Antigena Email

Desenvolvendo imunidade para sua caixa de entrada

Visão geral

- **Autoaprendizagem: entende o ser humano, não apenas o endereço de e-mail**
- **Identifica e-mails mal-intencionados não detectados por ferramentas tradicionais**
- **Eficaz contra todos os ataques avançados por e-mail, incluindo engenharia social**
- **Implantação rápida e virtual**

Ameaças por e-mail capturadas pela Antigena Email

- Spear-phishing
- Clonagem e engenharia social
- Comprometimento de e-mails corporativos
- Aquisição do controle de contas na cadeia de suprimentos
- Perda de dados externos
- Malware novo, desconhecido

> Ficamos impressionados com tudo o que nossas ferramentas tradicionais não identificaram e que foram capturadas pela Antigena Email.
>
> **– CTO, Bunim/Murray Productions**

Novas ameaças por e-mail estão conseguindo entrar

Os ataques por e-mail estão ficando cada vez mais sofisticados, com a IA ofensiva ameaçando superar as campanhas de ataque por e-mail em um futuro próximo. Está se tornando praticamente impossível distinguir e-mails falsos direcionados de comunicações genuínas.

Os novos ataques conseguem passar consistentemente por ferramentas tradicionais de segurança de e-mail, que observam e-mails individuais isoladamente e os comparam com regras e assinaturas de ataques mal-intencionados conhecidos. Com as cadeias de suprimentos se tornando mais complexas e os funcionários mais distribuídos e móveis, a necessidade de uma abordagem de autoaprendizagem orientada por IA para segurança de e-mail é cada vez mais necessária.

> Mais do que nunca, a segurança moderna de e-mail exige inovação e uma mudança de mentalidade para combater o cenário de ameaças em evolução.
>
> **– Gartner**

A primeira caixa de entrada com autodefesa do mundo

A Antigena Email é a primeira solução de Ciber IA do mundo para a caixa de entrada. Aprendendo o "padrão de vida" normal de cada usuário e correspondente, a tecnologia desenvolve um entendimento em evolução do "humano" nas comunicações por e-mail.

Enquanto as defesas tradicionais questionam se os elementos em um e-mail já foram observados em ataques históricos, a Antigena Email é a única solução que pode perguntar com segurança se seria incomum um destinatário interagir com um e-mail específico, no contexto de seu "padrão de vida" normal, bem como, no contexto do "padrão de vida" de seus colegas e de toda a organização.

Esse conhecimento contextual permite que a IA tome decisões altamente precisas e neutralize a gama completa de ataques por e-mail, desde e-mails falsificados "limpos" que buscam realizar um pagamento fraudulento até tentativas sofisticadas de spear-phishing.

Compreendendo o ser humano no e-mail

Inspirada no sistema imunológico humano, a Antigena Email usa a inteligência artificial da Darktrace para aprender um senso de "self" para cada usuário interno e externo, analisando as comunicações recebidas e enviadas juntamente com as comunicações internas.

Ao tratar os destinatários como indivíduos e colegas dinâmicos, a Antigena Email identifica de maneira exclusiva os desvios sutis da "norma", que revelam que e-mails aparentemente benignos são claramente mal-intencionados.

Caso de uso:
Aquisição do controle de contas na cadeia de suprimentos

Um dos ataques mais difíceis de detectar é a aquisição externa do controle de contas, em que um criminoso sequestra as credenciais de e-mail de um contato confiável e obtém acesso à caixa de entrada.

Depois de entrar, o invasor pode acessar o histórico de correspondências e gerar e-mails altamente convincentes, incorporando um link ou anexo mal-intencionado na conversa no momento certo.

Enquanto as defesas tradicionais supõem que se trata de um usuário confiável, a Antigena Email percebe o contrário. Ela analisa cada e-mail no contexto dos padrões de vida aprendidos e detecta até os desvios mais sutis. Isso abrange (mas não se limita a):

Localização incomum de login – a Antigena Email pode extrair o endereço IP localizável geograficamente do remetente genuíno e determinar se ele é raro de acordo com o histórico do padrão de vida do contato confiável. Embora um local de login raro isoladamente não possa acionar um alerta ou uma resposta autônoma, ele aparecerá no cálculo geral do sistema e na pontuação de anomalias.

Raridade de links – as pessoas geralmente compartilham links para sites que elas visitam e nos quais confiam. Ao observar esses links em e-mails internos, a Antigena Email pode determinar quais links e domínios são raros no contexto da organização. Isso também é útil em outros cenários de ameaças, ao determinar se o domínio de e-mail de um remetente específico foi observado em links internos compartilhados.

Destinatários incomuns – a Antigena Email modela os relacionamentos baseados em gráficos entre usuários e colegas internos e externos e entende seus relacionamentos em um nível granular. Se o invasor enviar vários e-mails para diversos destinatários na organização, a Antigena Email poderá estimar a probabilidade de esse grupo específico receber um e-mail da mesma fonte.

Anomalias comportamentais – Com o tempo, a Antigena Email aprende como diferentes remetentes constroem seus e-mails, analisando metadados e padrões ocultos de e-mail no conteúdo do corpo da mensagem. Ao aplicar IA a todos os e-mails recebidos, a Darktrace identifica mudanças sutis que podem indicar que o e-mail foi enviado por alguém que não é o verdadeiro titular da conta.

Ao correlacionar esses indicadores fracos, a Antigena Email chega rapidamente a uma pontuação abrangente de anomalia, determinando com confiança que o e-mail é mal-intencionado e neutralizando o ataque antes que ele possa causar impacto.

Descubra a Antigena Email em seu próprio ambiente com uma avaliação gratuita de 30 dias

Agendar uma demonstração