

Proofpoint Account Takeover Protection

다단계 계정 탈취 탐지, 조사 및 대응

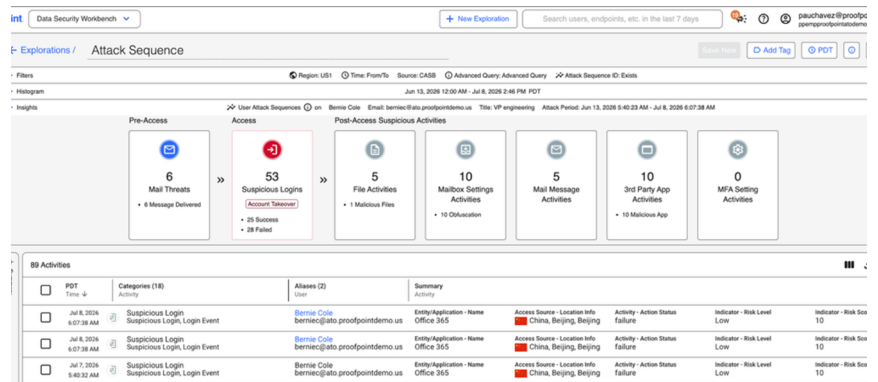
주요 내용

- 높은 정밀도로 다단계 계정 침해 탐지
- 공격 라이프사이클 전반에 걸친 통합 가시성으로 조사 가속화
- 자동화된 대응 및 수정을 통해 공격자의 체류 시간 단축
- 손상된 계정으로 인한 사기, 데이터 손실 및 비즈니스 중단 최소화
- Proofpoint Collaboration Security Prime으로 심층 방어 강화

Proofpoint Account Takeover Protection은 조직이 사전 액세스 지표와 성공적인 침해부터 사후 액세스 공격자 활동에 이르기까지 전체 계정 탈취(ATO) 라이프사이클 전반에서 손상된 사용자 계정을 탐지, 조사 및 차단하도록 지원합니다.

Proofpoint Nexus® AI 및 위협 인텔리전스를 기반으로 하는 Proofpoint Account Takeover Protection은 확인된 계정 침해에 대해 높은 신뢰도의 탐지 기능을 제공하는 동시에 공격자 행동에 대한 완벽한 가시성을 제공합니다. 보안 팀은 인시던트의 범위를 신속하게 파악하고, 조사를 가속화하며, BEC(비즈니스 이메일 사기 공격), 데이터 도난, 측면 이동 또는 기타 비즈니스에 영향을 미치는 공격으로 확대되기 전에 위협을 차단할 수 있습니다.

Proofpoint Collaboration Security Prime의 일부인 Proofpoint Account Takeover Protection은 Threat Protection Workbench 및 Threat Interaction Map과 통합되어 단일 손상된 계정을 넘어 조사를 확장합니다. 신원 침해를 이메일 위험, 사용자 상호 작용 및 공격자 활동과 연관시킴으로써 보안 팀이 공격 캠페인을 더 폭넓게 이해하도록 돕습니다. 이를 통해 더 빠른 조사, 더 정보에 입각한 대응 결정 및 더 강력한 복구가 가능해집니다.



1. 그림 1. 사전 액세스부터 사후 액세스 활동까지 ATO 공격 라이프사이클 전반에 걸친 포괄적 가시성을 확보합니다.

고신뢰도 ATO 탐지

Proofpoint Nexus AI 기반의 Proofpoint Account Takeover Protection은 Microsoft 365, Google Workspace 및 Okta 전반에서 확인된 계정 침해에 대해 높은 신뢰도의 탐지 기능을 제공합니다.

사전 액세스 지표부터 사후 액세스 공격자 행동까지, 계정 탈취 라이프사이클 전반에 걸친 사용자 활동을 지속적으로 분석함으로써 Proofpoint Account Takeover Protection은 확인된 침해를 높은 신뢰도로 식별하고 위험 심각도(심각, 높음, 중간)에 따라 탐지 우선순위를 지정합니다. 각 탐지 결과에는 해당 결과의 근거가 되는 행동 지표와 증거가 포함되어 있어, 분석가가 계정이 침해된 것으로 식별된 이유를 신속하게 파악하고 대응 노력의 우선순위를 정하며 확신을 가지고 조치를 취할 수 있도록 지원합니다.

완벽한 공격 가시성

계정 침해가 확인되면 Proofpoint Account Takeover Protection은 공격 시퀀스에 대한 완벽한 가시성을 제공하여 보안 팀이 공격이 어떻게 전개되었는지, 그리고 공격자가 액세스 권한을 획득한 후 어떤 활동을 했는지 파악할 수 있도록 합니다.

포괄적인 포렌식 인사이트를 통해 액세스 이후 활동(메일함 조작, 악의적 받은 편지함 규칙, OAuth 남용, 권한 변경, 내부 피싱, 의심스러운 이메일 활동 및 지속성 기법 포함)을 파악할 수 있습니다. 이는 분석가가 공격의 범위, 정교함 및 도달 범위를 신속하게 파악하는 데 도움이 됩니다. Proofpoint Account Takeover Protection은 공격 시퀀스를 재구성하고 영향을 받는 사용자와 자산을 강조함으로써 조사를 가속화하고, 더 정보에 입각한 대응 결정을 지원하며, 복구를 개선하는 데 도움을 줍니다.

자동화된 위협 대응

Proofpoint Account Takeover Protection은 공격자의 액세스를 차단하고 복구를 가속화하는 자동화된 수습 조치를 통해 조직이 활성 위협을 신속하게 억제하도록 돕습니다. 대응 조치에는 강제 비밀번호 변경, 사용자 비밀번호 재설정, 활성 사용자 세션 취소, 악성 메일함 규칙 제거, 승인되지 않은 타사 OAuth 애플리케이션 취소, 그리고 공격자의 지속성을 제거하고 계정 무결성을 복원하도록 설계된 기타 수습 조치가 포함됩니다.

보안 팀은 중요한 억제 조치를 자동화함으로써 공격자의 체류 시간을 줄이고, 측면 이동을 제한하며, 비즈니스 중단을 최소화하고, 계정 침해로부터의 복구를 가속화할 수 있습니다.

Proofpoint Collaboration Security Prime을 통한 심층 방어

Proofpoint Collaboration Security Prime의 일부인 Proofpoint Account Takeover Protection은 계정 침해를 넘어 전체적인 인간 공격 라이프사이클 전반에 걸쳐 조정된 보호를 제공합니다. Proofpoint Account Takeover Protection은 침해된 계정을 탐지, 조사 및 억제하는 반면, Prime은 침해 전 위협을 예방하고, 이메일 및 협업 채널 전반의 공격을 상관 분석하며, 적응형 교육을 통해 사용자 행동을 개선하고, Threat Protection Workbench 및 Threat Interaction Map을 통해 통합된 조사 및 대응을 제공함으로써 보호 기능을 향상시킵니다.

이러한 기능들은 함께 심층 방어 전략을 지원하여 조직이 단일 통합 플랫폼에서 공격을 예방하고, 활성 위협을 완화하며, 사용자 복원력을 강화하고, 보안 태세를 지속적으로 개선할 수 있도록 돕습니다.

자세한 내용은 proofpoint.com/kr에서

Proofpoint, Inc. 소개 Proofpoint, Inc.는 사람 중심 및 에이전트 중심의 사이버 보안 분야의 글로벌 리더로서 이메일, 클라우드 및 협업 도구 전반에 걸쳐 사람, 데이터 및 AI 에이전트가 연결되는 방식을 보호합니다. Proofpoint는 Fortune 100대 기업 중 80개 이상, 10,000개 이상의 대기업, 그리고 수백만 개의 소규모 조직이 위협 차단, 데이터 손실 방지, 그리고 사람 및 SI 워크플로 전반에 걸친 회복력 구축을 위해 선택한 신뢰받는 파트너입니다. Proofpoint의 협업 및 데이터 보안 플랫폼은 모든 규모의 조직이 AI를 안전하고 자신감 있게 채택하면서 직원을 보호하고 역량을 강화할 수 있도록 도와줍니다. www.proofpoint.com/kr에서 자세히 알아보십시오.

Proofpoint에 문의하기: [LinkedIn](#)

Proofpoint는 미국 및/또는 기타 국가에서 Proofpoint, Inc.의 등록 상표 또는 상호입니다. 여기에 포함된 모든 다른 상표는 해당 소유주의 재산입니다.