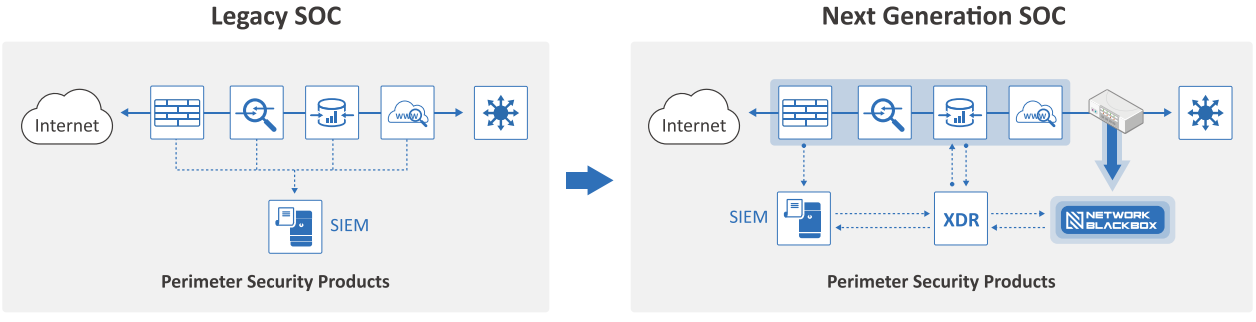
정부 사례 연구



소개

이 사례 연구는 보안 침해와 관련된 대응 시간을 줄이기 위해 정부 기관에서 고도화된 보안 운영 체계를 성공적으로 구현한 사례에 초점을 맞춥니다. 보안 위협이 계속 진화하고 더욱 정교해짐에 따라 정부 기관에서는 민감한 정보와 시스템을 보호하기 위한 강력한 보안 인프라를 구축하는 것이 필수적입니다.

해당 정부 기관은 보안 사고를 신속하게 탐지하고 대응할 수 있는 종합적인 보안 솔루션의 필요성을 인식하고, 철저한 평가 과정을 거쳐 보안 태세를 강화하고 대응 시간을 단축하기 위해 (주)쿼드마이너의 네트워크 탐지 및 대응(NDR) 솔루션을 선택했습니다.

이 사례 연구에서는 정부기관이 직면한 과제, (주)쿼드마이너가 구현한 솔루션, 고급 보안 운영 체제 도입을 통해 달성한 성과를 살펴봅니다.

배경

이 해외 정부 기관은 복잡한 보안 구성으로 여러 경계에 걸쳐 있는 통합 인터넷 네트워크를 운영합니다. 보호 대상 시스템, 기관, 부서, 인력이 다양하기 때문에 효과적인 사이버 보안 조치를 확보하는 것이 매우 중요합니다. 디지털화를 가속화하는 데 중점을 두면서 보안 과제가 더욱 복잡해졌고, 진화하는 위협에 대응할 수 있는 고도화된 보안 운영 체제가 필요해졌습니다. 이러한 목표를 달성하기 위해 미 연방수사국은 중앙 집중식 통합 보안 운영을 구현하여 포괄적인 사이버 보안 범위를 제공하고 있습니다. 그러나 보안 침해의 빈도와 정교함이 증가함에 따라 대응 시간을 단축하고 사고 대응 역량을 개선해야 할 필요성을 인식하게 되었습니다. 이에 따라 이 기관은 보안 태세를 강화하고 사이버 위협의 위험을 줄이기 위해 (주)쿼드마이너의 NDR 솔루션을 선택했습니다.

도전과제

이 정부 기관은 보안 운영과 관련하여 몇 가지 문제에 직면했습니다. 통합 인터넷 네트워크에는 여러 경계 보안 구성이 있어 보안 이벤트를 모니터링하고 탐지하기가 어려웠습니다.

또한 보안 이벤트 분석 시스템이 사일로화되어 있어 탐지된 보안 이벤트가 피해 시스템에 미치는 위험과 영향을 파악하는 데 어려움을 겪었습니다.

이전에는 너무 많은 경고를 생성하는 기존의 보안 이벤트 관리 시스템에 의존하고 있었기 때문에 보안팀이 인시던트의 우선순위를 정하고 적시에 대응하기 어려웠습니다. 이로 인해 대응 시간이 지연되어 보안 침해가 발생할 위험이 높아졌습니다.

또한, 정부 기관은 디지털화 노력을 가속화하고자 했기 때문에 보안 시스템이 민첩하고 새로운 기술과 위협에 적응할 수 있어야 했습니다. 이를 위해서는 여러 보안 솔루션을 통합하고 전체 보안 환경에 대한 중앙 집중식 모니터링을 제공할 수 있는 보다 진보된 보안 운영 체제가 필요했습니다.

솔루션

㈜쿼드마이너의 NDR 솔루션은 포괄적이고 통합된 보안 운영 체제를 구현할 수 있도록 지원함 으로써 정부 기관이 직면한 문제를 해결할 수 있었습니다. 이 솔루션은 보안 침해와 관련된 대응 시간을 단축하고 중앙 집중식 통합 보안 운영을 제공하는 것을 목표로 했습니다.

우선, NDR 솔루션은 캡처된 전체 패킷에서 재구축된 패킷 스트림으로 추출할 수 있는 풍부한 데이터셋과 메타데이터로 정보를 보강하여 네트워크 침해에 대한 결정적인 증거를 수집했습니다. 이를 통해 네트워크 트래픽을 상세히 분석하고 침해의 원인을 파악하는 데 도움이 되었습니다.

다음으로, 이 솔루션은 스텔라 사이버(XDR)와 기존 SIEM 및 네트워크 블랙박스의 통합을 통해 분석 프로세스를 자동화했습니다. 이를 통해 보안 이벤트와 각각의 위험 및 피해 시스템에 대한 영향을 더 빠르게 식별할 수 있었습니다. 또한 여러 보안 시스템을 통합하여 네트워크 보안 태세를 보다 포괄적이고 전체적으로 파악할 수 있었습니다.

마지막으로, 이 솔루션은 잠재적으로 취약점을 유발하고 보안 침해의 위험을 높일 수 있는 네트워크 구성 변경을 최소화하는 것을 목표로 했습니다. 네트워크 구성 변경을 모니터링하고 감지할 수 있는 시스템을 구현함으로써 정부기관은 승인된 변경만 이루어지고 이러한 변경이 네트워크 보안에 위험을 초래하지 않도록 보장할 수 있습니다.

결과

㈜쿼드마이너의 NDR 솔루션을 도입한 후 정부기관은 다음과 같은 성과를 달성했습니다.

• **보안 운영 체계 고도화:** NDR 솔루션을 통해 정부기관은 보안 사고를 실시간으로 탐지하고 대응할 수 있는 고도화된 보안 운영 체계를 구축할 수 있었습니다. 이를 통해 조직의 전반적인 보안 태세를 개선하는 데 도움이 되었습니다.

• **공격의 위험과 영향에 대한 즉각적인 판단:** NDR 솔루션을 통해 정부 기관은 확보된 증거를 바탕으로 공격의 위험과 영향을 즉시 판단할 수 있었습니다. 이를 통해 조직은 보안 사고에 신속하게 대응하고 사고의 잠재적 영향을 최소화할 수 있었습니다.

• **평균 탐지 시간 및 평균 대응 시간 단축:** 정부 기관은 NDR 솔루션을 통해 보안 인시던트에 대한 평균 탐지 시간(MTTD)과 평균 대응 시간(MTTR)을 단축할 수 있었습니다. 이는 보안 사고 분석 및 대응의 자동화를 통해 달성한 것으로, 지연을 최소화하고 보안 운영 센터의 전반적인 효율성을 개선하는 데 도움이 되었습니다.

• **내부 트래픽 보안을 강화하고 2차 프로젝트를 진행할 수 있는 가능성을 확인:** NDR 솔루션은 정부 기관에 내부 트래픽 보안에 대한 인사이트를 제공했습니다. 이를 통해 조직은 개선이 필요한 영역을 파악하고 전반적인 보안 태세를 강화하기 위한 2차 프로젝트의 우선순위를 정하는 데 도움이 되었습니다.

이 정부기관은 (주)쿼드마이너의 NDR 솔루션으로 보안 운영을 전반적으로 개선할 수 있었습니다. 이제 이 기관은 보안 사고에 실시간으로 대응할 수 있는 보다 발전되고 효율적인 보안 시스템을 구축하여 보안 사고의 위험과 영향을 줄일 수 있게 되었습니다.