내부망 위협징후 탐지체계 (ConnecTome NDR)

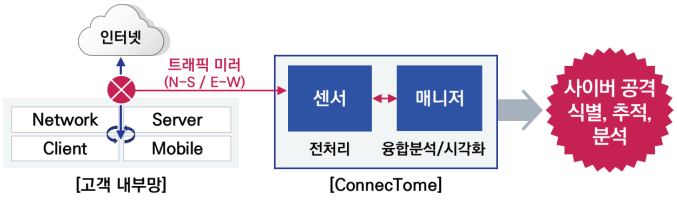
APT 공격 등 고도화·지능화된 방식으로 경계선 방어체계를 우회 침투하여
탐지되지 않은 채 내부망에서 은밀히 활동 중인 위협을 탐지하는 솔루션입니다.

필요성

"사이버 공격을 위해서는 네트워크 통신이 반드시 필요하며
이러한 통신데이터에는 **공격자의 움직임(통신사실)**이 숨어 있습니다."

01	02	03	04
내부망이 해킹된 상태로 침해가 진행되고 있는지 알 수 없다.(침해를 전제로 한 위협 대응 방식 필요)	방화벽, IDS/IPS, 백신, APT 대응체계 등을 우회한 고도화·지능화된 공격행위 (악성 호스트) 식별 필요	내부망 통신데이터 분석을 통해 보안관점의 IT자산 운용 및 위협 상황의 실시간 인식 및 대응 필요	식별된 침해지표 또는 위협 인텔을 기반으로 내부망 위협 탐지 및 침해사고 분석 체계 필요

운용개념

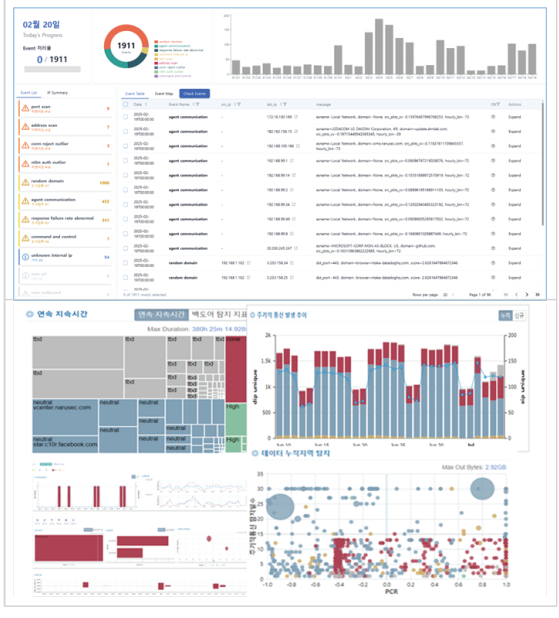


주요기능

1	실시간 **상황 이벤트 발생 및 분석** 기능 제공	• 센서/매니저, 네트워크/자산운용 변화 • IoC 기반 위협 탐지, 통신행위 기반 이상징후 등
2	실시간 **운용상황 및 위협상황 인식** 시각화 제공	• 센서/매니저/네트워크/로그/자산운용 변화, 통신 현황 등 종합적인 운용상황 파악 가능 • 탐지 위협 등 대한 종합적인 위협상황 파악 가능
3	내부망 **위협 추적(헌팅) 및 침해 분석** 기능 제공	
4	내부망 **위협의 인터넷 추적·분석**(N-TIS 연계) 등	

네트워크 트래픽과 활동을 실시간 모니터링하고 분석하여
내부망 위협 징후를 식별하여 대응하세요.

Cyber KillChain 초기침투 단계 이후의 내부망 위협 활동 식별



- 기존 보안체계를 우회 침투하여 내부망에서 은밀히 활동하는 **지능형 지속 위협(APT) 공격 식별**
- 목표 네트워크를 표적으로 특수 목적을 수행하도록 정밀하게 설계된 **맞춤형 표적 공격 식별**
- 조직 내부자의 악용/실수 또는 HW/SW 공급(유지보수) 업체를 통한 **공급망 위협 식별 등**

"네트워크 통신데이터를 신뢰하지 말고 검증하라!"
네트워크 통신데이터에 대한 ZeroTrust 원칙을 적용한 솔루션

특장점

01.

On-Premise 또는 Cloud 환경을 기반으로 위협 및 이상징후 식별에 특화된 **독창적인 통신데이터 수집**

- IP 주소, 포트, 연결 상태, 전송된 바이트 수, 프로토콜 정보 등 네트워크 연결에 대한 정보
- HTTP, DNS, FTP, Kerberos, SMB, SSH, SSL/TLS 등 다양한 프로토콜 트래픽 정보
- 응용계층 프로토콜 헤더값 분석/ 처리 후 저장
- 네트워크를 통해 전송되는 파일에 대한 정보 (파일의 해시값, 파일 이름, MIME 타입 등)
- ARP, ICMP, IP, TCP/UDP 기반의 세션 추적에 필요한 정보
- 네트워크 연결에서 발생하는 IP 주소의 지리적 위치 정보

내부망 통신 및 독창적인 메타데이터 생성

02.

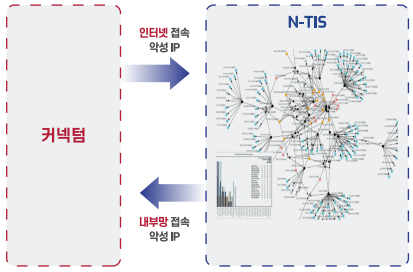
공격자 통신행위 탐지를 위한 통신특성 변화관리 기반의 **지능형 이상징후탐지모델 및 명령제어채널 자동 탐지 엔진(미국특허)을 적용**

총 00개의 위협 탐지 모델 기반 이상 징후 분석

03.

ConnecTome에서 식별한 위협에 대한 N-TIS 기반의 **인터넷 위협 경로 분석** 지원

* **N-TIS** : (주)나루씨큐리티(위협대응센터)에서 추적을 통해 관리하고 있는 위협 인텔리전스를 기반으로 위협분석을 지원하는 서비스

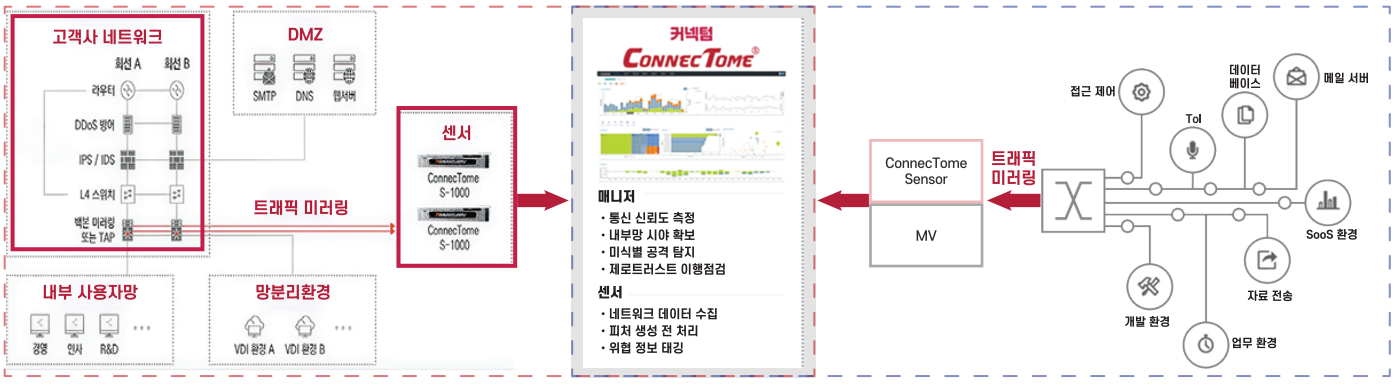


커넥텀과 N-TIS 연계를 통한 위협 분석

ConnecTome 구성 환경

01. On-Premise 환경

02. Cloud 환경



"**ConnecTome(커넥텀)**은 내부망에서 **공격자의 통신행위 탐지모델을 기반**으로 알려지지 않은 위협을 식별하는데 특화된 **NDR 솔루션**입니다."

01.
조직 **내부망에서** 탐지되지 않은 채 **은밀히 활동하는 위협을 탐지**할 수 있습니다.

02.
위협 식별(탐지) 시 **공격 경로 추적 및 피해 자산 식별**이 가능합니다.

03.
조직 내부 네트워크에서 **데이터 유출 징후를 식별**할 수 있습니다.

04.
침해지표를 기반으로 내부 네트워크에 대한 **위협 헌팅(정찰)**이 가능합니다.

05.
네트워크 트래픽 데이터를 기반으로 **위협분석 및 침해사고 조사 분석**이 가능합니다.