🌛

3 / 16 (1)

- ChatGpt
  - 시그니쳐
    - 악성 소프트웨어를 탐지하고 식별하는 데 사용되는 디지털 지문이다. 이 디지털 지문은 악성 코드의 특정 패턴을 나타내는 바이너리 데이터의 일련의 값으로 구성된다.
  - 시그니쳐 기반
    - 시그니쳐를 사용하여 악성 코드를 탐지하고 차단하는 기술이다. 이 기술은 주로 백신 소프트웨어에서 사용되며, 악성 코드 데이터베이스를 유지 관리하고, 컴퓨터 시스템에 설치된 소프트웨어와 파일을 스캔하여 악성 코드 시그니처를 비교하는 방식으로 작동한다.
    - 악성 코드의 시그니처가 이미 알려져 있으면, 백신 소프트웨어는 해당 시그니처가 감지되면 해당 소프트웨어나 파일을 차단하거나 삭제하는 등의 대응 조치를 취할 수 있다. 그러나 시그니처 기반 보안은 새로운 악성 코드나 변종에 대해서는 효과적이지 않을 수 있다. 이는 악성 코드가 새로운 시그니처를 생성하여 감지를 회피하기 때문이다.
    - 따라서 최근에는 시그니처 기반 방식을 보완하기 위해 행동 기반 보안 기술이 등장하고 있다. 이는 악성 코드가 실행되는 행동 패턴을 분석하고, 악성 행동을 탐지하는 방식으로 작동한다.
- 시그니쳐 기반
  - 시그니처(서명)
    - 바이러스의 흔적, 형태, 구성, 코드
    - 바이러스 샘플 이용
    - 백신 제작사들은 이러한 샘플을 수집하여 진단하고, 치료하는 방법을 알아내어 이를 안티바이러스 DB에 추가하여 치료
  - 동작 원리
    - 이미 발견된 악성 프로그램(바이러스)에 대한 전문가의 분석을 통해 시그니처를 생성하고, 이를 기반으로 동일한 악성 프로그램이 사용되는 경우, 이를 탐지

하는 방식

- 시그니처 기반으로 프로그램을 스캐닝하고 악성 구조가 탐지되는 경우, 악성 프로그램에 감염된 것으로 정의

- 한계
  - 완전 동일한 경우에만 동작
  - 알려지지 않은 악성프로그램에 대처 불가능
- 악성 프로그램
  - 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭
  - 멀웨어, 악성 코드, 바이러스, 웜바이러스, 트로이 목마 등
  - 스파이웨어
- 백신 종류 - 시그니쳐 기반 (관리 분야)
  - V3, 하우리 (ViRobot), 알약
  - Bitdefender(루마니아), Norton(Symantec/미국/캘리포니아), Mcafee(미국/캘리포니아), Kaspersky(러시아/모스코바), Panda(스페인), BullGuard(런던), ESET(슬로바키아), Avira(독일), Avast(체코/프라하), AVG(Avast개인), Trend-micro(PC-실린: 미국-대만-일본), F-secure(핀란드), Microsoft defender(MS)…
  - Virus Total
  - OS사의 백신 지원
- 차세대 방화벽
  - NGFW는 전통적인 방화벽 보다 더욱 진보된 기능을 제공한다.
  - 기존 방화벽은 3 ~ 4 계층에서 작동, 패킷의 내용은 검사하지 못한다.
  - 하지만 차세대 방화벽은 7계층 전체에서 작동하며, 패킷의 내용을 분석하고, 보안 위협에 대응할 수 있다.
  - 기존 패킷 필터링, 포트 및 프로토콜 기반의 제어보다 더 세분화된 제어 및 검사를 가능하게 하는 다양한 기술들을 적용하여 네트워크 보안의 효율성과 정확성을 높인다.
- IPS/IDS
  - IDS(Intrusion Detection System)와 IPS(Intrusion Prevention System)는 네트워크 보안 장비로서, 네트워크 내에서 흐르는 패킷과 플로우 데이터를 분

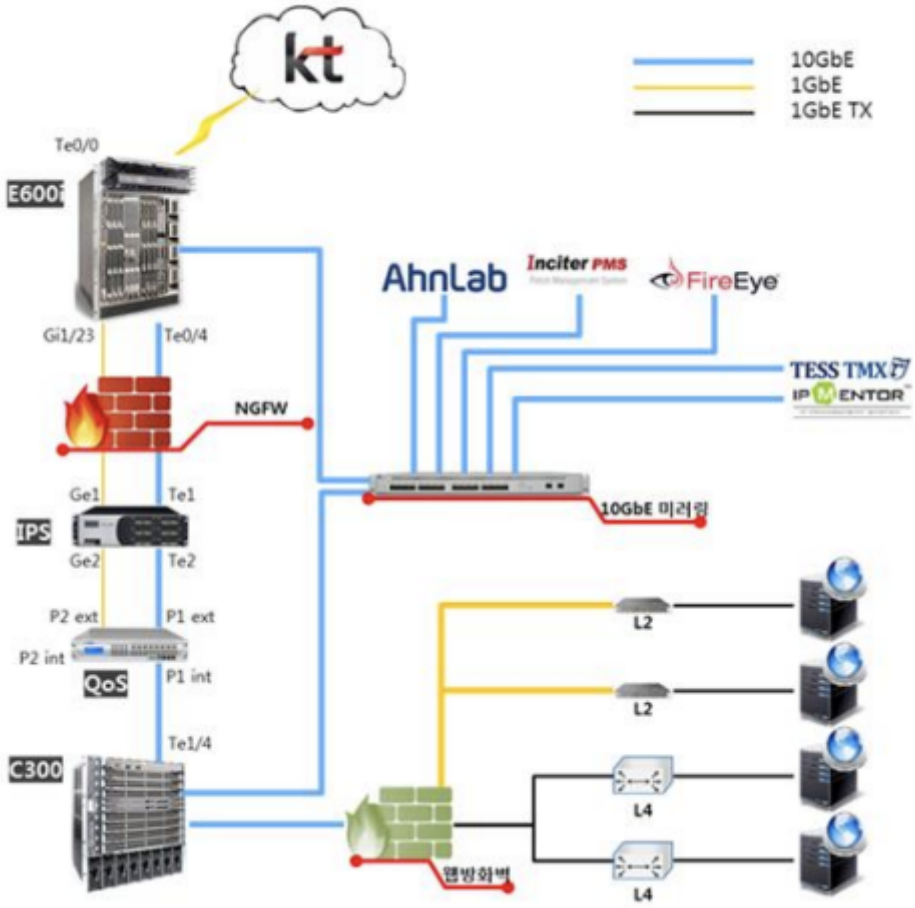
석하여 악성 행위를 탐지하고 차단하는 역할을 수행합니다.

- 패킷과 플로우 데이터는 네트워크에서 전송되는 데이터의 기본 단위입니다.
- 패킷은 데이터 전송 시 데이터를 분할한 작은 조각을 말하며, 각각의 패킷은 목적지에 도달할 때까지 독립적으로 전송됩니다.
- 플로우 데이터는 같은 출처와 목적지를 가지는 패킷의 그룹을 말합니다.

- IDS는 네트워크 트래픽을 모니터링하고, 이상행위를 탐지하는데 사용된다.
- IPS는 이상 행위 데이터를 탐지한 뒤 차단하는 기능을 가진다.
- 하지만 IDS와 IPS가 데이터의 흐름을 보호하는데 중요한 역할을 하지만, 완벽한 보호를 보장하지 않는다. 새롭게 등장할 경우 대처가 불가능하다. 그래서 보안전략을 수립해 다양한 보안 기술을 활용해야 한다.

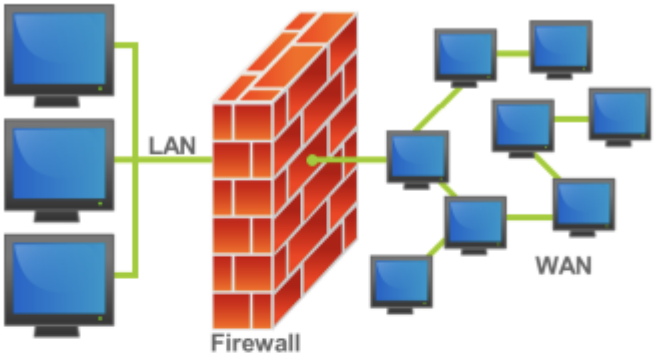
- IOC(Indicator of Compromise/침해지표) DB 활용
- 이후의 변화
  - 비서명 제품의 등장
  - Machie running, AI, BigData 기법

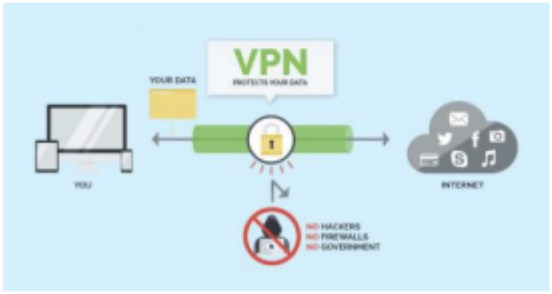
  - 센서, 기존 방화벽, IPS/IDS, 메타데이터 넷플로우, 또는 센서 및/또는 기타 네트워크 원격 측정의 전략적 배치를 가정하는 기타 네트워크 데이터 소스 활용
  - 북/남 트래픽과 동/서 트래픽은 물론 물리적 환경과 가상 환경 모두에서 트래픽을 모니터링

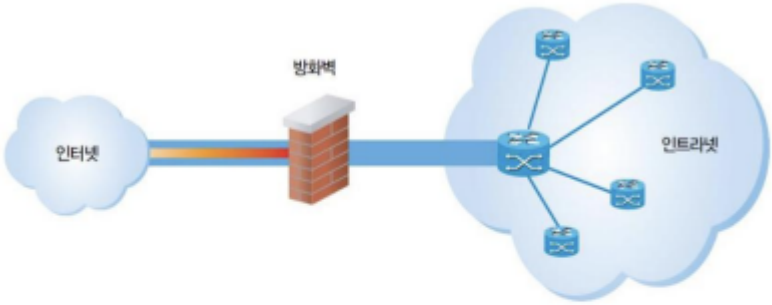


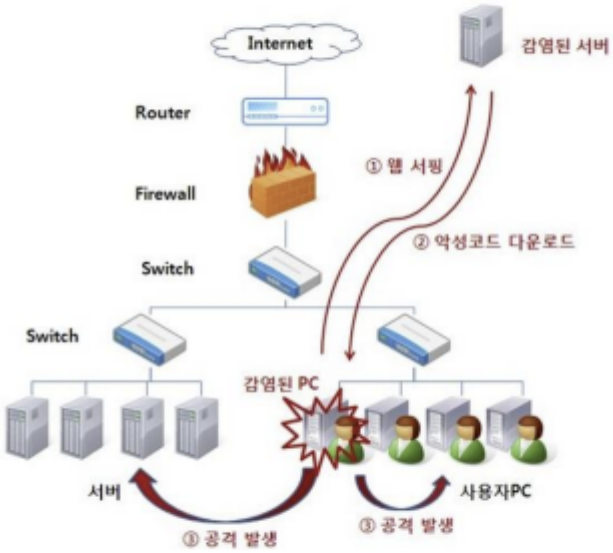
- 소프트웨어 제품 개발
  - DRM/ 문서 암호화
    - 디지털 권리 관리(Digital rights management, DRM)는 출판자 또는 저작권자가 그들이 배포한 디지털 자료나 하드웨어의 사용을 제어하고 이를 의도한 용도로만 사용하도록 제한하는 데 사용되는 모든 기술들을 지칭하는 용어이다. CDM(Content Decryption Module)에 기반한다.
    - 종종 복사 방지, 기술 보호 장치와 혼동하기도 한다. 디지털 권한 관리 설계의 일부
  - Host DLP (Data Loss Prevention)
    - vs Network DLP
    - 휴대용 저장장치로의 자료 유출을 방지
    - 실제 운영은 지정된 공간(폴더)으로부터 나올 때, 소정의 절차를 거치도록 하는 방식

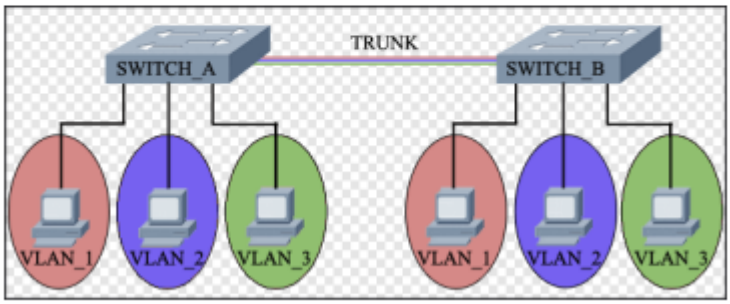
        - 보안 정책에 따라 미리 등록된 화이트 리스트로 지정된 컴퓨터, 사용자, 그룹만이 허가된 휴대용 기기 또는 장치를 사용하게 하고, 전송되
          는 모든 자료를 추적 및 관리하는 보안 시스템
    - 원격 제어 : RPC같은 원격 host접근 제어 프로그램
    - PC방화벽 : PC에 설치된 프로그램을 통하여 허가되지는 않은 트래픽이나 프로그램이 동작하지 않도록 하는 보안 시스템 또는 프로그램
    - DB접근제어 : DB사용자의 권한에 따라 명령어 등에 대한 제약을 하도록 관리는 보안 시스템
    - DB암호화
        - 누군가 인증되지 않은 사용자가 Databse에 접근하여 query하더라도 유의미한 데이터를 scanning할 수 없도록 특정 암호화 알고리즘에 의하여 암호화 하는 보안 시스템
        - Block방식과 file방식으로 나뉠 수 있음
    - 하드웨어 기반 제품 개발
        - 방화벽
            - 컴퓨터 네트워크에서 바라지 않거나 인증되지 않은 통신을 막도록 설계된 프로그램이나 하드웨어
            - 내부망과 외부망의 격리(IP, Port기반)
        - 보안스위치
            - L2/L3 스위칭과 보안 기능을 동시에 제공
            - MAC Flooding, MAC변조, ARP attack 대응
        - VPN Virtual Private Network
            - 공중 네트워크를 통해 한 회사나 몇몇 단체가 내용을 바깥 사람에게 드러내지 않고통신할 목적으로 쓰이는 사설 통신망
        - VLAN
            - 컴퓨터 네트워크에서 여러 개의 구별되는 브로드캐스트 도메인을 만들기 위해 단일 2계층 네트워크를 분할할 수 있는데, 이렇게 분리되면 패킷들은 하나 이상의 라우터들 사이에서만 이동할 수 있다. 이러한 도메인을 가상 랜(Virtual LAN)으로 부르며, 가상 근거리 통신망(Virtual Local Area Network), 가상 LAN(Virtual LAN), 또는 간단히 VLAN으로도 표기


LAN
WAN
Firewall


VPN
YOUR DATA
YOU
INTERNET

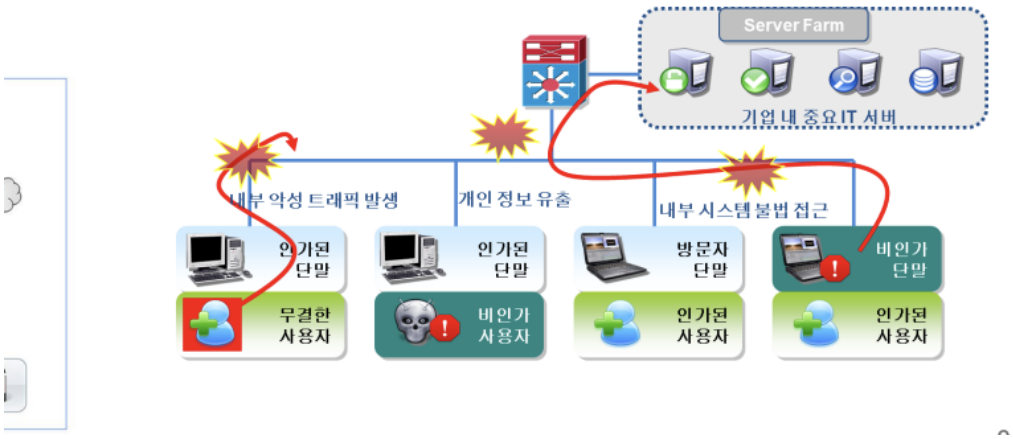






- 시스템 접근제어
- 네트워크 상에 존재하는 모든 시스템에 대한 단일 관문(gateway)로 구성
- 접근 제어 로그 증적 자료 취합
- 네트워크 접근제어 NAC Network Access Control
  - IP와 MAC을 가지고 있는 IP자산(PC 등)이 네트워크에 접근하기 전 보안 정책 준수 여부를 검사한 후, 내부 네트워크로의 접근 허용
  - 내부 방화벽 : 내부에서의 접근 경로 통제(vs 방화벽)
- 네트워크 DLP Data Loss Prevention

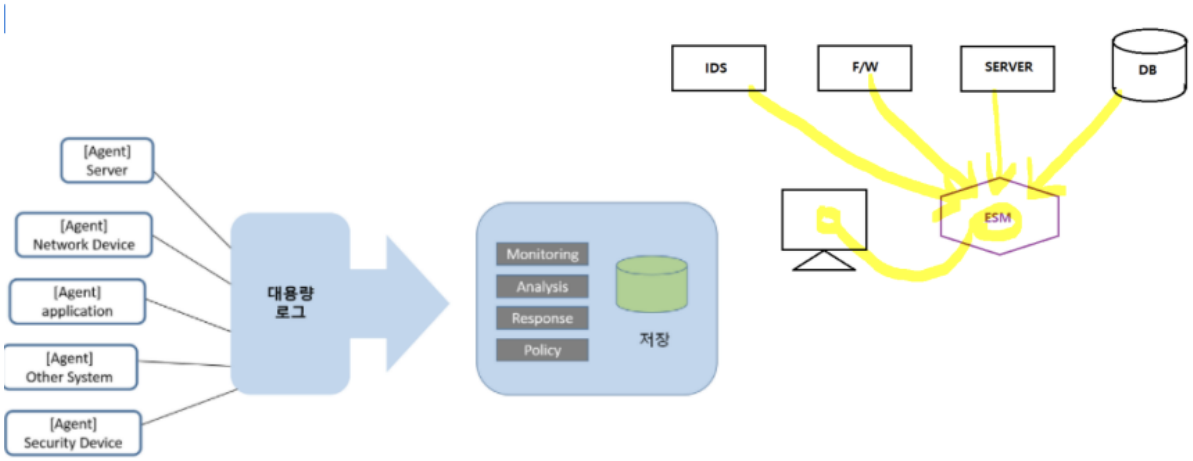
- 네트워크 행위를 통하여 내부 데이터의 유출을 방지(필터링)하거나 감시함.



- APT Advanced Persistent Threat
  - 고급"(advanced) 프로세스는 시스템 내의 취약점을 공격하기 위해 악성 소프트웨어를 이용한 복잡한 기법을 나타내고 "지속"(persistent) 프로세스는 외부 C&C(커맨드 앤드컨트롤) 시스템이 지속적으로 특정 대상의 데이터를 감시하고 추출한다. "위협"(threat) 프로세스는 공격을 지휘할때 인간이 동반됨을 뜻
- Anti-DDOS denial-of-service attack, DoS attack
  - 시스템을 악의적으로 공격해 해당 시스템의 리소스를 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격
  - 이를 막기 위한 시스템 또는 방어 체계

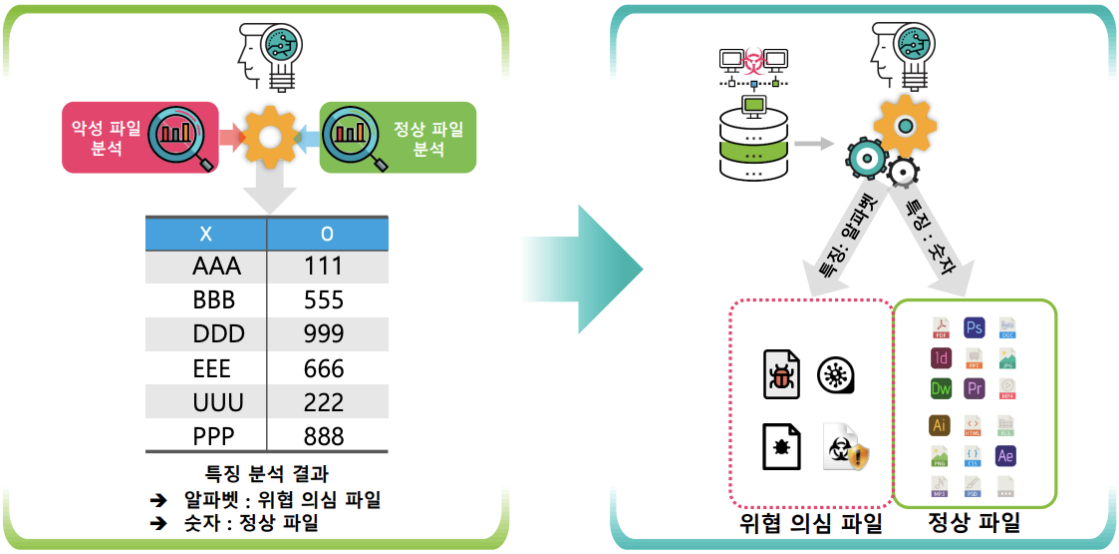
- 이벤트 분석 및 처리
  - ex. EDR, EPP 등
  - EDR Endpoint Detection & Response
    - 단말(PC 등)의 행위(정상/비정상)에 대한 반응 체계
  - ESM Enterprise Security Management
    - 통합 보안 관리 시스템
  - TMS Threat Management System
  - SIEM Security information and event management
    - 보안 정보 관리(SIM) + 보안 이벤트 관리(SEM)
    - 데이터와 포렌식 분석에 중점
  - 장애 예측 시스템
    - 행위 분석 + AI기술 접목

- 포렌직(디지털 포렌직 전문가)
  - 범죄에 사용된 컴퓨터나 범죄 행위를 한 컴퓨터로부터 디지털 정보를 수집하는 것
  - 컴퓨터에서 압수되는 디지털 증거물은생성/복사/변경/삭제가 용이한 특징을 가지고 있어특별한 절차와 방법들이 요구
- 로그분석

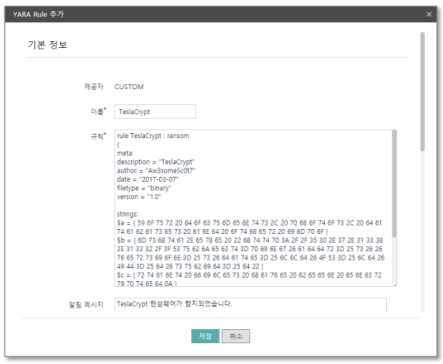
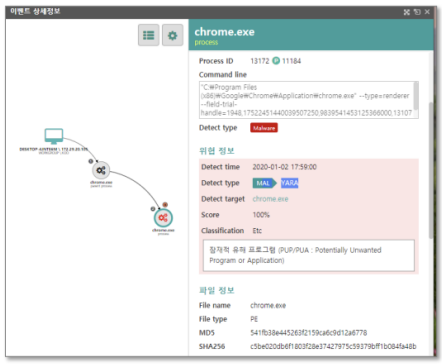


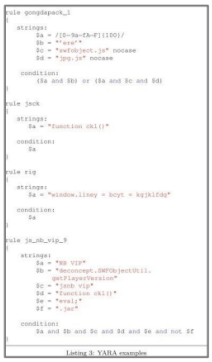
- 망 분리
  - 망 분리는 네트워크를 분할하여, 보안을 강화하는 것을 말한다.
  - 물리적 분리 - 서로다른 네트워크를 장비로 연결
  - 논리적 분리 - VPN
  - 제어 기술 분리 - 방화벽, 스위치, 라우터 장비를 이용해 분리
  - 기능 분리 - 서버를 분리 (데이터베이스 서버, 웹서버 분리)

- VDI - (Virtual Desktop Interface)
- 행위 기반
- 머신 러닝 (ML)
  - 악성파일 / 정상파일의 특징을 학습 / 분석하여, 의심되는 파일을 탐지하는 기술

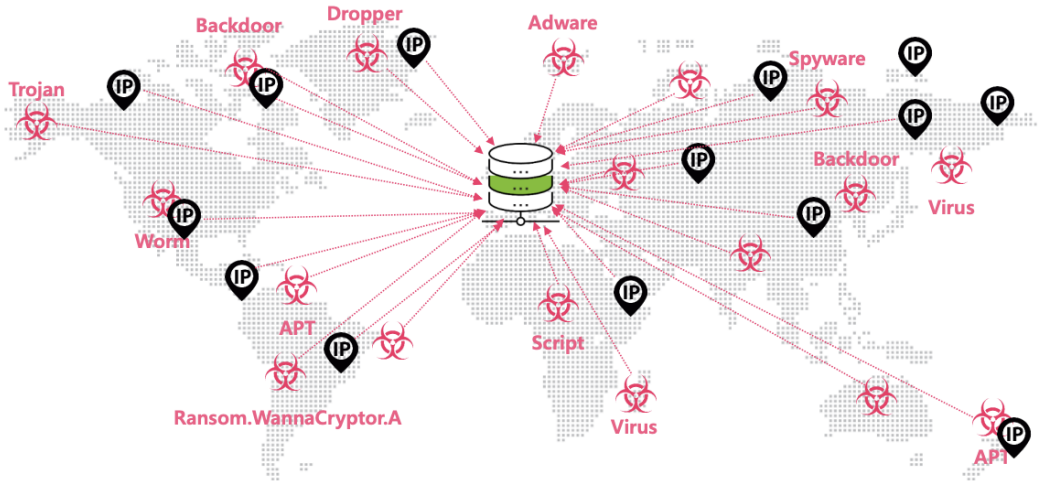


- YARA
  - 보안 관리자가 직접 생성한 패턴 매칭 탐지 기술
  - 문자열이나 바이너리 패턴(Hex String)을 기반으로 미리 정의된 시그니처로 악성 코드를 분류할 수 있게 하는 도구
  - 백신 등 endpoint에서도 활용하고 있는 탐지 기법
  - 고려사항
    - 모든 파일, 프로세스에 대해 행위 기반 탐지를 적용하기 위해서는 자원 소모가 많고 무겁게 동작

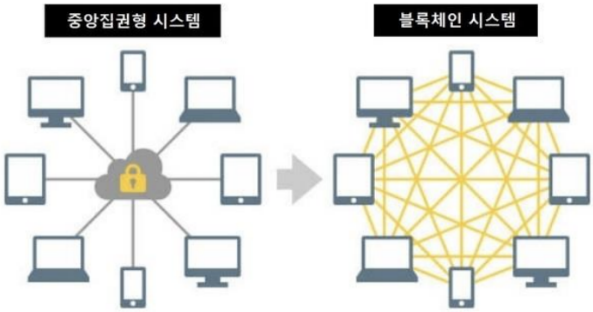





- IOC(침해 지표) 기반의 위협 탐지
  - IOC (Indicator Of Compromise, 침해지표)
    - 전 세계에서 탐지된 악성파일/IP 정보를 DB 화 하여 알려진 위협을 탐지합니다.

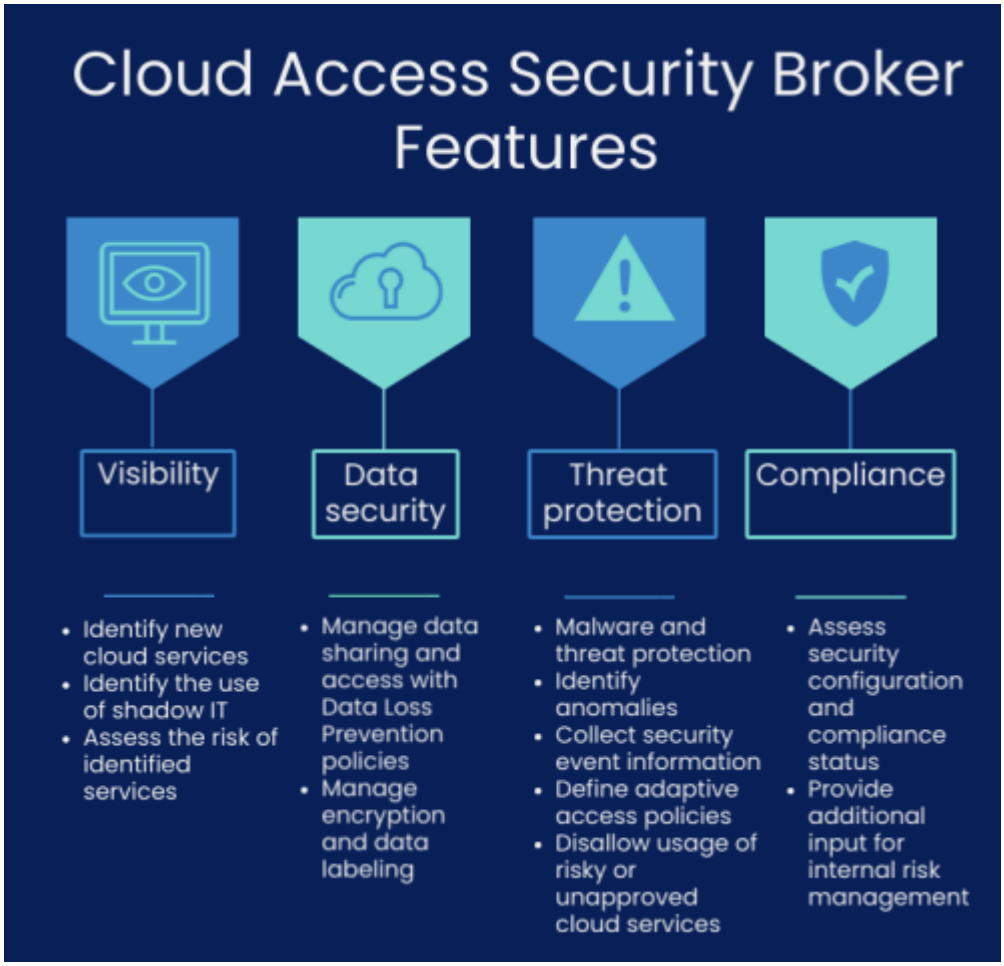


- 블록 체인
  - 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여, 누구라도 임의로 수정할 수 없고, 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술



- Cloud 보안 및 CASB
  - 클라우드에서의 보안 서비스 제공
  - CASB Cloud Access Security Broker
    - 클라우드 환경에서 안전을 담당하는 중개자 기능을 제공하는 보안 레이어
  - 주요 역할과 기능
    - 개별 사용자의 클라우드 이용 상황 가시화
    - 취약한 클라우드 애플리케이션 제거
    - 행위 분석을 통한 정보 유출 방지

        - 클라우드 환경을 이용한 기밀 정보의 암호화, 토큰화 등의 통합 보안 구현
    - CASB의 활용
        1. 개별 사용자의 애플릭이션 사용 현황 가시화
        2. 데이터 보호
        3. 사용자의 위협 행위 탐지 및 제어
            a. 공유 해제, 권한 변경 파일 암호화 등에 개입
        4. 데이터 통신 경로의 관리
            a. 클라우드 전환 구간에서의 프록시 기술 등을 통한 사용자 접근 또는 데이터 흐름에 대한 통합 관리
        5. 컴플라이언스
            a. 통합 위협 관리



- 보안 관제 및 운영

    - 보안 인프라의 원활한 본연의 기능 수행 및 감시
    - 보안 사고 발생 시, 사후 감사 활동
    - 정보보안 운영 (CISA, CISSP, CCFP, SSCP, CAP, CSSLP, HCISPP)
        - CISSP(Certified Information Systems Security Professional)
        - CCSP(Certified Cloud Security Professional)
        - CISA(Certified Information Systems Auditor)
        - CISM(Certified Information Security Manager)
        - CCFP(Certified Cyber Forensics Professional)
        - SSCP(Systems Security Certified Practitioner)
        - CAP(Certified Authorization Professional)
        - CSSLP(Certified Secure Software Lifecycle Professional)
        - HCISPP HealthCare Information Security and Privacy Practitioner
    - 프로젝트 관리(PMP)
- 보안 관리 (정책 & 법률)
    - 정책 준수
    - 법률 준수(인증 제도)
    - ISMS(Information Security Management System) 인증 심사 (인증심사원)
    - 보안 커설팅(정보보안기사)
    - 개인정보보호(CPPG/개인정보보호 관리사)
    - 정보 유출 방지(산업 보안 관리사)

- 다음 PPT 과제 주제 목록

분야	소프트웨어 제품		하드웨어 제품(어플라이언스)	
	시그니처 운영 (업데이트)	단순관리서버 (정책운용)	서버 탑재 형태 (서버의 action 사용)	시스템 형태 (복합적인 동작구조)
백신	O	O		
방화벽		O	O	
네트워크 접근제어		O		O
내PC지킴이		O	△	
IPS(ntrusion Prevention System)	O	O		O
IDS(Intrusion Detection System)	O	O	O	
Anti-DDOS	△	O	△	
NDR(Network Detection and response)		O	O	
EDR(Endpoint Detection and Response)	△	O		
EPP(Endpoint Protection Platform)	△	O		
NTA(Network Traffic Analysis)		O	△	
XDR(ALL-X Detection and Response)	△	O	△	
EMS(Event Management System)		O	△	
TMS(Traffic Management System)		O	△	
장애예측시스템		O		
DRM(Digital Right Management)		O		
Host DLP(Data Loss Prevention)		O		
Network DLP(Data Loss Prevention)		O	O	
랜섬웨어 방지		O		O
PC방화벽		O		
DB접근제어		O		
DB암호화		O		
보안스위치		O		O
VPN(Virtual Private Network)		O		O
VLAN(Virtual Local Area Network)		O		O
시스템 접근제어		O	O	
APT(지능형 지속 공격(Advanced Persistent Threat))		O	△	O
로그분석		O		
SEIM(Security information and event management)		O		