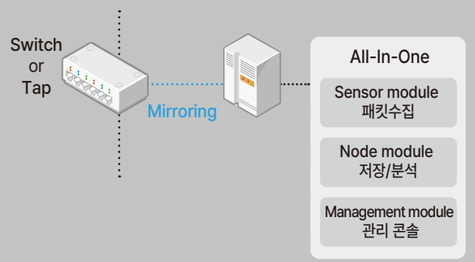
구성 방안 예시

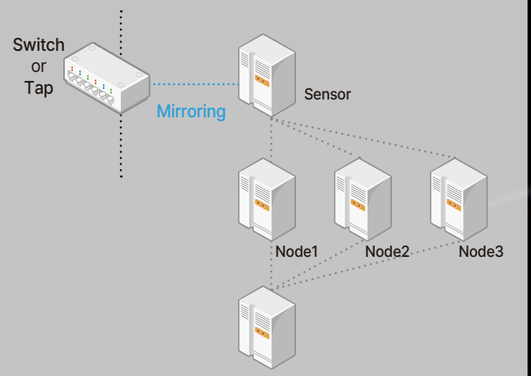
업무시간 평균 트래픽	풀패킷 보관 기간	메타데이터 보관 기간	SW Copy	구 성
250~500 Mbps	약 60일	1년 이상	1 Copy	All-In-One (AIO)
1 ~ 2 Gbps	약 45일	1년 이상	5 Copy	Expand Mode - Sensor 1 EA - Data Node 3 EA - Management 1 EA
5 ~ 7 Gbps	약 30일	1년 이상	7 Copy	Expand Mode - Sensor 1 EA - Data Node 5 EA - Management 1 EA

* 병렬 확장 시 최대 40G 처리 가능합니다.
* 고객사 환경에 따라 저장기간은 달라질 수 있습니다.
* HW 별도입니다.

All-In-One 구성



Expand Mode 구성



제품명		물품식별번호	조달 가격	납품기한
조달청 디지털서비스몰	넷블랙 2.0 NetBlack 2.0	24242615	66,000,000원	30일 (납품요구일로부터)
나라장터 종합쇼핑몰	QSV 5100 넷블랙 전용 H/W All-In-One, DataNode 용	24602874	30,800,000원	30일 (납품요구일로부터)
나라장터 종합쇼핑몰	QSV 5200 넷블랙 전용 H/W Sensor, Management 용	24602875	30,800,000원	30일 (납품요구일로부터)

NETWORK BLACKBOX

Avant-garde Network Detection and Response

SNA

(주)에스엔에이
서울시 성동구 성수일로 55 SK테크노빌딩 308호
https://snainfo.com 문의 : sna_sales@snainfo.com / Tel) 02-511-7060

1등급 GOOD SOFTWARE 조달청 디지털서비스몰 나라장터 종합쇼핑몰 SNA Quad Miners

NETWORK BLACKBOX
Avant-garde Network Detection and Response

NETWORK BLACKBOX – Gartner가 인정한 국내 유일의 NDR 솔루션

모든 네트워크 행위기반 학습을 통하여 사이버보안 위협을 예측하고 방어 할 수 있는 최신 기술을 제공합니다.

네트워크 풀패킷 기반의 차세대 위협 탐지

네트워크 블랙박스는 최대 40Gbps 트래픽을 안정적으로 수집하고 100% 풀패킷 데이터를 활용하여 모든 종류의 사이버보안 위협을 탐지합니다. 55종의 탐지 조건으로 다양한 행위에 대한 룰을 정의한 네트워크 블랙박스는 2만 5000개 이상의 위협탐지 룰을 기반으로 이상 징후를 실시간으로 파악하고 분석합니다. 또한, 다차원 분석 기법을 통해 정오탐을 빠르게 분별하고 위협이 탐지된 정확한 이유와 원인을 제공합니다.

대응할 수 없는 탐지 솔루션은 아무런 의미가 없습니다.

위협 탐지 및 대응의 차세대 해결책, 네트워크 블랙박스는 사건 전후의 전체 흐름을 파악하고 탐지된 위협에 빠르게 대응할 수 있는 확정적 증적 정보를 제공하여 보안 대응 시간을 현격하게 줄여줍니다. 또한 유연한 3rd-Party 연계를 통하여 기존 legacy 솔루션들과 함께 효과적으로 위협을 관리하고 대응할 수 있는 플랫폼 구축을 지원합니다.

Packet Stream

NETWORK BLACKBOX

IP Flow | Application | Metadata | Geo IP | Device | ... **80+** 데이터셋

메일 | 게시판 | SNS | 거래내역 | 번역 | ... **50+** 컨텐츠 파싱

HTML렌더링 | POST 통신 | 모든 종류의 파일 | 거래내역 | ... **100+** 추출 / 재현

Detail Packet Analyzer

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

네트워크 풀패킷 저장 및 복원

- 최대 40Gbps 까지 안정적인 수집
- 국내 특허 3건, 국제특허 1건
- 효율적인 사후 추적 프로세스 구현

네트워크 가시성 확보

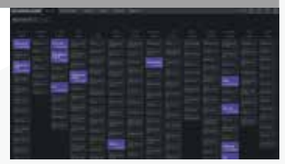
- 어플리케이션 계층(L2-L7)까지 재조합
- 300개 이상의 통신 프로토콜 처리 및 모니터링
- 네트워크에서 벌어지는 모든 행위 가시화

네트워크 트래픽 학습 및 비정상 행위/위협 탐지

- 모니터링 구간에 대한 통신환경 학습
- Non-Rule 기반의 위협 탐지
- 가시성 있는 위협 정보 제공

선제적 위협헌팅

- TTPs 관점의 분석 (MITRE ATT&CK 프레임워크)
- 주요 위협 그룹의 잠재적 위협 활동 헌팅
- 사용자룰 및 시나리오 분석 기능
- 콘텐츠 분석 및 회귀분석(Rebuilding) 기능 제공



확정적 증적 자료 제공

- 풀패킷 기반의 상세 패킷 및 원본 파일 제공
- SMTP/POP3 메일, 웹메일, Post 통신 추출
- 자체 파서를 통한 커스텀 추출룰 제공

유연한 3rd-Party 연계 지원

- RESTful API 제공, SYSLOG, File 연동 지원
- 타 솔루션 연계를 통한 다각적 분석
- SIEM, APT, SOAR, OCR, 인사정보 등

보안 사각 지대 해소

제로트러스트 관점의 전방위 보안강화

내외부에 위협에 대한 명확한 분석

컴플라이언스 위반 및 정보유출 탐지

위협 대응에 시간/비용 절감

효과적인 위협 관리 대응 플랫폼 구축