PREHĽAD

# INSPECT

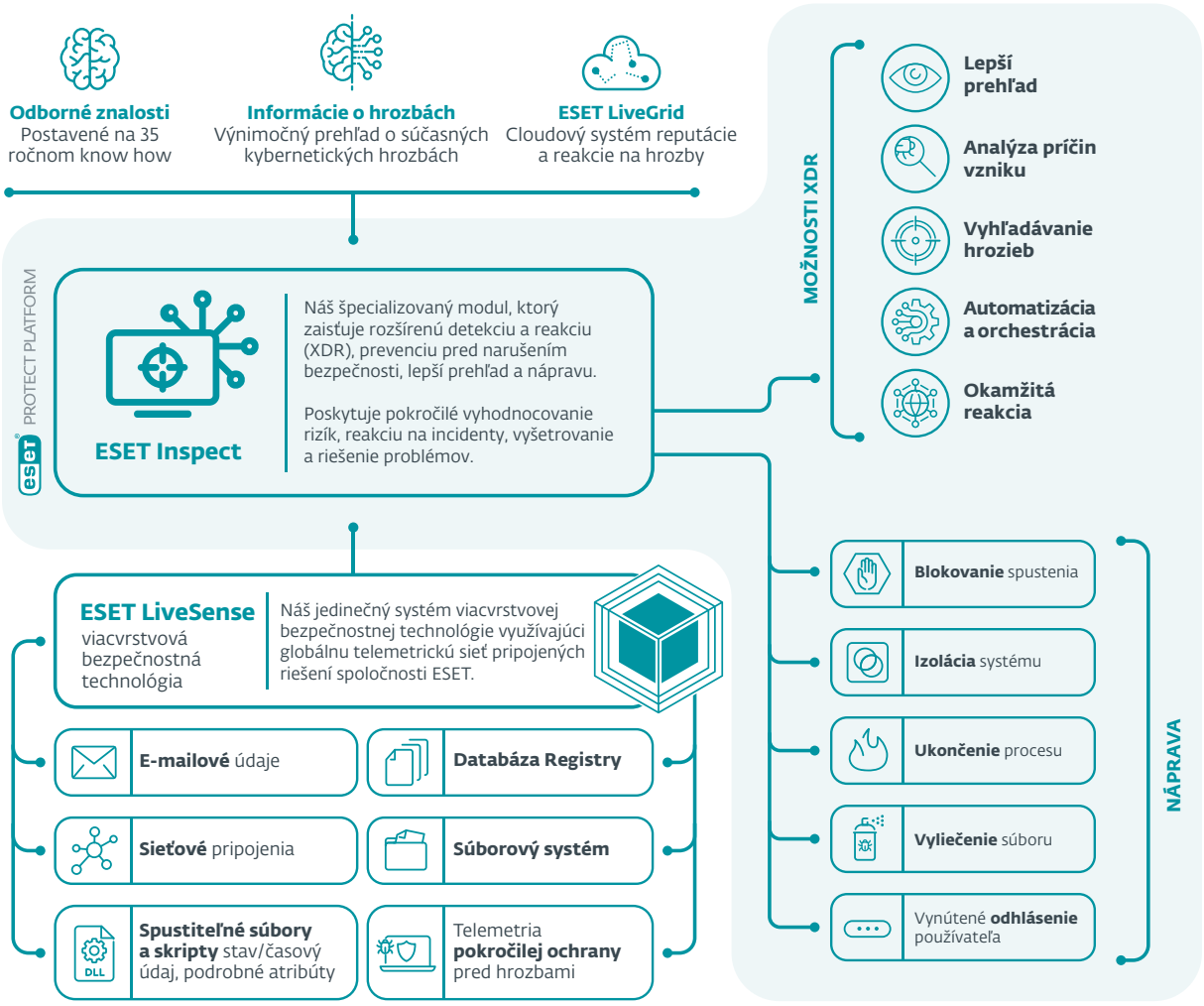
Modul platformy ESET PROTECT, ktorý zaisťuje rozšírenú detekciu a reakciu XDR. Zabezpečuje prevenciu, vynikajúci prehľad o celej sieti a nápravu.

Progress. Protected.

# Čo je **riešenie rozšírenej detekcie a reakcie (XDR)?**

**ESET Inspect, modul platformy ESET PROTECT, ktorý zaisťuje rozšírenú detekciu a reakciu, je nástroj na identifikáciu nezvyčajného správania a narušenia ochrany údajov, vyhodnocovanie rizík, riešenie incidentov, vyšetrovanie a nápravu.**

Pracovníkom, ktorých úlohou je reagovať na incidenty, umožňuje monitorovať a vyhodnocovať všetky aktivity v sieti a na pripojených zariadeniach. V prípade potreby tiež automatizuje okamžité nápravné opatrenia. Komplexné vyhľadávanie hrozieb je možné vďaka viac ako 800 pravidlám detekcie ESET, ktoré stále pribúdajú.




Digital Security
Progress. Protected.

# V čom je ESET iný

## KOMPLEXNÁ PREVENCIA, DETEKCIA A REAKCIA

Umožňuje rýchlu analýzu a nápravu akéhokoľvek problému so zabezpečením v sieti. Základné viacvrstvové zabezpečenie, v rámci ktorého každá vrstva odosiela údaje nástroju ESET Inspect, analyzuje obrovské množstvo údajov v reálnom čase, takže žiadna hrozba nezostane skrytá.

## RIEŠENIE OD VÝROBCU ZAMERANÉHO NA BEZPEČNOSŤ

ESET už viac ako 30 rokov bojuje proti kybernetickým hrozbám. Ako spoločnosť, ktorá si zakladá na vedeckých poznatkoch, je už dlho na čele vývoja v oblasti strojového učenia, cloudovej technológie, a po novom aj rozšírenej detekcie a reakcie.

## PREVENCIA JE LEPŠIA AKO LIEČBA

Riešenie XDR je úzko integrované s viacnásobne ocenenými bezpečnostnými produktmi ESET. Vďaka odhodlaniu vyvíjať vysokokvalitné detekčné technológie patrí ESET medzi svetovú špičku v oblasti prevencie pred hrozbami.

## DETAILNÝ PREHĽAD O SIETI

So zrozumiteľnými pravidlami detekcie (ESET ich má viac ako 800 a stále pribúdajú), pokročilými indikátormi preukazujúcimi narušenie zabezpečenia (IoC) a možnosťou vyhľadávania vám hĺbková kontrola spustiteľných súborov vo vašej sieti umožní identifikovať všetku podozrivú aktivitu.

## FLEXIBILNÉ NASADENIE

Rozhodnutie, ako nasadiť bezpečnostné riešenie, nechávame na vás.  S nástrojom ESET Inspect sa spája možnosť lokálneho aj cloudového nasadenia, vďaka čomu si prispôsobíte jeho nastavenie podľa svojich celkových nákladov stanovených na prevádzku a kapacity hardvéru.

## AUTOMATIZOVANÉ VYTVÁRANIE INCIDENTOV

Získajte dokonalý prehľad o automaticky vytváraných a prehľadne vizualizovaných incidentoch. ESET Inspect dáva do súvislosti obrovské množstvo dát s cieľom nájsť hlavné príčiny udalostí a skompilovať ich do komplexných incidentov, aby ste ich mohli okamžite vyriešiť.

## PRIPRAVENÝ OKAMŽITE REAGOVAŤ

Riešenie je pripravené na okamžité použitie, ale skúsení vyhľadávači hrozieb si ho môžu v prípade záujmu do detailov upraviť.

## MITRE ATT&CK

ESET Inspect pri zachytených detekciách poskytuje aj priamy odkaz na databázu znalostí na platforme MITRE ATT&CK™, aby ste jedným kliknutím mohli získať podrobné informácie aj o tých najzložitejších hrozbách.

## REPUTAČNÝ SYSTÉM

Dôkladné filtrovanie umožňuje bezpečnostným technikom identifikovať všetky preverené aplikácie pomocou rozsiahleho reputačného systému spoločnosti ESET. Náš systém reputácie obsahuje databázu stoviek miliónov bezpečných súborov. Bezpečnostné tímy sa tak môžu venovať neznámym a potenciálne škodlivým súborom, nie falošným poplachom.

## AUTOMATIZÁCIA A PRISPÔSOBENIE

Jednoducho si prispôsobte nástroj ESET Inspect na požadovanú úroveň podrobnosti a automatizácie. Pri úvodnom nastavení si s pomocou prednastavených používateľských profilov vyberte príslušný rozsah interakcie, ako aj typ a množstvo ukladaných dát. Učiaci sa režim následne zmapuje prostredie vašej firmy a tam, kde je to potrebné, vám navrhne výnimky z nesprávnych detekcií.

# Možnosti riešenia

## SYSTÉM SPRÁVY INCIDENTOV

Zoskupujte objekty, ako sú detekcie, počítače, spustiteľné súbory alebo procesy, do logických celkov a prezrite si potenciálne škodlivé udalosti na časovej osi s príslušnými akciami používateľa. ESET Inspect pracovníkom zodpovedným za riešenie incidentov automaticky navrhuje všetky súvisiace udalosti a objekty, čo môže výrazne pomôcť vo fáze triedenia, vyšetrovania a riešenia incidentov.

## MOŽNOSTI RÝCHLEJ REAKCIE

V rámci nástroja ESET Inspect je možné jedným kliknutím jednoducho spustiť rýchle akcie, ako sú manuálne kontroly, reštartovanie a vypnutie koncového zariadenia, izolovanie koncových zariadení od zvyšku siete, ukončenie akýchkoľvek spustených procesov či zablokovanie vybraných aplikácií na základe ich hodnoty hash. Vďaka možnosti rýchlej reakcie v nástroji ESET Inspect s názvom Terminal môžu navyše odborníci na bezpečnosť využívať komplexný balík možností vyšetrovania a nápravy v prostredí PowerShell.

## ANALÝZA PRÍČIN VZNIKU

Jednoducho si prezrite analýzu príčin vzniku a celú procesnú štruktúru akéhokoľvek potenciálne škodlivého reťazca udalostí, nechajte si zobraziť požadovanú úroveň podrobností a rozhodujte sa na základe obšírneho kontextu a vysvetlení legitímnych aj škodlivých zámerov, ktoré objasňujú naši odborníci na malvér.

## VEREJNÉ API

ESET Inspect poskytuje verejné rozhranie REST API, ktoré umožňuje prístup, export a riešenie detekcií, ako aj efektívnu integráciu s nástrojmi, ako sú napr. SIEM, SOAR, nástroje podpory a mnohé iné.

## VIACERO INDIKÁTOROV NARUŠENIA BEZPEČNOSTI

Zobrazte a zablokujte moduly na základe viac ako 30 rôznych ukazovateľov, medzi ktoré patrí hash, úpravy registra, zmeny súborov a sieťové pripojenia.

## VYHĽADÁVANIE HROZIEB

Použite účinné vyhľadávanie indikátorov IoC na základe zadanej požiadavky a využite filtre na triedenie nespracovaných dát podľa obľúbenosti súborov, reputácie, digitálneho podpisu, správania alebo iných kontextových informácií. Nastavenie viacerých filtrov umožňuje automatizované a jednoduché vyhľadávanie hrozieb a reakciu na incidenty vrátane schopnosti odhaliť a zastaviť pokročilé pretrvávajúce hrozby (APT) a cielené útoky.

## BEZPEČNÝ A BEZPROBLÉMOVÝ VZDIALENÝ PRÍSTUP

Riešenie incidentov a bezpečnostné služby môžu fungovať hladko len vtedy, keď je prístup k nim dostatočne jednoduchý, a to tak z hľadiska pripojenia ku konzole na strane pracovníka zodpovedného za riešenie incidentov, ako aj pripojenia ku koncovým zariadeniam. Pripojenie funguje takmer v reálnom čase, je maximálne zabezpečené a nie sú preň potrebné žiadne nástroje tretích strán.

## IZOLÁCIA OD SIETE JEDNÝM KLIKNUTÍM

Zadefinujte politiky prístupu k sieti, aby ste rýchlo predišli šíreniu malvéru naprieč celou sieťou. Napadnuté zariadenie je možné izolovať od siete jediným kliknutím v rozhraní nástroja ESET Inspect. Rovnako jednoduché je stav izolácie pre zariadenie ukončiť.

## DETEKCIA ANOMÁLIÍ A SPRÁVANIA

Skontrolujte akcie, ktoré boli vykonané spustiteľným súborom, a použite systém ESET LiveGrid®, ktorý na základe reputácie rýchlo posúdi, či sú spustené procesy bezpečné alebo podozrivé. Monitorovanie incidentov, ktoré súvisia s anomálnou aktivitou používateľov, zabezpečujú špeciálne pravidlá spúšťané na základe zachyteného správania, nie na základe detekčných vzoriek malvéru. Zaradenie počítačov do skupín podľa používateľov alebo oddelení umožňuje bezpečnostným tímom jednoducho identifikovať, či je používateľ oprávnený vykonať konkrétnu akciu alebo nie.

## INTERAKTÍVNE REPORTY O AKTIVITE

Narazili ste na podozrivý súbor? Odošlite ho do služby ESET LiveGuard Advanced na hĺbkovú analýzu prostredníctvom výkonného cloudového sandboxu. Za okamih dostanete interaktívny report o aktivite súboru, systémových zmenách či volaniach API, na základe ktorého sa môžete rozhodnúť všetko zablokovať.

## PRIRAĎOVANIE ZNAČIEK

Možnosť pridávať a odoberať značky pre jednotlivé objekty, ako sú napríklad počítače, výstražné upozornenia, vylúčenia, úlohy, spustiteľné súbory, procesy a skripty, slúži na jednoduché a rýchle filtrovanie. Značky sa zdieľajú medzi používateľmi, pričom novovytvorenú značku je možné priradiť v priebehu niekoľkých sekúnd.

## ZACHYTENIE PORUŠOVANIA FIREMNÝCH PRAVIDIEL

Zabráňte spúšťaniu škodlivých modulov na počítačoch vo firemnej sieti. Otvorená architektúra nástroja ESET Inspect poskytuje flexibilitu pri odhaľovaní porušovania pravidiel, ktoré sa týkajú používania konkrétnych druhov softvéru, napríklad torrentových aplikácií, cloudových úložísk, prehliadača Tor alebo iného nežiaduceho softvéru.

## OTVORENÁ ARCHITEKTÚRA A INTEGRÁCIE

ESET Inspect poskytuje jedinečnú detekciu na základe správania a reputácie, ktorá je pre bezpečnostné tímy úplne prehľadná. Všetky pravidlá sa dajú jednoducho upravovať prostredníctvom XML. Rovnako jednoduché je vytváranie nových pravidiel podľa potrieb konkrétnych firemných prostredí vrátane integrácií nástrojov SIEM.

## SOFISTIKOVANÉ VYHODNOTENIE ZÁVAŽNOSTI

Táto funkcia vám umožňuje stanoviť prioritu výstražných upozornení na základe ich závažnosti. Incidentom sa priraďuje úroveň závažnosti a správcovia tiež môžu jednoducho identifikovať počítače s vyššou pravdepodobnosťou možných incidentov.

eset Digital Security
Progress. Protected.

# Príklady použitia

## Detekcia správania a opakované porušovanie pravidiel

### PROBLÉM

Niektorí používatelia vo vašej sieti opakovane porušujú pravidlá v súvislosti s malvérom. Pravidelne sú infikované zariadenia tých istých používateľov. Je to v dôsledku rizikového správania? Alebo sa na nich útočníci zameriavajú častejšie než na ostatných?

### RIEŠENIE

- ✓ Jednoducho sledujte problémových používateľov a zariadenia.
- ✓ Rýchlo vykonajte analýzu príčin problémov a zistite zdroj infekcií.
- ✓ Vykonajte nápravu zistených vektorov infekcie, ako je napríklad e-mail, web alebo zariadenia USB.

## Jednoduché nastavenie a riešenie – aj bez potreby bezpečnostného tímu

### PROBLÉM

Nie všetky podniky majú k dispozícii osobitné bezpečnostné tímy, preto môže zadávanie a implementácia pokročilých pravidiel detekcie predstavovať problém.

### RIEŠENIE

- ✓ Viac ako 300 vstavaných, vopred nakonfigurovaných pravidiel.
- ✓ Kliknutím na jediné tlačidlo môžete rýchlo reagovať na incidenty a zablokovať alebo vypnúť zariadenia, prípadne ich umiestniť do karantény.
- ✓ Navrhované kroky na nápravu incidentov a ďalší postup sú integrované do výstrah.
- ✓ Pravidlá sa dajú jednoducho upravovať prostredníctvom jazyka XML. Rovnako ľahké je vytváranie nových pravidiel.

## Vyhľadávanie a blokovanie hrozieb

### PROBLÉM

Systém včasného varovania alebo bezpečnostné centrum vás upozornia na novú hrozbu. Čo spravíte?

### RIEŠENIE

- ✓ Využite systém včasného varovania na získanie údajov o blížiacich sa alebo nových hrozbách.
- ✓ Prehľadajte všetky počítače na prítomnosť novej hrozby.
- ✓ Prehľadajte všetky počítače s cieľom nájsť indikátory preukazujúce narušenie zabezpečenia a existenciu hrozby ešte pred zobrazením upozornenia.
- ✓ Zabráňte preniknutiu hrozby do siete alebo jej spusteniu v rámci organizácie.

## Prehľadnosť siete

### PROBLÉM

Niektoré podniky majú obavy v súvislosti s aplikáciami, ktoré používatelia spúšťajú v systémoch. Znepokojenie pritom nevyvolávajú len tradične inštalovateľné aplikácie, ale aj prenosné aplikácie, ktoré inštalovať netreba. Ako ich možno mať pod kontrolou?

### RIEŠENIE

- ✓ Jednoducho zobrazte a filtrujte všetky nainštalované aplikácie na zariadeniach.
- ✓ Zobrazte a filtrujte všetky skripty v zariadeniach.
- ✓ Bez problémov zablokujte spustenie neoprávnených skriptov alebo aplikácií.
- ✓ Upozornite používateľov na neoprávnené aplikácie a automaticky ich odinštalujte.

# Dôkladná detekcia hrozieb – ransomvér

## PROBLÉM

Firma potrebuje ďalšie nástroje na proaktívne odhaľovanie ransomvéru, nielen okamžité upozornenia na zistenie správania v sieti, ktoré pripomína ransomvér.

## RIEŠENIE

- ✓ Zadajte pravidlá na detekciu aplikácií, ktoré sa spustia z dočasných priečinkov.
- ✓ Zadajte pravidlá na detekciu súborov balíka Office (Word, Excel, PowerPoint), ktoré spustia ďalšie skripty alebo súbory.
- ✓ Nastavte upozornenia na prípady, keď sa v zariadení zistí niektorá z najčastejších prípon ransomvéru.
- ✓ Prezerajte si výstrahy funkcie Ransomware Shield z riešení ESET na ochranu koncových zariadení v jednej konzole.

# Prešetrenie a náprava zohľadňujúce kontext

## PROBLÉM

Užitočnosť údajov závisí od ich kontextu. Ak chcete uskutočňovať správne rozhodnutia, potrebujete poznať výstražné upozornenia, zariadenia, na ktorých k nim dochádza, a používateľov, ktorí ich vyvolávajú.

## RIEŠENIE

- ✓ Identifikujte a usporiadajte všetky počítače podľa služby Active Directory alebo automatického či manuálneho zoskupenia.
- ✓ Povoľte alebo zablokujte aplikácie alebo skripty na základe zoskupenia počítačov.
- ✓ Povoľte alebo zablokujte aplikácie alebo skripty podľa používateľa.
- ✓ Nastavte prijímanie upozornení len z určitých skupín.

ESET Digital Security
Progress. Protected.

# Toto je ESET

## Proaktívna ochrana. Minimalizujte riziká vďaka prevencii.

Buďte o krok vpred pred známymi aj novými kybernetickými hrozbami vďaka nášmu prístupu, ktorý je založený na umelej inteligencii a zameraný na prevenciu. Kombinovaním sily umelej inteligencie a odborných znalostí našich pracovníkov dokážeme poskytovať jednoduchú a efektívnu ochranu.

ESET PROTECT, naša cloudová platforma kybernetickej bezpečnosti s podporou XDR, kombinuje next-gen schopnosti prevencie, detekcie a proaktívneho vyhľadávania hrozieb so širokou škálou bezpečnostných služieb vrátane riadenej detekcie a reakcie (MDR). Naše vysoko prispôsobiteľné riešenia zahŕňajú podporu v lokálnom jazyku, majú minimálny vplyv na výkon zariadenia, identifikujú a zneškodnia známe aj nové hrozby ešte v zárodku, podporujú plynulý chod prevádzky a znižujú náklady na implementáciu a správu.

ESET chráni vašu firmu, aby ste mohli naplno využívať potenciál technológií.

## ESET V ČÍSLACH

**1 mld.+**
chránených používateľov internetu

**400-tis.+**
firemných zákazníkov

**200**
krajín a teritórií

**13**
globálnych centier výskumu a vývoja

## NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV

MITSUBISHI MOTORS
Drive your Ambition

Viac než 9 000 koncových zariadení chránených spoločnosťou ESET od roku 2017

Allianz Suisse

Viac než 4 000 e-mailových schránok chránených spoločnosťou ESET od roku 2016

Canon
Canon Marketing Japan Group

Viac než 32 000 koncových zariadení chránených spoločnosťou ESET od roku 2016

Bezpečnostný partner v oblasti poskytovania internetových služieb 2 miliónom zákazníkov od roku 2008

## UZNANIE

AV comparatives APPROVED Business Security DEC 2023

V nezávislých testoch AV-Comparatives dosahuje ESET stabilne najlepšie výsledky a najlepšiu mieru detekcie bez falošných poplachov alebo len s minimálnym počtom nesprávne detegovaných položiek.

G2 Leader WINTER 2024

Spoločnosť ESET neustále dosahuje najvyššie hodnotenia od používateľov na globálnej platforme G2 a jej riešenia oceňujú zákazníci po celom svete.

kuppingercole ANALYSTS

ESET je podľa spoločnosti KuppingerCole celkovým a trhovým lídrom v hodnotení MDR Leadership Compass 2023.

eset Digital Security
Progress. Protected.