FOLHA DE DADOS

Malwarebytes | minitel NEXT

MALWAREBYTES INCIDENT RESPONSE

O padrão de confiança em matéria de remediação de terminais automatizada

Quando ocorre um ciberataque, a rapidez é um dos fatores mais críticos no processo de remediação. As equipas de segurança preparadas para ciberataques deverão ter como objetivo erradicar ameaças do ambiente em menos de uma hora para combaterem eficazmente ciberameaças sofisticadas e evitarem os danos que uma violação bem sucedida pode infligir na reputação de uma organização e nos seus resultados.

Contudo, as empresas enfrentam o aumento da complexidade e a fuga de recursos do centro de operações de segurança (SOC) da gestão manual da remediação para locais distribuídos e uma equipa dispersa. Isto dá origem a tempos de resposta longos, que expõem a empresa a um risco considerável.

Investir numa solução que automatiza a remediação de terminais acelera significativamente os tempos de resposta e melhora as práticas de segurança no seu SOC.

VISÃO GERAL DO PRODUTO

O Malwarebytes Incident Response (IR) é um padrão de confiança em matéria de remediação de terminais automatizada que reforça a ciberresiliência empresarial através da redução dos seus tempos de reposta com uma remediação rápida e completa. Com a nossa abordagem automatizada, o Malwarebytes IR proporciona uma maior eficiência operacional que poupa tempo aos recursos de análise, preserva a produtividade do utilizador e melhora a sua postura de segurança empresarial.

As nossas opções de implementação flexíveis com a escolha de um agente persistente ou não persistente possibilitam-lhe uma implementação de acordo com a sua estratégia de terminais, e o API da solução fornece oportunidades de integração no seu stack de segurança, com vista ao reforço da automatização e à orquestração dos seus processos de segurança.

Com o Malwarebytes IR, a sua empresa obtém uma remediação eficaz e minuciosa de terminais à medida que os ataques ocorrem, e a nossa tecnologia de remediação patenteada remove artefactos dinâmicos e relacionados para garantir a desinfeção.

PRINCIPAIS VANTAGENS

Reduza os tempos de resposta

Obtenha o padrão de segurança em matéria de remediação de terminais automatizada, que lhe permite erradicar adversários com tempo de resposta reduzido e remediação completa.

Garanta maior eficiência operacional

Melhore as práticas no seu SOC com uma solução que acelera as operações de segurança, poupa tempo aos recursos de análise de segurança e preserva a produtividade do utilizador.

Implemente da forma que pretender

Com a escolha de um agente persistente ou não persistente, as nossas opções flexíveis possibilitam-lhe uma implementação de acordo com a sua estratégia de terminais.

Automatize a orquestração

O nosso API fornece oportunidades de integração dos seus investimentos em segurança com vista ao reforço da automação e à orquestração dos seus processos de segurança.

> O Malwarebytes é uma grande ajuda na automatização da resposta a ataques. A preparação transforma-se em retorno sobre o investimento. Seja ao reduzir o número de sistemas com imagem recriada ou ao fornecer preciosas informações para evitar uma violação, o Malwarebytes faz uma grande diferença no nosso retorno sobre o investimento em segurança.
>
> Bob Chadwick, Senior SOC Manager
> Analog Devices

CAPACIDADES

Resposta de terminais automatizada que reduz os tempos de resposta
A nossa abordagem automatizada permite aos seus analistas de segurança eliminar esforços manuais de remediar ataques, libertando o precioso tempo dos recursos, para que os seus analistas possam focar-se em iniciativas que gerem receitas. As tarefas automatizadas decorrem em menos tempo e com maior precisão e reduzem o seu tempo de resposta.

Uma remediação minuciosa que erradica o adversário
A maioria das soluções apenas remedeia componentes de malware ativos, o que não constitui uma remediação completa. O Malwarebytes Linking Engine aplica uma abordagem patenteada que também deteta e remove artefactos dinâmicos e relacionados. O nosso motor aplica a sequenciação associada para garantir a desinfeção de mecanismos de persistência de malware.

Agente persistente ou não persistente: implemente da forma que pretender
O Malwarebytes oferece opções flexíveis de implementação de uma forma adequada a si: escolha um agente persistente ou não persistente no terminal. As duas abordagens integram-se facilmente com a sua ferramenta de implementação para que seja transparente para o utilizador final.

A gestão em nuvem simplifica a resposta em locais dispersos
Gerido na nuvem, o Malwarebytes IR facilita a gestão das ações de resposta nos seus locais distribuídos e com uma equipa dispersa. Os painéis centralizados desta solução apresentam um único painel de vidro que permite que os seus analistas de segurança compreendam rapidamente a sua pegada de respostas a ataques e o estado da remediação.

Profunda inteligência sobre ameaças, que proporciona uma resposta de terminais eficaz
A nossa experiência em ciberinteligência na remediação significa que temos um profundo conhecimento dos ataques que se executam com sucesso em dispositivos empresariais. Isto proporciona à sua empresa uma solução baseada na inteligência em deteção e remediação de ameaças de milhões terminais com proteção Malwarebytes, tanto de empresas, como de consumidores.

Adapta-se às necessidades da maior empresa
Com a nossa solução em nuvem, não precisa adquirir ou gerir qualquer equipamento, e o Malwarebytes IR adapta-se para lidar prontamente com as necessidades de resposta a incidentes da sua empresa.

ORQUESTRE A AUTOMAÇÃO DOS SEUS INVESTIMENTOS EM SEGURANÇA

O Malwarebytes API fornece oportunidades de integração no seu stack de segurança, como o seu SIEM, SOAR e ITSM, com vista ao reforço da automatização e à orquestração dos seus processos de segurança. Isto proporciona uma ciberresiliência empresarial que é ágil, com ações mais rápidas que protegem e respondem a ataques à medida que ocorrem.

Security Orchestration, Automation and Response (SOAR)

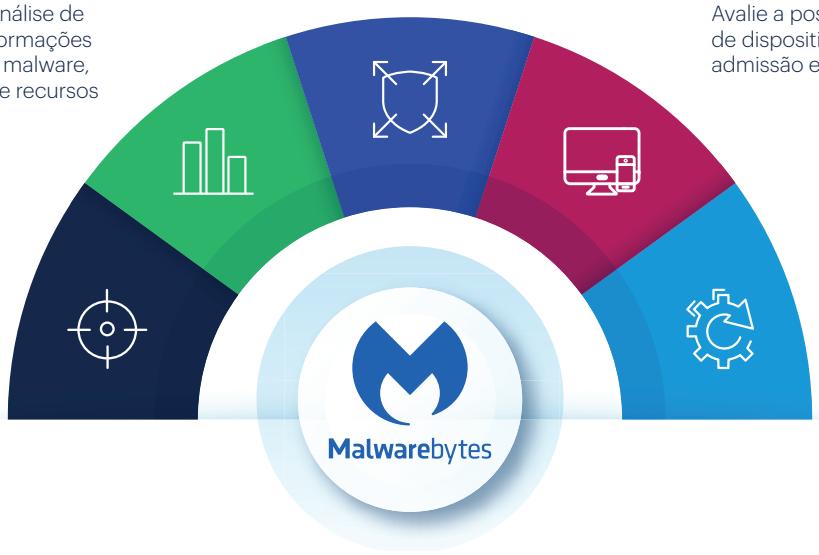
Automatize a resposta a uma possível ameaça, iniciando uma remediação Malwarebytes automatizada

Security Incident and Event Management (SIEM)

Enriqueça a sua análise de ameaças com informações específicas sobre malware, informações sobre recursos e tendências

Network Access Control (NAC)

Avalie a postura de segurança de dispositivos antes da admissão em rede



Unified Endpoint Management (UEM)

Planeie e gira a implementação nos seus terminais

Information Technology Service Management (ITSM)

Automatize os fluxos de trabalho e monitorize o progresso do incidente à remediação

Resposta a incidentes

Integrações API