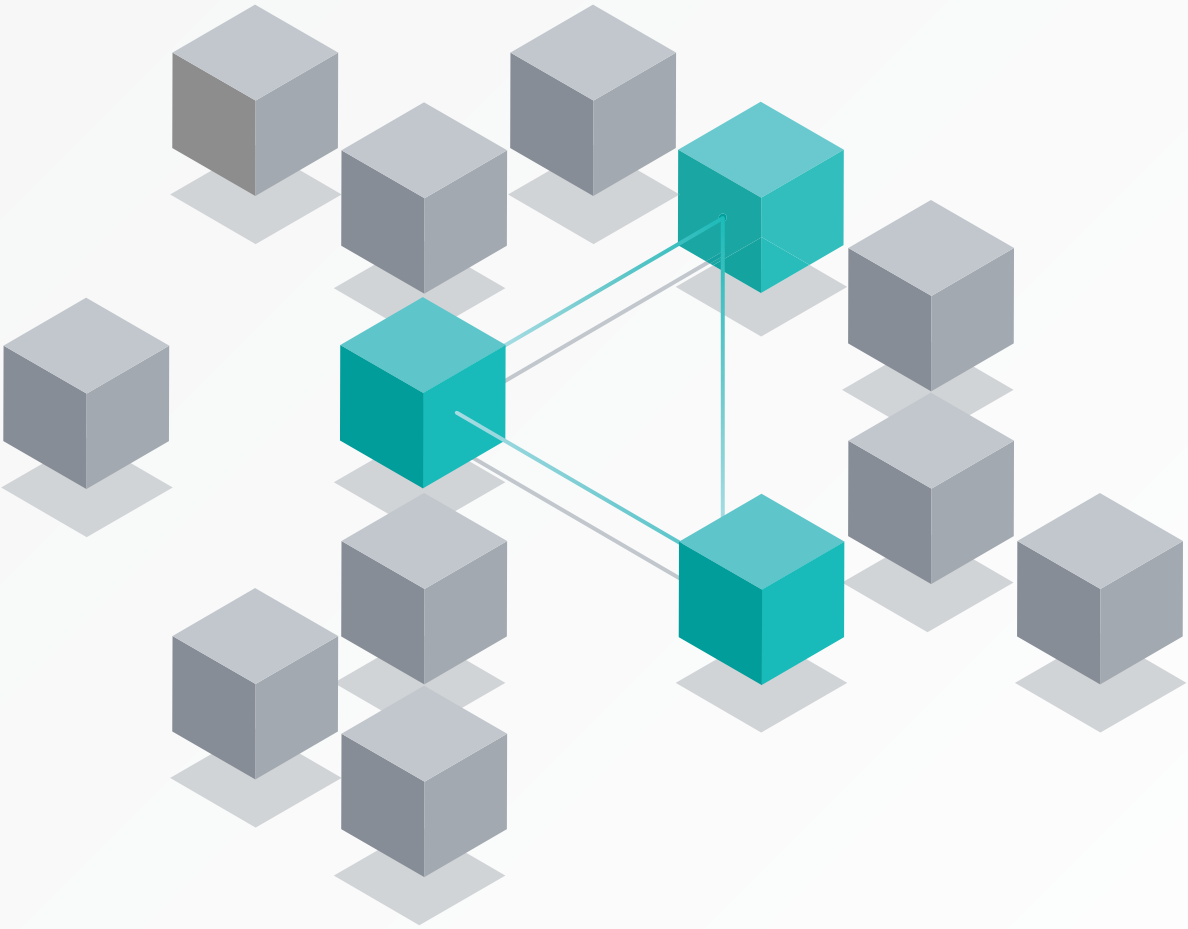
IBM Security QRadar EDR

Segurança de terminal automatizado e impulsionado por IA



O IBM Security QRadar oferece uma abordagem única e inovadora para a segurança de terminal.

A solução utiliza níveis excepcionais de automação inteligente, aproveitando a IA e o aprendizado de máquina para ajudar a detectar e corrigir ameaças sofisticadas, conhecidas e desconhecidas, em tempo quase real. Com visibilidade detalhada de todos os terminais, a solução combina recursos previsíveis, como mapeamento MITRE ATT&CK e visualizações de ataque, com IA e automação de duplo mecanismo para levar a segurança de terminal em um ambiente zero trust.

Por que o QRadar EDR?

1

Aprende continuamente à medida que a IA detecta e responde de forma autônoma, quase em tempo real, a ameaças novas e desconhecidas

2

Ajuda a proteger as infraestruturas off-line, bem como ambientes locais e na nuvem

3

Mapeia as ameaças à estrutura MITRE ATT&CK e utiliza uma árvore comportamental para facilitar análises e visualizações

4

Oferece uma API bidirecional que se integra a muitas ferramentas populares de gerenciamento de eventos e informações de segurança (SIEM) e de orquestração, automação e resposta de segurança (SOAR)

5

Fornece técnicas heurísticas, de assinatura e comportamentais em sua defesa multicamadas

6

Permite que os usuários construam estratégias de detecção personalizadas para atender a requisitos de conformidade ou específicos da empresa sem a necessidade de reinicializar o terminal

7

Simplifica e acelera a resposta por meio de remediação guiada ou autônoma

8

Oferece detecção e busca de ameaças automáticas impulsionadas por IA, incluindo telemetria a partir de indicadores que podem ser personalizados para detecção proprietária e busca granular

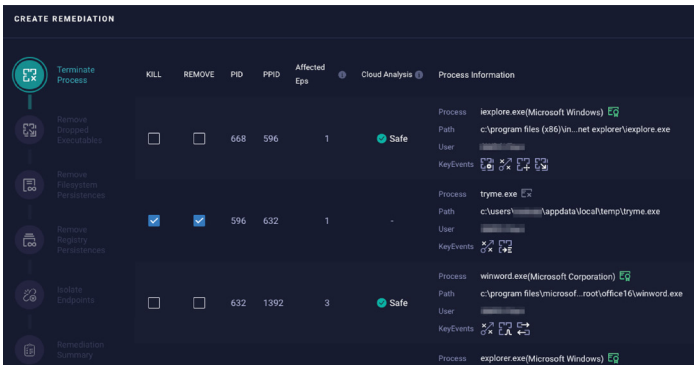
9

Disponibiliza a remediação com eliminação remota automatizada ou com um único clique

10

Proporciona uma visibilidade detalhada com NanoOS, uma abordagem exclusiva baseada em hypervisor que opera fora do sistema operacional e é projetada para ser invisível a invasores e malware

A árvore comportamental QRadar EDR fornece visibilidade total de alertas e ataques.



A automação corretiva do QRadar EDR simplifica a correção de incidentes com opções de clique.

Detecção e resposta de terminal (EDR) autônomas e impulsionadas por IA

- Utiliza IA e aprendizado de máquina com autoaprendizado contínuo para construir um padrão de referência dinâmico que protege os terminais de ameaças sem a necessidade de atualizações diárias
- Prepara sua organização para o futuro com prevenção autônoma de ransomware, ataques sem arquivos e em memória, tanto on-line quanto off-line
- Preenche as lacunas deixadas por soluções de antivírus (AV) tradicionais com maior detecção, visibilidade e controle

Alta resolução de ameaças

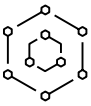
- Aumenta sua compreensão das ameaças em seu ambiente mapeado contra táticas e técnicas na estrutura do MITRE ATT&CK
- Ajuda a reduzir o tempo de investigação de minutos para segundos com inteligência de ameaças e classificação de análises
- Utiliza o monitoramento de prevalência para eliminar as suposições necessárias para compreender o impacto e a disseminação de artefatos infectados em toda a sua organização

Recursos completos de busca e resposta

- Fornece uma plataforma de busca de ameaças fácil e simples de usar com parâmetros de busca pré-configurados que não requerem conhecimento de consulta a bancos de dados
- Oferece orientação de remediação completa e automações de resposta por clique para ajudá-lo a conter qualquer situação em segundos

Monitoramento de conformidade

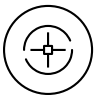
- Oferece total visibilidade do comportamento do usuário e do uso dos aplicativos para melhorar as políticas de conformidade de sua organização e fazer cumprir as normas
- Permite que os usuários elaborem estratégias de detecção personalizadas para atender a conformidade ou requisitos específicos da empresa usando o script DeStra (Estratégia de Detecção), sem a necessidade de reinicializar o terminal
- Permite que os usuários ativem atualizações em toda a organização sem intervenção ou tempo de inatividade do terminal



Automação corporativa

– Ajuda você a implementar rapidamente novas automações e funcionalidades em seus fluxos de trabalho existentes usando a API e integrações do QRadar EDR

– Integra-se com ferramentas SIEM e SOAR



Detecção e resposta gerenciadas (MDR)

– Fornece monitoramento, rastreamento e resolução de alertas críticos 24x7, mantendo você informado

– Ajuda a identificar e rastrear até mesmo os agentes mais sofisticados e a realizar campanhas avançadas de busca de ameaças usando tanto a IA como a profunda experiência em inteligência e análise da nossa equipe

– Contém e corrige as ameaças assim que elas são detectadas, minimizando os riscos de negócios e reduzindo os danos e a interrupção dos serviços

Implementação em qualquer ambiente

– Fornece opções para infraestruturas na nuvem e no local e funciona em ambientes off-line, sem a necessidade de atualizações diárias de assinaturas

– Instalado em segundos sem integrações complexas, torna-se operacional em minutos e coexiste perfeitamente com o software AV existente sem conflitos

– Não impacta o terminal durante a implementação, nas operações diárias e mesmo depois de responder a um incidente em tempo real

Veja mais informações em:
Para saber mais sobre o QRadar EDR, entre em contato com seu representante da IBM, seu Parceiro de Negócios IBM ou visite ibm.com/br-pt/products/qradar-edr

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP

Produzido nos Estados Unidos da América
Maio de 2023