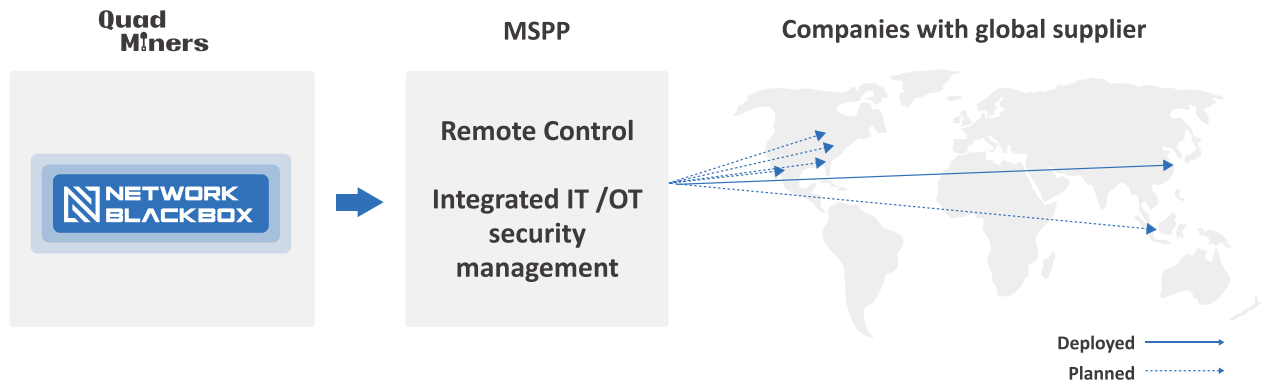


## 제조사 사례 연구

에너지 기업을 위한 (주)쿼드마이너의 풀패킷 NDR 솔루션



### 배경

(주)쿼드마이너는 최근 글로벌 시장을 선도하는 한국의 에너지 기업을 위해 네트워크 탐지 및 대응(NDR) 솔루션을 구축했습니다. 이 에너지 기업은 해외와 한국에 사업장을 두고 생산 시설의 글로벌화를 추진하고 있습니다. 이 기업은 중요 인프라와 운영의 보안을 보장하기 위해 국내 매니지드 보안 서비스 제공업체(MSSP)를 통해 해외 생산 시설에 대한 보안관제센터(SOC) 서비스를 제공하고 있었습니다.

그러나 사이버 보안 위협의 복잡성과 정교함이 증가함에 따라 산업 자동화 및 제어 시스템(IACS)의 보안을 강화하기 위해 다양한 솔루션을 검토해 왔습니다. 사이버 보안 인프라 구축은 선택이 아닌 필수였으며, 제로 트러스트 아키텍처 관점으로 정보기술(IT)과 운영기술(OT)영역 모두에 대한 사이버 보안 인프라 구축 전략을 일관되게 가져야 했습니다. 산업 자동화 및 제어 시스템(IACS) 네트워킹의 대체는 기술, 특히 IT와OT가 융합하는 것이기 때문입니다. (주)쿼드마이너의 NDR 솔루션은 실시간 가시성, 위협 탐지 및 사고 대응 기능과 관련하여 IT와 OT를 모두 포괄하여 사이버 보안 태세를 강화하고 중요 인프라를 보호할 수 있다는 점에서 선호되는 솔루션으로 선정되었습니다.

### 문제점

글로벌 배터리 업계를 선도하는 이 에너지 기업은 보안 운영과 관련된 몇 가지 문제에 직면하고 있었습니다. 이 기업은 해외 생산 시설에 보안관제센터(SOC) 서비스를 제공하기 위해 국내 매니지드 보안 서비스 제공업체(MSSP)에 의존하고 있었기때문에 SOC에서 탐지된 보안 위협을 직접 분석할 수 없었습니다. 이로 인해 위협 식별 및 대응 시간이 지연되어 잠재적인 보안 사고의 위험이 증가했습니다. 또한 해외 생산 시설별 IT팀과 OT팀 모두 가시성이 제한되어 있어 위협을 지속적으로 모니터링하고 대응하기가 어려웠습니다. 게다가 위협 관리를 운영할 IT 인력이 부족하여 보안 운영을 효과적으로 관리할 수 없었습니다. 이러한 문제로 인해 이 회사는 사이버 보안 태세를 강화하고 중요 인프라를 보호하기 위해 실시간 가시성, 위협 탐지 및 사고 대응 기능을 제공할 수 있는 솔루션을 찾게 되었습니다.

## 솔루션

(주)쿼드마이너의 NDR 솔루션을 도입한 이 회사는 SOC에서 직접 네트워크의 모든 위협을 탐지하고 분석할 수 있게 되어 잠재적 위협을 식별하고 대응하는 시간을 단축할 수 있게 되었습니다. 또한 풀 패킷 기반 NDR을 배포함으로써 IT와 OT 도메인 모두 네트워크 가시성을 확보하여 위협 대응 시간을 단축하고 전반적인 보안 태세를 강화할 수 있었습니다. (주)쿼드마이너는 풀패킷 데이터를 분석한 후 사용자 정의 및 개발을 통해 이 에너지 기업에서 사용되는 맞춤형 프로토콜을 포함하여 모드버스 등 ICS 산업 표준 프로토콜을 식별했습니다. 또한 (주)쿼드마이너의 NDR 솔루션은 위협에 대한 확실한 증거와 단일 위협 분석 기능을 제공함으로써 위협 대응 시간을 절약하고 일상적인 보안 작업을 줄일 수 있었습니다. 전체적으로 (주)쿼드마이너의 NDR 솔루션은 실시간 가시성, 위협 탐지, 사고 대응 기능을 제공하여 에너지 회사가 보안 문제를 해결하고 보안 운영을 강화하여 중요 인프라를 보호하는 데 도움이 되었습니다.

## 결과

(주)쿼드마이너의 NDR 솔루션을 도입한 결과, 글로벌 배터리 업체를 선도하는 이 에너지 기업의 사이버 보안 태세가 크게 개선되었습니다. 이 기업은 풀 패킷 NDR 배포를 통해 IT와 OT모두의 네트워크 가시성을 개선하여 사각지대를 최소화하고, 잠재적 위협에 대한 평균 탐지 시간(MTTD)과 평균 대응 시간(MTTR)을 단축할 수 있었으며, 적은 수의 보안 인력으로도 운영이 가능하게 됨으로써 글로벌 생산 시설에 효율적이고 일관된 보안 위협 대응 프로세스를 구축하는 데 도움이 되었습니다. 전반적으로 (주)쿼드마이너의 솔루션은 이 에너지 회사의 보안 요구 사항을 충족하는 효과적이고 효율적인 솔루션으로 입증되어 위협을 빠르고 효과적으로 탐지하고 대응할 수 있었습니다.

## IT 및 OT융합환경을 위한 NDR이 필요한 이유

제조업에 해당하는 기업들은 복잡하고 여러 위치에 걸쳐 있는 중요 인프라를 운영하기 위해 IT 네트워크에 의존하기 때문에 잠재적인 위협을 식별하고 사고에 대응하기가 어렵습니다. NDR 솔루션은 네트워크 활동에 대한 실시간 가시성을 제공하고 잠재적 위협을 탐지하며 사고에 신속하고 효과적으로 대응합니다. 제조업에 해당하는 기업들이 사이버 보안 위협으로부터 네트워크를 보호하고, 규정을 준수하고, 네트워크에 대한 포괄적인 가시성을 확보하고, 네트워크 성능을 최적화하고, 사고에 효율적으로 대응하려면 NDR 솔루션이 필수적입니다.

(주)쿼드마이너는 글로벌 시장에 풀패킷 캡처기반의 트래픽 전수 검사를 통해 위협 탐지 및 대응 기능을 제공하는 선도적인 NDR 소프트웨어 공급업체입니다. 관리자가 페이로드의 네트워크 트래픽에 대한 자세한 정보를 확인할 수 있고 보안을 더욱 심층적으로 강화할 수 있는 풀패킷 캡처 기능을 제공하는 것이 핵심 기술입니다. 이 기능을 통해 조직은 다른 보안 솔루션에서 탐지하지 못할 수 있는 위협을 탐지할 수 있으며, 위협에 대한 확실한 증거를 제공하여 조직이 신속하고 효율적으로 대응할 수 있도록 지원합니다. 또한 (주)쿼드마이너의 NDR 솔루션은 IT 및 OT 환경 전반에서 네트워크 가시성을 제공하여 조직이 사각지대를 최소화하고 위협 대응 시간을 단축할 수 있도록 지원합니다. 혁신과 고객 만족에 대한 강한 의지를 바탕으로 (주)쿼드마이너는 네트워크 보안을 강화하고자 하는 조직을 위한 신뢰할 수 있는 파트너로 자리매김했습니다. (주)쿼드마이너 네트워크 블랙박스 추가 탐지를 수행할 뿐만 아니라 기존 보안 인프라와 프로세스를 활용하고 발전시킬 수 있는 이상적인 위치에 자리 잡고 있습니다.