Cisco XDR로 보안 운영 간소화

더 많은 탐지, 더 빠른 조치, 생산성 향상

Cisco XDR은 탐지와 대응에 대한 보안 팀의 시각을 변화시킵니다. Cisco의 클라우드 기반 솔루션은 보안 운영을 간소화하고 보안 팀이 가장 정교한 위협을 탐지하고 우선순위를 지정하며 위협에 대응할 수 있는 역량을 강화해 줍니다. 광범위한 Cisco 보안 포트폴리오 및 타사 서비스와 통합되는 Cisco XDR은 현존하는 솔루션 중 가장 포괄적이고 유연합니다.

보안 실무자를 위해 보안 실무자가 설계한 Cisco XDR은 분석가가 여러 소스로부터 데이터를 집계하고 데이터의 상관관계를 파악하여 하나의 통합된 뷰에 종합함으로써 조사를 간소화하고, 오탐을 줄이고, 탐지에서 대응까지 가장 빠른 경로를 구축할 수 있도록 해줍니다.

구축 당시 기본으로 내장되는 자동화와 오케스트레이션, 가이드형 해결 권장 사항 덕분에 분석가가 반복적인 작업을 자동화하고, 더욱 효과적으로 위협을 완화할 수 있으므로 시간과 리소스를 절약하여 다른 중요한 보안 작업에 집중하는 데 활용할 수 있습니다.

데이터를 기반으로 하는 Cisco XDR 접근법을 통해 SOC 팀은 가장 영향력이 큰 이벤트를 정의하여 우선적으로 해결 전략을 집중시키므로 조직의 전반적인 보안 태세가 강화되고 회복탄력성이 높아집니다.

이점

벤더나 벡터가 무엇이든 가시성을 통합하여 사각지대 예방

네트워크, 클라우드, 엔드포인트, 이메일, 애플리케이션 전체에서 가시성을 확보하고 위협을 식별하여 여러 벤더 및 여러 벡터가 포함된 환경에서 보안을 효과적으로 구현합니다.

Cisco XDR을 사용하면 분산된 여러 개의 탐지 기술에서 얻은 데이터의 상관관계를 파악하여 통합된 뷰에 종합함으로써 조사 속도를 높이고 조사 절차를 간소화하며 인시던트에 신속하게 대응할 수 있습니다.

위협 탐지 및 대응 속도를 높여 중요한 문제 해결

여러 개의 텔레메트리 소스에서 탐지한 사항의 연관성을 파악하여 가장 큰 위협부터 우선순위를 지정합니다.

AI와 머신러닝을 활용하는 Cisco SDR을 사용하면 높은 신뢰도로 상관관계를 탐지하고, 중요한 사안에만 집중하며, 비즈니스 위험과 보안 위험의 관계를 효과적으로 파악할 수 있습니다.

증거를 기반으로 한 권장 사항으로 대응을 자동화하여 영향 최소화

모든 관련 제어 지점에서 자동화와 가이드형 대응 권장 사항을 사용하여 자신 있게 위협을 해소합니다.

Cisco XDR은 조사 시간을 단축하고 대응 속도를 높여 SOC 팀에서 에스컬레이션을 막고 회복탄력성을 높입니다.

데이터를 기반으로 한 인사이트를 통해 포괄적인 위협 탐지 및 대응 조치 제공

복합한 위협을 더 빠르게 탐지

- Cisco XDR은 엔드포인트, 이메일, 네트워크, 클라우드, 방화벽 등에 광범위한 기본 내장 통합을 제공하며 일부 타사 통합도 제공하여 가장 유연하고 확장 가능하며 효과적인 XDR 전략을 제공합니다.
- 온프레미스 네트워크와 퍼블릭 및 프라이빗 클라우드에서 텔레메트리를 활용하여 관리형 및 비관리형 디바이스에서 위협을 탐지하고, 어디에서 공격이 시작되었고 네트워크를 통해 어떻게 퍼져 나갔는지 등 이벤트의 상관관계를 파악할 때 중요한 컨텍스트를 확보합니다.
- Talas 위협 정보는 탐지 기능을 강화해 주므로 분석가가 최고 수준의 실용적인 정보 모음을 수집함으로써 더욱 풍부한 컨텍스트와 실제 위협 행동에 대한 인식을 바탕으로 알려진 위협과 신규 위협을 파악할 수 있습니다.

영향을 기준으로 위협의 우선순위 지정 및 가장 중요한 위협에 먼저 더 빠르게 대응

- 위험을 기반으로 우선순위를 지정하면 SOC 분석가가 가장 중대한 위협에 대한 알림에 집중할 수 있으므로 신속하고 효과적으로 조치를 취할 수 있습니다. 이 방식은 실제 심각도를 기준으로 우선순위를 지정하여 통합된 알림 뷰를 제공합니다.
- 위협 식별, 억제, 근절, 복구를 위한 가이드형 대응과 내장된 대응 조치를 통해 일관적이고 효과적으로 의사결정을 내림으로써 평균 대응 시간(MTTR)을 단축합니다.

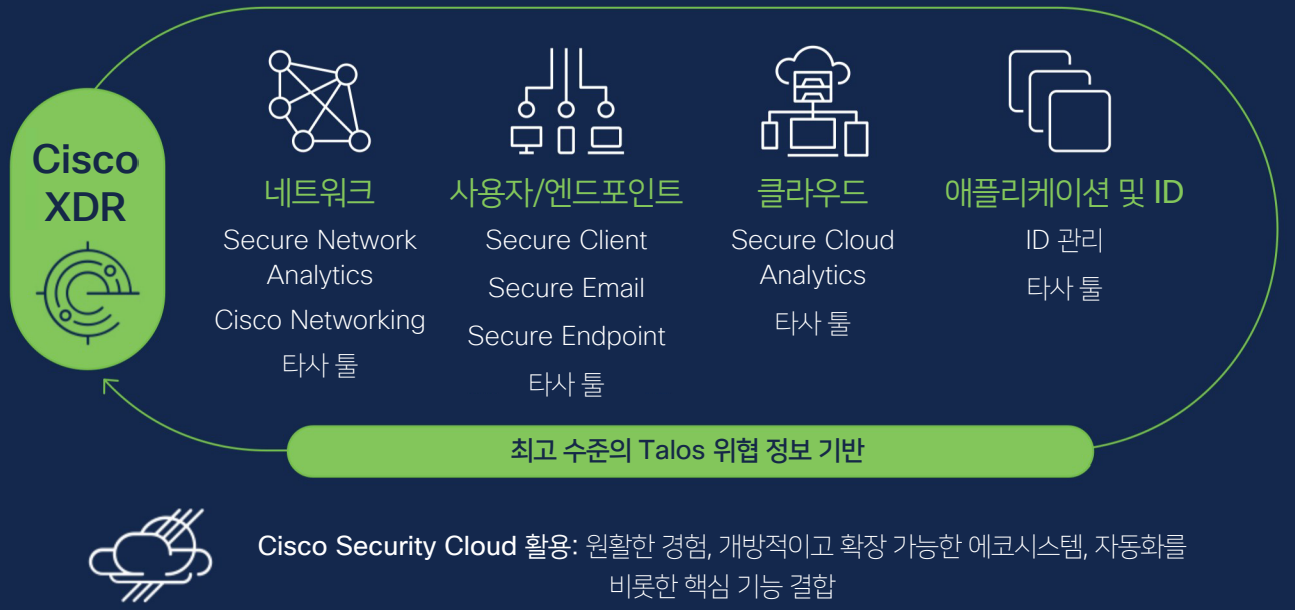
대응 시간 단축

- 기본 내장된 대응 조치와 오케스트레이션으로 신속하게 위협을 해소합니다. Cisco XDR을 사용하면 SOC 팀은 내장되거나 사용자 지정이 가능한 오케스트레이션 워크북을 다양하게 활용하여 클릭 몇 번으로 위협을 멈추고 위험을 완화할 수 있습니다.
- 반복적이고 시간이 많이 소요되는 작업을 자동화하고 SOC 팀에 바로 활용할 수 있는 모범 사례를 제공함으로써 한정된 리소스를 최대한 활용합니다. 자동화가 적합하지 않은 경우 Cisco XDR은 가이드형 대응 추천 및 권장 사항을 제공하여 SOC 분석가가 효과적은 대응 조치를 취할 수 있도록 돕습니다.
- Cisco의 기본 내장 솔루션 및 타사 솔루션을 아우르는 다양한 보안 제어와의 긴밀한 통합을 통해 광범위한 보안 툴로 대응 조치를 빠르게 적용합니다. 새로운 전술과 기법, 침해 징후에 관해 배우면서 분산된 알림 로그를 조사하여 위협 추적에서 적극적인 역할을 맡습니다.

조사 간소화:

- 통합된 컨텍스트와 단계적 공개 기법을 사용하여 조사를 간소화하고 조사 시간을 단축합니다. Cisco XDR은 수많은 부수적인 데이터로 분석가에게 부담을 주지 않고 현재 작업을 해결하는 데 필요한 정보를 보여줍니다. 필요하다면 조사에 도움이 되는 추가 정보를 클릭 한 번이면 확인할 수 있습니다.
- SOC 분석가들은 알림과 글로벌 인텔리전스, 영향의 전체 범위를 집계하여 언제나 대응 조치를 대비해 둘 수 있습니다.

사용자가 어디에 있든 요구 사항을 충족하는 SDR 제공



Cisco Security Cloud 활용: 원활한 경험, 개방적이고 확장 가능한 에코시스템, 자동화를 비롯한 핵심 기능 결합

Cisco XDR 자세히 알아보기: cisco.com/go/xdr