QUAD-X

Evolved NDR SIEM

전방위 네트워크 위협 분석 체계

QUAD-X Sensor

패킷을 어플리케이션 계층(L7)까지 재조합하여 네트워크에서 벌어지는 행위 탐지

고도로 정제된 데이터베이스를 통해 사이버 위협을 전방위로 분석하고, 단순 로그가 아닌 실제 패킷까지 확인 가능

QUAD-X Management

상관 분석, 임계치 기반 분석 및 다수의 장비에서 수집한 이벤트 분석

지도학습 기반의 인공지능 분석 엔진을 통해 위협을 다각도로 분석

QUAD-X Analyzer

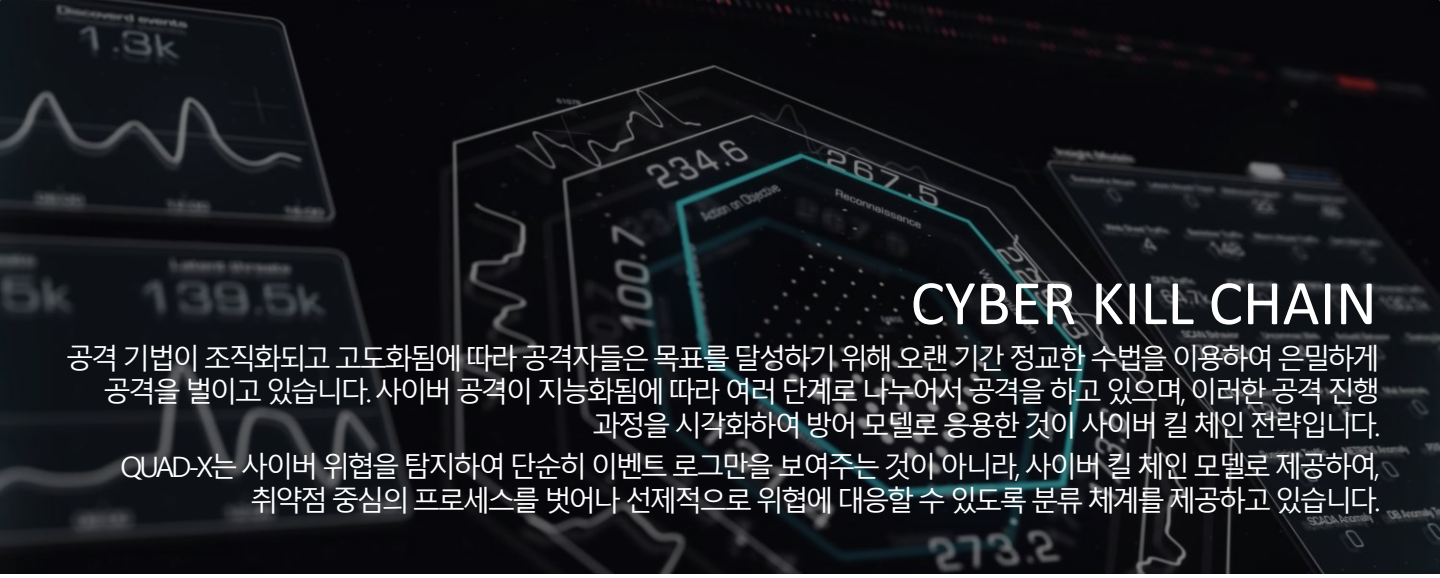
단순 로그 수집, 분석, 검색에서 그치지 않고, 네트워크 플로우를 비롯한 메타 데이터를 수집하여 보다 정밀하며, 포괄적인 상관관계 분석 및 컴플라이언스 관리 기능 제공

QUAD-X Master Analyzer

수집된 로그 및 플로우에 대한 정규화 및 인덱싱 기능 지원

수집된 데이터에 대한 유연한 스키마 확장, 보고서 기능 제공

Quad Miners



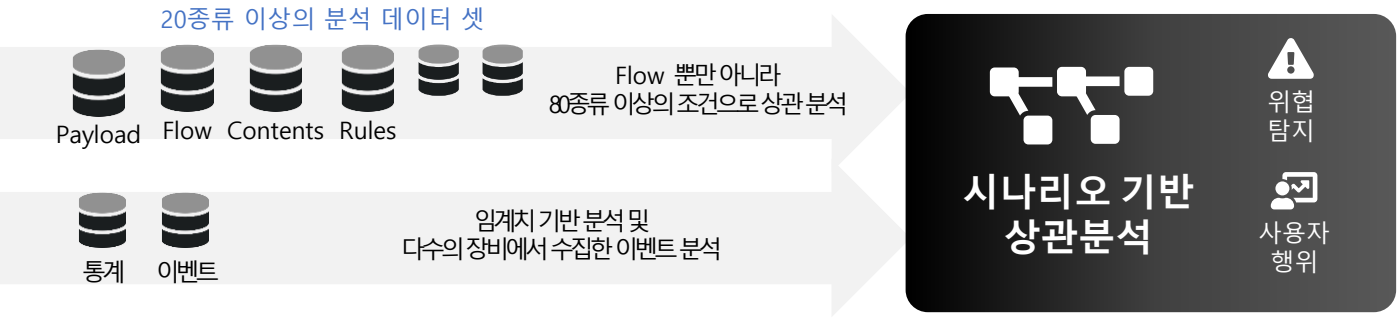
CYBER KILL CHAIN

공격 기법이 조직화되고 고도화됨에 따라 공격자들은 목표를 달성하기 위해 오랜 기간 정교한 수법을 이용하여 은밀하게 공격을 벌이고 있습니다. 사이버 공격이 지능화됨에 따라 여러 단계로 나누어서 공격을 하고 있으며, 이러한 공격 진행 과정을 시각화하여 방어 모델로 응용한 것이 사이버 킬 체인 전략입니다.

QUAD-X는 사이버 위협을 탐지하여 단순히 이벤트 로그만을 보여주는 것이 아니라, 사이버 킬 체인 모델로 제공하여, 취약점 중심의 프로세스를 벗어나 선제적으로 위협에 대응할 수 있도록 분류 체계를 제공하고 있습니다.

심층적인 네트워크 트래픽 분석

고도로 정제된 데이터베이스를 통해 사이버 위협을 분석하고, 단순 로그가 아닌 실제 패킷까지 확인할 수 있습니다.



지도학습 기반의 인공지능 분석 엔진

탐지된 이벤트 뿐만 아니라, 네트워크 상에서 벌어지는 다양한 행위를 학습하여 가장 정확하게 탐지합니다. 인공지능이 도출한 결과의 이유와 원인에 대한 설명이 가능한 지도학습 기반의 인공지능 솔루션입니다.

쿼드마이너 핵심 기술 중 하나는 패킷의 헤더 정보, 페이로드 정보, 플로우 정보, 풀패킷 정보를 선택하여 분석 및 저장관리가 가능하다는 점입니다. 기관 및 기업의 내부 보안정책에 따라서 선택적으로 적용 가능합니다.

Quad Miners