VISÃO GERAL DO PRODUTO

THREAT HUNTING

Investigação de ameaças sob demanda, análise da causa raiz e conselhos de correção sem a necessidade de recursos internos extras

ESET CYBERSOC

O serviço ESET Threat Hunting ajuda os clientes a investigar um dado conjunto de dados ,eventos e alarmes gerados pela solução de resposta e detecção endpoint da ESET —ESET Enterprise Inspector.

Por que o serviço Threat Hunting de ESET?

> OBTENHA O MÁXIMO DO EDR DA ESET

O ESET Enterprise Inspector é uma ferramenta EDR sofisticada para identificação de comportamento e violações anômalas, avaliação de risco, resposta a incidentes, investigação e correção.

Ele monitora e avalia todas as atividades acontecendo na rede em tempo real e permite que as organizações tomem ações imediatas se necessário.

O ESET Enterprise Inspector é um pré-requisito para o serviço ESET Threat Hunting.

> FALTA DE CONHECIMENTO DO PRODUTO

Usar novos produtos sem qualquer conhecimento prévio pode se tornar complicado, até para organizações com equipes de TI ou segurança dedicadas. Além disso, acompanhar o cenário de ciberameaças que muda muito rapidamente pode ser desafiador e, algumas vezes, pode ser melhor deixar isso para especialistas.

> FALTA DE MÃO-DE-OBRA

Ajuda os administradores de TI e equipes de segurança a priorizar sua carga de trabalho ao apontar apenas os eventos importantes. Além disso, uma organização pode levar meses para contratar e treinar uma equipe para implementar e monitorar uma plataforma de resposta e detecção de endpoint.

> FIQUE TRANQUILO

Se quaisquer anomalias ou violações forem identificadas, nossos especialistas podem encontrar rapidamente a causa raiz e corrigir os problemas que foram encontrados definitivamente.

> CUSTOS EM LONGO PRAZO

Criar equipes dedicadas e/ou contratar especialistas para realizar tarefas ocasionais de nicho pode incorrer em altos custos de longo prazo. Adquirir serviços e produtos de um único fornecedor reduz a complexidade para os departamentos de contabilidade—especialmente para corporações multinacionais que de outra forma teriam um grande número de fornecedores regionais.

Detalhes técnicos do serviço ESET Threat Hunting

> SOB DEMANDA

As organizações contatam os operadores do ESET Threat Hunting quando precisarem dos serviços.

> ANÁLISE DA CAUSA RAIZ

Os operadores de Threat Hunting analisam alarmes destacados para determinar sua causa raiz.

> CONSELHOS ÚTEIS

Os operadores revisam alarmes e reúnem suas descobertas em um relatório de status abrangente além de fornecer conselhos úteis para a organização.

> BASEADO EM ASSINATURA

As organizações adquirem serviços de Threat Hunting em períodos de tempo personalizáveis durante o qual os especialistas da ESET estão prontos para investigar ameaças quando for mais necessário.

> DADOS NO LOCAL

Todos os dados da organização e das ameaças continuam a ficar no local pela configuração de uma conexão VPN segura entre a organização e a ESET.

> AVALIAÇÃO INICIAL

Uma avaliação inicial detalhada é realizada para avaliar as políticas específicas de segurança da organização além de desenvolver um perfil interno.

As fases

Avaliação inicial

- Cada serviço começa com uma avaliação inicial não apenas do ambiente do cliente, mas da composição da organização e atitude de cibersegurança geral.
- Uma entrevista completa é realizada com membros relevantes da equipe organizacional para coletar todas as informações necessárias.
- O resultado desta fase é um Perfil de Segurança Organizacional que pode ser consultado futuramente por qualquer operador de Threat Hunting que precise de detalhes relacionados à organização para fazer a avaliação correta.
- Recomenda-se às organizações que contatem a ESET com quaisquer mudanças no ambiente devido à natureza sob demanda do serviço de Threat Hunting.

Operação regular

- Quanto solicitado, os especialistas de segurança da ESET começam a investigação dos eventos apontados para determinar a causa raiz e fornecem conselhos úteis personalizados para a organização específica.
- As descobertas de cada investigação são reunidas em relatórios de status abrangentes que expressam detalhes técnicos em linguagem compreensível para humanos.

ESET EM NÚMEROS

+110 Milhões de usuários no mundo

+ 400 Mil clientes corporativos

+200 países e territórios

13 centros de investigação e desenvolvimento