Coinvolgente per i dipendenti, efficiente per i manager.

Prova gratuita
k-asap.com/it

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky bring on the future

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

L'82% di tutti gli incidenti informatici è riconducibile a errori umani, con potenziali perdite di milioni di euro per le aziende. I programmi di formazione tradizionali non sono progettati per affrontare questo problema ed è necessario un nuovo tipo di approccio. La soluzione è Kaspersky ASAP.

L'errore umano è il rischio informatico più grande

Il 72%
dei dipendenti
ammette di aver svolto almeno un'attività rischiosa nell'anno precedente pur essendo consapevole dei rischi *

Il 51%
dei dipendenti
ritiene che la responsabilità di evitare che l'azienda cada vittima di attacchi informatici dovrebbe essere esclusivamente del reparto IT*

Il 55%
delle aziende
segnala minacce causate da un uso inappropriato delle risorse IT da parte dei dipendenti**

Il 51%
delle piccole imprese
ha subito un incidente di sicurezza a causa della violazione dei criteri di sicurezza IT da parte dei dipendenti**

Il 26%
dei dipendenti
riferisce di avere la stessa password per l'e-mail personale e l'account aziendale***

Ostacoli al lancio di un programma di Security Awareness che funzioni

Nonostante le aziende siano pronte a implementare i programmi di Security Awareness, non molte sono soddisfatte dei processi e dei risultati. Le PMI in particolare lo trovano impegnativo, in quanto tendono a non avere l'esperienza o le risorse necessarie.

Inadatto per gli studenti

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

Vengono indicate solo le cose da "non fare", anziché fornire istruzioni su "come fare" qualcosa

Le conoscenze acquisite non vengono consolidate

Lettura e ascolto non sono efficaci come l'attività pratica

Un impegno per gli amministratori

Come creare un programma e definire gli obiettivi?

Come gestire gli incarichi di formazione?

Come controllare i progressi compiuti

Come assicurarsi che il nostro staff sia pienamente coinvolto?

* Balancing Risk, Productivity, and Security", Delinea, 2021

** "ITSecurity Economics 2022", Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

Formazione efficiente e facile da gestire per le organizzazioni di qualsiasi dimensione

Kaspersky ASAP (Automated Security Awareness Platform) rappresenta l'elemento centrale del portfolio formativo Kaspersky Security Awareness. La piattaforma è uno strumento online che permette di sviluppare competenze pratiche e solide in materia di sicurezza informatica per i dipendenti durante tutto l'arco dell'anno, aiutando le organizzazioni **a ridurre il numero di incidenti informatici dovuti al fattore umano.**

Il processo di implementazione e gestione della piattaforma non richiede risorse o configurazioni specifiche e include una guida integrata per ogni passaggio del percorso verso una strategia aziendale di cybersecurity.

Contenuti significativi che non è possibile ignorare

Uno dei criteri più importanti nella scelta di un programma di sensibilizzazione è l'efficienza e, con ASAP, l'efficienza è integrata nei contenuti e nella gestione della formazione. I contenuti sono basati sull'esperienza acquisita in **oltre 25 anni nel settore della sicurezza informatica**, espressa in un modello formativo che comprende oltre **350 competenze pratiche essenziali di cybersecurity** che tutti i dipendenti dovrebbero avere.

Formate i vostri dipendenti sulla cybersecurity.
Cambiate il loro atteggiamento e comportamento e proteggete la vostra azienda e i vostri sistemi IT.

Formazione efficiente

Coerenza	– Contenuti ben strutturati – Moduli interattivi, costante rafforzamento, conduzione di test, attacchi di phishing simulati, per garantire l'applicazione delle competenze acquisite I contenuti e la struttura del materiale didattico tengono conto delle specificità della memoria umana e della 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 Esempi di situazioni reali, con cui i dipendenti possono relazionarsi direttamente, contribuiscono ad aumentare il coinvolgimento, aiutando la memorizzazione delle informazioni.
Positività	– 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 e distacco, mentre spiegazioni e principi perfettamente allineati 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. – Sincronizzazione con AD (Active Directory), SSO (Single Sign-On), Open API (la capacità di interagire con soluzioni di terze parti), onboarding online durante la prima visita, una sezione di domande frequenti e suggerimenti rendono la gestione della piattaforma comoda ed efficiente.
Facile da controllare	Dashboard "all-in-one" e report pratici: – report sull'avanzamento delle lezioni – report sui test e simulazione di attacchi di phishing
Facilità di coinvolgimento	La piattaforma invia automaticamente inviti e promemoria, nonché report a studenti e amministratori.

Opzioni di distribuzione

Kaspersky ASAP può essere fornito in tre diverse opzioni, a seconda delle preferenze:

- **Soluzione completamente online basata su cloud.** In questo caso, i dati dell'utente vengono gestiti nel pieno rispetto della normativa applicabile, a seconda della posizione del server selezionato. Ad esempio, se scegliete l'Europa, i dati verranno archiviati nell'Unione Europea (a Francoforte, in Germania) e tutti i dati legalmente protetti verranno elaborati secondo le normative sulla protezione dei dati dell'Unione Europea (GDPR).
- **Contenuto nel pacchetto SCORM.** Con questa opzione, i moduli di formazione possono essere integrati con il sistema LMS (Learning Management System) interno. Tuttavia, questa opzione non include test e attacchi di phishing simulati
- **On-premise.** Questa opzione è adatta ai clienti che necessitano di massimi livelli di riservatezza. Per le aziende vincolate da una qualche forma di controllo normativo, l'implementazione on-premise supporta la conformità, evitando possibili multe e sanzioni. Il materiale didattico viene distribuito nella rete del cliente e l'utente ha il controllo completo sull'hardware del server, sulla sicurezza dei dati e sulla configurazione. Gli utenti possono accedere ai materiali di formazione anche senza connettersi a Internet.

Gestione della piattaforma ASAP: semplicità attraverso la completa automazione

Avvio del programma in 4 semplici step

1

Aggiunta di utenti

Potete utilizzare la **sincronizzazione AD**, caricare un file .xlsx o aggiungerli manualmente

2

Divisione degli utenti in base ai gruppi

Dividete gli utenti manualmente o in base al livello di target desiderato

3

Avvio del programma di formazione

Dividete gli utenti manualmente o in base al livello di target desiderato e impostate la data di inizio per ciascun gruppo

4

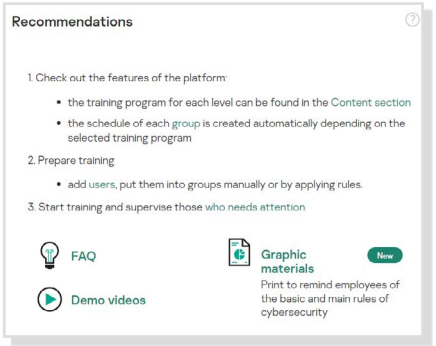
Gestione automatizzata dell'apprendimento tramite ASAP

ASAP propone una pianificazione per ciascun gruppo, crea inviti, promemoria e altre comunicazioni: tutto avviene automaticamente

Un approccio innovativo alla formazione

Kaspersky ASAP sta cambiando il modo di erogare contenuti didattici sulla sicurezza informatica. Adesso è possibile scegliere se assegnare ai dipendenti un **corso rapido** di livello base che aiuterà a soddisfare rapidamente i requisiti normativi per la formazione sulla sicurezza informatica, aggiornare le loro conoscenze oppure optare per il **corso principale** suddiviso in livelli di complessità

Onboarding durante il primo accesso, suggerimenti, domande frequenti e video dimostrativi che spiegano come funziona la piattaforma dal punto di vista dell'amministratore e dell'utente: tutto ciò di cui avete bisogno per iniziare il processo di formazione si trova nella pagina principale dell'amministratore.



Argomenti trattati

Argomenti trattati

Corso principale	Corso rapido
E-mail	E-mail
Password e account	Password e account
Siti Web e Internet	Siti Web e Internet
Social media e strumenti di messaggistica	Sicurezza dei dispositivi mobili
Sicurezza del PC	Social media
Dispositivi mobili	Risorse del computer
Protezione dei dati confidenziali	Protezione dei dati confidenziali
Dati personali	Doxing
GDPR	Sicurezza delle criptovalute
Industrial Cybersecurity	Sicurezza delle informazioni durante il lavoro in remoto
Sicurezza delle carte bancarie e PCI DSS	Legge federale 152-FZ (per la Russia)
Protezione fisica dei dati	Legge federale FZ-187 (Sicurezza dell'infrastruttura delle informazioni critiche in Russia)

Gli argomenti sono suddivisi in ampie sezioni, che riguardano numerosi concetti di sicurezza IT *.

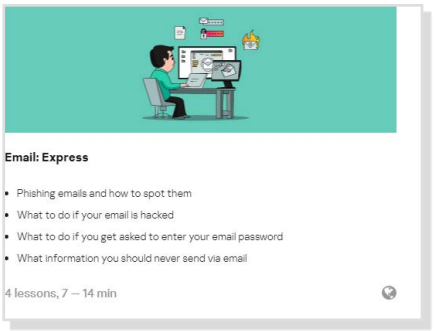
#Password #Phishing #Account aziendali #Messaggi pericolosi #Carte bancarie #Ransomware #SocialEngineering #File pericolosi #Lavorare con i browser #Etica aziendale #Anti-virus #Software dannoso #Applicazioni #Browser #Informazioni riservate #Archiviazione delle informazioni #Invio di informazioni #Dati personali #Internet e normative #Normative europee #Azienda #Collegamenti pericolosi #Siti Web falsi #Siti di ransomware #Backup #Dati mobili #Criptaggio #Servizi cloud #Spionaggio industriale #PCI DSS #Autenticazione a due fattori #Footprint digitale #Torrent #Catfishing #Attacco mirato #Hashing #Token #Blocchi pattern #Mining #Parental Control

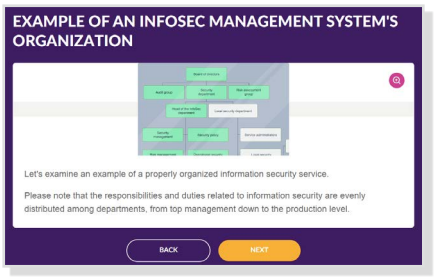
* Per l'elenco più recente di argomenti e concetti, visitate la pagina k-asap.com/it

Ciascun modulo comprende diversi livelli, in cui vengono spiegate nel dettaglio le competenze specifiche in materia di sicurezza IT. I livelli sono definiti in base al grado di rischio che consentono di contrastare: ad esempio, il livello 1 in genere è sufficiente per proteggere dagli attacchi più semplici e dagli attacchi di massa. I livelli più alti permettono di imparare a proteggersi dagli attacchi più sofisticati e mirati.

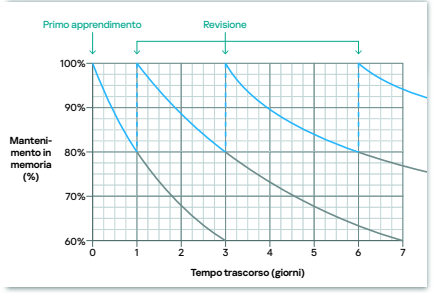
Esempio: competenze acquisite nell'argomento "Siti Web e Internet".

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
23 competenze, tra cui: – Riconoscere i finti pop-up – Fare attenzione ai reindirizzamenti – Distinguere i collegamenti di download autentici da quelli falsi – Riconoscere i file eseguibili trovati nel Web – Essere in grado di determinare l'autenticità di un'estensione del browser	**34 competenze, tra cui:** – Immettere i dati solo nei siti con un certificato SSL valido – Usare password diverse per registrazioni diverse – Riconoscere i siti falsi in base a diversi indicatori – Come evitare link numerici – Riconoscere gli indirizzi dei collegamenti di rete non validi dai sottodomini fasulli	**12 competenze, tra cui:** – Verificare i collegamenti di condivisione prima dell'invio – Utilizzare solo software di produttori affidabili per i torrent – Scaricare i contenuti legali solo dai torrent – Cancellare regolarmente i cookie del browser	**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) – Controllare i siti che utilizzano utilità speciali – Riconoscere se il browser è pensato per il mining – Evitare siti Black SEO
	+ rafforzamento delle competenze di base	+ rafforzamento delle competenze precedenti	+ rafforzamento delle competenze precedenti





Curva dell'oblio di Ebbinghaus



Corso rapido ASAP

Versione breve del corso di formazione audio/video. Ogni argomento sulla cybersecurity contiene diverse brevi lezioni per aiutare l'utente ad acquisire le competenze di base sulla sicurezza informatica.

- Teoria interattiva
- Video
- Test

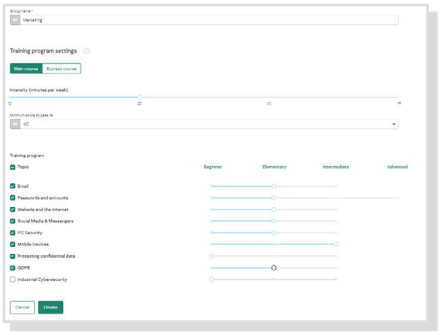
Gli attacchi di phishing simulati non sono inclusi nel percorso di apprendimento, ma possono essere assegnati separatamente dall'amministratore.

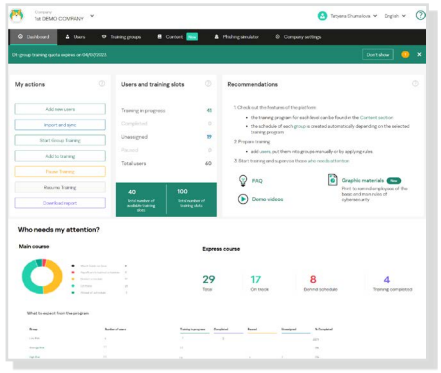
Corso principale ASAP

La formazione è basata sulle caratteristiche specifiche della memoria umana:

- Numerosi elementi formativi per lo sviluppo della consapevolezza:
  - Ogni unità comprende: un modulo interattivo, rafforzamento, valutazione (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 del nuovo modello comportamentale desiderato.
- Apprendimento modulare:
  - Gli elementi formativi si susseguono a determinati intervalli, eliminando la ripetitività delle lezioni e migliorando la memorizzazione. Gli intervalli si basano sullo studio della "Curva dell'oblio" di Ebbinghaus.
  - La ripetizione dei concetti crea abitudini comportamentali sicure e impedisce di dimenticare quanto appreso in precedenza.
- Efficienza della formazione, contenuti ben strutturati e bilanciati, basati su eventi e situazioni reali:
  - Numerosi esempi reali evidenziano l'importanza personale della sicurezza informatica per i dipendenti.
  - La piattaforma è incentrata sulle competenze di formazione, non solo sulla parte teorica: gli esercizi pratici e le attività legate al dipendente sono al centro di ogni modulo.

Percorso di apprendimento flessibile





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 formazione è possibile scegliere:

- Il corso rapido, il corso principale o una combinazione di entrambi.
- Argomenti di apprendimento per la formazione nel corso principale e/o nel corso rapido rivolta agli studenti del gruppo.
- Il livello target che gli studenti devono raggiungere per ciascun argomento scelto nel corso principale.

Il percorso di apprendimento sarà costruito automaticamente dalla piattaforma per ogni gruppo di studenti sulla base di queste impostazioni.

Tutto questo dalla dashboard

- Tutte le attività richieste per controllare e gestire la formazione (statistiche, riepiloghi delle attività e dei progressi degli utenti, slot di formazione, formazione di gruppo, suggerimenti su come migliorare i risultati) possono essere eseguite dalla dashboard. È possibile scaricare i report con un solo clic e configurare la frequenza dei report.

Esprimi le tue potenzialità

- I dipendenti possono studiare in qualsiasi momento e da qualunque dispositivo, con il design ottimizzato per i dispositivi mobili di ASAP che rende l'apprendimento pratico e conveniente.
- Gli utenti possono accedere al portale di formazione con i collegamenti personalizzati forniti nell'invito alla formazione o tramite un unico collegamento per tutti gli utenti con tecnologia Single Sign-On (SSO), se configurata dall'amministratore.

Personalizzazione

L'amministratore può modificare facilmente l'aspetto del programma:

- Sostituire il logo Kaspersky con il logo dell'azienda nel pannello di amministrazione, nel portale di formazione e nelle e-mail della piattaforma.
- Personalizzare i certificati.
- Aggiungere contenuti personali a qualsiasi lezione.

Integrazione

Potete utilizzare Open API per interagire con soluzioni di terze parti: Open API funziona tramite HTTP e offre una serie di metodi di richiesta/risposta.

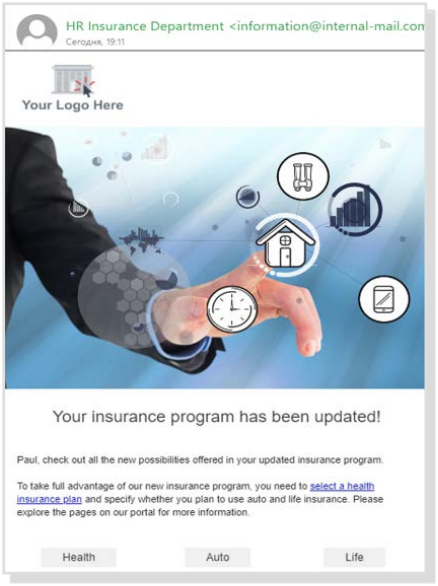
ASAP si integra con le piattaforme Kaspersky KUMA e XDR:
– L'amministratore può visualizzare un evento in XDR e adottare la risposta appropriata, inclusa l'assegnazione di un corso di formazione in ASAP.
– Integrazione automatica delle schede degli incidenti con informazioni sul livello di consapevolezza dell'utente vittima dell'attacco.

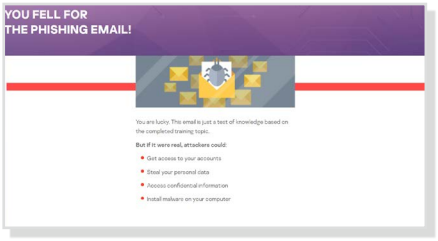
Localizzazione

ASAP è disponibile in 25 lingue diverse*. La localizzazione in ASAP va oltre la semplice traduzione: il testo e le immagini non solo vengono tradotti in lingue diverse, ma vengono anche adattati per riflettere le diverse culture e attitudini locali.

* Potete trovare l'elenco aggiornato delle lingue disponibili su k-asap.com/it

Esempio del modello di phishing simulato modificabile e feedback

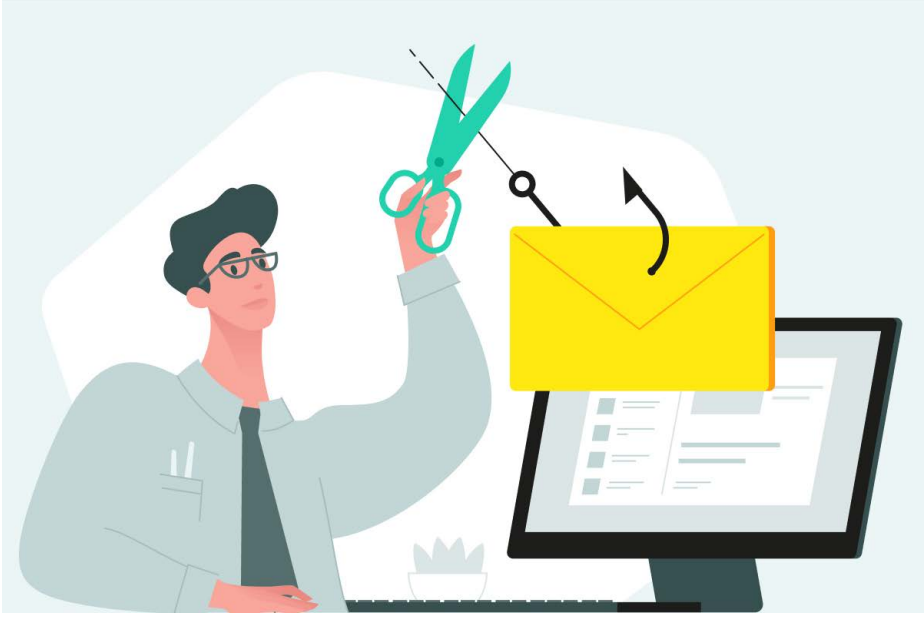




Campagne di phishing simulate

Le campagne di phishing vengono offerte in aggiunta alla formazione principale. Mettono alla prova le capacità pratiche dei dipendenti nell'evitare gli attacchi di phishing e aiutano i responsabili della formazione a identificare rapidamente le lacune nelle conoscenze degli utenti e incoraggiare l'approfondimento degli argomenti problematici. Le campagne di phishing sono anche un ottimo strumento per insegnare ai dipendenti a riconoscere i segnali potenzialmente pericolosi e mettere in pratica le proprie conoscenze.

La piattaforma viene fornita con modelli di e-mail già pronti contenenti esempi di phishing che possono essere inviati agli utenti in tutte le lingue disponibili. I modelli vengono regolarmente aggiornati e ne vengono aggiunti di nuovi. È inoltre possibile creare e-mail personalizzate in base a modelli predefiniti.



Provando un attacco di phishing simulato prima di iniziare la formazione sarà possibile mettere alla prova la resilienza dei dipendenti! Dipendenti e addetti alla gestione potranno così constatare i vantaggi della formazione.

I dipendenti possono anche dimostrare la loro comprensione di un argomento non facendosi ingannare da un attacco di phishing simulato e segnalando le e-mail di phishing tramite lo strumento per la segnalazione del phishing.

Lo strumento di segnalazione del phishing dimostra il livello di consapevolezza dei dipendenti, rimuove le e-mail dalla posta in arrivo e invia messaggi non solo all'amministratore della piattaforma, ma anche ai team di sicurezza IT, per aiutare le aziende a migliorare il rilevamento del phishing e i livelli di reazione.

Kaspersky ASAP per partner MSP/MSSP o aziende con una struttura geograficamente distribuita

La piattaforma consente di distribuire e gestire la formazione sulla sicurezza in più aziende da un'unica console predisposta per il multitenancy, senza la necessità di software aggiuntivo.

Buone notizie! Kaspersky ASAP dispone di una funzionalità di gestione delle licenze che consente di assegnare una quota per le licenze a ciascuna azienda con un determinato periodo di validità.

È inoltre possibile aggiungere ulteriori amministratori per ciascuna azienda e assegnare loro ruoli diversi.

Kaspersky Security Awareness – un nuovo approccio all'apprendimento di abilità di sicurezza IT

Principali elementi distintivi del programma

Solida competenza nel campo della cybersecurity
Oltre venticinque anni di esperienza nel campo della cybersecurity tradotti nella competenza che dà fondamento ai nostri prodotti

Formazione che modifica il comportamento dei dipendenti a ogni livello dell'organizzazione
Il nostro corso di formazione basato sulla gamification garantisce coinvolgimento e motivazione grazie all'istruzione unita al divertimento, mentre le piattaforme di apprendimento aiutano a interiorizzare le competenze di cybersecurity, per assicurare che le nozioni apprese non vadano perse nel tempo.

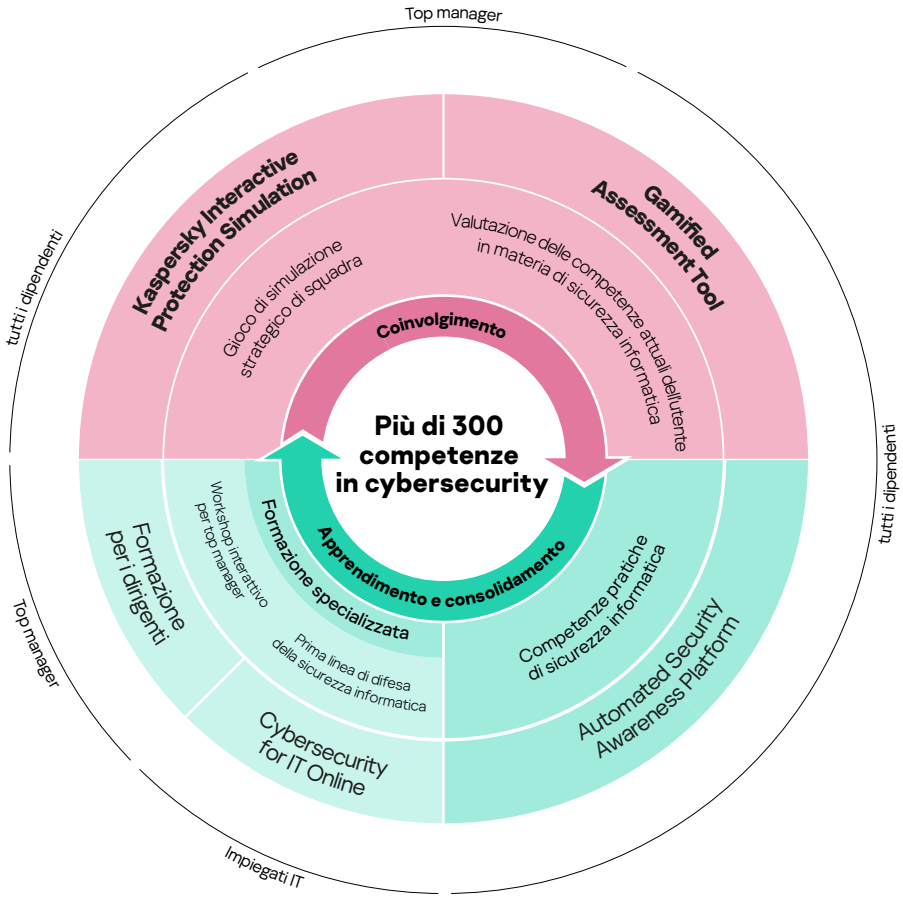
ASAP è un prodotto centrale nel portfolio Kaspersky Security Awareness.

Una soluzione di formazione flessibile per tutti

Kaspersky Security Awareness vanta una lunga storia di successi a livello internazionale. Utilizzata da aziende di ogni dimensione per la **formazione di oltre un milione di dipendenti in più di 75 paesi**, la soluzione combina gli oltre 25 anni di esperienza di Kaspersky nel campo della cybersecurity con le approfondite competenze nella formazione per gli adulti.

Il portfolio offre opzioni di formazione che promuovono una maggiore consapevolezza in merito alle problematiche della cybersecurity tra i dipendenti a tutti i livelli, consentendo loro di contribuire alla sicurezza informatica complessiva dell'organizzazione.

Poiché le modifiche comportamentali sostenibili richiedono tempo, il nostro approccio si basa sulla creazione di un ciclo di apprendimento continuo con più componenti. L'apprendimento basato sul gioco coinvolge i senior manager, trasformandoli in sostenitori delle iniziative di cybersecurity e dello sviluppo di una cultura della sicurezza. La valutazione basata sul gioco aiuta a definire le lacune nelle conoscenze dei dipendenti e a motivarli nell'apprendimento, mentre le piattaforme e le simulazioni online forniscono loro le competenze appropriate.



Prova gratuita della soluzione Kaspersky ASAP: k-asap.com/it
Enterprise Cybersecurity: https://www.kaspersky.it/enterprise-security
Kaspersky Security Awareness: www.kaspersky.it/awareness
Novità sulla sicurezza IT: business.kaspersky.com

www.kaspersky.it

kaspersky bring on the future