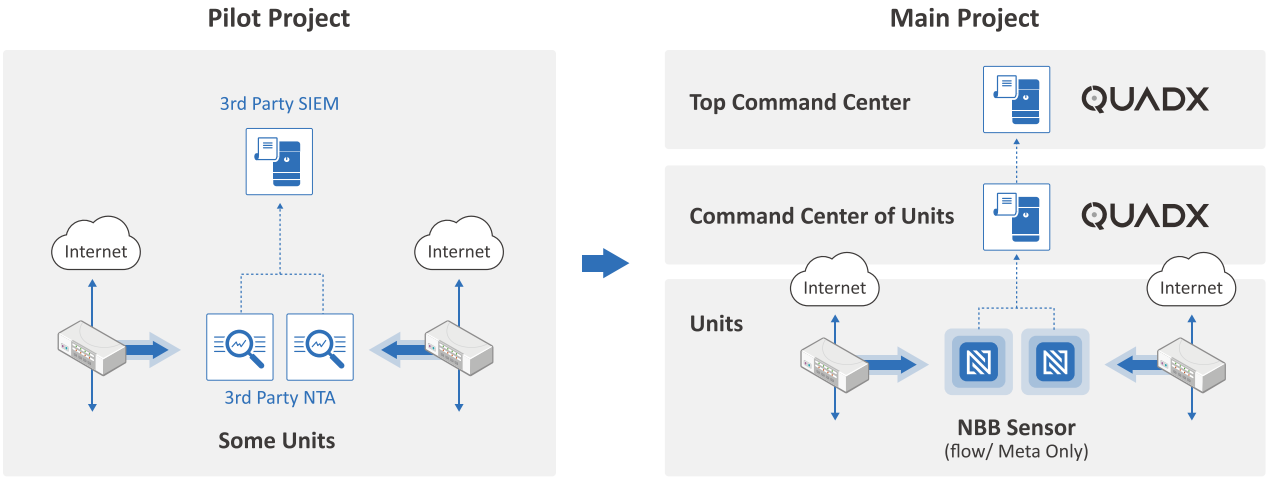
군 사례 연구



소개

오늘날 디지털 시대에 군은 국가 안보에 심각한 위험을 초래할 수 있는 사이버 위협에 직면하고 있습니다. 또한 군이 사이버 영역에서의 전략적 가치를 인식함에 따라 사이버 전은 현대전에서 그 중요성이 점점 더 부각되고 있으며, 사이버 공격을 통해 상대적으로 적은 전력대비 막대한 피해를 입힐 수 도 반대로 피해를 입을 수도 있습니다. 이러한 사이버 위협에 대응하기 위해 군은 사이버 위협을 신속하고 효과적으로 탐지하고 대응할 수 있는 강력한 사이버 보안 솔루션이 필요 했으며, 네트워크 탐지 및 대응(NDR) 솔루션의 선도적 공급업체인 (주) 쿼드마이너는 전군에 사이버 작전을 수행하고 있는 0000부대와 협력하여 전체 패킷 흐름 및 메타데이터 기반 트래픽 분석 시스템인 QUADX 차세대 SIEM 솔루션을 구축했습니다. 해당 사례 연구는 군이 직면한 과제와 (주) 쿼드마이너의 차세대 SIEM 솔루션이 풀패킷 캡처기반 트래픽 전수검사를 바탕으로 이러한 과제를 해결하는데 어떠한 도움이 되었는지 살펴보겠습니다.

배경

최근 몇 년간 특정 군별 네트워크(인터넷, 인트라넷 등)에서 플로우/메타 기반 분석 시스템을 시범적으로 도입하여 어느 정도 효과를 보이고 있었습니다. 하지만 종합적인 사이버 방호태세 확립을 위해서는 분산되어 있는 각 군별(육군,해군,공군,해병대, 국방부 직할부대 등) 네트워크의 모든 트래픽을 수집하여 전체 가시성을 확보할 필요가 있었고, 기존 보안 인프라와 네트워크 트래픽 분석(NTA)솔루션간 운영 효과를 검증 할 수 있는 보안 위협 관련 통합 분석 체계를 구축할 필요성이 있었습니다.

도전과제

군에서는 운용중인 시스템 전반의 보안 위협을 효과적으로 방어하기 위해 통합 분석 시스템이 필요 했습니다. 이를 위해서 분산된 보안 솔루션의 위협 이벤트를 통한 분석으로 통합해야 했는데, 전국에 분산되어 있는 군부대의 특성 그리고 모든 부대의 네트워크 통신에 대한 무손실 트래픽 정보 수집이 최우선의 과제 였습니다.

다음으로 NDR 솔루션은 기본 보안 운영체제를 즉시 지원할 수 있는 필수 데이터 분석 기능을 제공해야 하는데 이를 위한 솔루션이 전지역에 넓게 분포되어 있는 각 군의 트래픽을 커버해야 하므로 모든 엔드포인트와 인프라에서 네트워크 트래픽 데이터를 수집하고 분석해야 했습니다.

또한, 군에서는 보안 경보 및 이벤트에 대한 심층 조사에 활용 할 수 있는 풍부한 정보와 위협에 대한 가시성 확보를 위해 트래픽과 관련된 메타데이터를 포함한 분석을 위한 모든 네트워크 트래픽에 대한 전수 검사가 가능해야 했습니다.

마지막으로, 군에서는 빠르게 진화하는 위협 환경을 대응 할 수 있는 솔루션이 필요했으며, 이를 위해 NDR 솔루션에 대한 지속적인 업데이트와 개선 그리고 기존 보안 인프라와 통합할 수 있을 만큼 유연성을 갖춰야 했습니다.

솔루션

㈜쿼드마이너의 NDR 솔루션과 통합된 차세대 SIEM인 QUADX 는 군이 직면한 과제에 대한 포괄적인 해결방안을 제공할 수 있었습니다. 경쟁력 있는 POC를 통해 통합 관리 및 분석 시스템의 효과를 검증했으며, 패킷 데이터를 저장하지 않고도, 캡처된 트래픽에서 재구축된 패킷 스트림 분석을 통해 추출할 수 있는 데이터셋만을 가지고 메타데이터를 활용한 정보 보강을 통해서 이상 징후 및 다양한 위협에 대한 심층 조사를 위한 안정적이고 효과적인 솔루션임을 입증했습니다. 이 솔루션에는 보안 솔루션의 위협 이벤트 파싱을 통한 통합 지원, 각 지역의 센서를 통한 모든 통신 트래픽 수집, 군 특성에 맞는 이상 징후와 위협, 콘텐츠 탐지 기능 등이 포함되었습니다.

또한 ㈜쿼드마이너는 데이터 분석 및 위협헌팅 전문가 파견 지원을 통해 전국에 걸쳐 분포된 수많은 군부대를 대상으로 짧은 기간안에 보안 분석 체계를 구축했으며, 파견 인력를 통한 보안 위협에 대한 적시적인 대응으로 분석 및 대응시간을 획기적으로 단축할 수 있었습니다.

전반적으로 ㈜쿼드마이너의 솔루션은 군이 보안 목표를 달성할 수 있는 포괄적이고 효과적인 방법을 제공했습니다. 이 솔루션은 기존 보안 인프라와 원활하게 융합되었으며, 기존 보안 운영 체제를 즉각적으로 지원하는 데 필요한 데이터 분석 기능을 제공했습니다.

결과

㈜쿼드마이너의 차세대 SIEM솔루션인 QUADX 도입으로 군 전체에 메타 및 플로우 기반 데이터 분석을 체계화하여 통합 위협 탐지 및 데이터 분석 기능을 제공할 수 있게 되었습니다. 특히, 육군 사이버작전 센터의 트래픽 모니터링 및 분석 시스템을 통합하여 보안 위협을 중앙에서 효율적으로 모니터링하고 관리할 수 있게 되었습니다.

QUADX 솔루션은 네트워크 트래픽에 대한 향상된 가시성을 제공하고 보안 위협을 적시에 탐지하고 대응할 수 있게 함으로써 군의 사이버전 대비 태세를 크게 향상시켰으며, 풀패킷 캡쳐 기반 트래픽 단속체계로 전환해야 할 필요성을 증명하였습니다.

군에 QUADX 솔루션이 필요한 이유는 무엇인가요?

군은 사이버 보안 태세를 강화하고 잠재적인 사이버 위협으로부터 보호하기 위해 NDR(네트워크 탐지 및 대응) 솔루션이 통합된 차세대 SIEM 솔루션이 필요합니다. 군 내 다양한 기술 사용과 연결성이 증가함에 따라 사이버 공격과 잠재적인 데이터 유출의 위험이 점점 높아지고 있습니다. 쿼드마이너사의 차세대 SIEM인 QUADX 는 전체 네트워크에 대한 실시간 가시성과 위협 탐지 기능을 제공하여 보안팀이 모든 보안 사고를 신속하게 식별하고 대응할 수 있도록 지원합니다. 또한 QUADX 는 네트워크 트래픽 데이터를 분석하여 잠재적 취약점을 식별하는 데 도움이 되는 인사이트와 패턴을 파악할 수 있는 기능을 군에 제공할 수 있습니다. 전반적으로 QUADX는 사이버 위협을 탐지하고, 예방 및 대응하는 능력을 크게 향상시킬 수 있습니다.

NETWORK BLACKBOX

Network Blackbox is a next-generation NDR solution that integrates AI-driven detection, TTP-based threat hunting, and automated response with extracted irrefutable evidences from full packet capture.

Quad Miners

Contact Us

sales@quadminers.com