Antigena Email

이메일용 면역 체계 구축

한 눈에 보기

- 자가 학습 : 이메일 주소가 아닌 발신자를 파악
- 기존 툴이 놓치는 악성 이메일 식별
- 소셜 엔지니어링을 비롯한 모든 지능형 이메일 공격 차단에 유효
- 신속한 가상 배포

Antigena Email이 탐지하는 이메일 위협

- 스피어 피싱
- 소셜 엔지니어링 및 위장
- 비즈니스 이메일 보안 침해
- 공급망 계정 탈취
- 외부 데이터 손실
- 알려지지 않은 새로운 악성코드

> Antigena Email 과 달리 기존에 보유하고 있던 툴이 탐지에 실패하는 것을 보고 충격을 받았습니다 .
>
> – CTO, Bunim/Murray Productions

새로운 이메일 위협 침투

이메일 공격이 점점 정교해지면서 조만간 공격적인 AI 가 이메일 공격 캠페인에 대대적으로 나설 것으로 전망됩니다 . 표적 스푸핑 이메일과 진짜 통신을 구별하기가 거의 불가능해지고 있습니다 .

새로운 공격이 지속적으로 기존 이메일 보안 툴을 통과하고 있는데 , 이러한 툴은 개별 이메일을 격리 상태에서 관찰하고 이를 알려진 악성 공격 규칙 및 시그니처와 대조하는 방식입니다 . 공급망이 점점 복잡해지고 직원들이 분산된 모바일 환경에서 일하는 경우가 늘어나자 , AI 기반의 자가 학습 방식을 이메일 보안에 적용하는 것이 매우 중요해졌습니다 .

> 최신 이메일 보안을 위해서는 그 어느 때보다도 진화하는 위협 환경에 대응하기 위한 사고방식의 변화와 혁신이 필요합니다 .
>
> – Gartner

세계 최초의 자가 방어형 이메일

Antigena Email 은 세계 최초의 이메일용 Cyber AI 솔루션입니다 . 이 기술은 모든 사용자와 연락처의 정상적인 '행동 패턴' 을 학습하여 이메일 통신 내에서 다양하게 변화하는 '인적 요소' 를 파악합니다 .

기존 방어 체계는 이메일 요소들이 과거 공격에서 관찰되었는지 여부를 묻는 반면 , Antigena Email 은 수신자가 정상적인 '행동 패턴' 의 컨텍스트 내에서 특정 이메일과 동료 및 조직 내 다른 부서와 통신하는 것이 비정상적인지를 명확하게 묻는 유일한 솔루션입니다 .

이 컨텍스트별 정보를 통해 AI 는 매우 정확한 의사 결정을 내리고 , 부정 결제액을 송금하려는 '정상' 스푸핑 이메일에서 정교한 스피어 피싱 시도에 이르는 전방위적인 이메일 공격을 무력화할 수 있습니다 .

이메일 내 인적 요소 파악

인간의 면역 체계를 응용한 Antigena Email 은 Darktrace 의 핵심적인 인공지능을 사용하여 모든 내외부 사용자의 ' 고유 환경' 에 대한 감각을 학습함으로써 수평적인 내부 간 통신과 함께 인바운드 및 아웃바운드 통신을 분석합니다 .

Antigena Email 은 수신자를 동적인 개인 및 피어로 취급하여 정상으로 보이는 이메일이 명백한 악성임을 밝힘으로써 '정상 상태' 에서 벗어난 미묘한 이상 행동을 탐지하는 독보적인 기술입니다 .

활용 사례:공급망 계정 탈취

탐지하기가 가장 어려운 공격 중 하나는 바로 외부 계정 탈취입니다 . 이 경우 범죄자는 신뢰할 수 있는 연락처의 이메일 자격 증명을 탈취하여 이메일 액세스 권한을 획득합니다 .

공격자는 일단 내부로 침투하면 과거에 주고받은 이메일 기록에 액세스하고 정상처럼 보이는 이메일을 생성할 수 있으므로 , 적당한 때에 이메일에 악성 링크나 첨부파일을 포함시킵니다 .

기존의 방어 체계는 이를 신뢰할 수 있는 사용자라고 판단하지만 Antigena Email 은 아니라고 보는 것입니다 . Antigena Email 은 학습한 행동 패턴의 컨텍스트 내에서 각 이메일을 분석하고 거의 눈에 띄지 않는 이상 행동도 탐지해냅니다 . 여기에는 다음 사항이 포함됩니다 (그러나 이에 한정되지는 않음):

비정상적인 로그인 위치 – Antigena Email 은 실제 발신자의 지리적 위치를 식별할 수 있는 IP 주소를 추출하여 , 신뢰할 수 있는 연락처의 과거 행동 패턴을 기반으로 해당 IP 가 드문 것인지를 판단합니다 . 보기 드문 로그인 위치가 그 자체로는 알림이나 자율 대응을 트리거하지는 않을 수 있지만 , 해당 시스템의 전반적인 예측과 이상 징후 점수를 통해 명백하게 드러납니다 .

보기 드문 링크 – 사용자는 보통 자신이 방문하고 신뢰하는 웹사이트의 링크를 공유하는 경향이 있습니다 . Antigena Email 은 내부 메일에서 이러한 링크를 관찰하여 조직의 컨텍스트에서 어떤 링크와 도메인이 드문 것인지 판단합니다 .

비정상적인 수신자 – Antigena Email 은 내부 및 외부 사용자와 피어 간 관계를 그래프로 나타내며 그 관계를 세분화된 수준에서 파악합니다 . 공격자가 조직 내 다수의 수신자에게 여러 이메일을 전송하는 경우 , Antigena Email 은 이 특정 그룹이 동일 소스에서 이메일을 수신할 가능성을 판단합니다 .

이상 징후 행동 – 시간이 지날수록 Antigena Email 은 발신자의 이메일 작성이 얼마나 다른지를 학습하여 숨겨진 이메일 메타데이터와 본문의 패턴을 분석합니다 . Darktrace 는 AI 를 모든 인바운드 이메일에 적용하여 실제 계정 소유주가 아닌 사람이 이메일을 보냈음을 나타낼 가능성이 있는 미묘한 변화를 식별합니다 .

Antigena Email 은 이러한 취약 지표들의 상관성을 분석하여 신속히 포괄적인 이상 징후 점수를 도출하므로 , 해당 이메일이 악성이라고 확정하여 피해를 입기 전에 이를 무력화할 수 있습니다 .

30 일 무료 평가판으로 직접 Antigena Email 사용해보기

지금 데모 예약하기