Guia de compras para detecção e resposta a ameaças a identidades

Os atacantes cibernéticos costumam ser criativos, persistentes e focados. Contudo, eles também são bastante metódicos. Na maioria dos casos, ao chegar no meio da cadeia de ataque, eles utilizam ferramentas e técnicas prontamente disponíveis para descobrir e compreender o seu ambiente de TI. Eles procuram ampliar seus privilégios e movimentar-se lateralmente pela sua rede em busca de seu objetivo final: os seus ativos de TI mais críticos, ou seja, as "joias da coroa". E ao estabelecer presença na sua rede, com tempo de permanência suficiente, eles realmente chegam a esse destino final. A menos que você os detecte e responda efetivamente.

Atacantes sofisticados dependem de que as organizações visadas deixem para trás identidades e credenciais que possam ser utilizadas para levar adiante seus ataques. Porém, eles também esperam que o que veem seja real e que os dados coletados da rede, do usuário e do sistema sejam confiáveis. Isso é um ponto fraco fundamental. Com a implantação de sistemas de detecção e resposta a ameaças a identidades, essa expectativa torna-se um calcanhar de Aquiles. Esses sistemas protegem contra a progressão de ameaças baseadas em identidades. Eles defendem o meio da cadeia de ataque, onde ocorrem a ampliação de privilégios e a movimentação lateral.

Este guia de compras destaca as capacidades críticas necessárias para sistemas de detecção e resposta a ameaças a identidades. As recomendações aqui contidas baseiam-se no conhecimento da Proofpoint em áreas de controle de segurança, bem como em nossos anos de experiência na categoria emergente de detecção e resposta a ameaças a identidades.

Elas descrevem as seguintes áreas de cobertura:

- Requisitos gerais
- Descoberta e remediação de vulnerabilidades de identidade
- Detecção e resposta a ameaças ativas

Este guia também discute a importância cada vez maior de tecnologias enganosas. Ele explica como elas estão mudando as regras do jogo para sistemas de detecção e resposta a ameaças a identidades, em comparação com detecções tradicionais baseadas em assinatura ou comportamentos.

Esse conjunto de soluções é parte da plataforma integrada de segurança centrada no ser humano da Proofpoint que atende as quatro áreas de risco baseado em pessoas.

Geral

Em ataques cibernéticos de alto impacto, os adversários frequentemente utilizam phishing de credenciais, malware ou ameaças internas para o comprometimento inicial de um ambiente. Após entrar e desativar a segurança local baseada em agente, eles movimentam-se em direção ao alvo final. Essa movimentação — lateral quando dentro da empresa ou nuvem; vertical quando entra ou sai da empresa ou nuvem — exige tanto credenciais quanto conectividade. A essa altura, os perpetradores de ameaças estão no meio da cadeia de ataque. Utilizando inúmeras ferramentas e automação, os atacantes começam a se aproveitar de funcionalidades existentes por meio de mais garimpo de credenciais, varredura de rede e ampliação de privilégios. Como isso frequentemente aparenta ser atividade normal de usuários ou aplicativos, pode ser bastante desafiador de detectar com o uso de ferramentas tradicionais. Mas é aí que os sistemas de detecção e resposta a ameaças a identidades se destacam.

A tabela seguinte oferece uma visão das capacidades gerais que uma solução de detecção e resposta a ameaças a identidades deve oferecer para enfrentar esse desafio, tanto antes quanto após a chegada de um perpetrador de ameaças.

Áreas gerais de cobertura

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Compreender precisamente onde a organização está atualmente vulnerável a ampliação de privilégios e movimentação lateral	Um sistema de detecção e resposta a ameaças a identidades deve apontar as identidades atualmente vulneráveis e as credenciais associadas que constituiriam um caminho de ataque para um atacante após o comprometimento inicial. A solução também deve disponibilizar esses dados como contexto para sistemas que rastreiam as pessoas mais atacadas e mais privilegiadas na organização.
Descobrir e eliminar continuamente os caminhos de movimentação lateral e ampliação de privilégios	Um sistema de detecção e resposta a ameaças a identidades precisa: • Encontrar e apresentar caminhos de ataque de alto risco para ativos de TI críticos • Revelar conexões esquecidas e credenciais errantes que permitam a mobilidade do atacante • Priorizar e remediar automaticamente as identidades mais arriscadas para privar preventivamente os atacantes do que eles necessitam (e esperam encontrar) para se movimentarem dentro da rede sem serem detectados.
Melhorar a detecção e a resposta	Uma solução de detecção e resposta a ameaças a identidades deve detectar e responder a ameaças ativas com alta fidelidade (baixo índice de falsos positivos e falsos negativos). Além disso, ela deve coletar dados forenses com base nas fontes, em tempo real, de máquinas comprometidas para auxiliar na resposta a incidentes.
Identificar o quê e quem está sendo visado e atacado ativamente e compreender a causa-raiz de um ataque bem-sucedido	Uma solução de detecção e resposta a ameaças a identidades deve fornecer informações contextuais — quem, o quê, quando e como — para informar sobre todos os estágios da cadeia de ataque. Essa informação proporciona um contexto fundamental sobre o comprometimento inicial, movimentação lateral e quais falhas de controle contribuíram para quaisquer vazamentos de dados ou outras formas de impacto corporativo. Uma solução deve fornecer insights profundos sobre os passos de ampliação de privilégios e movimentação lateral, tanto potenciais quanto utilizados, de um ataque.

Descubra e corrija vulnerabilidades de identidade

Uma solução de detecção e resposta a ameaças a identidades deve permitir que você descubra e corrija vulnerabilidades de identidade antes que os atacantes possam se aproveitar delas. Ela deve ser capaz de mapear e oferecer uma visão abrangente da presença de identidades vulneráveis e privilegiadas em toda a empresa, inclusive provedores de identidade, endpoints, diretórios, armazenamentos de identidades e sistemas PAM, sejam estes hospedados na nuvem ou no local.

Descoberta e remediação de vulnerabilidades

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Descobrir e rastrear identidades vulneráveis na empresa	Uma solução de detecção e resposta a ameaças a identidades deve descobrir: • Configurações de PAM e gerenciamento de credenciais de contas de serviço, de administrador local e de domínio privilegiado insuficientes ou inadequados • Criação não intencional de contas de administrador oculto com privilégios excessivos • Encerramento inadequado de sessões de RDP • Credenciais armazenadas em endpoints — inclusive navegadores da Web, SSH, FTP, PuTTY, linhas de comando e bancos de dados — que armazenam temporariamente credenciais e tokens de acesso à nuvem nos endpoints
Descobrir e rastrear violações de políticas com base em contas	Uma solução de detecção e resposta a ameaças a identidades deve identificar: • Contas mal configuradas • Contas de aplicativos antigos • Contas inativas • Violações de política de senhas • Credenciais sujeitas a ataques do tipo kerberoasting • Contas de usuário não gerenciadas • Contas de serviço não gerenciadas
Corrigir ameaças a identidades automaticamente, sem afetar as operações da empresa	Uma solução de detecção e resposta a ameaças a identidades deve utilizar monitoramento contínuo e regras empresariais personalizáveis e automatizadas para eliminar violações de políticas de segurança, como: • Tokens de nuvem • Sessões de RDP inativas ou desconectadas • Credenciais armazenadas de ativos confidenciais • Contas de administrador local • Credenciais armazenadas temporariamente em navegadores, no Windows e em outros sistemas
Iniciar a remediação de vulnerabilidades de identidade por meio de integração com um sistema de gerenciamento de serviços de TI (ITSM)	Para aquelas vulnerabilidades que não podem ser remediadas com segurança por meio de automação, uma solução de detecção e resposta a ameaças a identidades deve ser capaz de abrir tíquetes no sistema de ITSM da organização, para que essas vulnerabilidades possam ser gerenciadas e remediadas como parte dos processos de TI normais da organização

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Visualizar e priorizar os caminhos de ataque disponíveis	Um sistema de detecção e resposta a ameaças a identidades deve: • Descobrir configurações inadequadas, exposições e identidades vulneráveis • Oferecer insights sobre como uma combinação dessas vulnerabilidades pode proporcionar caminhos de ataque aos ativos de TI mais valiosos ou a outros sistemas críticos ou confidenciais • Apresentar caminhos de ataque e mostrar como remediá-los de uma maneira decisiva e visualmente efetiva • Oferecer um gráfico interativo que proporcione orientação para remediação e um contexto mais profundo • Ajudar a visualizar o possível raio de alcance atual de aplicativos e permissões de um determinado usuário para auxiliar em investigações, tanto antes quanto após uma exploração
Descobrir e rastrear os ativos de TI mais valiosos	Controles de segurança baseados em detecção e resposta a ameaças a identidades devem: • Começar com a compreensão de quais sistemas de TI devem ser protegidos prioritariamente • Ser capazes de descobrir e sinalizar automaticamente ativos de nível 0 ocultos ou desconhecidos
Integrar-se com um amplo conjunto de sistemas de segurança e de TI	Uma solução de detecção e resposta a ameaças a identidades deve ser capaz de: • Operar de forma integrada e complementar a estrutura de segurança e de TI da organização • Descobrir vulnerabilidades de identidade e seus relacionamentos umas com as outras e com os ativos de TI mais valiosos da organização • Extrair e analisar dados do AD, Entra ID, armazenamentos de identidades na nuvem (como AWS e Okta), sistemas de PAM e endpoints, tanto clientes quanto servidores • PAMs, inclusive: CyberArk e Delinea • Oferecer ampla cobertura de endpoints, inclusive sistemas operacionais Windows, Linux e Mac • Integrar-se com EDR, SIEMs/XDRs, SOARs e sistemas operacionais host para detectar, investigar e responder a ameaças ativas, inclusive CrowdStrike Falcon, Splunk, LogRhythm e Microsoft Defender • Integrar-se com os sistemas de distribuição de software e ITSM da organização para propiciar colaboração entre equipes de segurança e de TI

Detectar e responder a ameaças

Uma solução de detecção e resposta a ameaças a identidades deve detectar com alta fidelidade e auxiliar em uma resposta eficiente a ameaças ativas. A tabela seguinte oferece um resumo das principais necessidades de detecção e resposta do cliente e das capacidades necessárias em um sistema de detecção e resposta a ameaças a identidades.

Detecção e resposta a ameaças

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Pegar os perpetradores de ameaças em flagrante no ato de tentar ampliar privilégios e movimentar-se lateralmente, antes que eles consigam chegar às "joias da coroa" da organização	Uma solução de detecção e resposta a ameaças a identidades deve ajudar você a detectar ações e tentativas de movimentação lateral e ampliação de privilégios por parte dos perpetradores de ameaças. Ela não deve exigir um agente persistente para não gerar o risco de que o agente seja contornado. A solução deve utilizar as seguintes metodologias: • Enganos com base em arquivos, por exemplo, com arquivos de MS Office, como MS Word ou MS Excel, utilizando modelos de documentos da organização e senhas realistas para dar impressão de autenticidade • Arquivos sinalizadores para rastrear a utilização dentro e fora da organização, também utilizando modelos com a marca da organização • Monitoramento do uso de arquivos sinalizadores utilizando uma solução de DLP para iniciar alertas investigativos em caso de movimentação dos arquivos enganosos • Implantação de objetos órfãos (ou uso de objetos existentes) do Active Directory como rastros enganosos • Uso do sistema de AD de produção apenas, eliminando a necessidade de criar um domínio de AD falso com confiança para o sistema de AD de produção • Distribuir amplamente indícios enganosos para proporcionar capacidades de detecção em nível de sistema, aplicativo e rede, inclusive: - Históricos de navegador - Conexões a bancos de dados - Dados de varredura - E-mails e mensagens do Teams - Sessões de FTP, RDP, PuTTY e SSH - Scripts - Compartilhamentos de arquivos - Credenciais de Windows - Artifícios enganosos na forma de ransomware - Artifícios enganosos na forma de ADRecon e Bloodhound - Artifícios enganosos na forma de Swift e mainframe • Detectar e gerar alertas sobre atividades e alterações de alto risco no Active Directory. Estas devem incluir: - Conexão interativa bem-sucedida em contas de serviço - Alterações em permissões de administrador SDHolder - DCSync realizado em uma conta que não seja de máquina - Abuso de delegação restrita - Conta de usuário ativada/desativada - Membro adicionado a um grupo administrativo - SPN adicionado a uma conta de computador

O papel do engano

Sistemas que detectam ameaças ativas não devem depender apenas de detecções baseadas em assinaturas ou comportamentos. Estas não são tão eficazes quanto deveriam e frequentemente produzem altos índices de falsos positivos e falsos negativos. A ampla distribuição de artifícios enganosos de alta qualidade pode mitigar esse problema e melhorar bastante a eficácia de um sistema de detecção e resposta a ameaças a identidades.

Tecnologias enganosas replicam com precisão credenciais, conexões, arquivos e outros dados de que o atacante necessita para avançar pela cadeia de ataque. Boas tecnologias de detecção criam e implantam artifícios enganosos que parecem reais, adaptados especificamente a cada organização. Elas identificam conexões e sistemas de rede, bem como ativos de nível 0 (as "joias da coroa"). E são muito difíceis de distinguir de recursos, serviços, características e ativos de TI reais.

Para que não sejam descobertos e contornados por perpetradores de ameaças, os artifícios enganosos não devem ter agentes. Eles devem ser capazes de:

- Expandir-se a ponto de cobrir todo o inventário de endpoints da organização para assegurar que os atacantes sejam descobertos prematuramente, logo após o comprometimento inicial
- Ser atualizados dinâmica e automaticamente
- Ser ajustados em resposta a alterações no ambiente de TI

Alertas acionados por artifícios enganosos devem se integrar perfeitamente com as tecnologias de monitoramento, caça a ameaças, visualização e telemetria existentes. Isso ajuda com medidas de contenção e remediação e respostas informadas. O sistema deve coletar dados forenses originais em tempo real do endpoint. Esses dados devem incluir detalhes sobre "quem, o quê, quando e onde" do ataque.

O sistema também deve fornecer esses dados às equipes de resposta a incidentes e ao SOC. Ele também deve proporcionar visibilidade sobre o quão próximo o atacante está de credenciais de administrador de domínio e ativos empresariais críticos.

SAIBA MAIS

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