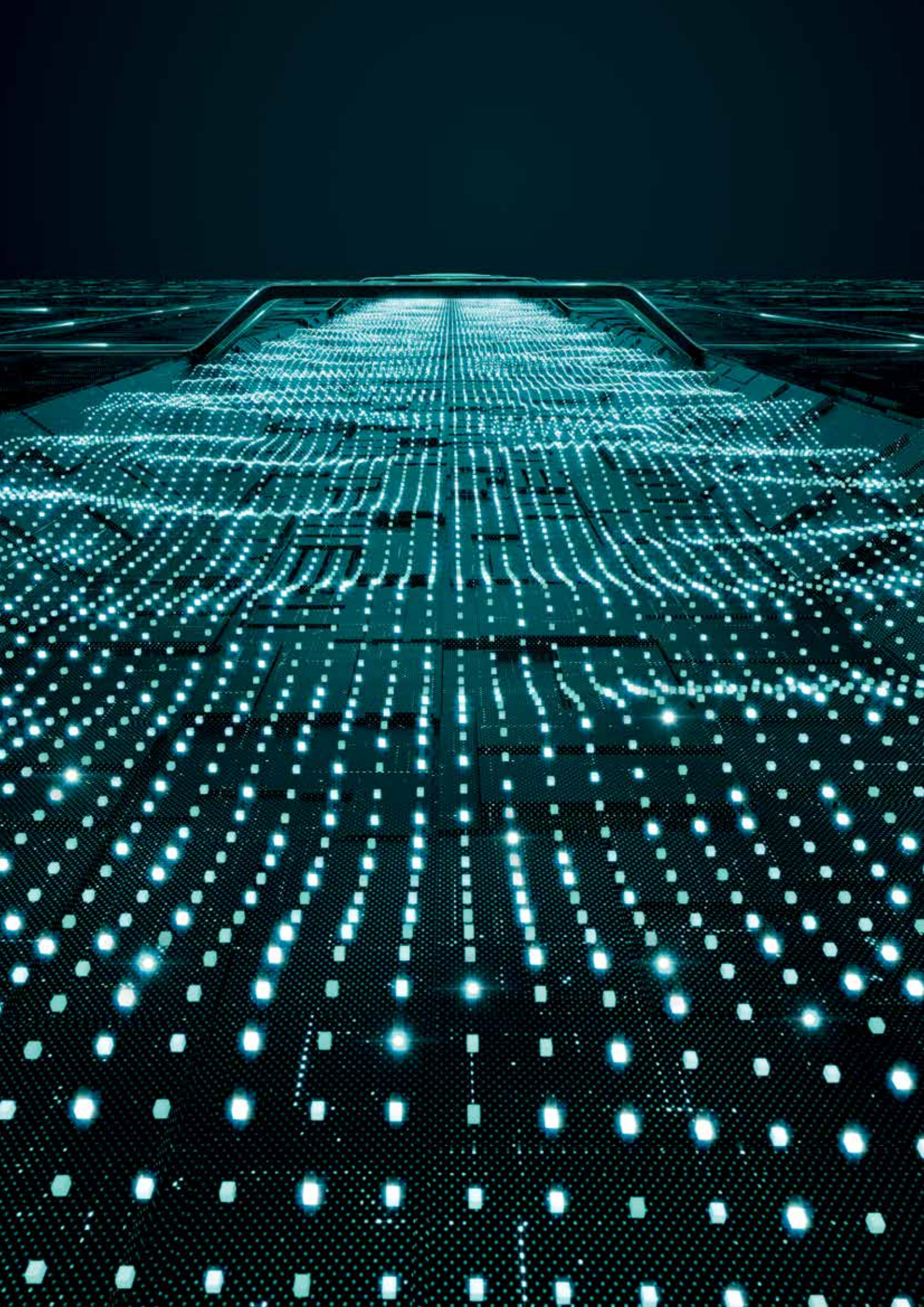
ENTERPRISE INSPECTOR

Nástroj EDR sloužící k **odhalení nezvyklého chování ve vaší počítačové síti.**

ENJOY SAFER TECHNOLOGY™



Co je **ESET Enterprise Inspector?**

ESET Enterprise Inspector je sofistikovaný nástroj, který slouží k identifikaci nezvyklého chování a průniků a posouzení rizik stejně jako k vyšetření, nápravě a odpovědi na bezpečnostní incidenty.

V reálném čase monitoruje a vyhodnocuje všechny aktivity v síti (například chování uživatelů, soubory, procesy, registry, paměť a události), což organizacím umožňuje v případě potřeby rychle zareagovat.

Proč **ESET Enterprise Inspector?**

ÚNIKY DAT

Firmy potřebují o úniku dat nejen vědět, ale zároveň musejí mít možnost úniku zabránit a napravit způsobené škody. IT týmy by měly mít přehled o tom, zda právě neprobíhá malwarový útok, nedochází k rizikovému chování uživatelů či na počítačích nejsou instalované nechtěné aplikace, které by přímo nebo nepřímo ohrožovaly finanční výsledky společnosti a její reputaci.

Největší nebezpečí útoku hrozí u firem, jež vlastní nějaká hodnotná data. Jde například o finanční instituce, zdravotní i jiné pojišťovny, úřady ve veřejném sektoru a podobně. To ovšem neznamená, že ostatní firmy jsou v bezpečí. Útočníci vždy poměřují riziko útoku s možným ziskem.

POKROČILÉ PERSISTENTNÍ HROZBY A CÍLENÉ ÚTOKY

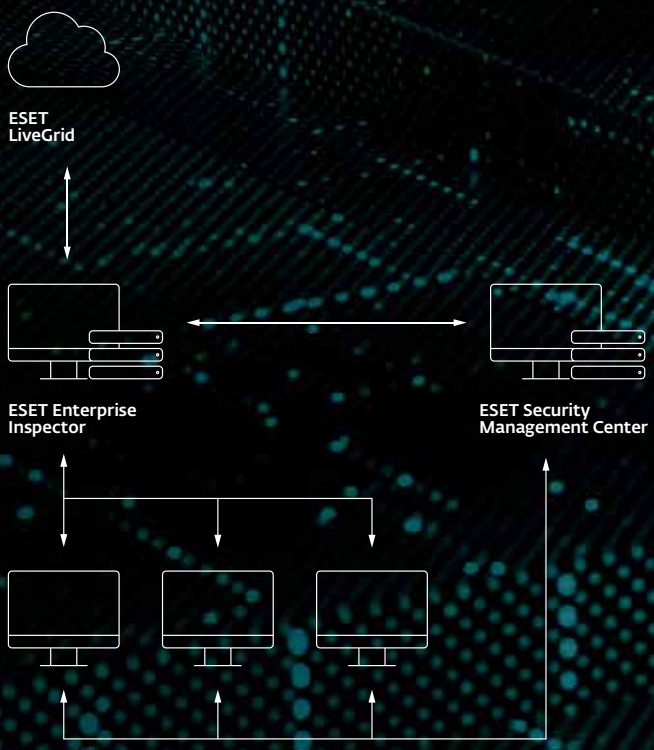
Systémy EDR se obvykle používají k identifikaci persistentních hrozeb (APT) a cílených útoků, snížení reakční doby na incident a k proaktivní preventivní ochraně proti útokům v budoucnu. Obzvláště důležitá je schopnost odhalovat APT, které mohou být aktivní dlouhou dobu, aniž by došlo k jejich odhalení. Následné škody tak mohou být pro firmu velmi citelné.

Poskytuje **unikátní detekci** založenou **na analýze chování a reputaci,** což je postup plně transparentní pro bezpečnostní týmy.

PŘEHLED O UDÁLOSTECH

Největším rizikem pro velké firmy jsou interní hrozby a phishingové útoky. Hrozí hlavně Společnostem a organizacím s velkým počtem zaměstnanců, kde je statisticky vyšší pravděpodobnost, že se někdo nechá nachytat a spustí škodlivý soubor. Další zmíněnou hrozbou u velkých společností jsou interní útoky – kvůli velkému počtu zaměstnanců se opět zvyšuje šance, že se nespokojený zaměstnanec bude snažit svým jednáním poškodit firmu.

Systémy EDR umožňují odpovědným IT pracovníkům mít lepší přehled o právě probíhajících událostech v síti. Od blokování infikovaných e-mailových příloh až po zajištění faktu, že zaměstnanci přistupují a používají jen data a zdroje, které potřebují ke své práci.



Ochrana koncových zařízení
Bezpečnostní řešení ESET odesílají do ESET Enterprise Inspectoru data ze všech vrstev ochrany.

+

ESET Enterprise Inspector
Sofistikovaný nástroj EDR, který v reálném čase analyzuje všechna dostupná data. Zásadně snižuje riziko, že nedojde k odhalení hrozby.

=

Kompletní řešení prevence a detekce, které umožňuje rychlou analýzu a reakci na jakýkoli bezpečnostní incident v síti.

IT týmy potřebují mít přehled, zda právě neprobíhá **malwarový útok, nedochází k rizikovému chování uživatelů** či na počítačích nejsou instalované **nechtěné aplikace**.

Výhody

SYNCHRONIZOVANÁ REAKCE

ESET Enterprise Inspector spolupracuje se všemi produkty v síti ESET, a vytváří tak konzistentní ekosystém, který umožňuje synchronizované řešení bezpečnostních incidentů. IT týmy pak mohou ukončit procesy, stáhnout soubor působící poplach či vypnout nebo restartovat vzdálený počítač přímo z konzole.

OTEVŘENÁ ARCHITEKTURA

Provádí unikátní založenou na analýze chování a reputaci. Všechna pravidla lze snadno editovat pomocí jazyka XML, aby co nejpřesněji vyhovovala specifickým potřebám každého firemního prostředí, včetně integrace s nástroji SIEM.

VZDÁLENÝ PŘÍSTUP

Správce může spustit PowerShell terminál v prostředí ESET Enterprise Inspector a vzdáleně kontrolovat a měnit konfigurace firemních počítačů, aniž by narušoval práci daného uživatele.

PODPORA RŮZNÝCH PLATFOREM

ESET Enterprise Inspector podporuje Windows a MacOS, takže jde o vhodný nástroj i do multiplatformních IT prostředí.

VEŘEJNÉ API

Umožňuje integrovat údaje z ESET Enterprise Inspectoru do již používaných nástrojů jako je SIEM, SOAR a podobně. Správce tak nemusí sledovat dva různé nástroje, ale otevřít ESET Enterprise Inspector jen například v případě probíhajícího útoku.

NASTAVENÍ CITLIVOSTI

Snížením citlivosti pravidel může správce snadno omezit počet falešných poplachů u konkrétních uživatelů nebo skupin. Kombinací kritérií jako název souboru, cesta, hash nebo parametry spuštění lze jemně vyladit podmínky aktivace pravidel podle vlastních potřeb.

MITRE ATT&CK™

ESET Enterprise Inspector odesílá informace o detekcích do globální databáze MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), kde na jedno kliknutí můžete najít detailní informace o velmi komplexních hrozbách,

REPUTAČNÍ SYSTÉM

Náš reputační systém obsahuje databázi o stovkách milionů souborů, které byly vyhodnoceny jako bezpečné, a bezpečnostní týmy se tak mohou zaměřit na ty neznámé nebo chybně detekované.

Příklady použití

Hloubková detekce hrozby – ransomware

Ransomware se snaží nepozorovaně nakazit co největší počet koncových zařízení. Pokouší se infikovat i zálohy, aby ani vrácení do předchozího stavu nezabránilo opětovnému spuštění škodlivého kódu.

ESET Enterprise Inspector rozšiřuje a doplňuje funkčnost produktů pro ochranu koncových stanic. Umožňuje proaktivní detekci ransomwaru, který již může existovat ve vaší síti. V typickém scénáři ransomwarové nákazy přijde uživateli do poštovní schránky e-mail s dokumentem v příloze. Uživatel jej otevře a následně je vyzván ke spuštění maker. Pokud k tomu dojde, do systému se nahraje spustitelný soubor, který začne šifrovat vše, co je pro něj dostupné, včetně mapovaných disků.

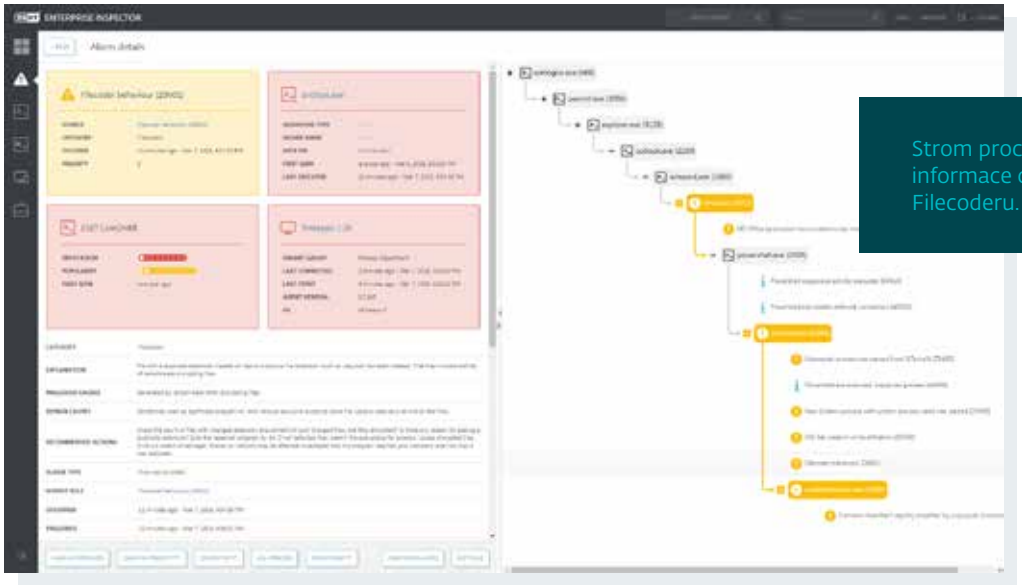
ESET Enterprise Inspector na takový druh chování upozorní správce IT, který na několik kliknutí uvidí, jaké soubory byly postiženy, kde a kdy došlo ke spuštění škodlivých souborů, a může zpětně analyzovat příčinu nákazy

PŘÍKLAD POUŽITÍ

Firmy požadují další nástroj na proaktivní detekci ransomwaru a rychlé upozornění na chování v síti, které činnost ransomwaru připomíná.

ŘEŠENÍ

- ✓ Vložení pravidel pro detekci aplikací v případě, že se spouští z dočasných adresářů.
- ✓ Vložení pravidel pro detekci souborů MS Office (Word, Excel, Powerpoint), pokud z nich dojde ke spuštění skriptů nebo spustitelných souborů.
- ✓ Upozornění na výskyt známých přípon typických pro ransomware.
- ✓ Správce vidí upozornění z bezpečnostních řešení (modul ochrany proti ransomwaru) na koncových stanicích ve společné konzoli.



Strom procesů a detailní informace o chování Filecoderu.

Detekce chování rizikových uživatelů

Nejslabším článkem při ochraně firemní sítě je uživatel sedící za klávesnicí, a to i ten bez zlých úmyslů.

ESET Enterprise Inspector umožňuje správci seřadit počítače podle počtu spuštění unikátních poplachů. Pokud uživatel spustí vícero poplachů, jde o jasný signál k ověření dané aktivity.

PŘÍKLAD POUŽITÍ

V síti se vyskytují klientské počítače, na kterých opakovaně dochází k infekci škodlivým kódem. Je to důsledek riskantního chování, nebo jsou dané počítače častěji cílem malwarových útoků?

ŘEŠENÍ

- ✓ Přehled o problémových uživatelích a zařízeních.
- ✓ Rychlé dokončení analýzy příčin problému a nalezení zdroje infekce.
- ✓ Oprava nalezených vektorů útoku, jako je e-mail, web nebo zařízení USB.

Hledání a blokace hrozeb

Hlavní výhodou ESET Enterprise Inspectoru je způsob, jakým hledá hrozby.

Jakoukoli škodlivou aktivitu lze snadno identifikovat a prošetřit pomocí filtrování posbíraných dat na základě popularity nebo reputace souboru, digitálního podpisu, chování a kontextových informací. Násobné filtry umožňují nastavit úroveň detekce dle specifických potřeb dané firmy a vytvořit úlohy, které automaticky hledají podezřelou aktivitu.

Jakoukoli škodlivou aktivitu lze snadno identifikovat a vyšetřit.

PŘÍKLAD POUŽITÍ

Systém včasného varování nebo bezpečnostní centrum (SOC) upozorní na novou hrozbu. Jak postupovat?

ŘEŠENÍ

- ✓ Systém včasného varování umožňuje získat data o nadcházejících nebo nových hrozbách.
- ✓ Prohledání všech počítačů na přítomnost nové hrozby.
- ✓ Nalezení indikátorů nákazy, které ukazují na existenci hrozby před samotným varováním.
- ✓ Blokace hrozby před infiltrací do sítě nebo spuštěním uvnitř sítě.

Přehled o dění v síti

ESET Enterprise Inspector je řešení s otevřenou architekturou, což umožňuje bezpečnostním týmům nastavit vlastní pravidla detekce útoků, která vyhovují specifickým požadavkům dané firmy.

Otevřená architektura také přináší možnost nastavení ESET Enterprise Inspectoru, aby detekoval porušení interních softwarových politik (používání torrentových sítí, cloudových úložišť, prohlížeče Tor, provozování vlastních serverů a podobně).

PŘÍKLAD POUŽITÍ

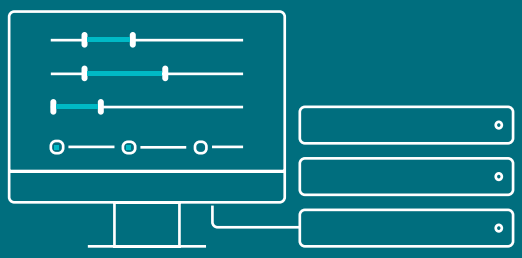
Pro bezpečnost firmy je důležité, aby existoval přehled o instalovaných a používaných aplikacích. A nejde jen o aplikace instalované standardním způsobem, ale i o přenosné aplikace, které není potřeba instalovat.

ŘEŠENÍ

- ✓ Přehled a možnost filtrování napříč všemi aplikacemi na všech zařízeních.
- ✓ Přehled a možnost filtrování všech skriptů napříč zařízeními.
- ✓ Snadná blokace spuštění neautorizovaných skriptů a aplikací.
- ✓ Upozornění uživatele na používání neautorizovaných aplikací a jejich odinstalace.

Pro bezpečnost firmy je důležité, aby existoval přehled o instalovaných a používaných aplikacích. A nejde jen o aplikace instalované standardním způsobem, ale i o přenosné aplikace, které není potřeba instalovat.

Bezpečnostní týmy můžou **nastavit vlastní pravidla** detekce útoků, která vyhovují specifickým požadavkům dané firmy.



Vyšetřování a náprava incidentů se znalostí kontextu

„Škodlivost“ aktivity závisí na kontextu.

Aktivity na počítačích administrátorů jsou zcela jiného charakteru než u pracovníků finančního oddělení. Při správném zařazení stanic do skupin je pro správce snadné určit, zda má konkrétní uživatel oprávnění k prováděné aktivitě na daném počítači. Synchronizací skupin z nástroje vzdálené správy ESET Security Management Center s pravidly z ESET Enterprise Inspectoru získá správce potřebné informace o kontextu prováděné aktivity.

PŘÍKLAD POUŽITÍ

Sesbíraná data by bez kontextu byla k ničemu. Aby se mohl správce správně rozhodnout, potřebuje vědět nejen o poplachu samotném, ale také o jeho zdroji a o uživateli, který jej spustil.

ŘEŠENÍ

- ✓ Identifikace a řazení všech počítačů dle Active Directory, automatické nebo manuální zařazení do skupin.
- ✓ Povolení či blokace aplikace nebo skriptů na základě zařazení počítače do skupin.
- ✓ Povolení či blokace aplikace nebo skriptu na základě uživatele.
- ✓ Upozornění pouze pro určité skupiny uživatelů.

Snadné nastavení i reakce – bez nutnosti bezpečnostního týmu

I když má firma dedikované bezpečnostní týmy, není vždy jednoduché najít nejpodstatnější spuštěné poplachy a rozhodnout o dalších krocích.

ESET Enterprise Inspector nabízí při nalezení hrozby další možné kroky. Soubory je možné blokovat na základě hashe, procesy ukončit nebo dát do karantény a vybrané počítače izolovat nebo vzdáleně vypnout.

PŘÍKLAD POUŽITÍ

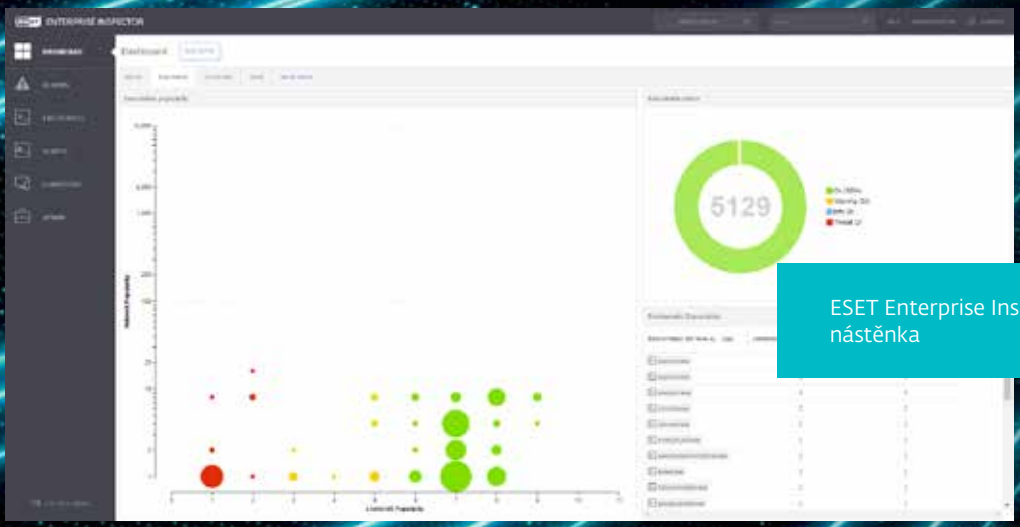
Ne všechny firmy mají vlastní bezpečnostní IT tým, takže implementace pravidel detekce může být náročným úkolem.

ŘEŠENÍ

- ✓ Přes 300 připravených pravidel.
- ✓ Snadná reakce pomocí jednoho kliknutí, které počítač zablokuje, ukončí nebo ho zařadí do karantény.
- ✓ Doporučený postup pro konkrétní poplachy.
- ✓ Pravidla lze snadno editovat nebo vytvářet pomocí XML.

„Škodlivost“ aktivity závisí na kontextu. Synchronizací skupin z nástroje vzdálené správy ESET Security Management Center s pravidly z ESET Enterprise Inspectoru správce získá potřebné informace o kontextu prováděné aktivity.

U každého spuštěného poplachu je připojen postup pro jeho nápravu.



ESET Enterprise Inspector - nástěnka

Technické funkce

HLEDÁNÍ HROZEB

Správce může filtrovat data na základě popularity souboru, reputace, digitálního podpisu, chování a kontextových informací. Nastavení více filtrů umožňuje automatické hledání hrozeb (včetně cílených útoků a pokročilých persistentních hrozeb), které lze přizpůsobit specifickým podmínkám dané sítě.

DETEKCE INCIDENTU (ANALÝZA PŘÍČINY)

V sekci poplachů jsou zařazené všechny bezpečnostní incidenty. Bezpečnostní tým si může prohlédnout analýzu příčiny poplachu, včetně informací o postižených souborech, kde a kdy byl spuštěn škodlivý skript, akce nebo spustitelný soubor.

VYŠETŘOVÁNÍ A NÁPRAVA

Správce může pro prevenci incidentů použít připravená pravidla nebo si vytvořit vlastní. Každý spuštěný poplach obsahuje informaci s doporučeným postupem nápravy. Specifické soubory je možné blokovat na základě hashe, procesy lze ukončit nebo přidat do karantény, a vybrané počítače izolovat nebo vzdáleně vypnout.

BLESKOVÁ IZOLACE

Definováním politik pro přístup k síti může správce rychle reagovat na probíhající malware útok. Jedním kliknutím v ESET Enterprise Inspector lze odpojit a izolovat infikované zařízení, a podobně rychle také zařízení připojit zpět do firemní sítě.

HODNOCENÍ RIZIKA

Správce si může hodnocení závažnosti poplachů nastavit podle zvolených atributů a jednoduše tak identifikovat počítače s vyšším rizikem potenciálního incidentu.

ŠTÍTKY

Administrátor může rychle filtrovat objekty v ESET Enterprise Inspector jako jsou počítače, poplachy, výjimky, úlohy, spustitelné soubory, procesy a skripty. Štítky se sdílejí mezi uživateli, po vytvoření je může správce přiřadit během pár sekund..

SBĚR DAT

Prohlédněte si podrobné informace o nově spuštěných modulech, včetně údajů o času spuštění, uživateli, době aktivity a postižených zařízeních. Všechna data se ukládají lokálně jako prevence úniku citlivých dat.

BEZPEČNÉ PŘIHLÁŠENÍ

Dvoufaktorová autentizace je další vrstvou ochrany, která zabrání útočníkovu v přístupu na zařízení, i když má správné heslo.

DETEKCE INDIKÁTORŮ NÁKAZY

Správce může zkontrolovat a zablokovat moduly na základě 30 různých indikátorů, jako je hash, modifikace registrů, změny souboru a síťového připojení.

DETEKCE CHOVÁNÍ A ANOMÁLIÍ

Zkontrolujte akci, kterou provedl spustitelný soubor, a s pomocí reputačního systému ESET LiveGrid můžete rychle zjistit, zda je spuštěný proces bezpečný nebo podezřelý. Řazení počítačů do skupin dle uživatele, oddělení nebo jiných kritérií umožňuje bezpečnostním týmům rychle zjistit, zda konkrétní uživatel má, nebo nemá oprávnění k provedení dané akce.

PORUŠENÍ FIREMNÍ POLITIKY

Blokujte spuštění škodlivých modulů. Otevřená architektura ESET Enterprise Inspectoru umožňuje správcům detekovat porušení firemních politik o používání povoleného softwaru (torrenty, cloudová úložiště, anonymní prohlížení webu pomocí Toru atd.)

O ESETu

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která díky dlouhodobě vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100. Za těmito úspěchy stojí zejména dlouhodobé investice do vývoje.

Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

ESET V ČÍSLECH

110m+
uživatelů po celém světě

400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

NAŠI ZÁKAZNÍCI

MITSUBISHI MOTORS
Drive your Ambition

Zákazníkem od roku 2017
více než 14,000 licencí

Canon
Canon Marketing Japan Group

Zákazníkem od roku 2016
více než 9,000 licencí

Allianz Suisse

Zákazníkem od roku 2016
více než 4,000 mailboxů

T

ISP partnerem od roku 2008
2 miliony zákazníků

ESET je v souladu s ISO/IEC 27001:2013, mezinárodně uznávaným a použitelným bezpečnostním standardem pro implementaci a správu bezpečnosti informací. Certifikaci uděluje akreditovaný certifikační orgán SGS a potvrzuje plný soulad ESET s nejlepšími přístupy v daném oboru.

ESET odesílá informace do globálně přístupné databáze MITER ATT&CK. ESET je jedním z nejvýznamnějších prodejců a aktivních přispěvatelů, potvrzuje tak svůj závazek poskytovat co nejlepší ochranu komunitě a zákazníkům.

OCENĚNÍ

ESET byl jediným Vyzyvatelem v hodnocení Gartner Magic Quadrant for Endpoint Protection Platforms 2019, již druhým rokem za sebou.

ESET byl ohodnocen jako Strong Performer ve zprávě The Forrester Wave(TM): Endpoint Security Suites, Q3 2019.

ESET ohodnocen jako „Top Player" ve zprávě Radicati Endpoint Security 2019, která zvažovala dvě hlavní kritéria: funkčnost a strategickou vizi.

Společnost Gartner nepodporuje žádného prodejce, produkt ani službu, které uvádí ve svých výzkumných publikacích, a jejím cílem není doporučit uživatelům technologií jen prodejce s nejlepším hodnocením. Výzkumné publikace společnosti Gartner obsahují názory výzkumných organizací Gartner a neměly by vyznít jako tvrzení faktu. Gartner se zříká všech záruk, vyjádřených nebo předpokládaných s ohledem na výzkum, včetně záruky obchodovatelnosti nebo vhodnosti pro konkrétní účel.

Gartner Peer Insights je bezplatná platforma pro hodnocení navržená pro osoby s rozhodovacím právem pro nákup firemního softwaru a služeb. Recenze prochází přísným procesem validace, aby se zajistilo, že informace jsou autentické. Recenze společnosti Gartner Peer Insights představují subjektivní názory jednotlivých koncových uživatelů na základě jejich vlastních zkušeností a nepředstavují názory společnosti Gartner nebo jejích přidružených společností.

ENJOY SAFER TECHNOLOGY™

190717