CROWDSTRIKE

FALCON DISCOVER
IT 안전 관리 솔루션

네트워크상의 사용자와 구성요소를 실시간으로 확인할 수 있으며 사용자 환경 내의 시스템, 실행 중인 소프트웨어, 사용자 계정 활용 방식에 대해 정확한 인벤토리를 즉시 확인할 수 있습니다.

FALCON DISCOVER — 실시간 확인 기능 및 인벤토리 관리

네트워크상의 컴퓨터와 애플리케이션을 파악 및 추적해야 하는 IT 팀과 보안 팀에게 유용한 Falcon Discover™는 CrowdStrike™의 IT 안전 관리 솔루션입니다. Falcon Discover 는 시스템, 애플리케이션 사용, 사용자 계정 사용을 실시간으로 모니터링하고 인벤토리 목록을 작성합니다.

- **네트워크에 연결된 사용자를 언제든 확인 가능** — 실시간 시스템 인벤토리 기능으로 드릴다운 옵션을 갖춘 간편한 대시보드에서 해당 환경 내의 관리 장치 및 비관리 장치를 모두 확인할 수 있습니다.

- **사용자가 실행하는 애플리케이션을 파악** — 실시간 애플리케이션 인벤토리 기능을 사용하면 드릴다운 옵션을 갖춘 간편한 대시보드를 통해 해당 환경에서 실행되는 모든 애플리케이션을 확인할 수 있습니다. 엔드포인트에 영향을 미치지 않고 '현재' 어떤 호스트에서 어떤 앱이 실행 중인지 확인 가능합니다. 또한 애플리케이션이 처음 시작된 시간을 밝혀내고 같은 앱이 실행되는 다른 엔드포인트로 이동하여 더욱 풍부한 배경 정보를 확보하며 애플리케이션별 또는 호스트별 사용을 파악할 수 있습니다.

- **사용자 환경 전체에서 사용자 계정 접근이 이루어지는 지점과 방법을 확인** – 계정 모니터링 기능으로 기업 전반에 걸친 관리자 자격 증명 및 비밀번호 초기화 사용을 가시적으로 확인할 수 있습니다. Falcon Discover 는 자격 증명이 사용되는 로그온 추세(활동/기간)와 비밀번호 업데이트 정보에 대한 분석 정보를 제공합니다.

주요 이점

» 사용자의 자산과 애플리케이션에 대해 실시간 기록 확인 가능

» 더욱 효과적인 위협 대응 준비

» 비정상적 컴퓨터를 즉각적으로 파악

» 보호되지 않은 시스템 탐색

» 사용자가 실제로 사용하고 있는 애플리케이션 파악

» 권한 있는 계정에 접근이 수행되는 지점 확인

제품의 주요 기능

위협 대응 준비

- **선제적인 보안 태세 강화** — Falcon Discover 를 통해 사용 중인 부분을 파악할 수 있으므로 최적의 공격 대응 준비가 가능합니다. Falcon Discover 는 사용자 환경 내의 무단 시스템/애플리케이션 보고를 통해 공격에 앞서 보안 문제를 해결하므로 사용자의 보안 태세가 개선됩니다.

- **필요 없는 취약 애플리케이션 탐지** — 패치되지 않았거나 취약한 애플리케이션의 사용 여부를 탐지하므로 공격으로 피해를 입기 전에 패치를 진행할 수 있습니다.

- **보호되지 않는 비정상적 시스템 치료** — 시스템 인벤토리를 통해 관리되지 않는 시스템을 검색 및 치료하는 동시에 보호되지 않는 BYOD 또는 타사 시스템과 같이 사용자 네트워크에 위험 요소가 될 수 있는 시스템을 해결할 수 있습니다.

- **권한 있는 계정 악용 위험 완화** — 기업 전반에 걸쳐 관리자 자격 증명의 생성과 사용을 모니터링하며 해당 자격 증명이 부적절하고 상황에 맞지 않게 사용되고 있는지 여부를 탐지합니다.

보안 이외에도 다양한 효과

- **라이센싱 비용 감소** — 실시간 애플리케이션 인벤토리 기능으로 사용자의 애플리케이션 실행 빈도 및 지속 시간을 확인할 수 있어 라이센스 비용과 실제 요구사항의 균형을 잡을 수 있습니다.

- **규제 준수 요건 충족** — Falcon Discover 는 일부 규제 준수 요건 확보에 필요한 확인 및 인벤토리 기능을 완전 자동화하여 규제 준수 의무를 더욱 편리하게 달성하고 유지관리 및 증명할 수 있습니다.

즉각적인 가치 실현 —

- **시간, 노력, 비용 절감** — 클라우드 방식의 Falcon Insight 는 CrowdStrike Falcon™ 플랫폼을 통해 제공되며 온프레미스 관리 인프라가 필요하지 않습니다.

- **즉각적인 가동** — Falcon Discover 는 재부팅이나 쿼리 작성, 기본 설정, 복잡한 구성 과정 없이도 몇 시간이면 구축할 수 있으며 설치하는 즉시 실행되어 모니터링 및 기록이 가능합니다.

- **성능 저하 없음** — 인벤토리 검색이 클라우드에서 이루어지며 엔드포인트와 네트워크에 영향을 미치지 않습니다.

예방적 보안 이상의 다양한 효과

보안 기능으로 보호가 이루어지지 않는 지점의 검색을 시작하므로 빈틈을 해결하고 더욱 효과적으로 위협 대응을 준비할 수 있습니다. Falcon Discover 는 보안 팀과 IT 팀이 오늘날의 정교한 위협에 대한 종합적 방어를 확보하는 데 필요한 확인 기능과 정보를 제공합니다.

CROWDSTRIKE

CrowdStrike 는 클라우드 제공 방식의 차세대 엔드포인트 보호 부문 최고의 기업입니다. CrowdStrike 는 차세대 안티바이러스, 엔드포인트 탐지 및 대응(EDR), 24 시간 관리형 위협 사냥 서비스를 통합하고 단일 경량 에이전트를 통해 제공하는 최초이자 유일한 기업으로 엔드포인트 보호 부문의 혁신을 이루어냈습니다.

자세히 알아보기:

www.crowdstrike.com