OVERVIEW

THREAT INTELLIGENCE

Fluxuri de informații unice și rapoarte de la profesioniștii de top din industrie

Progress. Protected.

De ce să adăugați ESET în infrastructura dvs. CTI?

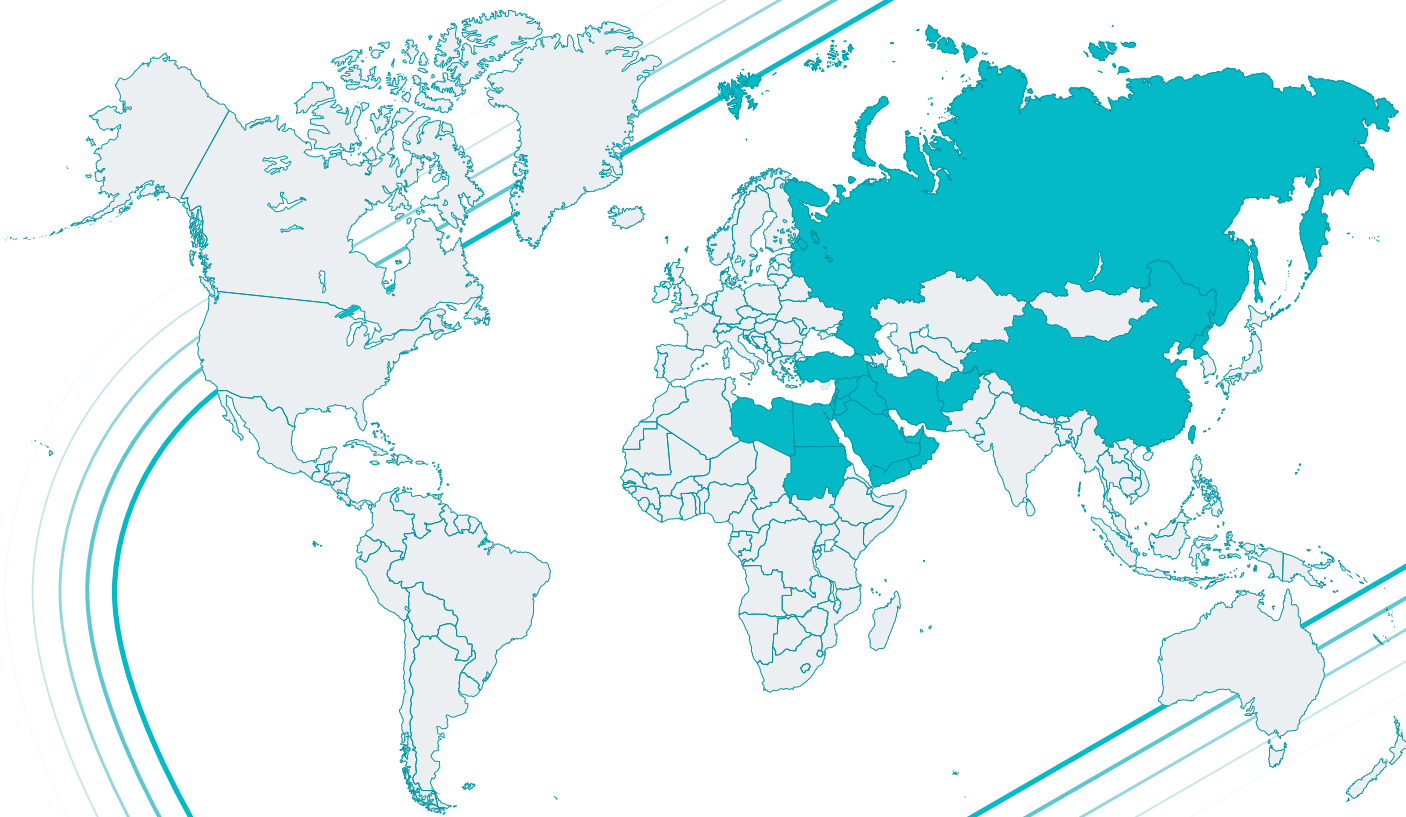
Înțelegerea peisajului actual al amenințărilor și a tacticilor utilizate de infractorii cibernetici oferă un avantaj esențial de cunoaștere. Aceste informații permit organizațiilor să își **consolideze** eficient **sistemele interne de apărare**. Informațiile de înaltă calitate reprezintă fundamentul oricărei strategii solide de cyber threat intelligence (CTI).

De peste 35 de ani, ESET este o companie privată, fără datorii și aflată într-o creștere constantă. Succesul nostru se bazează pe o abordare de tip „prevention-first", susținută de inteligența artificială și îmbunătățită de expertiza umană. În centrul operațiunilor noastre se află **sistemul unic Global Threat Intelligence, sprijinit de o rețea extinsă de cercetare și dezvoltare,** coordonată de cercetători recunoscuți în industrie. Dedicăm timpul necesar pentru a înțelege cu adevărat amenințările cibernetice, astfel încât să le putem combate eficient. .

Indiferent cât de avansate sunt soluțiile dvs. actuale de CTI, **integrarea ESET în infrastructura dvs. vă va oferi o valoare excepțională**. Fluxurile noastre complete de threat intelligence, rapoartele APT și rapoartele eCrime vă ajută să rămâneți cu un pas înaintea amenințărilor emergente, consolidând apărarea existentă prin informații acționabile și cercetare de ultimă generație.

Valorificați telemetria unică ESET

Prezența globală a ESET, construită de-a lungul deceniilor, ne oferă acces la o **bibliotecă vastă și diversificată de informații** provenite de la milioane de noduri. Spre deosebire de mulți competitori, telemetria noastră este deosebit de puternică în regiuni considerate **„mai interesante" din punct de vedere geopolitic** în lumea apărării cibernetice. Această acoperire unică se traduce direct în informații de nivel superior. Prin valorificarea telemetriei ESET, beneficiați de acces la **informații de înaltă calitate și acționabile**, care vă îmbunătățesc capacitățile de detectare și răspuns la amenințări.

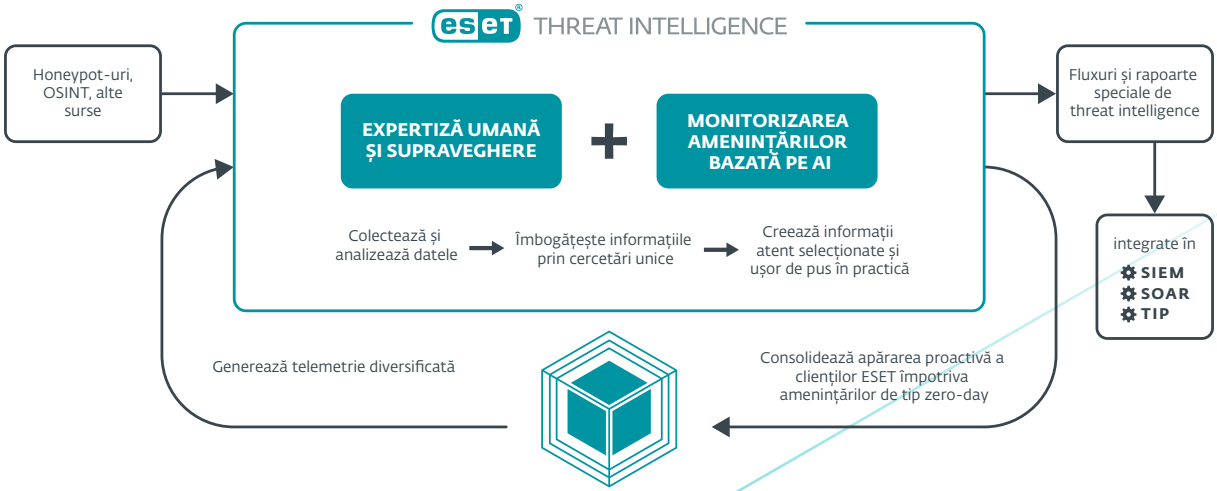


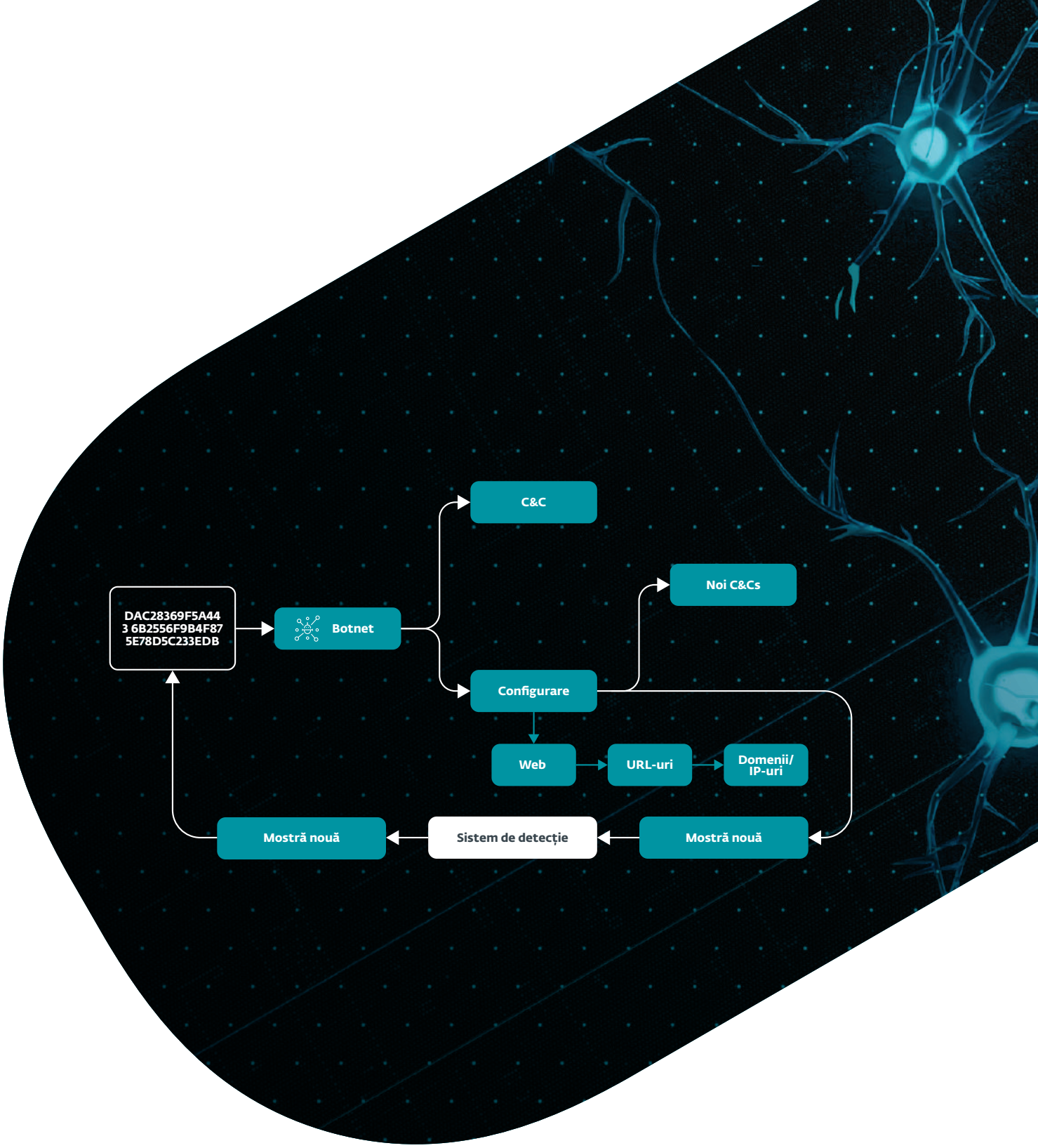
eset Cybersecurity
Progress. Protected.

Informații unice și îmbogățite pentru perspective acționabile

Threat intelligence nu înseamnă doar colectarea indicatorilor și prezentarea lor într-un pachet – ESET merge mult dincolo de acest nivel. Folosim tehnologii avansate și expertiză extinsă pentru a procesa și îmbogăți informațiile noastre de intelligence, asigurându-ne că acestea oferă valoare reală afacerii dvs.

1. **Telemetrie completă:** Informațiile noastre pornesc de la o gamă largă de date de telemetrie generate de ESET LiveSense, tehnologia noastră de securitate multistrat integrată în platforma ESET PROTECT Platform. Acest lucru asigură o colectare amplă și profundă de date din surse diverse.
2. **Metode diverse de colectare:** Pe lângă LiveSense, utilizăm diferite metode de colectare și monitorizare, inclusiv honeypot-uri, senzori, resurse OSINT, web crawling (atât pe web-ul public, cât și pe deep web) și Threat Tracking. Rezultatul este un volum semnificativ de date de înaltă calitate
3. **Procesare avansată:** Odată colectate, toate datele sunt procesate prin sistemele noastre backend robuste, care utilizează inteligența artificială pentru a clasifica și analiza automat informațiile. Acest lucru garantează că sunt evidențiate doar informațiile de intelligence cele mai relevante și acționabile.
4. **Analiză realizată de experți:** Dincolo de procesarea automată, echipa noastră de analiști și cercetători specializați în threat intelligence joacă un rol esențial. Aceștia studiază și analizează continuu diverși actori ai amenințărilor, motivațiile lor, TTP-urile (tactici, tehnici și proceduri) și instrumentele utilizate. Această verificare umană adaugă un nivel suplimentar de profunzime și acuratețe informațiilor noastre, depășind ceea ce pot realiza singure machine learning-ul și automatizarea.





Mostrele pe care le primim prin telemetrie sunt supuse unei analize comportamentale și structurale aprofundate. Acest proces generează indicatori suplimentari utili, îmbogățind și mai mult informațiile noastre de threat intelligence. Prin examinarea atentă a fiecărei mostre, extragem informații valoroase care sporesc calitatea și eficiența generală a intelligence-ului nostru, oferindu-vă o înțelegere mai cuprinzătoare a peisajului amenințărilor.

Securitate superioară prin rapoarte APT detaliate

Redactate într-un limbaj concis și orientat spre acțiune pentru a îmbunătăți postura de securitate a organizației dvs, rapoartele noastre APT oferă informații detaliate despre campaniile malware, metodele de distribuție și actorii implicați. Beneficiați de acces la serverul nostru MISP și la consilierul AI, precum și de posibilitatea de a programa sesiuni live cu experții de top în threat intelligence ai ESET pentru informații complete și aplicabile.

PUNEM CELE MAI BUNE CERCETĂRI ALE NOASTRE LA ÎNDEMÂNA DVS.

Echipa noastră de cercetare este recunoscută în industria securității digitale datorită blogului premiat WeLiveSecurity. Sunt disponibile cercetările de înaltă calitate ale echipei și rezumatele activităților APT, împreună cu informații mult mai detaliate. Clienții ESET beneficiază de acces exclusiv în avans la tot conținutul publicat pe WeLiveSecurity.

CONȚINUT CURATORIAT ȘI ACȚIONABIL

Rapoartele oferă o cantitate mare de context despre ceea ce se întâmplă și de ce. Datorită acestui lucru, organizațiile se pot pregăti din timp pentru ceea ce ar putea urma. Important, experții noștri se asigură că informațiile sunt ușor de înțeles.

LUAȚI DECIZII CRUCIALE RAPID

Toate acestea ajută organizațiile să ia decizii cruciale și oferă un avantaj strategic în lupta împotriva criminalității digitale. Ele oferă o înțelegere a ceea ce se întâmplă în „partea întunecată a internetului" și furnizează un context esențial, astfel încât organizația dvs. să poată face rapid pregătirile interne.

ACCES LA UN ANALIST ESET

Fiecare client care comandă pachetul APT Reports Premium va avea, de asemenea, acces la un analist ESET pentru până la patru ore pe lună. Acest lucru oferă oportunitatea de a discuta subiectele în detaliu și de a ajuta la rezolvarea oricăror probleme rămase..

ESET AI ADVISOR

ESET AI Advisor utilizează inteligență artificială avansată și expertiză în APT pentru a oferi informații la cerere și măsuri de protecție împotriva atacurilor cibernetice. Disponibil sub forma unui chatbot, acesta răspunde întrebărilor legate de securitate, oferă rezumate APT, compilează IoC-uri și TTP-uri și generează reguli YARA pentru o înțelegere rapidă și prevenirea amenințărilor.

		Rapoarte APT	Rapoarte APT Advanced	Rapoarte APT Ultimate
Rezumat de activitate bilunar	Rapoarte care sintetizează activitatea tuturor grupurilor APT acoperite, așa cum este detaliat mai sus (două rapoarte pe lună)	✓	✓	✓
Rapoarte de analiză a amenințărilor	Analize tehnice personalizate sau periodice ale amenințărilor predominante (~30 pe an)	✓	✓	✓
Prezentare generală lunară	Compilație lunară de informații cu o prezentare executivă a amenințărilor	✓	✓	✓
Rezumat lunar	Indexul și rezumatul executiv al rapoartelor și evenimentelor lunii	✓	✓	✓
Acces anticipat la WeLiveSecurity	Acces anticipat la rapoarte de amenințări și articole selectate de pe WeLiveSecurity	✓	✓	✓
Flux de IOC pentru APT	Acces complet la fluxul STIX/TAXII care conține indicatori de compromitere (IOC) din rapoarte	✓	✓	✓
Acces la serverul MISP	Acces complet la serverul MISP al ESET, care conține toate informațiile disponibile din rapoarte	✗	✓	✓
ESET AI Advisor	Acces la ESET AI Advisor, care oferă informații și rezumate ale rapoartelor disponibile despre APT-uri	✗	✓	✓
Acces la analiști	Acces la analist prin diverse platforme, cum ar fi MS Teams și e-mail, limitat la patru ore pe lună (non-cumulativ, incluzând timpul de pregătire)	✗	✗	✓

De la indicatori la informații: depășiți criminalitatea cibernetică

Rapoartele ESET Threat Intelligence despre eCrime oferă informații detaliate despre ransomware și operațiuni mai largi de criminalitate cibernetică. Acestea oferă vizibilitate asupra instrumentelor folosite de atacatori, infrastructurii și strategiilor de monetizare, bazate pe cercetarea globală și telemetria ESET. Soluția permite trecerea dincolo de indicatorii de compromitere (IoC), oferind informații contextuale care consolidează apărarea proactivă și deciziile strategice.

Ceea ce diferențiază rapoartele ESET eCrime

APĂRARE PROACTIVĂ

Obține informații nu doar despre grupurile de eCrime, ci și despre afiliații care duc efectiv la îndeplinire atacurile. Înțelege modul lor de operare și anticipează următoarele acțiuni pentru a rămâne cu un pas înainte.

EFICIENȚĂ OPERAȚIONALĂ

Folosește informații clare și curate, bazate pe incidente reale, pentru a elimina zgomotul inutil. Ajută echipa să detecteze mai ușor amenințările, să răspundă mai rapid și să se concentreze pe investigațiile care contează cel mai mult.

VIZIBILITATE EXCLUSIVĂ

Depășește fluxurile publice de amenințări și obține o înțelegere mai profundă a tacticilor de monetizare, a infrastructurii și a comportamentului afiliaților în practică – totul susținut de telemetria și cercetarea globală ESET.

		Rapoarte eCrime	Rapoarte eCrime Advanced
Rezumat al activității LUNAR	○ Campanii recente de ransomware și infostealere sintetizate în informații strategice clare ○ Cine este vizat, cum se desfășoară atacurile, ce a mers prost ○ Lecții cheie, IOC și recomandări pentru consolidarea rezilienței	✓	✓
Analiză tehnică LUNAR	○ Analize aprofundate ale unor actori de amenințare specifici (de ex. FIN7) ○ Lanț complet de atac: de la accesul inițial până la furtul de date ○ Tactici, instrumente și infrastructură ale atacatorilor, mapare MITRE ATT&CK®, IOC	✓	✓
Rezumat lunar PERIODIC	○ Prezentare generală, pregătită pentru nivel executiv, a activității recente de ransomware/infostealere ○ Tendințe cheie, incidente notabile, amenințări emergente ○ Ajută conducerea să evalueze riscurile și să stabilească priorități fără complexitate tehnică	✓	✓
Fluxuri eCrime	○ IOC actualizați și selecționați privind grupuri de ransomware, afiliații acestora și campanii de infostealere ○ Disponibili în format standard STIX/TAXII	✓	✓
ESET AI Advisor	○ Folosește informații despre eCrime pentru a răspunde la întrebări legate de amenințări ○ Ajută la interpretarea incidentelor și a comportamentului atacatorilor ○ Oferă acces imediat la informații de securitate pentru echipe și factorii de decizie	✗	✓
Acces la serverul MISP	○ Integrare directă cu surse de threat intelligence verificate ○ Ingerare automată de IOC-uri pentru îmbogățirea apărării ○ Optimizează fluxurile operaționale, accelerează detectarea amenințărilor și sprijină răspunsul la incidente	✗	✓

Fluxuri de date clare și concise

Îmbunătățiți vizibilitatea asupra peisajului de amenințări cu ajutorul telemetriei unice ESET. Vă oferim fluxuri de date atent curatoriate, în formatele JSON și STIX 2.1, care se integrează ușor în instrumente SIEM, TIP sau SOAR. Spre deosebire de mulți alți furnizori de threat intelligence, **acordăm o atenție deosebită filtrării și evaluării datelor, pentru a asigura relevanța acestora**. Acest lucru permite declanșarea automată de acțiuni în sistemele de securitate existente atunci când este necesar, oferind analiștilor de threat intelligence o imagine completă asupra peisajului global al amenințărilor.

- Date îmbogățite cu metadate, detaliate și atent selecționate, cu un nivel foarte redus de fals-pozitive
- Ne asigurăm că datele sunt de dimensiuni reduse, cu relevanță ridicată, deduplicate și însoțite de scoruri de încredere
- Rezultat al unui proces avansat de filtrare, cu analize realizate de cercetătorii ESET
- Lider pe piață, în special în ceea ce privește datele despre botnet -uri
- Cerințe reduse de întreținere datorită conținutului atent selecționat
- Fluxuri de date în timp real – doar IOC recenți și relevanți

FLUX DE DATE MALWARE

Informații în timp real despre mostre de malware nou descoperite, caracteristicile acestora și IOC. Include hash-uri de fișiere, timestamp-uri și tipuri de amenințări, pentru a vă ajuta să blocați fișierele malițioase înainte să producă daune.

FLUX RANSOMWARE

Date în timp real despre familii active de ransomware și mostre predominante. Permite blocarea proactivă a atacurilor pentru a preveni brețele de securitate și întreruperile costisitoare.

FLUX BOTNET

Alimentat de trackerul de botnet-uri ESET, acest flux include trei sub-fluxuri: botnet, C&C și ținte. Oferă detalii de detecție, hash-uri de fișiere, timestamp-uri ale ultimei comunicări, fișiere descărcate, IP-uri, protocoale și informații despre ținte.

FLUX APT IOC

Informații despre APT bazate pe cercetarea ESET. Exportate din serverul intern MISP al ESET și aliniate cu rapoartele APT. Disponibile fie ca parte a rapoartelor, fie ca flux de sine stătător.

FLUX ADWARE PUA

ESET are peste două decenii de experiență în clasificarea aplicațiilor potențial nedorite (PUA), oferind o inteligență cu profunzime și precizie ridicate. Fluxul Adware furnizează informații în timp real despre adware activ și amenințări similare, permițând blocarea proactivă înainte de impact.

FLUX DE APLICAȚII PUA CU DUBLĂ UTILIZARE

Urmărește instrumente legitime (de ex. soluții RMM) care sunt utilizate abuziv de atacatori, ajutând la detectarea din timp a abuzului și reducând zgomotul prin date atent filtrate, cu un nivel scăzut de redundanță.

FLUX DE DOMENII

Oferă date despre domenii malițioase, inclusiv numele domeniului, adresa IP și data asociată. Domeniile sunt clasificate în funcție de severitate, permițând prioritizarea acțiunilor, cum ar fi blocarea domeniilor cu risc ridicat.

FLUX URL

Un flux selectat de URL-uri specifice, cu informații detaliate despre fiecare adresă și domeniile de găzduire asociate. Include doar rezultate cu nivel ridicat de încredere, susținute de explicații clare, ușor de înțeles, pentru URL-urile marcate.

FLUX IP

Primiți date acționabile despre IP-uri malițioase. Structura este similară cu cea a fluxurilor de domenii și URL-uri. Vă ajută să identificați amenințările comune, să blocați IP-urile cu severitate ridicată, să monitorizați cele cu risc scăzut și să investigați mai departe folosind date suplimentare pentru a evalua potențialul impact.

FLUX AMENINȚĂRI ANDROID

Oferă informații în timp real despre amenințările Android predominante și IOC, permițând blocarea proactivă. Este creat pe baza telemetriei ESET și se actualizează aproape în timp real, cu deduplicare zilnică.

FLUX INFOSTEALERE ANDROID

Un flux specializat din categoria amenințărilor Android, care oferă detalii despre mostrele actuale de infostealere și date asociate. Vă ajută să obțineți vizibilitate asupra familiilor active și să le blocați proactiv înainte de a produce daune.

FLUX URL-URI DE TIP SCAM

Rămâneți cu un pas înaintea fraudelor cu date în timp real despre URL-uri malițioase. Acoperă magazine online frauduloase, escrocherii de investiții, fraude de tip dating și înșelătorii legate de criptomonede. Este creat din toate sursele URL ale ESET, aproape în timp real, iar deduplicarea are loc la fiecare 24 de ore.

FLUX CRIPTOSCAM

Rămâneți cu un pas înaintea fraudelor cripto prin actualizări în timp real despre domenii, URL-uri și date asociate escrocheriilor. Sursa este telemetria extinsă ESET, oferind informații timpurii și direcționate pentru a vă ajuta să blocați proactiv amenințările și să vă protejați activele.

FLUX ATAȘAMENTE EMAIL MALIȚIOASE

Emailul este o țintă principală pentru atacuri. Acest flux oferă date în timp real despre atașamente de email malițioase, provenite din telemetria extinsă de scanare email a ESET.

FLUX URL-URI DE PHISHING

Oferă informații în timp real despre URL-uri de phishing active, din baza de date dedicată ESET. Este actualizat continuu, cu deduplicare zilnică, ajutând la detectarea și blocarea site-urilor frauduloase înainte de compromiterea datelor sensibile.

FLUX SMISHING

Oferă informații la timp despre atacuri de tip SMS phishing (smishing), inclusiv domenii, URL-uri și indicatori asociați. Datele provin din telemetria extinsă ESET și sunt actualizate aproape în timp real, cu deduplicare zilnică.

FLUX FRAUDE SMS

Protejează împotriva escrocheriilor prin SMS, oferind date în timp real despre domenii și URL-uri malițioase. Actualizat aproape în timp real din telemetria ESET și deduplicat zilnic, ajută la identificarea și blocarea amenințărilor sofisticate.

FLUX ECRIME

Oferă date clare și acționabile despre operațiuni de criminalitate cibernetică și eCrime bazat pe malware, monitorizând de la grupuri de ransomware și afiliații acestora până la campanii de infostealere, permițând echipelor să treacă de la reacție la apărare proactivă a organizației.

Experimentați puterea ESET Threat Intelligence

Programați astăzi o demonstrație și descoperiți valoarea de neegalat pe care ESET Threat Intelligence o poate aduce organizației dvs. Cu o rată de reînnoire de 100%, clienții noștri mulțumiți sunt o dovadă a eficienței soluțiilor noastre. Permiteți-ne să vă arătăm cum vă putem îmbunătăți apărarea cibernetică..

Nu sunteți încă pregătit pentru o demonstrație?

Începeți prin a crea un cont de tip preview în portalul ESET Threat Intelligence pentru a explora fluxurile de date și rapoartele APT.

eset Cybersecurity
Progress. Protected.

Acesta este ESET

Apărare proactivă. Minimizați riscurile prin prevenție.

Rămâneți cu un pas înaintea amenințărilor cibernetice cunoscute și emergente — atacuri direcționate, amenințări zero-day, ransomware, phishing și multe altele — prin abordarea noastră AI-nativă, orientată pe prevenție. ESET combină puterea inteligenței artificiale cu expertiza umană pentru a oferi protecție simplă și eficientă.

Experimentați o securitate de top, bazată pe știință, susținută de peste 30 de ani de inteligență globală internă privind amenințările cibernetice. Rețeaua noastră extinsă de cercetare și dezvoltare, condusă de cercetători recunoscuți în industrie, alimentează platforma noastră de securitate cibernetică premiată, orientată către cloud.

Soluțiile ESET sunt personalizabile, includ suport local și au un impact minim asupra performanței. ESET vă protejează afacerea, astfel încât să puteți valorifica pe deplin potențialul tehnologiei.

ESET ÎN CIFRE

1mld+
utilizatori de internet protejați

500k+
clienți business

178
țări

11
centre globale R&D

CÂȚIVA DINTRE CLIENȚII NOȘTRI

MITSUBISHI MOTORS
Drive your Ambition

protejat de ESET din 2017
peste 9,500 de dispozitive

protejat de ESET din 2019
1,200 dispozitive & 2,700 de căsuțe de e-mail

Canon
Canon Marketing Japan Group

protejat de ESET din 2016
peste 23,000 de dispozitive

partener de securitate ISP din 2008
bază de 2 milioane de clienți

RECUNOAȘTERE DIN INDUSTRIE

SE LABS ® AWARDS
Enterprise Endpoint (Windows)
WINNER 2025

Câștigător al premiilor pentru **Cel mai bun endpoint enterprise** și **Cel mai bun endpoint pentru afaceri mici** la SE Labs Awards 2025

Gartner Peer Insights **Customers' Choice** 2026

Recunoscut drept **„Customers' Choice"** în raportul Gartner® Peer Insights™ **„Voice of the Customer" în categoria Endpoint Protection Platforms) 2026**

FROST & SULLIVAN

Nominalizat ca **„Leader"** în Frost Radar: Endpoint Security 2025, demonstrând excelență în creștere și inovație