1. 사전 정보 요청 개요

1.1 사업명 및 기간

- 사업명 : N-EDR 시스템 구축
- 사업기간 :

1.2 사전 정보 요청 배경 및 목적

- **더욱 정교해지고, 지능화 되는 보안 위협**
    - 매일 새로운 악성코드와 수백 수천의 변종이 생겨남에 따라 보안 위협의 종류가 다양해지고 있어 기존의 보안 시스템으로 방어하는데 한계가 드러나고 있음
    - 또한 보안 위협의 공격 방법이 점점 더 정교해지고 지능화 됨에 따라 위협을 선 차단한다는 전통적인 보안 방법으로는 차단하는 것이 어려움
- **보안 패러다임의 변화**
    - 과거 전통적인 보안 개념이 위협을 차단하는 것이라면, 최근에는 이미 조직 내에 위협이 침투했다는 가정 하에 빠르게 위협을 탐지하고 대응하는 개념으로 패러다임이 전환
    - 조직 내의 엔드포인트는 보안 위협의 시작점이 되며 공격자들이 조직 내부를 파악하기 위해 사용하는 교두보가 됨으로 조직 내 모든 엔트포인트의 가시성을 확보하고, 위협을 탐지하여 대응할 수 있는 시스템이 필요
- 따라서 기존 엔드포인트 보안 시스템(DLP, DRM, APT 및 랜섬웨어 대응 솔루션 등) 의 한계를 극복하고, 엔드포인트에서 수집된 프로세스, 파일 접근 정보, 네트워크 이벤트 등을 통해 엔드포인트 가시성을 확보하고 침해 사고 등의 보안 위협을 탐지하는 EDR(Endpoint Detection & Response) 시스템이 요구됨

1.3 EDR 시장 동향 (가트너)

- 엔드포인트 보안 제품은 사용자에게 제공되는 정보와 경고를 향상시키고 응답 및 치료 기능을 자동화하는 방향으로 통합이 이루어질 것으로 예상됨
- Gartner 의 예측은 적어도 2020 년까지 EDR 의 연간 성장률이 거의 50 %에 이를 것으로 예상

1.4 기대효과

- **엔드포인트 가시성 확보 및 모니터링**
    - 조직 내 모든 엔드포인트에 대해 빠르게 가시성을 확보하고, 엔드포인트에서 발생하는 행위들을 모니터링

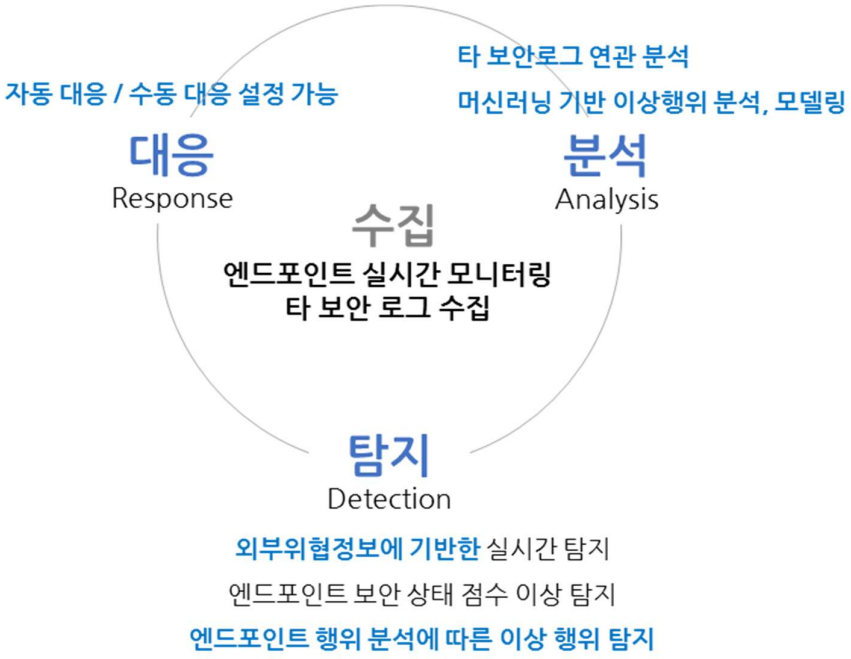
- 개별 엔트포인트들의 최신 상세 정보와 행위를 준-실시간(Near-realtime)으로 검색 및 분석하고, 엔드포인트를 효율적으로 관리
- 시각화 (프로세스간 관계, 파일간 관계 등), 타임라인(개별 엔트포인트의 시간대별 수행 내역)을 통한 위협 분석

- **조직 내 위협 탐지와 대응**
  - 침해지표(IOC) 및 위협 정보(Threat Intelligence)를 통한 알려진 위협 탐지
  - 머신러닝 기술을 활용한 엔드포인트 이상행위 등 알려지지 않은 위협 식별
  - 위협이 탐지된 엔드포인트의 즉각적인 파악과 대응을 위한 보안정책 적용
  - 소수의 보안관리자가 조직 내 다수의 엔트포인트에 대한 네트워크 차단, 파일 삭제, 프로세스 종료 등의 빠른 대응 가능

2. N-EDR 제품의 특징

2.1 보안 사이클

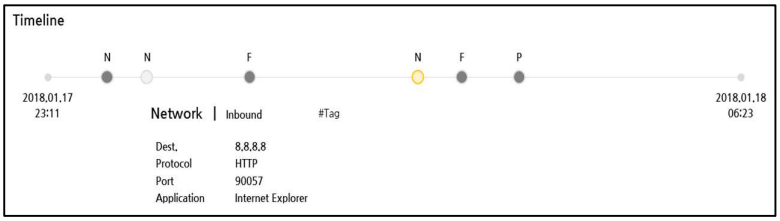
- N-EDR 의 보안사이클
  - **데이터 수집 – 탐지 – 대응 – 분석**의 보안사이클



2.2 쿼리 기반 검색을 통한 빠른 분석 및 대응 기능 제공

- 검색 (쿼리 기반) → 인지 (엔드포인트 위협 정보 파악) → 대응 (프로세스 강제 종료 등)

<쿼리 기반 검색>

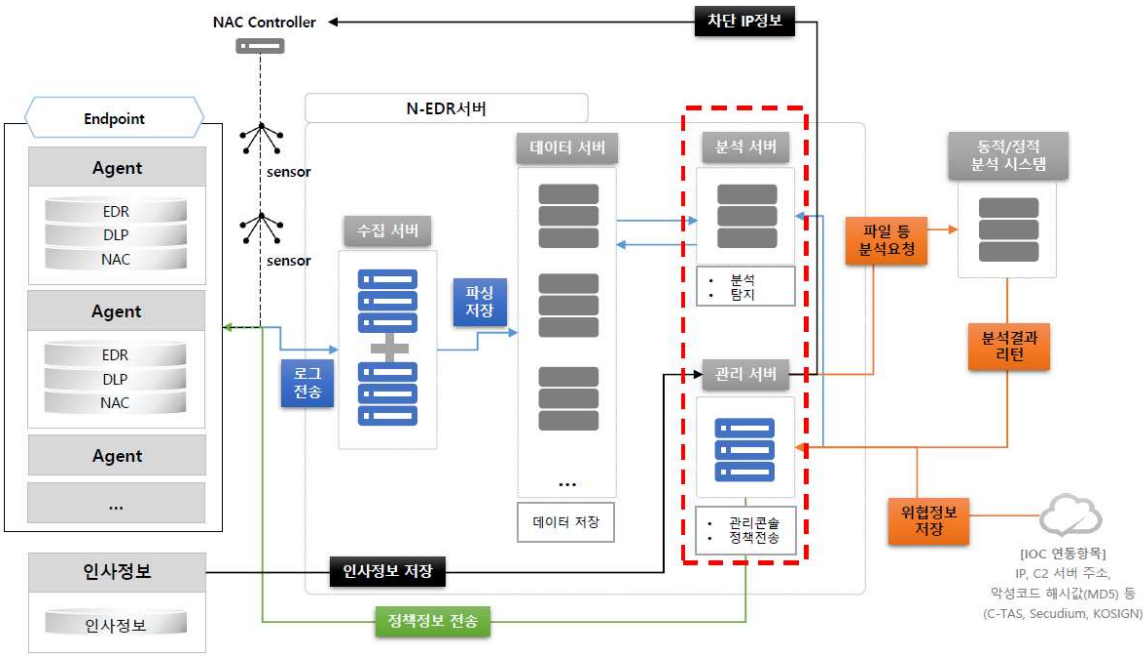


<검색된 결과에 대한 분석>

<대응>

2.3 N-EDR 아키텍처

- N-EDR 은 하나의 에이전트에서 수집, 탐지 및 대응을 수행
- 수집된 정보는 N-EDR 의 빅데이터 저장소에 저장
- 저장된 정보로 머신러닝을 방법론을 통한 알려지지 않은 위협에 대한 탐지를 수행



3. N-EDR 상세 기능

3.1 엔드포인트 데이터 수집

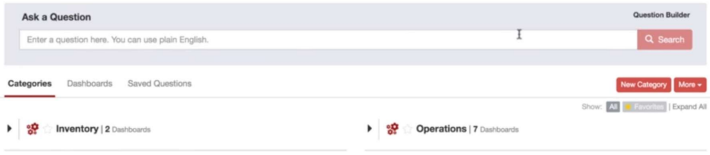
- H/W 자산 정보 수집
  - H/W 고유키, CPU 정보, 메모리 및 스토리지 용량 / 수량 등 하드웨어 기본 정보 수집
  - 네트워크 카드 수량 및 기본 정보, MAC 주소, IP 등 네트워크 정보 수집
  - PC 내 설치된 추가 매체 및 장치 관련 정보 (H/W 종류, 제품명, 버전 등) 수집
- S/W 자산 정보 수집
  - 설치된 OS 명, 버전, 종류 및 컴퓨터 이름 등 기본 운영체제 관련 정보를 수집
  - 추가 설치된 S/W의 명칭, 게시자, 버전, 용량, 설치경로 및 설치일자 정보를 수집
  - 삭제된 S/W의 명칭, 게시자, 버전, 용량, 설치경로 및 삭제일자 정보를 수집
- 사용자 정보 수집
  - OS 사용자 계정명, 사용 권한, 로그인 / 로그아웃 시간, PC-On / OFF 시간 등을 수집
  - Agent 로그인 계정 및 권한, Agent 로그인 / 로그아웃 시간 등을 수집
  - 사용자의 사원번호 및 부서, 직급, 정규직 구분, 퇴직 (예정)일, 퇴직 여부, 적재일 등의 사용자 관련 기본 인사 정보를 수집
- 포렌식 데이터 수집
  - 사용 프로세스 이름, 사용자 및 게시자 명, 이미지 경로 등을 수집
  - 레지스트리 명 및 생성 / 수정 / 삭제 / 차단 요청 등에 대한 레지스트리 관련 정보 수집
  - 네트워크 IP, MAC 주소 및 TCP, UDP 등의 프로토콜, 목적지 관련 네트워크 관련 정보 수집
  - 파일 생성 / 수정 / 삭제 이벤트 관련 이벤트 발생시간, 사용자명, 개인정보 및 대외비 정보 포함 여부, 허용 시작 / 종료일 등의 파일 관련 정보 수집

3.2 탐지

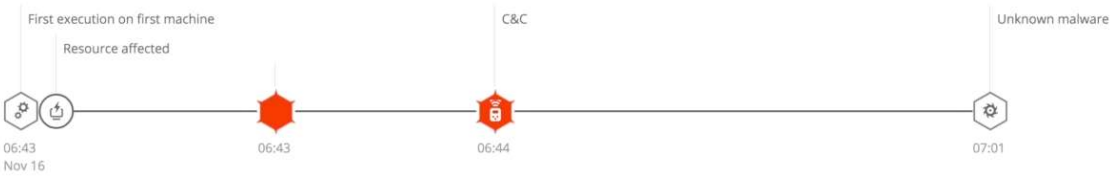
- 보안위협 탐지 기능 제공
  - 외부 위협 정보(IOC 등)에 기반한 실시간 탐지 수행
  - 정적분석과 동적분석(ex, Sandbox 등)을 통한 악성코드 탐지
  - 머신러닝을 통한 사용자 이상행위 탐지

3.3 대응

- 보안 위협 대응 기능 제공
  - 조사 및 분석을 위한 통합 검색
  - 사용자, 엔드포인트, 네트워크, 프로세스, 파일 등의 상태에 대한 탁월한 가시성 확보
  - 탐지된 위협에 대한 자동 대응 설정 지원 : 보안/통제 정책 등
  - 비정상 행위 탐지 시 사용자에게 6하 원칙 기반의 소명처리 프로세스를 제공
- 위협 탐지 및 조사를 위한 인터페이스 제공



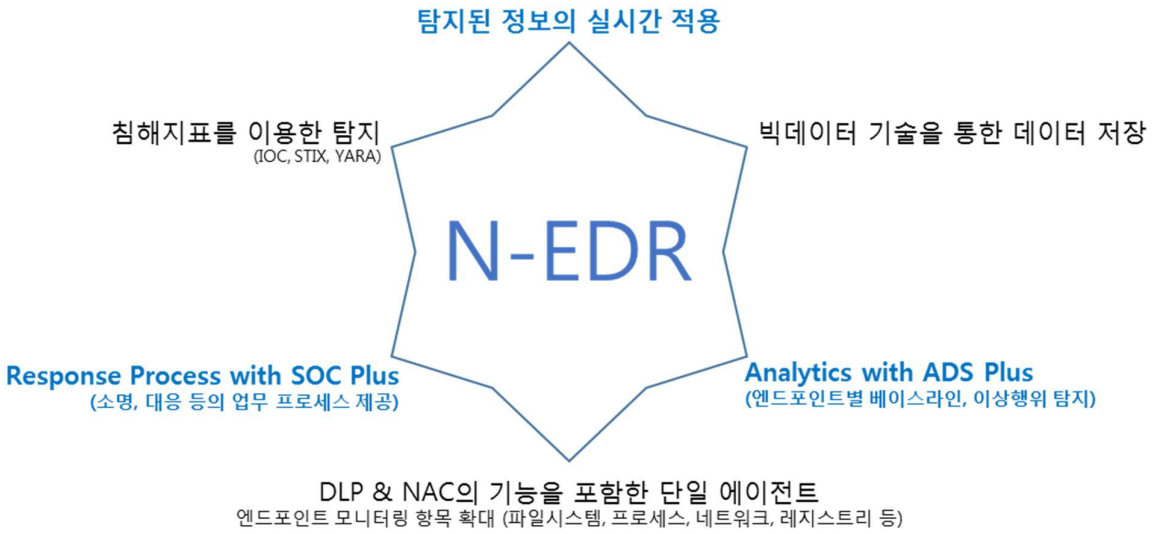
- 탐지된 위협에 대한 타임라인, 사이버 킬 체인 등의 단계에 따라서 모든 엔드포인트 조사



- 탐지된 위협에 대한 자동/수동 대응 설정
  - 위협이 탐지 후 대응 정책에 따라 매체 차단, 프로세스 종료/삭제, 어플리케이션 차단, 네트워크 격리/차단, 파일 삭제/암호화, 시스템 종료 등의 기능을 제공

4. N-EDR 제품의 차별화 포인트

4.1 닉스테크 N-EDR 의 6 가지 차별화 포인트



4.2 통합 에이전트

- EDR, DLP, NAC 기능을 통합하는 하나의 에이전트 제공을 통해 사용 편의성 증대
- 다수의 보안 에이전트가 통합됨으로 엔드포인트에서 사용하는 리소스 최소화 및 효율 극대화
- 관리 포인트 감소로 운영 효율성 증대

4.3 머신러닝 기술

- 다수의 대형 고객사에 머신러닝 기반 이상행위탐지 솔루션 공급 및 구축 경험
- 축적된 머신러닝 기술을 기반으로 엔드포인트 이상행위 탐지 모델의 정확성 및 효율성 제공
- 악성행위도 이상행위의 한 분류로써 이상행위 기반 머신러닝 알고리즘으로 탐지 가능

4.4 엔드포인트 관리 및 제어 기술

- 20 년 넘게 엔드포인트 보안 기술을 개발하면서 축적된 기술 노하우
- 네트워크접근통제(NAC) 솔루션을 통해 엔드포인트 정보 수집, 무결성 검증, 단말 인증 현황 등 엔드포인트 가시성에 대한 기술력을 확보
- 자료유출방지(DLP) 솔루션을 통해 엔드포인트 통제 및 제어 기술력 확보

5. 닉스테크 소개

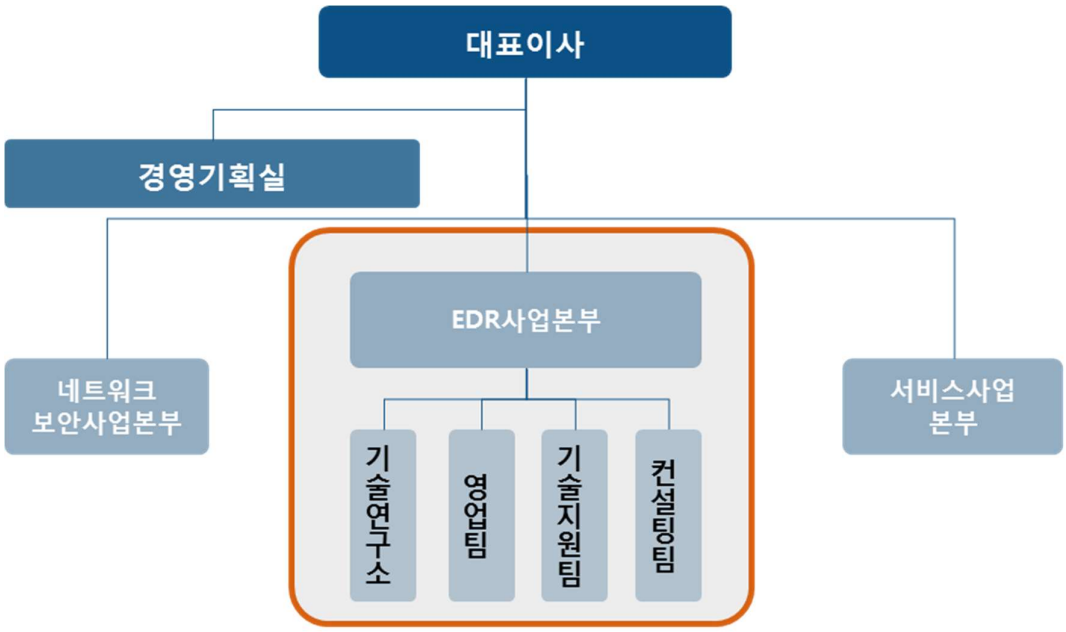
5.1 일반현황

닉스테크㈜는 1995 년에 설립되어 엔터프라이즈 보안 전문 기업으로써 Endpoint 및 네트워크 보안 솔루션을 개발 및 판매하고 있습니다. 본 사업에는 EDR 솔루션인 N-EDR 을 제안합니다.

회 사 명	닉스테크㈜	대표자	박동훈
주 소	서울특별시 성동구 왕십리로 58, 10 층 (성수동 1 가, 포휴)		
전 화 번 호	Tel : 02-3497-8900		
사 업 분 야	Endpoint 보안 소프트웨어 개발		
회사설립년도	1995 년 10 월		
해 당 부 분 사 업 기 간	1995 년 10 월 ~ 현재 (22 년 1 개월)		
보유인력현황 (총원 114 명)	개 발 인 력 : 32 명 기술지원인력 : 37 명		

5.2 조직 및 인원현황

닉스테크㈜는 보안 전문 기업으로서 보안 시장에 역동적으로 진출하여 완벽한 프로젝트 수행사례를 만들어가고 있습니다. 이러한 전문기술 및 구축 노하우를 기반으로 본 사업을 성공적으로 수행하도록 하겠습니다.



부서	인원	수행업무
기술연구소	41명	• 제품 기획 및 머신러닝 방법론 개발 • N-EDR 시스템 개발 • 솔루션 품질관리 • 프로젝트 품질관리
영업팀	4명	• 제품 영업
기술지원팀	16명	• 제품 구축 및 유지보수 수행
컨설팅팀	2명	• 제품 Pre-Sales