



OVERVIEW

# THREAT INTELLIGENCE

Feeds e relatórios de inteligência exclusivos,  
elaborados por especialistas líderes do setor

Progress. Protected.



# Por que adicionar a ESET ao seu stack de CTI?

Compreender o cenário atual de ameaças e as táticas utilizadas pelos cibercriminosos proporciona uma vantagem estratégica fundamental. Essa visão permite que sua organização **fortaleça seus sistemas internos de defesa de forma eficaz**. Dados de inteligência de alta qualidade são a base de qualquer estratégia robusta de Cyber Threat Intelligence (CTI).

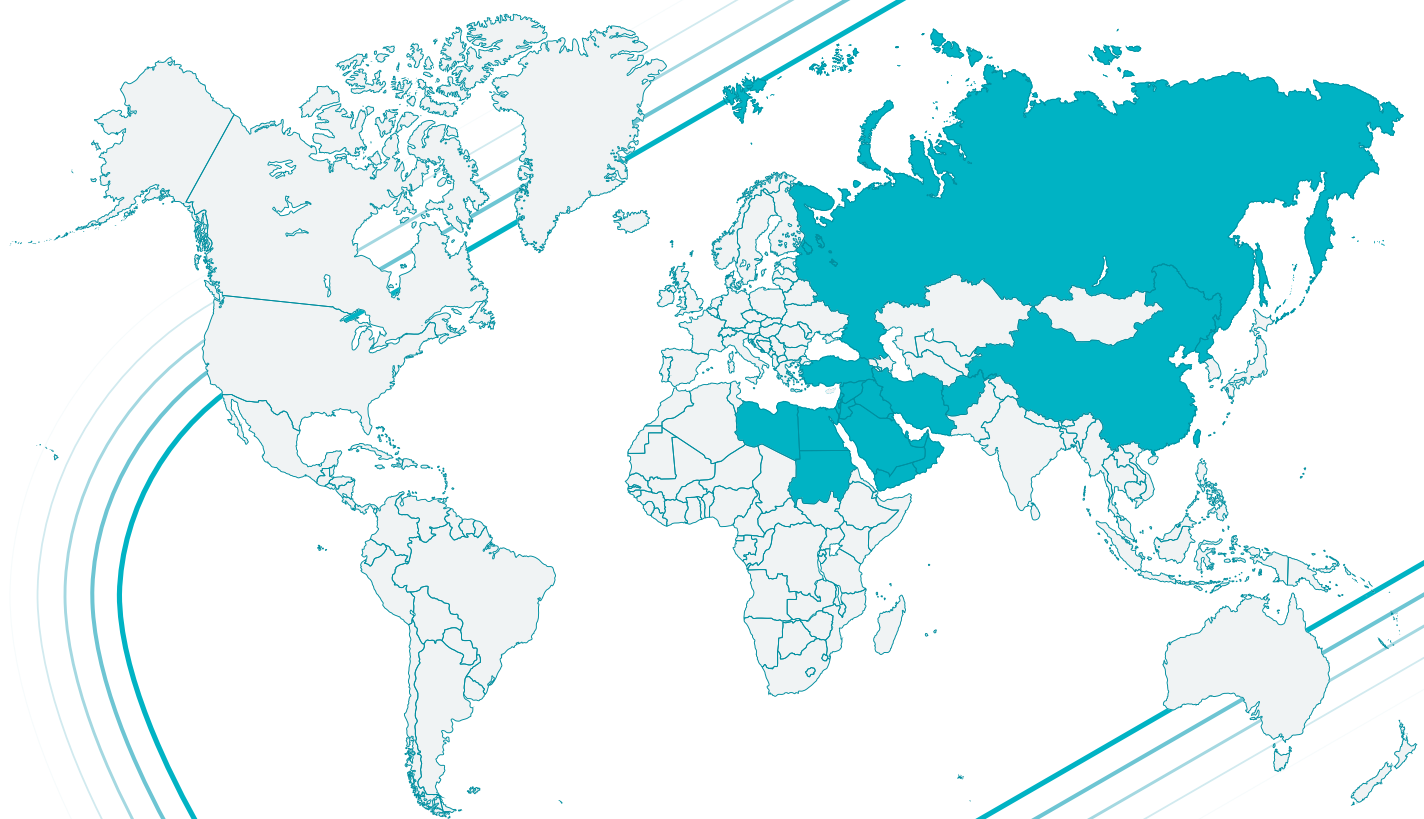
Há mais de 35 anos, a ESET é uma empresa privada, sem dívidas e em constante crescimento. Nosso sucesso é fundamentado em uma abordagem de “prevenção em primeiro lugar”, impulsionada por IA e potencializada pela expertise humana. No centro de nossas operações está **nossa exclusiva Inteligência Global de Ameaças, apoiada por uma ampla rede de P&D liderada por pesquisadores**

**reconhecidos no setor**. Dedicamos o tempo necessário para compreender profundamente as ciberameaças, o que nos permite combatê-las com eficácia.

Independentemente do nível de maturidade das suas soluções atuais de CTI, integrar a **ESET ao seu stack agregará valor incomparável**. Nossos feeds abrangentes de inteligência de ameaças, relatórios de APT e análises sobre eCrime garantem que você esteja sempre um passo à frente das ameaças emergentes, reforçando suas defesas existentes com insights acionáveis e pesquisas de ponta.

# Aproveite a telemetria exclusiva da ESET

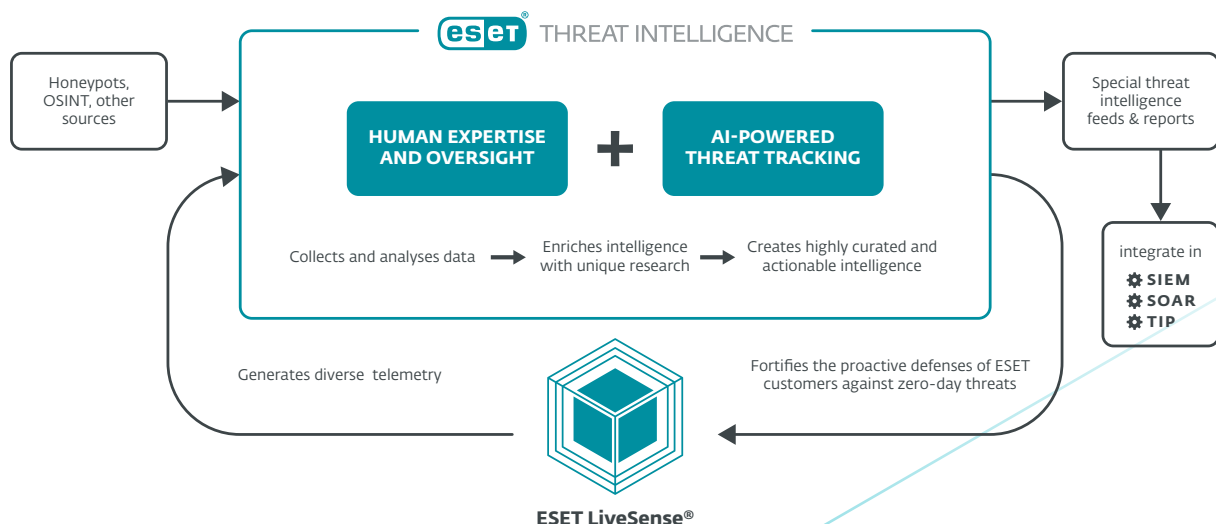
A presença global da ESET, construída ao longo de décadas, oferece a você uma **base de inteligência rica e diversificada**, proveniente de milhões de endpoints. Diferentemente de muitos concorrentes, **nossa telemetria é especialmente robusta em regiões consideradas “mais estratégicas”** do ponto de vista geopolítico no cenário da ciberdefesa. Essa cobertura exclusiva se traduz diretamente em inteligência superior para sua organização. Ao aproveitar a telemetria da ESET, você obtém acesso a informações valiosas e acionáveis de alta qualidade, **fortalecendo suas capacidades de detecção e resposta a ameaças**.



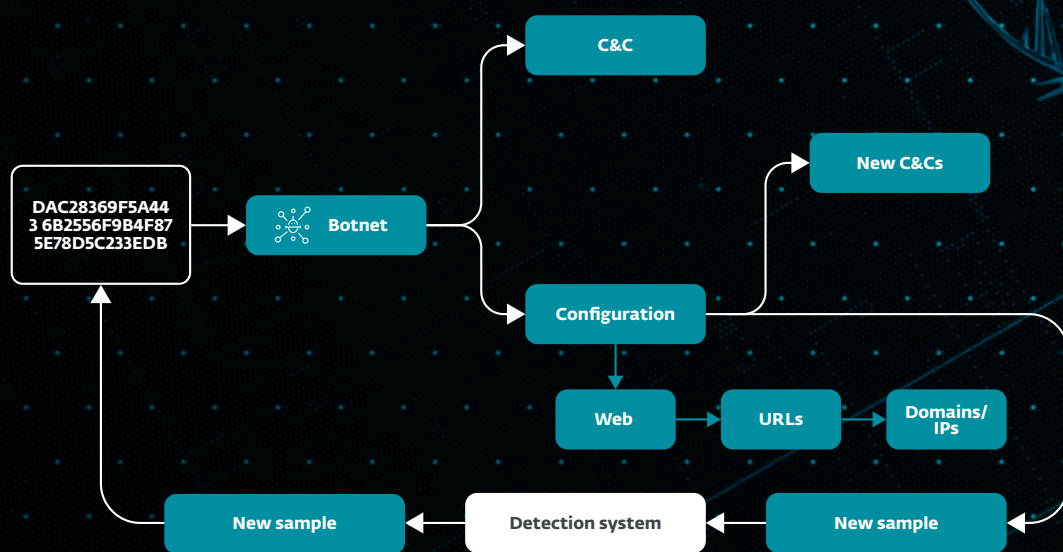
# Inteligência exclusiva e enriquecida para gerar insights acionáveis

A inteligência de ameaças não se resume à simples coleta e consolidação de indicadores — a ESET vai muito além. Utilizamos tecnologia avançada e ampla expertise para processar e enriquecer nossa inteligência, garantindo que ela gere valor real para o seu negócio.

- 1. Telemetria abrangente:** Sua inteligência começa com uma ampla gama de dados de telemetria gerados pelo ESET LiveSense, nossa tecnologia de segurança multicamadas integrada à plataforma ESET PROTECT. Isso garante uma coleta de dados ampla e profunda, proveniente de diversas fontes.
- 2. Métodos diversificados de coleta:** Além do LiveSense, utilizamos diversos métodos de monitoramento e coleta, incluindo honeypots, sensores, recursos de OSINT, web crawling (tanto na clear web quanto na deep web) e Threat Tracking. Isso resulta em um volume significativo de dados de alta qualidade à sua disposição.
- 3. Processamento avançado:** Após a coleta, todos os dados são processados por nossos robustos sistemas de backend, que utilizam IA para classificar e analisar automaticamente as informações. Assim, apenas a inteligência mais relevante e acionável é destacada.
- 4. Análise especializada:** Além do processamento automatizado, nossa equipe qualificada de analistas e pesquisadores de inteligência de ameaças desempenha um papel fundamental. Eles estudam e analisam continuamente diferentes atores de ameaças, suas motivações, TTPs (táticas, técnicas e procedimentos) e ferramentas utilizadas. Essa validação humana adiciona uma camada extra de profundidade e precisão à inteligência, indo além do que o aprendizado de máquina e a automação podem alcançar sozinhos.







As amostras recebidas por meio da telemetria passam por uma análise aprofundada, tanto comportamental quanto estrutural. Esse processo gera indicadores adicionais relevantes, enriquecendo ainda mais sua inteligência de ameaças. Ao examinar minuciosamente cada amostra, extraímos informações valiosas que elevam a qualidade e a eficácia geral da nossa inteligência, proporcionando uma visão mais abrangente e precisa do cenário de ameaças.

# segurança superior por meio de relatórios detalhados de APT

Redigidos em linguagem clara e orientada à ação para fortalecer a postura de segurança da sua organização, nossos relatórios de APT oferecem uma visão aprofundada das campanhas de malware, seus métodos de distribuição e os atores envolvidos.

Tenha acesso ao nosso servidor MISP, ao nosso consultor de IA e agende sessões ao vivo com os principais especialistas em inteligência de ameaças da ESET para obter uma inteligência completa e pronta para agir.

## NOSSA MELHOR PESQUISA AO SEU ALCANCE

Nossa equipe de pesquisa é amplamente reconhecida na indústria de segurança digital graças ao premiado blog WeLiveSecurity. O trabalho de investigação de alta qualidade e os resumos de atividades de APTs (Ameaças Persistentes Avançadas) estão à sua disposição, juntamente com conteúdos ainda mais detalhados e aprofundados. Como cliente ESET, você tem acesso antecipado e exclusivo a todo o conteúdo do WeLiveSecurity.

## CONTEÚDO ACIONÁVEL E CURADO

Nossos relatórios oferecem um contexto aprofundado sobre o que está acontecendo e por quê. Com isso, sua organização pode se antecipar e se preparar para possíveis cenários futuros. E, mais importante, nossos especialistas garantem que o conteúdo seja claro, objetivo e fácil de compreender.

## TOME DECISÕES CRUCIAIS

Tudo isso capacita você e sua organização a tomarem decisões estratégicas e críticas, garantindo uma vantagem competitiva no combate ao cibercrime. Você passa a ter uma compreensão clara do que acontece no "lado oculto da internet", além do contexto essencial para preparar suas defesas internas de forma ágil e eficaz.

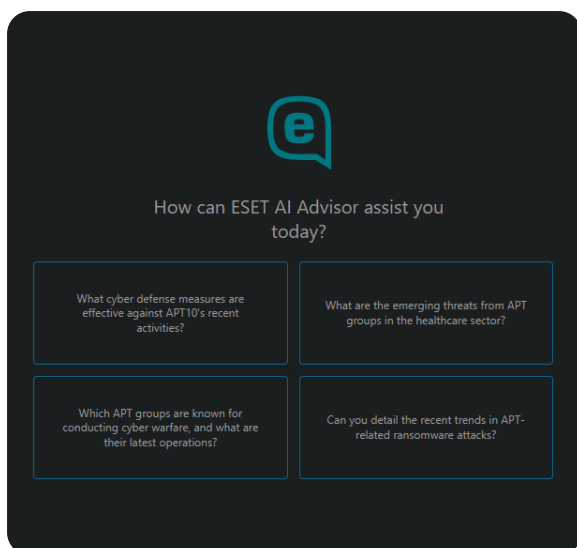
## ACESSO A UM ANALISTA DA ESET

Ao contratar o pacote APT Reports Premium, você terá acesso direto a um analista da ESET por até quatro horas mensais. Isso permite discutir temas com maior profundidade e esclarecer quaisquer dúvidas pendentes com suporte especializado.



## ESET AI ADVISOR

O ESET AI Advisor utiliza IA avançada e expertise em APT para fornecer informações sob demanda e medidas de proteção contra ciberataques. Disponível no formato de chatbot, ele responde às suas consultas de segurança, oferece resumos de APT, reúne IoCs (Indicadores de Comprometimento) e TTPs, além de gerar regras YARA para que você compreenda e previna ameaças com total agilidade.





|                                                     |                                                                                                                                                                   | APT Reports | APT Reports Advanced | APT Reports Ultimate |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------|----------------------|
| <b>Relatórios quinzenais de resumo de atividade</b> | Relatórios que consolidam a atividade de todos os grupos APT monitorados, conforme detalhado anteriormente (dois relatórios por mês)                              | ✓           | ✓                    | ✓                    |
| <b>Relatórios de análise de ameaças</b>             | Análises técnicas regulares ou personalizadas sobre as ameaças mais prevalentes (aproximadamente 30 por ano)                                                      | ✓           | ✓                    | ✓                    |
| <b>Resumo mensal (monthly overview)</b>             | Compilação mensal de informações com foco executivo sobre as ameaças atuais                                                                                       | ✓           | ✓                    | ✓                    |
| <b>Compêndio mensal (monthly digest)</b>            | Índice e resumo executivo dos relatórios e eventos ocorridos ao longo do mês                                                                                      | ✓           | ✓                    | ✓                    |
| <b>Pré-acesso ao welivesecurity</b>                 | Acesso antecipado a relatórios de ameaças e artigos selecionados do WeLiveSecurity                                                                                | ✓           | ✓                    | ✓                    |
| <b>Feed de ioc de APT</b>                           | Acesso completo ao feed em formato STIX/TAXII, contendo os IoCs (Indicadores de Comprometimento) presentes nos relatórios                                         | ✓           | ✓                    | ✓                    |
| <b>Acesso ao servidor MISP</b>                      | Acesso total ao servidor MISP da ESET, com todas as informações disponíveis nos relatórios para integração aos seus sistemas                                      | ✗           | ✓                    | ✓                    |
| <b>ESET AI Advisor</b>                              | Acesso ao consultor de IA da ESET, que fornece insights estratégicos e resumos dos relatórios de APT disponíveis                                                  | ✗           | ✓                    | ✓                    |
| <b>Acesso a analistas</b>                           | Comunicação direta com analistas por meio de plataformas como MS Teams e e-mail, limitada a quatro horas mensais (não cumulativas, incluindo tempo de preparação) | ✗           | ✗                    | ✓                    |



# De indicadores a inteligência: Seja mais estratégico que o cibercrime (eCrime)

Os relatórios de eCrime da ESET Threat Intelligence oferecem uma visão aprofundada das operações de ransomware e do cibercrime em geral. Tenha visibilidade sobre as ferramentas utilizadas pelos atacantes, sua infraestrutura e suas estratégias de monetização, com o respaldo da pesquisa global da ESET. Vá além dos IoCs e acesse inteligência contextual que fortalece sua defesa proativa e aprimora sua tomada de decisões estratégicas.

## O QUE TORNA OS RELATÓRIOS DE eCrime DA ESET DIFERENTES

### DEFESA PROATIVA

Obtenha inteligência não apenas sobre os grupos de eCrime, mas também sobre os afiliados que efetivamente executam os ataques. Entenda como eles operam e antecipe seus próximos movimentos para se manter sempre um passo à frente.

### EFICIÊNCIA OPERACIONAL

Utilize informações claras e curadas, baseadas em incidentes reais, para eliminar o ruído. Facilite a detecção de ameaças pela sua equipe, acelere as respostas e direcione as atividades de threat hunting para onde realmente importa.

### VISIBILIDADE EXCLUSIVA

Vá além dos feeds públicos de ameaças com uma visão mais profunda das táticas de monetização, da infraestrutura e do comportamento real dos afiliados — tudo respaldado pela pesquisa e pela telemetria global da ESET.

|                                       |                                                                                                                                                                                                                                                                                                                                                 | eCrime Reports | eCrime Reports Advanced |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------------|
| <b>Resumo de atividade</b><br>MENSUAL | <ul style="list-style-type: none"> <li>As campanhas mais recentes de ransomware e infostealers, sintetizadas em informações estratégicas e objetivas</li> <li>Quem são os alvos, como os ataques se desenvolvem e o que falhou</li> <li>Principais lições aprendidas, IoCs e orientações práticas para fortalecer sua resiliência</li> </ul>    | ✓              | ✓                       |
| <b>Análise Técnica</b><br>MENSUAL     | <ul style="list-style-type: none"> <li>Análises aprofundadas sobre atores de ameaças específicos (ex.: FIN7)</li> <li>Cadeia completa do ataque: do acesso inicial ao roubo de dados</li> <li>Táticas dos atacantes, ferramentas utilizadas, infraestrutura, mapeamento no MITRE ATT&amp;CK® e IoCs (Indicadores de Comprometimento)</li> </ul> | ✓              | ✓                       |
| <b>Compêndio mensal</b><br>MENSUAL    | <ul style="list-style-type: none"> <li>Resumo executivo sobre a atividade recente de ransomware e infostealers</li> <li>Principais tendências, incidentes relevantes e ameaças emergentes</li> <li>Apoia a liderança na avaliação de riscos e na definição de prioridades, sem complexidade técnica</li> </ul>                                  | ✓              | ✓                       |
| <b>Feed de eCrime</b>                 | <ul style="list-style-type: none"> <li>IoCs atualizados e curados sobre grupos de ransomware, seus afiliados e campanhas de infostealers</li> <li>Disponível no formato padrão STIX/TAXII</li> </ul>                                                                                                                                            | ✓              | ✓                       |
| <b>ESET AI Advisor</b>                | <ul style="list-style-type: none"> <li>Utiliza informações de eCrime para responder às suas perguntas relacionadas a ameaças</li> <li>Ajuda a interpretar incidentes e o comportamento dos atacantes</li> <li>Torna a inteligência de ameaças acessível de forma imediata para suas equipes e tomadores de decisão</li> </ul>                   | ✗              | ✓                       |
| <b>Acesso ao servidor MISP</b>        | <ul style="list-style-type: none"> <li>Integração direta com inteligência de ameaças curada</li> <li>Ingestão automática de IoCs para enriquecer suas defesas</li> <li>Otimize seus fluxos de trabalho, acelere a detecção e fortaleça a resposta a incidentes</li> </ul>                                                                       | ✗              | ✓                       |



# Feeds de dados claros e objetivos

Aprimore sua visibilidade do cenário de ameaças com a telemetria exclusiva da ESET. Fornecemos feeds de dados altamente curados nos formatos JSON e STIX 2.1, integrando-se perfeitamente às suas ferramentas de SIEM, TIP ou SOAR.

Diferentemente de muitos provedores de Threat Intelligence (TI), aplicamos um rigoroso processo de filtragem e validação para garantir que nossos feeds sejam meticulosamente avaliados e realmente relevantes.

Isso permite que seus sistemas de segurança executem ações automáticas quando necessário, ao mesmo tempo em que capacita seus analistas com uma visão abrangente e estratégica do panorama global de ameaças.

- Garantimos que os dados sejam leves, altamente relevantes, livres de duplicidades e acompanhados de confidence scoring (pontuação de confiança)
- São resultado de um processo avançado de filtragem, enriquecido com inteligência estratégica fornecida pelos pesquisadores da ESET
- Referência de mercado, especialmente em dados relacionados a botnets
- Baixa necessidade de manutenção, graças ao conteúdo devidamente curado
- Feeds em tempo real, contendo apenas IoCs (Indicadores de Comprometimento) recentes e prevalentes

## FEED DE DADOS MALICIOSOS

Informações em tempo real sobre amostras de malware recém-descobertas, suas características e IoCs. Inclui hashes de arquivos, carimbos de data e hora e tipos de ameaças, ajudando você a bloquear arquivos maliciosos antes que causem danos.

## FEED DE RANSOMWARE

Dados em tempo real sobre famílias de ransomware ativas e amostras prevalentes. Permite bloqueio proativo para prevenir violações de segurança e interrupções custosas.

## FEED DE BOTNETS

Impulsionado pelo rastreador de botnets da ESET, este feed inclui três subfeeds: botnet, C&C (Comando e Controle) e alvos. Fornece detalhes de detecção, hashes de arquivos, registros da última comunicação, arquivos baixados, endereços IP, protocolos e informações sobre os alvos.

## FEED DE IOC DE APT

Insights sobre Ameaças Persistentes Avançadas com base nas pesquisas da ESET. É exportado do servidor MISP interno da ESET e alinhado aos relatórios de APT. Está disponível como parte dos relatórios ou como feed independente para integração ao seu stack.

## FEED DE PUA / ADWARE

A ESET possui mais de duas décadas de experiência na classificação de PUAs (Aplicações Potencialmente Indesejadas), o que confere profundidade e precisão incomparáveis à sua inteligência. Os feeds de adware fornecem informações em tempo real sobre adware ativo e ameaças semelhantes, permitindo bloqueio proativo antes do impacto.

## FEED DE PUA / APLICATIVOS DE DUPLO USO (DUAL-USE)

Monitora ferramentas legítimas (por exemplo, RMMs) que são utilizadas indevidamente por atacantes. Isso ajuda a antecipar abusos dessas aplicações, reduzindo o ruído com dados personalizados e de baixa redundância.

## FEED DE DOMÍNIOS

Fornecer dados sobre domínios maliciosos, incluindo nome de domínio, endereço IP e data associada. Os domínios são classificados por nível de severidade, permitindo priorizar ações, como o bloqueio de domínios de alto risco.

## FEED DE URL

Feed curado de URLs específicas, com informações detalhadas sobre cada endereço e seus domínios de hospedagem. Inclui apenas achados de alta confiança, respaldados por explicações claras e de fácil compreensão sobre as URLs sinalizadas.

## FEED DE IP

Receba dados acionáveis sobre IPs maliciosos. Sua estrutura é idêntica à dos feeds de domínios e URLs. Utilize-o para identificar ameaças comuns, bloquear IPs de alta severidade, monitorar as de menor risco e aprofundar investigações com dados adicionais para avaliar possíveis impactos.

## FEED DE AMEAÇAS PARA ANDROID

Oferece informações em tempo real sobre ameaças prevalentes no Android e seus IoTs, permitindo bloqueio proativo. É criado com base na telemetria da ESET e atualizado quase em tempo real, com deduplicação diária.

## FEED DE INFOTEALERS PARA ANDROID

Feed especializado dentro das ameaças para Android, que fornece detalhes sobre amostras atuais de infostealers e dados relacionados. Oferece visibilidade aprofundada sobre famílias ativas, permitindo bloqueio proativo antes que causem danos.

## FEED DE URL DE GOLPES (SCAMS)

Mantenha-se um passo à frente dos golpes com dados em tempo real sobre URLs fraudulentas. Abrange e-commerces falsos, golpes de investimento, golpes românticos e fraudes com criptomoedas. É gerado a partir de todas as fontes de URLs da ESET quase em tempo real, com deduplicação a cada 24 horas.

## FEED DE GOLPES CRIPTO (CRYPTOSCAM)

Antecipe-se a golpes envolvendo criptomoedas com atualizações em tempo real sobre domínios e URLs maliciosas, além de dados associados. Proveniente da ampla telemetria da ESET, fornece inteligência antecipada e segmentada para bloqueio proativo e proteção de ativos.

## FEED DE ANEXOS DE E-MAIL MALICIOSOS

O e-mail é um dos principais vetores de ataque. Este feed disponibiliza dados em tempo real sobre anexos maliciosos identificados pela extensa telemetria de varredura de e-mails da ESET.

## FEED DE URL DE PHISHING

Entrega inteligência em tempo real sobre URLs de phishing ativas a partir do banco de dados dedicado da ESET. Atualizado continuamente e com deduplicação diária, ajuda a detectar e bloquear sites fraudulentos antes que comprometam dados sensíveis.

## FEED DE SMISHING

Fornecer informações atualizadas sobre phishing via SMS (smishing), incluindo domínios, URLs e indicadores relacionados. Baseado na telemetria global da ESET, é desenvolvido quase em tempo real com deduplicação diária.

## FEED DE GOLPES POR SMS (SMS SCAM)

Proteja-se contra golpes via SMS com um feed em tempo real sobre domínios e URLs maliciosas. Atualizado quase em tempo real e deduplicado diariamente, auxilia na identificação e bloqueio de ameaças sofisticadas.

## FEED DE ECRIME

Obtenha dados claros e acionáveis sobre operações de cibercrime e eCrime baseado em malware. Monitore desde grupos de ransomware e seus afiliados até campanhas de infostealers, permitindo que sua equipe evolua da reação para uma postura de defesa proativa.

## Experience the power of ESET Threat Intelligence

Schedule a demo with us today and discover the unparalleled value ESET Threat Intelligence can bring to your organization. With a 100% renewal rate, our satisfied customers are a testament to the effectiveness of our solutions. Let us show you how we can enhance your cybersecurity defenses.

## Not ready for a demo call yet?

Start by creating [a preview account](#) in the ESET Threat Intelligence portal to explore feeds and APT reports.



# Isso é a ESET

## Defesa proativa. Minimize riscos com prevenção.

Mantenha-se um passo à frente das ameaças cibernéticas conhecidas e emergentes com nossa abordagem de prevenção, nativa de IA. Combinamos o poder da IA e a experiência humana para tornar a proteção fácil e eficaz.

Experimente a proteção de classe mundial graças à nossa inteligência global em ameaças cibernéticas interna, compilada e analisada por mais de 30 anos, que impulsiona nossa vasta rede de P&D liderada por pesquisadores renomados na indústria.

O ESET PROTECT, nossa plataforma de cibersegurança XDR baseada na nuvem, combina capacidades de prevenção de próxima geração, detecção e caça proativa a ameaças com uma ampla variedade de serviços de segurança, incluindo detecção e resposta gerenciadas.

Nossas soluções altamente personalizáveis incluem suporte local e têm um impacto mínimo no desempenho, identificando e neutralizando ameaças conhecidas e emergentes antes que possam ser executadas, apoiando a continuidade dos negócios e reduzindo o custo de implementação e gestão.

A ESET protege o seu negócio para que você possa desbloquear todo o potencial da tecnologia.

## ESET EM NÚMEROS

**1bn+**

usuários  
da internet  
protegidos

**500k+**

clientes  
empresariais

**176**

países e  
territórios

**11**

centros globais  
de P&D

## ALGUNS DOS NOSSOS CLIENTES



protegidos pela ESET  
desde 2017 mais de 9.000  
endpoints



protegidos pela ESET desde  
2016 mais de 4.000 caixas de  
entrada



protegidos pela ESET  
desde 2016 mais de 32.000  
endpoints



Parceiro de segurança de ISP  
desde 2008  
Base de clientes de 2 milhões

## RECONHECIMENTO



A ESET é uma das principais empresas  
em **testes independentes realizados**  
testes independentes realizados.



A ESET consistentemente alcança as  
melhores classificações na plataforma  
global de avaliações G2, e suas soluções  
são amplamente **apreciadas por**  
**clientes em todo o mundo.**



A ESET foi reconhecida como Líder  
em segurança de endpoints no IDC  
MarketScape: Worldwide Modern  
Endpoint Security for Midsize Businesses  
2024 Vendor Assessment.