조달청 디지털서비스몰 1등급 GOOD Software

Security AI Network Data Society

NDR 솔루션 (Network Detection and Response)

MNX

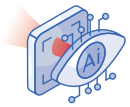
네트워크 상의 모든 트래픽을 수집-분석-기록하여 가시성을 확보하고, 이상 징후를 탐지하여 자동으로 대응하는 NDR 솔루션입니다.

MNX 소개

디지털 자산을 보호하기 위해서는 유출입되는 네트워크 트래픽을 모니터링하고 관리할 수 있는 정교한 솔루션이 필요합니다.
MNX는 모든 네트워크 트래픽 실시간으로 수집하고, AI를 활용해 위협과 이상 징후를 빠르게 탐지합니다.
보안 담당자는 시나리오 기반의 PlayBook을 이용해 위협을 효과적으로 관리할 수 있고, 즉각적인 대응이 가능합니다.

01 위협 이중 탐지

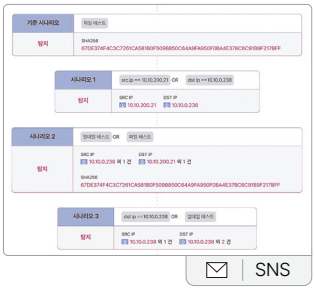
시그니처 기반은 물론 MNX만의 AI 모델을 활용한 이중 탐지로 위협을 빠짐없이 검출해냅니다.



시그니처	AI 모델
Suricata	DGA 모델
Yara	악성탐지
⋮	

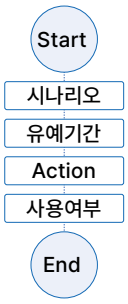
02 위협 시나리오

원하는 탐지 조건을 시나리오로 생성해 특정 위협을 빠르게 식별할 수 있습니다.

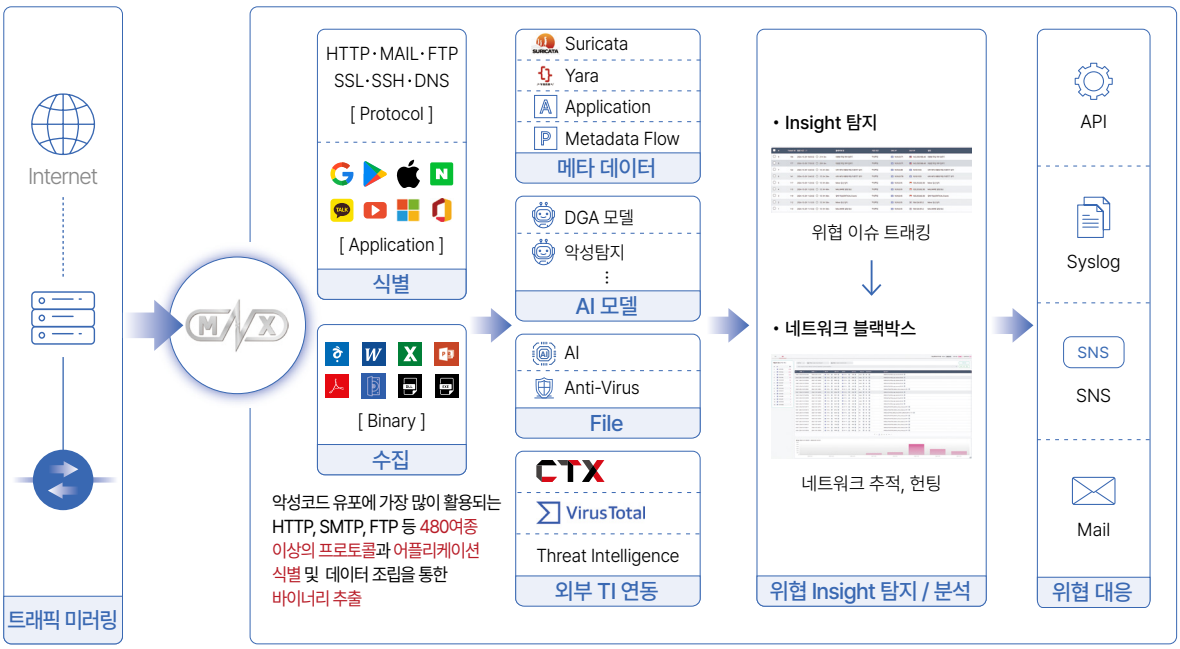


03 PlayBook

위협 탐지 시 관리자가 등록한 PlayBook에 따라 위협을 자동으로 알리고 대응합니다.



세부구성



핵심기술

*Data Plane Development Kit 인텔에서 공개 SW로 발표한 인텔 NIC 전용 고속 네트워크 패킷 처리 기술

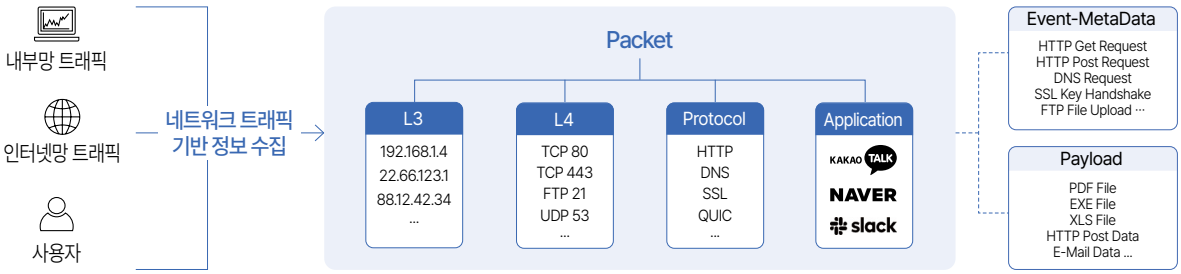
Step1. 수집 40Gbps DPDK* 기반 트래픽 무손실 수집

스위치 포트 미러링으로 커널을 거치지 않고 네트워크 카드에서 수신한 패킷을 직접 받아 서비스 장애 및 패킷 손실 없이 대용량 네트워크 트래픽을 빠르게 수집합니다. 네트워크에 연결된 IT 기기들을 식별하여 최신의 자산 인벤토리를 유지하고 자체 MNX 센서를 통해 패킷 처리 성능 저하 요소들을 해결하였습니다.

패킷 처리 성능저하 요소	DPDK 기반 MNX 패킷 수집
1 CPU 처리속도와 메모리/PCI 인터페이스 사이에서 발생하는 처리 속도 차이	1 다수의 패킷을 처리하는 I/O 최적화 기술인 배치 패킷 처리 기술 구현
2 네트워크 패킷마다 동적으로 패킷을 위한 버퍼 메모리 할당/해제	2 네트워크 패킷에 대한 고정 길이의 메모리를 사전 할당
3 공유 데이터 구조에 대한 접근으로 인한 병목 현상 시, 패킷처리 성능 저하	3 불필요한 대기시간이 발생하지 않도록 Lockless 큐 구현
4 리눅스 페이지 테이블 사이즈(4Kbyte)로 인한 TBL Miss 계속 발생	4 TBL Miss를 줄이기 위해 1GB Huge 페이지를 사용하는 기술 구현
5 최적화되지 않은 인터럽트 기반의 물리 NIC, 가상 NIC 드라이버	5 최적화된 폴 기반의 NIC 드라이버
6 멀티 프로세서 사용하더라도 성능이 Scale 되지 않음	6 Run-to-complete 모델을 통해 Horizontal Scalability 제공
7 리눅스 스케줄러의 Thread 스위칭 오버헤드	7 CPU Core Isolation 기술로 성능 향상

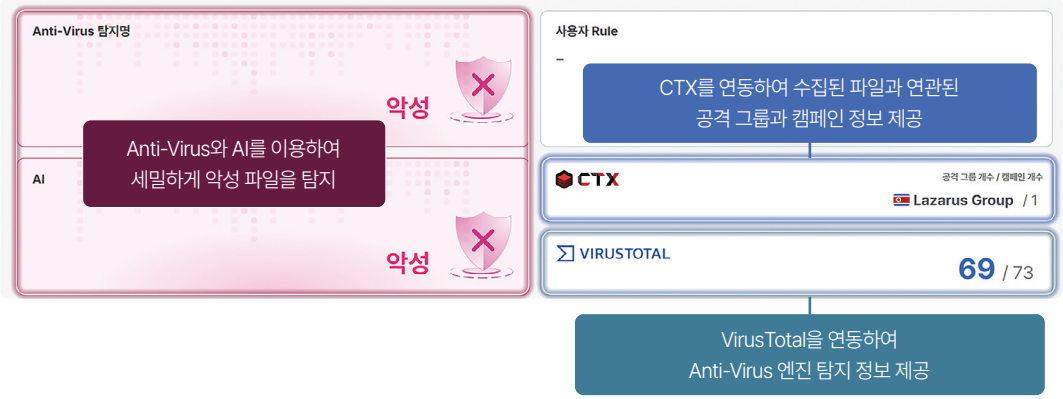
Step2. 분석 DPI(Deep Packet Inspection)를 통한 가시성 확보와 상세한 메타데이터 추출

네트워크 레이어의 최상위에 있는 L7 패킷 전체에 대한 검사를 수행, 480종 이상의 IT L7 프로토콜을 식별하고 파일의 악성 여부까지 분석합니다. 세션 별 SRC IP, DST IP, Protocol, Application 정보를 제공하여 상세한 트래픽 정보를 확인할 수 있습니다.



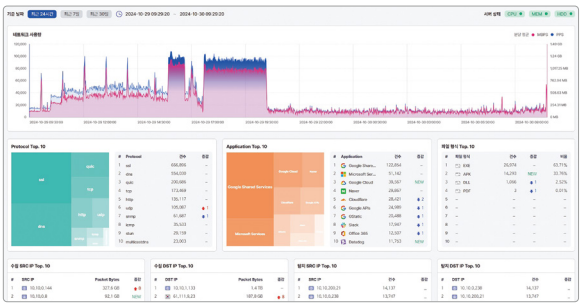
Step3. 탐지 심층적 악성 파일 탐지

자체 보유한 빅데이터 기반의 정제된 데이터셋으로 학습된 AI를 이용하여 알려지지 않은 위협을 식별하고, Anti-Virus로 알려진 위협을 식별합니다. 또한 다양한 TI(Threat Intelligence)를 연동하여 좀 더 세부적인 분석이 가능합니다.



주요기능

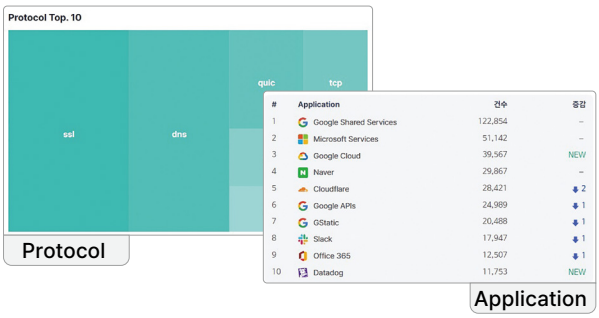
수집



네트워크 전체 트래픽 수집

- 유출입되는 전체 트래픽 수집·저장
- 식별된 모든 데이터 검색 가능
- 상세 Payload 확인 가능 (공격 성공 여부 등)
- 내·외부 공격 정보 확인 및 역추적 가능

분석

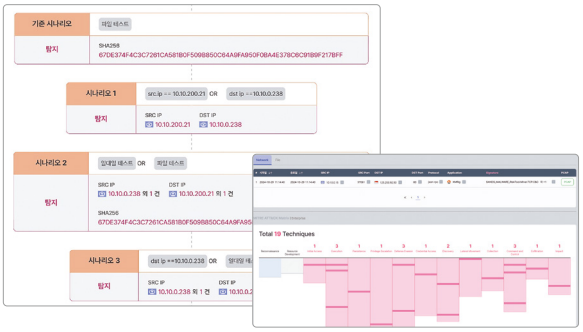


DPI 엔진 기반 심층 분석

- 자체 개발 DPI 엔진으로 Protocol 및 Application 분석
- 비인가 Application에 대한 내부 사용자 식별

Torrent | 비인가 VPN | Youtube | 과다사용 IP | ···

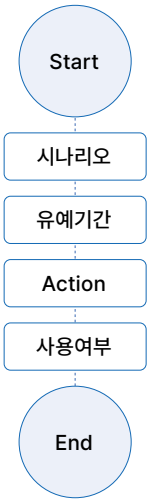
탐지



시나리오 중심 실시간 위협 탐지

- 네트워크 세션 베이스 상세 탐지 시나리오 생성
- MITRE ATT&CK T-ID 매핑 기능
- 위협 시나리오 100여 종 제공

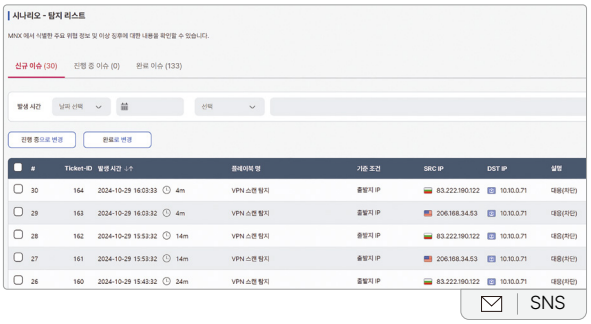
자동 대응



PlayBook 기반 자동 대응

- 단일/다중 시나리오 기반 PlayBook 생성
- SNS, Syslog, E-Mail, API 등 자동화 대응
- 자동화 대응 PlayBook 50여 종 제공

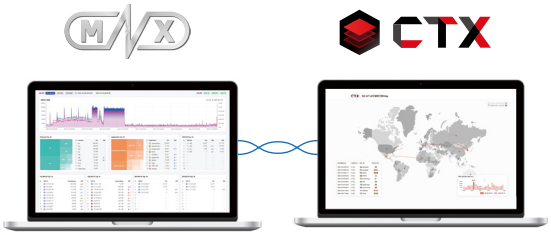
관리



Insight 탭을 통한 위협 관리

- 위협요소 강력 트래킹
- 이슈 상태 상세 관리 (신규-진행중-완료)
- 이슈 연관 정보 및 상세 데이터 확인
- 탐지 내역 자동 알림 (E-Mail, SNS 연동)

연동



CTI 서비스 연동

- CTX(ctx.io)와 연동하여 위협 인텔리전스 확인
- 연관된 공격 그룹, 캠페인 정보 활용
- 기타 CTI 서비스 연동 지원
  EX) VirusTotal 등···

필요성

ENVIRONMENT	AS-IS	TO BE
생성형 AI 등 최신 기술을 활용한 정교한 사이버 공격 증가	최신 유형의 위협을 자체적으로 탐지하기가 어려워요	**AI 탐지 모델** 자체 개발한 AI 모델을 활용해 잘 알려지지 않은 위협까지 심층적으로 탐지
네트워크 내부에서 발생하는 이상행위 탐지의 중요성 증가	네트워크 내부 활동에 대한 가시성이 부족해 잠재적 위협을 조기에 식별하기 어려워요	**자동 대응** 실시간 네트워크 모니터링을 통해 모든 트래픽을 분석하고, 위협 탐지 시 생성된 PlayBook에 따라 자동으로 경고 및 대응 조치가 가능합니다. (EX. SNS, E-Mail, 사내 방화벽 차단 등)
보안 사고 발생 시 신속한 원인 분석과 대응 필요성 증대	전체 트래픽을 저장하지 않아서 로그가 없고, 수많은 로그를 수동으로 분석해야 해서 대응 시간이 지연돼요	**전문 검색 or 네트워크 블랙박스** 전체 네트워크 데이터를 저장하고, 전문 검색 및 회귀분석을 지원하여 위협 발생 시 빠른 원인 분석이 가능합니다.

도입효과

자산 식별 기능과 NDR의 핵심 기능 네트워크 블랙박스를 포함한 MNX는 위협 관리를 위한 인사이트를 스스로 생성해 보안 관리자에게 필요한 우선 순위를 결정합니다. 이렇게 위협을 탐지하고 네트워크 가시성을 극대화하여 다양한 위협 요소로부터 신속하게 대응할 수 있으며 네트워크 자산을 보호할 수 있습니다.

시간 단축 및 비용 절감

핵심 위협 정보 제공으로
업무 시간 단축 및
비용 절감 효과

가시성 확보

네트워크 가시성을
확보해 모든 트래픽
효율적으로 모니터링

탐지율 향상

AI 기반 탐지 모델로
악성코드 및 네트워크
이상징후를 빈틈없이 탐지

효과적인 보안 체계 구축

사용중인 보안 솔루션과
연동하여 보다 효과적인
보안 체계 구축 가능
EX) SIEM, SOAR 등…

SANDS Lab
KOSDAQ
코스닥상장법인
주식회사 샌즈랩 경기도 과천시 과천대로 7나길 25. 12층 샌즈랩
Tel. 02-704-7502 | **E-Mail.** contact@sandslab.io | https://www.sandslab.io

샌즈랩 바로가기