Kaspersky Interactive Protection Simulation

Sviluppare la consapevolezza della cybersecurity tra top manager e decision maker

kaspersky bring on the future

Ulteriori informazioni sono disponibili sul sito
kaspersky.it/awareness

Kaspersky Interactive Protection Simulation

Il fattore umano

Una delle principali problematiche relative alla sicurezza che le aziende di oggi si trovano ad affrontare è che i vari senior manager considerano la cybersecurity da punti di vista diversi e le attribuiscono priorità differenti. Questo può comportare un processo decisionale che può essere definito "il triangolo delle Bermuda della sicurezza":

- Le aziende considerano le misure di sicurezza
- un ostacolo al raggiungimento degli obiettivi di business (maggiore convenienza/velocità/efficienza).
- I responsabili della sicurezza informatica possono percepire la cybersecurity come una questione che esula dalle loro competenze, in quanto legata agli investimenti e all'infrastruttura.
- I responsabili del controllo dei costi possono non comprendere che le spese per la cybersecurity comportano un ritorno in termini di ricavi e risparmi, anziché generare costi.

La collaborazione e la comprensione reciproca tra queste tre figure sono fondamentali per un approccio efficace alla sicurezza informatica. Tuttavia, i tradizionali programmi di formazione, come corsi ed esercitazioni di gruppo, presentano dei problemi: richiedono tempo, sono troppo tecnici, risultano poco adatti per i manager impegnati e non consentono di sviluppare un "linguaggio comune".

La cyber immunity di un'azienda parte dai vertici dell'organizzazione

Oggi molte aziende considerano la sostenibilità dell'infrastruttura IT una priorità. Tuttavia, poiché in genere le questioni relative alla cybersecurity rientrano nelle responsabilità del reparto IT e del personale addetto alla sicurezza informatica, in azienda può venirsi a creare una cultura frammentata riguardo ai comportamenti appropriati da adottare. Concentrati principalmente su vendite, esperienza del cliente, costi e rischi, mentre lavorano per raggiungere i propri obiettivi, i dirigenti aziendali spesso trascurano la sicurezza informatica. Senza il supporto di una dirigenza che sia di esempio, la creazione di una cultura unificata della cybersecurity può essere irraggiungibile.

Il 76% dei CEO ammette di ignorare i protocolli di sicurezza per ottenere più rapidamente i risultati desiderati, sacrificando la sicurezza a favore della velocità*.

Il 62% dei manager ammette che i problemi relativi alla comunicazione sulla sicurezza IT all'interno della propria organizzazione hanno portato ad almeno un incidente di cybersecurity**.

Il 51% dei professionisti impegnati nel settore della sicurezza informatica trova molto difficile parlare di un aumento del budget per la sicurezza IT... ma è sulla stessa lunghezza d'onda in merito alle strategie di comunicazione realizzabili.

La maggior parte dei dirigenti **(56%) e del personale IT (48%)** concorda sul fatto che la presentazione di esempi presi dalla vita reale sia il modo migliore per agevolare la comunicazione delle questioni relative alla sicurezza informatica**.

Vantaggi di Kaspersky Security Awareness

Kaspersky Security Awareness è una soluzione collaudata, efficace ed efficiente, con 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 di Kaspersky Academy nella formazione per gli adulti.

Il portfolio è composto da interessanti prodotti 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.

Ogni prodotto incluso nel portfolio svolge un ruolo specifico nel ciclo di apprendimento complessivo ed è disponibile anche come soluzione autonoma.

Un gioco di simulazione aziendale strategico sulla cybersecurity rivolto ai dirigenti

Kaspersky Interactive Protection Simulation (KIPS) è un gioco di simulazione aziendale strategico a squadre, che dimostra la connessione tra efficienza aziendale e cybersecurity.

Con il ruolo di membri del team di sicurezza IT in un ambiente aziendale simulato, i partecipanti devono affrontare una serie di minacce informatiche impreviste senza compromettere l'operatività e la redditività dell'azienda.

Devono sviluppare una strategia di difesa informatica scegliendo tra i migliori controlli proattivi e reattivi a loro disposizione. Ogni loro scelta determina un cambiamento nel modo in cui si svolge lo scenario e, in ultima analisi, influisce sulle entrate che l'azienda realizza o meno.

Trovando un equilibrio fra priorità tecniche, aziendali e di sicurezza e i costi di un cyberattacco reale, i team analizzano i dati e prendono decisioni strategiche sulla base di informazioni incerte e risorse limitate. Se sembra realistico, è perché tutti gli scenari sono basati su eventi reali.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

KIPS è un gioco dinamico sulla Security Awareness con un approccio basato sull'apprendimento pratico:

- Divertente, coinvolgente e rapido (2 ore).
- Il lavoro di squadra crea collaborazione.
- La competizione stimola la capacità di analisi e l'intraprendenza.
- Il gioco consente di migliorare la comprensione delle misure di cybersecurity.
- Tutti gli scenari e gli attacchi sono basati su casi reali

Perché KIPS funziona

Destinata a esperti di sistemi aziendali, personale IT e line manager, la formazione KIPS mira a promuovere la consapevolezza dei rischi e dei problemi di sicurezza derivanti dalla complessità dei moderni sistemi informatici.

Ogni team è composto da 4-6 persone e ha il compito di gestire un'azienda che comprende gli impianti di produzione e i computer che li controllano. Nel corso della simulazione, gli impianti di produzione generano entrate, sensibilizzazione del pubblico e risultati di business. Al tempo stesso, i team devono affrontare gli attacchi informatici che minacciano di compromettere le prestazioni aziendali.

Al termine della simulazione, i partecipanti avranno acquisito competenze importanti e utili, che potranno mettere in pratica nel proprio lavoro.

- Gli attacchi informatici comportano un danno economico e devono essere affrontati dal management
- La collaborazione tra i decision maker IT e non IT è essenziale per assicurare un approccio efficace alla cybersecurity all'interno di ogni azienda
- Un budget di sicurezza adeguato non causerà il fallimento dell'azienda, ma i mancati guadagni a seguito di un attacco informatico andato a segno potrebbero farlo...
- Le persone si abituano ai controlli di sicurezza e imparano a capirne l'importanza (formazione sugli audit, anti-virus e così via).

KIPS è disponibile in due modalità:

KIPS Live è un'opzione molto popolare che crea un'atmosfera di coinvolgimento ed entusiasmo, oltre che un ottimo strumento per motivare il personale e promuovere una cultura della cybersecurity all'interno di un'organizzazione.

Nella **versione KIPS Online** gli utenti possono interagire con un numero elevato di partecipanti ovunque si trovino.

Perfetto per organizzazioni globali o attività pubbliche, KIPS Online può essere unito a KIPS Live per aggiungere team remoti all'evento in sede.

- Fino a 300 team (= 1.000 partecipanti) contemporaneamente, da qualsiasi parte del mondo.
- I vari team possono scegliere una lingua diversa per l'interfaccia di gioco.
- Dalla libreria i clienti possono personalizzare gli scenari preinstallati determinando il numero e il tipo degli attacchi sferrati durante il gioco.
- I clienti con una licenza che consente loro di utilizzare KIPS senza limitazioni durante il periodo di licenza possono adattare le impostazioni predefinite o personalizzare lo scenario a ogni sessione di gioco, scegliendo e combinando diversi attacchi dalla libreria. Grazie a questa funzionalità è possibile rendere il gioco ancora più interessante perché sempre diverso.
- Un altro vantaggio della versione online è che consente di visualizzare le statistiche delle scelte dei partecipanti, ottenere dati sulle azioni dei team in determinate situazioni e confrontare le azioni dei partecipanti in relazione alla sessione di gioco precedente.

KIPS mostra:

- Il ruolo svolto dalla cybersecurity per la redditività e la continuità aziendale.
- Le sfide emergenti e le minacce affrontate dalle aziende.
- Gli errori tipici relativi alla cybersecurity che le aziende commettono.
- In che modo la cooperazione tra i team aziendali e di sicurezza aiuta a mantenere operazioni stabili e una protezione continua contro le minacce informatiche.

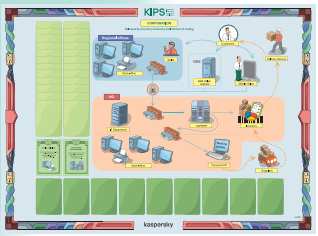
A seconda dello scenario, i team sono responsabili della sicurezza IT dell'azienda in un determinato settore. Il loro compito è garantire il normale funzionamento dell'azienda, mantenere i rapporti con clienti e fornitori e individuare e neutralizzare le minacce informatiche.

Nel momento in cui l'azienda subisce un attacco informatico, i partecipanti sperimentano l'impatto sulla produzione e sui ricavi e imparano dunque ad adottare diverse soluzioni e strategie IT e aziendali per ridurre al minimo l'impatto dell'attacco senza perdite sui guadagni.

Vince la squadra che completa il gioco con il maggior profitto, avendo individuato e analizzato tutte le insidie nel sistema della cybersecurity e avendovi adeguatamente risposto.

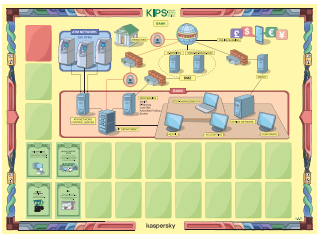
Scenari KIPS aziendali per tutti i settori verticali

Corporation



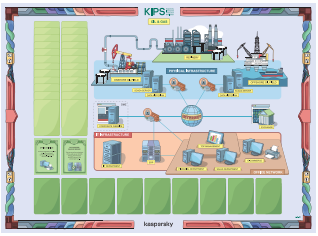
Protezione dell'azienda da **ransomware, APT, problemi di sicurezza associati all'automazione.**

Banche



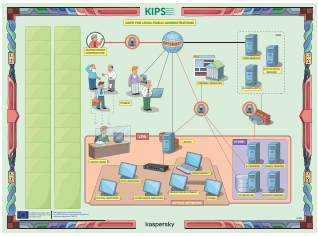
Protezione degli istituti finanziari dalle **APT emergenti di alto livello, come Tyupkin e Carbanak.**

Settore Oil & Gas



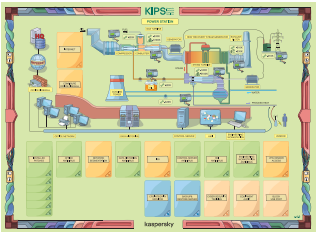
Analisi dell'impatto di un'ampia gamma di minacce, **dal defacing del sito Web a un vero ransomware e una APT sofisticata.**

Pubbliche amministrazioni locali



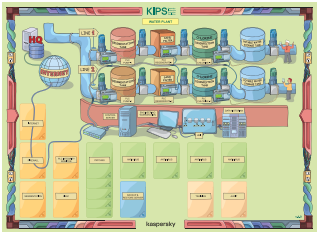
Protezione dei server Web pubblici da attacchi ed exploit.

Centrali elettriche



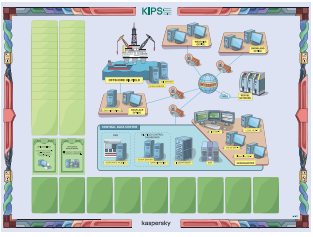
Protezione dei sistemi di controllo industriali e delle infrastrutture critiche dagli attacchi informatici in stile Stuxnet.

Impianti idrici



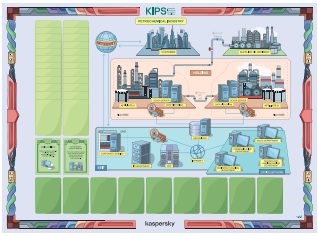
Protezione dell'infrastruttura IT di un impianto di depurazione dell'acqua, assicurando la stabilità di due linee di produzione.

Compagnie petrolifere



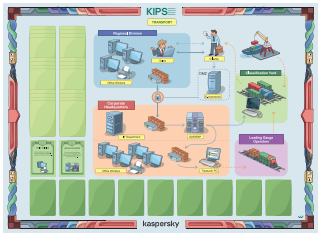
Mantenimento della sicurezza informatica per proteggere le entrate di un'azienda globale con uffici in tutto il mondo.

Settore petrolchimico



Mantenimento del normale funzionamento della nuova succursale di un'importante holding petrolchimica, incentrata sulla produzione di etilene.

Trasporti

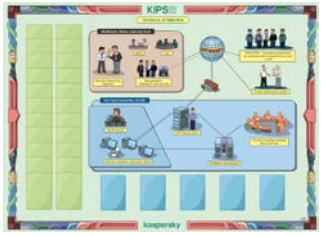


Protezione di una società di logistica da **Heartbleed, APT, ransomware B2B e minacce interne.**

Aeroporto

Assicurazione della protezione dei passeggeri e della consegna puntuale delle merci in aeroporto, proteggendo le risorse da numerosi attacchi informatici e minacce.

Attribuzione tecnica



Analisi e attribuzione tecnica al fine di determinare la responsabilità di un complesso attacco APT contro i server delle Nazioni Unite.

PICCOLE E MEDIE AZIENDE

Protezione delle attività aziendali di una PMI dalle minacce alla sicurezza informatica legate a DDoS, ransomware, violazione di app mobili e furto di identità.

Telecomunicazioni

Protezione delle risorse di una grande holding composta da una società di telecomunicazioni, un provider di servizi cloud, uno sviluppatore di giochi e la sede centrale.

Come ottenere ancora di più da KIPS

È possibile completare l'esperienza KIPS con il corso **Formazione per il management**, incluso nel portfolio Security Awareness di Kaspersky. Questo corso di formazione per il management può essere seguito prima o dopo aver svolto gli scenari KIPS, in base all'approccio alla Security Awareness. Potenziate la vostra esperienza KIPS scoprendo cosa significa l'attuale panorama delle minacce per la vostra azienda, quali azioni intraprendere in caso di attacco informatico, oltre a una serie di altre informazioni interessanti, pertinenti e utili. Il corso di formazione per il management è disponibile in due formati: tramite un workshop interattivo offline o un corso online.

Che cosa dicono gli utenti e i clienti KIPS sul gioco

Kaspersky Industrial Protection Simulation è stato davvero fondamentale e dovrebbe diventare obbligatorio per tutti gli esperti di sicurezza.

Warwick Ashford,
Computer Weekly

Al CERN abbiamo un numero enorme di sistemi di progettazione e IT, a cui lavorano migliaia di persone. Proprio per questo, l'aumento della consapevolezza e il coinvolgimento delle persone nella gestione della cybersecurity sono essenziali per la sicurezza informatica. La formazione di Kaspersky si è dimostrata coinvolgente, efficiente ed efficace.

Stefan Luders,
CERN CISO

È stato veramente importante e alcuni partecipanti hanno chiesto di usare il gioco anche nelle loro aziende.

Joe Weiss PE,
CISM, CRISC, membro ISA

Dobbiamo costruire una rete di persone basata sull'affiliazione e la cooperazione, e KIPS offre la soluzione perfetta per farlo.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, Repubblica Ceca

Come prepararsi per una sessione KIPS

Pianificazione: organizzare KIPS come evento separato o come sessione all'interno di un seminario/conferenza/evento esistente (in questo caso, il momento ottimale per proporre una sessione KIPS è la sera della prima giornata).

Gruppo: 20-100 persone, divise in gruppi di 3-4 partecipanti. In teoria, ogni squadra deve essere formata da personale amministrativo, tecnici e responsabili della sicurezza IT/CISO:

- Se possibile, includere almeno un rappresentante di ogni ruolo/funzione.
- Le squadre possono essere costituite da persone provenienti dalla stessa azienda/dipartimento oppure da aziende/dipartimenti diversi.
- Non è importante che i partecipanti si conoscano.

Configurazione: il gioco richiede 1,5-2 ore, ma la stanza deve essere a disposizione dei trainer di Kaspersky 2 ore prima dell'inizio, per la preparazione e la configurazione.

Stanza: circa 3 m2 a persona, senza colonne, apparecchiature AV standard: proiettore (6-8 lumen), schermo, sistema audio (altoparlanti, controllo remoto, microfoni).

Wi-Fi con accesso a Internet (per l'accesso al server di gioco KIPS) a 4 Mbps per gli iPad con supporto Wi-Fi o altri tablet delle singole squadre (4 persone).

Attrezzatura: tavoli da 4 persone per i partecipanti (forma rettangolare non inferiore a 75 x 180 cm oppure rotonda con diametro di almeno 1,5 m). I partecipanti devono sedersi ai tavoli in gruppi di 4. Tavoli per i trainer, sedie per tutti i partecipanti.

Riferimenti e case study

Allo sviluppo del gioco KIPS hanno partecipato esperti di sicurezza industriale provenienti da oltre 50 Paesi.

- Il gioco è stato tradotto in inglese, russo, tedesco, francese, giapponese, spagnolo (Europa), spagnolo (America latina), portoghese, turco, italiano, cinese, olandese e arabo.
- KIPS è utilizzato da numerose agenzie governative, tra cui CyberSecurity Malaysia, l'NSA della Repubblica Ceca e il Cyber Security Centrum dei Paesi Bassi, per aumentare il livello di consapevolezza per centinaia di esperti all'interno di organizzazioni nazionali responsabili di infrastrutture critiche
- KIPS è concesso in licenza da importanti autorità che si occupano di istruzione come il SANS Institute, dove viene utilizzato nella formazione degli studenti SANS in tutto il mondo
- KIPS è concesso in licenza da fornitori e vendor di servizi di sicurezza, tra cui Mitsubishi-Hitachi Power Systems, dove viene utilizzato nella formazione per i clienti di infrastrutture critiche
- KIPS fa parte del progetto Geiger della Commissione Europea per formare e proteggere le piccole e micro imprese dalle minacce informatiche e migliorare la loro gestione della privacy

Sessioni "Train-The-Trainer" disponibili

Se un cliente desidera utilizzare KIPS per la formazione di un pubblico più vasto (un maggior numero di dipendenti, manager ed esperti di più dipartimenti o sedi), può essere utile acquistare la licenza per la formazione KIPS, formare trainer interni e organizzare sessioni KIPS in base ai tempi e alle esigenze del cliente.

Questo tipo di licenza include:

- Il diritto a utilizzare internamente il programma di formazione KIPS.
- Il materiale formativo e il diritto a usarlo/riprodurlo.
- Nome utente/password per il server del software KIPS per tutta la durata della licenza.
- Manuale del trainer e formazione sulla gestione del programma KIPS rivolta ai responsabili.
- Manutenzione e supporto (aggiornamenti e supporto per il software KIPS e i contenuti formativi).
- Personalizzazione opzionale degli scenari KIPS (costo supplementare).

KIPS per i partner e i centri di formazione

KIPS offre ai partner una grande opportunità per trarre vantaggio dalle soluzioni di Security Awareness in vari modi. Non solo possono venderlo come prodotto, ma possono anche proporlo ai clienti del loro centro di formazione o persino condurre sessioni in autonomia. Gli specialisti della formazione di Kaspersky possono fornire assistenza per migliorare le competenze dei partner per la formazione, se scelgono tale opzione.

Kaspersky Security Awareness

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 in ogni livello dell'organizzazione

Il nostro corso di formazione basato sulla gamification garantisce il coinvolgimento e la motivazione dell'edutainment, mentre le piattaforme di apprendimento aiutano a interiorizzare le competenze di cybersecurity, per assicurare che le nozioni apprese non vadano perse nel tempo.

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

Poiché le modifiche comportamentali sostenibili richiedono tempo, il nostro approccio si basa sulla creazione di un ciclo di apprendimento continuo, che include 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.

Ciclo di apprendimento continuo

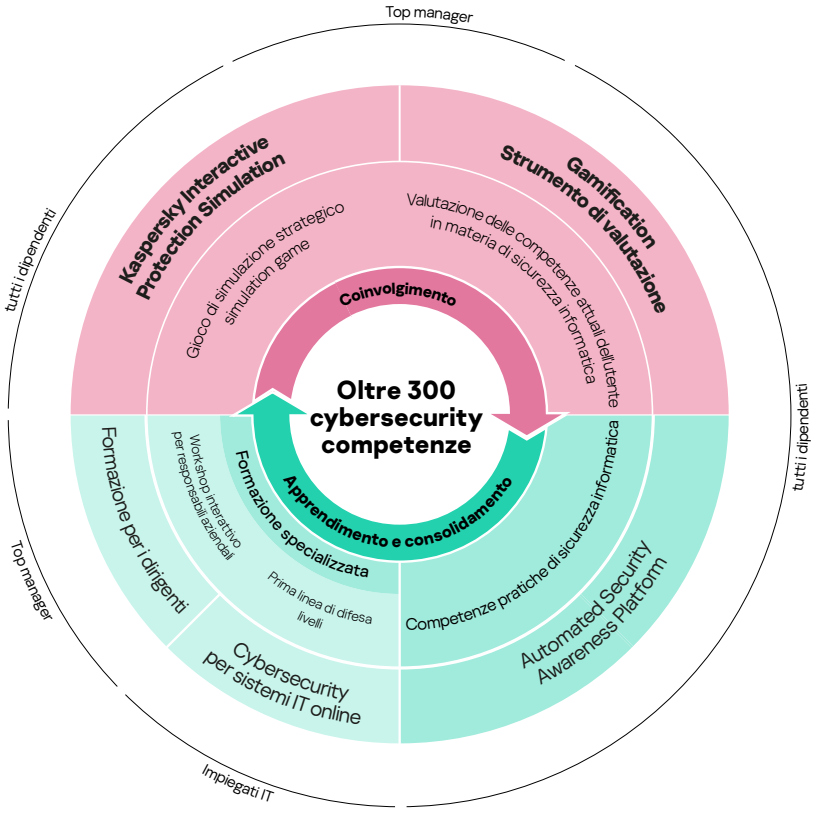
Coinvolgimento / motivazione
- Perché ne ho bisogno?
- Cognizione

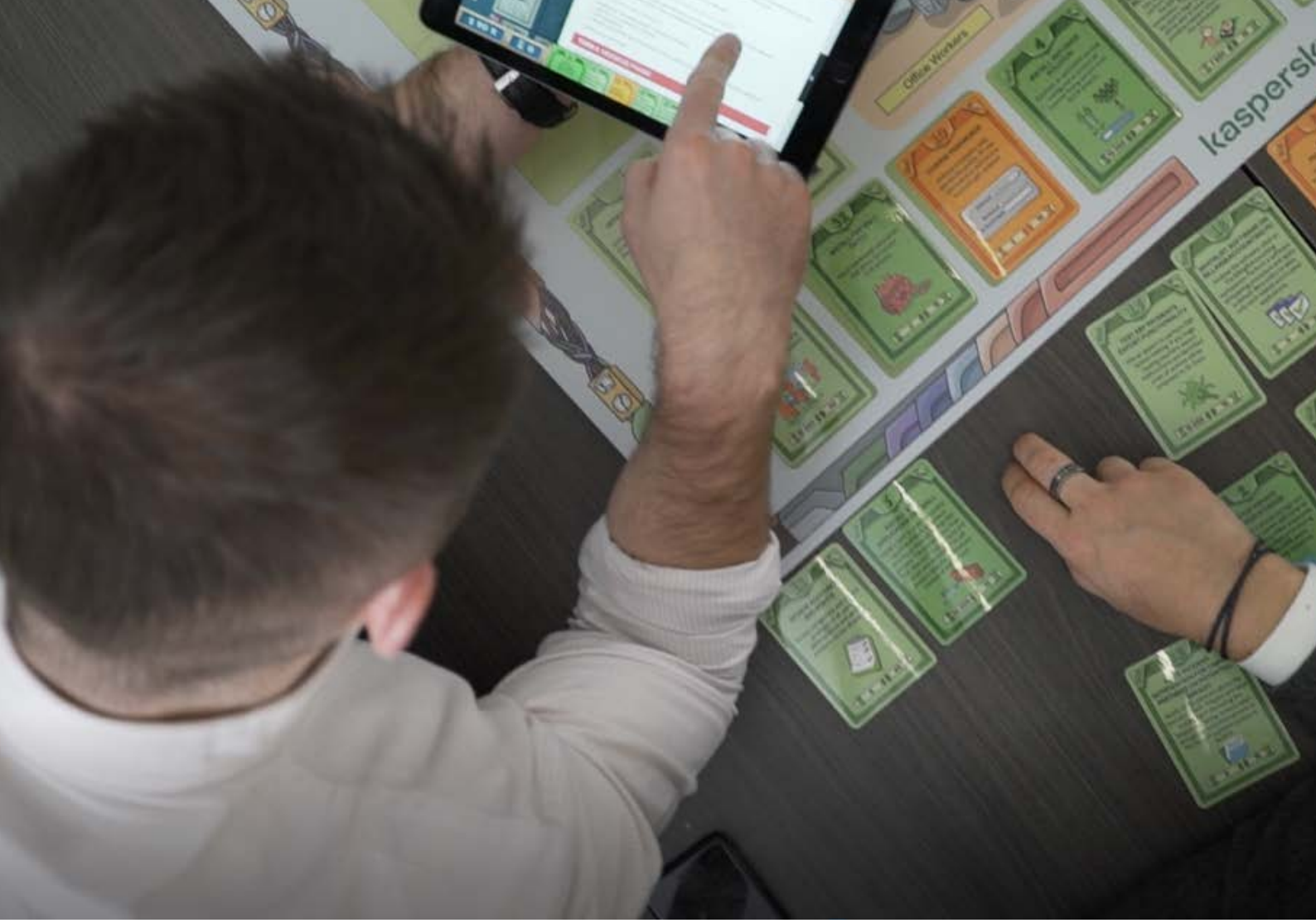
Punto di partenza
- Sono consapevole?
- Cosa so e dove sono le falle?

Apprendimento
- Micro apprendimento
- Apprendimento continuo
- Adattabilità

Consolidamento
- Ho capito bene?
- Me lo ricordo ancora?
- Ho agito conformemente?

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





Enterprise Cybersecurity: www.kaspersky.it/enterprise-security
Kaspersky Security Awareness: www.kaspersky.it/awareness

www.kaspersky.it

kaspersky