Proofpoint Threat Response Auto-Pull

Coloque automaticamente em quarentena o e-mail malicioso pós-entrega

Principais vantagens

- Coloque automaticamente em quarentena os e-mails maliciosos que passam pelas soluções de perímetro
- Reduza exponencialmente o tempo despendido na segurança e na troca de mensagens com as equipes ao tratar da coordenação e resposta de segurança
- Aproveite a inteligência sobre ameaças da Proofpoint na classificação de mensagens
- Monitore automaticamente a caixa de correio de abuso quanto à presença de ameaças
- Coloque em quarentena as mensagens encaminhadas a indivíduos específicos ou a listas de distribuição
- Rastreie campanhas de phishing denunciadas parcialmente e elimine o desperdício de tempo com mensagens denunciadas indevidamente

O Proofpoint Threat Response Auto-Pull (TRAP) permite que os seus administradores de segurança e de mensagens simplifiquem o processo de resposta a incidentes de e-mail. Quando e-mails maliciosos são detectados, o TRAP os analisa e os remove automaticamente. Ele também coloca em quarentena os e-mails indesejados que chegaram às caixas de entrada dos usuários. O Proofpoint TRAP reduz o tempo que as suas equipes de segurança e de mensagens precisam para limpar o e-mail.

O e-mail é o vetor de ataque nº 1. Ele é responsável por mais de 90% das violações de dados. Como as ameaças baseadas em e-mail tornaram-se mais avançadas, as organizações estão diante de um número crescente de mensagens maliciosas. Esses e-mails podem conter links de phishing que são ativados após a entrega ou podem utilizar técnicas avançadas para evitar detecção, o que pode resultar em falsos negativos e permitir que os e-mails cheguem aos usuários finais. Para reduzir o risco de ameaças e minimizar o impacto potencial de uma violação, as equipes de segurança de e-mail precisam analisar e limpar esses e-mails maliciosos. Processar um pequeno número de e-mails pode não ser muito demorado, mas incidentes que envolvem centenas ou milhares de e-mails maliciosos podem sobrecarregar rapidamente as equipes de segurança e seu gerenciamento pode se tornar demasiadamente tedioso.

Acompanhamento de encaminhamentos e expansão de listas de distribuição

O TRAP ajuda os administradores a lidar com e-mails maliciosos ou indesejados que são encaminhados para outrem. Ele tem uma lógica interna que pode detectar quando uma mensagem é encaminhada ou enviada para uma lista de distribuição. Ele também expande automaticamente a lista de destinatários para localizar e eliminar a mensagem. O tratamento automatizado do processo de eliminação de e-mails encaminhados pode poupar bastante tempo e trabalho aos administradores.

Opções de distribuição flexíveis

O TRAP pode ser implementado na nuvem, hospedado pela Proofpoint. Também pode ser implementado no local, através do VMware e do AWS. Essa flexibilidade

permite que o TRAP seja utilizado em vários sistemas de e-mail, como Microsoft 365, Microsoft Exchange e Google Workspace. A opção mais moderna e conveniente é a implementação na nuvem. Ela exige menos trabalho para ser configurada e economiza na manutenção devido a suas atualizações de software automatizadas.

Gerenciamento de e-mail fora de banda

O TRAP permite colocar em quarentena e-mails que possam ser ameaças à segurança ou que violem a política da empresa. Ele faz isso utilizando arquivos CSV, a pesquisa inteligente da Proofpoint ou relatórios de incidentes manuais. Forneça alguns elementos de informação fundamentais e o TRAP removerá rapidamente os e-mails especificados das caixas de entrada dos usuários. Ele também oferece uma lista de atividades que mostra quem leu os e-mails, bem como o status de quaisquer tentativas de recall. Isso ajuda a assegurar que e-mails potencialmente nocivos ou inadequados seja identificados rapidamente e tirados de circulação.

Compartilhamento de inteligência multivetorial com o Proofpoint Nexus Threat Graph

O Proofpoint Nexus Threat Graph agrega e correlaciona dados de ameaças de múltiplas fontes, como e-mail, nuvem, rede e redes sociais. Ele oferece proteção e resposta em tempo real para todos os produtos da Proofpoint. Além disso, ele está integrado na plataforma da Proofpoint. Portanto, não exige nenhuma instalação ou gerenciamento adicional.

Quando se torna parte dessa rede, você tem acesso às seguintes vantagens:

- Inteligência sobre ameaças em tempo real de uma comunidade de mais de 115.000 clientes
- Visibilidade multivetorial em e-mail, nuvem, rede e redes sociais
- Informações sobre mais de 100 perpetradores de ameaças rastreados para compreender suas motivações e táticas

O TRAP utiliza inteligência do Nexus Threat Graph para associar destinatários a identidades de usuário. Ele também revela as campanhas associadas e identifica os domínios e endereços IP utilizados nos ataques. Com base nessas informações, o TRAP pode executar ações automatizadas com usuários visados de determinados departamentos ou grupos com permissões especiais. Quando detectamos e-mails maliciosos com links, anexos ou IPs suspeitos no site de um cliente, nós compartilhamos essas informações com toda a nossa base de clientes para proteção futura e para colocar em quarentena quaisquer mensagens entregues na caixa de entrada do usuário.

Triagem aprimorada

A capacidade do TRAP de investigar URLs seguramente com a tecnologia Proofpoint Browser Isolation melhora o processo de triagem de incidentes para os analistas. A tecnologia permite que analistas avaliem o conteúdo de um URL sem expor a organização a riscos. Isso os ajuda a avaliar com rapidez e precisão incidentes que envolvem URLs, possibilitando a tomada de providências apropriadas para proteger a organização.

Closed-Loop Email Analysis and Response

O Closed-Loop Email Analysis and Response (CLEAR) ajuda os usuários a identificar e lidar com e-mails potencialmente maliciosos rapidamente. Ele combina as capacidades do PhishAlarm, do PhishAlarm Analyzer e do TRAP para oferecer uma resposta rápida e eficaz a mensagens denunciadas. Com o CLEAR, os e-mails denunciados são enviados para uma caixa de correio para denúncia de abuso. Em seguida, eles são analisados automaticamente em relação à inteligência sobre ameaças da Proofpoint e outras fontes para determinar se possuem conteúdo malicioso. Caso uma correspondência seja encontrada, a mensagem é removida da caixa de entrada do destinatário e colocada em quarentena. Isso ajuda a evitar ataques ativos e a proteger a sua organização. Funcionários informados são uma linha de defesa importante contra ameaças cibernéticas. O CLEAR ajuda a capacitá-los a denunciar e lidar com possíveis ameaças em questão de minutos.

SAIBA MAIS

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

Sobre a Proofpoint

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.proofpoint.com/br**.