CROWDSTRIKE
ENDPOINT SECURITY

엔드포인트 보호와 가시성을 통해 완벽한 보안 침해 방지

개요

매년 전세계에서 생성되는 Malware 의 수는 수십억개에 이르고 있습니다.이러한 방대한 양의 Malware 를 탐지하기 위해 AV 의 시그니처가 효과가 있을까요? 또한, 현재 사이버 위협은 Malware-free 형태의 공격으로 변화되고 있어 시그니처 자체로는 더 이상 지능화된 공격을 탐지 및 차단 할 수 없습니다.

CrowdStrike Endpoint Security 는 인공지능/머신러닝 기반 AV (NGAV), 엔드포인트 탐지 및 대응 (EDR), 관리형 위협 헌팅, 통합 위협 인텔리전스 등 다양한 기능을 결합하여 침해를 차단합니다.

CrowdStrike 조직 내 **Overwatch** 팀은 침해 위험을 24/7/365 상시 모니터링하고 사용자에게 공격 징후와 대응방법을 알려줌으로써 보안 침해를 사전 방지 하도록 도와줍니다.

기술적 특징

단일화된 경량 에이전트

- 복잡한 AGENT 감소 + No 시그니쳐 - 성능 저하없이 모든 워크로드 보호(CPU 1%/ Mem 40MB)

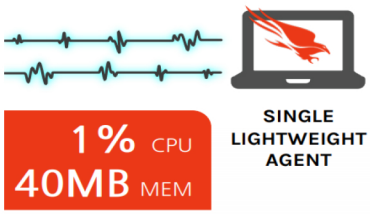

그림 1. 단일화 된 경량 에이전트

MULTI OS

Windows, Mac, Linux, iOS, Android, Cloud workload, Container 지원

PREVENTION

머신 러닝 , 취약점 차단, IOA (Indicators Of Attack) 기술 결합

DETECTION & RESPONSE

실시간 수집, 빠른 검색, 실시간 대응, 위협 헌팅 서비스 제공

IT HYGENE & VULNERABILITY 관리

자산 관리, 사용자 관리, 어플리케이션 관리/ 취약점 관리

위협 그래프

- 400여개 이벤트 타입을 매주 약 3.5조개 위협 데이터를 수집하고 강력한 AI 기반으로 데이터 분석
- AI, 머신러닝 분석으로 사이버 위협 공격 유형별, 그룹별 분류하고 최적의 대응 방안 안내

클라우드 전용 보안 플랫폼

- 신속한 구현과 확장성 용이, 대량 검색
- 클라우드 기반 위협 헌팅 엔진으로 과거의 공격으로부터 학습하여 사전 대응 가능
- 위협 인텔리전스 정보 제공과 엔드포인트 보호 기능이 자동 연계되어 빠른 조사/대응 구현

FALCON PLATFORM ENDPOINT SECURITY

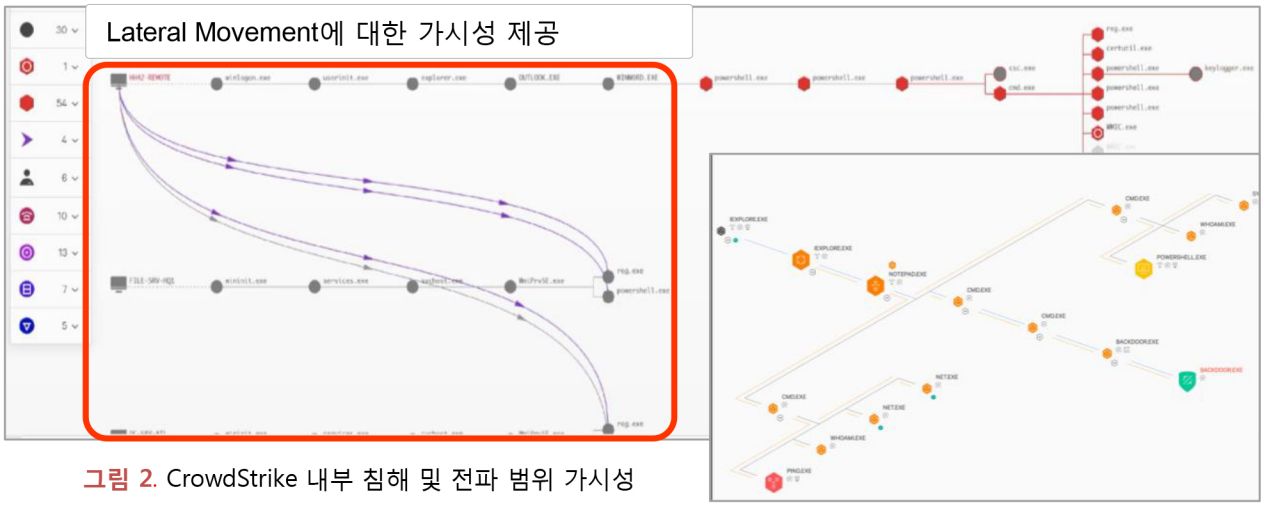

그림 2. CrowdStrike 내부 침해 및 전파 범위 가시성

주요 서비스

그림 3. Endpoint Security 주요 서비스

FALCON PREVENT
Next-Generation Antivirus
차세대 백신 (NGAV)

FALCON OVERWATCH
Managed Threat Hunting
관리형 위협 헌팅 (MTH)

FALCON INSIGHT
Endpoint Detection & Response
엔드포인트 탐지 및 대응(EDR)

FALCON PREVENT	• 인공지능/머신 러닝 기반 차세대 통합 안티 바이러스 서비스
FALCON INSIGHT	• 실시간 분석, 자동 처리, 독보적인 가시성 기반 위협 탐지/대응 서비스
FALCON OVERWATCH	• 확장된 가시성으로 완벽한 엔드포인트 보안 관리형 위협 헌팅 서비스

주요 이점

강력한 위협 방어	전문성 결합	복잡성 단순화	즉각적인 가치 실현
• 정교한 방어 기술 • 위협 인텔리전스 내장 • 위협 분석가 전문성	• 전문적 위협 헌팅 • 전반적인 방어 및 개선 관리 • 위협 인텔리전스	• 통합 에이전트 • 아키텍처 단순화 • 운영 간소화	• 즉시 적용 솔루션 • 손쉬운 배포 • 컨설팅 불필요

제품문의 : 02-2105-4547 / security-sales@isd.co.kr