Proofpoint Threat Response Auto-Pull

악성 이메일 전송 후 자동 격리

주요 이점

- 경계 솔루션을 우회하는 악성 이메일 자동 격리
- 메일 보안 오케스트레이션 및 대응 시 보안 및 메시지 팀이 소요하는 시간을 크게 절감
- 메시지 분류에 Proofpoint 위협 인텔리전스 활용
- 악용 메일함에 대한 위협 자동 모니터링
- 개인 또는 배포 목록에 전달된 메시지 격리
- 부분적으로 신고된 피싱 캠페인 추적 및 잘못 신고된 메시지에 불필요하게 소요하는 시간 제거

Proofpoint TRAP(Threat Response Auto-Pull)을 사용하는 메시지 및 보안 관리자는 이메일 사고 대응 프로세스를 간소화할 수 있습니다. 악성 이메일이 감지되면 TRAP가 이를 분석하고 자동으로 제거합니다. 또한 사용자의 받은 편지함에 도달한 원치 않는 이메일을 격리하기 위해 조치를 취합니다. Proofpoint TRAP를 사용하면 보안 및 메시지 팀이 이메일을 정리하는 데 필요한 시간을 줄일 수 있습니다.

이메일은 1순위 공격 벡터입니다. 이메일은 데이터 유출의 90% 이상을 담당합니다. 이메일 기반 위협이 더욱 지능화되면서 조직은 점점 더 많은 악성 메시지에 직면하고 있습니다. 이러한 이메일에는 전달 후 활성화되는 피싱 링크가 포함되어 있을 수도 있고, 고급 기술을 사용하여 탐지를 회피할 수 있으며, 이로 인해 위음성이 발생하고 최종 사용자에게 이메일이 전달될 수 있습니다. 위협 위험을 줄이고 침해로 인한 잠재적 영향을 최소화하기 위해 이메일 보안 팀은 이러한 악성 이메일을 분석하고 정리해야 합니다. 적은 수의 이메일을 처리하는 데는 그다지 시간이 많이 걸리지 않을 수 있지만, 수백 또는 수천 개의 악성 이메일과 관련된 사고는 보안 팀을 빠르게 압도하고 관리하기 너무 지루해질 수 있습니다.

전달 및 배포 목록 확장

TRAP는 관리자가 다른 사람에게 전달되는 악성 또는 원치 않는 이메일을 처리하는 데 도움이 됩니다. TRAP에는 메시지가 배포 목록에 전달되거나 전송되는 시기를 감지할 수 있는 로직이 내장되어 있습니다. 그리고 TRAP는 수신자 목록을 자동으로 확장하여 메시지를 찾아내고 취소합니다. 전달된 이메일 취소 프로세스를 자동으로 처리하면 관리자가 많은 시간과 노력을 절약할 수 있습니다.

유연한 배포 옵션

TRAP는 Proofpoint에서 호스팅하는 클라우드에 배포할 수 있습니다. 또는 VMware 및 AWS를 통해 온프레미스에 배포할 수도 있습니다. 이러한 유연성을 통해 TRAP는 Microsoft 365, Exchange 및 Google Workspaces와 같은 다양한 이메일 시스템과 함께 사용할 수 있습니다. 보다 현대적이고 편리한 옵션은 클라우드 배포입니다. 자동화된 소프트웨어 업데이트로 인해 설정에 드는 수고가 적고 유지 관리 비용도 절감됩니다.

대역 외 이메일 관리

TRAP를 사용하면 보안을 위협하거나 회사 정책을 위반할 수 있는 이메일을 격리할 수 있습니다. CSV 파일, Proofpoint Smart Search 또는 수동 사고 신고서를 사용하여 이 작업을 수행합니다. 몇 가지 주요 정보를 제공하면 TRAP가 사용자의 메일함에서 지정된 이메일을 신속하게 제거합니다. 또한 이메일을 읽은 주체와 리콜 시도의 상태를 표시하는 활동 목록도 제공합니다. 이는 잠재적으로 유해하거나 부적절한 이메일을 신속하게 식별하여 유포되지 않게 하는 데 도움이 됩니다.

Proofpoint Nexus 위협 그래프를 통한 교차 벡터 인텔리전스 공유

Proofpoint Nexus 위협 그래프는 이메일, 클라우드, 네트워크, 소셜 미디어와 같은 다양한 소스의 위협 데이터를 집계하고 상호 연관시킵니다. 모든 Proofpoint 제품에 대한 실시간 보호 및 대응을 제공합니다. 그리고 Proofpoint 플랫폼에 통합됩니다. 따라서 추가 설치나 관리가 필요하지 않습니다.

이 네트워크의 일원이 되면 다음과 같은 이점을 누릴 수 있습니다.

- 115,000명 이상의 고객이 제공하는 실시간 커뮤니티 위협 인텔리전스
- 이메일, 클라우드, 네트워크 및 소셜 미디어 전반에 걸친 다중 벡터 가시성
- 100명 이상의 추적 위협 행위자에 대한 정보를 통해 위협 요소의 동기와 전술 파악

TRAP는 Nexus 위협 그래프의 인텔리전스를 사용하여 수신자를 사용자 ID와 연결합니다. 또한 연관된 캠페인을 찾아내고 공격에 사용된 IP 주소와 도메인을 식별합니다. 이 정보를 기반으로 TRAP는 특별한 권한을 가진 특정 부서 또는 그룹에 속한 대상 사용자에 대해 자동화된 조치를 취할 수 있습니다. 고객 사이트에서 링크, 첨부 파일 또는 의심스러운 IP가 포함된 악성 이메일을 탐지하면 향후 보호를 위해 이 정보를 전체 고객 기반과 공유하고 사용자의 받은 편지함에 전달된 모든 메시지를 격리합니다.

향상된 분류

Proofpoint Browser Isolation 기술을 사용하여 URL을 안전하게 조사하는 TRAP의 기능은 분석가의 사고 분류 프로세스를 향상시킵니다. 이 기술을 통해 분석가는 조직을 위험에 노출시키지 않고 URL의 내용을 평가할 수 있습니다. 이를 통해 URL과 관련된 사고를 신속하고 정확하게 평가할 수 있으며, 조직을 보호하기 위해 적절한 조치를 취할 수 있습니다.

Closed-Loop Email Analysis and Response (CLEAR)

Closed-Loop Email Analysis and Response (CLEAR)는 사용자가 잠재적으로 악성일 수 있는 이메일을 신속하게 식별하고 처리하는 데 도움이 됩니다. PhishAlarm, PhishAlarm Analyzer, TRAP의 기능을 결합하여 신고된 메시지에 빠르고 효과적으로 대응합니다. CLEAR를 사용하면 신고된 이메일이 악용 메일함으로 전송됩니다. 그런 다음 Proofpoint 위협 인텔리전스 및 기타 소스와 비교하여 자동으로 분석되어 악성 콘텐츠가 포함되어 있는지 확인합니다. 일치하는 항목이 발견되면 해당 메시지는 수신자의 받은 편지함에서 제거되고 격리됩니다. 이는 적극적인 공격을 방지하고 조직을 보호하는 데 도움이 됩니다. 정보를 습득한 직원은 사이버 위협에 대한 중요한 방어선입니다. CLEAR는 단 몇 분 만에 잠재적인 위협을 신고하고 해결할 수 있도록 지원합니다.

자세한 정보

자세한 내용은 **proofpoint.com**을 참조하십시오.