BDO

Varuhi kibernetske varnosti

Mesec kibernetske varnosti

Pomanjkanje človeških virov za zagotavljanje kibernetske varnosti in umetna inteligenca (UI)

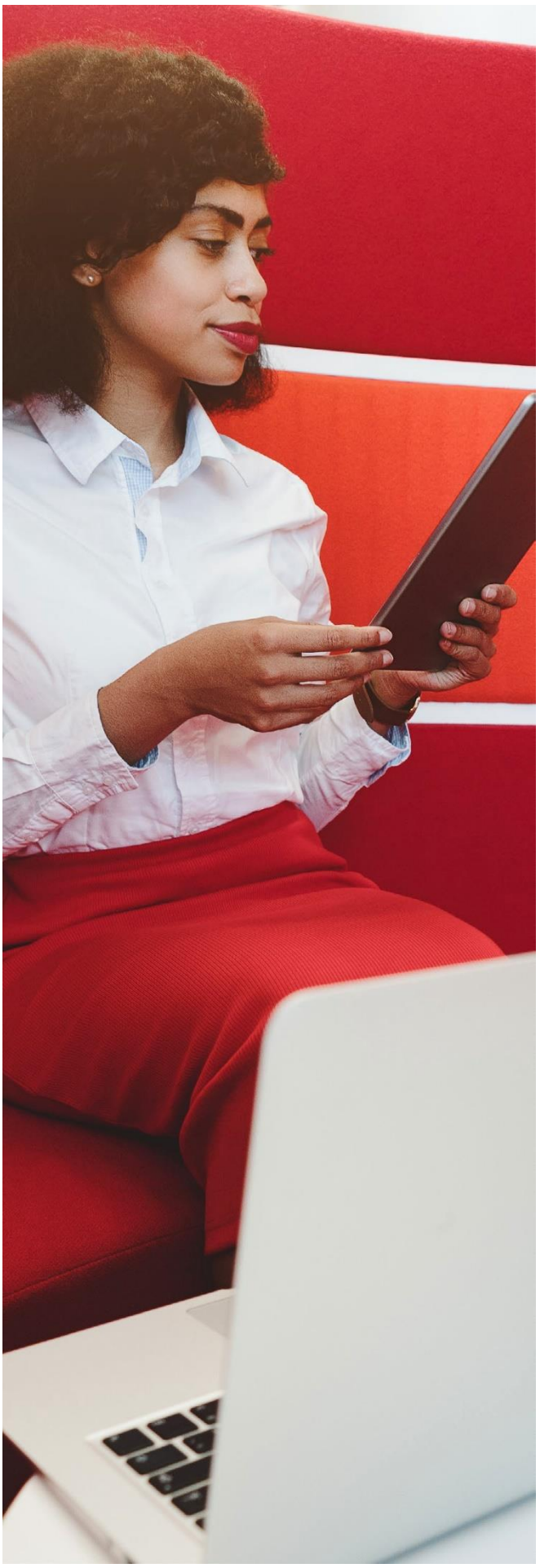
Pomanjkanje človeških virov za zagotavljanje kibernetske varnosti in umetna inteligenca (UI)

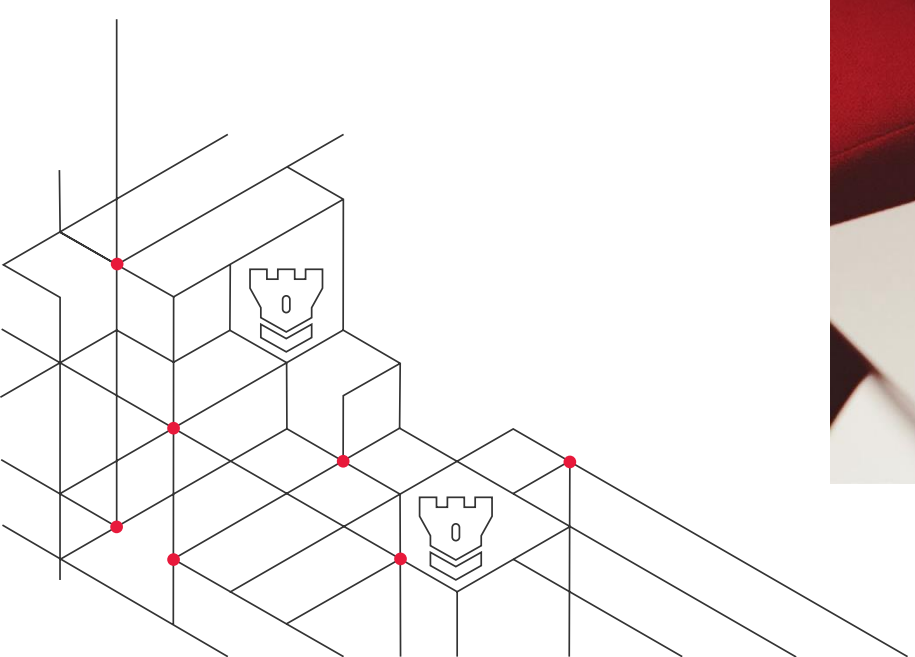
V dobi, ko digitalna preobrazba spreminja svet, se soočamo s pomembnim izzivom: vse večjim razkorakom med organizacijami, ki so na nasprotnih koncih spektra kibernetske odpornosti. Pomemben prispevek k tej vrzeli prispeva pomanjkanje usposobljenih strokovnjakov za kibernetsko varnost. Ker se obseg, hitrost in zahtevnost kibernetskih groženj še naprej povečujejo, organizacije težko učinkovito zavarujejo svoj hitro rastoči digitalni odtis. Pomanjkanje človeških virov za obvladovanje kibernetskih tveganj, pospešeno uvajanje novih tehnologij in nenehno spreminjajoče se okolje groženj predstavljajo veliko tveganje za vse organizacije, ki uporabljajo tehnologijo po vsem svetu.

Septembra 2024 je Mednarodni konzorcij za certificiranje varnosti informacijskih sistemov (ISC) izvedel študijo, ki opozarja na vse večje pomanjkanje zaposlenih na področju kibernetske varnosti. Študija je pokazala, da na svetu primanjkuje 4,8 milijona kibernetskih strokovnjakov, ki so potrebni za učinkovito varovanje organizacij. ISC navaja, da se je ta vrzel znatno povečala, saj ocenjuje, da se je ta v letu 2024 v primerjavi s preteklim letom povečala za 19 %.

> “Študija ISC o kibernetski varnosti poudarja zaskrbljujoče mnenje strokovnjakov za kibernetsko varnost. Po dveh letih upadanja naložb v zaposlovanje in možnosti strokovnega razvoja se organizacije zdaj soočajo s precejšnjim pomanjkanjem znanja in spretnosti ter kadrov. Gre za problem, ki povečuje splošno tveganje na področju informacijske varnosti" je dejal izvršni podpredsednik ISC za korporativne zadeve Andy Woolnough.
> "V času, ko globalna nestabilnost in nove tehnologije, kot je umetna inteligenca, hitro povečujejo število groženj, so naložbe v razvoj znanj in spretnosti ter novo generacijo kibernetske delovne sile še pomembnejše kot kdaj koli prej. To bo strokovnjakom za kibernetsko varnost omogočilo, da se spopadejo s izzivi na tem področju v prihodnosti in poskrbijo za varnost naših sredstev”

Pomanjkanje kibernetskih talentov je posledica pomanjkanja kakovostnega usposabljanja in izobraževanja zaposlenih v organizacijah. Pomanjkanje finančnih sredstev pa pogosto predstavlja težave pri ohranjanju usposobljenega kadra s tega področja. K zapletenosti prispeva tudi zahtevna vloga strokovnjakov za kibernetsko varnost, ki se pogosto spopadajo z omejenim proračunom, ki upočasnjuje napredek, velikim številom zahtevkov in stalnimi zahtevami organizacije. Obeti se zdijo mračni in če se ne popravijo, bodo imeli dolgoročne posledice za organizacije vseh velikosti. Osredotočiti se moramo na dve področji. Prvo in najbolj očitno je razviti vire, ki jih že imamo v naših organizacijah, ter jim zagotoviti izkušnje in sposobnosti, ki jih potrebujejo, da nam pomagajo pri varovanju naših sredstev. Druga naloga je izkoriščanje novejših in naprednejših tehnoloških zmogljivosti, ki tem posameznikom pomagajo, da sledijo povečanemu obsegu dela, tako da se oni sami osredotočijo na kompleksne naloge, medtem ko s pomočjo tehnologije opravljajo manj zahtevne naloge. Medtem ko se spopadamo s pomanjkanjem človeških virov se sodobne rešitve, kot sta umetna inteligenca (UI) in avtomatizacija, pojavljata kot ključna dejavnika za zapolnitev te vrzeli in zaščito naših sistemov.

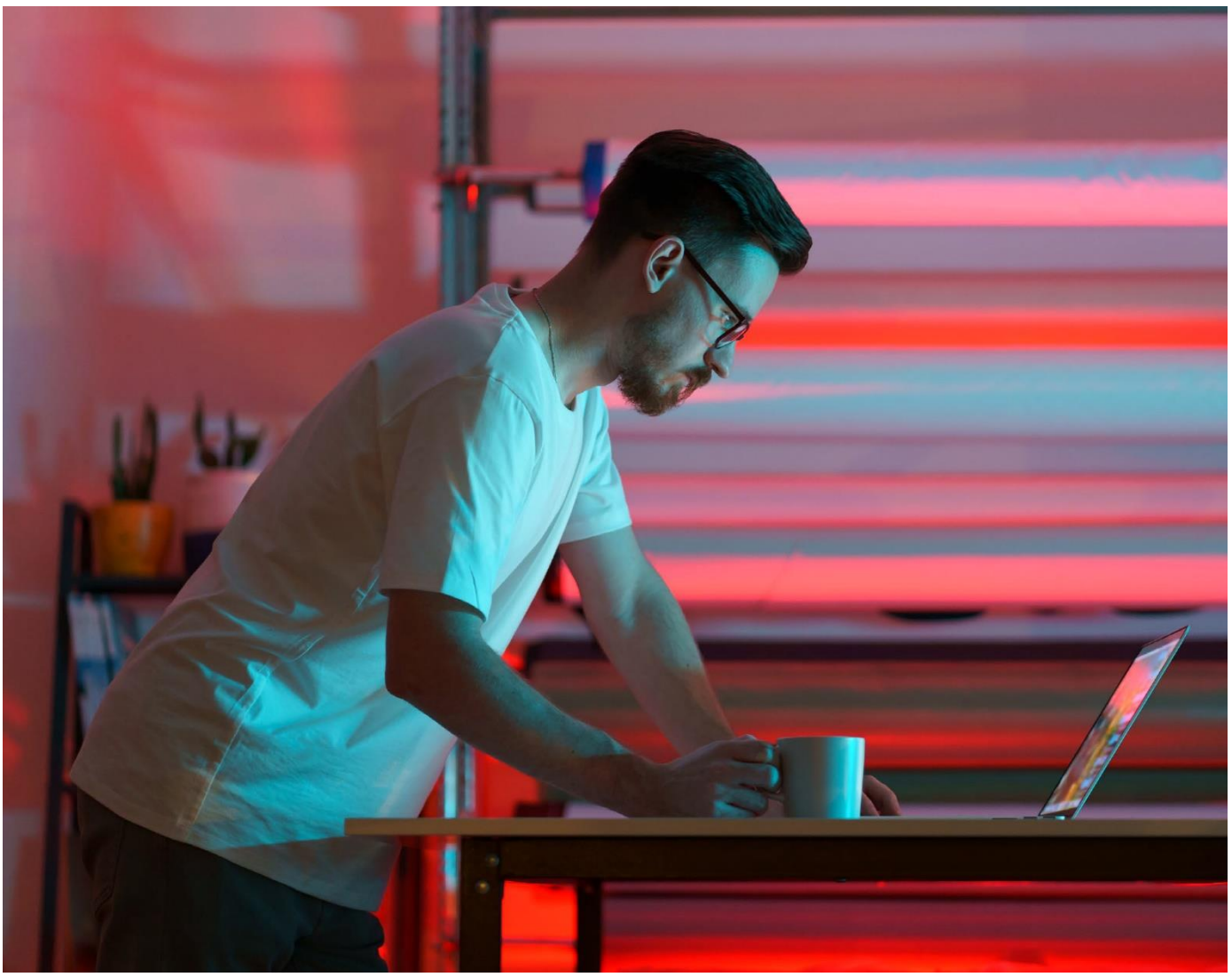




Obseg pomanjkanja človeških virov za zagotavljanje kibernetske varnosti

Trenutna vrzel v znanju s področja kibernetske varnosti predstavlja velik izziv - izziv, ki ga je treba rešiti, saj je bistvo le tega hitrost tehnoloških sprememb. Industrija 4.0 nam je omogočila nove načine dela, sodelovanja in avtomatizacije, za katere si nismo mislili, da so mogoči. Z vsakim tehnološkim razvojem se pojavi eksponentno več možnosti novih napadov, saj napadalci iščejo slabosti v sistemih in uporabljajo prefinjene taktike, da bi pridobili dostop do teh nenehno spreminjajočih se tehnoloških sredstev. Nenehni razvoj zahteva delovno silo za kibernetsko varnost, ki je usposobljena za tradicionalna temeljna varnostna načela, hkrati pa je sposobna ostati dovolj okretna, da se prilagodi novim tehnologijam in sodobnim metodam zaščite.

Zaradi hitrosti poslovnega in tehnološkega razvoja je strokovnjakom za kibernetsko varnost težko slediti tempu, še posebej na trgu, kjer je prisotno pomanjkanje nadarjenih kadrov. Poleg tega so napadalci vedno več korakov pred njimi. Zato je treba nenehno skrbeti za izobraževanje, stalno učenje strokovnjakov na tem področju o sodobnih metodah zagotavljanja kibernetske varnosti. Ključno je osredotočanje na zaposlovanje talentov z akademskimi in praktičnimi izkušnjami.



UI: pomoč pri zagotavljanju kibernetske varnosti

Razvoj tehnologije je tudi spodbuda za ekipe, ki skrbijo za zagotavljanje kibernetske varnosti. Kot priložnost za boj proti pomanjkanju talentov, umetna inteligenca in avtomatizacija ponujata priložnost za bolj trajnosten in učinkovit program kibernetske varnosti. Umetna inteligenca ne bo nadomestila človeškega strokovnega znanja, vendar jo je mogoče uporabiti kot učinkovito sredstvo, ki bo povečalo človeška prizadevanja, omogočila ljudem, da bodo lahko držali korak z napredkom, in organizacijam omogočilo, da z manj sredstvi naredijo več.

Umetna inteligenca in strojno učenje z velikimi jezikovnimi modeli analizirata velike količine podatkov z veliko hitrostjo, z zmožnostjo iskanja vzorcev in opozarjanja na tveganja v skoraj realnem času. Tako lahko posameznike, ki upravljajo s kibernetsko varnostjo, seznanite z največjimi tveganji, da se lahko osredotočijo na bolj zapletene primere. Tradicionalna orodja za kibernetsko varnost, ki temeljijo na znanih vzorcih, se pogosto zanašajo na binarno logiko in skoraj vedno ustvarjajo nezadovoljstvo in odvračajo pozornost strokovnjakov za kibernetsko varnost. Sistemi umetne inteligence se lahko učijo iz podatkov, vzorcev. Ti sistemi se prilagodijo tako, da opozorijo na zadeve, ki so najpomembnejše za analizo s strani človeških virov. Ne glede na to, ali se uporabljajo za prepoznavanje novih in nenavadnih vzorcev vedenja ali za prepoznavanje neznanega vedenja, ki posnema vedenje, ki je najpogostejše pri kibernetskem napadu, te tehnologije bistveno povečujejo sposobnost organizacije, da se odzove na nove grožnje. Takšne grožnje bi sicer ostale neopažene z običajnimi sistemi, kar pomaga osebju, ki v organizaciji skrbi za kibernetsko varnost, hitrejše odkrivanje vzrokov in hitrejše zmanjševanje groženj z manj človeškimi viri. Prednost umetne inteligence, ki obvladuje ponavljajoče se aktivnosti, je učinkovit način, da naredite več z istimi viri. Njena najpomembnejša vrednost pa je v tem, da lahko dopolnjuje in nadgrajuje človeško strokovno znanje. Umetna inteligenca ne more nadomestiti dolgoletnih izkušenj ter institucionalnega in kontekstualnega znanja, ki ga zagotavljajo strokovnjaki za kibernetsko varnost. Vendar bo sodelovanje med človeško in umetno inteligenco prineslo veliko bolj odporno strategijo kibernetske obrambe in bolj odporno organizacijo.

Priložnosti za povečanje učinkovitosti z umetno inteligenco

V okviru upravljanja kibernetskih tveganj je veliko področij, na katerih lahko storitve umetne inteligence dopolnjujejo znanja, ki jih zagotavljajo ljudje. V nadaljevanju so navedeni primeri storitev umetne inteligence, ki jih je mogoče uporabiti:

Odkrivanje groženj

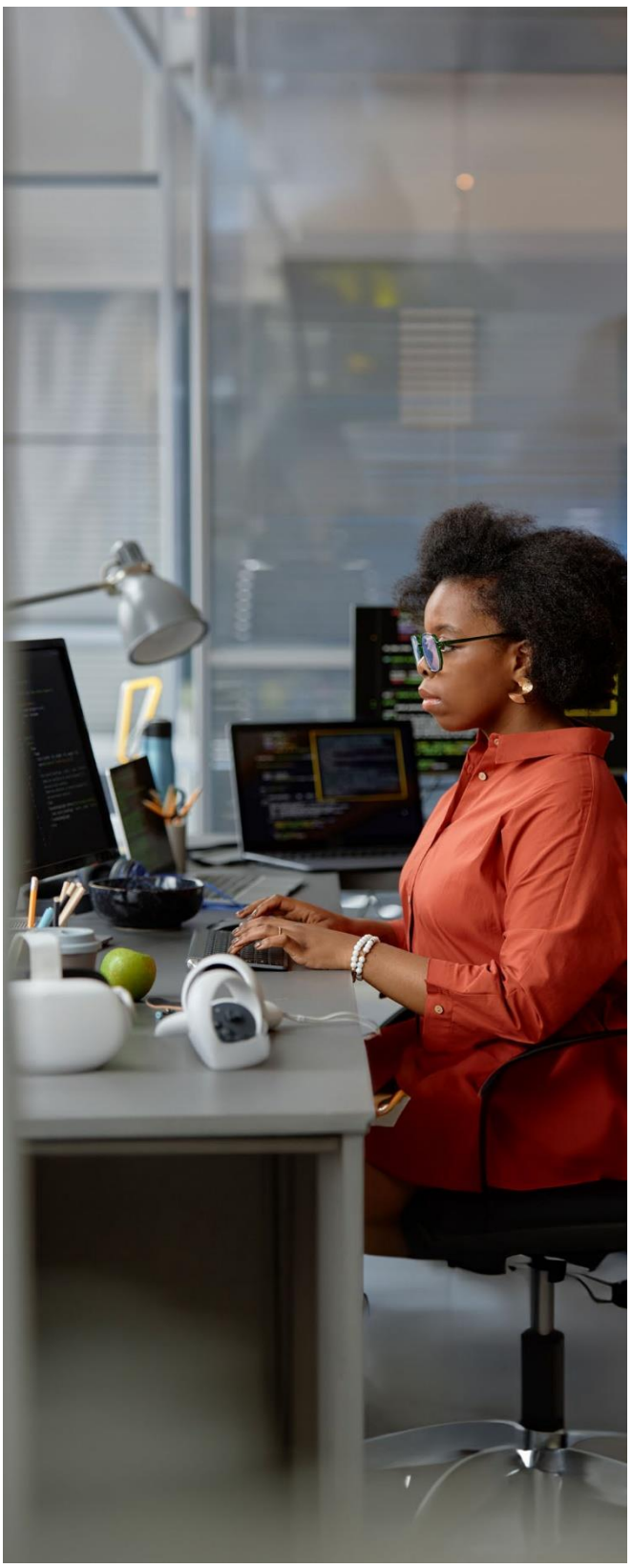
Umetna inteligenca je lahko neverjetno učinkovito in natančno orodje za spremljanje omrežne dejavnosti, saj s pomočjo hevristike in strojnega učenja omogoča iskanje naprednih kibernetskih groženj in prepoznavanje neobičajnih vzorcev v prometu. Te storitve, ki jih poganja umetna inteligenca, lahko prevzamejo "težko delo" pri analizi omrežja in forenziki, kar omogoča odkrivanje groženj skoraj v realnem času in varnostnim analitikom omogoča pridobivanje pomembnih koreliranih podatkov.

Upravljanje ranljivosti

VM platforme, ki jih poganja umetna inteligenca, se lahko uporabijo za zagotavljanje podatkov in poročil, ki omogočajo natančen vpogled v varnostni položaj organizacije. Ta orodja uporabljajo zmogljivosti za dejansko preizkušanje možnosti izkoriščanja ranljivosti, kar organizaciji omogoča, da prednostno razvrsti prizadevanja za odpravo pomanjkljivosti na podlagi dejanskega tveganja s pomočjo kompenzacijskih kontrol.

Odziv na incidente

Orodja umetne inteligence lahko opravijo začetne faze odzivanja na incidente s samodejno identifikacijo in obvladovanja ugotovljenih groženj. Z njihovo pomočjo se lahko skrajša čas, potreben za odzivanje na grožnje, ekipe za kibernetsko varnost pa imajo na voljo več časa, da se lahko osredotočijo na dejavnosti za odpravljanje napak.



Zaključek: Zapolnitev vrzeli s sodelovanjem

Pomanjkanje človeških virov, ki skrbijo za kibernetsko varnost na svetovni ravni, je zaskrbljujoč izziv, ki ogroža trajnost našega digitalnega ekosistema. Z uporabo umetne inteligence, avtomatizacije in sodobnih izobraževalnih tehnik bomo uspešni pri krepitvi kibernetskih talentov in povečanju obstoječe delovne sile, da bi organizacijam omogočili učinkovitejše povečevanje njihovih prizadevanj za varnost.

Čeprav lahko umetna inteligenca bistveno pripomore pri prevzemanju rutinskih nalog, bodo človeški viri vedno potrebni za zagotavljanje konteksta, ustvarjalnosti in strateškega razmišljanja. Skupaj bodo premostili prepad.