Umelá inteligencia v spoločnosti ESET

Juraj Jánošík, viceprezident spoločnosti ESET pre umelú inteligenciu
Ondrej Kubovič, špecialista spoločnosti ESET na digitálnu bezpečnosť
Filip Mazán, senior manažér spoločnosti ESET pre AI výskum
Kamil Pšenák, senior produktový manažér spoločnosti ESET pre AI

Cybersecurity
Progress. Protected.

ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava,
Slovenská republika; tel. č: +421 2 322 44 111,
fax: +421 2 322 44 109, www.eset.sk

Umelá inteligencia v spoločnosti ESET

Juraj Jánošík, Ondrej Kubovič, Filip Mazán a Kamil Pšenák

Prvé vydanie vydané v Slovenskej republike v 2. kvartáli 2026

Prvý raz predstavené na konferencii ESET World 2026 v Berlíne | 19. – 20. máj 2026

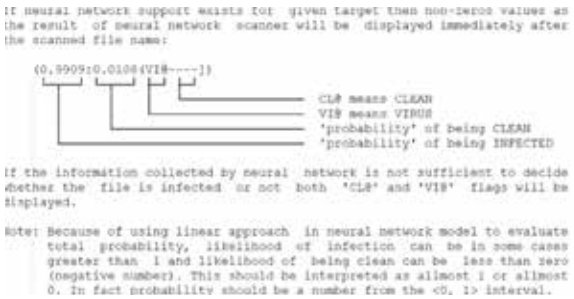
Spoločnosť ESET počas celej svojej histórie dokazuje, že zodpovedná inovácia – najmä v oblasti nových a rýchlo sa rozvíjajúcich technológií, ako sú strojové učenie a umelá inteligencia (AI) – je vo sfére kybernetickej bezpečnosti nielen možná, ale aj nevyhnutná.

Od roku 1997, keď odborníci spoločnosti ESET uskutočnili svoje prvé experimenty s využitím neurónových sietí na detekciu hrozieb, sa ich prístup vyznačoval premysleným začlenením týchto technológií. Počnúc prvými verziami až po dnešné pokročilé systémy sa výskum a vývoj spoločnosti ESET opiera o dôkladné vedecké testovanie, drobnohľad a dôraz na bezpečnosť používateľov, ako aj praktický prínos.

Strojové učenie ešte predtým, než sa stalo populárnym

Cesta spoločnosti ESET v oblasti umelej inteligencie začala už v roku **1997**, kedy sa zamerala na zlepšenie **detekcie makrovírusov**, ako aj na testovanie a overenie, či algoritmy strojového učenia môžu prispieť k lepšej ochrane jej zákazníkov.

Obrázok 1: Výsledky spracovania vzoriek prostredníctvom viacvrstvového detekčného jadra a nástrojov detekcie vrátane vzoriek, ktoré boli neurónovými sieťami (NEURAL PATTERN), ako aj inými vlastnými detekčnými technológiami, identifikované ako „vírus“.



Obrázok 2: Úryvok z príručky k heuristickému skeneru makrovírusov využívajúcemu neurónové siete.

V rámci prelomového roku **2005** spoločnosť ESET nasadila svoju **technológiu detekcie na úrovni DNA**. Extrahovaním kľúčových charakteristík – „génov“ potenciálne škodlivých vzoriek – vytvorili inžinieri spoločnosti ESET všeobecné profily DNA, ktoré sa stali základom pre presné rozlišovanie neškodných a škodlivých súborov a umožnili detekciu doposiaľ neznámych hrozieb s podobnými vlastnosťami, ktoré sa začali objavovať v nasledujúcich rokoch.

Tento proces, pravidelne aktualizovaný automatizovanými systémami aj výskumníkmi, sa stal flexibilnou, adaptívnou a, čo je najdôležitejšie, bezpečnou vrstvou ochrany.

Zdieľanie expertízy: **automatizácia a výskum hrozieb**

V očakávaní nárastu hrozieb, ktoré sa budú snažiť využívať potenciál strojového učenia – dnes bežne označovaného ako umelá inteligencia (AI) – spoločnosť ESET rozšírila využívanie tejto technológie s cieľom dosiahnuť vyššiu výkonnosť v reálnych podmienkach.

Od roku **2006** sú **odborné backendové systémy** založené na strojovom učení kľúčovou súčasťou spracúvania, triedenia, označovania a detekcie rastúceho množstva vzoriek – ich počet sa zvýšil z desiatok tisíc jedinečných vzoriek analyzovaných denne na súčasnú úroveň 750 000.

Tieto backendové systémy podporované umelou inteligenciou odbremenili bezpečnostných expertov spoločnosti ESET, vďaka čomu sa dnes môžu viac sústrediť na výskum tých najzaujímavejších zo vznikajúcich hrozieb namiesto riešenia zdĺhavých a repetetívnych úloh. Zhromaždené informácie o hrozbách položili základy pre vývoj nových pokročilých ochranných technológií, ktoré spoločnosti pomáhajú riešiť konkrétne vektory útokov ešte aj dnes.

Vývoj a spustenie cloudového reputačného systému **ESET LiveGrid®** v roku **2010** viedlo k ďalšiemu zlepšeniu v oblasti detekcie a reakcie. Vďaka osvojeniu online učenia začala spoločnosť ESET poskytovať aktualizácie databázy hrozieb svojim klientom po celom svete v priebehu niekoľkých minút. Táto technológia opäť nebola žiadnou „čiernou skrinkou“, ale neustále sa vyvíjajúcou, monitorovanou vrstvou, ktorá sa prispôsobovala na základe nových vzoriek a hrozieb a poskytovala najaktuálnejšie informácie o vznikajúcich hrozbách takmer okamžite.

Dôkladná integrácia namiesto ošiaľu

Na konci druhej dekády 21. storočia viedol prudký rozvoj hĺbkového učenia a neurónových algoritmov k rozmachu v oblasti kybernetickej bezpečnosti, pričom mnohí novovzniknutí postfaktuálni dodávatelia riešení využili tento rozruch a nasľubovali nereálne výsledky. Spoločnosť ESET sa rozhodla k integrácii pristúpiť opatrne, nie na základe vzniknutého ošiaľu.

Zatiaľ čo sa mnohí kokurenti ponáhľali s nasadením tejto technológie s cieľom vyhodnocovať prakticky akékoľvek škodlivé správanie – čo bol prístup, ktorý v konečnom dôsledku zahltil bezpečnostných špecialistov falošnými detekciami – spoločnosť ESET sa rozhodla pre dôkladné testovanie svojich prístupov využívajúcich AI na konfrontáciu hrozieb z reálneho sveta. Na základe výsledkov tohto procesu vytvorili inžinieri spoločnosti ESET presnú kombináciu neurónových sietí typu LSTM (Long Short-Term Memory), rozhodovacích stromových štruktúr a tradičných monitorovaných metód učenia s cieľom vytvoriť **modul pokročilého strojového učenia ESET**.

Táto nová technológia, ktorá bola verejnosti predstavená v roku **2017**, dokázala skĺbiť vysokú mieru detekcie s takmer nulovou mierou falošných poplachov – čo je kľúčový faktor vymedzujúci každodenné operácie už beztak preťažených bezpečnostných pracovníkov.

V tom istom roku výskumníci spoločnosti Google uverejnili článok s názvom „Attention Is All You Need“ (Stačí len pozornosť), v ktorom predstavili architektúru transformátorov a odštartovali novú éru inovácií v oblasti umelej inteligencie. **V roku 2020 sa spoločnosť ESET stala jedným z prvých dodávateľov bezpečnostných riešení**, ktorý nasadil **model detekcie založený na transformátoroch** ako dodatočnú vrstvu ochrany pred kybernetickými hrozbami. Stojí za zmienku, že k tomuto pokroku došlo už roky predtým, než sa transformátory stali hnacou silou nástrojov generatívnej umelej inteligencie, ako je napríklad ChatGPT od spoločnosti OpenAI.

Časová os najdôležitejších míľnikov vývoja AI technológií v spoločnosti ESET

1997

Prvé použitie neurónových sietí v produktoch ESET na účely detekcie makrovírusov.

2005

Detekcia ESET na úrovni DNA, synonymum pre online strojové učenie, využíva gény malvéru na detekciu súčasných aj nových hrozieb.

2010

ESET LiveGrid®, cloudový reputačný systém, využíva detekcie na úrovni DNA na zrýchlenie aktualizácií na strane používateľov.

2017

Pokročilé strojové učenie ESET v cloude využíva AI na podporu vlastných automatizovaných systémov detekcie.

2018

ESET LiveGuard, cloudový sandbox poháňaný umelou inteligenciou, poskytuje zákazníkom spoločnosti ESET analýzu na vyžiadanie s dobou spracovania v priebehu niekoľkých minút.

2019

Pokročilé strojové učenie ESET v produktoch pre koncové zariadenia využíva AI na podporu našich **automatizovaných systémov detekcie.**

2020 – 2021

Modely založené na transformátoroch sú nasadené do riešení spoločnosti ESET fungujúcich v cloude a na koncových zariadeniach.

2023

Do ESET Inspect bol pridaný nástroj na automatizované vytváranie incidentov, ktorý v množstve zachytených údajov prehľadne identifikuje jednotlivé incidenty.

2024

Spustenie nástroja ESET AI Advisor, bezpečnostného poradcu poháňaného AI, ktorý dokáže generovať podrobné popisy incidentov a odpovedať na otázky týkajúce sa ich rozsahu.

AI v spoločnosti ESET dnes: **výkonná, overená, efektívna**

Ďalšia kapitola analýzy založenej na umelej inteligencii v spoločnosti ESET sa začala zavedením služby **ESET LiveGuard Advanced** (predtým známej ako **ESET Dynamic Threat Defense**). Je navrhnutá ako cloudový sandbox a spája niekoľko nezávislých vrstiev detekcie vrátane pokročilej extrakcie a kontroly, statickej a dynamickej analýzy, experimentálneho detekčného jadra a hĺbkovej analýzy správania.

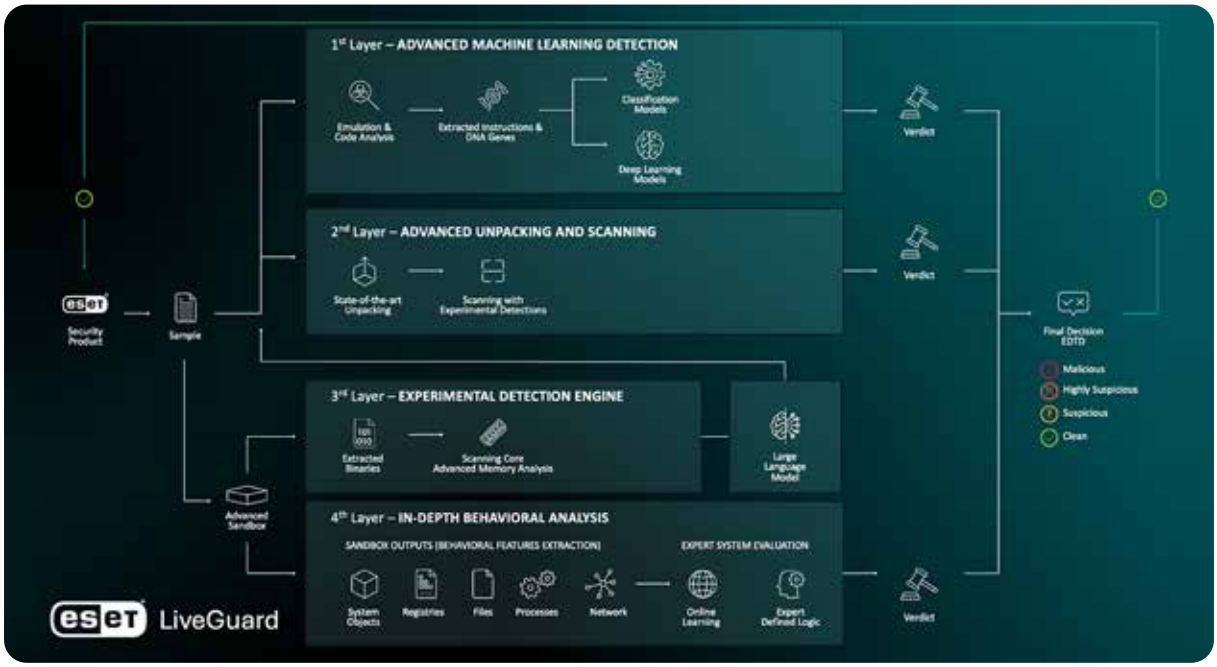
Namiesto toho, aby mal prevahu len jeden AI systém, ESET LiveGuard Advanced využíva viacero typov algoritmov a rozhodovacích bodov, pričom ich výstupy neustále vzájomne overuje a koreluje. Údaje získané na základe dôkladnej viacvrstvovej analýzy sa následne zosumarizujú do konečného záveru a predložia zákazníkovi, ktorý žiadosť vytvoril, pričom zaslaná vzorka je zaradená do jednej zo štyroch kategórií: škodlivá, veľmi podozrivá, podozrivá alebo bezpečná.

Trénovacie dáta pre ESET LiveGuard Advanced sú starostlivo vyberané z neustále aktualizovanej **databázy s objemom viac ako 65 TB**, ktorá obsahuje presne klasifikované binárne súbory vrátane škodlivých, potenciálne nechcených, potenciálne nebezpečných a neškodných vzoriek. Na rozdiel od tohto obrovského súboru údajov je veľkosť optimalizovaného, rýchleho a mimoriadne efektívneho modulu umelej inteligencie, ktorý je distribuovaný zákazníkom, väčšinou menšia ako **20 MB**.

Aby si spoločnosť ESET udržala najvyšší výkonnostný štandard v prostredí neustále sa meniacich hrozieb, každý týždeň opätovne trénuje svoj model umelej inteligencie. Tento model detekcie sa skladá približne z jedného milióna parametrov, a je teda oveľa menší ako modely všeobecného použitia, ktoré zvyčajne obsahujú bilióny parametrov.

Kombinácia presných trénovacích dát, optimalizácie, výpočtového výkonu a množstva analytických prístupov umožňuje službe ESET LiveGuard Advanced detekciu širokej škály útokov, medzi ktoré patria:

- **doposiaľ neznáme hrozby,**
- **exploity zamerané na zero-day zraniteľnosti,**
- **útoky založené na skriptoch,**
- **bezsúborový malvér**
- **a techniky „living-off-the-land“.**



Obrázok 4: Zjednodušená schéma spracovania vzoriek službou ESET LiveGuard Advanced

Vďaka výkonnej backendovej infraštruktúre cloudového sandboxu ESET **je možné 99 % vzoriek zaslaných zákazníkmi analyzovať** za menej ako **5 minút**. Toto zdrojovo náročné spracúvanie zároveň prebieha v prísne kontrolovaných a robustných cloudových prostrediach prevádzkovaných spoločnosťou ESET. Zaistená je tak bezpečnosť procesu, ako aj **minimálny vplyv** na výpočtové zdroje klientov.

Služba ESET XDR: **robustná, odolná, spoľahlivá**

S postupným zdokonaľovaním strojového učenia a umelej inteligencie preukázali predchádzajúce úspešné implementácie fakt, že vedecký prístup inžinierskych tímov spoločnosti ESET zaručuje vysokú mieru detekcie a zároveň zabezpečuje odolnosť voči vonkajším zásahom. Aj dnes, namiesto toho, aby sa ESET spoliehal na najnovšie trendy v oblasti algoritmov, naďalej využíva svoj **viacvrstvový prístup založený na viacerých modeloch**, ktorý zahŕňa učenie s dohľadom aj bez dohľadu, hĺbkové učenie, heuristické vrstvy a transformátory.

Predtým, ako implementujeme akékoľvek nové modely alebo metódy, musia najskôr prejsť rozsiahlym porovnávacím testovaním – keďže nie všetky modely umelej inteligencie sú rovnako vhodné na použitie v oblasti bezpečnosti. Inžinieri spoločnosti ESET následne starostlivo vyberajú prístupy, ktoré sa osvedčili ako **odolné voči manipulácii útočníkov a ich vyvíjajúcim sa taktikám** a ktoré **minimalizujú množstvo upozornení** pre bezpečnostných pracovníkov **tým, že udržujú nízku mieru falošných detekcií.**

Praktické výsledky sú viditeľné v **platforme ESET PROTECT** – riešení rozšírenej detekcie a reakcie (XDR) spoločnosti ESET – ktorá umožňuje správu desiatok tisíc zariadení z jednej centrálnej konzoly na správu. Vstavaná technológia, zahŕňajúca aj umelú inteligenciu, spracováva veľké množstvá údajov zhromaždených z koncových zariadení, porovnáva ich s globálnou databázou hrozieb spoločnosti ESET a následne sumarizuje výsledky do prehľadných schém a reportov. Platforma ESET PROTECT nevyužíva možnosti umelej inteligencie len na detekciu, ale aj na analýzu a koreláciu agregovanej aktivity na koncových zariadeniach.

Prostredníctvom integrovaného korelačného jadra **ESET LiveCortex**[1] umelá inteligencia **zoskupí súvisiace udalosti**, **odfiltruje nepodstatné informácie** a **vizuálne znázorní hrozby** spôsobom, ktorý pomáha bezpečnostným tímom rýchlo porozumieť situácii a konať. Výstupy jadra ESET LiveCortex sú obohatené o údaje špecifické pre daného zákazníka a kontextové podrobnosti, ako sú názvy počítačov, používateľské účty a sieťové špecifiká, čím poskytujú vysoko relevantné vysvetlenia a odporúčania prispôsobené konkrétnemu používateľovi.

Tým sa výrazne zlepšuje zrozumiteľnosť zložitých údajov, znižuje množstvo upozornení a urýchľuje reakcia na incidenty v situáciách, kde minúty môžu rozhodovať o tom, či dôjde k narušeniu bezpečnosti alebo k úspešnej obrane systému.

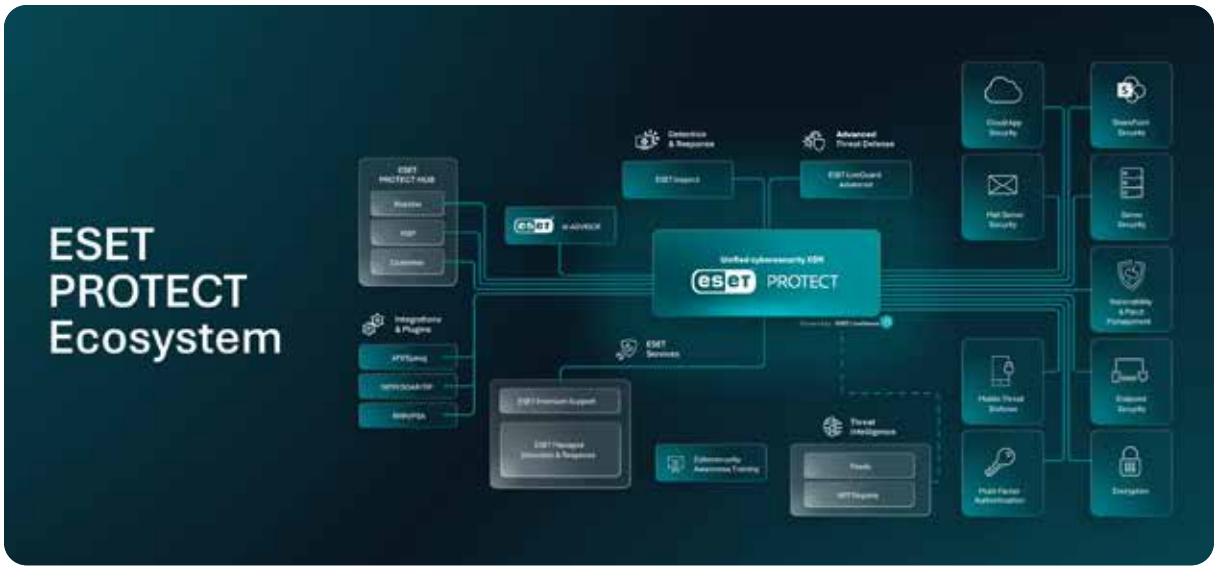
Spoľahlivé **Live AI**

V rámci ďalšieho rozvoja inovácií spoločnosť ESET v roku **2024** predstavila nástroj AI Advisor, predchodcu dnešného **Live AI**. Systém je vyvinutý s ohľadom na umelú inteligenciu založenú na agentoch, ktorý spája to najlepšie z ľudských odborných znalostí, schopností veľkých jazykových modelov (LLM) a ďalších techník vrátane **generovania doplneného vyhľadávaním** (RAG), pričom bol integrovaný do ESET Inspect (dnes súčasť ESET XDR) a neskôr pridaný aj do ESET Threat Intelligence.

Vďaka tomu, že je systém ESET Live AI založený na LLM technológii, ktorá je prirodzene predurčená na spracovanie a generovanie výstupov v ľudskom jazyku – autonómne vytvára názvy a popisy incidentov, čím zefektívňuje bezpečnostné operácie. Zaisťuje tak okamžitú a intuitívnu detekciu hrozieb, znižuje počet nesprávnych detekcií, zefektívňuje správu chráneného prostredia a podporuje operácie zamerané na vyhľadávanie hrozieb.

Systém LiveAI je tiež schopný vytvárať reporty potrebné na účely dodržiavania predpisov a auditu, podrobne odpovedať na otázky týkajúce sa konkrétnych detekcií, vyšetrovať akékoľvek dané incidenty, odporúčať opatrenia na opravu v reálnom čase a dokonca vytvárať odkazy, pomocou ktorých je možné okamžite identifikovať a izolovať dotknuté zdroje.

[1] Predtým známy ako Správca incidentov



Obrázok 5: Ekosystém ESET PROTECT

S cieľom zaistiť, aby boli odpovede systému ESET LiveAI vždy založené na faktoch, využívajú sa techniky RAG na vyhľadávanie spoľahlivých informácií o hrozbách zozbieraných spoločnosťou ESET. Na zmiernenie rizika halucinácií model funguje na základe **bezpečnostných opatrení** navrhnutých spoločnosťou ESET, ktoré sú neustále aktualizované, a vždy uvádza odkazy na svoje zdroje.

Líder v oblasti informácií o kybernetických hrozbách

Telemetria spoločnosti ESET, ktorá slúži 500 000 firemným zákazníkom, 110 miliónom priamych zákazníkov a vyše miliarde nepriamych používateľov, denne získava obrovské množstvo najnovších údajov o hrozbách. Špičkové automatizované systémy a tím pozostávajúci z viac ako 850 výskumníkov a odborníkov na technológie analyzujú tento tok údajov s cieľom odhaliť nové techniky a taktiky útočníkov, vďaka čomu je spoločnosť ESET lídrom v oblasti informácií o kybernetických hrozbách.

ESET Threat Intelligence (ETI) využíva skúsenosti odborníkov nazbierané za viac ako 35 rokov v kombinácii so spracúvaním umelej inteligencie, korelujúc indikátory preukazujúce narušenie zabezpečenia a taktiky, techniky a postupy (TTP) útočníkov s cieľom každoročne poskytovať bezpečnostným špecialistom štruktúrované a praktické informačné kanály a tisíce stránok reportov. Na spracovanie tohto množstva informácií je k dispozícii aj platforma ETI, ktorá umožňuje vyhľadávať a sumarizovať výsledky výskumu spoločnosti ESET.

Inovácie a obmedzenia AI

Takmer tri desaťročia experimentovania a vývoja bezpečnostných technológií súvisiacich s umelou inteligenciou priniesli spoločnosti ESET jedinečné poznatky, komplexné pochopenie existujúcich obmedzení a predovšetkým širší pohľad. Spoločnosť ESET si uvedomuje, že technológia umelej inteligencie je sama osebe neutrálna. Zodpovedné nasadzovanie umelej inteligencie stojí na rozhodnutiach: zapájať ľudí do rozhodovacieho procesu, nastaviť pevné mantinely, zamerať sa na prínos pre používateľa a vždy sa riadiť etickými princípmi.

Dobrým príkladom je rozpoznávanie nových rizík, ktoré so sebou generatívna umelá inteligencia prináša, ako deepfake videá, vkladanie inštrukcií do príkazov alebo manipulácia s modelmi. Spoločnosť ESET rieši tieto problémy prostredníctvom praktického prístupu založeného na viacvrstvovej ochrane, pričom sa zameriava predovšetkým na základné prvky a infraštruktúru, na ktorej škodlivá AI aktivita stojí. Inými slovami, ESET zachytáva znaky, ako škodlivé skripty, phishingové odkazy, podvodné domény a odhaľuje podozrivé správanie súborov, než aby sa zapájal do súbojov medzi AI modelmi, ktoré sú náročné na zdroje – a často aj zbytočné.

Uplatňovanie tejto pragmatickej stratégie zaručuje, že produkty ESET si udržia nízku záťaž na systém používateľa, sú dostupné v rôznych prostrediach a zároveň si zachovávajú vysokú mieru detekcie a nízku mieru falošných poplachov.

Táto **adaptabilita** sa prejavuje aj v **schopnosti detegovať** najnovšie hrozby vrátane malvéru napísaného v moderných, **platformovo nezávislých jazykoch ako Go**. Zároveň to poukazuje na prístup, pri ktorom partnerstvá s lídrami v odvetví a využívanie výskumu prostredia hrozieb podporujú vývoj nových, špičkových vrstiev AI obrany.

Súčasný projekt v rámci výskumu a vývoja skúma celý rad **vylepšení automatizácie** pre ESET LiveCortex (súčasť platformy ESET PROTECT), kde umelá inteligencia bude prinášať nielen praktické odporúčania, ale aj poskytovať **riešenia konkrétnych incidentov na jedno kliknutie,** čím sa zníži pracovná záťaž bezpečnostných pracovníkov monitorujúcich prostredie.

Medzi ďalšie smery skúmané inžiniermi spoločnosti ESET patria úzka spolupráca s lídrami v oblasti hardvérových riešení – ako napríklad **Intel** – na integráciu s neurónovými procesormi (NPU) a pokračujúca podpora hlavných platforiem. Cieľom je optimalizovať moduly spoločnosti ESET založené na umelej inteligencii tak, aby fungovali rýchlejšie a efektívnejšie, čím sa ďalej zníži záťaž na systémy zákazníkov.

Budovanie dôvery tam, kde žiadna nie je

Spoločnosť ESET ako dodávateľ bezpečnostných riešení prirodzene spracúva veľké množstvá škodlivého obsahu, z ktorého veľká časť zahŕňa osobne identifikovateľné informácie (personally identifiable information - PII). Aby chránil súkromie používateľov, ESET využíva rámcové komerčné riešenia rozšírené o **vlastné filtre a analyzátory**, ktoré ESET odborníci vyvinuli a doladili na maximálnu presnosť. Týmto spôsobom ESET **zabezpečuje anonymizáciu všetkých osobne identifikovateľných informácií** ešte pred odoslaním obsahu do modelu LLM.

Obrázok 6: Príklad anonymizácie osobne identifikovateľných informácií (PII) pomocou vlastných filtrov a analyzátorov, ktoré vyvinuli odborníci spoločnosti ESET.

Hoci je tento prístup vysoko účinný pri ochrane údajov PII, spoločnosť ESET ho neustále a dôkladne testuje, aby zabezpečila ochranu aj iných citlivých typov údajov – ako sú dokumenty, heslá, kľúče API a zložité príkazy obsahujúce dôverné informácie špecifické pre jednotlivých zákazníkov – bez toho, aby bola ohrozená presnosť detekcie hrozieb.

Otázky dôvery sa však netýkajú len osobne identifikovateľných informácií. Podľa hĺbkových rozhovorov s vybranými zákazníkmi z rôznych odvetví patrilo k hlavným obavám aj využívanie AI pri práci s duševným vlastníctvom a ďalšími citlivými dátami.

AI infraštruktúra v spoločnosti ESET

S prechodom organizácií od experimentovania s AI četbotmi k zavádzaniu práce s AI agentmi, stále viac údajov, rozhodnutí a úloh kritických pre chod firmy sa zveruje čoraz autonómnejším systémom, čo výrazne zvyšuje riziko útokov. Spoločnosť ESET odpovedá na tieto narastajúce riziká rozširovaním vlastnej AI infraštruktúry, pričom ale kontrolu ponecháva v rukách používateľov a správcov.

Ochrana AI konverzácií ESET

Prvý nasadený modul našej AI infraštruktúry sa zameriava na riziká spojené s AI četbotmi vrátane úniku citlivých informácií, ako sú heslá, kľúče API, technické alebo obchodné know-how či iné dôverné údaje. Takéto informácie môže zamestnanec neúmyselne prezradiť vo svojom vstupe, ale systém umelej inteligencie ich môže získať aj zo zdrojov organizácie a odhaliť vo výstupe.

Produkty ESET tiež kontrolujú v príkazoch a odpovediach četbotov prítomnosť škodlivých odkazov, URL adries, kódu alebo inštrukcií, ktoré môžu viesť k ohrozeniu bezpečnosti. Kontrola prebieha bez ohľadu na to, či takéto informácie neúmyselne poskytol používateľ, vložil ich do príkazu útočník alebo boli vytvorené četbotom. Všetky relevantné udalosti sú správcom k dispozícii v konzole platformy ESET PROTECT.

Ochrana dodávateľského reťazca ESET

ESET AI Skills Checker – a jeho vylepšená verzia, integrovaná do produktov ESET – boli navrhnuté špeciálne pre rozvíjajúci sa ekosystém umelej inteligencie založenej na agentoch, ktorý je obohatený o tzv. rozšírenia („skills“). Tieto drobné nástroje alebo doplnky poskytujú agentovi pokyny, ako má úlohu vykonať, vrátane toho, ktoré služby má použiť a aké kroky má podniknúť.

Spracovanie jednotlivých rozšírení spoločnosťou ESET zahŕňa:

- **kontrolu obsahu daného rozšírenia vrátane inštrukcií a rôznych artefaktov, ako sú skripty alebo neznáme binárne súbory,**
- **extrakciu a následnú kontrolu všetkých externých URL adries,**
- **analýzu celého reťazca škodlivého kódu,**
- **simuláciu ich správania v prostredí sandboxu.**

V prvých týždňoch od spustenia v marci 2026 spoločnosť ESET preskenovala takmer 800 000 jedinečných rozšírení. Viac ako 60 000 bolo vyselektovaných na ďalšiu analýzu, ktorá zatriedila 25 000 z nich do kategórie podozrivých rozšírení, kde by stačili len drobné úpravy na to, aby sa rozšírenie stalo škodlivým. Ďalších 3000 rozšírení bolo zablokovaných a označených za jednoznačne škodlivé.

Keď ku kontrole a opätovnej kontrole nových a aktualizovaných rozšírení pridáme kontroly neškodných rozšírení, celkový počet kontrol vykonaných za prvé mesiace prevádzky dosahuje niekoľko miliónov, pričom v niektorých dňoch pribudnú do databázy spoločnosti ESET aj stovky tisíc nových záznamov.

Rozšírenia umelej inteligencie založenej na agentoch však tvoria len časť softvérového dodávateľského reťazca a často využívajú externé repozitáre, balíky, dátové súbory a pluginy. Postarať sa o ich bezpečnosť si preto vyžaduje ísť nad rámec tradičnej kontroly malvéru, ktorá sa zameriava na škodlivé prvky, ako sú skripty, phishingové odkazy, podvodné domény a škodlivé súbory. S cieľom rozšíriť túto vrstvu ochrany inžinieri spoločnosti ESET integrujú do výstupov ESET riešení poháňaných umelou inteligenciou spracúvanie reputácie balíkov, overovanie pôvodu dátových súborov, detekciu kompromitovaných správcovských účtov a identifikáciu ďalších vysoko rizikových závislostí.

Obrázok 7: Ochrana na úrovni siete pre komunikáciu medzi agentmi.

ESET Secure AI Relay

Kontrola AI rozšírení založených na agentoch, ako aj vstupov a výstupov četbotov, je len prvým krokom v rámci širšieho systému, ktorý spoločnosť ESET v súčasnosti vyvíja: bezpečné prepojenie medzi používateľmi, AI agentmi, firemnými aplikáciami a AI modelmi.

ESET Secure AI Relay je navrhnutý tak, aby fungoval ako sprostredkovateľ, ktorý deteguje škodlivé vzorce, vynucuje dodržiavanie pravidiel organizácie, zabraňuje zdieľaniu citlivých dát s neautorizovanými modelmi, blokuje prístup AI nástrojov k vyčleneným zdrojom a zabezpečuje, aby výstupy modelov nezavádzali do firemných procesov škodlivé prvky.

Inžinieri spoločnosti ESET sa tiež zaoberajú výskumom ochrany na úrovni siete pre komunikáciu medzi AI agentmi. Prostredníctvom ochrany štandardných protokolov umelej inteligencie, ako sú Model Context Protocol (MCP) a Agent2Agent (A2A) Protocol, spoločnosť ESET smeruje k rozšíreniu platformy ESET XDR o funkcie bezpečnostného proxy.

Tieňová AI a vyhľadávanie zdrojov s využitím AI

S cieľom riešiť rastúcu výzvu v podobe tieňovej AI (tzv. „shadow AI“) platforma ESET PROTECT umožňuje monitorovanie umelej inteligencie a bude ďalej rozšírená o funkciu vyhľadávania zdrojov s využitím AI. Zatiaľ čo sa monitorovanie umelej inteligencie zameriava konkrétne na identifikáciu a sledovanie využívania AI, spoločnosť ESET zároveň skúma možnosti založené na agentoch, ktoré dokážu posúdiť širšie sieťové prostredie a odhaliť aj skryté alebo ťažko detegovateľné zdroje.

Tieto nástroje spoločne identifikujú, kde sa umelá inteligencia využíva, a zmapujú prepojenia medzi aplikáciami a firemnými databázami, analyzujú toky údajov z pohľadu útočníka s cieľom posúdiť riziko a pomôžu organizáciám dodržiavať interné pravidlá a regulačné požiadavky.

Pokročilé AI projekty

Spoločnosť ESET využíva aj korelačné schopnosti systémov, ako je napríklad ESET LiveCortex, aby vytvorila AI-natívnu platformu na zber a spracovanie dát, ktorá identifikuje relevantné signály z rôznych zdrojov. Patria medzi ne ESET technológie, údaje OSINT, aktuálne databázy CVE, externé informačné kanály, vlastné zdroje vybrané zákazníkmi a produkty tretích strán. Cieľom je spracovať veľké množstvo informácií do zoznamu bezpečnostných rizík zoradených podľa priority, vďaka čomu sa budú môcť bezpečnostné tímy zameriavať na to najdôležitejšie.

Napokon, s víziou zachovania nezávislosti od veľkých poskytovateľov umelej inteligencie a prehĺbenia porozumenia a príležitostí aj obmedzení využitia AI v oblasti kybernetickej bezpečnosti, spoločnosť ESET investuje do vlastných špecializovaných základných modelov.

Tento projekt bude zahŕňať – a zároveň prevyšovať – architektúry založené na transformeroch a veľkých jazykových modeloch (LLM), ktoré pomôžu organizáciám nielen riešiť existujúce bezpečnostné výzvy, ale aj simulovať rôzne scenáre a vyhodnocovať budúci vplyv nových hrozieb a obranných stratégií.

AI pre SOC tímy

Výskum a vývoj spoločnosti ESET sa zameriava aj na novú generáciu **AI bezpečnostných operačných centier (SOC)**. Prémiové bezpečnostné služby – ako napríklad reakcia na incidenty, bezpečnostné audity a penetračné testy – sú nákladné a ich ponuka je obmedzená, čím sú dostupné predovšetkým pre veľké firmy. Zároveň stredným a menším organizáciám často chýbajú odborné znalosti a zdroje, ktoré by im umožnili využívať tieto kapacity, a to aj napriek tomu, že zložitosť hrozieb, telemetrie a bezpečnostných nástrojov neustále rastie.

Narastajúca škála, zložitosť a rýchlosť hrozieb využívajúcich AI aj bezpečnostných operácií si vyžadujú nový prístup. Bezpečnostné (SOC) centrá využívajúce umelú inteligenciu môžu zautomatizovať značnú časť svojich pracovných postupov, čím pomôžu skúseným analytikom predísť preťaženiu alertmi a umožnia im zamerať sa na strategické problémy s najvyššou prioritou. Vďaka tomu by sa mohla ochrana na úrovni Enterprise stať cenovo dostupnejšou a prístupnejšou pre širšie spektrum organizácií a používateľov, pričom by tieto riešenia boli zároveň jednoducho prevádzkovateľné.

Predikcia, prevencia, ochrana

Pri skúmaní nových možností v oblasti bezpečnosti spoločnosť ESET zároveň reflektuje na potenciálne budúce výzvy súvisiace s využívaním najnovších modelov umelej inteligencie zo strany útočníkov. Patria medzi ne:

- **optimalizované techniky útokov a malvéru,**
- **vylepšené sociálne inžinierstvo,**
- **nárast počtu podvodných, phishingových a dezinformačných kampaní,**
- **vyhľadávanie zraniteľností s cieľom zneužitia,**
- **identifikácia osôb s vysokou mierou zraniteľnosti na sociálnych sieťach a ich manipulácia s cieľom zapojiť ich do rôznych „podporných“ úloh pri kybernetických útokoch (prevod peňazí, distribúcia, výpočtový výkon pre útoky DDoS atď.),**
- **trénovanie malých open-source modelov na spracovanie odcudzených osobných údajov a generovanie na mieru šitých podvodov.**

V spoločnosti ESET sa využívanie umelej inteligencie vyznačuje jej včasným zavedením, dôsledným vedeckým prístupom a oporou v dôkladnom pochopení trendov a smerovania vývoja hrozieb. V spojení s pokročilou automatizáciou, dôkladným ľudským dohľadom a dôrazom na orientáciu na používateľa v každom kroku, ponúka spoločnosť ESET model, ako využívať možnosti umelej inteligencie v prospech všetkých. Týmto spôsobom spoločnosť ESET prispieva k tomu, aby boli bezpečnostní odborníci vždy o krok vpred, a to používaním inteligentných, adaptívnych a predovšetkým bezpečných a dôveryhodných nástrojov zabezpečenia.

Filozofia spoločnosti ESET pre AI

Za posledné tri desaťročia sa spoločnosť ESET etablovala ako líder v oblasti kybernetickej bezpečnosti využívajúcej AI, pričom bez kompromisov kladie dôraz na bezpečnosť, transparentnosť a prospech používateľov a opiera sa o komplexné technické znalosti, zodpovednú inováciu a pochopenie toho, aké veľké riziko so sebou prináša zabezpečenie digitálnych prostredí.

Spoločnosť si uvedomuje sociálnu a etickú zodpovednosť v súvislosti s umelou inteligenciou a uprednostňuje praktické metódy, ktoré blokujú vektory útokov s cieľom chrániť veľký počet používateľov, namiesto toho, aby sa zameriavala na nespoľahlivú detekciu každej potenciálnej hrozby individuálne.

Spoločnosť ESET využíva sofistikovanú, viacvrstvovú integráciu AI modelov – v kombinácii s tradičnými metódami detekcie a odborným dohľadom človeka – aby zabezpečila, že pri rozhodovaní sa zohľadňuje kontext a vplyv na používateľa, namiesto spoliehania sa výlučne na automatizované systémy.

Nástroje ako ESET Live AI umožňujú tímom spravovať bezpečnosť systému bez ohľadu na úroveň ich technickej odbornosti alebo zložitosť prostredia, ktoré spravujú, čím prispievajú k efektívnej spolupráci medzi ľuďmi a umelou inteligenciou.

Neustále investície do výskumu a vývoja a praktických technológií zaručujú, že technológie spoločnosti ESET sa prispôsobujú novým hrozbám a neprestávajú prinášať úžitok používateľom – od jednotlivcov až po veľké spoločnosti.

O spoločnosti ESET

ESET® poskytuje najmodernejšie kybernetické zabezpečenie, ktoré predíde útokom skôr, ako k nim vôbec dôjde. Kombináciou sily umelej inteligencie a ľudských odborných znalostí si ESET udržiava náskok pred známymi aj novovznikajúcimi kybernetickými hrozbami a chráni tak firmy, kritickú infraštruktúru aj jednotlivcov. Či už ide o ochranu pracovných staníc, cloudu alebo mobilných zariadení, ESET cloudové riešenia a služby založené na umelej inteligencii si zachovávajú vysokú efektívnosť a ľahko sa používajú. Technológie spoločnosti ESET sú postavené na účinnej detekcii a reakcii, mimoriadne bezpečnom šifrovaní a dvojfaktorovej autentifikácii. Vďaka nepretržitej ochrane v reálnom čase a silnej lokálnej podpore zaisťujeme bezpečnosť používateľov a sústavný chod firiem. Neustále sa vyvíjajúce digitálne prostredie si vyžaduje progresívny prístup k zabezpečeniu: ESET sa venuje výskumu na najvyššej svetovej úrovni a efektívne zhromažďuje informácie o najnovších hrozbách, pričom nezastupiteľnú rolu tu zohrávajú centrá výskumu a vývoja a tiež silná globálna sieť partnerov. Viac informácií nájdete na stránke www.eset.com alebo sledujte naše sociálne siete, podcasty a blogy.

ESET Cyber Security | Riešenia pre veľké organizácie, firmy a domácnosti | ESET

Najlepšie IT bezpečnostné riešenia pre domáce a firemné zariadenia. Vyskúšajte antivírusovú a internetovú ochranu od spoločnosti ESET pre operačné systémy Windows, Android, Mac či Linux.

Cybersecurity
Progress. Protected.

www.eset.com