Guia de compras de soluções de gerenciamento de ameaças internas

Este guia de compras destaca as capacidades mais importantes para uma solução de gerenciamento de ameaças internas (ITM). Ele resume o que a Proofpoint aprendeu criando programas bem-sucedidos de ITM para organizações de todos os portes, no mundo todo e em todos os mercados verticais. Seu objetivo é ser um guia de referência para leitores que estão começando sua jornada de ITM ou que estão atualizando sua solução de ITM existente.

Comece com segurança centrada em pessoas

Para defender dados contra ameaças internas, você precisa de uma solução compatível com um modelo de segurança centrado em pessoas. Um modelo de segurança centrado em pessoas proporciona visibilidade total sobre comportamentos arriscados dos usuários e como os usuários interagem com dados confidenciais. Isso assegura que você tenha um contexto importante sobre suas intenções quando algo feito por eles parecer prejudicial à organização, seja intencionalmente ou inadvertidamente.

Com uma solução que segue uma abordagem centrada em pessoas, você pode compreender rapidamente o seu risco interno com base em indicadores comportamentais. Quando esses indicadores são observados holisticamente, no decorrer do tempo e no contexto de outras atividades, eles podem indicar que um usuário pode estar causando danos a uma organização e justificar mais investigações para determinar a resposta mais apropriada.

Elementos-chave de uma solução de ITM

Para evitar ameaças internas, você precisa ser capaz de identificar, proteger, prevenir e responder a incidentes causados por elementos internos. Só é possível reduzir os seus riscos de ameaças internas fazendo tudo isso de forma coordenada e com uma abordagem proativa.

Identificar

Você precisa de uma solução que ofereça visibilidade sobre comportamentos arriscados antes que uma ameaça interna ocorra. É desejável identificar padrões comportamentais anômalos com base em uma referência. A solução deve permitir o monitoramento de usuários arriscados, como usuários com acesso privilegiado, riscos de evasão, funcionários demissionários, terceirizados, executivos e usuários sob investigação. Fatores de estresse, como uma mudança na situação empregatícia (como rescisão ou demissão), mudanças na empresa (como uma fusão, aquisição ou reorganização) e comportamentos preocupantes (como atos associados a insatisfação ou conflito financeiro) também devem ser levados em consideração ao identificar usuários arriscados.

Cada organização deve decidir quais controles de prevenção funcionam melhor para si com base em seus objetivos empresariais, cultura e velocidade de inovação.

Proteger

Deseja-se uma solução que ajude a proteger sistemas e dados confidenciais com controles de segurança centrados em pessoas. Políticas e regras devem ser criadas com indicadores comportamentais para ajudar na proteção contra comportamentos arriscados.

É importante impedir que um usuário viole, acidental ou intencionalmente, a política de segurança, e isso se consegue por meio de instrução do usuário, lembretes em tempo real e bloqueio, quando necessário. Nem todas as atividades podem ou devem ser bloqueadas; recomenda-se que a prevenção deve estar em equilíbrio com a produtividade dos usuários. Cada organização deve decidir quais controles de prevenção funcionam melhor para si com base em seus objetivos empresariais, cultura e velocidade de inovação.

Também é importante que uma solução de ITM ofereça uma maneira flexível e fácil de gerenciar o acesso aos dados dos usuários. Deseja-se uma solução que tenha controles de acesso para garantir que os analistas de segurança tenham visibilidade sobre os dados somente na medida em que isso for necessário.

Detectar

Uma solução de ITM deve proporcionar alertas e atividades em tempo real sobre o comportamento dos usuários. Alertas de atividades de usuários arriscados podem incluir:

- Ocultação de informações
- Elevação de privilégios
- Desvio de controles de segurança
- Vazamento de dados
- Download de software não aprovado
- Sabotagem de TI
- Criação de uma porta dos fundos
- Acesso não autorizado
- Uso inaceitável

Quando uma regra é violada, a solução deve capturar “quem, o quê, quando e onde” da atividade de um usuário para proporcionar contexto e insights detalhados sobre comportamentos e intenções. A solução também deve capturar imagens de tela para oferecer provas irrefutáveis como parte das investigações. É importante que uma solução de ITM tenha a flexibilidade de responder dinamicamente a comportamentos arriscados e capturar imagens de tela somente após um alerta ser gerado, ajudando a proteger a privacidade dos usuários e possibilitando que os analistas de segurança trabalhem com mais eficiência.

Usuários descuidados são a principal causa de perda de dados e ameaças internas. Eles podem ser caracterizados como tendo boas intenções, mas que tomam decisões ruins. Contudo, seus erros podem ter graves consequências.

Responder

É importante investigar e responder aos incidentes com rapidez e eficiência. Por quanto mais tempo uma ameaça interna persistir, mais danos ela pode causar à sua reputação e à sua lucratividade. Fluxos de trabalho investigativos são fundamentais para rastrear o status de um incidente, especialmente quando a investigação envolve departamentos fora da segurança, como os de RH, jurídico, de conformidade e de privacidade. Uma solução de ITM robusta também deve se integrar com um sistema centralizado de gerenciamento de eventos, como um SIEM com o qual a equipe de analistas de segurança já trabalhe.

3 principais casos de uso

Existem três tipos principais de ameaças internas. Todos são causados por pessoas. Uma solução de ITM centrada em pessoas precisa lidar com:

- **Usuários descuidados.** São pessoas que não têm cuidado e cometem erros.
- **Usuários maliciosos.** São pessoas cuja intenção é causar danos.
- **Usuários comprometidos.** São pessoas cujas credenciais podem ter sido roubadas por um perpetrador de ameaças externo.

1. Usuários descuidados e erros comuns

Usuários descuidados são a principal causa de perda de dados e de ameaças internas, segundo o relatório Data Loss Landscape de 2024 da Proofpoint. Tais usuários podem ser caracterizados como tendo boas intenções, mas que tomam decisões ruins. Frequentemente, eles querem apenas fazer seu trabalho com o máximo de eficiência. Porém, seus erros podem ter consequências graves, como interrupção de negócios, danos à marca, enfraquecimento perante a concorrência, multas e violações de regulamentos e ações judiciais.

Veja a seguir algumas das maneiras pelas quais esses usuários geram risco:

- Envio de e-mails para pessoas erradas, com ou sem anexos
- Compartilhamento de dados confidenciais em sites de GenAI
- Visitação de sites de phishing
- Instalação de software não autorizado
- Compartilhamento público de arquivos e dados confidenciais
- Envio de informações de identificação pessoal (PII) para uma conta de e-mail pessoal
- Armazenamento de dados corporativos confidenciais em dispositivos pessoais

Usuários maliciosos são perigosos porque estão na posição ideal para se apoderar de dados confidenciais e causar danos a uma organização. Eles são motivados por ganho pessoal.

Proteção contra comportamento descuidado

Uma solução de ITM eficaz detecta e previne atividades arriscadas. Ela também oferece instruções aos usuários descuidados para ajudá-los a compreender o que há de errado em seus comportamentos para que eles possam mudá-los.

O que procurar:

- **Classificação.** Certifique-se de que e-mails, dados e conteúdos sejam monitorados consistentemente, tanto manualmente quanto por inteligência artificial (AI) para identificar e classificar os usuários arriscados. Quando um usuário é classificado como de alto risco, o sistema atribui uma pontuação de risco para proteger devidamente os dados.
- **Monitoramento.** A solução deve monitorar atividades e comportamentos arriscados, como uso não autorizado de aplicativos e da Web, alterações em tipos e nomes de arquivos de documentos confidenciais, acesso a dados fora do escopo do trabalho e vazamento de um grande volume de documentos confidenciais. O monitoramento de grupos de alto risco pode identificar usuários que precisem de um nível de monitoramento mais profundo.
- **Prevenção.** Os usuários devem ser impedidos de vazar dados confidenciais por endpoints. Isso inclui e-mails mal direcionados (com ou sem anexos), unidades USB, uploads na Web, sincronização na nuvem, compartilhamento em rede e impressão. Se os usuários cometerem um erro, eles devem receber imediatamente uma mensagem de advertência contextualizada que os permita remediar e evitar o incidente em tempo real, sem a participação de um administrador. Conforme o caso, os usuários podem explicar porque precisam de acesso aos dados. Com isso, a equipe de segurança é notificada, podendo permitir ou negar a solicitação.
- **Educação contínua.** Usuários descuidados frequentemente não sabem que seu comportamento é arriscado. Uma solução de ITM deve oferecer instrução e treinamento ao usuário final por meio de notificações de comportamentos arriscados e links para políticas corporativas.

2. Usuários maliciosos

Usuários maliciosos são perigosos porque estão na posição ideal para se apoderar de dados confidenciais e causar danos a uma organização. Além disso, eles são motivados por ganho pessoal. Funcionários demissionários são um dos tipos mais arriscados de elementos internos, mas há vários outros tipos.

Os principais tipos de ameaças internas maliciosas são:

- **Fraude.** Envolve atos enganosos que causam perturbações nos negócios
- **Sabotagem.** Inclui danos a um sistema ou destruição de dados
- **Roubo.** Envolve subtração de quaisquer informações valiosas ou pertencentes a uma organização
- **Espionagem.** Envolve a venda de dados valiosos, segredos comerciais etc. a um concorrente ou adversário

Um sistema centrado em pessoas monitora alguns usuários mais rigorosamente que outros. Ele também aplica controles de segurança mais rígidos aos usuários mais arriscados.

O que torna os elementos maliciosos uma ameaça tão grande é que eles desfrutam da confiança alheia. Sendo assim, eles podem esperar pacientemente pela oportunidade certa e usar seu acesso privilegiado para encontrar dados valiosos e pontos fracos na segurança. Além disso, as empresas frequentemente geram vulnerabilidades ao permitir que seus funcionários acessem e armazenem dados em seus dispositivos pessoais. Isso torna ainda mais fácil que os funcionários roubem dados confidenciais e causem danos.

Proteção contra usuários maliciosos

Um sistema centrado em pessoas pode monitorar alguns usuários mais rigorosamente que outros. Ele também aplica controles de segurança mais rígidos aos usuários mais arriscados. Além disso, ele bloqueia proativamente ações maliciosas com base em fatores de risco, como quando um funcionário pede demissão ou é despedido.

O que procurar:

- **Visibilidade.** Visibilidade sobre comportamentos e atividades de dados proporciona uma visão holística e oferece insights contextualizados sobre o que o usuário está fazendo e suas intenções. Deve-se coletar telemetria sobre as interações dos usuários com dados e sistemas — como quando eles renomeiam um arquivo confidencial ou fazem upload de tal arquivo para um site não autorizado ou uma pasta de sincronização na nuvem. Se um usuário faz download de aplicativos não autorizados, adultera controles de segurança ou instala um navegador TOR, essas atividades arriscadas também devem ser monitoradas. Uma cronologia de eventos contextualizada ajuda a compreender o “quem, o quê, quando e onde” da atividade do usuário e oferece insights sobre o que o usuário estava fazendo antes e após um alerta.
- **Biblioteca de ameaças.** Você quer uma biblioteca de ameaças abrangente, com alertas sobre os casos de uso de ameaças internas mais comuns (como descumprimento de expediente, vazamento de dados e desvio de controles de segurança). Isso assegura que você esteja operacional rapidamente, com regras para os indicadores comportamentais mais comuns.
- **Investigações.** Você quer uma solução que ofereça imagens de tela e metadados detalhados de atividades do usuário que possam oferecer evidências forenses em investigações. Fluxos de trabalho colaborativos são importantes para o gerenciamento de incidentes internos. Como investigações internas envolvem partes interessadas fora do âmbito da segurança, como departamentos de RH, jurídico, de privacidade e de conformidade, é interessante compartilhar relatórios de risco de usuário em formatos acessíveis e de fácil leitura, como PDF.
- **Controles de privacidade.** Uma solução de ITM robusta inclui recursos como controles de acesso baseados em atributos, mascaramento e anonimização de dados e suporte para data centers multirregionais para cumprir requisitos de residência e privacidade de dados e eliminar parcialidade nas investigações. É desejável poder mudar dinâmica e flexivelmente a política de monitoramento de um usuário em tempo real caso o usuário dispare um alerta, assegurando a privacidade do usuário ao capturar imagens de tela somente quando necessário.

3. Usuários comprometidos

Usuários comprometidos podem ter suas contas sequestradas e utilizadas indevidamente por um perpetrador de ameaças externo. Uma vez comprometidas as contas, os atacantes passam a ter acesso a dados e sistemas como se fossem uma pessoa de dentro da empresa. O que torna os usuários comprometidos tão desafiadores é que perpetradores de ameaças podem ficar à espreita em sistemas internos durante meses até serem descobertos.

Os atacantes cibernéticos externos contam com a exploração de vulnerabilidades humanas. A engenharia social (e o phishing em particular) é uma das maneiras mais comuns pelas quais os atacantes enganam os usuários. Isso não é uma surpresa, considerando-se sua alta taxa de êxito: 71% das organizações sofreram pelo menos um ataque de phishing bem-sucedido.

Técnicas de phishing comuns incluem:

- Envio de links maliciosos, anexos maliciosos e solicitações de dados
- Smishing (phishing por SMS)
- Phishing em redes sociais
- Entrega de ataques orientados para telefones (TOAD)
- Comprometimento de e-mail corporativo (BEC)
- Autenticação por múltiplos fatores (MFA)

O objetivo final é o mesmo: os perpetradores de ameaças externos querem acesso a sistemas e dados valiosos para explorar para ganho financeiro e benefício próprio.

Proteção contra usuários comprometidos

Uma solução de ITM eficaz proporciona visibilidade e contexto para ajudar a compreender se o comportamento do usuário é incomum. Se um usuário é propenso a clicar em links de phishing, por exemplo, você pode monitorar esse usuário arriscado quanto a qualquer comportamento incomum. Você também pode proteger os dados assegurando que somente quem realmente precise possa vê-los.

O que procurar:

- **Monitoramento proativo.** Ao criar e salvar explorações personalizadas, as suas equipes podem pesquisar regularmente vazamentos de dados e atividades arriscadas. Pessoas muito atacadas (Very Attacked People ou VAPs), com histórico de clicar em anexos ou links maliciosos ou de interagir com aplicativos vulneráveis, podem ser monitoradas quanto a comportamentos incomuns que possam indicar um usuário comprometido. A mesma abordagem pode ser utilizada para outros grupos de alto risco, como funcionários demissionários ou usuários com acesso privilegiado. Como é impossível identificar antecipadamente todos os elementos internos arriscados, a solução de ITM deve ser capaz de alterar, dinâmica e flexivelmente, a política de monitoramento de um usuário em tempo real, caso o usuário dispare um alerta.
- **Controles de acesso adaptáveis.** Você pode aplicar regras de acesso condicional a dados, como listas de permissão e/ou de bloqueio de países, redes ou endereços IP de alto risco. Também é possível limitar o acesso a dados confidenciais a determinados usuários e grupos privilegiados e permitir uploads e downloads somente em dispositivos gerenciados. Com controle de acesso baseado em atributos, você pode lidar com exigências de privacidade.
- **Integrações.** Uma solução de ITM eficaz complementa o seu sistema de segurança, ajudando a proporcionar contexto. A razão disso é que ela facilita a integração com uma variedade de ferramentas, inclusive:
  - Coordenação de segurança, automação e resposta (SOAR)
  - Gerenciamento de eventos e informações de segurança (SIEM)
  - Resposta a incidentes
  - Sistemas de gerenciamento de tíquetes
- **Arquitetura moderna.** A vantagem de uma plataforma nativa em nuvem é que ela pode ser dimensionada para centenas de milhares de usuários. A solução de ITM deve coletar telemetria através de um agente de endpoint leve que não prejudique a produtividade dos usuários e não entre em conflito com outras soluções.

Conclusão

Proteger a sua organização contra o risco interno, seja este intencional ou não, requer uma solução de ITM que viabilize uma abordagem proativa. Uma solução de ITM deve ter visibilidade sobre comportamentos arriscados e a capacidade de responder dinâmica e automaticamente. Considerando-se a colaboração cruzada para apoio a iniciativas de risco interno, uma solução de ITM deve permitir fluxos de trabalho investigativos e coletar evidências irrefutáveis, como imagens de tela, para acelerar as investigações. Finalmente, uma solução de ITM deve ser capaz de se expandir com a sua empresa, aproveitar os seus investimentos existentes e oferecer controles de privacidade e acesso flexíveis para assegurar conformidade. O uso de uma solução de ITM com essas capacidades necessárias ajuda a assegurar que a sua empresa esteja protegida contra o risco interno viabilizando a sua equipe de segurança.

SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.