VISÃO GERAL DO PRODUTO

THREAT MONITORING

Seja contatado proativamente pelos especialistas da ESET sempre que uma anomalia de segurança ou possível violação for detectada em tempo real

ESET CYBERSOC

O serviço ESET Threat Monitoring ajuda os clientes a navegar pela grande quantidade de dados reunidos, eventos e alarmes gerados pela solução de detecção e resposta de endpoint da ESET —ESET Enterprise Inspector—e aproveita o potencial completo da ferramenta sem ter que mudar suas prioridades de TI existentes.

Por que o serviço Threat Monitoring da ESET é necessário?

> 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 Monitoring.

> 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

As organizações podem ficar tranquilas sabendo que especialistas em segurança estão monitorando seu ambiente diariamente em busca de anomalias ou violações potenciais. Se algo for identificado, as organizações serão contatadas proativamente para que possam corrigir rapidamente os problemas encontrados.

> CUSTOS A 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 traz tranquilidade aos departamentos de contabilidade, especialmente para corporações multinacionais.

Detalhes técnicos do serviço Threat Monitoring da ESET

> MONITORAMENTO DIÁRIO

A console de gerência da organização será verificada por um operador da ESET ao menos uma vez a cada 24 horas em dias úteis regulares.

> RELATÓRIO COMPILADO

Os operadores de Threat Monitoring reúnem suas descobertas em relatórios de status claros e compreensíveis e se comunicam com o contato da organização para alertá-los sobre quaisquer eventos críticos que justifiquem atenção imediata.

> AJUSTES CONTÍNUOS

Após a criação de um relatório, os operadores de monitoramento de ameaças criam novas regras e/ou exclusões além de recomendações de como proceder em caso de uma ameaça real.

> DADOS NO LOCAL

Todos os dados da organização e 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.

Se quaisquer anomalias ou violações potenciais forem identificadas, as organizações serão contatadas proativamente para que possam corrigir rapidamente os problemas encontrados.

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 Monitoring que solicite detalhes relacionados à organização para fazer avaliações corretas.

Operação regular

- Os operadores do ESET Threat Monitoring fazem login diariamente para verificar eventos e alarmes, e subsequentemente ajustar as regras internas e configurações conforme necessário.
- As descobertas de cada investigação são reunidas em relatórios de status abrangentes que expressam detalhes técnicos em linguagem compreensível por humanos.
- As organizações são contatadas para alerta de quaisquer eventos críticos que justifiquem atenção imediata. .

Otimização

- Esta fase começa após alguns poucos dias consecutivos da execução do EDR da ESET—ESET Enterprise Inspector—no ambiente ao vivo da organização.
- Durante esta fase, os operadores revisam os alarmes gerados e regras que os dispararam.
- Levando em consideração o ambiente da organização e avaliação inicial, exclusões são criadas para todos os falsos positivos e eventos que são inofensivos.

ESET EM NÚMEROS

+110 Milhões de usuários en el mundo

+ 400 Mil clientes corporativos

+200 países e territórios

13 centros de investigação e desenvolvimento