VISÃO GERAL

THREAT INTELLIGENCE

Feeds de inteligência exclusivos e relatórios de APT dos principais profissionais do setor

Progress. Protected.

Obtenha uma perspectiva única sobre o cenário de ameaças

RECEBA INFORMAÇÕES EXCLUSIVAS
A ESET reúne inteligência contra ameaças de uma variedade única de fontes e conta com uma experiência de campo incomparável, auxiliando no combate a ataques de cibersegurança cada vez mais sofisticados.

TENHA VANTAGENS SOBRE OS ADVERSÁRIOS
A ESET "segue o dinheiro", monitorando especialmente os locais em que foram detectados grupos de APT que visam empresas ocidentais, como Rússia, China, Coreia do Norte e Irã. Receba informações sobre novas ameaças em primeira mão.

TOME DECISÕES IMPORTANTES MAIS RAPIDAMENTE
Previna ameaças e tome decisões mais rápidas e eficazes com os relatórios abrangentes e feeds cuidadosamente selecionados da ESET. Diminua a sua exposição às ameaças predominantes, com alertas antecipados de especialistas.

MELHORE A SUA POSTURA DE CIBERSEGURANÇA
Com as informações dos feeds de inteligência da ESET, aprimore seus recursos de busca e correção de ameaças, bloqueie APTs e ransomwares e melhore a sua arquitetura de cibersegurança.

INVESTIGAÇÃO DE AMEAÇAS AUTOMATIZADA
A tecnologia da ESET tem uma busca de ameaças ininterrupta, em múltiplas camadas, desde a pré-inicialização até o estado de repouso. Beneficie-se da telemetria em todos os países em que a ESET realiza a detecção de ameaças emergentes.

Vantagens da ESET

Expertise humana aliada ao machine learning. Nosso sistema de reputação, o LiveGrid®, é composto por 110 milhões de sensores em todo o mundo e verificado por nossos centros de P&D.

EXPERTISE HUMANA ALIADA A MACHINE LEARNING
O uso de machine learning para automatizar decisões e avaliar possíveis ameaças é uma parte essencial da abordagem da ESET. É tão potente, porém, quanto as pessoas que estão por trás do sistema. A expertise humana é fundamental para fornecer a inteligência contra ameaças mais precisa possível, pois os agentes de ameaças podem ser oponentes inteligentes.

SISTEMA DE REPUTAÇÃO POTENTE — LIVEGRID®
Os produtos ESET Endpoint contam com um sistema de reputação na nuvem que fornece informações relevantes sobre as ameaças mais recentes e arquivos inofensivos. Nosso sistema de reputação, o LiveGrid®, é composto por 110 milhões de sensores em todo o mundo, cuja saída é verificada por nossos centros de P&D, proporcionando aos clientes o mais alto nível de confiança ao visualizar informações e relatórios em seu console.

ORIGEM NA UNIÃO EUROPEIA, PRESENÇA MUNDIAL
Com sede na União Europeia, a ESET está no setor de segurança há mais de 30 anos, com 22 escritórios em todo o mundo, 13 instalações de P&D e presente em mais de 200 países e territórios, o que nos auxilia a fornecer aos nossos clientes uma perspectiva global sobre todas as tendências e ameaças mais recentes.

Relatórios de ameaças persistentes avançadas (APT)

NOSSAS MELHORES PESQUISAS AO SEU ALCANCE

Nossa equipe de pesquisa é amplamente conhecida no setor de cibersegurança, em virtude do nosso premiado blog We Live Security. As pesquisas de excelência da equipe e os resumos das atividades de APT estão disponíveis, junto com informações muito mais detalhadas. Os clientes ESET recebem uma prévia exclusiva de todo o conteúdo do We Live Security.

CONTEÚDO PRÁTICO E SELECIONADO

Os relatórios fornecem informações contextuais para entender melhor sobre os acontecimentos e suas razões. Dessa forma, as organizações podem se preparar com antecedência para eventuais incidentes. É importante ressaltar que nossos especialistas garantem um conteúdo de fácil entendimento.

TOME DECISÕES IMPORTANTES RAPIDAMENTE

Todas essas informações auxiliam as organizações na tomada de decisões cruciais, resultando em uma vantagem estratégica no combate ao cibercrime. Elas fornecem uma compreensão sobre o que acontece no "lado ruim da internet", oferecendo um contexto fundamental para que sua organização possa se preparar internamente de forma ágil.

ACESSO A ANALISTAS DA ESET

Todo cliente que solicitar o pacote APT Reports Premium também terá acesso a um analista da ESET, por até quatro horas por mês, com a oportunidade de discutir tópicos de forma mais detalhada e obtendo auxílio na resolução de problemas pendentes.

COM OS RELATÓRIOS DE APT, VOCÊ RECEBE

- Acesso a análises técnicas particulares e aprofundadas
- Relatórios de resumo de atividades de grupos de APT
- Um resumo mensal para os seus executivos de C-level
- Acesso direto a um profissional de cibersegurança da ESET
- Acesso ao nosso servidor MISP

ANÁLISE APROFUNDADA

O pacote inclui relatórios mensais de análise técnica detalhada descrevendo campanhas recentes, novos conjuntos de ferramentas e assuntos relacionados. Além disso, a cada duas semanas, você receberá um relatório de resumo de atividades, com a descrição das mais recentes campanhas de APT monitoradas pela equipe de pesquisa da ESET, provenientes de diferentes agentes de ameaças, bem como seus alvos e, evidentemente, os indicadores de comprometimento (IoCs) associados. Uma síntese mensal combina informações de todos os relatórios de análise técnica e resumo de atividades lançados no mês anterior, em formato mais curto e de fácil compreensão.

A disponibilidade dos relatórios e feeds do ESET Threat Intelligence varia conforme o país. Para mais informações, entre em contato com o representante local da ESET.

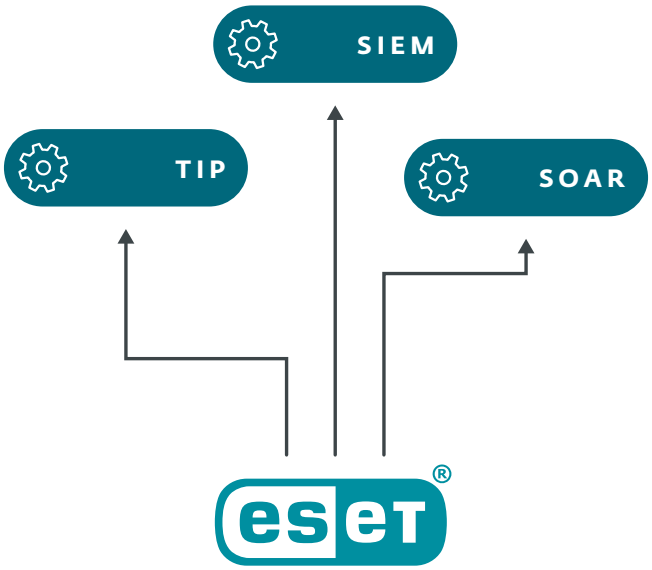
Integre o ESET Threat Intelligence em seu sistema

Integrar a telemetria ESET é simples e melhora a funcionalidade do seu TIP, SIEM ou SOAR

Temos uma API abrangente, com documentação completa

Fornecemos dados em formatos padronizados – como feeds JSON e STIX via TAXII – possibilitando a integração em qualquer ferramenta

Para IBM QRadar, Anomali e Logpoint, disponibilizamos manuais de integração passo a passo, para uma implementação rápida e descomplicada, e estamos constantemente adicionando suporte para outras plataformas



Como é gerada nossa inteligência contra ameaças? Ciclo de vida da inteligência contra ameaças da ESET

A criação da nossa inteligência é um ciclo que se fortalece por si.

Utiliza-se uma ampla variedade de dados gerados pela telemetria do ESET LiveSense, nossa tecnologia de segurança multicamadas integrada à Plataforma ESET PROTECT.

A telemetria coletada é complementada por diversas fontes adicionais, como honeypots ou OSINT.

Em seguida, ela é processada em nossos sistemas robustos de rastreamento e processamento de malware aprimorados por IA. Esses sistemas são capazes de descobrir e incorporar uma grande quantidade de informações contextuais aos dados de inteligência.

Como elemento crucial, nossa equipe especialista em inteligência contra ameaças supervisiona o produto final, garantindo sua constante atualização com dados recentes, auxiliando na tomada de decisões mais informadas e ágeis.

Feeds de inteligência exclusivos da ESET

Aumente sua perspectiva do cenário mundial de ameaças com base em uma telemetria exclusiva. Os feeds da ESET provêm dos nossos centros de pesquisa em todo o mundo, oferecendo uma visão abrangente e permitindo que você bloqueie rapidamente indicadores de comprometimento em seu ambiente. Os feeds estão nos formatos • JSON • STIX 2.1

FEED DE ARQUIVOS MALICIOSOS

Esse feed fornece informações em tempo real sobre novas amostras de malware recém-descobertas, suas características e IoCs. Assim, é possível compreender quais arquivos maliciosos estão em circulação, bloqueando-os de forma proativa, antes de causarem danos. O feed apresenta domínios maliciosos, incluindo hashes de arquivos, carimbos de data e hora, tipo de ameaça detectada e outras informações detalhadas.

FEED DE DOMÍNIOS

Esse feed pode ser utilizado para bloquear domínios considerados maliciosos. O feed inclui informações como nomes de domínio, endereços IP e as datas a eles associadas. Os domínios são classificados com base em sua gravidade, permitindo ajustar a sua resposta, por exemplo, para bloquear apenas domínios de alta gravidade.

FEED DE IP

Esse feed compartilha IPs considerados maliciosos e os dados associados a eles. A estrutura dos dados é bastante semelhante à utilizada para os feeds de domínio e URL. O principal caso de uso aqui é compreender quais IPs maliciosos estão atualmente em circulação, bloquear os IPs de alta gravidade, identificar os menos graves e investigar mais a fundo.

FEED DE URL

De forma semelhante ao feed de domínios, o feed de URL analisa endereços específicos, incluindo informações detalhadas sobre os dados relacionados à URL, bem como informações sobre os domínios que as hospedam. Todas as informações são filtradas para exibir somente resultados de alta confiabilidade.

FEED DE BOTNETS

Com base na exclusiva rede de rastreamento de botnets da ESET, o feed de botnets apresenta três tipos de subfeeds: botnets, comando e controle (C&C) e alvos. Os dados fornecidos incluem itens como detecção, hash, última atividade, arquivos baixados, endereços IP, protocolos, alvos e outras informações.

FEED DE APT

Esse feed consiste em informações sobre ameaças persistentes avançadas (APTs) produzidas pelas pesquisas da ESET. Em termos geais, o feed é uma exportação a partir do servidor MISP interno da ESET. Todos os dados compartilhados também são explicados com mais detalhes nos relatórios de APT. O feed de APT também integra os relatórios de APT, mas pode ser adquirido de forma separada.

Com os feeds ESET, você recebe

- ✓ DADOS SELECIONADOS
- ✓ CONTEÚDO PRÁTICO
- ✓ MENOS FALSOS POSITIVOS
- ✓ ATUALIZAÇÕES FREQUENTES
- ✓ API ABRANGENTE

A disponibilidade dos relatórios e feeds do ESET Threat Intelligence varia conforme o país. Para mais informações, entre em contato com o representante local da ESET.

Sobre a ESET

Cibersegurança empresarial de última geração

NÃO APENAS INTERROMPEMOS VIOLAÇÕES, NÓS AS IMPEDIMOS DE OCORRER

Diferentemente das soluções convencionais, que têm uma abordagem de reação às ameaças já executadas, a ESET oferece uma abordagem única de prevenção baseada em IA, aliada à expertise humana, uma renomada inteligência global contra ameaças e uma extensa rede de pesquisa e desenvolvimento (P&D), liderada por pesquisadores aclamados no setor, sempre buscando a inovação contínua da nossa tecnologia de segurança multicamadas.

Experimente uma proteção sem igual contra ransomwares, phishing, ameaças de dia zero e ataques direcionados com a nossa premiada plataforma de cibersegurança XDR na nuvem, que combina prevenção, detecção e busca proativa de ameaças de última geração. Nossas soluções altamente personalizáveis incluem suporte local. Com impacto mínimo no desempenho do endpoint, identificam e neutralizam ameaças emergentes antes que possam ser executadas, garantindo a continuidade dos negócios e reduzindo os custos de implementação e gerenciamento.

Em um mundo em que a tecnologia permite o progresso, a ESET garante a proteção do seu negócio.

A ESET EM NÚMEROS

Mais de 1 bilhão
de usuários da internet protegidos

Mais de 400 mil
clientes empresariais

200
países e territórios

13
centros globais de P&D

RECONHECIMENTOS NO SETOR

A ESET é reconhecida por mais de 700 avaliações coletadas na Gartner Peer Insights

A ESET é reconhecida por sua retribuição à comunidade, com o Prêmio Tech Cares 2023, da TrustRadius

RECONHECIMENTO DE ANALISTAS

Em 2023, a IDC colou a ESET entre os cinco principais fornecedores de inteligência contra ameaças, com destaque para o perfil do ESET Threat Intelligence.

A ESET foi reconhecida como "Top Player" no Advanced Persistent Threat (APT) Protection - Market Quadrant 2023 do Radicati, pelo quarto ano consecutivo.

A ESET é a empresa líder em software de cibersegurança independente, e está classificada entre as 10 melhores de um total de 354 colaboradores no framework MITRE ATT&CK.

CERTIFICAÇÃO ISO EM SEGURANÇA

A ESET está em conformidade com a ISO/IEC 27001:2013, norma de segurança internacionalmente reconhecida e aplicável na implementação e gestão de segurança da informação. A certificação é concedida pelo organismo de certificação credenciado SGS e demonstra a total conformidade da ESET com as melhores práticas líderes do setor.

ALGUNS DE NOSSOS CLIENTES

protegida pela ESET desde 2017, mais de 9 mil endpoints

protegida pela ESET desde 2016, mais de 4 mil caixas de e-mail

protegida pela ESET desde 2016, mais de 32 mil endpoints

Partner de segurança para ISP desde 2008, 2 milhões de clientes

ALGUNS DE NOSSOS PRINCIPAIS PRÊMIOS

★★★★★

"A IMPLEMENTAÇÃO FOI MUITO SIMPLES. EM COOPERAÇÃO COM A EQUIPE TÉCNICA BEM TREINADA DA ESET, COLOCAMOS NOSSA NOVA SOLUÇÃO DE SEGURANÇA ESET EM FUNCIONAMENTO EM POUCAS HORAS."

Gerente de TI, Diamantis Masoutis S.A., Grécia, mais de 6 mil dispositivos

★★★★★

"FICAMOS MUITO IMPRESSIONADOS COM O APOIO E ASSISTÊNCIA QUE RECEBEMOS. ALÉM DE SER UM ÓTIMO PRODUTO, O EXCELENTE ATENDIMENTO E SUPORTE QUE RECEBEMOS FOI O QUE REALMENTE NOS LEVOU A MIGRAR TODOS OS SISTEMAS DA PRIMORIS PARA A ESET."

Joshua Collins, gerente de operações de data center, Primoris Services Corporation, Estados Unidos, mais de 4 mil dispositivos