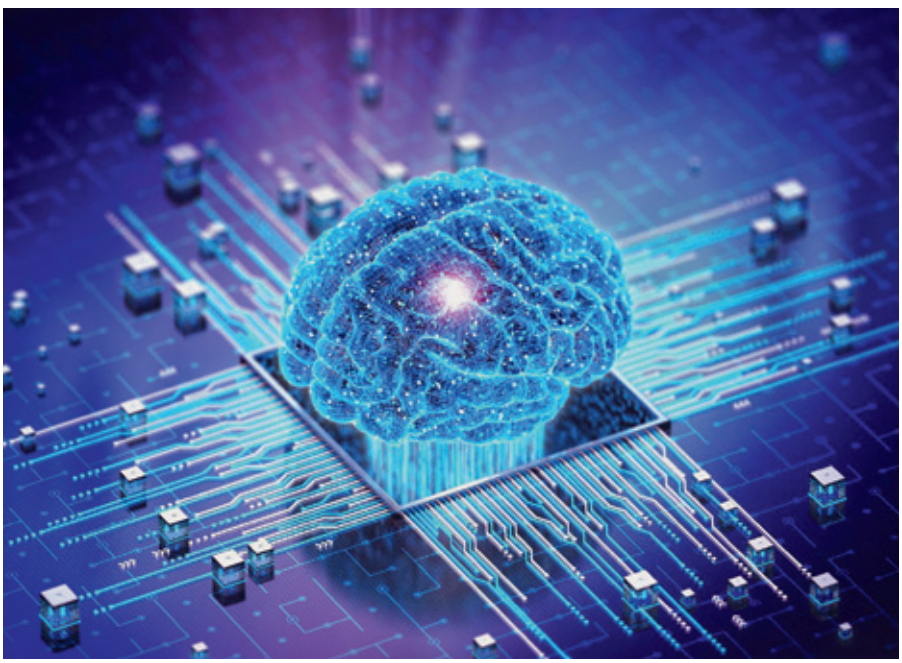
Umělá inteligence v kybernetické bezpečnosti

Co myslíte, může samotná automatizace zabezpečit vaši organizaci? V minulosti, ale i dnes lidé věří, že budoucnosti budou dominovat plně autonomní roboti pohánějící svět, zatímco lidé budou odpočívat u bazénu.



V současnosti je ale tato utopická vize strojově řízené společnosti spíše fikcí než realitou. Přílišné spoléhání se na stroje jako například v seriálu Rodina Smolíkova má daleko k vytvoření dokonalé společnosti a mohlo by nás zavést na cestu připomínající dystopickou budoucnost zobrazenou v animovaném WallE. V tomto filmu je lidstvo líčeno tak, že ztratilo svou kreativitu, nezávislost a kritické myšlení, stalo se samolibým a závislým na technologii. To je ostré varování před tím, co se stane, když lidé přenechají příliš mnoho kontroly automatizaci.

Navzdory obavám a rizikům spojeným s generativní umělou inteligencí představují tyto technologie pro organizace také příležitost, jak posílit obranu kybernetické bezpečnosti a podpořit své často přetížené týmy kybernetické bezpečnosti. Vzhledem ke stále rostoucímu objemu a složitosti kybernetických hrozeb mohou nástroje poháněné umělou inteligencí pomoci bezpečnostním týmům automatizovat rutinní a opakující se bezpečnostní úkoly, což umožní analytikům soustředit se na kritičtější aspekty jejich práce a zlepšit provozní efektivitu.

Umělá inteligence transformuje kybernetickou bezpečnost na obou stranách

Generativní nástroje umělé inteligence (AI), jako je ChatGPT a další, umožňují kyberzločincům škálovat a automatizovat své útoky v míře, která dříve nebyla možná. Dokonce i začínající kyberzločinci mohou tyto nástroje používat k usnadnění psaní škodlivého kódu nebo k řešení problémů s dosavadními kmeny malwaru, aby odstranili případné nedostatky a zvýšili jejich účinnost.

Ačkoli ChatGPT má zavedena určitá ochranná opatření, která uživatelům brání v generování malwaru nebo jiného obsahu pro nekalé účely, bezpečnostní analytici společnosti Bitdefender zjistili, že tato ochranná opatření lze se správnými technikami a znalostmi poměrně snadno obejít. Využitím nástrojů generativní umělé inteligence k zefektivnění vývoje malwaru a automatizaci distribuce svých útoků mohou skupiny kyberzločinců zvýšit jejich četnost a rozprostřít širší síť, aby se zaměřily na více potenciálních obětí.

Zachovat lidský faktor v bezpečnostním řešení je zásadní pro udržení připravenosti

Tesla může být schopna řídit sama, ale k jejímu zapojení je stále zapotřebí člověk. Totéž lze říci o kybernetické bezpečnosti. AI dokáže bezpečnostním analytikům ubrat spoustu těžké práce, ale součástí bezpečnosti musí být vždy člověk, který tyto nástroje neustále trénuje, aktualizuje a monitoruje. Je důležité si uvědomit, že umělá inteligence je pouze nástroj, jehož účelem je rozšířit lidské činnosti.

To také znamená, že AI je jen tak dobrá, jak dobrá jsou data, která do ní lidé vkládají.

Jednotná platforma pro kybernetickou bezpečnost

Naštěstí existuje nástroj, který vám pomůže spravovat vaše schopnosti AI a udržovat vaše bezpečnostní nástroje podle aktuálních zásad a chování. Řešení Bitdefender Extended Detection and Response (XDR) poskytují inventarizaci IT aktiv a jejich chování v reálném čase, stejně jako aktuální hodnocení hrozeb a potenciálních zranitelností organizace.

Díky více než 480 patentům z oblastí, jako jsou strojové učení a umělá inteligence, které komponuje do svých produktů, dokáže řešení XDR zpracovat a analyzovat velké objemy bezpečnostních dat a poskytovat doporučení pro odstranění bezpečnostních mezer a nápravu dopadů útoků. I díky zapojení AI a ML do bezpečnostních systémů je Bitdefender lídrem v kyberbezpečnosti.

Bitdefender začleňuje umělou inteligenci a strojové učení do svých řešení kybernetické bezpečnosti již od roku 2008. Například Bitdefender GravityZone eXtended Detection and Response (XDR) využívá ML technologie ke korelaci a analýze obrovského množství bezpečnostních dat z různých senzorů a zdrojů v rámci celé organizace. GravityZone Incident Advisor pak prezentuje výsledky v lidsky čitelném formátu, který umožňuje bezpečnostním profesionálům rychle přijmout doporučená opatření.

Ale i XDR je jen nástroj, i když vysoce inteligentní, který však potřebuje člověka, aby jej aplikoval tím nejvhodnějším a optimálním způsobem.