Formazione dedicata alla risposta agli incidenti per il personale IT generico

Cybersecurity for IT Online

Prova gratuita
cito.kaspersky.com

kaspersky bring on the future

Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online (CITO)

Corso di formazione interattivo rivolto al personale IT generico al fine di costruire solide competenze in termini di cybersicurezza e risposta agli incidenti

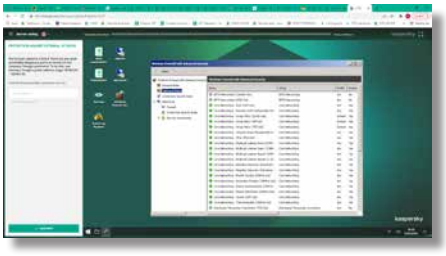
Di fatto, non è possibile adottare un efficace approccio aziendale alla Cybersecurity senza offrire una formazione sistematica a tutti i dipendenti coinvolti.
La maggior parte delle aziende fornisce corsi di formazione su due livelli ben distinti: formazione per specialisti, riservato ai team di sicurezza IT, e Security Awareness per i dipendenti non IT. Kaspersky offre un set completo di prodotti per entrambi i livelli. Ma cosa manca? Per i team IT, i service desk e le altre categorie di personale con competenze tecniche avanzate, i programmi di awareness standard non sono sufficienti. Tuttavia, a queste figure non è richiesto di diventare esperti di cybersicurezza. Sarebbe infatti un'operazione eccessivamente dispendiosa in termini di tempo e risorse.

Modalità di formazione

I corsi di formazione sono interamente online. I partecipanti hanno bisogno solo dell'accesso a Internet e del browser Chrome nel PC. Ciascuno dei 6 moduli è costituito da una breve panoramica teorica, seguita da consigli pratici e 4-10 esercizi, che trattano competenze specifiche e consentono di imparare a utilizzare il software e gli strumenti di sicurezza IT durante il lavoro quotidiano.

Il piano di formazione è pensato per essere distribuito e completato nel corso di un anno. Il tasso di avanzamento consigliato è di 1 esercizio a settimana e il completamento di ogni esercizio richiede dai 5 ai 45 minuti.

La versione corrente della formazione è rivolta all'ambiente aziendale Windows.



Metodo di erogazione dei corsi di formazione:
Formato SCORM o cloud

Prima linea di risposta agli incidenti

Kaspersky propone il primo corso di formazione online sul mercato dedicato ai professionisti IT generici che operano in ambiente aziendale. Si tratta di un corso composto da 6 moduli*:

- Software dannoso
- Programmi e file potenzialmente indesiderati
- Concetti di base sulle investigation
- Phishing incident response
- Sicurezza dei server
- Sicurezza con Active Directory

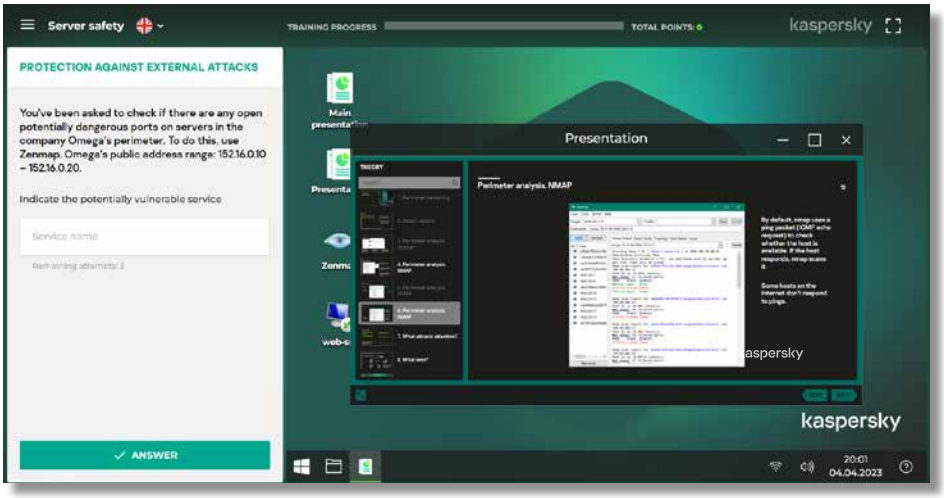
Il programma di formazione fornisce ai professionisti IT competenze pratiche per riconoscere un possibile scenario di attacco in un incidente apparentemente innocuo e su come raccogliere i dati relativi a un incidente affinché vengano gestiti dal personale di sicurezza IT. Sviluppa inoltre la capacità di ricerca degli indicatori di attività dannose, consolidando il ruolo di tutti i membri del team IT come prima linea di difesa per la sicurezza.

Perché la formazione CITO è efficace?

- Interattiva: la stimolazione di processi reali senza rischi per il computer
- Crea competenze e conoscenze con un apprendimento pratico
- Processo di apprendimento intuitivo: navigazione pratica e suggerimenti
- Tratta tutti i principali problemi e argomenti di sicurezza IT che lo staff IT generico riscontra durante le attività

Processo di apprendimento

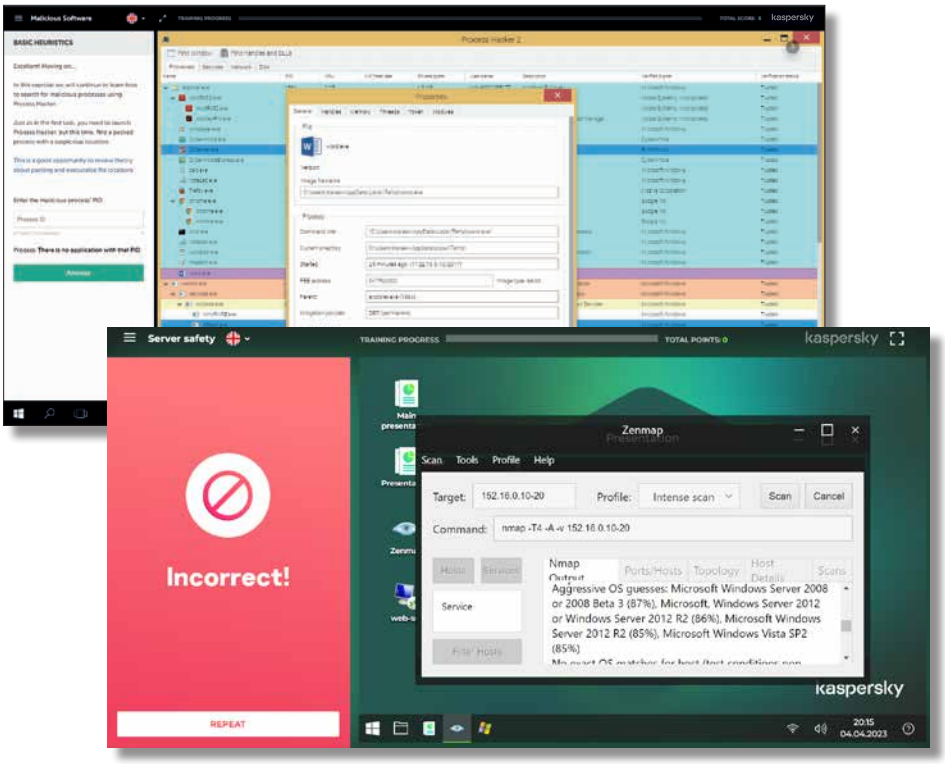
Ogni blocco di esercizi di apprendimento è composto da due parti: parte teorica e parte pratica, con attività che simulano i processi reali relativi alle spiegazioni precedenti.



* per l'elenco più recente degli argomenti fai clic su cito.kaspersky.com

Al termine della lezione, completa l'attività

Se l'hai completata correttamente, verrai reindirizzato alla sezione di esercizi successiva, in caso contrario, potrai usare i suggerimenti o rileggere il materiale della lezione.

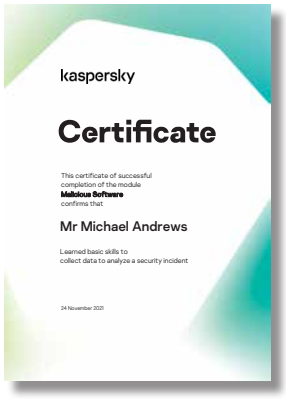


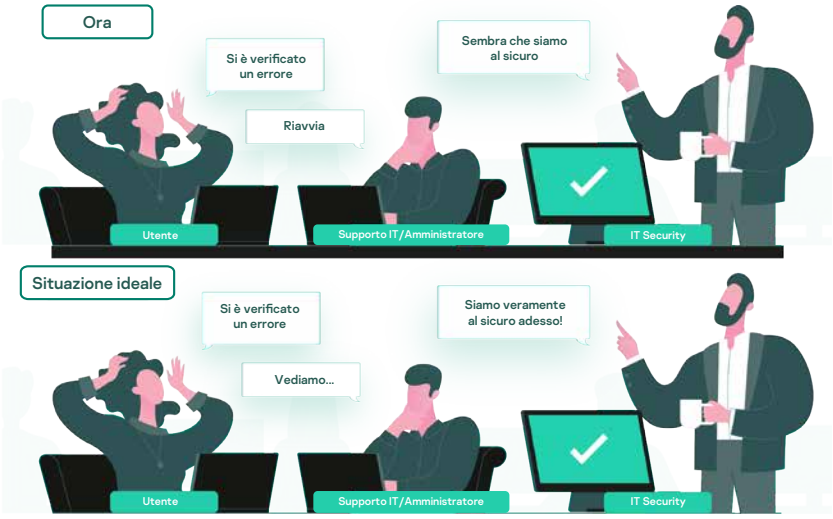
A chi è destinata questa formazione?

Questa formazione è consigliata a tutti gli esperti IT all'interno della vostra organizzazione, in particolare agli addetti ai service desk e agli amministratori di sistema. Tuttavia, il corso è utile anche alla maggior parte dei membri dei team non specializzati in sicurezza IT.

Certificati

Al termine di ciascun modulo i dipendenti riceveranno certificati personali

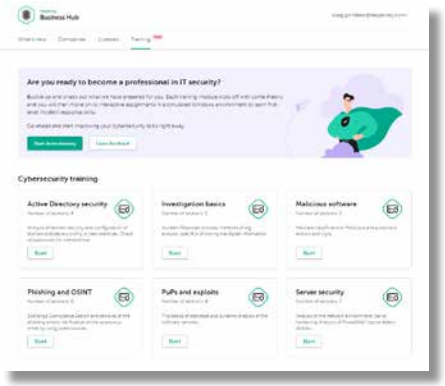




Argomenti e risultati della formazione

Nome del modulo	Target di riferimento	Conoscenze acquisite	Atteggiamento personale	Competenze acquisite	Esercitazione pratica nell'ambito del modulo
Software dannoso	Utenti con diritti di amministratore su server e/o workstation	Tecniche e classificazione del malware Azioni e sintomi di software dannoso e sospetto Concetti di base sull'analisi euristica	Il malware può trovarsi ovunque nel computer Il malware può sottrarre i dati in vari modi È obbligatorio segnalare tutti i potenziali incidenti sospetti al team di sicurezza	Verifica dell'esistenza o dell'assenza di un incidente correlato al malware	Utilizzo degli strumenti ProcessHacker, Autoruns, Fiddler e Gmer per il rilevamento del malware

Nome del modulo	Target di riferimento	Conoscenze acquisite	Atteggiamento personale	Competenze acquisite	Esercitazione pratica nell'ambito del modulo
File e programmi potenzialmente indesiderati (PuP)	Utenti autorizzati a installare software aggiuntivo e utenti che valutano o aprono file ricevuti dall'esterno	Concetti di base sull'analisi statistica e dinamica di campioni di software e documenti sospetti	I documenti (PDF, docx) possono contenere exploit I file privi di firma possono contenere malware o riskware Tutti i file eseguibili privi di firma devono essere verificati per controllare la presenza di possibili infezioni Una firma digitale non garantisce che il file non contenga funzionalità dannose	Utilizzo dei sistemi di monitoraggio degli eventi relativi al sistema e alla sandbox Uso di motori statistici Rimozione dei programmi PuP	Analisi statica (firma) e statistica (virustotal) dei campioni di software Utilizzo di procmon per la ricerca di exploit e di comportamenti dannosi del software Analisi dei file con il sandbox Cuckoo Creazione di script per la rimozione del malware tramite AVZ
Concetti di base sulle investigation	Dipendenti IT che partecipano ad attività di analisi forense o di risposta agli incidenti gestite dal team di sicurezza	Il processo di risposta agli incidenti Metodi per l'analisi dei log Specifiche per l'archiviazione delle informazioni digitali	Se si sospetta un incidente di cybersicurezza, occorre segnalarlo immediatamente al team di sicurezza e raccogliere prove digitali L'analisi deve essere eseguita con la collaborazione e sotto la supervisione del team di sicurezza	Raccolta di prove digitali Analisi del traffico con NetFlow Analisi della timeline Analisi del registro eventi	Raccolta dei dati dalla memoria volatile e non volatile (FTK-imager) Analisi dei log per scoprire l'origine e i collegamenti dell'attacco (eventlogexplorer) Analisi dei movimenti laterali tramite NetFlow (ntop) Analisi del disco tramite Autopsy
Phishing and Open Source Intelligence (OSINT)	Dipendenti IT che partecipano ad attività forensi o di incident response	Moderni metodi di phishing Metodi di analisi per le intestazioni e-mail	Il phishing può essere molto sofisticato e, quindi, difficilmente rilevabile, ma non può mai sfuggire alla ricerca manuale Le e-mail di phishing devono essere eliminate dalle caselle di posta degli utenti	Analisi ed eliminazione delle e-mail di phishing dalle caselle di posta degli utenti Intelligence open-source per determinare quello che gli hacker sanno sulla vostra azienda	Ricerca e rimozione delle e-mail di phishing nelle cassette postali di Exchange Utilizzo di Recon-ng per la ricognizione del web
Sicurezza dei server	Amministratori server	Analisi dell'ambiente di rete Hardening dei server Analisi dei log PowerShell per rilevare gli attacchi	La compromissione del perimetro di rete è uno dei maggiori vettori di attacco. Rimuovere tutte le vulnerabilità è impossibile, pertanto è necessario ridurre la superficie di attacco per ostacolare il più possibile gli attacchi. Questa strategia consente quanto meno di guadagnare tempo per il rilevamento.	Ricerca di servizi di rete vulnerabili e non standard Configurazione dei sistemi in base al principio "Default Deny" Ricerca degli indicatori di attacco nei log PowerShell	Utilizzo di Nmap per il rilevamento dei servizi di rete vulnerabili Configurazione di Criteri restrizione software per il controllo dei programmi e di Windows Firewall per il controllo di rete Analisi degli eventi utilizzando Event Log Explorer
Sicurezza con Active Directory	Amministratori Active Directory	Utilizzo di un'API per verificare le password in un database di password compromesse Configurazione dei criteri dei domini in base ai suggerimenti Metodi per l'analisi della sicurezza dei domini Active Directory	La configurazione Active Directory predefinita non è ottimale dal punto di vista della sicurezza. L'autore dell'attacco può elevare i privilegi in diversi modi. Analisi dei suggerimenti di sicurezza, utilizzo degli strumenti che offrono migliore visibilità per Active Directory	Verifica sicura degli hash delle password in un database Ricerca delle incoerenze tra i criteri dei domini effettivi e consigliati Valutazione della sicurezza delle impostazioni Active Directory	Utilizzo dell'API Have I Been Pwned? per effettuare ricerche nel database delle password compromesse Utilizzo di Policy Analyzer per confrontare i criteri di dominio attuali con le best practice Utilizzo dei report Ping Castle



Integrazione con Kaspersky Endpoint Security Cloud

Potenzia le tue capacità di cybersecurity e ottieni il massimo dai prodotti specializzati per la sicurezza informatica con la formazione CITO, disponibile per gli utenti di KES Cloud Pro direttamente dal Business Hub.

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

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.

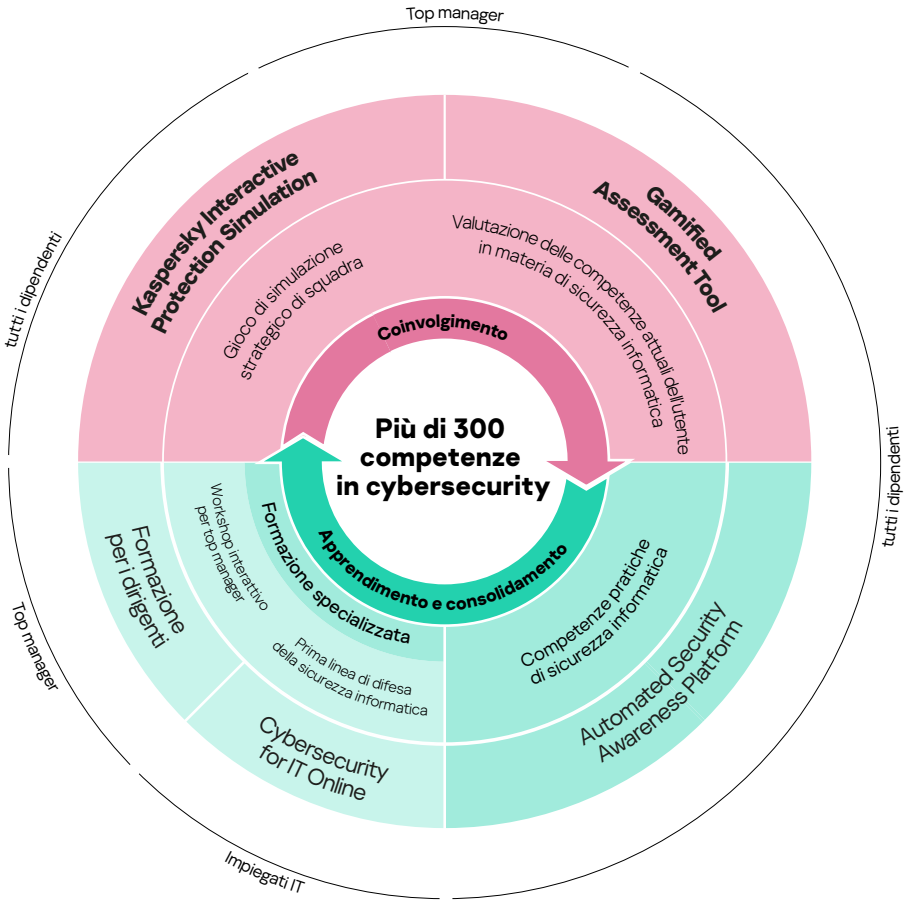
Il portfolio offre interessanti prodotti di formazione che promuovono una maggiore consapevolezza in merito alle problematiche della cybersecurity tra i dipendenti a tutti i livelli, consentendo loro di contribuire alla sicurezza informatica complessiva dell'organizzazione.

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.

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 cybersicurezza, per assicurare che le nozioni apprese non vadano perse nel tempo.



Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.it/awareness
Kaspersky Cybersecurity for IT Online: cito.kaspersky.com

www.kaspersky.it

kaspersky bring on the future