실시간 위협 헌팅의 비밀과 거짓말

부제: 실시간 위협 헌팅의 중요성 및 방안

2024.03.21

발표자 : 전 덕 조

(주)씨큐비스타

(주) 에이스네트피아

위협 헌팅의 필요성

Why threat Hunting is important

교묘한 위협은 자동화된 사이버보안을 우회할 수 있기 때문에 위협 헌팅이 매우 중요!

자동화된 보안 도구와 1, 2단계 보안 운영 센터(SOC) 분석가들이 대략 80%의 위협을 처리할 수 있지만, 여전히 나머지 20%의 위협을 처리할 수 없음 .

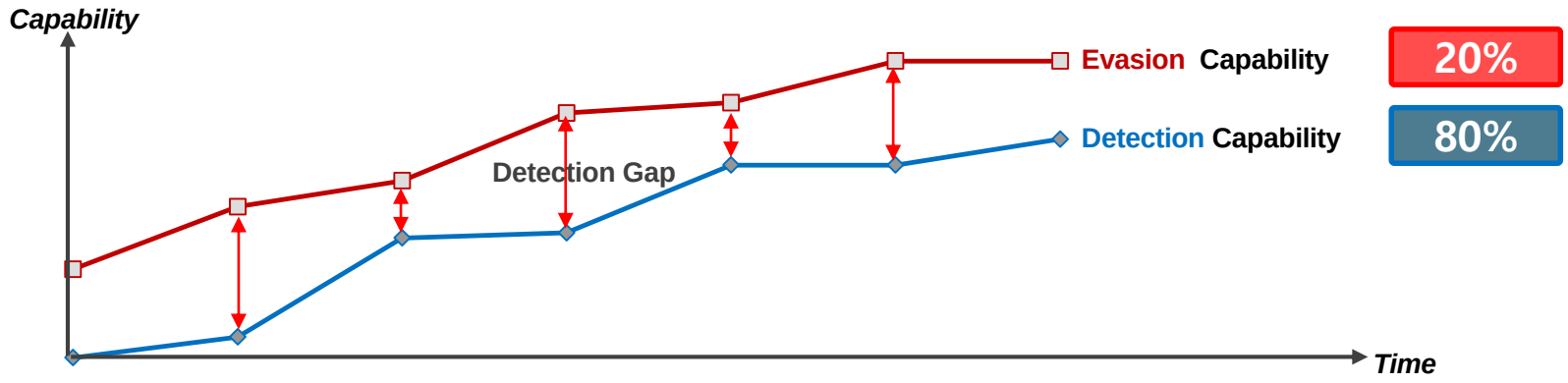
나머지 20%의 위협은 상당한 피해를 줄 수 있는 교묘한 위협이 포함되어 있을 가능성이 높음.

충분한 시간과 자원이 주어지면, 이러한 교묘한 위협은 어떤 네트워크라도 침입하여 평균적으로 280일 동안 탐지를 회피할 수 있음.

효과적인 위협 헌팅은 침입에서 발견까지의 시간 갭(Gap)을 줄여 공격자에 의한 피해 규모를 줄이는 데 도움이 됨.

공격자들은 흔히 발견되기 전에 수 주일에서 심지어 수개월 동안 잠복함.

그들은 데이터를 수집하고 기밀 정보나 자격증명을 찾아내서 추가 접근을 가능하도록 설정하는데, 이는 중대한 데이터 유출로 이어질 수 있음.



공격 발생시, 기존 보안이 놓친 위협의 정확한 탐지와 탐지 속도가 핵심입니다!
➔ 신속한 위협 헌팅 == 피해 최소화

무엇을 헌팅하여야 하는가?

국가 지원 해커를 포함한 모든 지능형 공격에 대한 위협 헌팅!!!

National Security Agency

	NSA TAO 지능형 공격 방법	NSA 지능형 위협 대응 권고사항
1	**초기 정찰 (Initial Reconnaissance)** • 스캐닝 : 운영 체제 식별, 취약점 조사	초기 정찰 (Initial Reconnaissance) • 스캐닝 탐지 / 중요 자산 접속 감시 / 내부 네트워크 통신 모니터링
2	**초기 침입 (Initial Exploitation)** • 악성코드 첨부 이메일 발송 / 감염 웹사이트 접속 유도 • 감염된 이동식 매체 발송	초기 침입 (Initial Exploitation) • 악성코드 탐지 : 파일 평판
3	지속성 확보(Establish Persistence) • 추가 백도어 설치 • 은닉	지속성 확보(Establish Persistence) • 사용자 행위 감시 / 악성 사이트 탐지 : 도메인 평판 / 내부 네트워크 통신 모니터링
4	공격 도구 설치 (Install Tools) • 추가 공격 도구 다운로드	공격 도구 설치 (Install Tools) • 악성코드 탐지 : 파일 평판
5	내부망 이동 (Move Laterally) • 중요 시스템 또는 중요 데이터베이스로 이동	내부망 이동 (Move Laterally) • 내부 네트워크 통신 모니터링 • 계정 접속 감시
6	수집 / 유출 (Collect, Exfil, Exploit) • 중요 데이터 유출 • 데이터 손상, 조작 및 파괴	수집 / 유출 (Collect, Exfil, Exploit) • 실시간 네트워크 모니터링 • 해커가 노리는 대상 파악

통신 이상 탐지

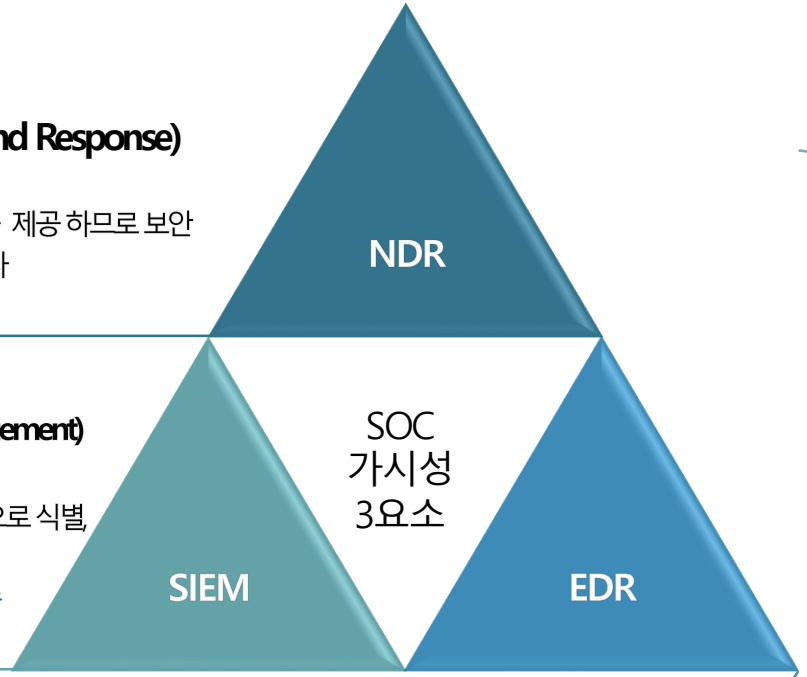
악성코드 탐지

보안 관제 (80%)에서 놓친 위협을 찾아내기 위해서는 보다 풍부한 데이터 분석을 통해 20% (악성코드 및 네트워크 공격 행위)를 신속하게 찾아내서 대응함으로써 피해를 최소화 해야 함!!!

어떤 도구로 위협을 헌팅 할 것인가?

SOC Visibility Triad

Gartner



모든 통신, (cf. 파일)

NDR (Network Detection and Response)

- NDR은 네트워크에 대한 가시성을 제공 하므로 보안 스택에서 가장 중요한 기술 중 하나
- SIEM/EDR 보완

탐지 로그, 대용량, 오탐 포함

SIEM (Security Information & Event Management)

- SIEM은 조직의 사이버 보안 이벤트를 실시간으로 식별, 모니터링, 기록 및 분석
- **미탐** 및 오탐으로 인한 업무 생산성 저하 이슈

단말 파일, 프로세스 뷰

EDR (Endpoint Detection and Response)

- EDR은 단말 내부의 악의적인 활동을 탐지 하는데 중점을 둔 행동 지향적인 보안기술
- 단말의 파일 및 프로세스 뷰 (* 전체 적 뷰 X)
- 서버, IoT 장치 및 임베디드 장치 등에 에이전트 배포 불가 (관리되지 않는 장치 증가 ➔ 보안 홀)

보이지 않는 것으로부터
자산을 보호 할 수 없기 때문에
가시성에 집중

보안 전문가는
네트워크 기반 기술을 통해
위협에 대한 빠른 가시성 획득

출처 : Applying Network-Centric Approaches for Threat Detection and Response (2019)

보안관제 고도화 : SOC Visibility Triad 구현

Gartner

보안 관제의 패러다임 변화: 로그 모니터링에서 탐지&대응 위주의 보안 관제로

10년 전에는 가능했었지만...

SIEM

SIEM이 **높은 이벤트 볼륨, 특정 유형의 데이터, 그리고 다양한 다른 문제 (오탐, 미탐 등)를 처리할 수 없음.**

보안 팀은 SIEM **유즈 케이스를 구축하거나 이를 유지하는 데 어려움**을 겪음.

복잡한 SIEM 유즈 케이스를 선택, 구축 및 유지 관리하는 데 필요한 기술 및 인적 자원은 엄청남.

➔ 오늘날의 기업은 BYOD, SaaS, IoT, 그리고 클라우드 데이터 센터와 같은 **혼합 환경으로 훨씬 더 복잡해 짐.**

EDR 우선으로 변화

EDR 우선 적용

SIEM의 효율적인 운영에 대해 고민하던 사람들이 **EDR 우선 접근 방식으로 옮겨 감.**

그러나 EDR은 기업의 모든 장치나 워크로드를 커버할 수 없으며 그 설치 위치 상, **단말 내부의 파일과 프로세스**의 로컬 뷰 만을 제공

NDR 추가로 변화

NDR !!!

SIEM/EDR 보완 대책의 필요성 (NDR 대두!) ➔ 오늘날 NDR의 빠른 채택을 주도

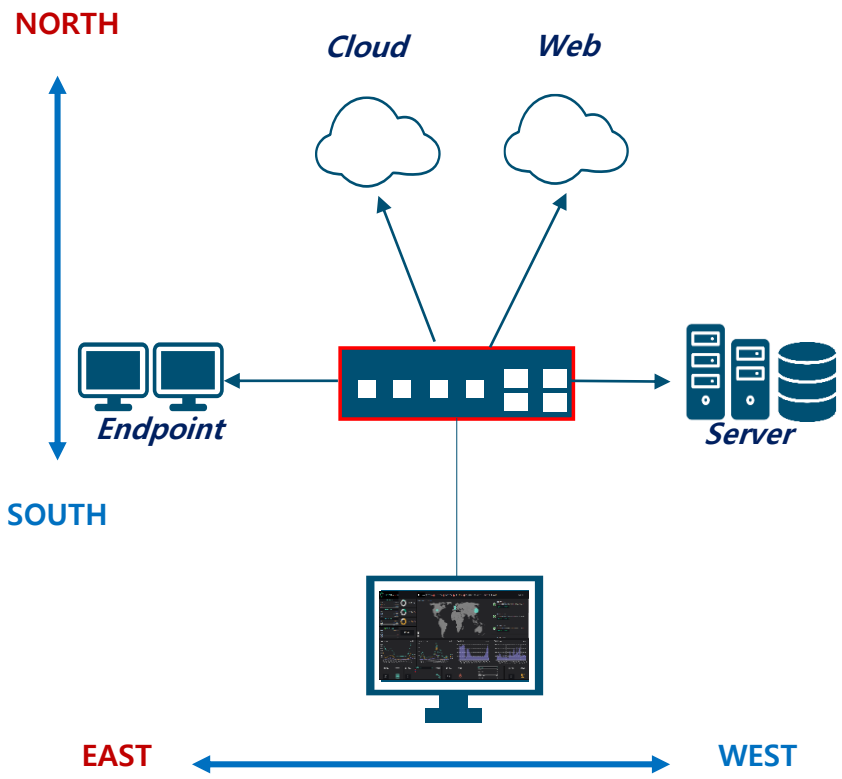
NDR은 클라우드 및 데이터 센터 워크플로우부터 사용자 및 IoT 장치에 이르기까지 **네트워크 내부의 완전한 가시성을 제공**

➔ **보안 운영에 대한 수많은 가치를 제공하며, EDR 및 SIEM 워크플로우에 명확성을 제공함**

탐지와 대응(Detection& Response) 중심 보안 전략 (가트너 권고 사항)

출처: Gartner Security & Risk Management Summit Presentation, Outlook of Security Operations, Gorka Sadowski, Toby Bussa, 17-20 June 2019.

NDR (Network Detection and Response)



NDR 정의

모든 네트워크 트래픽을 수집하여, 기업 네트워크를 지속적으로 모니터링함으로써 누락없는 가시성을 제공하고, **고급 행동 분석, 머신 러닝 등을 사용하여 지능형 위협과 비정상적인 행동을 탐지하여 대응**할 수 있도록 함.
(※ 비시그니처 방식)

NDR 기능

NDR 솔루션은 **명령 및 제어(C&C), 측면 이동(Lateral Movement), 유출(Exfiltration), 악성코드 활동 징후를 나타내는 트래픽 이상을 식별함.**
사이버 공격을 정확히 식별하기 위해, **내부 호스트와 인터넷 사이의 North-South 트래픽** 뿐만 아니라
내부 서버를 포함한 내부 호스트 사이의 East-West트래픽을 검사함.

NDR 효과

NDR이 SIEM/SOAR, 엔드포인트 탐지 및 대응(EDR)과 같은 다른 보안 솔루션과 통합될 때,
네트워크의 사각지대를 해소하고 더 견고한 사이버보안 전략을 개발할 수 있음.
NDR 솔루션은 엔드포인트에 한정된 EDR 도구보다 더 포괄적인 데이터를 제공함.
또한, 공격자에 의해 조작될 수 있고 상세하지 않은 로그 데이터에 의존하는 **SIEM 보다 더 상세한 모든 네트워크 통신 데이터를 제공함**

NDR을 사용하여 탐지 가능한 위협

원하는 정보에 접근하기 위해서는 피할 수 없는 유일한 통로, 네트워크

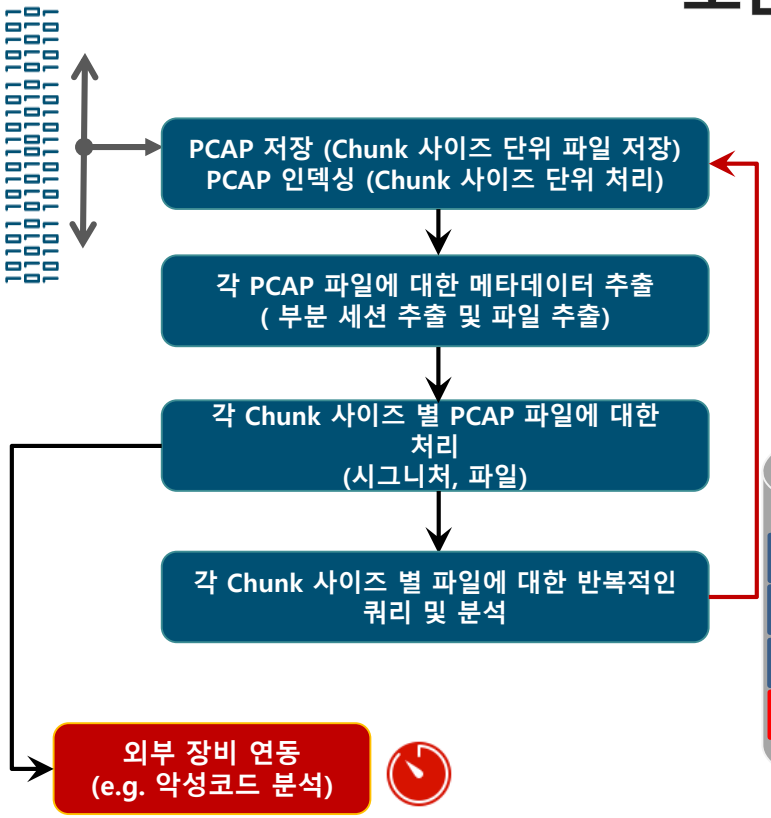
- ✓ **외부 공격 시도:** 네트워크 경계를 통해 시도되는 침입 시도, 스캐닝 활동 또는 다른 형태의 공격 탐지.
- ✓ **C&C(C2) 트래픽:** 공격자가 네트워크 내부의 악성 소프트웨어와 통신하기 위해 사용하는 명령 및 제어 서버와의 네트워크 트래픽 탐지.
- ✓ **피싱 및 스피어 피싱 시도:** 악의적인 이메일을 통해 사용자의 자격 증명을 탈취하려는 시도 탐지.
- ✓ **익스플로잇 활동:** 취약점을 이용하여 시스템을 침투하거나 데이터를 탈취하는 활동 탐지.

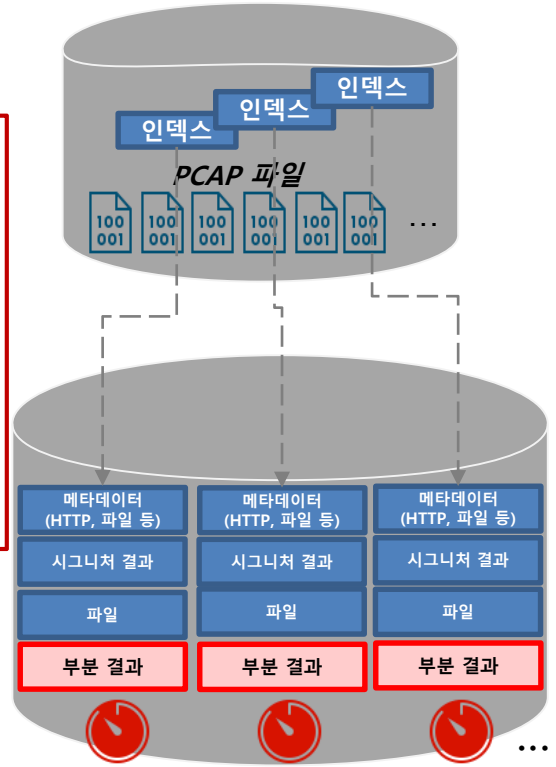
- ✓ **수평 이동:** 공격자가 네트워크 내에서 다른 시스템이나 데이터에 접근하기 위해 이미 침투한 시스템에서 다른 시스템으로 이동하는 행위.
- ✓ **내부자 위협:** 조직 내부의 사용자가 악의적인 목적으로 또는 실수로 조직의 데이터나 시스템에 해를 끼치는 경우.
- ✓ **데이터 유출:** 민감한 정보가 조직의 내부 네트워크에서 무단으로 외부로 전송되는 경우.
- ✓ **악성 소프트웨어 확산:** 네트워크 내부에서 악성 소프트웨어가 확산되어 다른 시스템을 감염시키는 경우.
- ✓ **비정상적인 네트워크 행동:** 사용자의 정상적이지 않은 네트워크 사용 패턴이나 시스템 활동을 포함.

출처 paloalto What Is Network Detection and Response (NDR)?

모든 패킷 수집 및 저장, 분석 방식

National Security Agency





Full Packet 수집 기반 NDR 기술 특징

- 모든 비트, 바이트, 헤더 값을 사용하여 문제가 발생했을 때 실제로 무슨 일이 일어났는지 전체적으로 파악
- 패킷 분석을 위해서는 시간 및 전문 경험, 인내심이 필요

실시간 위협 헌팅 제약 요소

- 시그니처 및 TI 정보 의존적 탐지

Ex) 패킷 데이터가 대량 발생: 저장 비용 : 5Gbps 5분 ➔ 200GB PCAP

➔ 지난 몇 시간 또는 몇일 데이터를 확인하기 위한 충분한 데이터를 저장하기 어려움.

- **실시간 탐지는 불가능하며, 상당한 분석 시간 요소**
- **시그니처 및 TI 의존적인 탐지는 NDR 특징이 아님 (Gartner)**
- 악성코드 탐지: 제3 자 솔루션 필요
- **운영을 위해서는 전문기술, 전문 경험, 인내심이 필요**

Gartner

NDR 요건	✓네트워크 이상 행위를 탐지하기 위해 ML 또는 고급 분석 기술 (※비 시그니처)
NDR 장비 제외 요건	✓ 주로 전체 패킷 캡처 (PCAP) 데이터의 저장 및 분석을 통해 탐지 기능보다 네트워크 포렌식을 강조하는 경우

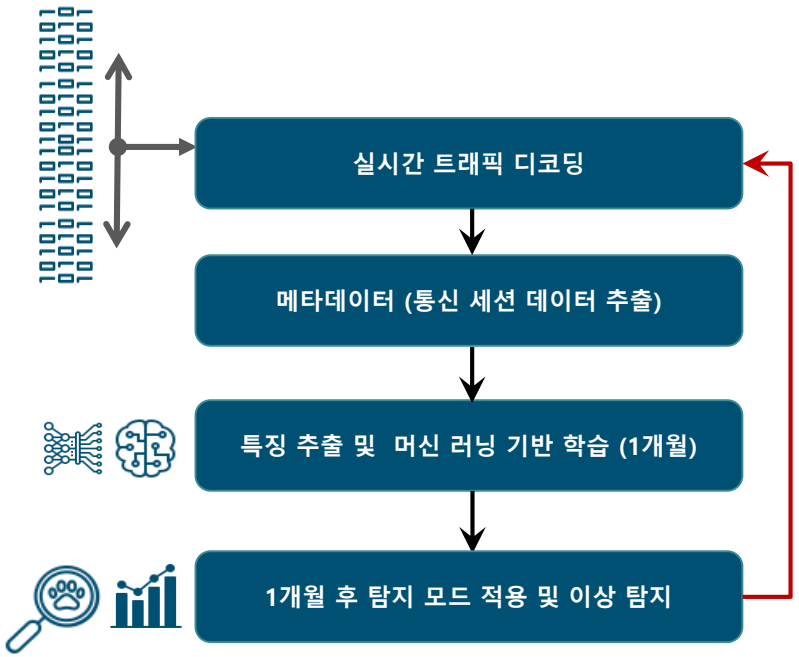
통신 이상 탐지 (X)

악성코드 탐지 (*일부)

출처 : NDR Market Guide (December 2022)

머신 러닝 기반 이상 탐지 방식 NDR

National Security Agency



AI 기반 NDR 기술 특징

- 1개월 학습 이후 정상과 다른 이상 통신 세션을 탐지할 수 있음

실시간 위협 헌팅 제약 요소

- **약 1개월의 학습 기간 필요**
- **"정상과 다른 것"이 항상 악성은 아님.**
- **➔ 탐지 결과 해석이 어려우며 해석 할 수 없는 경우가 대부분**
- **학습 기간(1개월 소요)로 이미 유입되어 있는 위협 탐지 불가**
- **운영을 위해서는 전문기술, 전문 경험, 인내심이 필요**
- **악성코드 탐지 기능 없음**

NDR 이상행위 탐지 요건

✓ 네트워크 이상 행위를 탐지하기 위해 ML 또는 고급 분석 기술 (※ 비 시그니처 기반)

통신 이상 탐지

악성코드 탐지 (X)

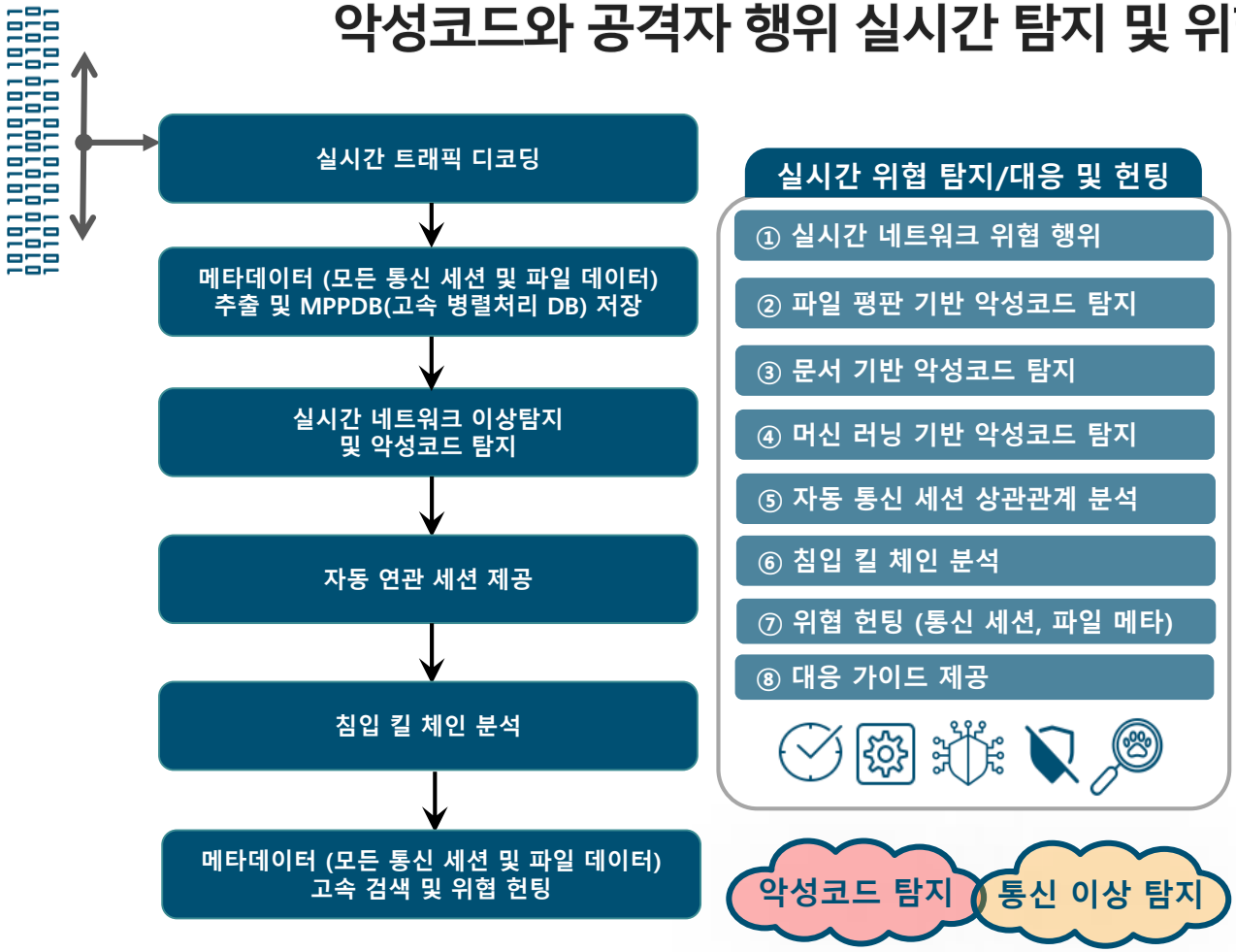
Gartner

출처 : NDR Market Guide (December 2022)

실시간(신속한) 위협 탐지 및 헌팅을 위해서는?

National Security Agency

악성코드와 공격자 행위 실시간 탐지 및 위협 헌팅 지원



실시간 NDR 기술 특징

- 실시간 프로토콜 디코딩 및 패이로드 추적을 통한 통신 및 파일 메타데이터 추출
- 실시간 세션 Counting 및 Frequency 기반 공격행위 탐지
- 추출된 파일 기반 FDR 기반 고속 악성코드 탐지

실시간 위협 헌팅

- "실시간" 악성코드 탐지 / 위협 특정
- "실시간" 네트워크 이상행위 탐지 / 위협 특정
- 탐지된 위협과 관련된 통신 세션 상관관계 분석
- 공격자 추적 및 위협 헌팅
- 탐지된 위협에 대한 대응 가이드 제공

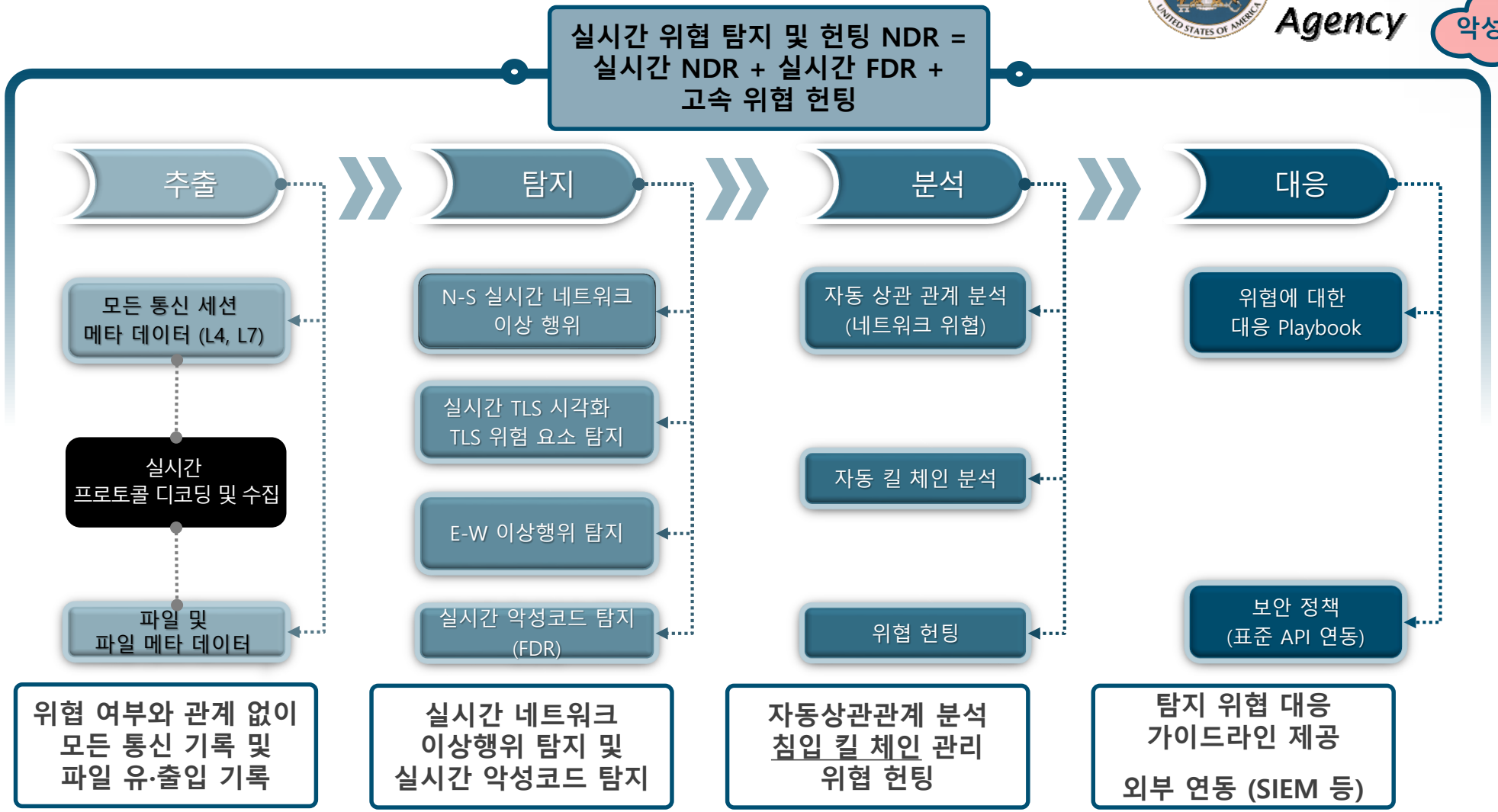
- 이미 유입(감염)된 위협 환경 즉각 적용 가능
- 이동 설치가 용이하며 즉각적인 위협 탐지 및 헌팅
- 사람의 개입 최소화 운영 (SIEM/SOAR 연동 등)

20% 위협의 효과적인 헌팅: 실시간 위협 탐지 및 헌팅 아키텍처

National Security Agency

통신 이상 탐지

악성코드 탐지



실시간 위협 탐지 및 헌팅 NDR: 공격 행위 탐지

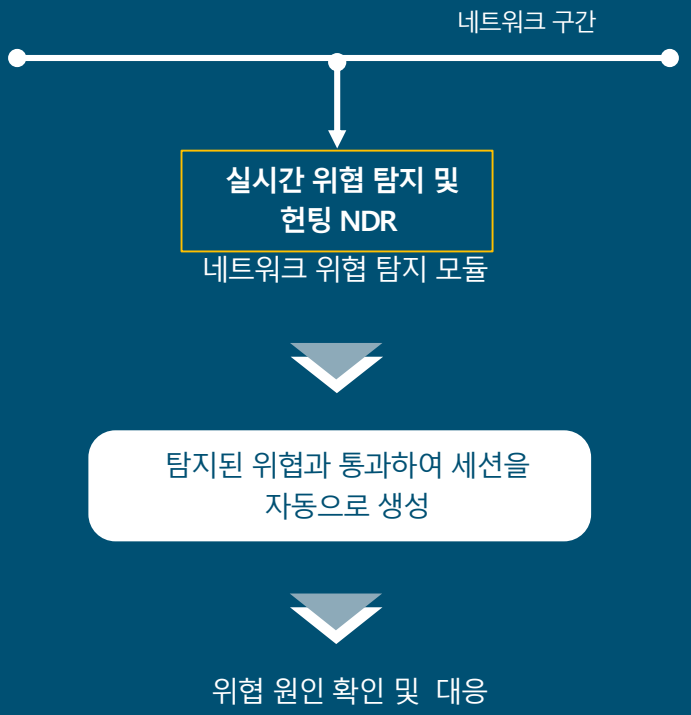
네트워크 위협 특정

FDR (File Detection and Response)

Open NDR

경계 보안을 통과하여
네트워크 내부 에서 일어나는 위협들

- 포트 스캐닝
- 어드레스 스캐닝
- 웹 기반 악성코드 전송
- 이메일 기반 악성코드 전송
- Drive-by-download 행위
- SSH 패스워드 무차별 대입 공격
- FTP 패스워드 무차별 대입 공격
- RDP 패스워드 무차별 대입 공격
- 네트워크 침입 (익스플로잇)
- 어플리케이션 익스플로잇
- 의심스러운 외부 향 통신
- 위장 채널
- C&C 탐지
- C&C 회피 기술 (DGA / Fast-Flux)
- 데이터 유출 (Large Upload) 의심 행위
- SSL/TLS 핑거프린트 기반 악성코드



실시간 위협 탐지 및 헌팅 NDR은 네트워크 내부에서 일어나는 위협을
특정함으로 인해 별도의 분석 전문가 없이도 직관적인 대응이 가능 합니다.

실시간 위협 탐지 및 헌팅 NDR: 악성코드 탐지

네트워크 내부 위협을 특정

FDR (File Detection and Response)

Open NDR

네트워크 구간

네트워크 통해 이동하는
파일을 추출

실시간 위협 탐지 및 헌팅 NDR

데이터 유출에 대한 실시간 탐지 ,
파일에 대한 악성 여부 확인

- 머신러닝(ML)
- **평판 (30여종)**
- YARA Rule
- 문서 스크립트 탐지 모듈

※ FDR은 현재 미 국방부 공유 글로벌 네트워크인 JIE(Joint Information Environment)에서 사용 중인 보안솔루션 입니다.

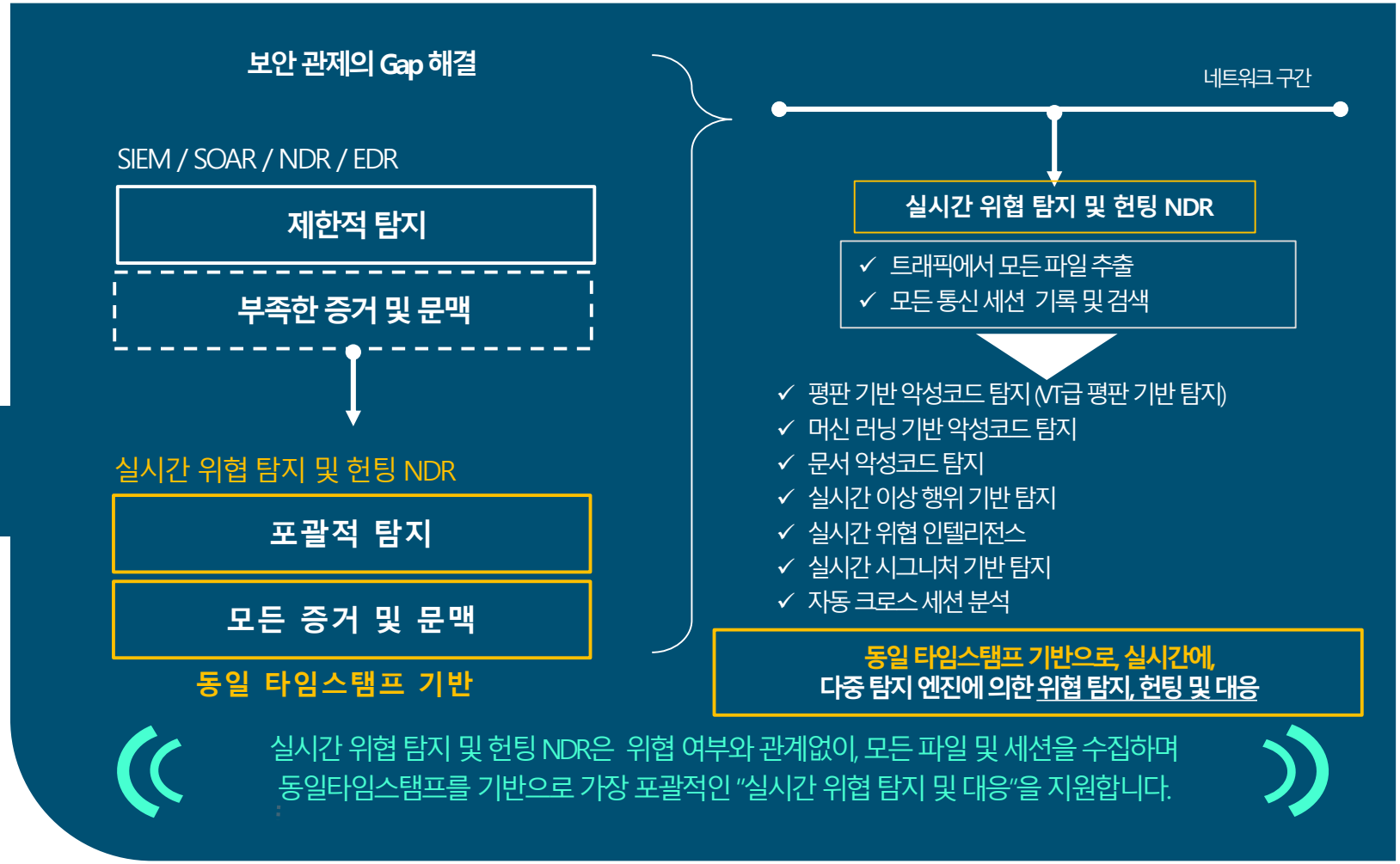
실시간 위협 탐지 및 헌팅 NDR은 DFI (Deep File Inspection), 머신러닝(ML) 등을 활용하여
네트워크 구간의 파일을 자동 수집 및 분석하고 위협을 사전에 탐지합니다.

실시간 위협 탐지 및 헌팅 NDR: 위협 헌팅

암호화 트래픽
잠재 위협 탐지 및 대응

FDR (File Detection and Response)

Open NDR



실시간 위협 탐지 및 헌팅 NDR Summary

네트워크상의 위협을 신속하게 가시화 함으로써 공격자의 Dwell 타임을 줄이는 것이 핵심 !

Real-time DETECT, HUNT, RESPOND

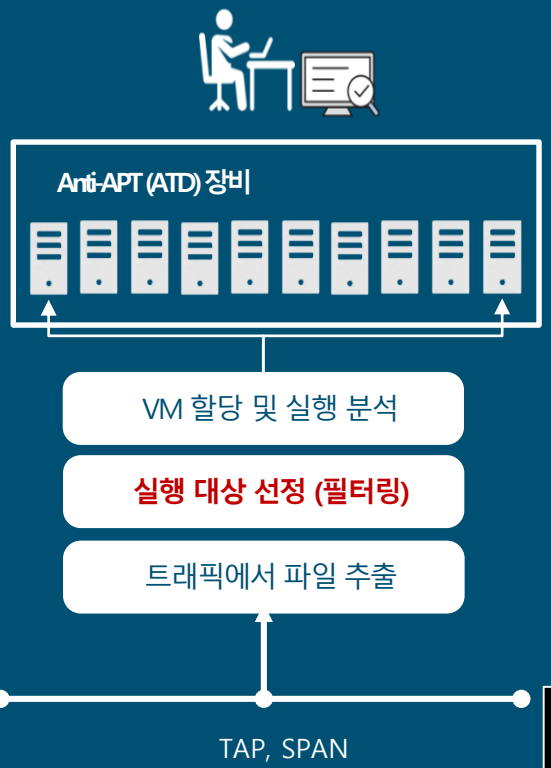
실시간 FDR + 실시간 NDR + 고속 위협 헌팅

- 실시간 악성코드 탐지
- 실시간 네트워크 위협 탐지
- 자동 킬 체인 분석
- 세션 교차 분석
- 사각지대 없는 양방향 통신 기반 위협 헌팅 및 사고 분석
- 암호화 통신 분석 (메타데이터)
- 대응 가이드 라인 제공

Cf.) Why FDR?

출현 배경

파일 탐지 및 대응 (FDR)는 미국 국방부(DoD)를 공격하는 국가 지원 위협에 의한 일간 "수백만 건의 파일 기반 공격"에 대응하기 위해 미국 국방부를 방어하는 임무를 맡은 SOC 분석가와 위협 헌터들의 경험에서 비롯됨.



우회 기술의 발전

악성코드가 Anti-VM, Anti-Sandbox 기능을 갖춤

필터링의 한계

파일의 구조를 분석하여 악성코드 특징이 있는 것만 선별 ➔ 악성코드 자체를 필터링!!

분석 성능 문제

실행 분석은 자원이 많이 소요되어 수만개 ~ 수백만개 파일을 분석할 수 없음 (성능: 1Gbps 128 대?)

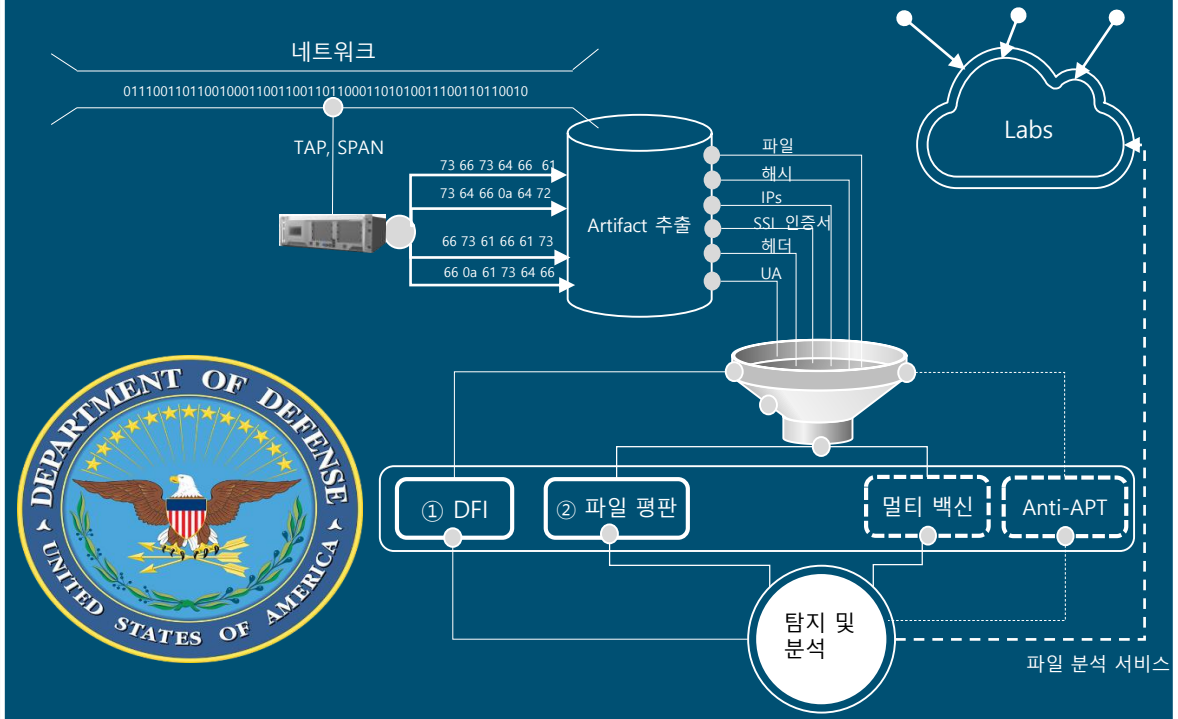
제한된 파일 타입 지원

실행 파일 및 문서 파일 위주 지원

※ 글로벌 선도 Anti-APT 악성코드 탐지율 : 50%
※ 일간 분석 가능 악성코드: 수 백 ~ 수 천개

FDR 사용 이유

FDR (File Detection Response)
➔ 미국 국방부(DoD)를 노리는 일간 수백 만개 파일에 대한 누락없는 고속 악성코드 탐지! (※ 30여종 의 파일 타입 지원)



Cf.) Why FDR?

FDR 사용자(일부)

FDR (File Detection Response) : 현재 미 국방부(DoD) 공유 글로벌 네트워크인 JIE(Joint Information Environment)에서 채택 사용 중인 솔루션 중 하나

미국 국방부 산하 보안정보체계국(DISA) (Defense Information Systems Agency)

미국 국방부 산하 국방위협감축국 (DTRA) (Defense Threat Reduction Agency)

미국 국방부 산하 육군부 (Department of the Army)

미국 국방부 소속 정보부대 국가정찰국 (NRO) (National Reconnaissance Office)

미국 국방부 (펜타곤 PENTCIRT) (Pentagon CIRT) Computer Incident Response Team

미국 방위산업체

FDR 사용 이유

ATD (Anti-APT) 기술적 한계

- 분석 성능: VM 대수의 한계 (성능: 1Gbps: 128 대?)
- 미탐: 파일 구조에 의한 필터링 (다수 악성코드 발생시, 분석 안함: 구조 판단 및 필터링)
- 우회: 우회 기법 (샌드박스 우회)
- 파일 타입: 제한된 파일 타입 지원 (실행파일, 문서 파일)

미국 국방부(DoD)는 적성국가 등 수많은 해커들이 노리는 목표이므로 일간 수십만 개의 다양한 파일 타입에 대한 감시 필요!

Carrier Extensions	Archive Formats	MIME Types
• CHM • DOC* • EMF • EXE • HTA • HTML • JAR • JS • LNK • PDF • PPT* • PS1 • SWF • WMF • XLS*	• 7Z • AR • ARC • ARJ • BZIP2 • CAB • COMPRESS • CPIO • DEB • FLAC • GZIP • ISO • LZMA • RAR • RPM • TAR • XZ • ZIP	• application/cdf* • application/java* • application/msword* • application/pdf* • application/vnd* • application/x-java* • application/x-shockwave-flash* • text/rtf*

Cf.) Batch 처리 vs. 실시간 처리

	배치 처리	실시간 처리
처리 방식	일정량의 통신 데이터 (Chunk) 가 모아서 데이터를 저장한 후, 일괄 처리하는 방식 반복적인 수집 및 처리	통신이 발생하면 획득한 데이터를 즉시 처리하는 방식
하드웨어	대규모 데이터를 저장하는 데 필요한 스토리지 필요 배치 처리를 위한 처리 자원은 비교적 적음	현재 데이터 패킷을 처리하는 데 필요한 스토리지가 적음 실시간 처리를 위해 많은 처리 자원이 필요
성능	지연 시간은 몇 분, 몇 시간 또는 수일 수 있음	지연 시간은 밀리 초 단위로 보장
데이터 세트	대규모 데이터 단위	지속적인 데이터 스트림
분석	장 시간의 복잡한 계산 및 분석	신속한 계산 및 분석