PREHĽAD

THREAT INTELLIGENCE

Jedinečné informačné kanály a reporty o APT
od najlepších odborníkov v odvetví

Progress. Protected.

Prečo pridať informácie o kybernetických hrozbách od spoločnosti ESET do svojho portfólia zabezpečenia?

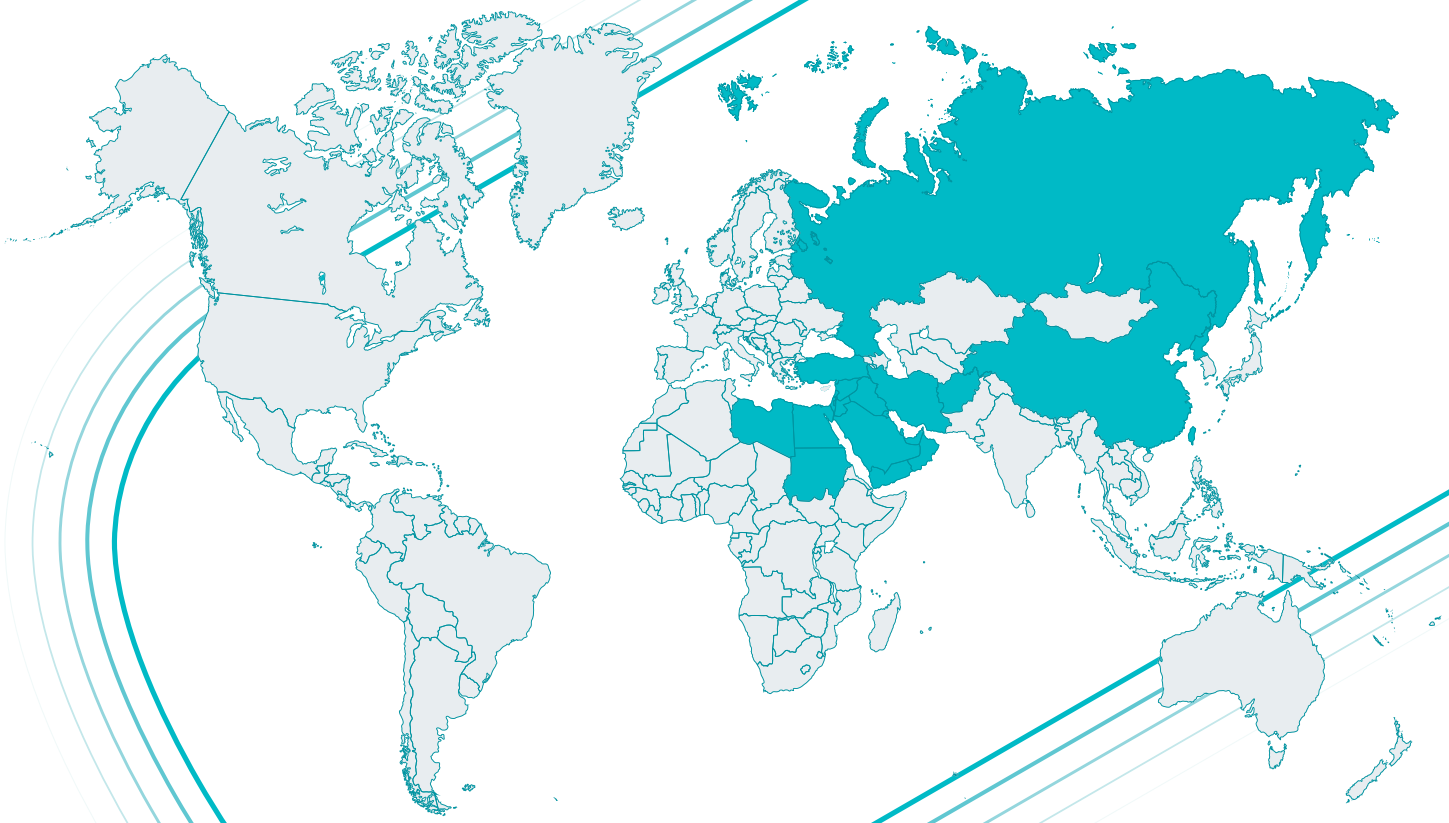
Pochopením súčasného prostredia hrozieb a taktík, ktoré kybernetickí zločinci používajú, získajú organizácie kľúčovú výhodu v podobe znalostí. Takéto poznatky im umožnia efektívne **posilniť** svoje **interné obranné mechanizmy**. Vysokokvalitné údaje o hrozbách sú základom každej spoľahlivej stratégie informácií o kybernetických hrozbách (CTI).

Spoločnosť ESET je už viac ako 35 rokov súkromnou spoločnosťou, ktorá nemá dlhy a neustále rastie. Náš úspech sa zakladá na prístupe zameranom na prevenciu a je poháňaný umelou inteligenciou s využitím ľudských odborných znalostí. Jadrom našich operácií sú **jedinečné znalosti globálneho tímu ESET Threat Intelligence podporené rozsiahlou sieťou výskumu a vývoja** pod vedením uznávaných odborníkov. Venujeme čas reálnemu pochopeniu kybernetických hrozieb, čo nám umožňuje účinne sa proti nim brániť.

Bez ohľadu na to, ako pokročilé sú vaše súčasné riešenia CTI, integráciou **produktov ESET do vášho portfólia zabezpečenia nadobudnete jedinečnú hodnotu**. Naše komplexné informačné kanály o hrozbách a podrobné reporty o APT vám zaistia náskok pred vznikajúcimi hrozbami a rozšíria vaše súčasné ochranné mechanizmy o užitočné poznatky a špičkový výskum.

Využite jedinečnú telemetriu spoločnosti ESET

Globálne pôsobenie spoločnosti ESET budované po desaťročia nám zaisťuje **bohatú a rôznorodú knižnicu informácií o hrozbách** z miliónov uzlov. Na rozdiel od mnohých konkurentov je naša telemetria obzvlášť silná v regiónoch, ktoré sú z geopolitického hľadiska vo svete kybernetickej obrany považované za **„zaujímavejšie“**. Toto jedinečné pokrytie sa priamo premieta do špičkových informácií o hrozbách. Využitím telemetrie spoločnosti ESET **získate prístup ku kvalitným a praktickým poznatkom**, ktoré rozšíria vaše schopnosti detekcie a reakcie na hrozby.

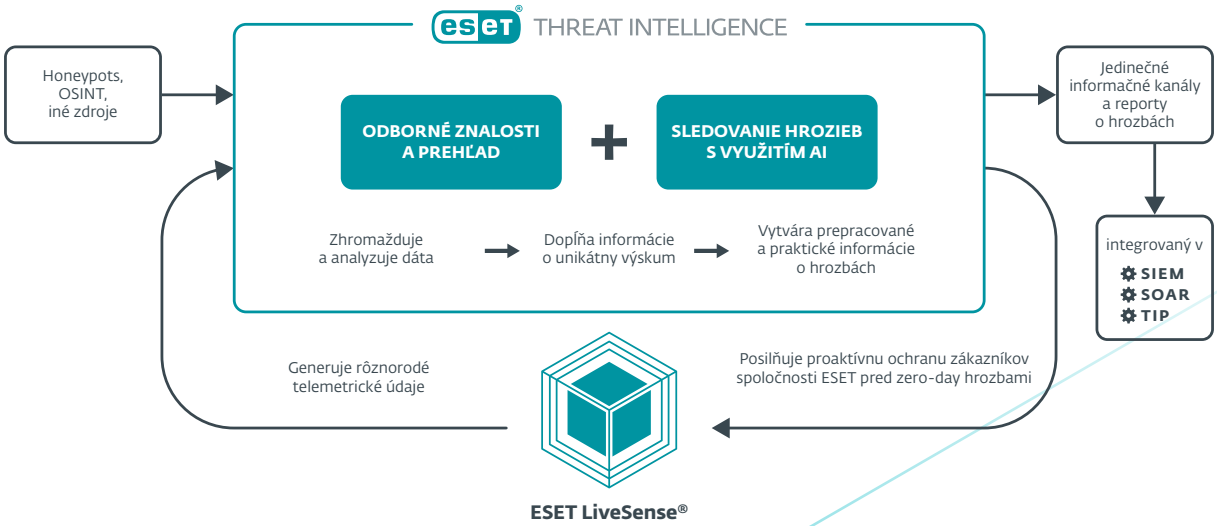


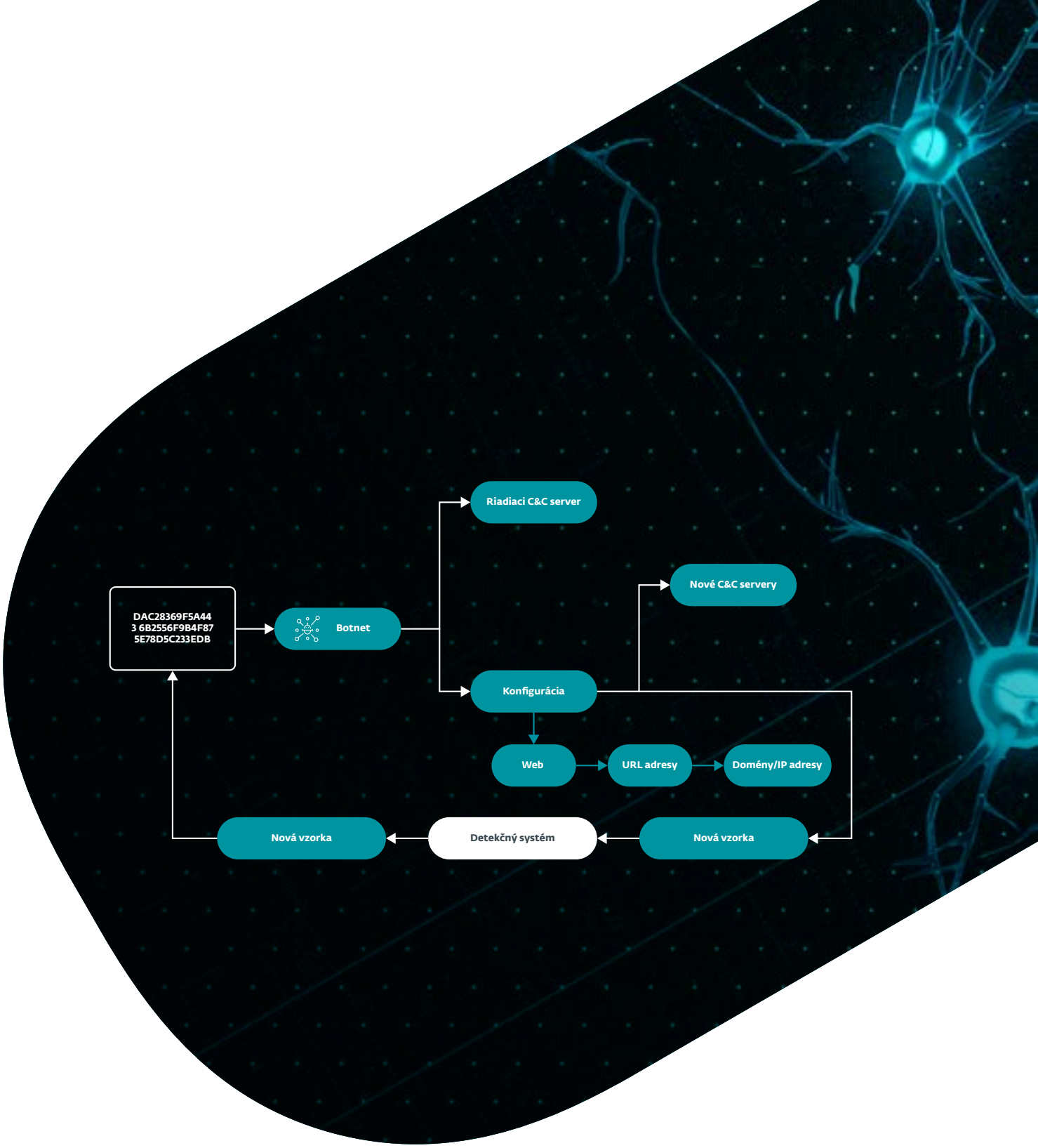
eset Digital Security
Progress. Protected.

Jedinečné a podrobné informácie prinášajúce praktické poznatky

Získavanie informácií o hrozbách nie je len o zhromažďovaní indikátorov a ich štruktúrovaní – ESET ide oveľa ďalej. Pri spracúvaní a dopĺňaní našich informácií využívame pokročilé technológie a špičkové odborné znalosti, aby sme vašej firme prinášali skutočnú hodnotu.

1. **Komplexná telemetria:** Využívame rozsiahlu škálu telemetrických údajov generovaných našou viacvrstvovou bezpečnostnou technológiou ESET LiveSense, ktorá je súčasťou platformy ESET PROTECT. Zaisťujeme tak rozsiahly a hĺbkový zber dát z rôznych zdrojov.
2. **Rôzne metódy zhromažďovania:** Okrem technológie LiveSense využívame rôznorodé metódy zberu a monitorovania dát vrátane zariadení zámerne nasadených na zlákanie malvéru (tzv. honeypots), senzorov, informácií dostupných z otvorených zdrojov (OSINT), prehľadávania webu (štandardného webu aj deep webu) a sledovania hrozieb. Výsledkom je značný objem vysokokvalitných údajov.
3. **Pokročilé spracúvanie:** Po zhromaždení sa všetky dáta spracúvajú prostredníctvom našich robustných backendových systémov, ktoré využívajú umelú inteligenciu na automatickú klasifikáciu a analýzu informácií. Zdôraznené sú tak len tie najrelevantnejšie a najpraktickejšie informácie.
4. **Odborná analýza:** Okrem automatizovaného spracúvania zohráva kľúčovú úlohu aj náš kvalifikovaný tím analytikov a výskumníkov zameraných na informácie o hrozbách. Tí neustále skúmajú a analyzujú rôznych útočníkov, ich motiváciu, taktiky, techniky a postupy (TTP) a používané nástroje. Ľudský element prehlbuje a spresňuje získavané informácie o hrozbách a presahuje možnosti samotného strojového učenia a automatizácie.





Vzorky, ktoré získavame prostredníctvom telemetrie, podrobujeme hĺbkovej analýze aktivity a štruktúry. Tento proces prináša ďalšie užitočné indikátory, ktoré obohacujú naše informácie o hrozbách. Dôkladným skúmaním každej vzorky získavame cenné poznatky, ktoré zvyšujú celkovú kvalitu a efektivitu našich informácií a poskytujú vám komplexnejší prehľad o prostredí hrozieb.

Špičkové zabezpečenie vďaka podrobným reportom o APT

Naše stručné a praktické reporty o APT zlepšujú stav zabezpečenia vašej organizácie a poskytujú vám podrobný prehľad o kampaniach a distribúcii malvéru, ako aj o zapojených útočníkoch. Získajte prístup k nášmu serveru MISP a nástroju AI Advisor a rezervujte si stretnutie naživo so špičkovými expertmi spoločnosti ESET na analýzu hrozieb, vďaka ktorým získate komplexné a praktické informácie.

NÁŠ NAJLEPŠÍ VÝSKUM MÁTE NA DOSAH RUKY

Náš výskumný tím je v oblasti digitálnej bezpečnosti dobre známy, a to vďaka oceňovanému blogu WeLiveSecurity. Nájdete tu rozsiahle výskumy či súhrnné poznatky o aktivite APT skupín, ako aj ďalšie podrobné informácie. Zákazníci spoločnosti ESET navyše získavajú exkluzívnu predbežnú ukážku všetkého nového obsahu na WeLiveSecurity.

DÔKLADNE SPRACOVANÝ OBSAH A PRAKTICKÉ VYUŽITIE

Reporty obsahujú množstvo informácií a pomáhajú lepšie pochopiť, čo sa v oblasti hrozieb deje a z akých príčin. Organizácie sa tak dokážu vopred pripraviť na to, čo by sa mohlo stať. V neposlednom rade naši odborníci zaisťujú, aby bol obsah ľahko zrozumiteľný.

NEODKLADAJTE KĽÚČOVÉ ROZHODNUTIA

Spomínané informácie pomáhajú organizáciám prijímať zásadné rozhodnutia a poskytujú im strategickú výhodu v boji proti digitálnej kriminalite. Vďaka nim možno ľahšie pochopiť, čo sa deje na „odvrátenej" strane internetu. Prinášajú dôležitý kontext, aby mohla vaša organizácia rýchlo podniknúť prípravné kroky na internej úrovni.

PRÍSTUP K ANALYTIKOVI SPOLOČNOSTI ESET

Každý zákazník, ktorý si objedná balík PREMIUM reporty o APT, bude môcť využívať aj služby analytika spoločnosti ESET, a to až štyri hodiny mesačne. Zákazník tak má príležitosť podrobnejšie prediskutovať potrebné témy s odborníkom a získať pomoc pri riešení komplexných problémov.

ESET AI ADVISOR

ESET AI Advisor využíva pokročilú umelú inteligenciu a odborné znalosti v oblasti APT na poskytovanie informácií a bezpečnostných opatrení proti kybernetickým útokom na požiadanie. Je dostupný ako chatbot, ktorý rieši bezpečnostné otázky, ponúka súhrnné reporty o aktivite APT, kompiluje indikátory IoC a taktiky, techniky a postupy (TTP) útočníkov a generuje pravidlá YARA na rýchle pochopenie hrozieb a ich prevenciu.

		Reporty o APT	Reporty o APT Úroveň Advanced	Reporty o APT Úroveň Ultimate
Dvojtýždenný súhrn aktivity	Reporty sumarizujúce aktivitu všetkých pokrytých skupín APT, ako je uvedené vyššie (dva reporty mesačne)	✓	✓	✓
Reporty o analýze hrozieb	Prispôsobená alebo pravidelná technická analýza prevládajúcich hrozieb (~30 ročne)	✓	✓	✓
Mesačný prehľad	Mesačná kompilácia informácií so stručným prehľadom hrozieb	✓	✓	✓
Mesačný súhrn	Index a stručný prehľad reportov a udalostí za daný mesiac	✓	✓	✓
Skorší prístup k portálu WeLiveSecurity	Exkluzívny prístup k reportom o hrozbách a vybraným článkom na WeLiveSecurity	✓	✓	✓
Kanál o indikátoroch IoC skupín APT	Úplný prístup ku kanálu STIX/TAXII, ktorý obsahuje indikátory IoC z reportov	✓	✓	✓
Prístup k serveru MISP	Plný prístup k serveru ESET MISP, ktorý obsahuje všetky informácie dostupné v reportoch	✗	✓	✓
ESET AI Advisor	Prístup k nástroju ESET AI Advisor, ktorý poskytuje prehľad a zhrnutie dostupných reportov o APT	✗	✓	✓
Prístup k analytikom	Prístup k analytikom prostredníctvom rôznych platforiem, ako je MS Teams a e-mail, obmedzený na štyri hodiny mesačne (nekumulatívny, vrátane času na prípravu)	✗	✗	✓

Spoznajte silu ESET Threat Intelligence

Naplánujte si s nami demo ešte dnes a zistite, akú jedinečnú hodnotu môže ESET Threat Intelligence priniesť vašej organizácii. Naši spokojní zákazníci so 100 % mierou obnovenia sú dôkazom účinnosti našich riešení. Ukážeme vám, ako môžeme posilniť vašu kybernetickú bezpečnosť.

Ešte nie ste pripravený na demo hovor?

Začnite vytvorením náhľadového účtu na portáli ESET Threat Intelligence a preskúmajte kanály aj reporty o APT.

Jasné a stručné informačné kanály

Rozšírte si prehľad o hrozbách vďaka jedinečnej telemetrii spoločnosti ESET. Naše dôkladne spracované dátové kanály sú dostupné vo formátoch JSON a STIX 2.1 a je možné ich bezproblémovo integrovať do platformy na sledovanie hrozieb (TIP), ako aj nástrojov SIEM alebo SOAR. Na rozdiel od mnohých dodávateľov v oblasti informácií o hrozbách dbáme na to, aby boli naše **kanály dôkladne filtrované a vyhodnocované** s cieľom zaistiť ich relevantnosť. Vďaka tomu môžu existujúce bezpečnostné systémy automaticky prijímať potrebné opatrenia a analytici získajú komplexný prehľad o globálnych hrozbách.

- Podrobné a dôkladne prepracované údaje bohaté na metadáta s nízkym výskytom falošných poplachov
- Kompaktné a deduplikované dáta s vysokou úrovňou relevancie a priradeným skóre dôveryhodnosti
- Výsledok pokročilého filtrovania s poznatkami výskumníkov spoločnosti ESET
- Vedúca pozícia na trhu, najmä pre dáta o botnetoch
- Nenáročná údržba vďaka dôkladne spracovanému obsahu
- Informačné kanály aktualizované v reálnom čase obsahujúce iba nové a rozšírené indikátory narušenia bezpečnosti (IoC)

INFORMAČNÝ KANÁL O ŠKODLIVÝCH DÁTACH

Tento kanál poskytuje cenné informácie o novoobjavených vzorkách malvéru, ich vlastnostiach a indikátoroch IoC v reálnom čase. Využitím týchto údajov môžete proaktívne blokovať škodlivé súbory skôr, ako vám spôsobia problémy. Kanál obsahuje podrobnosti, ako sú hashe súborov, časové známky a typy zistených hrozieb.

INFORMAČNÝ KANÁL O RANSOMVÉRI

Bojujte proti ransomvéru vďaka aktuálnym údajom o najčastejších vzorkách. Náš kanál poskytuje prehľad o aktívnych rodinách ransomvéru, čo ich umožňuje proaktívne blokovať. Buďte o krok vpred pred hrozbami a chráňte svoju organizáciu pred únikmi údajov a nákladnými narušeniami zabezpečenia.

INFORMAČNÝ KANÁL O BOTNETOCH

Využite poznatky z našej vlastnej siete na sledovanie botnetov v rámci informačného kanála o botnetoch. Tento kanál sa skladá z troch typov čiastkových informačných kanálov, ktoré prinášajú informácie o samotných botnetoch, riadiacich C&C serveroch a ich cieľoch. Poskytuje základné údaje vrátane podrobností o detekcii, hashov súborov, časových známok poslednej komunikácie, stiahnutých súborov, IP adries, protokolov a cielených informácií.

INDIKÁTORY IOC SKUPÍN APT

Využite cenné informácie z nášho vlastného kanála o APT, ktorý poskytuje prehľad o pokročilých pretrvávajúcich hrozbách na základe výskumu spoločnosti ESET. Tento kanál je exportovaný z interného servera MISP spoločnosti ESET a obsahuje údaje, ktoré sú podrobnejšie popísané v reportoch o APT. Informačný kanál o APT je súčasťou ponúkaných reportov o APT, ale je možné si ho zakúpiť aj samostatne.

INFORMAČNÝ KANÁL O DOMÉNACH

Blokujte domény, ktoré sa považujú za škodlivé, vrátane názvu domény, IP adresy a ďalších súvisiacich údajov. Informačný kanál hodnotí domény na základe úrovne ich závažnosti, čo vám umožňuje primerane nastaviť reakciu – môžete napríklad blokovať len domény s vysokou úrovňou závažnosti.

INFORMAČNÝ KANÁL O URL

Využite dôkladne zostavený kanál o URL, ktorý sa zameriava na konkrétne adresy. Poskytuje podrobné informácie týkajúce sa každej URL a zahŕňa údaje o hostiteľských doménach. Kanál je zostavený tak, aby zobrazoval len výsledky s vysokou mierou dôveryhodnosti, pričom zrozumiteľnou formou informuje o tom, prečo bola URL adresa označená.

INFORMAČNÝ KANÁL O IP ADRESÁCH

Získavajte praktické dáta z tohto kanála, ktorý poskytuje informácie o škodlivých IP adresách. Štruktúra údajov je veľmi podobná štruktúre použitej pre informačné kanály zamerané na domény a URL adresy. Používaním tohto kanála môžete identifikovať najrozšírenejšie škodlivé IP adresy, proaktívne blokovať IP adresy s vysokou úrovňou závažnosti, detegovať menej závažné IP adresy a podrobnejšie ich skúmať na základe ďalších údajov s cieľom vyhodnotiť potenciálne škody.

INFORMAČNÝ KANÁL O HROZBÁCH PRE SYSTÉM ANDROID

Tento kanál poskytuje aktuálne informácie o najčastejších hrozbách pre Android a ich indikátoroch IoC, čo ich umožňuje proaktívne blokovať. Čerpá informácie z telemetrie ESET a aktualizuje sa takmer v reálnom čase s dennou deduplikáciou.

INFORMAČNÝ KANÁL O INFOSTEALEROCH ZAMERANÝCH NA SYSTÉM ANDROID

Tento vyhradený kanál poskytuje podrobnosti o aktuálnych a rozšírených vzorkách infostealerov zameraných na systém Android spolu so súvisiacimi údajmi. Využitím týchto informácií získate prehľad o rodinách infostealerov, ktoré sú aktívne v reálnom svete. A čo je ešte dôležitejšie, môžete ich proaktívne blokovať skôr, ako spôsobia akúkoľvek škodu.

INFORMAČNÝ KANÁL O PODVODNÝCH URL ADRESÁCH

Predchádzajte podvodom vďaka aktuálnym údajom o falošných URL adresách. Náš kanál pokrýva obchody s elektronikou, investičné podvody, podvody súvisiace so zoznamovaním a kryptomenami. Je vytvorený zo všetkých zdrojov spoločnosti ESET o URL adresách v takmer reálnom čase, pričom deduplikácia prebieha každých 24 hodín.

INFORMAČNÝ KANÁL O KRYPTOMENOVÝCH PODVODOCH

Buďte o krok vpred pred kryptomenovými podvodmi vďaka aktuálnym informáciám o falošných doménach, URL adresách a súvisiacich údajoch. Náš kanál, ktorý čerpá informácie z rozsiahlej telemetrie ESET, poskytuje včasné a cielené informácie na proaktívne blokovanie hrozieb a ochranu vašich aktív.

INFORMAČNÝ KANÁL O ŠKODLIVÝCH E-MAILOVÝCH PRÍLOHÁCH

E-mail je hlavným cieľom útokov. Náš kanál, ktorý čerpá informácie z rozsiahlej telemetrie ESET o kontrole e-mailov, poskytuje údaje o škodlivých e-mailových prílohách v reálnom čase. Predchádzajte hrozbám vďaka aktuálnym a praktickým informáciám a chráňte svoju organizáciu.

INFORMAČNÝ KANÁL O PHISHINGOVÝCH URL ADRESÁCH

Zostaňte v bezpečí vďaka aktuálnym údajom o najčastejších phishingových URL adresách. Náš kanál, ktorý čerpá informácie z databázy ESET o phishingových URL adresách, sa aktualizuje takmer v reálnom čase s dennou deduplikáciou. Predchádzajte narušeniam zabezpečenia identifikáciou a blokovaním podvodných stránok skôr, ako spôsobia škodu.

INFORMAČNÝ KANÁL O SMISHINGU

Chráňte sa vďaka aktuálnym údajom o smishingových doménach, URL adresách a súvisiacich údajoch. Náš kanál, ktorý čerpá informácie z rozsiahlej telemetrie ESET, sa aktualizuje takmer v reálnom čase s dennou deduplikáciou.

INFORMAČNÝ KANÁL O PODVODNÝCH SMS

Chráňte sa pred podvodnými SMS správami vďaka nášmu kanálu zahŕňajúcemu škodlivé domény a URL adresy s aktuálnymi informáciami. Tento kanál, aktualizovaný takmer v reálnom čase z rozsiahlej telemetrie spoločnosti ESET a denne deduplikovaný, vám pomáha identifikovať a blokovať sofistikované hrozby.

O spoločnosti ESET

Minimalizácia rizík vďaka preventívnemu prístupu

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.

Spoznajte najlepšiu ochranu vo svojej triede vďaka našim interným globálnym informáciám o kybernetických hrozbách, ktoré zbierame a skúmame už viac ako 30 rokov a ktoré sú základom našej rozsiahlej siete výskumu a vývoja pod vedením uznávaných odborníkov.

ESET PROTECT, naša cloudová platforma kybernetickej bezpečnosti s podporou XDR, kombinuje inovatívne 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

12
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 JUL 2024

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 FALL 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.