Nicstech N-EDR (Endpoint Detection & Response) 소개서

Endpoint Detection & Response

Smart Security & Service
닉스테크

Nicstech N-EDR

Nicstech N-EDR　　구성도　　기능　　조사분석-화면예시

Why Nicstech N-EDR?

Endpoint DR

1 엔드포인트란? 데스크탑, 노트북, 모바일 기기 등을 모두 포함하는 개념

2 **엔드포인트에서의 수집 및 탐지**

- 보호 : 기밀성, 무결성, 검증
- 수집 : 엔드포인트 식별, HW정보, S/W정보, 사용자 정보, 프로세스/파일/레지스트리/네트워크
- 탐지 : IOC 탐지, 악성코드 탐지(타시스템 연동), 사용자 이상행위 탐지

3 **원 에이전트**

Why Nicstech N-EDR?

E D_{etection} R

1 위협이란?

- 데이터 유출
- 데이터 유실 (랜섬웨어 등)
- 데이터 변경
- 감염 (Lateral Movement)
- 권한 상승
- C&C or 원격제어 등

2 알려진 위협과 알려지지 않은 위협 탐지 Known & Unknown Threat

- **악성코드 탐지 (타 솔루션/서비스 연계)**
- **룰 기반 탐지**
- **인공 지능 탐지**

Why Nicstech N-EDR?

E D R esponse

1 탐지된 위협에 대한 조사 및 대응

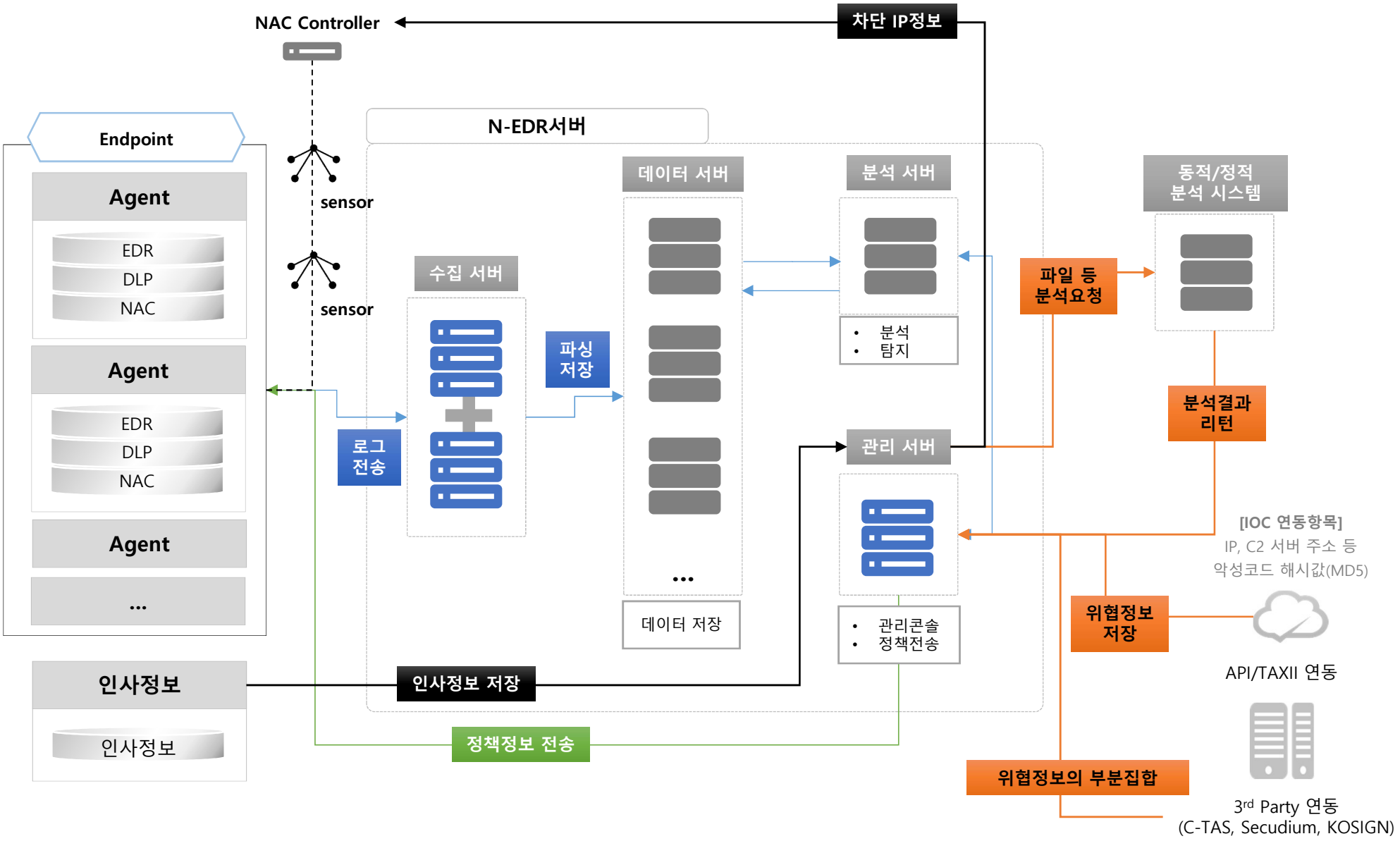
2 조사 및 분석

- 조사 및 분석을 위한 통합 검색
- 사용자, 엔드포인트, 네트워크, 프로세스, 파일 등의 상태에 대한 탁월한 가시성 확보
- 보안 분야 외 자산 전체 현황에 대한 분석 기능 (DLP 기능 최대한 활용)

3 대응

- 탐지된 위협에 대한 자동 대응 설정 지원 : 보안/통제 정책 등
- 비정상 행위 탐지 시 사용자에게 6하 원칙 기반의 소명처리 프로세스를 제공
- DLP, NAC 이용한 네트워크, 호스트 차단

N-EDR 시스템 구성도


NAC Controller
차단 IP정보
N-EDR서버
Endpoint
Agent
EDR
DLP
NAC
Agent
EDR
DLP
NAC
Agent
...
인사정보
인사정보
sensor
sensor
수집 서버
로그 전송
파싱 저장
데이터 서버
데이터 저장
분석 서버
• 분석
• 탐지
관리 서버
• 관리콘솔
• 정책전송
인사정보 저장
정책정보 전송
파일 등 분석요청
동적/정적 분석 시스템
분석결과 리턴
[IOC 연동항목]
IP, C2 서버 주소 등
악성코드 해시값(MD5)
위협정보 저장
API/TAXII 연동
위협정보의 부분집합
3rd Party 연동
(C-TAS, Secudium, KOSIGN)

N-EDR 기능

에이전트

수집

HW 자산 정보
SW 자산 정보
사용자 정보
프로세스
레지스트리
네트워크
파일
정적/동적 정보
인사정보

탐지

IOC

대응

매체제어
프로세스 차단 외
어플리케이션 차단 외
레지스트리 삭제 외
네트워크 격리 외
파일 삭제 외
소명처리: 수동 (SOC Plus 연계)

서버

모니터링

대시보드
조직별/사용자별 이벤트 발생현황

탐지

IOC 탐지
AI 탐지
시나리오탐지

검색 : 통합검색 페이지

조직/사용자/어플/프로세스/파일

조사

이벤트
조직목록
사용자목록
엔드포인트목록
프로세스목록
파일목록
자산현황
감사로그

대응

정책설정
조직/사용자/프로세스/파일/IOC별
IOC 목록
태깅목록
업무처리 SOC 연결
보고서

외부 연동 시스템

정적/동적분석(악성)

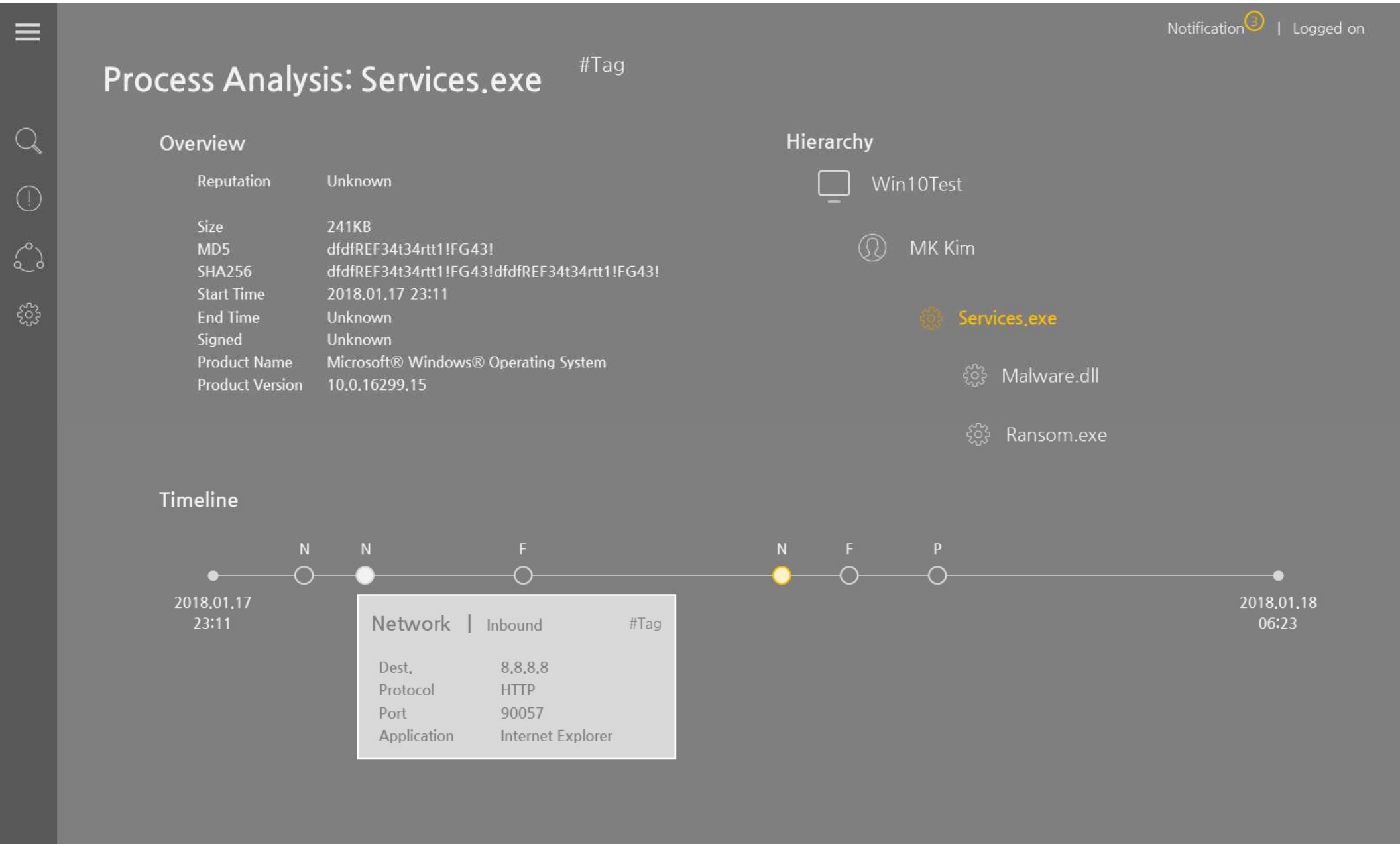
엔피코어, VirusTotal, MAA 등

IOC 정보 수집

시큐디움, C-TAS 외

백신 연계

조사 분석 - 화면예시


Notification 3 | Logged on
Process Analysis: Services.exe
#Tag
Overview
Reputation Unknown
Size 241KB
MD5 dfdfREF34t34rtt1!FG43!
SHA256 dfdfREF34t34rtt1!FG43!dfdfREF34t34rtt1!FG43!
Start Time 2018.01.17 23:11
End Time Unknown
Signed Unknown
Product Name Microsoft® Windows® Operating System
Product Version 10.0.16299.15
Hierarchy
Win10Test
MK Kim
Services.exe
Malware.dll
Ransom.exe
Timeline
N N F N F P
2018.01.17 23:11
2018.01.18 06:23
Network | Inbound #Tag
Dest. 8.8.8.8
Protocol HTTP
Port 90057
Application Internet Explorer

감사합니다.