PŘEHLED

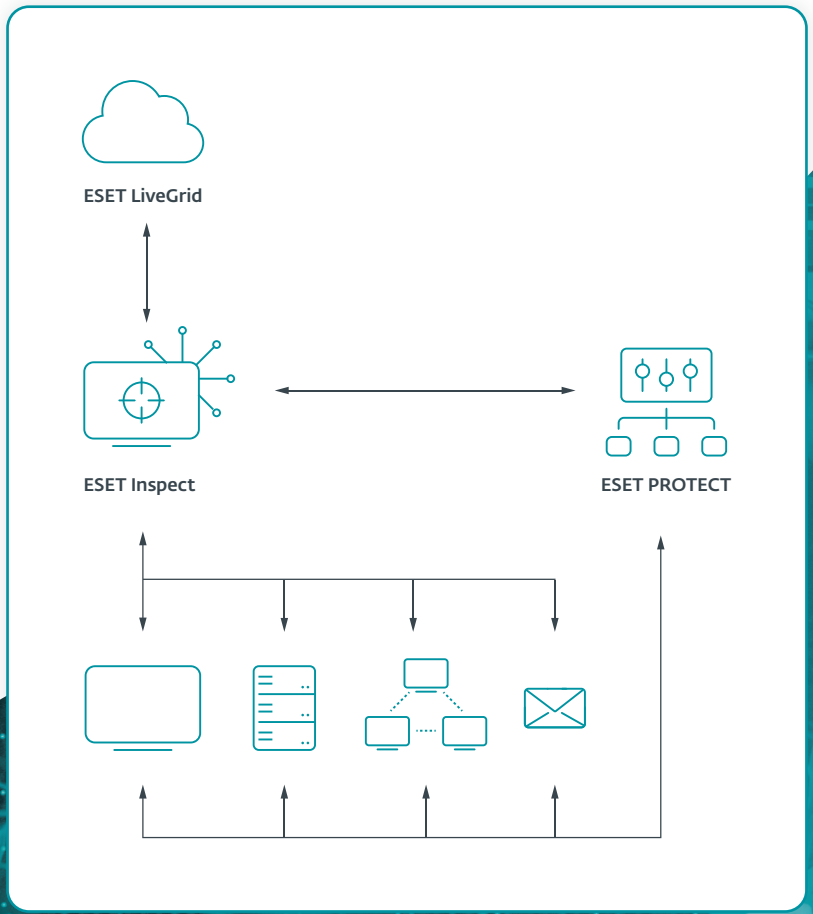
INSPECT

Komponenta platformy ESET PROTECT sloužící k odhalení nezvyklého chování v síti, reakci a nápravě.

Co je **řešení rozšířené detekce a reakce (XDR)**?

ESET Inspect je součást platformy ESET PROTECT zajišťující funkce XDR (detekce problémů a reakce na ně). Je to nástroj k identifikaci neobvyklého chování a narušení zabezpečení, hodnocení rizik, reakci na incidenty, jejich vyšetřování a nápravě.

Umožňuje specialistům zodpovědným za reakci na incidenty monitorovat a vyhodnocovat všechny aktivity v síti a na připojených zařízeních. V případě potřeby dokáže pomoci automatizovat okamžitá nápravná opatření. Více než 800 pravidel detekce společnosti ESET (a další stále přibývají) umožňuje komplexní vyhledávání hrozeb.



Výhody řešení ESET

KOMPLEXNÍ FUNKCE PREVENCE, DETEKCE A REAKCE

Umožňuje rychlou analýzu a nápravu jakéhokoli bezpečnostního problému v síti. Vícevrstvé bezpečnostní nástroje ESET, které z každé vrstvy odesílají data do služby ESET Inspect, zvládají v reálném čase analyzovat obrovské množství dat, takže jim neunikne žádná hrozba.

ŘEŠENÍ OD DODAVATELE SPECIALIZOVANÉHO NA ZABEZPEČENÍ

Společnost ESET bojuje proti kybernetickým hrozbám již více než 30 let. Staví při tom na vědeckém výzkumu a dlouhodobě je na špičce v oborech, jako jsou strojové učení, cloudové technologie a dnes také XDR.

PREVENCE JE LEPŠÍ NEŽ LÉČBA

Řešení XDR společnosti ESET úzce propojuje se svými oceňovanými produkty pro prevenci hrozeb. Neustále usilujeme o vývoj kvalitních technologií pro detekci hrozeb, proto jsou špičkové i naše technologie pro jejich prevenci.

DETAILNÍ PŘEHLED O SÍTI

Díky transparentním pravidlům detekce (ESET jich má přes 800 a další stále přibývají), pokročilým ukazatelům narušení systému a vyhledávacím funkcím vám hloubková kontrola spustitelných souborů (In-Depth Executable Review) v síti umožní odhalit cokoli podezřelého.

FLEXIBILNÍ NASAZENÍ

Sami rozhodnete, jak řešení nasadíte: ESET Inspect může běžet na vašich vlastních serverech lokálně, nebo v cloudu. Můžete tak nastavení vyladit podle svých cílů v oblasti celkových nákladů a kapacity hardwaru.

ŘEŠENÍ, KTERÉ MŮŽE HNED ZAČÍT FUNGOVAT

Řešení ESET je připravené k okamžitému spuštění. Zároveň ale dovoluje, aby ho zkušení specialisté na vyhledávání hrozeb podrobně vyladili.

MITRE ATT&CK

Svoje funkce pro detekci zakládá ESET Inspect na znalostní databázi MITRE ATT&CK™ (Adversarial Tactics, Techniques, and Common Knowledge). Ta dovoluje jediným kliknutím vyhledat podrobné informace i o těch nejkomplexnějších hrozbách.

REPUTAČNÍ SYSTÉM

Rozsáhlé možnosti filtrování umožňují specialistům na zabezpečení s využitím robustního reputačního systému ESET rozpoznat všechny aplikace, o kterých je známo, že neobsahují problémy. Systém společnosti ESET obsahuje databázi stovek milionů neškodných souborů. Bezpečnostní týmy tak mohou soustředit své úsilí na neznámé, potenciálně škodlivé soubory, nikoli na falešně detekované problémy.

AUTOMATIZACE A PŘIZPŮSOBENÍ

Řešení ESET Inspect můžete snadno vyladit na takovou úroveň podrobností a automatizace, jakou potřebujete. Během úvodního nastavení si s pomocí přednastavených uživatelských profilů zvolíte požadovanou míru interakce a typ a množství dat, která se mají ukládat. Software poté v režimu učení zmapuje prostředí vaší firmy a tam, kde je třeba, navrhne výjimky, které pokryjí falešná varování.

Možnosti řešení

SYSTÉM SPRÁVY INCIDENTŮ

Objekty, jako jsou detekce, počítače, spustitelné soubory či procesy, můžete seskupit do logických jednotek, které vám umožní zobrazit potenciálně škodlivé události na časové ose spolu se souvisejícími akcemi uživatelů. ESET Inspect specialistovi, který na incident reaguje, automaticky navrhne všechny související události a objekty. To může výrazně pomoci ve fázích třídění, šetření i řešení incidentu.

MOŽNOSTI OKAMŽITÉ REAKCE

Součástí řešení ESET Inspect jsou snadno dostupné akce, které umožňují reagovat jedním kliknutím: například restartování a vypnutí koncového zařízení, izolace koncových zařízení od zbytku sítě, spuštění volitelné kontroly, ukončení veškerých běžících procesů a blokování libovolné aplikace na základě její hodnoty hash. Možnost okamžité reakce navíc bezpečnostním specialistům umožňuje využít úplnou sadu možností šetření a nápravy v prostředí PowerShell.

ANALÝZA PRVOTNÍCH PŘÍČIN

U jakéhokoli potenciálně škodlivého řetězce událostí si můžete jednoduše zobrazit analýzu prvotních příčin a úplný procesní strom, přejít na požadovanou úroveň podrobností a informovaně se rozhodovat na základě podrobných souvislostí a vysvětlení neškodných i škodlivých příčin.

VEŘEJNÉ ROZHRANÍ API

Řešení ESET Inspect zahrnuje veřejné rozhraní REST API, které umožňuje přístup k detekcím a jejich export a nápravu. Rozhraní usnadňuje účinnou integraci s nástroji jako SIEM, SOAR, nástroji pro správu ticketů podpory a mnoha dalšími aplikacemi.

VÍCE UKAZATELŮ NARUŠENÍ

Můžete zobrazit a blokovat moduly na základě více než 30 různých ukazatelů, včetně hodnot hash, změn registru a souborů nebo připojení k síti.

VYHLEDÁVÁNÍ HROZEB

Účinné vyhledávání ukazatelů narušení založené na dotazech a možnosti filtrování surových dat vám nabízí třídění podle popularity souborů, reputace, digitálních podpisů, chování a jiných kontextových informací. Když si nastavíte více filtrů, můžete využít snadné automatizované vyhledávání hrozeb a reakci na incidenty, které zahrnují i možnost detekovat a zastavit pokročilé trvalé hrozby a cílené útoky.

BEZPROBLÉMOVÝ A BEZPEČNÝ VZDÁLENÝ PŘÍSTUP

Reakce na incidenty a bezpečnostní služby jsou operativní jen v případě, že jsou snadno dostupné a specialista se může jednoduše připojit jak ke konzoli, tak ke koncovým zařízením. Připojení funguje prakticky v reálném čase a využívá maximální bezpečnostní opatření bez nutnosti nasazovat nástroje třetích stran.

IZOLACE JEDNÍM KLIKNUTÍM

Můžete definovat zásady přístupu k síti, které rychle zastaví laterální pohyb škodlivého kódu. Napadené zařízení izolujete od sítě jediným kliknutím v rozhraní ESET Inspect. Ze stavu omezení však zařízení také snadno odeberete.

DETEKCE NEOBVYKLÉHO CHOVÁNÍ

Můžete zkontrolovat akce prováděné spustitelným souborem a využít reputační systém ESET LiveGrid®, který vám pomůže rychle zhodnotit, zda jsou spuštěné procesy bezpečné, nebo podezřelé. Monitorování neobvyklých incidentů souvisejících s uživateli je možné díky konkrétním pravidlům nastavit tak, aby je spustilo určité chování, nikoli jednoduchý škodlivý kód nebo detekce. Seskupení počítačů podle uživatelů či oddělení umožňuje bezpečnostním týmům určit, zda má uživatel oprávnění provádět konkrétní akci.

OZNAČOVÁNÍ ŠTÍTKY

Přiřazením a odebíráním štítků můžete rychle filtrovat objekty, jako jsou počítače, upozornění, výjimky, úlohy, spustitelné soubory, procesy a skripty. Štítky se sdílejí mezi uživateli a jakmile je vytvoříte, dají se přiřadit během pár sekund.

DETEKCE PORUŠENÍ FIREMNÍCH ZÁSAD

Můžete zablokovat škodlivé moduly tak, aby se nedaly spustit na žádném počítači v síti vaší firmy. Otevřená architektura řešení ESET Inspect dovoluje flexibilně rozpoznávat porušení zásad, které platí pro používání určitých typů softwaru, jako jsou torrentové aplikace, cloudová úložiště, prohlížeče Tor nebo jiný nežádoucí software.

OTEVŘENÁ ARCHITEKTURA A INTEGRACE

ESET Inspect nabízí jedinečnou detekci na základě chování a reputace, která je pro bezpečnostní týmy zcela transparentní. Všechna pravidla lze snadno upravovat ve formátu, takže je můžete jemně odladit nebo vytvořit na míru potřebám specifického podnikového prostředí, včetně integrací SIEM.

PROPRACOVANÉ SKÓROVÁNÍ

Určit prioritu v závažnosti varování vám pomůže funkce stanovení skóre, která incidentům připíše hodnotu závažnosti a umožní správcům rychle rozpoznat počítače, kde je vyšší pravděpodobnost, že došlo k incidentu.

SHROMAŽĎOVÁNÍ MÍSTNÍCH DAT

K dispozici máte komplexní data o nově spuštěných modulech, včetně času spuštění, uživatele, který je zahájil, doby setrvání a napadených zařízení. Všechna data se ukládají lokálně, aby se předešlo únikům citlivých dat.

Případy použití

Detekce chování a uživatelé opakovaně porušující pravidla

PROBLÉM

V síti máte uživatele, u kterých se opakovaně vyskytuje škodlivý kód. Titíž uživatelé znovu a znovu zažívají napadení počítače. Je to kvůli tomu, že se chovají riskantně? Nebo jsou z nějakého důvodu terčem útočníků častěji než jiní?

ŘEŠENÍ

- ✓ Problémové uživatele a zařízení si můžete snadno zobrazit.
- ✓ Rychle proveďte analýzu prvotních příčin, která nalezne zdroj napadení.
- ✓ Proveďte nápravu u zjištěných vektorů infekce: může to být e-mail, web nebo USB zařízení.

Vyhledávání a blokování hrozeb

PROBLÉM

V systému včasného varování nebo v centru bezpečnostních operací se zobrazí nové varování před hrozbou. Jak teď budete postupovat?

ŘEŠENÍ

- ✓ Využijte systém včasného varování k získání dat o chystaných a nových hrozbách.
- ✓ Prohledejte všechny počítače, zda se v nich nevyskytuje nová hrozba.
- ✓ Vyhledejte ve všech počítačích ukazatele narušení, které by naznačovaly, že se hrozba vyskytla ještě před varováním.
- ✓ Zablokujte hrozbu, aby se nemohla infiltrovat do sítě nebo spustit v systémech organizace.

Jednoduché nastavení a jednoduchá reakce – není nutné zapojovat bezpečnostní tým

PROBLÉM

Ne každý podnik má vyhrazený bezpečnostní tým. Zadávání pokročilých pravidel detekce a jejich implementace pak mohou být náročné.

ŘEŠENÍ

- ✓ Více než 300 integrovaných předem konfigurovaných pravidel.
- ✓ Jednoduchá možnost reakce: jedním kliknutím zařízení zablokujete, ukončíte nebo odešlete do karantény.
- ✓ Do varování jsou integrované návrhy nápravných opatření a dalších kroků.
- ✓ Pravidla můžete upravovat v jazyce XML a jednoduše je tak podle potřeby ladit nebo vytvářet nová.

Přehled o síti

PROBLÉM

Některé podniky mají obavy z aplikací, které v systému spouštějí uživatelé. Problémem nejsou jen tradičně instalované aplikace, ale i ty přenosné, které se ve skutečnosti neinstalují. Jak je udržíte pod kontrolou?

ŘEŠENÍ

- ✓ Jednoduše si zobrazte všechny aplikace nainstalované na zařízeních a podle potřeby je filtrujte.
- ✓ Zobrazte si a filtrujte všechny skripty na zařízeních.
- ✓ Jednoduše zablokujte spuštění neautorizovaných skriptů či aplikací.
- ✓ Napravte problém tím, že uživatele upozorníte na neautorizované aplikace a automaticky je odinstalujete.

Hloubková detekce hrozeb – ransomware

PROBLÉM

Podniky chtějí mít více nástrojů k proaktivní detekci ransomwaru a dostat včas upozornění, pokud se v síti zjistí chování, které ransomware připomíná.

ŘEŠENÍ

- ✓ Zadejte pravidla, která detekují aplikace spouštěné z dočasných složek.
- ✓ Zadejte pravidla, která detekují soubory Office (Word, Excel, PowerPoint), když spouštějí další skripty či spustitelné soubory.
- ✓ Nastavte si varování pro případ, že se na zařízení zjistí nejběžnější přípony ransomwarových souborů.
- ✓ Zobrazte si na konzoli řešení ESET Endpoint Security také varování z nástroje Ochrana proti ransomware.

Šetření a náprava vycházející z kontextu

PROBLÉM

Data jsou jen tak dobrá, jako kontext, který k nim máme. Máte-li se správně rozhodovat, potřebujete vědět, co vám varování sdělují, na kterých zařízeních se vyskytují a kteří uživatelé je spouštějí.

ŘEŠENÍ

- ✓ Identifikujte a roztřiďte všechny počítače podle údajů ze služby Active Directory, automatických nebo ručních seskupení.
- ✓ Na základě seskupení počítačů můžete povolovat nebo blokovat aplikace a skripty.
- ✓ Povolovat nebo blokovat aplikace a skripty můžete také podle uživatele.
- ✓ Můžete si nastavit oznámení jen pro určité skupiny.

ESET Digital Security
Progress. Protected.

O společnosti ESET

TECHNOLOGIE PŘINÁŠEJÍ POKROK. ESET® JE TADY, ABY JE CHRÁNIL.

Společnost ESET už přes 30 let přináší technologické inovace a ta nejpokročilejší řešení kybernetického zabezpečení na trhu. Moderní ochranu koncových zařízení zajišťujeme díky vícevrstvým bezpečnostním technologiím ESET LiveSense® v kombinaci s průběžným využíváním strojového učení a cloud computingu. Řešení ESET stojí na špičkových informacích o hrozbách a jedinečném výzkumu a nabízejí dokonale vyvážené funkce pro prevenci a detekci hrozeb a reakci na ně. Skvěle se ovládají a jsou bezkonkurenčně rychlá. Naší misí tak je chránit pokrok našich zákazníků a zajistit jim maximální ochranu.

ESET V ČÍSLECH

Více než miliarda
chráněných uživatelů na internetu

Přes 400 tisíc
firemních zákazníků

195
zemí a oblastí

13
globálních výzkumných center

NĚKTEŘÍ Z NAŠICH ZÁKAZNÍKŮ

MITSUBISHI MOTORS
Drive your Ambition

využívá ochranu produkty ESET od roku 2017, více než 9 000 koncových zařízení

Allianz Suisse

využívá ochranu produkty ESET od roku 2016, více než 4 000 poštovních schránek

Canon
Canon Marketing Japan Group

využívá ochranu produkty ESET od roku 2016, více než 32 000 koncových zařízení

partnerem zabezpečení ISP od roku 2008, 2 miliony zákazníků

UZNÁNÍ V OBORU

MITRE ATT&CK™

ESET je jedním z nejčastěji odkazovaných a nejvíce angažovaných dodavatelů, kteří se přímo podílejí na ladění a doplňování znalostní databáze MITRE ATT&CK.

G2 Leader SPRING 2023

Řešení ESET pravidelně získávají nejvyšší hodnocení na globální platformě G2 pro uživatelské recenze a oceňují je zákazníci po celém světě.

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

V hodnocení Advanced Persistent Threat Market Quadrant 2023 společnosti Radicati získala společnost ESET už čtvrtý rok po sobě titul Top Player.