Quad Miners

Network Blackbox v4.0

현 보안운영의 문제점

클라우드를 포함한 IT기술의 발전과 OT 환경의 자동화 추세에 따른 공격표면의 확장,
그리고 비즈니스의 디지털화 확산에 의한 디지털 자산의 중요성 급상승 대비
보안운영의 비효율성으로 인한 접근통제 실패로 인한 금전적 피해 확산

폭증하는 트랜잭션

- 위협 가시화 사각지대
- 확증 없는 통계 기반의 추정형태

고밀도의 복잡성

- 60가지 이상의 보안 제품
- 인력 부족 및 전문성 결여

넘쳐나는 보안 경보

- 일당 150개의 티켓
- 일당 10만건 이상의 보안 이벤트

반복적인 작업

- 탐지에 대한 매뉴얼한 확인 및 검증
- 대응을 위한 반복적인 대응 룰 변경

전문가 부족

- 숙련된 SOC 운영 요원의 부족
- 비효율적인 인적 자원 운영

느린 대응

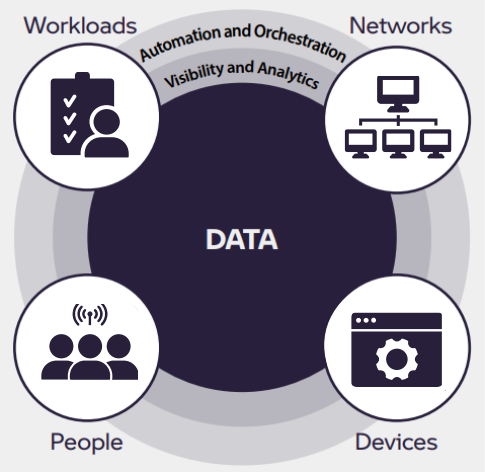
- 너무 많은 추가조사 대상
- 즉각적인 위협 대응 불가

제로 트러스트 아키텍처 적용을 통한 문제해결

기존의 접근방식

위치기준 신뢰정책	신뢰대상을 내부/외부로부터의 접속으로만 구분
네트워크 접속 기반	경계만 뚫리면 내부에서는 손쉽게 공격전이, 목적달성 용이
보안경계의 확장성 결여	내/외부, 모바일, 클라우드 등 다중환경 보안성 미고려

제로 트러스트 접근방식



Forrester 제로 트러스트 확장모델(ZTX)과 NDR

액세스단위 신뢰정책

언제, 어디에서, 누가 접속을 하더라도 모든 접속 확인

어플리케이션 접속 기반

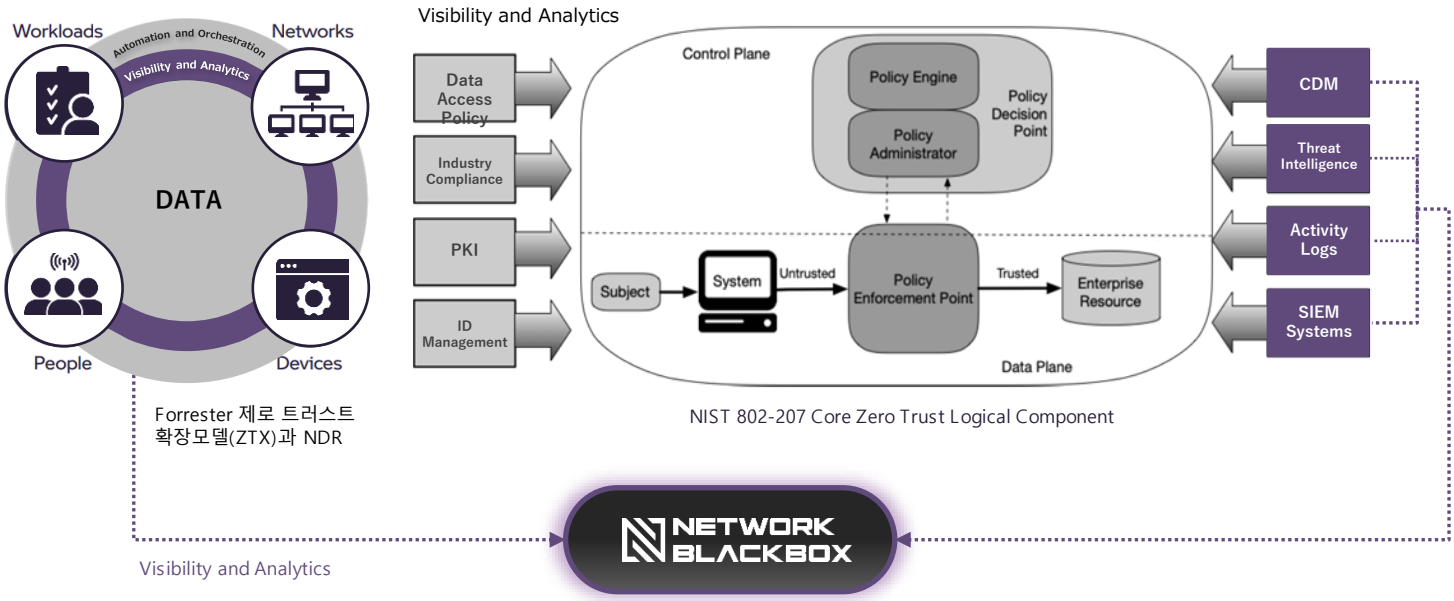
확인된 사용자의 적법한 단말 및 접속이 아닌 경우 차단

일관된 보안정책 전역 확장

모든 환경에서의 신원/신뢰 확인 기반 보안 정책 적용

제로트러스트 아키텍처 상의 NDR 포지셔닝

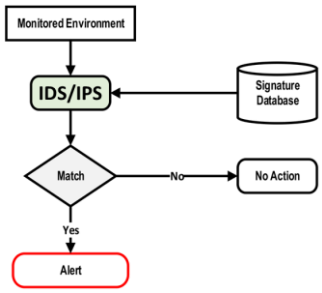
네트워크 전반에 걸친 가시성과 비정상행위 판별을 위한 분석 기능 수행,
동적인 접근제어 정책을 결정하기 위한 신뢰판단용 데이터 제공(PIP, Policy Input Point)



제로트러스트 환경하에서의 차별화된 NDR 기능 효과

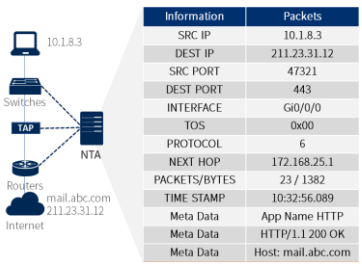
풀패킷 캡처 기반의 트래픽 전수검사와 트래픽 리빌드를 통한 확정적 증적 확보로
추정이 아닌 확정적인 비정상행위 및 위협 식별

❶ Intrusion Detection System Intrusion Prevention System



- Payload Inspection
- Signature 기반의 Known Attack 탐지
- 공격의 위험도 및 영향도 확인을 위한 Victim 시스템 추가 조사 필요

❷ Network Traffic Analytics

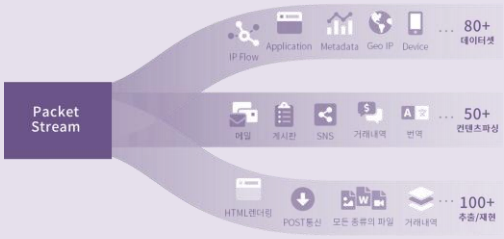


- 일부 Packet 수집, IP Flow 및 Metadata 추출
- 이상행위분석 기반 Unknown Attack 및 Signature 기반 Known Attack 탐지
- 공격의 위험도 및 영향도 확인을 위한 Victim System 추가 조사 필요

❸ Network Detection and Response

NETWORK BLACKBOX

**Full Packet Capture 기반
트래픽 전수 검사기반 NDR**



- IP Flow, Metadata, Contents, Files 추출
- 이상행위분석 기반 Unknown Attack 및 Signature 기반 Known Attack 탐지
- 수집된 증적정보기반 공격의 위험도 및 영향도 확정, 추가조사 불필요
- 트래픽 리빌드, 회귀적 분석/조사 지원

Quad Miners NDR 핵심기술(Core Technology)

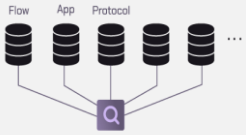
기업 네트워크에서 발생하는 모든 사이버 보안 위험을 탐지하고 대응하는
차세대 네트워크 탐지 및 대응 솔루션입니다.

최대 40Gbps 네트워크로 모든 데이터를 빠짐없이 수집 및 저장

고성능 패킷 스트림 저장 시스템

초고속 대규모 네트워크 환경에서 손실 없이 저장하려면 분산 구조로 저장하는 시스템이 필요합니다.

10-2080477



고속 패킷 검색 방법

검색 조건에 특화된 DB를 생성하여 사용자정의 패턴을 고속으로 검색합니다.

KR2019-008860

패턴 기반 색인 처리 시스템

패킷 재조합 후에 패턴 분석을 하여 판별한 후 해당 애플리케이션에 맞게
실시간으로 색인 처리를 합니다.

10-2080478

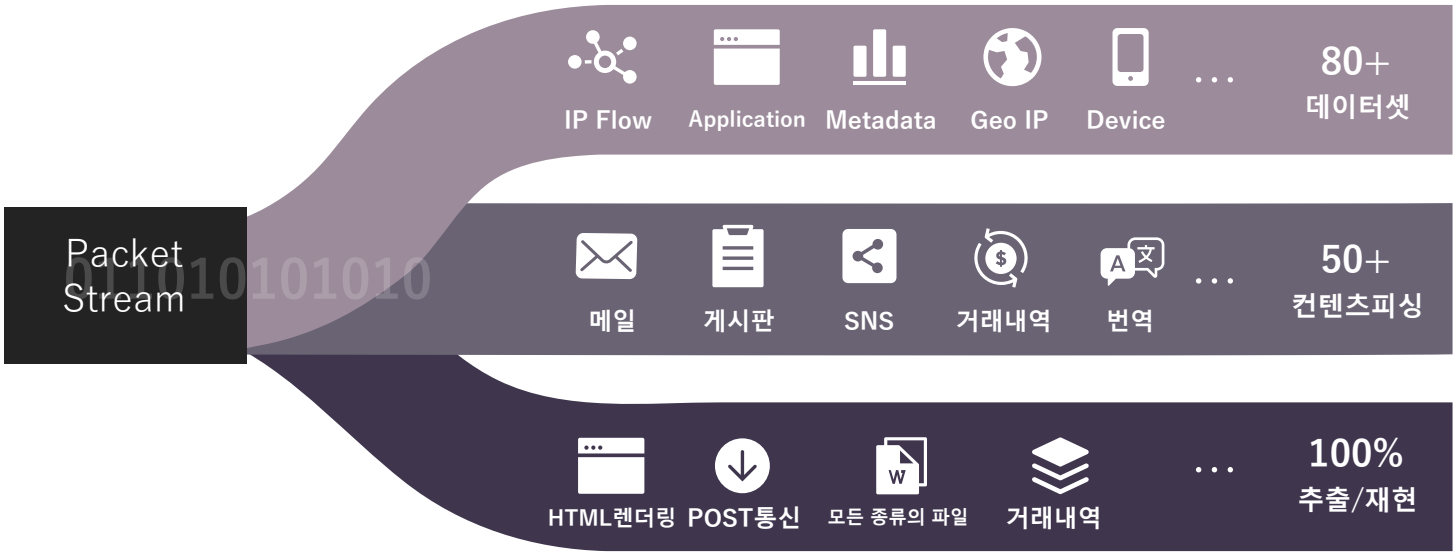
시나리오 중심 실시간 공격 감지 시스템

시도학습 기반의 위협 헌팅 모델로 고도화된 위협과 이상 징후를 찾아 실시간으로 사냥합니다.

10-2080479

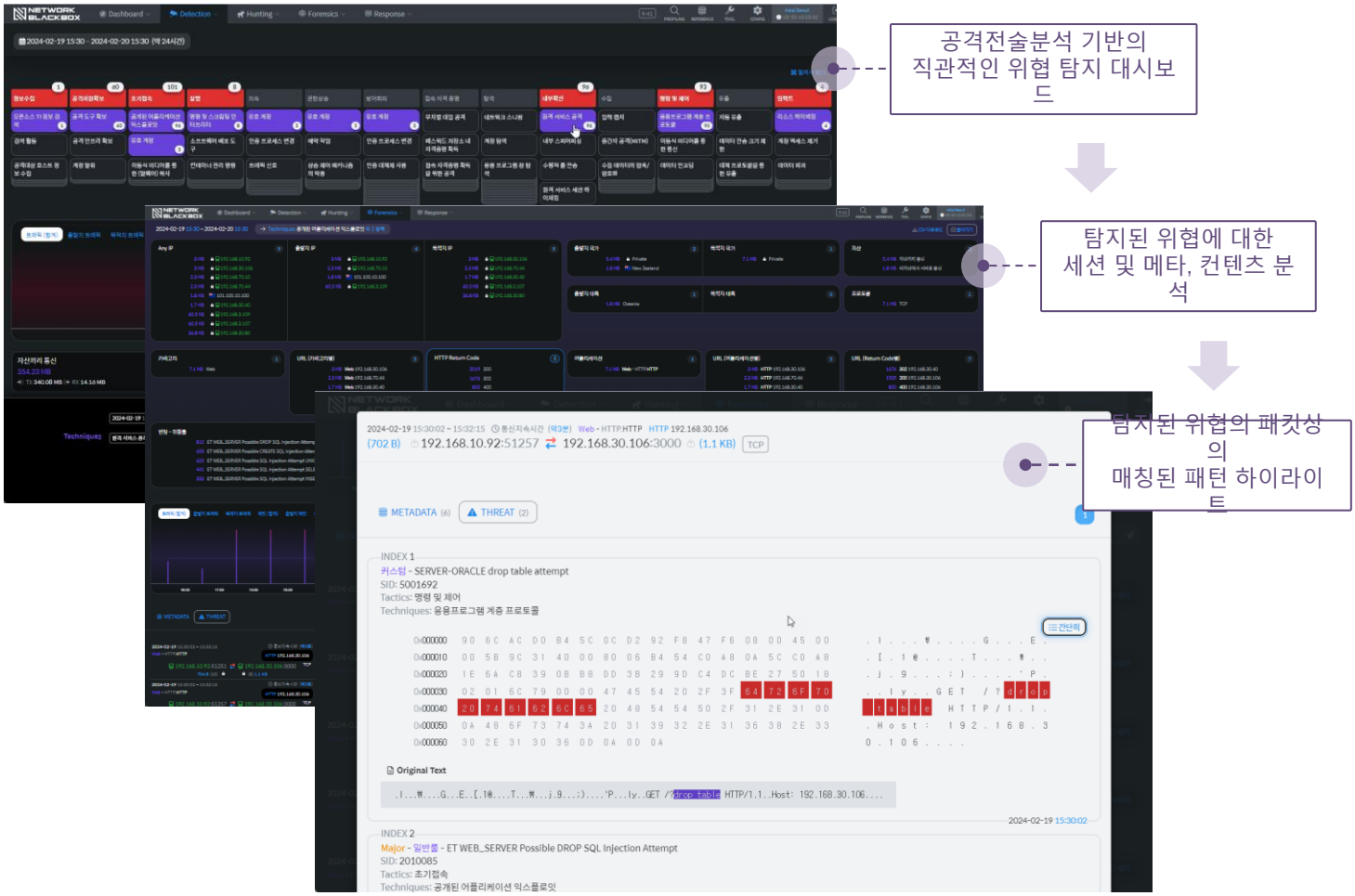
모든 패킷을 **100%** 저장하고 분석하므로
모든 종류의 사이버 보안 위협을 탐지하고 대응할 수 있습니다.

풀 패킷 스트림을 어플리케이션 레벨까지 재조합, 다양한 증적 데이터를 추출하고 분석



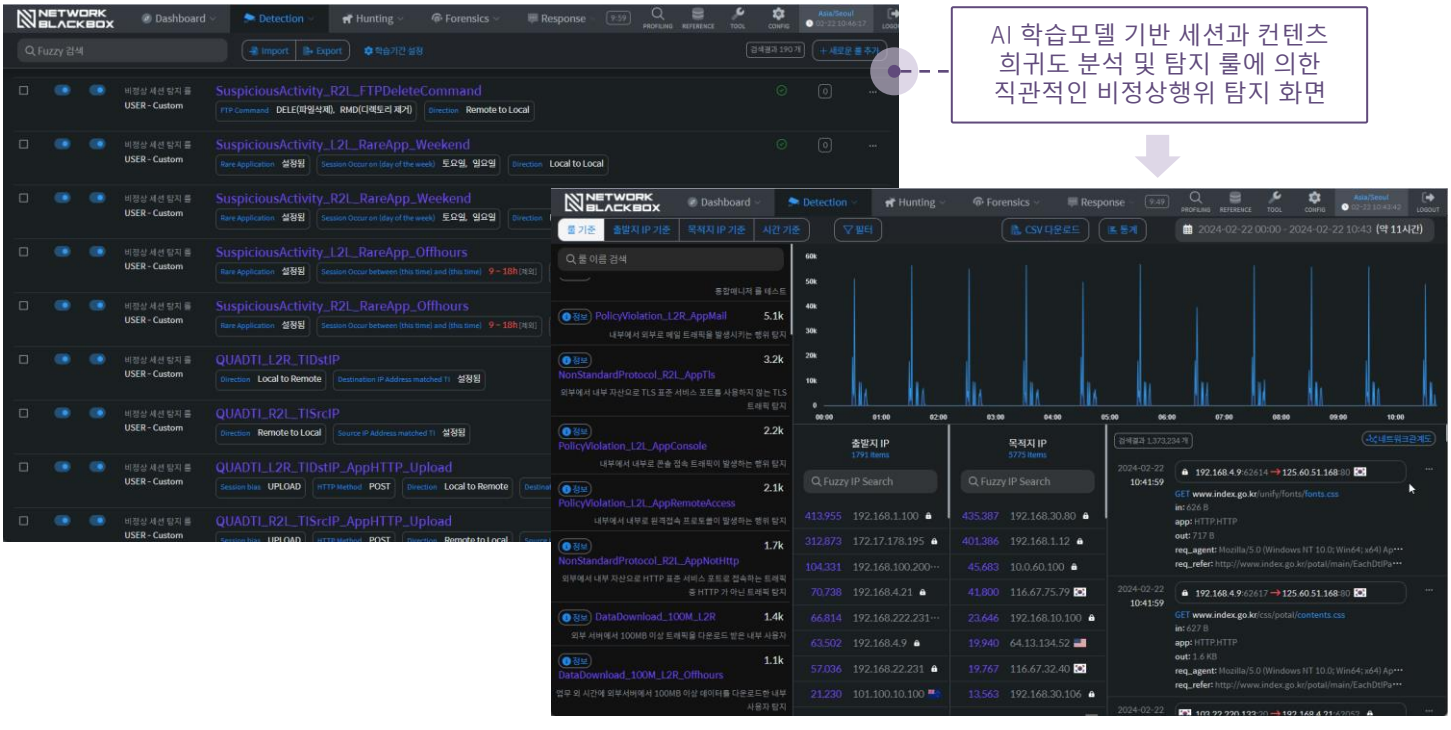
Network Blackbox v4.0 주요기능 – 위협 탐지 및 분석

주요한 공격에 대한 공격전술(TTPs)분석기반의 네트워크상의 위협탐지에서 분석 및 판단 후 대응까지 드릴다운 형태의 직관적이고 효율적인 위협탐지 및 대응 기능 제공



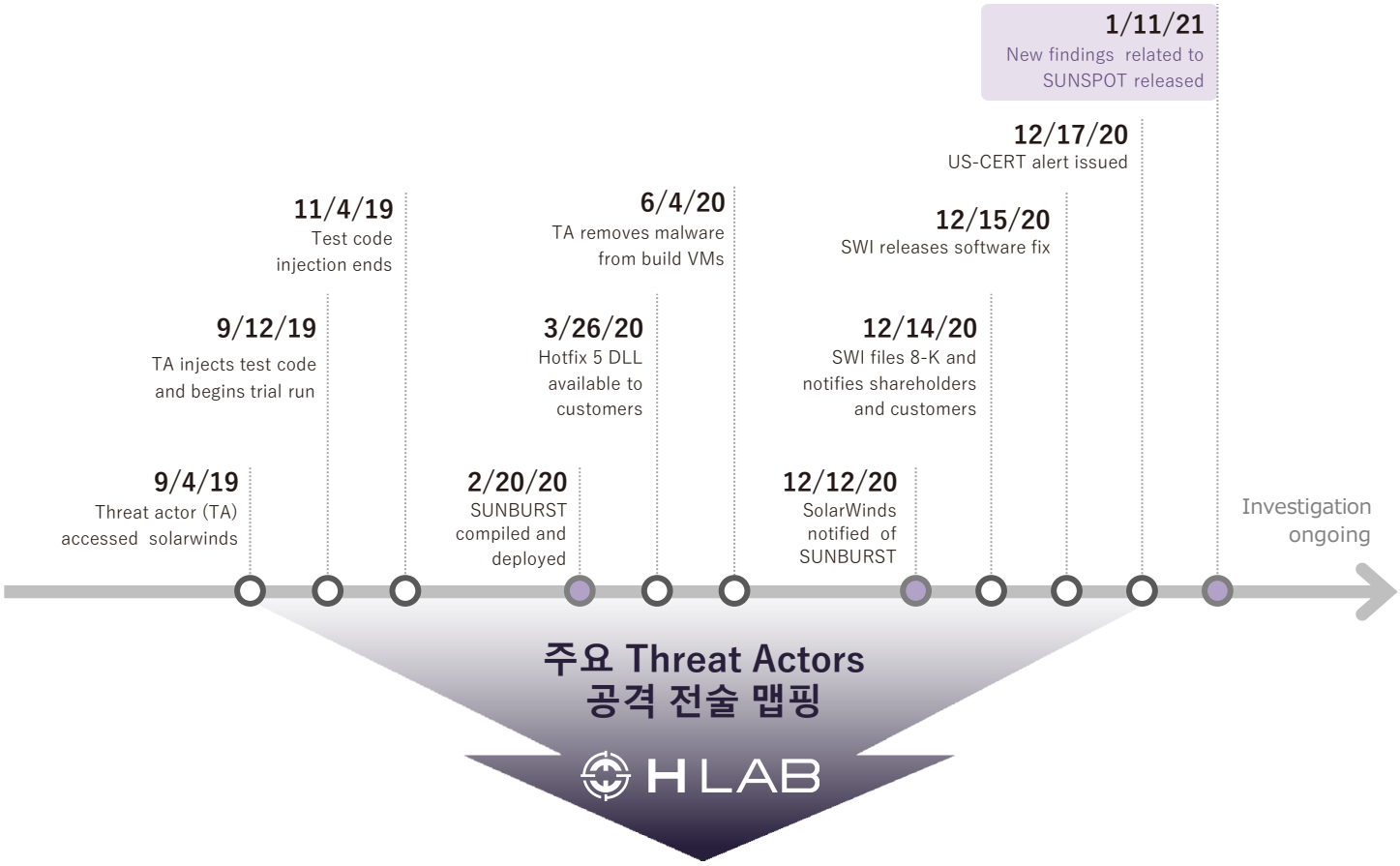
Network Blackbox v4.0 주요기능 - 이상/비정상행위 탐지 및 분석

AI 기술을 이용한 이상 및 비정상행위 탐지와 위협정보(CTI)를 이용한 주요 침해사고의 IoC 및 IoA 기반 탐지

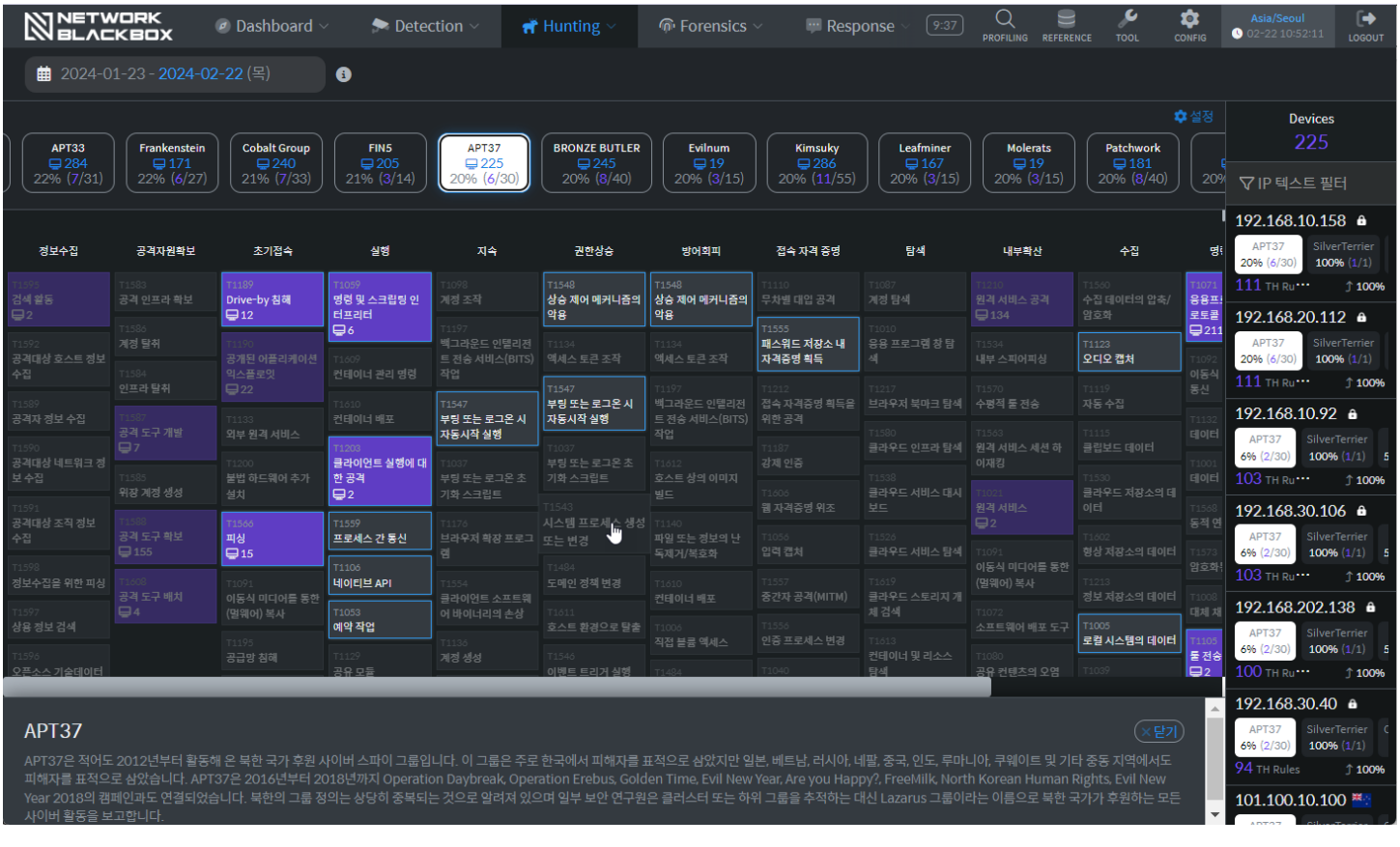


Network Blackbox v4.0 주요기능 - 시계열 시각화기반 위협헌팅

최신 침해사고에 대한 공격전술(TTPs) 분석 및 MITRE AT T&CK 맵핑된 위협헌팅 룰 생성

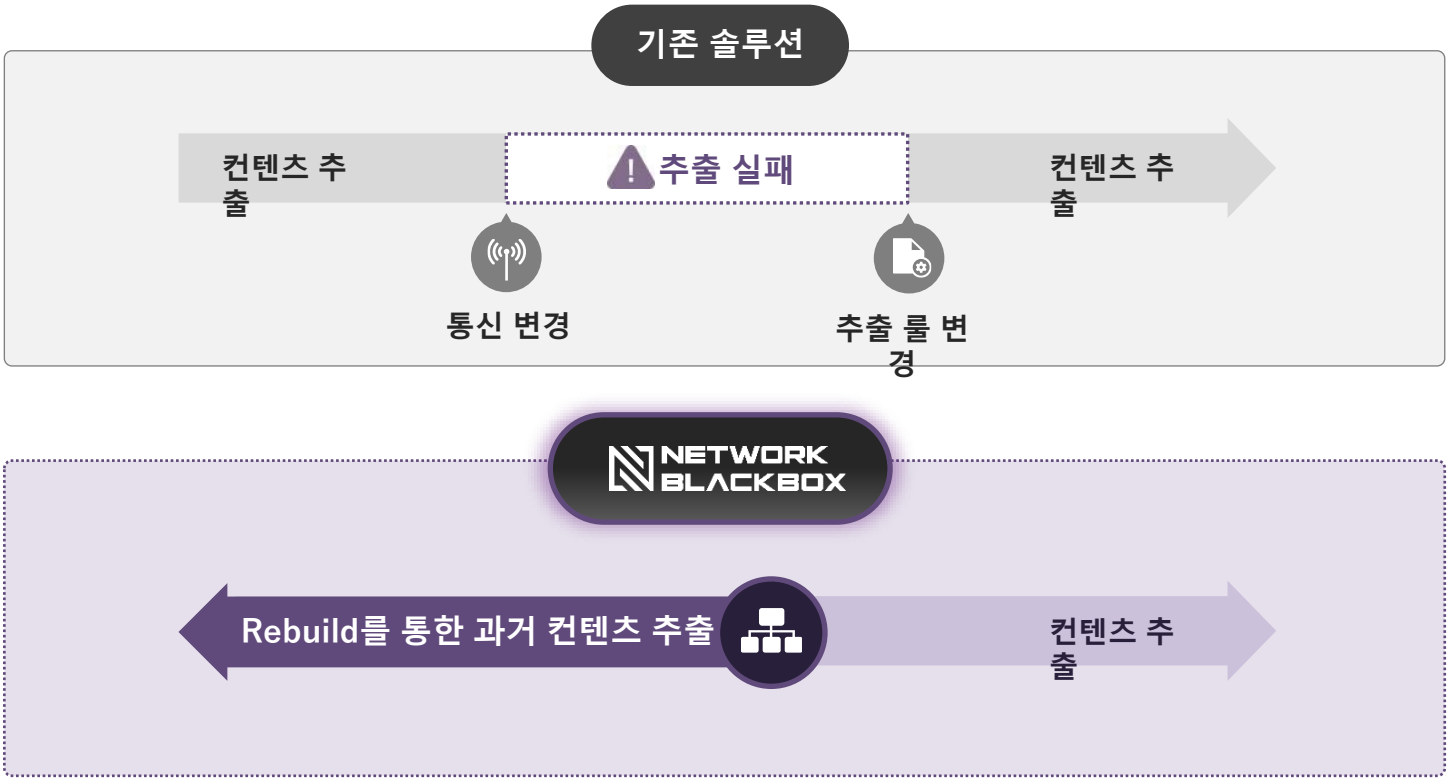


자사 위협헌팅 전문연구원에 의한 최신 침해사고 및 적대적 위협그룹 대상 위협헌팅룰 생성 및 배포,
복합적인 공격 전술기반의 잠재된 위협을 시계열형태로 시각화



Network Blackbox V4.0 주요기능 - 트래픽 리빌드

컨텐츠 추출 및 회귀적 분석(Retrospective Analysis)을 위한 풀패킷 스트림 리빌드



Network Blackbox v4.0 주요기능 - xSec 기반 확정적 증적 추출

고속 검색, 패킷 상세 정보부터 사용자 화면 복원, 파일추출, 세션기반 PCAP 다운로드 및 보존

55종의 검색 조건

빠른 검색

패턴 기반 색인 처리
기술을 기반으로
빠른 검색을 제공합니다.

특허10-2019-0073261

다양한 조건

25종의 Header/ Meta
/Session조건과 30종의
웹 Meta조건을 제공합니다.

다양한 통계

세션 및 Bytes 기반
트래픽은 물론 출발지,
목적지, 국가, Port 등
다양한 통계를 제공합니다.

Detail Packet Analyzer

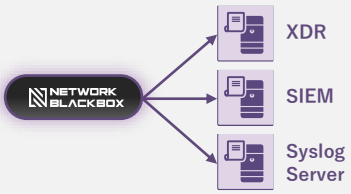
- Flow 정보
- Network Handshake
- Metadata
- Request/Response
- HEX
- 웹 화면 복원
- 파일 추출
- 패킷 격리
- Pcap download

Network Blackbox v4.0 주요기능 – 다양한 방식의 3rd Party 연동

자체 Syslog, Rest API 및 타사 API 기반 개발 등, 다양한 방식의 높은 타사 솔루션 연동 및 호환성 지원

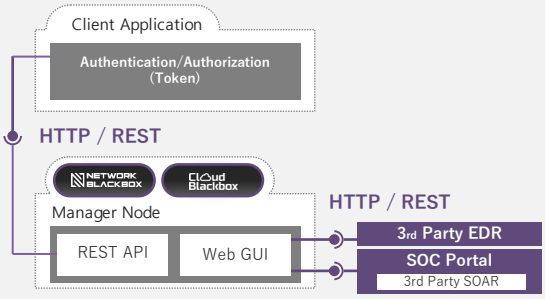
❶ Network Blackbox Syslog

- **CEF**(Common Event Format) Syslog 형태로 전송
- 동시에 **다중 목적지로 동시 전송 지원**
- Syslog **유형별 선택적 전송 지원**
- **Syslog 유형**
  - ✓ 시스템 로그
  - ✓ Audit 로그
  - ✓ 세션 로그
  - ✓ 탐지 로그
  - ✓ 메타 로그



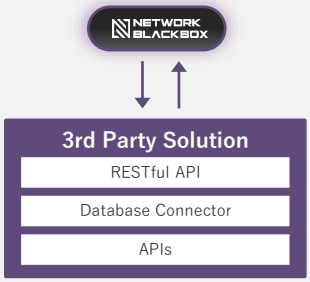
❷ Network Blackbox RESTful API

- 자체 제공 RESTful API를 3rd Party 솔루션에서 **호출 형태** 통합
- Network Blackbox 에 저장된 다양한 형태의 데이터 **검색, 조회, 전송** 지원
- **지원 API**
  - ✓ 세션 조회
  - ✓ 컨텐츠 검색(파일 포함)
  - ✓ 패킷 상세 조회
  - ✓ 탐지룰 조회

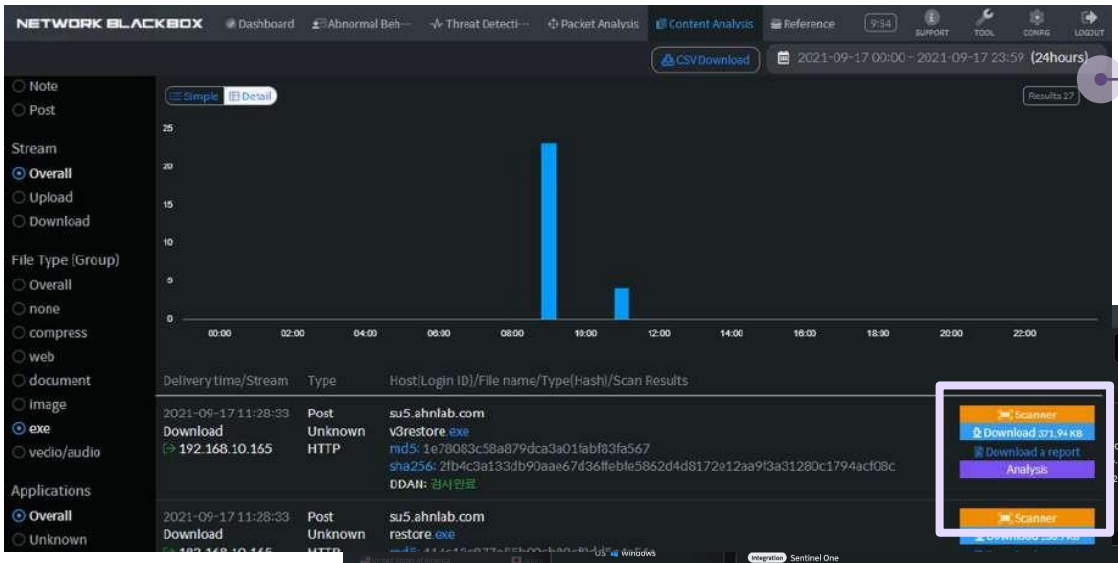


❸ Develop using 3rd party API

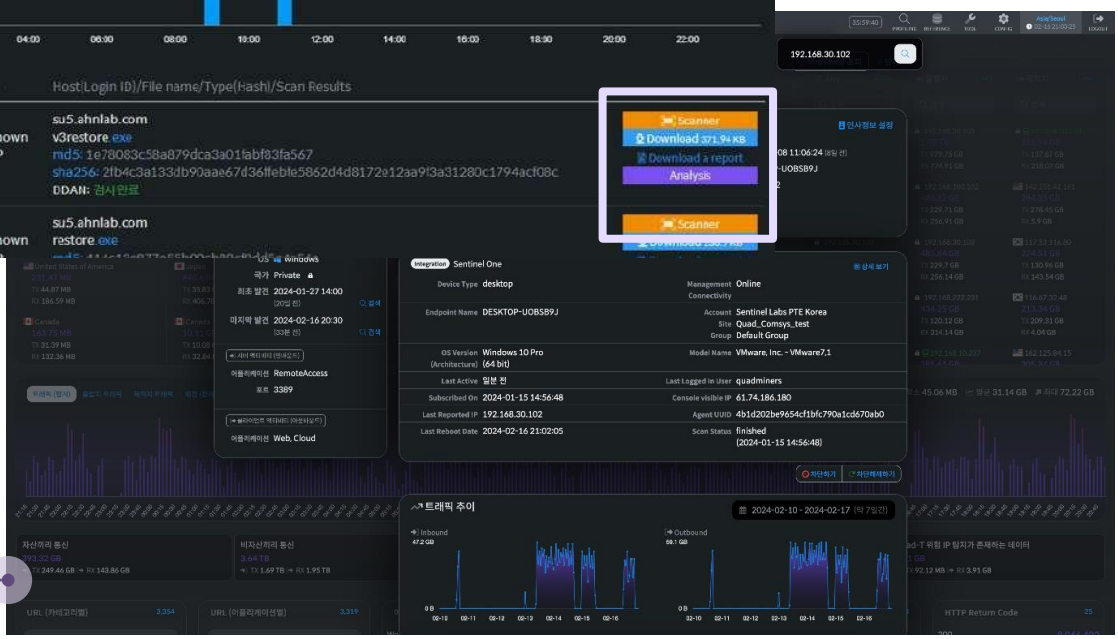
- 3rd Party 에서 제공하는 다양한 방식의 API 및 통합방식을 토대로 한 **Network Blackbox 기능 개발**
- 상호간 **Interactive한 동작 필요 시 권장**되는 통합방식
- 개발범위에 따라 **추가적인 비용 필요 할 수 있음**



<3rd Party APT 솔루션 연동 예시 화면>



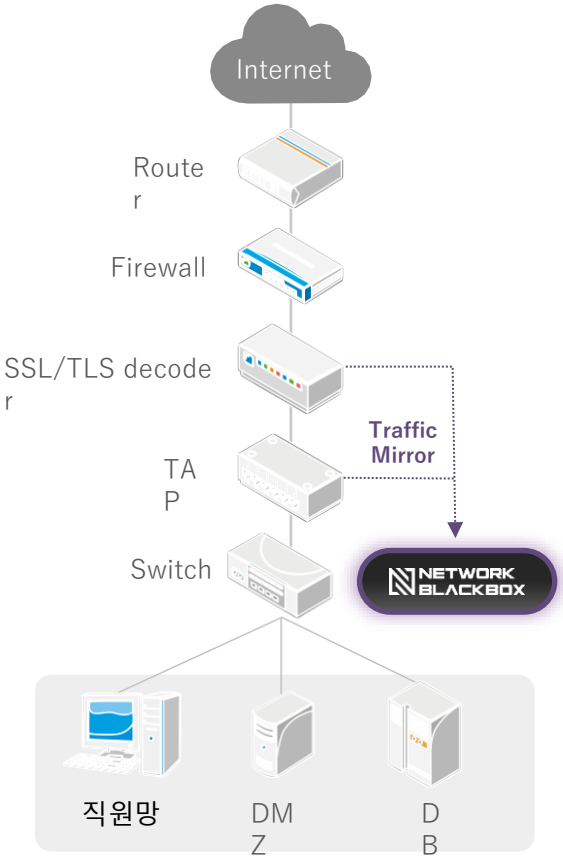
APT 솔루션 연동을 통해 추출한 파일 악성여부 검색과 동적 분석 연동 예시



EDR 솔루션과의 연동을 통한 IP Profiling 정보상에 단말정보와 더불어 IoC와 최근 스캔 정보 표기 예시

Quad Miners NDR- Network Blackbox- 기본구성

사고 기록 전체를 분석하는 항공기 블랙박스처럼 네트워크 트래픽 전체를 손실 없이 수집해서
사이버 보안 위협을 탐지하고 분석합니다.



빠른 구축 / 시스템영향

- 별도로 PC에 프로그램(에이전트)을 설치할 필요가 없습니다.
- 패킷을 미러링하기 때문에 네트워크 망에 어떠한 영향도 없습니다.

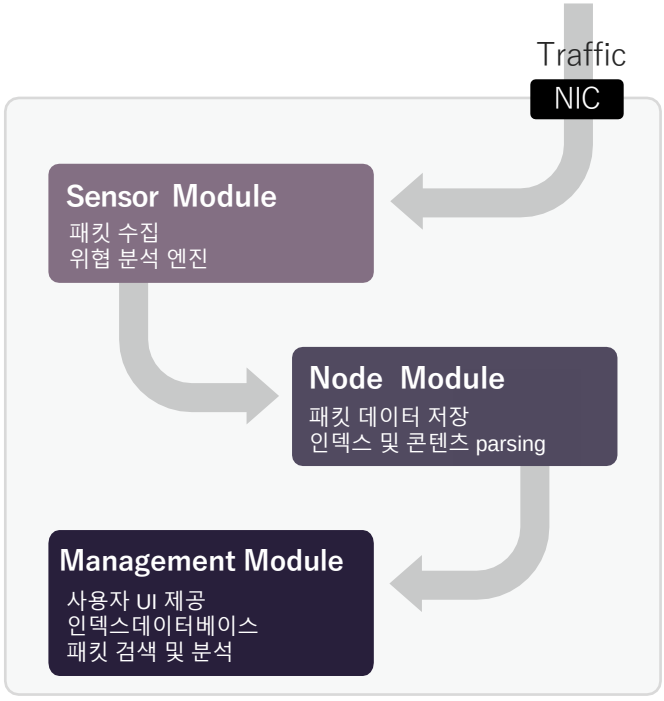
복호화 장비 연동

- 복호화 프록시 장비가 있을 경우, 해당 장비로부터 복호화된 패킷을 미러링하여 저장 가능합니다.

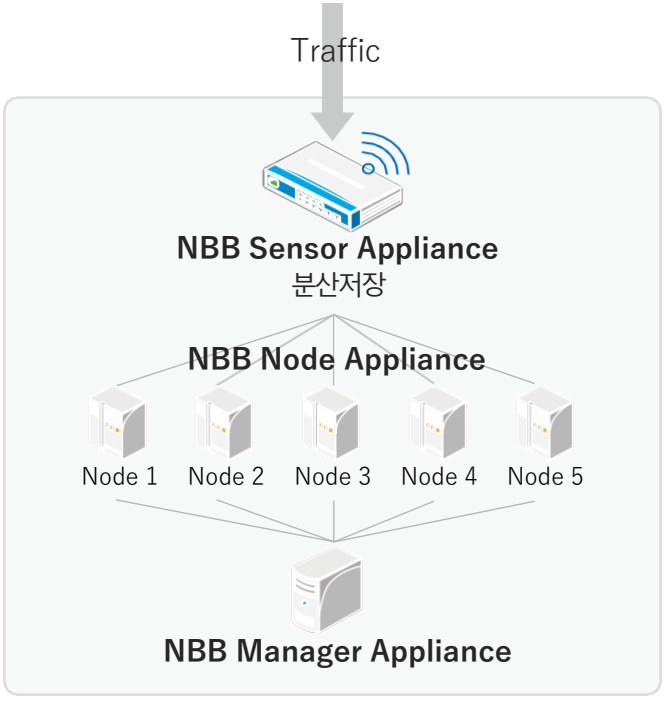
Agentless

- 별도 PC에 프로그램(에이전트) 설치 필요 없음

Quad Miners NDR- All-in-one과 확장형 구성



All In One



Expanded

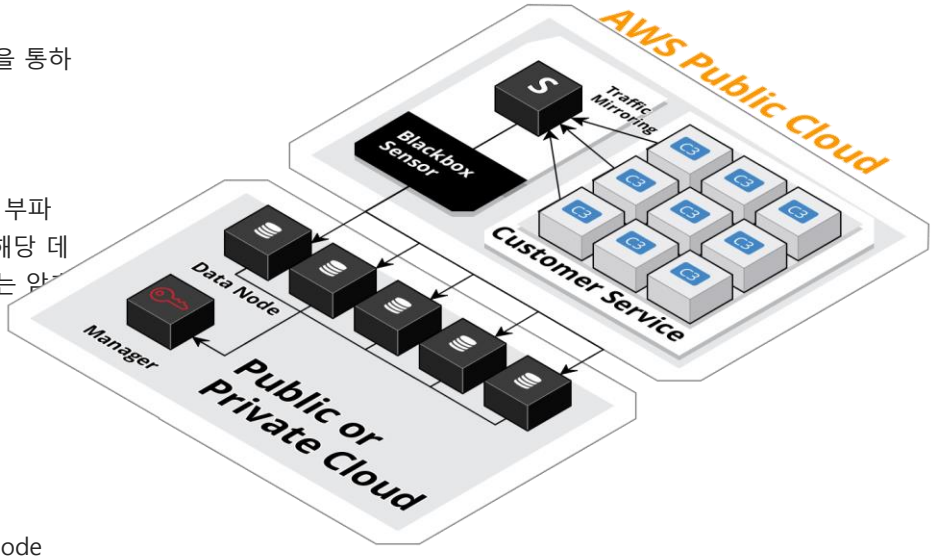
Quad Miners NDR- Cloud Blackbox - 구성 방식

AIO 모델과 확장형 모델을 모두 지원하나, DATA 관리 측면에서 확장형 모델 권장

Cloud Blackbox

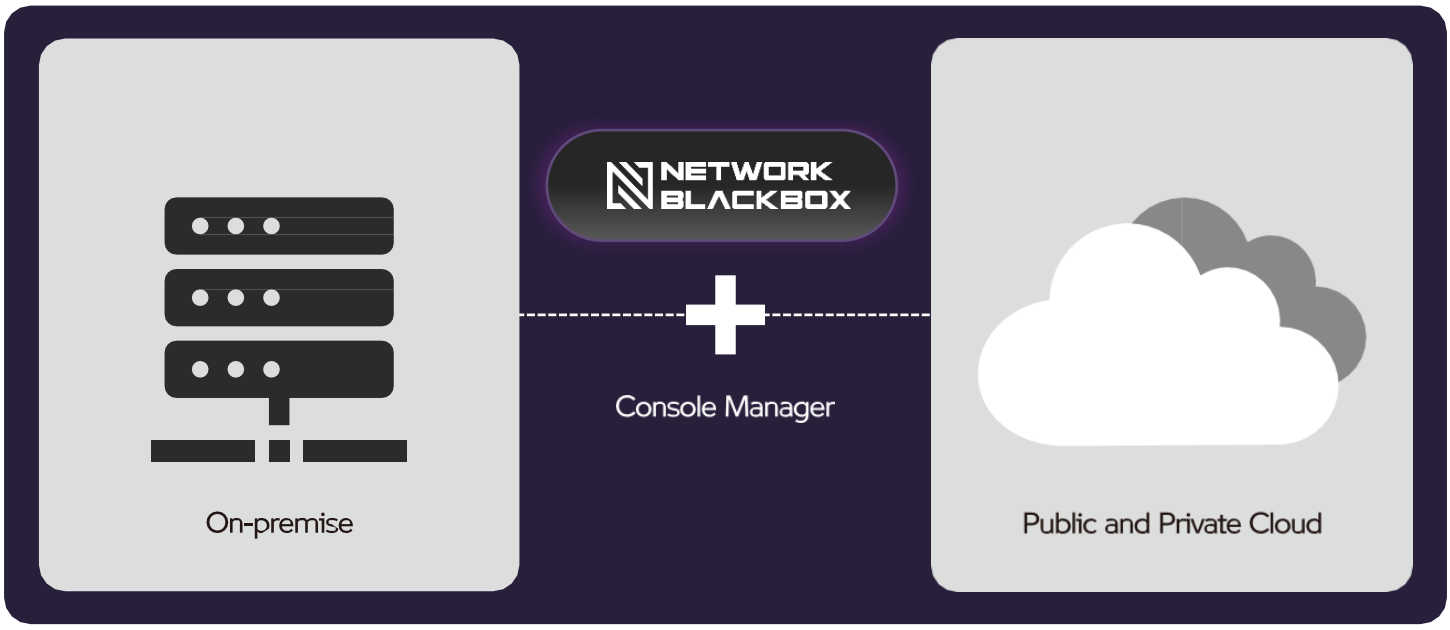
아래와 같은 작업을 수행할 수 있습니다

- 클라우드 블랙박스의 센서는 고객의 APC에 별도의
  인스턴스로 설치되며 트래픽 VPC 미러링을 통하여
  데이터를 수집하고 분석합니다.
- 센서에서 만들어진 각종 메타데이터 및 첨부파일 등은 CBB Node Instance에 저장되며 해당 데이터는 CBB Manager Instance 서버에 있는 암호화 키로
  암호화 저장합니다.
- 고객은 매니저에 접속하여 모든
  데이터를 확인하며 분석하게 됩니다.
- CBB Node의 저장공간을 늘리려면 CBB Node Instance를 확장하여 분산저장 할 수 있으며,
  저장공간 확보 및 검색속도를 더 높여줍니다.



Quad Miners NDR- Product

네트워크 장애 포인트 없이 어디에서나 풀 패킷 수집 및 분석 수행



Public 은 물론 Private Cloud(K85)까지 하이브리드 클라우드 환경 지원

Why Quad Miners NDR?

확정적 증적을 토대로 설명가능한 인공지능(XA) 보안관제 체계화 지향

기존 네트워크 보안 위협 분석/탐지 기술 및 문제점

- 피동적 분석 및 방어
- 각 시스템간 통합의 어려움
- 탐지-대응 소요시간 증가
- 이동성 고려 결여
- 통합 후 유지관리의 어려움
- 구성의 복잡성
- 운용/전문 인력 요구 증가
- 도입/운용 비용 증가

해결방안

기대효과

- 네트워크 보안 위협 분석/탐지체계 통합 및 단순화
- 탐지된 위협에 대한 자동 증적화, 탐지-대응 시간 최소화
- 알려지지 않은 공격에 대한 능동적 대응
- 단일시스템화, 이동성 및 호환성 문제 해결

Xsec 기반 사이버 공격 능동 감시 통제 시스템

풀-패킷 분석 데이터 자동 증적화 및 보고

인공지능 기반 다면분석 비정상행위 탐지기술

TTP 기반 자동화된 위협 헌팅 기술 및 시계열화

+

- NIDS 탐지 및 대시보드
- 패킷 분석 및 재조합 기능
- 통계기반 비정상행위 탐지기능
- 컨텐츠 추출, 재현, 분석 기능
- Q-Link 빅데이터 엔진
- 패턴 기반 색인 처리 기술 (패킷 최적화 처리)
- 초고속 메타데이터 다중 검색 기술 (R-Search 검색 엔진)
- 고성능 패킷 스트림 저장 기술 (패킷스트림 DB)

글로벌 성과와 경쟁력

글로벌 리서치 기관인 가트너에서 Quad Miners를 NDR 영역 대표 벤더로 선정(2020-2021)

03/25/2021 Gartner

Emerging Technologies: Adoption Growth Insights for Network Detection and Response

Published 24 March 2021 - ID G00743919 - 19 min read

By Analysts Nat Smith, Christian Canales, Josh Chessman

Initiatives: Emerging Technologies and Trends Impact on Products and Services

The network detection and response market continues to grow quickly, but trends within the market are stabilizing. To maximize revenue, product leaders should focus roadmaps and go-to-market efforts on the government industry, larger companies and technical role buyers.

- MixMode (Network Traffic Analytics)
- Plixer (Plixer Scrutinizer)
- Quad Miners (Network Blackbox)
- Tencent (T-Sec NTA)
- Vectra (Cognito)
- Vehere (PacketWorker)
- VMware (Lastline Defender)

03/25/2021 Gartner

Emerging Technologies: Adoption Growth Insights for Network Detection and Response

Published 24 March 2021 - ID G00743919 - 19 min read

By Analysts Nat Smith, Christian Canales, Josh Chessman

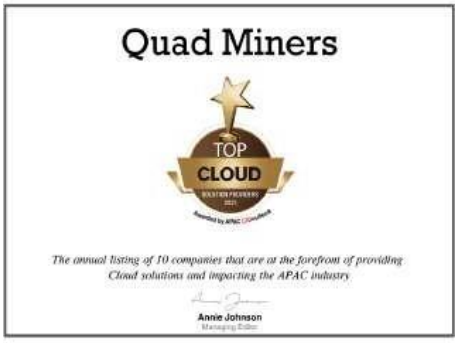
Initiatives: Emerging Technologies and Trends Impact on Products and Services

The network detection and response market continues to grow quickly, but trends within the market are stabilizing. To maximize revenue, product leaders should focus roadmaps and go-to-market efforts on the government industry, larger companies and technical role buyers.

- MixMode (Network Traffic Analytics)
- Plixer (Plixer Scrutinizer)
- Quad Miners (Network Blackbox)
- Tencent (T-Sec NTA)
- Vectra (Cognito)
- Vehere (PacketWorker)
- VMware (Lastline Defender)

Quad Miners 기술력 (기술특허 및 국제인증)

글로벌 수상 경력



Top Cloud
Solution Providers 2021
by APAC CIO Outlook
(2021年)

Top Tech Company of 2020
by APAC Business Headlines
(2020年)

Top 10 Cyber Security
Solution Providers – 2019
by APAC CIO Outlook
(2019年)

Quad Miners NDR- Network Blackbox- Win case

1 Energy

Network Blackbox의 풀패킷 기반 기술의 차별성을 이용한
글로벌 기업의 보안관제 고도화 사례

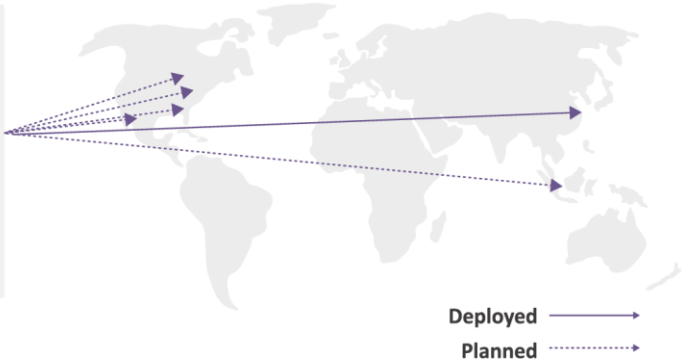
Quad Miners

NETWORK BLACKBOX

MSPP

원격관제
IT/OT
통합보안관리

글로벌 기업 생산 시설



Background

- 전세계 배터리 산업을 선도하고 있는 에너지 분야 기업으로 생산 시설의 글로벌화 추진
- 국내 MSSP사에서 한국은 물론 해외 생산시설의 보안관제 서비스 제공
- ICS 에 대한 보안 강화 목적으로 다양한 솔루션 검토 중

Challenge

- 탐지된 보안 위협에 대한 현업 시스템 직접 분석 불가
- 위협 확인 및 대응 시간 지연
- IT 및 OT 영역에 대한 제한적 보안 가시성
- 각 지역의 생산시설별로 일관되지 않은 보안 모니터링 및 대응
- 위협 탐지-확인-대응에 대한 전문가 부족

Solution

- MSSP사 블루팀 주관 경쟁 PoC 에서 모의침투 테스트 → NBB 위협 탐지 및 분석 비교 평가 1위 (경쟁사 Darktrace, Stella Cyber, Nozomi)
- 풀패킷 기반의 위협탐지 및 확정적 증적 제공 기능
- ICS 관련 프로토콜 및 어플리케이션 식별과 정보 수집
- 통합 보안관리 콘솔상에서 단일 뷰 모니터링 및 분석

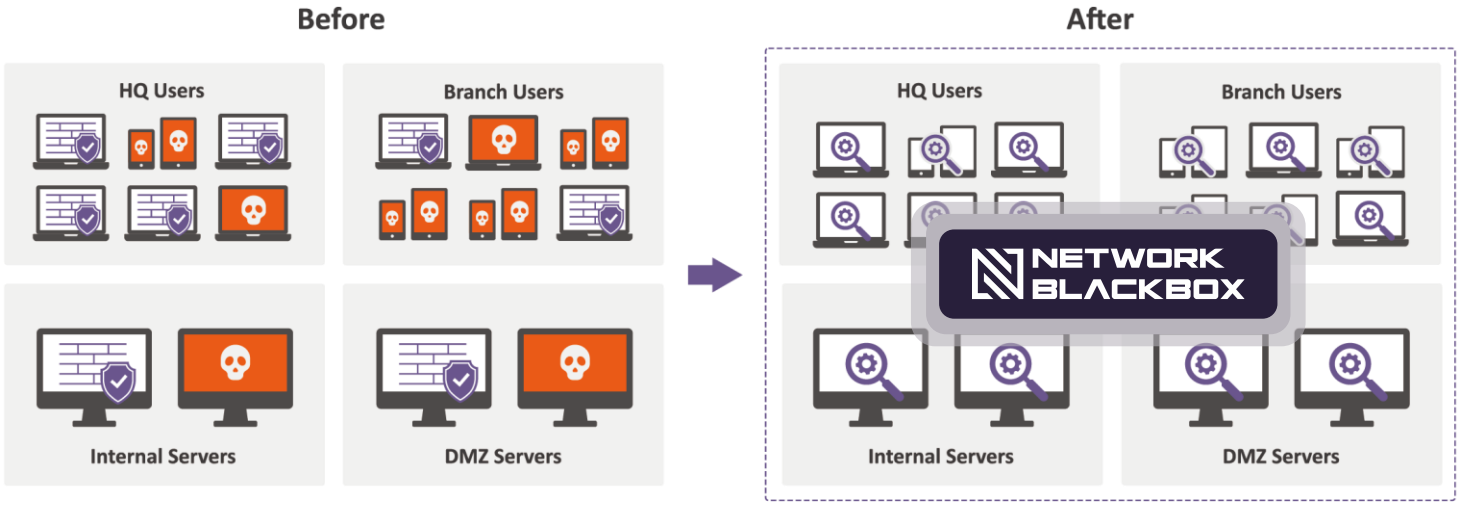
Outcome

- 풀패킷 기반의 확정적 증적을 기반으로 한 MTTD, MTTR 단축
- 소수의 보안인력으로 국내는 물론 글로벌 생산 시설까지 일관된 보안 관제 프로세스화 및 효율화
- IT 및 OT 영역에 대한 보안 가시성 확보

Quad Miners NDR- Network Blackbox- Win case

② Banking

본사 및 지점 랜섬웨어 대응 사각지역 해소 및
전사적 통합 검역소 구축 사례



Background

- 국내 No.1 은행
- 본사 및 다수의 지점과 다중 데이터센터 운영
- 본사 – 지점간, 본사 및 지점 – 데이터센터간 그리고 대고객 서비스망 상의 트랜잭션

Challenge

- EPP/EDR 위주의 악성코드 및 랜섬웨어 대응 체계
- Agent 가 설치되지 않은 다수의 단말 및 IOT 단말 그리고 서버에서의 악성코드 감염 사각지대 발생
- 인터넷망 위주의 경계보안 집중

Solution

- 코어 및 백본 스위치에서의 South-North, East-West 트래픽 미러링
- NPB를 이용한 중복제거 및 세션기반 미러링 트래픽 로드밸런싱
- Network Blackbox 를 이용한 파일 전수 추출
- Network Blackbox 와 멀티 APT 엔진연동을 통한 통합검역소화

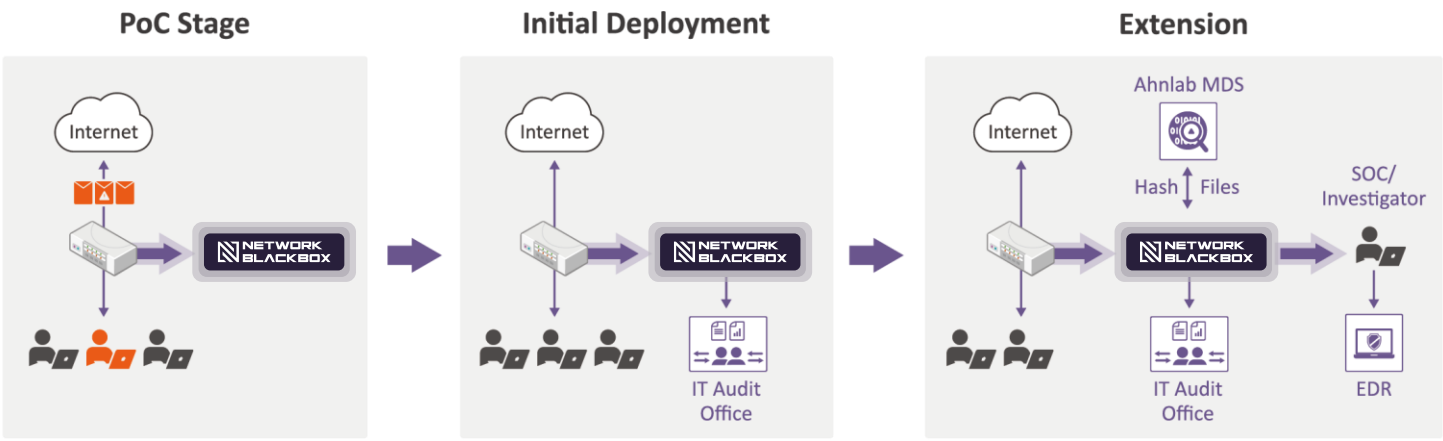
Outcome

- 사각지역 없는 악성코드 대응 체계 구축
- 효율적인 파일 해쉬값 및 원본파일 동적 분석을 통해 전체 트래픽상의 파일 전수 검사
- 다중 APT 솔루션 연동을 통한 악성코드 분석 및 대응 체계화

Quad Miners NDR- Network Blackbox- Win case

❸ Securities

금융사 poc를 통한 개인정보 유출 정황탐지,
도입 후 APT 솔루션 연동 확장 운영 사례



Background

- 국내 No.1 증권사
- 애널리스트들의 업무 특성상 투자 정보 획득을 위한 안전한 인터넷 사용 보장 필요
- Shadow IT 업무환경에 대한 보안대책 필수

Challenge

- Shadow IT → 애널리스트들의 다양한 방식의 정보 교환(e.g. Cloud, Web Mail, SaaS File Exchange)
- DLP 솔루션을 보유하고 있으나 보안정책이 적용되는 어플리케이션 제한으로 사각지역 발생
- IT 감사실의 지연된 대응

Solution

- Custom Application Parser 제공, 경쟁 PoC에서 유일하게 정보유출 정황 탐지 (경쟁사 RSA, Darktrace)
- 초기 인터넷망 풀패킷 수집 및 컨텐츠 감사 정책 위반 탐지적용
- 파일 동적분석 시스템 (Ahnlab MDS) 연동, 인터넷 구간 파일 전수 검사 및 SOC 연계 EDR 실시간 대응 시스템으로 확장

Outcome

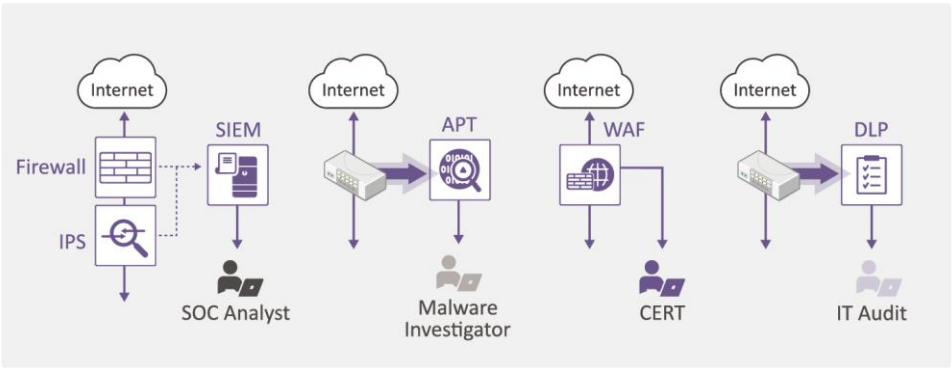
- Shadow IT 환경에서의 IT 감사활동 사각지역 축소
- 인터넷을 통한 악성파일 및 정보 유출에 대한 동시 보안과 실시간 대응 시스템화
- 침해사고에 대한 가시성 확장 및 대응시간 감소

Quad Miners NDR- Network Blackbox- Win case

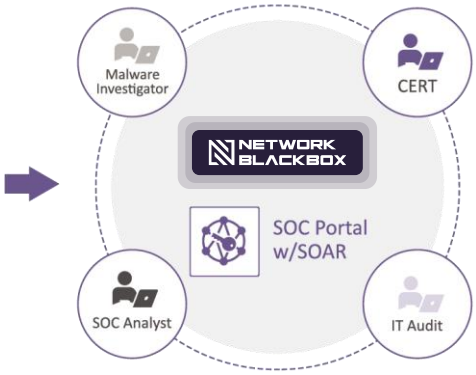
❹ eCommerce

대규모 트랜잭션 환경에서의 사일로화된 대응체계,
전체 보안팀 체계 일원화 및 증적 데이터 공유 시스템화

Before



After



Background

- 글로벌 초대형 e-Commerce 회사
- 사용자 1500만 명 이상, 매일 수억 건의 인터넷 주문 거래
- CI/CD를 넘어 실시간 컨텐츠 변경 지속
- 다양한 부서에서의 커뮤니케이션

Challenge

- 사일로화된 보안 제품의 배치
- 각 보안 팀별 담당 보안솔루션 및 보안 활동
- 동일한 보안 위협 및 침해사고에 대한 각각의 분석결과
- 내부망 통신에 대한 보안 가시성 결여 (East-West)

Solution

- SOC 포털을 통한 관련 보안팀 업무 창구 일원화
- 내외부 통신에 대한 Full Packet Capture 기반의 트래픽 전수 검사
- Network Blackbox 를 이용한 보안위협 및 침해사고 증적 공유
- 대응 프로세스상 관련 보안 팀별 대응 절차화

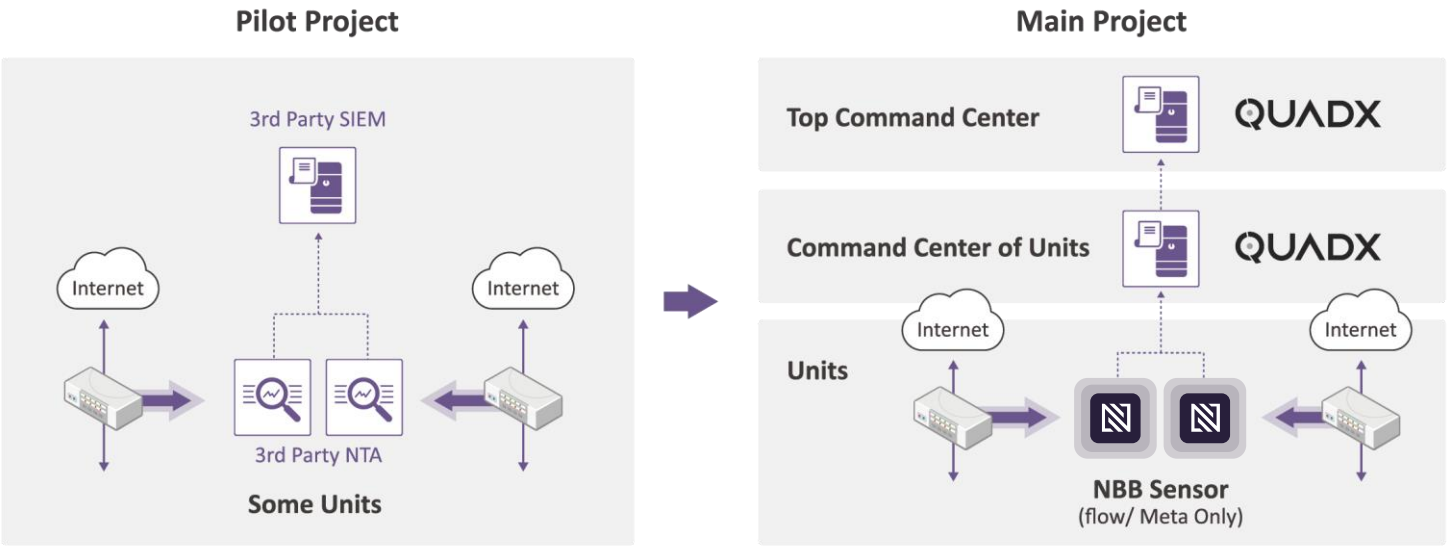
Outcome

- 보안 위협 및 침해사고 분석에 대한 단일뷰 형태의 정보공유
- 유형별 지연 없는 대응 프로세스 화로 탐지, 분석 및 대응 시간 단축
- Lateral Movement 에 대한 위협 탐지 및 연계 대응 구현

Quad Miners NDR- Network Blackbox- Win case

❺ Military

전군 플로우 및 메타데이터 기반 트래픽 분석 체계 구축 완료, 풀패킷기반 트래픽 전수검사 필요성 검증 사례



Background

- 특정 군 사용자 망(인터넷, 인트라넷)에 대한 플로우/메타 기반의 분석 시스템 파일럿 테스트 완료
- 기존 보안 인프라스트럭처와 NTA 간의 운용 효용성 검증 완료
- 전군 확대 필요

Challenge

- 군체계 상 전군 통합 분석 시스템화 필수
- 전국지역에 대한 안정성 있는 정보 수집 체계화
- 기존 보안운영체계를 즉시적으로 지원 가능한 데이터 분석 능력 필수 요건화

Solution

- 경쟁 PoC를 통한 QuadX 솔루션의 통합관리 및 분석 체계화 검증
- 군특성에 맞는 비정상, 위협 및 컨텐츠 탐지 기능화
- 전국지역 최단기간 체계 구성
- 자사 데이터 분석가 파견 지원

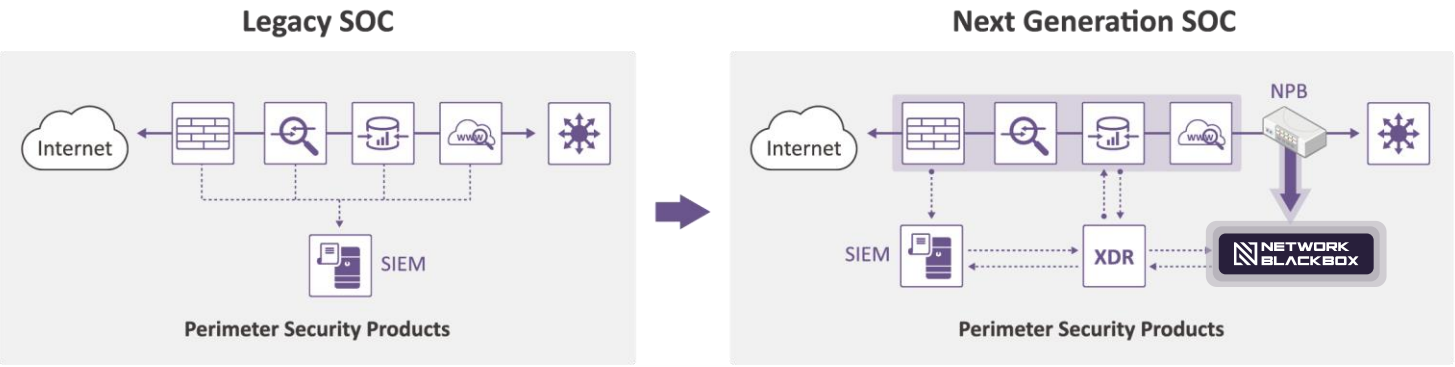
Outcome

- 전군 메타 및 플로우 기반 데이터 분석 체계화
- 최상위 센터에서의 전군 모니터링 및 분석 체계 통합
- 전군 사용자에 대한 Cyber Warfare 대비 태세 지원
- 풀패킷 캡처기반 트래픽 전수검사 체계화로의 마이그레이션 필요성 확보

Quad Miners NDR- Network Blackbox- Win case

6 Government

보안 침해와 관련된 응답 시간을 줄이기 위한
고급 보안 운영 체제 구현 사례



Background

- 글로벌 정부기관 통합 인터넷망 다중 경계 보안 구성
- 중앙 집중식 통합보안관제
- 보호대상 시스템 담당 기관, 부서 및 담당자 다수
- Digitalization 가속화

Challenge

- 탐지 또는 발생된 보안 이벤트 중심의 메뉴얼한 모니터링 집중
- 사일로화된 보안 이벤트 분석 체계
- Victim 시스템에 대한 탐지된 보안 이벤트의 위험도 및 영향도 확인불가 또는 지연 발생

Solution

- Network Blackbox를 이용한 풀패킷 캡처 기반 트래픽 전수검사 결과로 증적 수집
- 신규 XDR(Stellar Cyber)과 기존 SIEM, 그리고 NBB 간의 통합 기능으로 자동화된 분석체계화
- 네트워크상의 구성변경 최소화

Outcome

- 선진화된 보안운영시스템화
- 확보된 증적을 토대로 공격의 위험도 및 영향도 즉시 확인
- MTTD, MTTR 최소화
- 정부 내부 트래픽 보안 강화 가능성 확인 및 2차 프로젝트화

NOTE

Provides Intuitive and Precise
Cyber Defense Solutions to the world

NETWORK BLACKBOX QUADX Cloud Blackbox PcapBox CYBER DEFENSE BLACKBOX

Contact Us

Korea : DREAUM 6F Sunghong Tower, #138 Teheran-ro, Gangnam-gu, Seoul, South Korea(F 06236)

Japan : Kasumigaseki Bldg. 5F. 3-2-5, Kasumigaseki, Chiyoda-ku, Tokyo, Japan (T 100-6005)

USA : 16310 NORTHERN BLVD STE 311 FLUSHING, NY 11358-2666

Singapore : 9 Straits View, Marina One West Tower #05-07 Singapore (018937)

sales@quadminers.com 02-548-112 0507-803 559 https://www.quadminers.com