IBM QRadar

Perceba e detecte ameaças modernas com a mais sofisticada plataforma de análise de dados de segurança

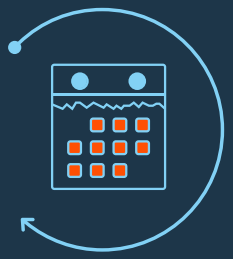
Conheça nosso site

Fale com especialista

White paper da IBM sobre segurança

Conquiste o desconhecido

Os profissionais de segurança vivem em um mundo de constantes incertezas. As ameaças e os ataques atingem as organizações por todos os ângulos, a cada minuto do dia.
Quando um invasor consegue obter acesso, ele se move lentamente e em silêncio. Ele busca dados valiosos e cobre suas pegadas. Na verdade, um estudo recente constatou que o tempo médio para identificar um ataque era de 156 dias e o tempo médio para contê-lo era de 82 dias. Como consequência, a vida em um centro de operações de segurança (SOC) é muito estressante e muitas equipes simplesmente ignoram aquilo o que não querem saber.



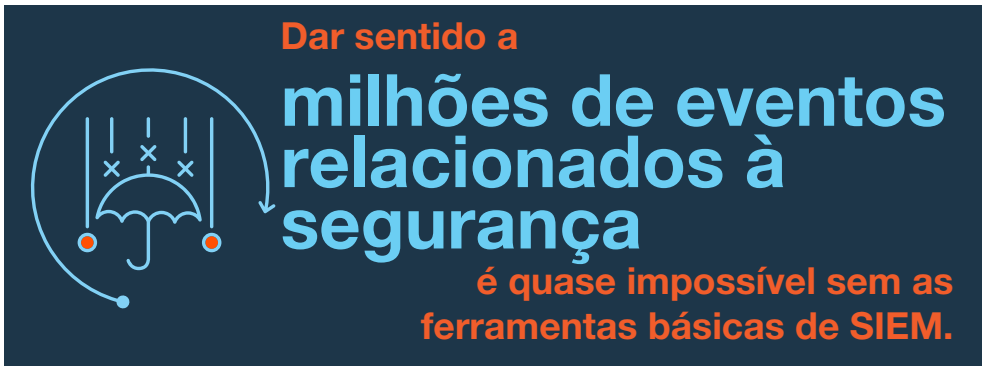
Os invasores podem estar à espreita em uma organização de 8 a 9 meses antes que sejam descobertos.[1]

Foi-se o tempo em que a tarefa das equipes de segurança se limitava a proteger o perímetro, bloquear as diferentes formas de acesso à internet e apagar os últimos "incêndios". Hoje em dia, as organizações exigem uma conectividade mais onipresente para manter a empresa em funcionamento e, ao mesmo tempo, deter ameaças avançadas e identificar fraudes e riscos internos, tudo isso garantindo que as normas sejam constantemente respeitadas. Os novos requisitos exigem a análise do maior número possível de informações para detectar atividades ameaçadoras ocultas sob a superfície e dar uma resposta mais rápida. Os analistas do SOC devem aperfeiçoar sua capacidade de detectar desvios da atividade normal e as soluções escolhidas por eles devem poder ser escaladas até o último nível da empresa com uma mesma plataforma coesa.

"2015 Cost of a Data Breach Study: Global Analysis" (Estudo sobre o custo do vazamento de dados: Análise global), Ponemon Institute Research Report, maio de 2015.

Detecte ameaças e tome uma ação

Para se manter à frente, as organizações devem ser capazes de "perceber" cadeias de atividades maliciosas da mesma forma que as pessoas percebem uma situação de perigo ao ver, ouvir, cheirar ou sentir um ambiente conflitante. Elas precisam de uma plataforma de segurança que seja capaz de:

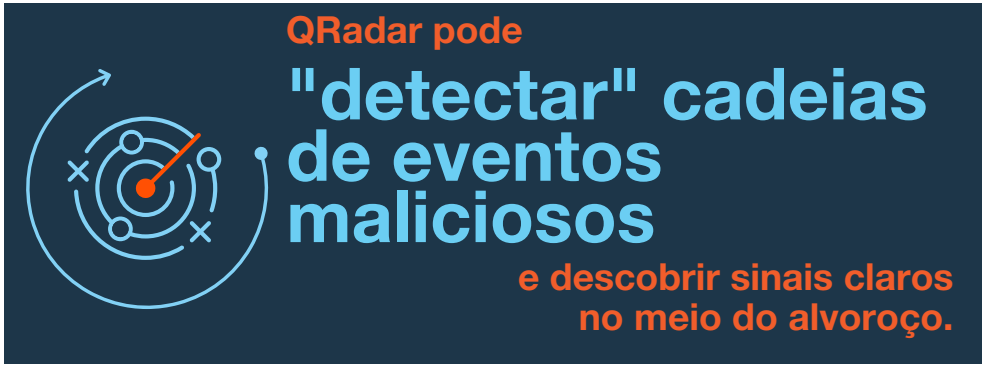


- Ser implantada rapidamente em toda a rede, incluindo os recursos localizados na nuvem
- Detectar diferenças sutis no ambiente, como possíveis intrusos ou infiltrados
- Descobrir ataques sem depender de um número limitado de pessoas com formação muito especializada
- Coletar, padronizar e correlacionar bilhões de eventos, dando prioridade a um pequeno número de questões
- Identificar as principais vulnerabilidades e os principais riscos para evitar invasões

O aspecto positivo disso é que os analistas do SOC de hoje em dia não estão sozinhos. Do mesmo modo que os invasores se juntaram para compartilhar conhecimento e técnicas, a comunidade de segurança respondeu compartilhando seus recursos. O surgimento dessa nova inteligência sobre ameaças e de recursos para compartilhar aplicativos contribui para limitar a eficácia dos novos malwares e kits de exploração, bem como o impacto das vulnerabilidades do dia zero e dia um. No entanto, muitos analistas do SOC continuam limitados por sistemas antiquados de gestão de registros ou por soluções básicas de informações de segurança e gestão de eventos (SIEM) que geram um número excessivo de alertas usando uma única instância de comportamento suspeito.

Uso de análise de dados para eliminar ameaças

As violações mais graves à segurança não começam com uma grande explosão. Pelo contrário. Os criminosos cibernéticos lançam ataques "lentos e de baixa intensidade" que podem se prolongar durante meses. Não seria incrível poder identificar mudanças no ambiente sutis e relacionadas entre si e alertar as equipes de segurança quando coisas estranhas começassem a aparecer?



IBM® QRadar® Security Intelligence Platform é a única solução de segurança alimentada pelo IBM Sense Analytics e que pode:

- Desenvolver perfis de usuários e recursos de acordo com atividades legítimas de base
- Detectar condutas anormais em pessoas (equipe interna, colaboradores, clientes, convidados), redes, aplicativos e dados
- Relacionar as atividades suspeitas atuais e passadas para aumentar a precisão dos incidentes identificados
- Recuperar e reproduzir a atividade da rede e investigar o conteúdo dos pacotes em seu formato original
- Descobrir e priorizar pontos fracos antes que sejam explorados

Os produtos isolados que realizam a análise de um momento determinado são pouco confiáveis. Eles não são capazes de associar a nova atividade na rede com os usuários "de risco", que podem ser aqueles que visitaram sites de má reputação no passado. O Sense Analytics contribui para eliminar ameaças relacionando os comportamentos dos usuários a eventos registrados, fluxos da rede, inteligência sobre ameaças, vulnerabilidades e o contexto empresarial. Ele permite que as organizações se concentrem nas ameaças mais imediatas e perigosas, buscando indícios claros no meio do alvoroço. Além disso, ele as orienta em seus esforços de remediação para minimizar possíveis danos.

Como funciona o Sense Analytics?

Sem dados, a análise de dados torna-se inútil. Sem muitos dados, ela é simplesmente insuficiente. Alguns desses dados provêm de sua rede, enquanto outros estão armazenados em aplicativos, alguns derivam de análises anteriores e outros, ainda, provêm de uma fonte externa. O QRadar coleta dados brutos de segurança de todos os dispositivos, aplicativos e usuários da rede, tanto nas instalações da organização como aqueles armazenados em um ambiente de nuvem.

O Sense Analytics pode:

- Analisar dados de cargas de trabalho
- Compreender o contexto
- Criar perfis de uso

Depois da coleta dos dados, os appliances do QRadar realizam análises em tempo real para buscar sinais imediatos de risco e, posteriormente, complementam os resultados com outros dados de inteligência armazenados sobre a rede, o usuário ou metadados de arquivos. O QRadar permite que as equipes de segurança compreendam de que maneira as atividades atuais estão relacionadas com o que aconteceu no passado, e um elemento fundamental para detectar a mudança é poder contar com os parâmetros adequados para a atividade de base.

Analisar dados de segurança para detectar ameaças

QRadar com Sense Analytics utiliza análise avançada com base em estados para transformar os dados de segurança atuais em informações úteis e significativas. As equipes de segurança podem definir diversos tipos de condições que as ajudem a detectar atividades potencialmente maliciosas, como:

Utilizando o QRadar, uma empresa internacional do setor elétrico pode analisar

2 milhões de eventos diários,

correlacionando dados em tempo real para identificar os 20-25 ataques em potencial que apresentam maior risco.

- Mudanças de conduta para detectar desvios dos padrões regulares

- Anomalias que podem indicar um novo tráfego na rede ou um tráfego que para repentinamente

- Violações de limites para descobrir ocorrências de uma atividade que superam um determinado nível

Uma mudança no comportamento normal dos usuários ou de identidades costuma ser um dos primeiros sinais de que a rede foi violada e de que talvez as credenciais de alguma pessoa tenham sido comprometidas. O Sense Analytics não apenas compara a atividade em tempo real com padrões históricos, mas também detecta novos usos dos aplicativos, novas visitas ao site e novas atividades de transferência de arquivos. Ele também pode ajudar a descartar falsos positivos usando dados de sistemas de identidades da organização, permitindo que os analistas do SOC vejam relatórios recentes das mudanças de cargo de pessoas concretas.

Compreender o contexto analisando os eventos correspondentes a fluxos e pacotes

Uma fonte de contexto extremamente eficaz e que costuma ser ignorada são os dados nativos do fluxo da rede (aqueles que identificam os endereços IP, portas, protocolos e inclusive aplicativos ou conteúdo de "carga útil" que transitam pela rede) captados por meio de inspeções Deep Packet imediatas ou a recuperação de pacotes completos posteriormente ao incidente. Isso possibilita que as equipes de segurança:

Utilizando o QRadar, uma importante empresa de serviços de saúde detectou que dados de pacientes estavam sendo transmitidos para fora da empresa sem criptografia. Graças à rápida detecção, o risco foi corrigido sem demora e eles conseguiram evitar possíveis sanções.

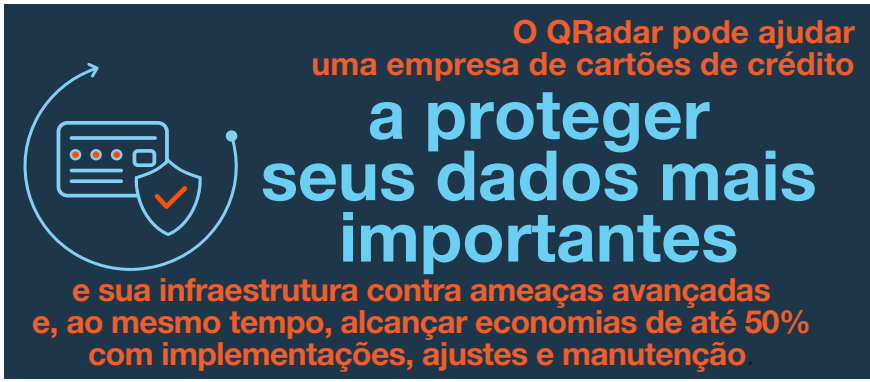
- Criem perfis do tráfego de rede "normal" e obtenham alertas ao mudar as condições
- Encontrem hosts novos ou comprometidos que se comuniquem com IPs maliciosos
- Detectem novas ameaças à segurança sem usar assinaturas
- Reproduzam passo a passo as ações de um invasor ou usuário malicioso detectado
- Obtenham visibilidade da camada do aplicativo e detectem conteúdo suspeito ou usos inadequados

O Sense Analytics usa dados da rede para proporcionar contexto para cada evento, incidente ou ataque correlacionado. Ele pode detectar se um servidor web deixou de responder a comunicações, identificar uma mudança importante no nível da atividade dos serviços que costumam ser usados e gerar alertas se surgirem novos serviços ou protocolos na rede. Essa análise também revela tipos de aplicativos e identifica falhas entre portas e protocolos, o que pode contribuir para acelerar as investigações.

Criar perfis de uso para armazenar informações úteis e contribuir com a gestão de riscos

Uma solução de segurança criada para buscar rapidamente entre os dados em tempo real deixará de perceber muitos incidentes que exigem um conhecimento prévio dos principais aplicativos, das pessoas que os usam, de seus níveis de desempenho típicos, de seus hosts associados e de como passam por períodos de maior e menor atividade.

O conhecimento desses parâmetros é crucial para obter dados de inteligência usados para agir.

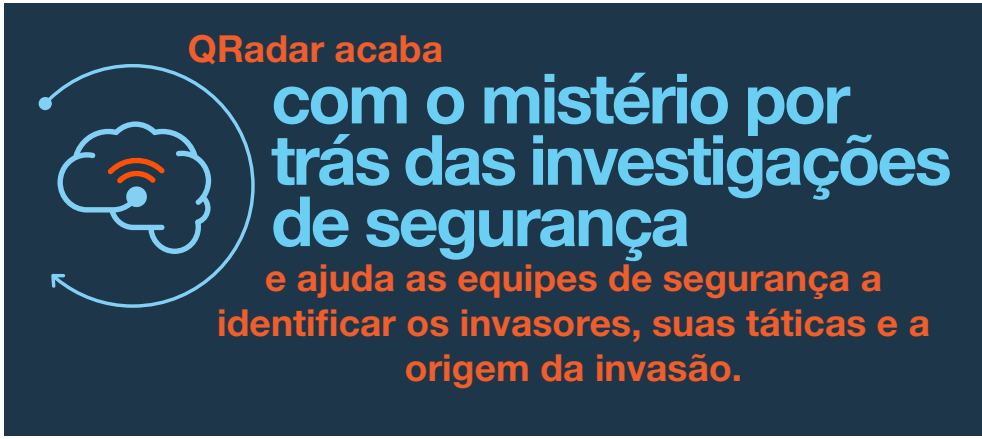


A possibilidade de armazenar conhecimento por meio de perfis de recursos e pessoas é uma das características na qual o Sense Analytics se baseia. O QRadar descobre recursos automaticamente e cria perfis de recursos usando dados de fluxo da rede e detecção de vulnerabilidades. Os perfis definem o que é cada recurso, identificam como ele se comunica com outros recursos, criam uma lista de aplicativos autorizados e indicam a presença de vulnerabilidades conhecidas. Em seguida, o QRadar usa todo esse contexto para reduzir as interferências e apresentar os incidentes com grande precisão.

Igualmente importante para a detecção de ataques e violações é a criação de informações sobre o que os usuários da rede estão fazendo. O QRadar pode rastrear endereços IP e MAC, identidades de e-mail e nomes de usuários de chat, por exemplo, e pode usar outros programas de gestão de identidades e acesso da IBM ou de terceiros para oferecer um contexto valioso para as investigações de incidentes. Ele pode usar todas essas associações para qualificar o âmbito da análise de dados e incluir ou excluir pessoas ou identidades associadas a atividades suspeitas que estejam acontecendo no momento ou que tenham sido observadas no passado.

Explore casos de uso que demonstram a eficácia do Sense Analytics

Em muitos ambientes, a despreocupação e as distrações em torno das práticas de segurança fazem com que alguns recursos cruciais não tenham necessariamente a segurança que poderiam ou deveriam ter. As organizações precisam limitar os aspectos negativos de uma inevitável invasão. Elas precisam de soluções que abrangem todo o ambiente, sem pontos cegos.



Desde o momento da instalação, o QRadar começa a criar dados de inteligência de segurança que são úteis de imediato e podem reforçar as defesas da organização. Alguns dos casos de uso nos quais a solução oferece um rápido valor são:

- Detecção avançada de ameaças
- Proteção de dados críticos
- Monitoramento de ameaças internas
- Gestão de riscos e vulnerabilidades
- Detecção de tráfego não autorizado
- Investigação forense

Casos de uso:

Detecção avançada de ameaças

Usando a análise de dados em tempo real, as equipes de segurança podem detectar se um host visitou um domínio possivelmente malicioso, mas, é possível que não emitam um alerta se for uma visita isolada. No entanto, se o mesmo host começar a demonstrar um comportamento diferente, detectado pelo uso da análise histórica a longo prazo, e também começar a transferir um volume de dados estranhamente elevado que desvia do seu comportamento habitual, a combinação dessas três condições permite que o QRadar produza um único alerta de intensidade elevada.

O QRadar também pode detectar uma mudança repentina no tráfego da rede, por exemplo, o surgimento de um novo aplicativo em um host ou o encerramento de um serviço habitual, e pode considerar essa uma condição anômala. As anomalias não são fáceis de serem detectadas pelas equipes de segurança por meio de buscas nos registros do sistema, diferente das assinaturas de malware e de outros ataques definidos contra vulnerabilidades conhecidas. Uma anomalia é, por definição, uma raridade que só pode ser detectada por uma solução de segurança que monitore e crie perfis das ações de todos os usuários e entidades.

Casos de uso:

Proteção de dados críticos

De um dia para o outro, um novo aplicativo começa a funcionar em um host da rede. Essa atividade pode ser resultado de um novo requisito da empresa ou, simplesmente, de alguém que tenha instalado um aplicativo de chat. Mas se esse host tiver acesso a dados críticos e também estiver associado a uma vulnerabilidade conhecida, o QRadar pode criar um alerta de alta prioridade para que as equipes de segurança investiguem o incidente rapidamente.

O QRadar detecta de forma rápida quando o tráfego de um evento supera um nível de atividade específico e gera um alerta. O limite pode se basear em qualquer dado coletado no QRadar, como configurações de dispositivo de rede, servidores, telemetria do tráfego de rede e aplicativos, além de usuários finais e suas atividades. Assim, em caso de mudança ou anomalia de conduta, o QRadar pode ampliar os dados do alerta com o contexto das identidades dos usuários, portas e protocolos em uso, reputações de IP e atividades de ameaça denunciadas para proporcionar às equipes de segurança uma perspectiva mais aprofundada do incidente.

Casos de uso:

Monitoramento de ameaças internas

Um representante de atendimento ao cliente repentinamente começa a fazer download do dobro de dados do que costumava fazer usando um sistema de informações sobre clientes, o que poderia fazer parte de uma nova atividade de análise de vendas. Mas se o QRadar sabe que esse representante recentemente acessou um site potencialmente suspeito e agora comprova que foram enviadas pequenas quantidades de dados ao site de uma empresa concorrente, a equipe de segurança será informada antes que uma grande quantidade de informações seja filtrada.

O QRadar se diferencia de outros produtos de segurança pelos perfis de entidades e pessoas. A combinação de um abrangente conjunto de dados, contexto empresarial e inteligência sobre ameaças, juntamente com a capacidade de detectar desvios do comportamento normal e reconhecer quais comportamentos não são permitidos ou apropriados, oferece uma capacidade de detecção de incidentes extremamente potente.

Casos de uso:

Gestão de riscos e vulnerabilidades

Quando uma nova entidade aparece na rede, o QRadar detecta automaticamente sua existência por meio da criação passiva de perfis de registros e dados de fluxo. Com seu detector de vulnerabilidades perfeitamente integrado, o QRadar pode examinar essa nova entidade para descobrir se ela tem alguma vulnerabilidade urgente ou de risco elevado que a exponha a possíveis fontes de ameaças.

Por exemplo, quando um novo servidor é adicionado à rede, o QRadar pode detectar se ele carece de correções críticas ou se tem credenciais administrativas predeterminadas. Além disso, ele pode notificar a equipe correspondente para corrigir o problema e/ou programar uma correção, e escalar o problema caso a tarefa não seja resolvida rapidamente.

E, principalmente, as novas vulnerabilidades descobertas são automaticamente relacionadas aos dados existentes sem que seja necessário fazer uma nova detecção, o que contribui para aumentar a velocidade e a precisão da detecção.

As economias operacionais resultantes também permitem que os analistas de segurança dediquem mais tempo a táticas proativas, como análises de riscos e atividades de correção de vulnerabilidades.

Casos de uso:

Detecção de tráfego não autorizado

Num momento em que a maioria das organizações permite que seus funcionários usem dispositivos próprios (BYOD), as equipes de segurança vêm observando um aumento do tráfego associado aos aplicativos de redes sociais. Os usuários costumam acessar seus sistemas de e-mail corporativo e se mantêm conectados com os amigos por meio do Facebook, LinkedIn, Twitter e outros serviços, tudo isso usando o mesmo dispositivo. O QRadar coleta e analisa esses dados e gera alertas se, por exemplo, as sessões de chat começarem a se conectar pela porta 80, que normalmente é reservada para o tráfego HTTP. Novas conexões com servidores de botnet conhecidos permitem que se comprove mais rapidamente a entrada de malware e advertem a equipe de segurança para que as devidas ações sejam tomadas.

O QRadar coleta e analisa dados de dispositivos móveis e BYOD tanto da camada de rede como de sistemas de gestão de pontos de conexão. Ele pode detectar possíveis ameaças, como dispositivos com jailbreak,

aplicativos suspeitos instalados em um dispositivo ou comunicações de internet potencialmente maliciosas, e colocar o dispositivo em quarentena e/ou escalar o problema para a equipe de segurança responsável.

Casos de uso:

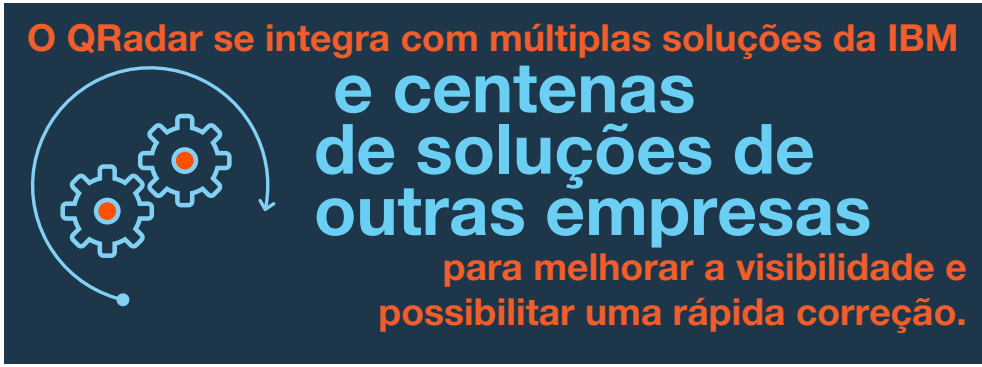
Investigação forense e rastreamento de ameaças

Durante a investigação de um delito, um analista de segurança descobre que um ou diversos funcionários foram vítimas de um ataque de phishing e que o invasor acessou um servidor interno. O padrão corresponde a um dos identificados pelo X-Force e sabe-se que ele injeta software "cavolo de troia" de acesso remoto (RAT), que é difícil de detectar.

Com poucos cliques, o QRadar recupera todos os pacotes de rede associados ao incidente e reconstrói os movimentos passo a passo, indicando para o analista de segurança com total clareza exatamente onde e quando o software RAT foi instalado. O fluxo de trabalho forense permite que o analista crie rapidamente um perfil completo do software malicioso e reconstrói as rotas de infecção por meio da análise de links para identificar o "paciente zero" e outros infectados. O resultado é que a equipe de segurança pode remediar rapidamente os danos e minimizar as recorrências.

A IBM proporciona inteligência prática para adotar uma defesa ativa e reforçar a proteção

A segurança das informações é uma das prioridades de qualquer equipe de administração, mas muitas organizações continuam dependendo de dezenas de produtos isolados para obter informações sobre momentos determinados. Funcionários com um nível de preparo elevado usam mecanismos de busca para alinhar montanhas de dados, mas cada vez mais os invasores evitam sua detecção por meio de trocas de IP, protocolos, portas e aplicativos nos quais é preciso introduzir, ampliar e coletar dados de grande valor depois que uma invasão acontece.



O IBM QRadar é diferente. Ele é implementado rapidamente, independentemente da escala da rede, e começa a oferecer resultados em questão de horas. Suas capacidades, semelhantes às cognitivas, e os dados de inteligência armazenados podem associar ataques relacionados procedentes do mesmo lugar ou correspondentes aos mesmos dados afetados. QRadar fornece essas informações imediatamente úteis para atender às necessidades atuais e futuras, desde a detecção avançada de ameaças até o monitoramento de ameaças internas, detecção de fraude, gestão de riscos e vulnerabilidades, investigações forenses e gestão de relatórios de conformidade.

Entre os principais motivos pelos quais os líderes em segurança escolhem o QRadar destacam-se:

- Seu painel de controle de segurança fácil de usar, que destaca as ameaças mais importantes e colabora com um fluxo de trabalho rápido e eficaz para investigação e correção
- Escalabilidade quase ilimitada, apoiada por dados de inteligência sobre ameaças X-Force e pela eficiência colaborativa do IBM X-Force Exchange
- IBM Security App Exchange, com aplicativos desenvolvidos pela IBM e por outras empresas que ampliam as capacidades do QRadar, sem torná-lo mais complexo
- Sua plataforma única integrada com visibilidade global, que fornece informações úteis sobre atividades de rede, aplicativos e usuários

Veja com nitidez as ameaças mais importantes

Uma vez detectada a ameaça, o ataque ou a invasão, é o momento de agir. O QRadar capacita as equipes de segurança com uma interface de usuário com base na Web que tem a mesma aparência em toda a plataforma.

Muitas das maiores empresas do mundo usam o QRadar para

evitar aparecer nos noticiários.

Passar do monitoramento do registro de atividades para a vigilância das atividades na rede, a revisão de incidentes relacionados, a execução de análises de risco e vulnerabilidade ou a realização de análise forense é tão simples quanto um clique na tela para que você tenha acesso a todas as informações em um painel de controle. Cada painel de controle inclui informações abrangentes sobre inteligência de segurança organizadas em exibições gráficas de atividades recentes, as quais podem ser investigadas com apenas alguns cliques.

Dedique alguns minutos para analisar os picos ou examine todos os detalhes de um incidente. As equipes de segurança podem compreender rapidamente a natureza do problema ressaltado, as vulnerabilidades exploradas, a entrada de algum botnet, RAT ou outro programa de malware, e o alcance dos dados perdidos. Esse é o momento de agir antes que algum dano real aconteça.

Alcance a potência necessária para agir em qualquer escala

QRadar inclui hardware, software e modelos de appliances virtuais para

reduzir o tempo de implantação.

Usando a plataforma QRadar completa, as equipes de segurança podem compreender com clareza e sem demora o que aconteceu e quais são os riscos caso elas não tomem nenhuma atitude. As principais funções, como monitoramento de ameaças, gestão de riscos e vulnerabilidades e geração de relatórios de conformidade estão ao alcance de um clique e podem trocar informações entre si. Além disso, o QRadar desfruta de total integração com dados de inteligência de ameaças de X-Force para obter atualizações a cada hora sobre as técnicas de ataques globais e conjuntos de malware.

Caso uma invasão aconteça, a tecnologia forense integrada ao QRadar oferece aos analistas do SOC dados dos pacotes correspondentes ao incidente, detalhando passo a passo as ações dos invasores com clareza e precisão. Para desativar algumas ameaças, basta bloquear as comunicações com endereço IP externo, embora muitas vezes seja preciso mobilizar as equipes de resposta a situações de emergência para isolar e reconfigurar hosts, desabilitar o malware e corrigir as vulnerabilidades. Mas e se a equipe não sabe exatamente o que fazer? É o momento de pedir ajuda, colaborar uns com os outros, buscar uma solução ou até mesmo contratar os serviços de uma equipe profissional.

A estrutura aberta do QRadar e do IBM Security App Exchange facilitam uma maior integração com as soluções da IBM e de outras empresas. Por exemplo, um dos aplicativos do site transmite os dados do incidente do QRadar para a Incident Response Platform de Resilient Systems para ação imediata. Outro aplicativo proporciona uma capacidade semelhante para compartilhar dados com a solução de gestão de pontos de conexão Carbon Black Enterprise Response.

Amplie suas capacidades com o IBM Security App Exchange

O IBM Security App Exchange amplia exponencialmente a flexibilidade do QRadar. Esse centro de colaboração permite que clientes, desenvolvedores e parceiros compartilhem aplicativos, extensões de aplicativos de segurança e melhorias para os produtos IBM Security.

Com o IBM Security App Exchange, as organizações podem:

- Conseguir aplicativos que ampliam as capacidades das soluções de segurança da IBM
- Compartilhar melhores práticas e aprender com os outros
- Encontrar soluções e casos de uso que aumentam o valor estratégico das operações de segurança

A IBM comprova determinados critérios estabelecidos em todo o código antes que apareça no site. E as equipes de segurança podem baixar e instalar as soluções de maneira independente, fora dos ciclos de atualizações oficiais dos produtos. Desse modo, é possível aplicar novos casos de uso de segurança sem aumentar desnecessariamente a complexidade da solução.

Em termos concretos, os usuários do QRadar podem baixar conteúdo para setores, ameaças, dispositivos e de fornecedores específicos pelo IBM Security App Exchange. Além disso, podem acessar relatórios personalizados, painéis de controle, análises especializadas e informações sobre ameaças.

Implemente uma única plataforma com visibilidade global

Os ambientes de segurança atuais são excessivamente complexos: é comum que os dados de segurança estejam distribuídos entre diversos produtos de diferentes fornecedores, com diferentes interfaces e formatos de armazenamento. Para detectar com eficácia as ameaças existentes e emergentes, as equipes de segurança precisam de uma visão consolidada desses dados, juntamente com análises completas para detecção de ameaças e capacidades de resposta. O QRadar usa uma única base de dados federada para todos os dados de segurança, criada especificamente para captura de dados escalável a partir de sistemas locais ou na nuvem, armazenamento, geração de relatórios e maior velocidade de busca.

QRadar é implementado com rapidez, sem que você precise de um exército de especialistas, além de oferecer uma central de comando por meio de um único console.

Do mesmo modo, o QRadar é otimizado para a análise de incidentes passados e em tempo real e para detectar incidentes poucos segundos depois que eles ocorrem, em vez de levar horas, dias ou semanas.

A solução também oferece um conjunto muito integrado de casos de segurança e outros disponíveis pelo IBM Security App Exchange. As equipes de segurança podem usar um único console com painéis de controle para todas as funções, como monitoramento de segurança em tempo real, gestão proativa de riscos e vulnerabilidades, e detecção, análise forense e correção de incidentes. Essa central única para as operações de segurança e resposta reúne inteligência de produtos da IBM e de outros fabricantes, além de contar com o apoio de uma interface de usuário e um fluxo de trabalho sempre semelhante, o que aumenta em grande medida a eficácia de suas operações de segurança.

Mais informações

Para obter mais informações sobre o IBM QRadar Security Intelligence Platform com Sense Analytics, entre em contato com seu representante ou parceiro de negócios da IBM.

Sobre o IBM Security

O IBM Security oferece um dos conjuntos mais avançados e integrados de produtos e serviços de segurança empresarial. O portfólio, respaldado pelo desenvolvimento e pela investigação internacionalmente prestigiados de X-Force, proporciona recursos de inteligência em segurança para ajudar as organizações a proteger globalmente funcionários, infraestruturas, dados e aplicativos, oferecendo soluções para gestão de acessos e identidades, segurança de base de dados, desenvolvimento de aplicativos, gestão de riscos, gestão de pontos finais e segurança de redes, entre outros. Essas soluções permitem que as organizações gerenciem os riscos de maneira eficaz e implementem uma segurança integrada para ambientes remotos, na nuvem, redes sociais e outras arquiteturas empresariais. A IBM opera uma das organizações de investigação, desenvolvimento e entrega de segurança mais amplas do mundo, monitora 15 milhões de eventos de segurança por dia em mais de 130 países e possui mais de 3.000 patentes de segurança.

Conheça nosso site

Fale com especialista

IBM Security
Route 100
Somers, NY 10589

O site da IBM está disponível em: **ibm.com**/br

WGW03211-BRPT-00