한눈에 보기

이점

- 클라이언트 간, 서버 간, 클라이언트-서버간 트래픽을 비롯한 모든 네트워크 상호작용을 통해 가시성을 확보하여 내부 위협과 외부 위협을 모두 탐지
- 강화된 보안 분석을 수행하고 심층적인 컨텍스트를 확보하여 공격을 의미할 수 있는 다양한 이상 행동 탐지
- 전체 네트워크에서 위협 탐지, 사고 대응, 포렌식 가속화 및 향상
- 네트워크 활동에 대한 감사 기록을 통해 심층적인 포렌식 조사 지원
- 네트워크 전반의 가시성을 확장하여 규정준수, 네트워크 분할, 성능 모니터링 및 용량 계획 간소화

Lancope StealthWatch System

네트워크 전반의 가시성을 향상하여 위협 탐지 강화

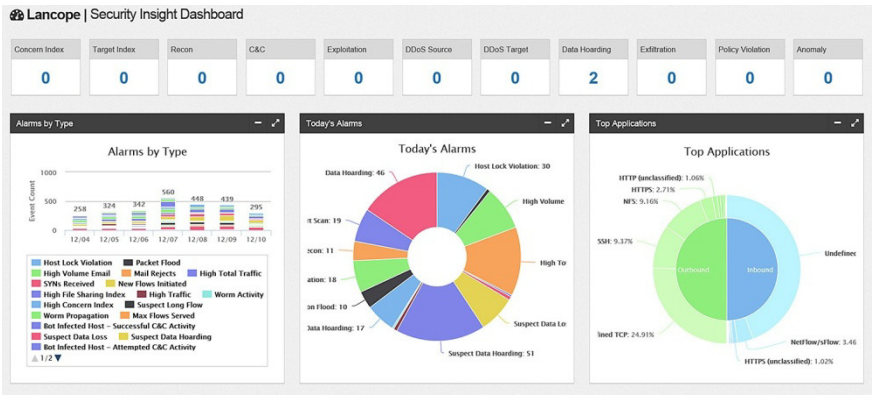
오늘날 엔터프라이즈 네트워크는 그 어느 때보다도 더 복잡하고 분산되어 있습니다. 매주 새로운 보안 당면 과제가 발생합니다. 지속적으로 발전하는 위협 환경과 클라우드 컴퓨팅, IoT(Internet of Things) 등과 같은 트렌드로 인해 상황은 더욱 복잡해지고 있습니다. 안타깝게도, 점점 더 많은 사용자와 디바이스가 네트워크에 추가되면서 네트워크에 일어나는 일을 파악하는 것이 더욱 어려워졌습니다. 또한 보이지 않는 것을 보호할 수는 없습니다.

네트워크에서 이상 행동이 발생할 수 있는지 여부를 확인하려면 알려지거나 알려지지 않은 모든 트래픽 플로우, 애플리케이션, 사용자 및 디바이스를 들여다 봐야 합니다. StealthWatch 시스템에서는 정교한 행동 분석을 사용하여 기존 인프라의 데이터를 실행 가능한 인텔리전스로 변환하여 네트워크 가시성과 보안을 향상하고 사고 대응을 가속화합니다.

사고 대응 및 포렌식 가속화를 위한 지속적인 네트워크 트래픽 분석

StealthWatch 시스템은 네트워크 전반의 의심스러운 사고에 대한 네트워크 가시성, 보안 및 대응 시간을 획기적으로 개선합니다. 보안 운영 직원이 네트워크, 데이터 센터, 클라우드에서 모든 사용자, 디바이스 및 트래픽에 대한 실시간 상황을 인식하도록 도와줍니다. 또한 모든 네트워크 트래픽에 대한 지속적인 실시간 모니터링과 포괄적인 보기를 제공하여 보안 팀에서 보안 사고 전, 중, 후에 위협에 빠르고 효율적으로 대응할 수 있도록 지원합니다.

StealthWatch에서는 컨텍스트 인식 보안 분석을 적용하여 이상 행동을 자동으로 탐지함으로써 악성코드, 제로 데이 공격, DDoS(Distributed Denial-of-Service) 시도, APT(Advanced Persistent Threat), 내부자 위협을 비롯한 다양한 공격을 식별할 수 있습니다.



"StealthWatch에서는 구축과 동시에 부정행위를 하는 400개의 호스트를 파악하고 네트워크 위협을 90% 줄일 수 있도록 도와주었습니다."

Dartmouth College

"MEMC Electronic Materials, Inc.에서는 StealthWatch를 통해 네트워크 기준 설정, 실시간 위협 탐지, 사고 대응, 포렌식 조사, 네트워크 문제 해결 능력이 향상되었습니다."

Brian Barry
보안 관리자,
MEMC Electronic Materials, Inc.

"Lancope의 StealthWatch 시스템은 네트워크 내에서 실제로 발생하고 있는 일들에 대한 통찰력을 제공하고, 표준 플로우 데이터를 사용하여 보고 이력과 향상된 문제 알림을 최적의 조합으로 결합하는 제품입니다."

Steve Mould
선임 IT 설계자, Experian

StealthWatch에서는 이 모든 작업을 수행하기 위해 다음을 제공합니다.

- 네트워크 경계, 내부, 데이터 센터, 프라이빗 및 퍼블릭 클라우드에 대한 심층적 가시성
- NetFlow를 사용하여 이상 행동을 쉽게 파악할 수 있는 기준을 설정함으로써 정상적인 네트워크 동작을 간편하게 파악
- 분산된 네트워크에서 디바이스, 애플리케이션 및 사용자를 지속적으로 모니터링
- 강화된 보안 분석 및 인텔리전스를 제공하여 공격을 의미할 수 있는 다양한 이상 행동 탐지
- 실시간 위협 탐지를 통해 사고 대응 시간 가속화
- 포괄적인 네트워크 감사 추적을 통한 탁월한 포렌식 조사
- 네트워크 계획, 세그멘테이션, 진단 및 규정준수 검증을 위한 간소화된 기능
- Cisco TrustSec® 기술을 지원하는 네트워크 인프라, Cisco® ISE(Identity Services Engine) 및 하드웨어와 통합하여 Network as a Security Sensor 및 Enforcer 사용

다음 단계

StealthWatch에서는 대용량의 네트워크 데이터를 수집 및 분석하여 아무리 크고 동적인 네트워크에 대해서도 포괄적인 가시성과 보호를 제공합니다. StealthWatch에 대한 자세한 내용을 알아보려면 www.cisco.com/go/stealthwatch를 방문하거나 현지 Cisco 어카운트 담당자에게 문의하십시오.

C45-736510-00 01/16