Cisco Stealthwatch Cloud

프라이빗 네트워크, 퍼블릭 클라우드 및 하이브리드 환경 보호

2017년 Cisco 연간 사이버 보안 보고서에 따르면, 보안 경고 중 56%만 조사되었으며 그중 절반 이상이 해결되지 않은 상태로 남아 있다고 합니다. 보안 경고에 대응하기란 까다로운 일이며, 대부분의 조직에는 이를 처리할 수 있는 보안 직원조차 없습니다. 또한 규모에 관계없이 모든 기업이 온프레미스 인프라는 물론, 퍼블릭 클라우드 환경을 보호해야 하는 까다로운 문제에 직면해 있습니다.

이를 해결하기 위해서는 오탐 수를 줄이는 솔루션과 더불어, 퍼블릭 클라우드 워크로드를 효과적으로 보호하는 보안 수단을 보완하는 것이 시급합니다. 하지만 퍼블릭 클라우드 인프라는 온프레미스 인프라와는 성격이 다릅니다. 퍼블릭 클라우드는 자산 변동률이 매우 높지만 네트워크 모니터링 기능을 그다지 많이 제공하지 않습니다. 오탐 수를 줄이는 동시에 효과적인 보안을 제공하려면 새로운 접근 방식이 필요합니다.

특정 직원의 클라우드 자격 증명 정보가 피싱이나 다른 방법으로 침해되었다고 상상해 보십시오. 이 직원이 다른 나라에서 로그인해서 이런 일이 발생한 것인지, 아니면 다른 원인이 있는 것인지 확인할 수 있는 방법이 있습니까? Cisco® Stealthwatch Cloud는 이러한 유형의 악의적인 활동을 실시간으로 식별할 수 있도록 실행 가능한 보안 인텔리전스와 가시성을 제공합니다. Stealthwatch Cloud를 통해 보안 사고가 치명적인 보안 침해로 발전하기 전에 빠르게 대응할 수 있습니다.

또한 프라이빗 네트워크부터 지사, 퍼블릭 클라우드에 이르기까지 사용자 환경 전반에서 내/외부 위협을 탐지할 수 있습니다. Stealthwatch Cloud는 클라우드에서 제공되는 SaaS(Software-as-a-service) 솔루션으로, 사용이 쉽고 구매가 간단하며 운영 및 유지관리가 간편합니다. 데이터를 수신하면 더는 구성 작업이나 디바이스 분류 작업을 필요로 하지 않습니다. 또한, 모든 분석이 자동화됩니다.

이점

- **실행 가능한 인텔리전스:** 프라이빗 네트워크부터 퍼블릭 클라우드에 이르기까지 사용자 환경 전반에 대한 가시성을 통해 확보
- **신속한 탐지:** 지능형 위협과 보안 침해 지표를 빠르게 인식
- **비즈니스 보안 강화:** 보안 강화와 동시에 운영 오버헤드 감소
- **오탐 비율 대폭 감소:** 기본적인 관찰을 통한 하이파이(Hi-Fi) 경고 활용
- **한층 강력한 보안:** 퍼블릭 클라우드를 포함하여, 엔터프라이즈 전반의 보안 강화

"우리는 개선된 네트워크 보안 모니터링 방법을 찾고 있었습니다. 이 서비스를 사용한 결과, VPC 내 모든 디바이스를 포함하여 관련 네트워크 활동을 더 꼼꼼하고 자세하게 파악할 수 있게 되었습니다. 또한 의심스럽거나 비정상적인 동작을 발견하면, 빠르게 조치하여 잠재적 문제를 해결할 수도 있습니다."

-Taylor Higley,
미국 공무원 연합
국장

엔티티 모델링을 통한 사용자 환경 보호

위협은 끊임없이 진화하고 있습니다. 미래의 공격을 탐지하기 위해서는 이보다 한발 앞선 보안 솔루션이 필요합니다. Stealthwatch Cloud는 네트워크 내에서 발생하는 동작을 바탕으로 위협을 탐지하는 행동 모델링 방식을 사용합니다. 예를 들어, 도메인 컨트롤러가 FTP(File Transfer Protocol)를 사용하여 데이터를 전송하기 시작했다면, 이는 보안 침해의 첫 번째 징후일 가능성이 큽니다. Stealthwatch Cloud는 이 행동을 실시간으로 탐지하고 사용자에게 경고를 보냅니다.

Stealthwatch Cloud는 동적 학습을 활용하여 각 디바이스 및 네트워크 엔티티에 대한 일종의 시뮬레이션 같은 모델을 생성합니다. 이 모델의 기능은 다음과 같습니다.

- 특정 엔티티의 행동을 바탕으로 엔티티의 역할을 동적으로 확인한 후 해당 역할에 부합되지 않는 활동을 탐지
- 행동과 데이터 전송 및 액세스 특성과 관련하여 비정상적이고 갑작스러운 변화를 식별
- 유사한 디바이스와 다르게 행동하는 엔티티가 있을 경우 탐지
- 프로토콜과 포트 사용, 디바이스와 리소스 프로파일 특성 및 블랙리스트에 있는 통신을 포함한 조직의 정책을 엔티티가 위반할 경우 이를 식별
- 과거 활동을 기반으로 호스트 행동이나 디바이스 행동을 예측하고 그러한 예측과 관찰된 행동을 비교하여 평가

Stealthwatch Cloud의 이러한 기능 덕분에 직원은 원인 파악을 위해 직접 로그 데이터를 분석하는 데 시간을 쏟기보다는, 문제를 해결하는 데 더 많은 시간을 쓸 수 있습니다.

퍼블릭 클라우드에서의 위협 탐지

조직에서 점점 더 많은 IT 리소스를 퍼블릭 클라우드로 옮기고 있기 때문에, 클라우드 자산을 표적으로 하는 위협 요소를 탐지하기 위한 가시성을 높여야 합니다. 또한 사용하기 쉽고 효율적으로 운영할 수 있는 솔루션이 필요합니다. Stealthwatch Cloud의 퍼블릭 클라우드 모니터링은 AWS(Amazon Web Services) 및 Microsoft Azure 환경에서 워크로드를 매우 안전하게 보호하는 데 필요한 가시성과 위협 탐지 기능을 제공합니다.

Stealthwatch Cloud의 퍼블릭 클라우드 모니터링은 Amazon VPC(Virtual Private Cloud) 플로우 로그를 포함해 AWS의 텔레메트리 네이티브 소스를 사용하여, 소프트웨어 에이전트 필요 없이 클라우드 내 모든 활동을 모니터링합니다. 이러한 환경에서 서비스 가용성을 저해하지 않고 수분 정도의 짧은 시간 내에 Stealthwatch Cloud를 배포할 수 있습니다.

Stealthwatch Cloud는 이 데이터를 활용하여 각 클라우드 리소스의 행동을 모델링(엔티티 모델링이라고 함)합니다. 이 모델링을 통해 갑작스러운 행동 변화, 악의적인 활동, 보안 침해 징후를 탐지할 수 있습니다.

지금 바로 환경 보호

위험성이 없는 무료 평가판으로 지금 Stealthwatch Cloud를 사용해 보십시오. 자세한 내용을 보려면, https://www.cisco.com/go/stealthwatch-cloud를 방문하거나, 해당 지역 Cisco 어카운트 담당자에게 문의하십시오.

프라이빗 네트워크도 함께 보호

이제 네트워크 가시성 및 위협 탐지는 대규모 엔터프라이즈만을 위한 기능이 아닙니다. Ponemon Institute에서 직원이 1000명 미만인 기업을 대상으로 진행한 설문조사에 따르면, 응답자 55%가 지난해 사이버 공격을 경험했으며 약 1/3이 보안 침해의 근본 원인을 파악하지 못했다고 합니다. Stealthwatch Cloud의 프라이빗 네트워크 모니터링은 고가의 장비나 IT 리소스 없이도, 보안 담당 직원의 업무를 늘리지 않고도, 실시간으로 네트워크에 대한 위협을 탐지할 수 있는 우수한 가시성을 제공합니다.

Stealthwatch Cloud는 수많은 네트워크 텔레메트리와 로그를 수신합니다. 또한 엔티티 모델링을 기반으로 각 네트워크 엔티티의 역할과 엔티티의 정상 행동을 파악합니다. 엔티티가 이전과 다른 비정상적인 행동을 보이거나 악의적인 활동의 징후를 보이면 경고가 생성되므로 보안 전문가가 빠르게 조사에 착수하여 대응할 수 있습니다.

C45-739611-00 09/17