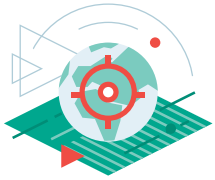
Task ed esercizi basati sulla simulazione per creare competenze pratiche e mantenere gli utenti attivi e motivati





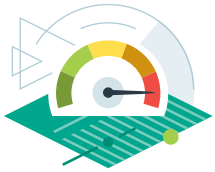
Kaspersky Security Awareness

Principali fattori di differenziazione del programma



Formazione mirata e basata sulla funzione aziendale
- Si apprende ciò che è necessario sapere in base al proprio ruolo e profilo di rischio
- Esempi basati su eventi e situazioni reali: le competenze acquisite si possono utilizzare immediatamente
- Apprendimento attraverso la pratica

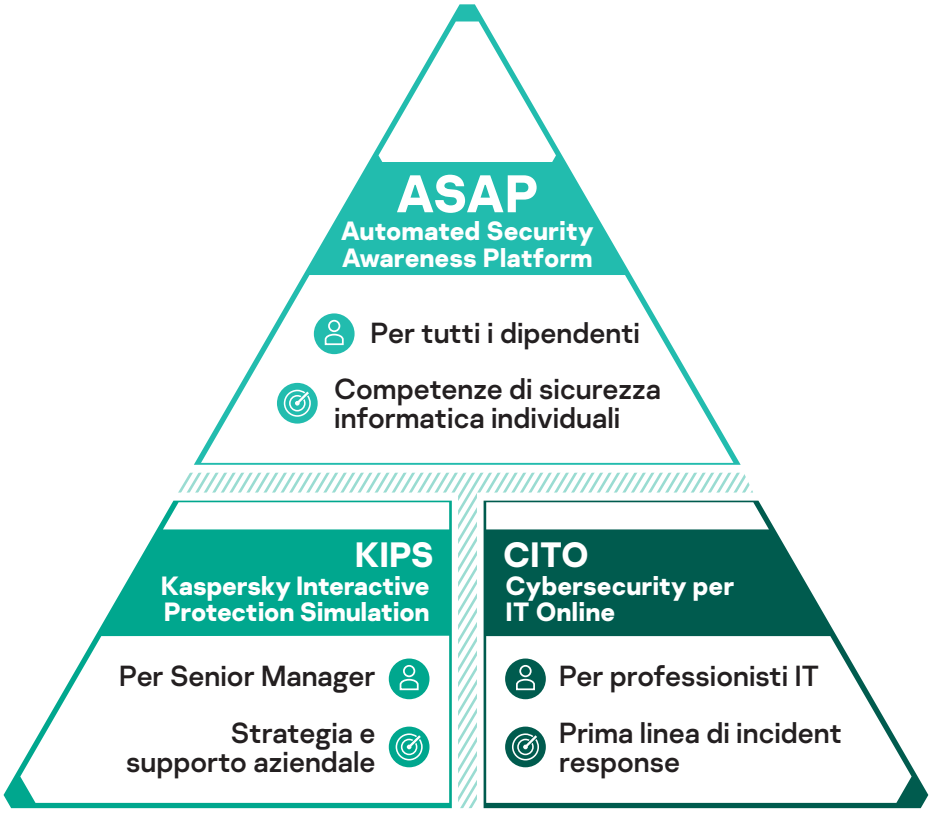
Incentrato sulla persona
- La formazione è strutturata in modo tale da riflettere il naturale modo di pensare delle persone
- Imprime una forte spinta proattiva verso l'adozione di modelli di comportamento sicuri
- Informazioni e competenze fornite si assimilano con facilità, grazie a metodologie basate sulle caratteristiche peculiari della memoria umana



Apprendimento incrementale continuo
- Dal modulo più semplice a quello più complesso
- Estensione e applicazione a nuovi contesti delle conoscenze precedentemente acquisite

Facile da controllare e da gestire
- Online
- Gestione automatizzata dell'apprendimento
- Invio in automatico di inviti ed e-mail motivazionali, con suggerimenti e raccomandazioni individuali per ogni studente

Formati di apprendimento diversi, per i vari livelli della struttura organizzativa



Prova gratuitaKaspersky ASAP: k-asap.com
Cybersecurity aziendale: https://www.kaspersky.it/enterprise-security
Kaspersky Security Awareness: www.kaspersky.com/awareness
IT Security News: business.kaspersky.com

www.kaspersky.it

kaspersky BRING ON THE FUTURE