한눈에 보기

"Cisco Identity Services Engine은 매우 유연한 운영 액세스 관리를 제공함과 동시에 네트워크에 대한 무단 액세스를 전부 차단했습니다."

Mirko Berlier,
Cisco 엔지니어 겸 Expo 2015 아키텍트

"Stealthwatch에 내장된 행동 경보는 예전에 없었던 완전히 새로운 탐지 기능을 제공합니다."

Mike Sheck,
사고 대응팀
Cisco CSIRT

Stealthwatch 및 ISE를 통해 진정한 가시성 확보

성장 동력으로서 보안을 활용

조직은 모빌리티, 사물인터넷(IoT), 클라우드, 첨단 분석 등의 트렌드에 힘입어 디지털화의 이점을 누리기 위해 앞다투어 경쟁하고 있습니다. 이러한 이점의 핵심은 네트워크를 디지털 발전 속도에 맞추고 위협으로부터 조직을 안전하게 보호하는 것입니다. 기업은 보안에 대한 확신이 있을 때 혁신이 가능하며 새로운 기술을 도입하고 새로운 서비스를 개발할 수 있습니다. 안타깝게도 최근 설문 조사에 따르면 조직의 39%가 사이버 보안 우려 때문에 미션 크리티컬한 이니셔티브를 중단한 경험이 있다고 합니다.

설령 시스템이 감염되었다는 사실을 알게 되더라도 네트워크 남용과 내부 위협에 취약하게 만드는 공격이 어디에서 진행되는지, 또 어떻게 진행되는지 항상 알 수는 없습니다. 조직은 위협 탐지 및 대응 속도를 높이기 위해 풍부한 사용자 및 디바이스 세부 정보를 바탕으로 광범위한 네트워크 가시성을 제공하는 솔루션이 필요합니다.

Stealthwatch와 Cisco Identity Services Engine만이 360° 보기를 확인하고 위협에 신속하게 대응하며 성장하는 디지털 비즈니스를 보호하도록 지원할 수 있습니다.

360°로 보기

더 신속하게 위협에 대응

성장하는 디지털 비즈니스를 보호

360°로 보기

Stealthwatch 및 ISE를 통합하여 탁월한 가시성과 제어를 확보할 수 있습니다.

- Stealthwatch를 통해 네트워크에서 호스트와 사용자 정보를 지속적으로 모니터링, 분석, 분리, 범주화 및 저장할 수 있습니다.
- ISE를 통해 관리자는 각 개별 디바이스 유형, 운영 체제, 컴플라이언스 상태, 연결 방법, 지리적 위치 등에 대한 세부 정보를 확인할 수 있습니다.
- 환경에서 이상 트래픽을 발견할 수 있습니다. Stealthwatch는 이상 행동을 자동적으로 탐지하도록 상황 인식 보안 분석을 적용하여 악성코드, 제로데이 공격, DDoS(Distributed Denial-of-Service) 공격, APT(Advanced Persistent Threat), 내부자 위협을 비롯한 다양한 공격을 식별할 수 있습니다.
- 언제 개별 사용자가 의심스러운 행동을 했는지 정확히 알 수 있습니다. Stealthwatch를 통해 관리자는 자신만의 임계값을 설정하여 사용자가 해당 임계값을 넘으면 경보를 유발할 수 있습니다.

의료 분야를 선도하는 한 회사에서 ISE와 Stealthwatch를 사용해 가시성을 확보하고 사이버 공격을 예방하고 있습니다.

당면 과제:

- 네트워크 전반에서 500개의 사이트와 25만 개의 디바이스 보호
- 네트워크 위협에 대한 가시성 및 제어 확보
- HIPAA 컴플라이언스 요건 충족

해결책:

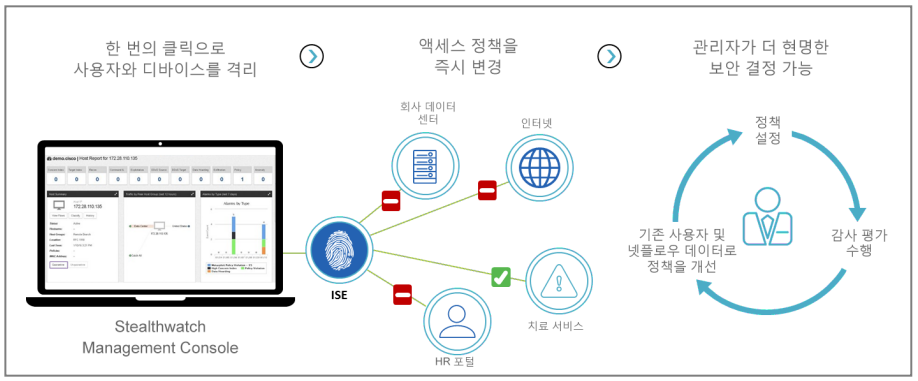
- Cisco ISE와 Stealthwatch를 이용하여 NaaS(Network as a Sensor) 및 NaaE(Network as an Enforcer) 역할 가능
- 네트워크 세그멘테이션 및 사용자 액세스 제어 정책 시행

결과:

- 예정보다 6개월 앞서 전 사이트 구축 완료
- 며칠씩 걸리던 위협 대응 시간이 단 몇 분으로 단축
- 정보 안전 및 HIPAA 표준 준수 가능

Rapid Threat Containment를 이용한 대응

보안이 아무리 발전하더라도 모든 위협을 다 차단할 수는 없습니다. 솔루션은 더 큰 벽을 세우는 것이 아니라 대응 속도를 높이는 것입니다.



- Stealthwatch가 비정상적인 트래픽을 탐지하면 경보를 발행하여 관리자에게 사용자를 격리하는 옵션을 제공합니다. Stealthwatch는 pxGrid를 통해 격리 명령을 직접 ISE에 내릴 수 있습니다.
- 관리자는 분석을 기반으로 결정을 내릴 수 있어서 사용자 액세스를 취소하거나 ISE를 통해 단 한 번의 클릭으로 사용자를 격리할 수 있습니다. ISE가 격리된 개인의 액세스 정책을 다시 할당하기 때문에 관리자는 전체 시스템 정책을 수정하거나 변경할 필요가 없습니다.
- 사후 감사 추적으로 보안 침해의 침입 경로를 찾습니다. Stealthwatch는 짧게는 수개월, 길게는 수년간 모든 네트워크 활동 기록을 저장합니다.

신속한 위협 대응에 대한 자세한 내용은 www.cisco.com/go/rtc를 참조하십시오.

성장하는 디지털 비즈니스를 보호

기업이 새로운 이니셔티브나 기술을 더욱 자신감 있게 추진 하려면 새로운 보안 문제없이 확장할 수 있다고 확신할 수 있어야 합니다.

- 보안을 장애 요소로 여기지 말고 안전한 액세스 및 가시성을 위해 네트워크 세그멘테이션의 기반을 마련해야 합니다.
- 관리자가 민감한 자산에 대한 액세스를 신중하게 제어하고 언제, 누가 정보에 액세스하려고 했는지 정확하게 파악하고 네트워크, 환경, 클라우드와 관련된 새로운 영역에 대한 가시성을 확장할 수 있습니다.
- 네트워크 가시성을 손상시키지 않으면서 사용자, 디바이스, 비지니스를 추가합니다. ISE에서 끊임없이 업데이트하는 디바이스 프로필 피드를 통해 관리자가 새로운 디바이스를 설정해야 하는 부담을 덜어줍니다.
- 사각지대를 생성하지 않고 환경을 확장합니다. Stealthwatch 구축은 플로우 스티칭 및 중복 제거와 동시에 600만 fps 속도로 5만 플로우 소스 데이터 처리가 가능합니다.
- 사일로 관리 소스와 관련된 관리자의 부담을 덜어줍니다. 네트워크 전반의 플로우는 Stealthwatch Management Console에서 중앙 집중적으로 표시됩니다. REST API를 통해 서드파티 기술과 서비스를 쉽게 통합할 수 있습니다.

다음 단계

자세한 내용을 알아보려면 www.cisco.com/go/Stealthwatch, www.cisco.com/go/ise를 방문하십시오.