VISÃO GERAL

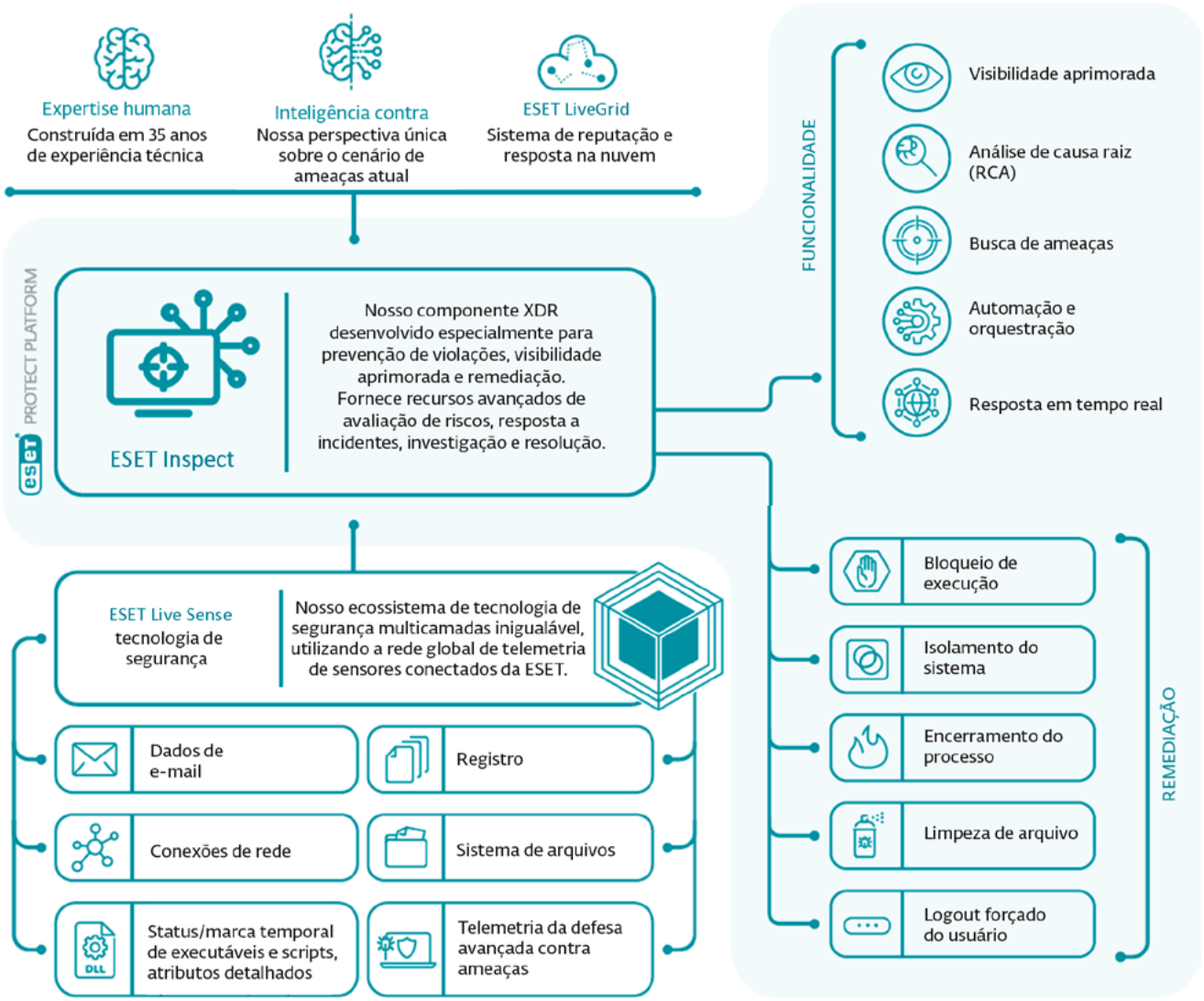
INSPECT

O componente XDR da plataforma ESET PROTECT previne violações, proporcionando visibilidade aprimorada e remediação.

O que é uma solução de detecção e resposta estendida (XDR)?

O ESET Inspect, componente XDR da plataforma ESET PROTECT, é uma ferramenta para identificação de comportamentos anômalos e violações, avaliação de riscos, resposta a incidentes, investigações e remediação.

Ele permite aos respondentes de incidentes monitorarem e avaliarem todas as atividades na rede e nos dispositivos conectados. Também auxilia na automação de ações de remediação imediatas, caso seja necessário. As mais de 800 regras de detecção da ESET, e que seguem aumentando, possibilitam uma busca de ameaças abrangente.



O diferencial da ESET

PREVENÇÃO, DETECÇÃO E RESPOSTA COMPLETAS

Permite a análise e a remediação de qualquer problema de segurança na sua rede. A segurança multicamadas da ESET, em que cada camada envia dados para o ESET Inspect, analisa grandes quantidades de dados em tempo real, para que nenhuma ameaça passe despercebida..

SOLUÇÃO DE UM FORNECEDOR QUE PRIORIZA A SEGURANÇA

A ESET vem combatendo ciberameaças há mais de 30 anos. Como uma empresa com base científica, esteve na vanguarda de desenvolvimentos como o machine learning, tecnologia em nuvem e, agora, a XDR.

É MELHOR PREVENIR DO QUE REMEDIAR

A abordagem da ESET para a XDR está estreitamente relacionada aos seus produtos de prevenção multipremiados. Devido ao compromisso com o desenvolvimento de tecnologias de detecção de alta qualidade, a tecnologia de prevenção da ESET é referência mundial.

VISIBILIDADE DETALHADA DA REDE

Com regras de detecção transparentes (a ESET tem mais de 800 e segue expandindo), IoC (indicadores de comprometimento) avançados e capacidade de pesquisa, uma análise aprofundada de executáveis da sua rede permite a identificação de todas as atividades suspeitas.

FLEXIBILIDADE DE IMPLEMENTAÇÃO

Escolha a forma de implementação da sua solução de segurança: o ESET Inspect pode ser executado por meio de seus próprios servidores, no local, ou por uma instalação com base nuvem, permitindo o ajuste da sua configuração conforme as suas metas de TCO e capacidades de hardware.

GERAÇÃO AUTOMÁTICA DE INCIDENTES

Obtenha visibilidade completa com incidentes automaticamente gerados e bem visualizados. O ESET Inspect correlaciona grandes volumes de dados para encontrar eventos de causa raiz, compilando-os em incidentes abrangentes e permitindo que você os resolva de forma imediata.

PRONTA PARA USO

A solução ESET opera sem a necessidade de configurações adicionais, mas é suficientemente robusta para permitir ajustes detalhados por buscadores de ameaças experientes.

MITRE ATT&CK

O ESET Inspect vincula suas detecções à estrutura MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), a qual, com apenas um clique, fornece informações abrangentes até mesmo sobre as ameaças mais complexas.

SISTEMA DE REPUTAÇÃO

A filtragem extensiva permite aos engenheiros de segurança identificarem todos os aplicativos conhecidos, utilizando o robusto sistema de reputação da ESET. O sistema da ESET conta com um banco de dados de centenas de milhões de arquivos benignos, garantindo que as equipes de segurança possam dedicar seu tempo aos arquivos desconhecidos e potencialmente maliciosos, em vez de falsos positivos.

AUTOMATIZAÇÃO E PERSONALIZAÇÃO

Ajuste facilmente o ESET Inspect ao nível de detalhe e automatização conforme a sua necessidade. Escolha o nível de interação desejado, além do tipo e quantidade de dados a serem armazenados, durante a configuração inicial, com o auxílio de perfis de usuário pré-definidos. Em seguida, deixe o modo de aprendizagem mapear o ambiente da sua organização e sugerir exclusões para falsos positivos, quando necessário.

Digital Security
Progress. Protected.

Funcionalidades da solução

SISTEMA DE GERENCIAMENTO DE INCIDENTES

Agrupe, em unidades lógicas, objetos como detecções, dispositivos, executáveis ou processos para visualizar eventos potencialmente maliciosos em uma linha do tempo, com ações de usuário relacionadas. O ESET Inspect sugere automaticamente ao respondente de incidente todos os eventos e objetos relacionados que podem auxiliar nas etapas de triagem, investigação e resolução de um incidente.

OPÇÕES DE RESPOSTA EM TEMPO REAL

O ESET Inspect oferece ações de resposta de fácil acesso em apenas um clique, como reiniciar e desligar um endpoint, isolar os endpoints do restante da rede, executar uma varredura sob demanda, encerrar processos em execução e bloquear qualquer aplicativo com base em seu valor de hash. Além disso, devido à opção de resposta em tempo real do ESET Inspect, chamada terminal, os profissionais de segurança podem se beneficiar do conjunto completo de opções de investigação e remediação no PowerShell.

ANÁLISE DE CAUSA RAIZ

Visualize facilmente a análise de causa raiz e a árvore de processos completa de qualquer cadeia de eventos potencialmente maliciosos, aprofunde-se no nível de detalhe desejado e tome decisões informadas com base no contexto fornecido e nas explicações para as causas benignas e maliciosas, elaboradas por nossa equipe de especialistas em malware.

API PÚBLICA

O ESET Inspect dispõe de uma API REST pública, que permite acessar e exportar detecções e sua remediação, possibilitando a integração efetiva com ferramentas como SIEM, SOAR, ferramentas de help desk e muitas outras.

MÚLTIPLOS INDICADORES DE COMPROMETIMENTO

Visualize e bloqueie módulos com base em mais de 30 indicadores diferentes, incluindo hash, alterações de registro, alterações de arquivo e conexões de rede.

BUSCA DE AMEAÇAS

Utilize a poderosa busca baseada em IoC e aplique filtros aos dados brutos para classificação com base na popularidade do arquivo, reputação, assinatura digital, comportamento ou outras informações contextuais. A configuração de diversos filtros permite uma busca fácil e automatizada de ameaças e resposta a incidentes, incluindo a capacidade de detectar e interromper APTs e ataques direcionados.

ACESSO REMOTO SEGURO E TRANQUILO

A resposta a incidentes e os serviços de segurança são eficientes e de fácil acesso, tanto em termos da conexão do respondente de incidentes ao console, quanto da conexão com os endpoints. A conexão funciona em velocidade quase em tempo real, com medidas de segurança máximas aplicadas, tudo sem a necessidade de ferramentas de terceiros.

ISOLAMENTO EM UM CLIQUE

Defina políticas de acesso à rede para interromper movimentos laterais de malware de forma ágil. Isole um dispositivo comprometido da rede com apenas um clique na interface do ESET Inspect. Além disso, remova dispositivos do estado de contenção facilmente.

DETECÇÃO DE ANOMALIAS E COMPORTAMENTOS

Verifique as ações desempenhadas por um arquivo executável e utilize o sistema de reputação LiveGrid® da ESET para avaliar, de forma ágil, se os processos executados são seguros ou suspeitos. O monitoramento de incidentes anômalos relacionados ao usuário é possível devido a regras específicas elaboradas para o acionamento por comportamento, não apenas por detecções simples de malware ou baseadas em assinaturas. O agrupamento de dispositivos por usuário ou departamento permite às equipes de segurança identificarem se o usuário tem permissão para executar uma determinada ação.

CATEGORIZAÇÕES

Atribua e remova tags para filtragem rápida de objetos, como dispositivos, alarmes, exclusões, tarefas, executáveis, processos e scripts. As tags são compartilhadas entre os usuários e, após serem criadas, podem ser atribuídas imediatamente.

DETECÇÃO DE VIOLAÇÃO DE POLÍTICAS DA EMPRESA

Bloqueie a execução de módulos maliciosos em qualquer dispositivo da rede da sua organização. A arquitetura aberta do ESET Inspect oferece flexibilidade para detectar violações de políticas aplicadas ao uso de softwares específicos, como aplicativos de torrent, armazenamento em nuvem, navegação Tor ou outros softwares indesejados.

ARQUITETURA ABERTA E INTEGRAÇÕES

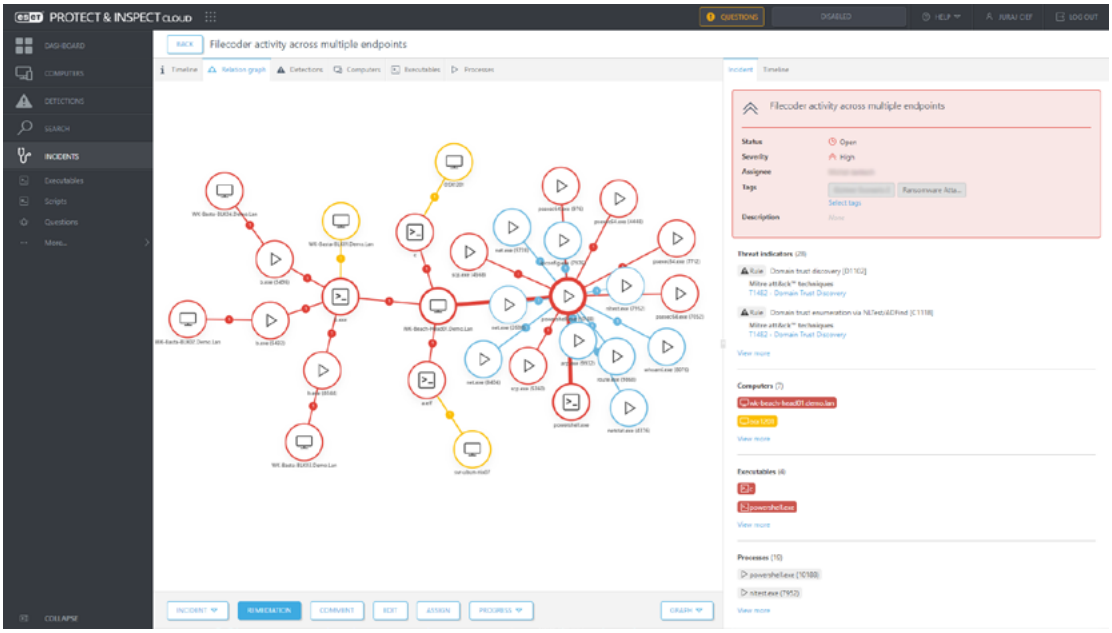
O ESET Inspect oferece uma detecção única baseada em comportamento e reputação, totalmente transparente para as equipes de segurança. Todas as regras são facilmente editáveis via XML, permitindo ajustes refinados, ou facilmente criadas para atender às necessidades de ambientes corporativos específicos, incluindo integrações do SIEM.

PONTUAÇÃO SOFISTICADA

Priorize a gravidade dos alarmes com uma funcionalidade de pontuação que atribui um valor de gravidade aos incidentes e permite aos administradores identificarem rapidamente os dispositivos com maior probabilidade de incidentes.

COLETA DE DADOS LOCAL

Visualize dados abrangentes sobre um módulo recém-executado, incluindo o horário de execução, o usuário que executou, o tempo de permanência e os dispositivos afetados. Todos os dados são armazenados de forma local para evitar o vazamento de dados confidenciais.



Casos de uso

Detecção de comportamento e infrações reincidentes

PROBLEMA

Em sua rede, há usuários que são reincidentes em termos de malware, esses mesmos usuários seguem sendo infectados repetidamente. Essa situação ocorre devido a comportamentos arriscados? Ou eles estão apenas sendo alvos com uma frequência maior em relação a outros usuários?

SOLUÇÃO

- ✓ Visualize facilmente usuários e dispositivos que apresentam problemas.
- ✓ Conclua rapidamente uma análise de causa raiz para encontrar a origem das infecções.
- ✓ Remedie os vetores de infecção encontrados, como e-mails, web ou dispositivos USB.

Busca e bloqueio de ameaças

PROBLEMA

Seu sistema de alerta antecipado ou centro de operações de segurança (SOC) emite um novo alerta de ameaça. Quais devem ser seus próximos passos?

SOLUÇÃO

- ✓ Utilize o sistema de alerta antecipado para obter dados sobre novas ou futuras ameaças.
- ✓ Faça uma busca da nova ameaça em todos os dispositivos.
- ✓ Procure por indicadores de comprometimento em todos os dispositivos, que evidenciem a existência da ameaça antes do alerta.
- ✓ Bloqueie a ameaça para impedir sua infiltração na rede ou execução dentro da organização.

Configuração e resposta fáceis — dispensa equipe de segurança

PROBLEMA

Nem todas as empresas contam com equipes de segurança dedicadas, por isso, introduzir e implementar regras de detecção avançada pode ser um desafio.

SOLUÇÃO

- ✓ Mais de 300 regras pré-configuradas integradas.
- ✓ Responda facilmente, com apenas um clique, para bloquear, encerrar ou isolar dispositivos.
- ✓ Ações de remediação propostas e próximos passos estão integrados aos alertas.
- ✓ As regras são editáveis por meio da linguagem XML para facilitar ajustes refinados ou a criação de novas regras.

Visibilidade da rede

PROBLEMA

Algumas empresas estão preocupadas com os aplicativos executados pelos usuários em seus sistemas. É necessário se preocupar não apenas com aplicativos instalados tradicionalmente, mas também com aplicativos portáteis que não são realmente instalados. Como manter o controle sobre os aplicativos?

SOLUÇÃO

- ✓ Visualize e filtre facilmente todos os aplicativos instalados, em todos os dispositivos.
- ✓ Visualize e filtre todos os scripts nos dispositivos.
- ✓ Bloqueie facilmente a execução de scripts ou aplicativos não autorizados.
- ✓ Realize a remediação notificando os usuários sobre aplicativos não autorizados e os desinstale automaticamente.

Detecção aprofundada de ameaças — ransomwares

PROBLEMA

Uma empresa busca ferramentas adicionais para detecção proativa de ransomwares, além de receber notificações imediatas caso comportamentos semelhantes a ransomwares sejam observados na rede.

SOLUÇÃO

- ✓ Defina regras para detectar aplicativos executados por meio de pastas temporárias.
- ✓ Defina regras para identificar arquivos do Office (Word, Excel, PowerPoint) que executem scripts ou executáveis adicionais.
- ✓ Receba alertas quando forem encontradas alguma das extensões mais comuns de ransomwares em um dispositivo.
- ✓ Visualize alertas do escudo anti-ransomwares das soluções de segurança de endpoint da ESET no mesmo console.

Investigação e remediação conscientes do contexto

PROBLEMA

A precisão dos dados depende do contexto. Para decisões eficazes, é essencial compreender quais são os alertas, em quais dispositivos estão ocorrendo e quais usuários estão provocando esses alertas.

SOLUÇÃO

- ✓ Identifique e classifique todos os dispositivos de acordo com o Active Directory, agrupamentos automáticos ou manuais.
- ✓ Permita ou bloqueie aplicativos ou scripts com base no agrupamento de dispositivos.
- ✓ Permita ou bloqueie aplicativos ou scripts com base no usuário.
- ✓ Receba notificações apenas para determinados grupos.

ESET Digital Security
Progress. Protected.

Sobre a ESET

Cibersegurança de última geração para empresas

NÃO APENAS INTERROMPEMOS VIOLAÇÕES, NÓS AS IMPEDIMOS DE OCORRER.

Diferente 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 para 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

ALGUNS DE NOSSOS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegida pela ESET desde 2017, mais de 9 mil endpoints.

Allianz Suisse

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

Canon
Canon Marketing Japan Group

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

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

RECONOCIMIENTOS

AV comparatives APPROVED Business Security JUL 2023

A ESET recebeu o prêmio Business Security APPROVED da AV-Comparatives no Business Security Test, em julho de 2023.

Leader SUMMER 2023

A ESET alcança, de forma consistente, as melhores classificações na plataforma global de análise de usuários G2, tendo suas soluções apreciadas por clientes em todo o mundo.

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

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