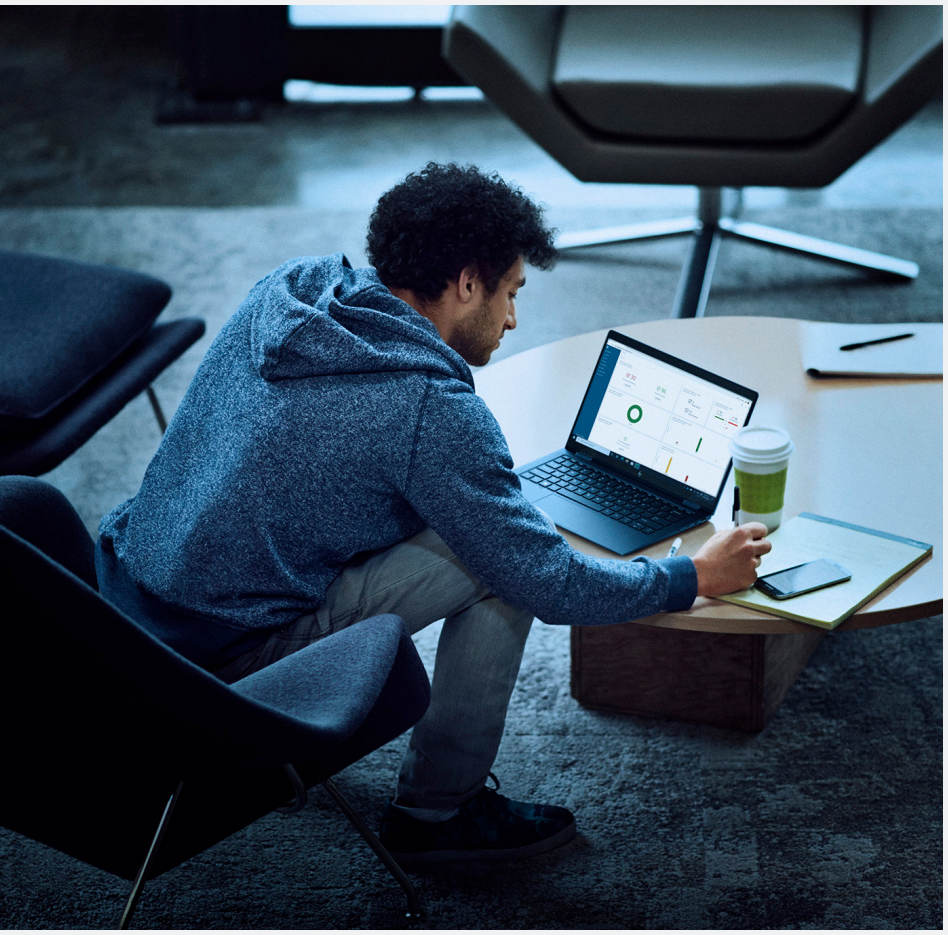
PER CONTRASTARE GLI HACKER SERVONO I TALENTI GIUSTI:

SCOPRITE COME UTILIZZARE RAFFORZARE LE CAPACITÀ DI CYBERSICUREZZA DEL VOSTRO TEAM

LE AZIENDE SI TROVANO AD AFFRONTARE UNA CARENZA GLOBALE DI TALENTI IT. COSA FARE PER AUMENTARE LA PRODUTTIVITÀ DELLA VOSTRA FORZA LAVORO?



L’85%

DELLE AZIENDE SEGNALA UNA CARENZA DI COMPETENZE IN MATERIA DI CYBERSICUREZZA[2]

La criminalità informatica è sempre più presente nelle prime pagine dei giornali. Giorno dopo giorno, nuove minacce alla sicurezza creano problemi per i professionisti IT di tutto il mondo.

E non si tratta di problemi da poco. Il costo medio di una violazione è di $8,7 milioni negli Stati Uniti e di $3,86 milioni a livello globale. Se si aggiungono i numerosi endpoint remoti coinvolti negli attuali ambienti di lavoro ibrido, i costi aumentano ulteriormente.

Le perdite sono i mancati ricavi derivanti dalle interruzioni dei sistemi, ma anche effetti difficili da quantificare, come la perdita di business e il duro lavoro necessario per acquisire nuovi clienti a seguito di un danno di immagine.[1]

La soluzione più ovvia per rispondere a questi rischi sembrerebbe quella di assumere più specialisti per proteggere l‘azienda. Tuttavia, è proprio la carenza di personale qualificato a rappresentare un problema di sicurezza oggi.

È una situazione che riguarda l’intero settore. A livello globale, mancano più di 3 milioni di esperti.[3] Nonostante gli attacchi in aumento e l’85% delle organizzazioni che segnalano una carenza di competenze in materia di sicurezza informatica,[2] le assunzioni sono in calo.[3]

HP WOLF SECURITY

LE MINACCE SONO IN CRESCITA

102 MILIONI
DI NUOVE MINACCE MALWARE OGNI MESE[4]

IL 60%
DELLE AZIENDE È STATO COLPITO DA ATTACCHI ORIGINATI DAI DIPENDENTI[5]

+58%
DI ATTACCHI DI PHISHING NELL'ULTIMO ANNO[5]

+63%
DI CAMPAGNE DI PHISHING E POST FAKE SUI SOCIAL MEDIA RELATIVI AL COVID-19[6]

COSTO MEDIO DI UNA VIOLAZIONE DI DATI:[1]

PER CONTRASTARE GLI HACKER SERVONO I TALENTI GIUSTI

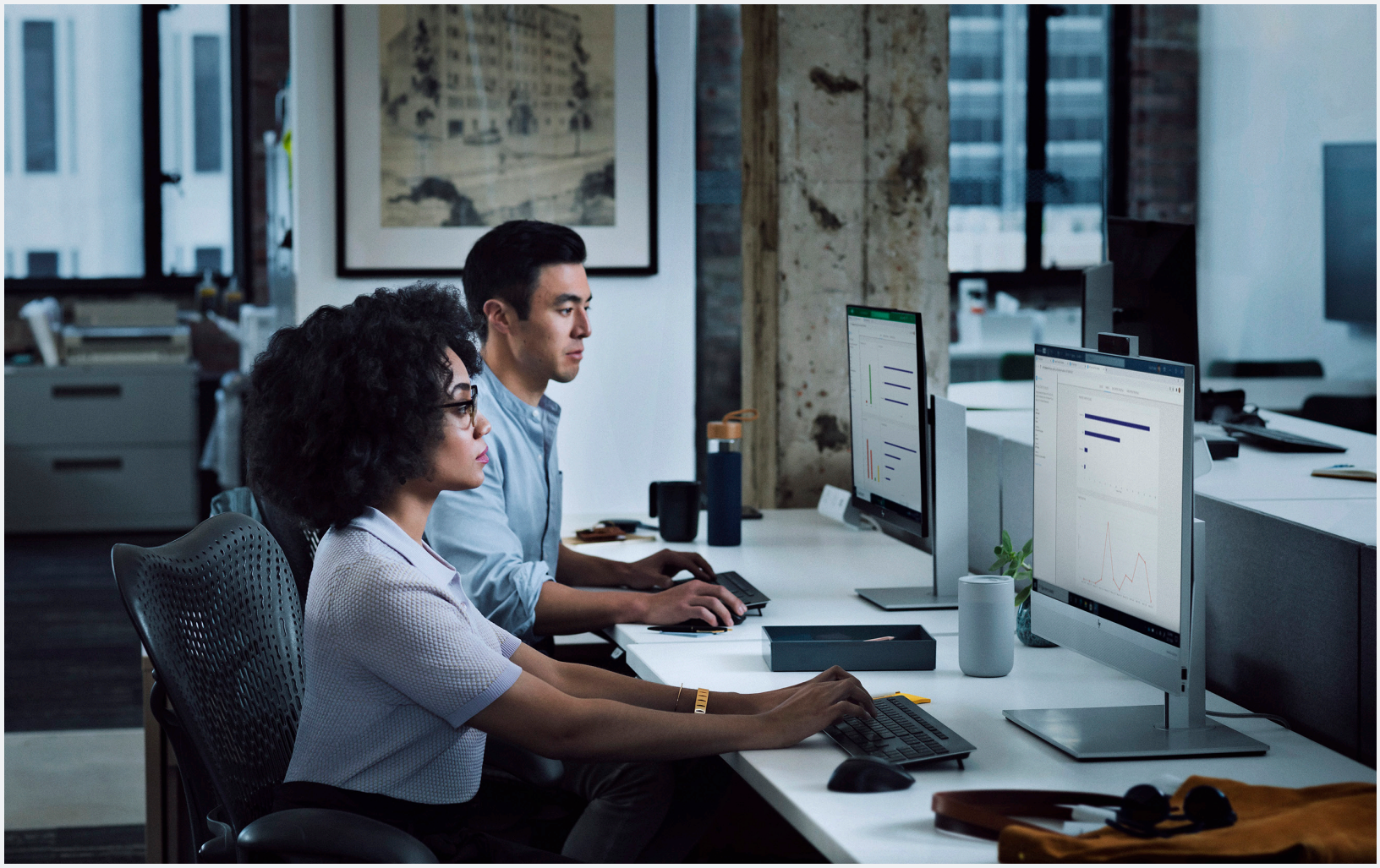
PERCHÉ È DIFFICILE CREARE UN POOL DI ESPERTI DI CYBERSICUREZZA

Le competenze di cybersicurezza sono molto specifiche, e non tutti i percorsi di formazione IT dedicano particolare attenzione a questa tematica. Istituti e università stanno lavorando per colmare questa lacuna, ma la preparazione della prossima generazione di talenti richiede tempo. Secondo Cybercrime Magazine, negli Stati Uniti, solo il 3% dei laureati ha competenze legate alla cybersicurezza.

James Hadley, fondatore e CEO di Immersive Labs, afferma che è necessario un maggiore impegno nel promuovere le professionalità possibili in questo campo.

“La maggior parte dei paesi sviluppati sta avviando una serie di iniziative per aumentare le persone attratte da una prospettiva di carriera nella cybersicurezza, a partire dai primi anni della scuola”, afferma Hadley. „La cybersicurezza non è hacking. Il problema è proprio questo: l‘esperto di cybersicurezza è spesso descritto come hacker, e in questo modo è difficile attrarre nuovi talenti, specialmente le donne. Bisogna fare di più per eliminare lo squilibrio di genere”.

Nel frattempo, ecco alcune opzioni pratiche per le aziende alla ricerca di talenti.



PER CONTRASTARE GLI HACKER SERVONO I TALENTI GIUSTI

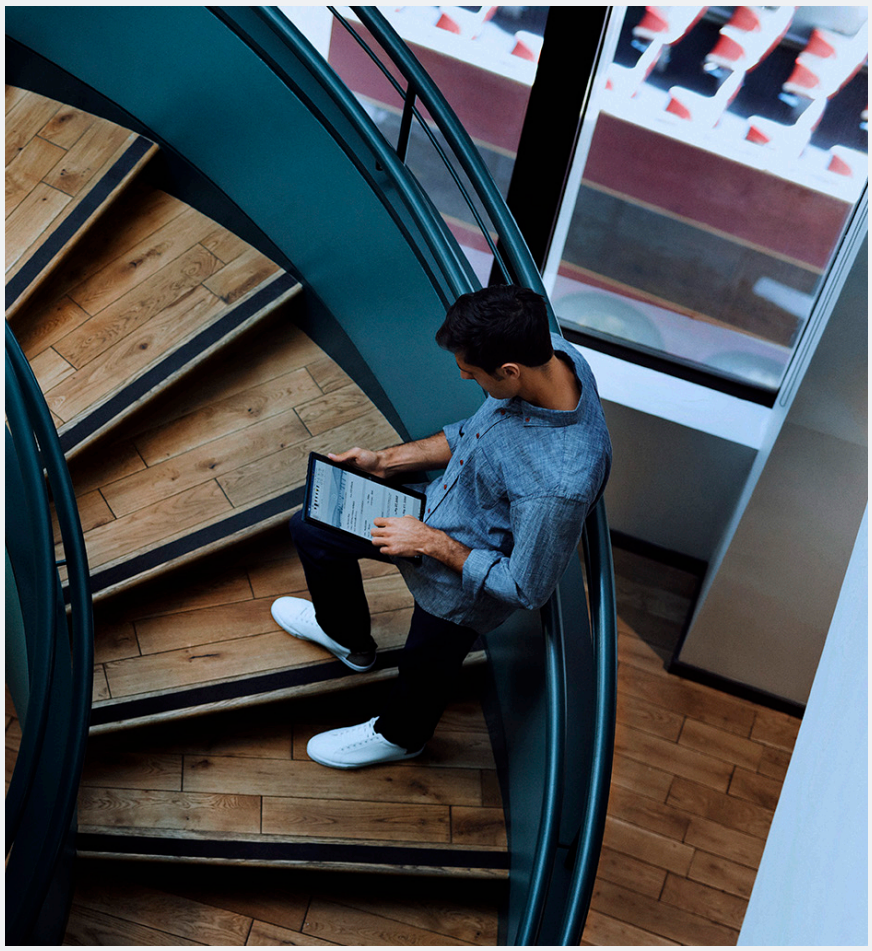
VALORIZZATE I TALENTI DI CUI DISPONETE

SONO QUALITÀ COME IL PENSIERO ANALITICO, LA CAPACITÀ DI RISOLUZIONE DEI PROBLEMI E LA PERSEVERANZA CHE CONTANO.

Non trascurate una fonte naturale di talenti: i vostri dipendenti attuali, che possono essere formati su competenze difficili da trovare, come la cybersicurezza. Fate emergere il loro potenziale nascosto e fateli crescere, assegnando loro nuove responsabilità.

Hadley sottolinea che il background accademico ha poca influenza sul potenziale di un individuo: „sono qualità come il pensiero analitico, la capacità di risoluzione dei problemi e la perseveranza che contano“, spiega. „Se una persona possiede questi attributi, è un buon candidato per la cybersicurezza.“

Ma ci sono anche altri vantaggi. Una nuova formazione aiuta i dipendenti a focalizzarsi più attentamente sugli obiettivi aziendali. Inoltre, una formazione pagata dal datore di lavoro genera fidelizzazione:[8] coinvolge i dipendenti che mirano a crescere professionalmente.



AUTOMAZIONE E ANALYTICS

Un altro modo per consentire ai vostri attuali team IT di contrastare gli attacchi informatici, anche se le loro competenze in fatto di cybersicurezza sono limitate, è quello di dotarsi di soluzioni tecnologiche complete e sempre attive. Lasciate che l'automazione faccia il lavoro pesante, consentendo così ai vostri tecnici di dedicarsi alle attività più strategiche per il vostro business.

Le aziende che hanno adottato tecnologie di intelligenza artificiale, machine learning e analytics nella loro strategia di sicurezza subiscono perdite di gran lunga inferiori a chi è rimasto indietro. Il costo medio di una violazione nelle aziende che hanno automatizzato la sicurezza è stato di $2,45 milioni, rispetto ai $6,03 milioni delle aziende senza automazione.[1] Non c'è da meravigliarsi, quindi, se il 43% delle aziende afferma di preferire queste soluzioni di sicurezza IT più avanzate.

Le soluzioni che utilizzano la gestione centralizzata basata su cloud consentono ai team IT di vedere e controllare ciò che accade a livello della sicurezza dei dispositivi, dalle nozioni di base alle metriche più avanzate. L'associazione di protezioni sempre attive con una migliore visualizzazione dei dati semplifica l'identificazione dei punti deboli, il contenimento delle violazioni e la valutazione dei rischi relativi a hardware e patch obsoleti.

HP TECHPULSE[9] AIUTA I PROFESSIONISTI IT A SVILUPPARE NUOVE COMPETENZE

ACQUISITE LE COMPETENZE DI CYBERSICUREZZA CHE MANCANO ALLA VOSTRA AZIENDA AFFIDANDOVI AL SERVIZIO DI SICUREZZA DEGLI ENDPOINT PIÙ AVANZATO[10]

Con HP, potete difendere i vostri dispositivi e al contempo sviluppare nuove competenze IT. HP Wolf Pro Security Service[11,12] offre alle piccole e medie imprese una protezione da grande azienda, senza la necessità di possedere competenze interne.

UNA GESTIONE DELLA SICUREZZA DEGLI ENDPOINT COMPLETA, SENZA COMPLICAZIONI:

- Livelli di protezione progettati per le esigenze degli enti governativi, e avanzate funzionalità antivirus basate sull'intelligenza artificiale[13,14], per garantire la sicurezza dei vostri dati, credenziali e dispositivi aziendali.
- Informazioni tempestive e strategiche sul vostro parco dispositivi, inclusi i tentativi di attacco e le potenziali minacce, tramite un'unica dashboard basata su cloud.
- La competenza in materia di sicurezza informatica[15] viene fornita come servizio, in modo che i vostri team IT interni possano sviluppare e maturare nuove conoscenze.

NON SOTTOVALUTATE I RISCHI: ASSICURATEVI LE GIUSTE COMPETENZE.

Scoprite di più su HP Wolf Pro Security Service

I servizi HP sono disciplinati dai termini e dalle condizioni di servizio HP forniti o indicati al cliente al momento dell'acquisto. Il cliente potrebbe disporre di ulteriori diritti legali a seconda delle leggi locali vigenti; tali diritti non sono in alcun modo alterati dai termini e dalle condizioni di servizio HP o dalla Garanzia limitata HP fornita con il prodotto HP.

HP WOLF SECURITY

1. 15th Annual 2020 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute, luglio 2020

2. CyberEdge 2020 Cyberthreat Defense Report, marzo 2020

3. (ISC)² Cybersecurity Workforce Study, aprile 28, 2019

4. AV-Test SECURITY REPORT 2019/2020, 26 agosto 2020

5. Mimecast The State of Email Security 2020, giugno 2020

6. The Impact of the COVID-19 Pandemic on Cybersecurity, ISSA, 30 luglio 2020

7. https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

8. https://applied.economist.com/articles/a-route-map-for-retraining-workers

9. HP TechPulse è una piattaforma di telemetria e analisi che fornisce dati critici su dispositivi e applicazioni e non viene venduta come servizio autonomo. La piattaforma HP TechPulse rispetta i rigorosi requisiti del GDPR in materia di privacy ed è certificata in base agli standard ISO27001, ISO27701, ISO27017 e SOC2 Type2 per la sicurezza delle informazioni. È necessario l'accesso a Internet, con connessione al portale TechPulse. Per i requisiti di sistema completi, visitare il sito hpdaas.com/requirements.

10. Sulla base dell'analisi interna di HP dei servizi di sicurezza degli endpoint basati su deep learning e protetti con isolamento, inclusi SaaS e servizi gestiti. Straordinariamente sicuro sulla base dell'isolamento delle applicazioni e sulla protezione degli endpoint con deep learning su PC Windows 10 a Luglio 2020.

11. HP Security ora è HP Wolf Security. Le funzionalità di sicurezza variano a seconda della piattaforma; per maggiori dettagli, consultare la scheda tecnica dei prodotti.

12. HP Wolf Pro Security Service è venduto separatamente. Per i requisiti completi del sistema, consultare http://www.hpdaas.com/requirements. I servizi HP sono disciplinati dai termini e dalle condizioni di servizio applicabili di HP, forniti o indicati al cliente al momento dell'acquisto. Il cliente potrebbe disporre di ulteriori diritti a seconda delle leggi locali vigenti; tali diritti non sono in alcun modo alterati dai termini e dalle condizioni di servizio HP o dalla Garanzia limitata HP fornita con il prodotto HP. Per i requisiti di sistema completi, visitare il sito www.hpdaas.com/.

13. HP Sure Click è disponibile in PC HP selezionati e richiede Windows 10. Per i dettagli completi, consultare https://bit.ly/2PrLT6A_SureClick.

14. La funzionalità HP Sure Sense è disponibile solo su PC HP selezionati e non è disponibile con Windows10 Home.

15. I Security Expert sono disponibili solo con il piano Proactive Security Enhanced.

4AA7-3855ENW, Rev 1, Aprile 2021