안녕하세요. 이찬우라고 합니다.

금융협회/카카오/SK(Cloud)/쿠팡/뤼이드(산타페이)

현 AI-THE,CEO

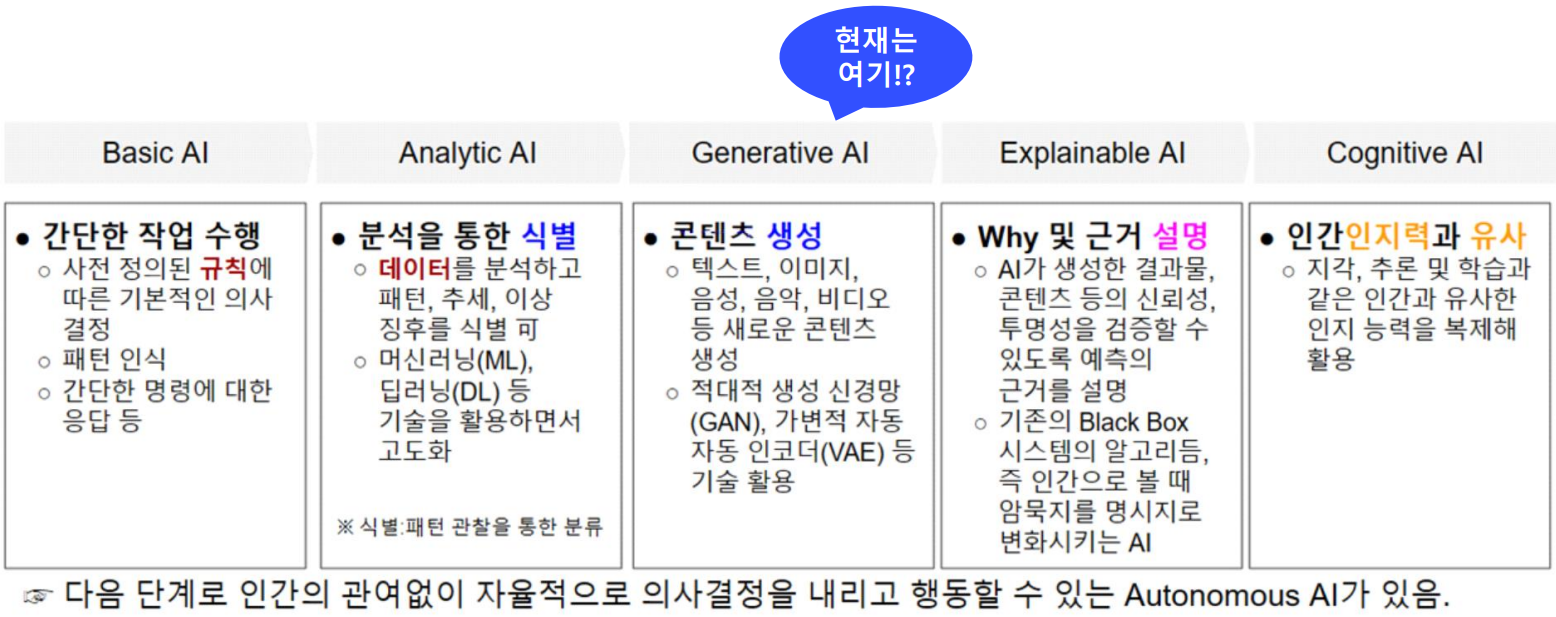
--------------------------------------------------------------------------------

//Intro

AI를 사용할 때 Chaining Prompting를 이용하여 원하는 답에 가까운 출력을 얻는 것이 중요함.

> Chaining Prompting : 자세한 질문을 연속적으로 입력함.

AI가 학습의 단계에서 추론의 단계로 넘어감.



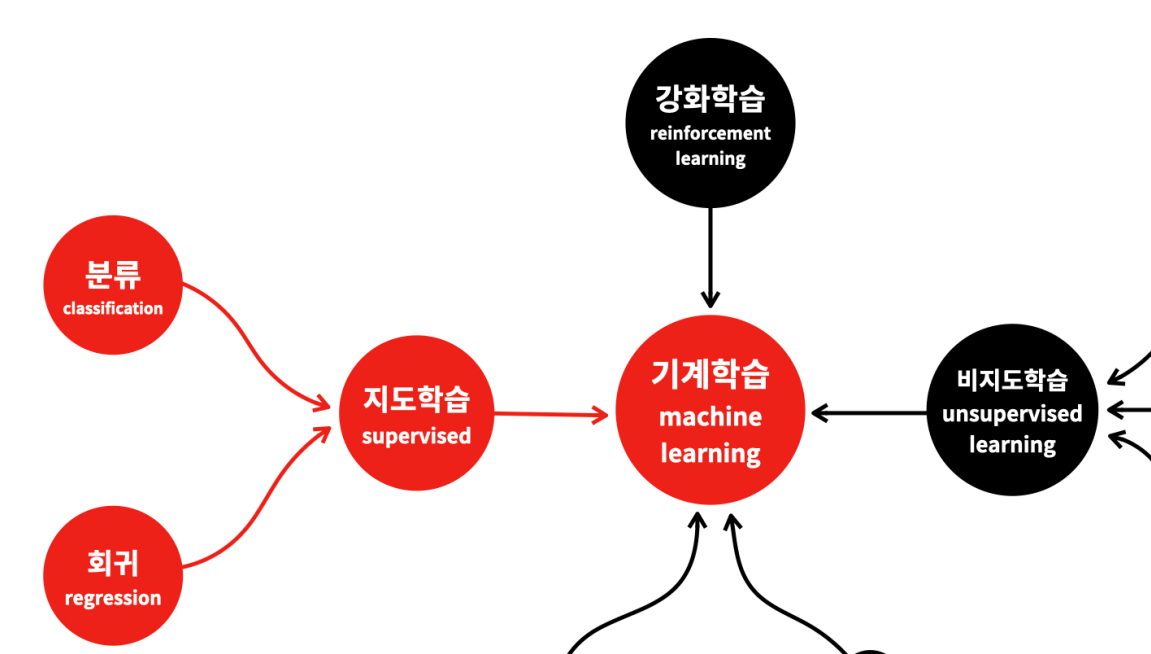
> IT분야에 종사하게 되면 신기술에 대한 지속적인 관심을 가지고 있는 것을 추천함.

보안과 AI는 아버지가 같다.

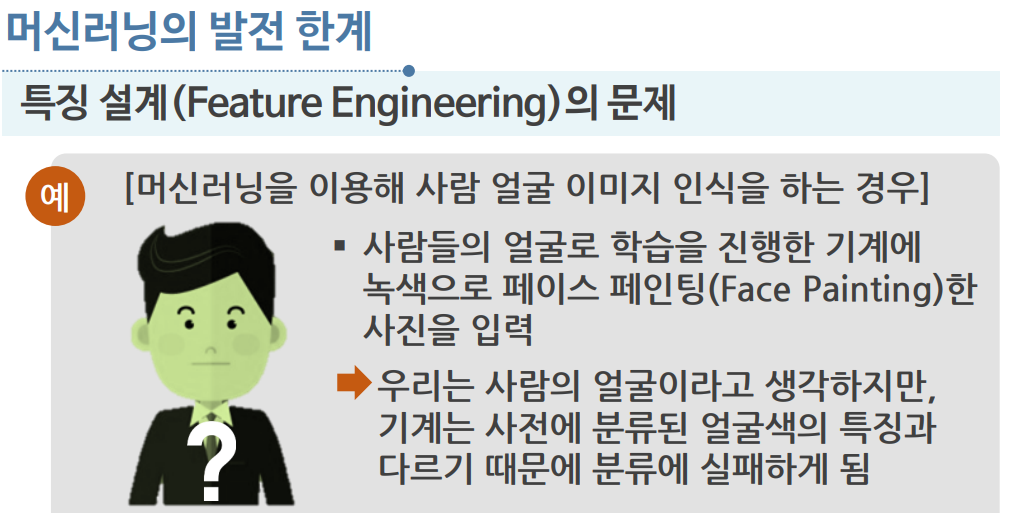
> 튜링머신 : 최초의 컴퓨터, 2차세계대전당시 상대의 암호문서를 복호화 하기위해 사용됨.

연속형 정보(정량적 결과) > 회귀

범주형 정보(정성적 결과) > 분류



ML의 한계 : 특징 설계 : 얼마나 효과적인 특징을 찾아내느냐에 달려있음.



// 해킹

해킹 차단 : 의도하지 않은 동작 + 권한 상승 | 차단(일회성, 기술, 연속성 고려 X)

-> 개발자, 분석가, AV 개발자, 솔루션 엔지니어 (기술)

정보 보호 : 해킹 차단 + 증명 | 지속가능성(조직, 정책, 예산, 사람, 솔루션) + PDCA(백신 설치 계획서 + 백신 설치 + 백신 운영(정책 수정, 업그레이드) + 백신 업그레이드(개선)) -> ISMS 인증 취득, 사고 면피/경감, 과징금/과태료 수준 완화, 고객 피해보상 경감

-> 기업의 보안담당자, CISO, 보안팀, 보안센터, 컨설팅, 관제 (정책, 관리, 법규)

Sample. 회귀분석과 클러스터링이라는 방식을 활용해서 AV(안티 바이러스)와 멀웨어 탐지에 인공지능을 활용하고 있다. 회귀분석의 어떠한 특징 때문에 멀웨어 탐지에 이용할 수 있는지, 또한 클러스터링이라는 방식도 어떠한 특징 때문에 멀웨어 탐지에 주로 이용되는지, 이걸 Anomaly Detection 이라고 하는데, 쉽게 설명해줘. (단, 왜 분류보다는 회귀가 이용이 되는지, 또한 클러스터링(군집화 기법)이 주로 사용되는지를 강조해서 설명해줘.)

- 정적 : 문제+정답

- 동적 : 문제(정답X)

> 보안에서는 동적(비지도학습)학습을 통한 ML이 많이 사용됨.

//악성코드

개념 : 한 줄의 코드, 세 줄의 코드 : CPU, Mem, Disk 동작이 가능한 프로그램

> 컴퓨터의 기능 악용(설계자가 의도한 행위 -> 의도하지 않은 행동을 유발) anomaly Detection 이상징후 탐지

>> UAC(User Access Control) : 사용자 계정 컨트롤

>> ex) regedit 등 중요 파일 혹은 프로그램에 접근할 때 뜨는 알람.

공격 대상의 흐름 : 기계(서버) -> 사람(PC) 취약점 - USB 외장하드 무선통신망(Wifi, 블루투스)

> PerfektBlue : 블루투스 신규 취약점(25.07)(https://www.dailysecu.com/news/articleView.html?idxno=167926)



- 모든 악성코드 유입 지점은 인터넷(퍼블릭 클라우드) : 망분리

> 망분리 되어 있는 경우 “PC 2배”가 되고 ,”망연계”로 연결되어 있음,

> “AD”로 전체 파일 및 프로그램이 중앙집중적으로 관리되고 있으며, NAS는 공동으로 활용함,

>”복합기” 같은 경우는 1대를 다 같이(내부망PC는 물론 외부망PC도)

- 오픈소스를 이용한 Phising : https://www.boannews.com/media/view.asp?idx=129218

> github에 개발자들이 코멘트를 작성하는 부분에 파일 업로드시 자동으로 URL이 배정됨 > 코멘트에 멀웨어를 업로드하여 피싱.



- 최근 : 깃허브, 페이스북, 인스타그램, 유투브, 디스코드, 챗GPT, Claude 등 (오픈소스)

- 가장 심각한 망분리의 위협 : RAT(원격 악성코드), VPN(가상사설망)

> RAT : Remote Access Trojan

> 전자금융감독규정 시행세칙/[별표 7] 망분리 대체 정보보호통제 / 클라우드 관련 업무를 한다면 씹어먹어야 됨.

>> 내부로 혹은 외부로의 자료 전송 시 탐지/차단 및 사후 모니터링 필요.

>> APT(지능형 해킹)에 대한 차단 대책 수립 및 적용 필요.

- 트로이 목마 : Office프로그램 - 외부 객체 참조 OLE

> ex) 매크로, VBA, 프로시져 -> 파일리스 악성코드

> OLE : Object Linking and Embedding , 매크로 기능 등

> 파일리스 : "호출-실행-삭제" 단계를 거쳐 해당 악성코드 파일이 남아있지 않음

- 악성코드는 현재 로그인되어 있는 사용자 권한으로 실행된다. | 관리자 권한으로 실행

> 현재 윈도우에 로그인한 계정은 "사용자" 권한이 아닌 "관리자" 권한임.

\* 악성코드가 주로 컴퓨터에 하는 일 : 프로세스 내장, 메모리/CPU 활용, 부팅 시퀀스 삽입, 관리자 권한(Escalation), 백도어, 파괴(로그)

- 설치 관점에서 악성코드가 갖는 특징 : 더블클릭(사용자 행위), 설치 권한(UAC, 코드 사이닝)

> 코드 사이닝 : 디지털 서명을 통한 무결성과 출처에 대한 보장

>> ex) 게시자를 알 수 없음.

>> 북한에서 좋아하는 방식 : 코드 서명을 해킹하여 악성코드를 포함한 파일에 입혀서 배포함.

// 망분리와 클라우드보안

- 24년 8월 " 금융 분야 망분리 개선 로드맵", 금융위원장 "단계적으로 폐지하겠다"

> 망분리 : 악성코드 유입차단(인터넷 차단), 내부정보 유출차단(인터넷 유출)

> 생성형 AI(인터넷), 클라우드(인터넷) : 기술 경쟁력 악화, IT 직원 이직, R&D 어려움

> 망분리 완화(점진적 축소)

> 국가정보원, 국가망 보안 계획 수립 - 2024년 9월 청와대 사이버 안보 기본 계획 (N2SF)

- 팔란티어 : 미국의 빅 데이터 프로세싱 기업

> 앞으로 : 클라우드 보안, 제로 트러스트, 데이터 공유

- KT는 AWS(Amazone)에서 Azure(MS)로 거의 다 넘어갔음.(MS와의 연계)

// Q&A(프로그램 추천 등)

"NotebookLM"(Google) : 생성형 AI 기반 노트 App> 설치해서 활용해봐라

"Feedly" : 뉴스 크롤링 App

"카피킬러" : 결과물에 생성형 AI가 적용된 정도를 확인하는 도구

> 그냥 복붙은 안되고, 결과물에 대한 이해가 필요함.

Q. 백신을 여러개 깔면 보안이 더블버거마냥 늘어날까

- 느려진다. (성능, 경합, 충돌) BSoD

- 엔진의 성능 거의 동일한데, 패턴이 다름(조금의 도움은 될 수 있음) - 정규표현식(구글 기반 virustotal)

\* Host(PC) : YARA Ruleset

\* Network : Snort RuleSet

Q. 백신을 선택하는 기준이 단순 취향일까

- 백신이 악성코드를 탐지하는 방법 : 회사마다 다름 (통상, 코드 메모리에 로드) - 암호화/난독화 탐지

"avTest" : 백신들에 대한 벤치마킹테이블(BMT) 확인가능

- 백신의 업그레이드/패치 속도 : OS 설치(운영체제 업데이트, 패치, 환경 변화) - 빌드

> 백신의 등급에 따라 패치 안내를 미리 받는 기간이 다름.

- 성능 대비 가격 : CrwodStrike(EDR 적인 요소, 성능, 가격, 클라우드 기반)

- AV(탐지,차단) -> EDR(IR, 원격, 증거, 명령어) ->

> AV는 대응이 없음, 탐지 및 차단만

Q. 무료 오픈소스(윈도우 디펜더) 백신을 사용하면 되는데, 이걸 왜 사용하지 않을까

- 기업용 : 중앙집중적인 관리(관리자 페이지), 일괄 업데이트/삭제/다운그레이드, 기술지원/유지보수/라이센스(책임지는 사람이 없다.), SSO/감사로깅/AD/내부그룹웨어/내부망분리/보안 연동(기능 지원, 프로토콜 지원)

> Windows Defender는 관리자 페이지(위의 기능들이 가능한)가 없음.

//AI for Security

지도 : 악성코드 패턴(Yara 룰셋), 정규표현식 -> 많이 학습

> 개 정보, 고양이 정보 - 개와 고양이

> 호랑이 : 미탐

비지도 : 악성코드(특징) -> 많이 학습

> 개 정보, 고양이 정보 - 2가지 동물

> 호랑이 : 큰 고양이 65%

(참고)CIC(쿠팡, AI+Cloud)

코드유사도 : 분석 결과 주석, 개행문자등 코드의 특징적인 부분들을 비교한 정도.

Q. 사이버 킬 체인

- 오프라인 전쟁 : 킬 체인 (온라인)

- 악성코드의 동작에는 항상 "순서"가 존재함. (전략)

1) 정찰 : 정보 수집

- 도구 : 구글, 사람, 문서, 공간, SNS, 스캐닝, 다크웹

2) 공격 대상 선정

- ROI가 있는 대상인가? (내가 들이는 노력 vs 취할 수 있는 이익)

- 취약점이 많은 대상인가? (Attack Surface, 공격 표면)

- 깨진 유리창의 법칙 : 깨진 유리창 화장실 vs 잘 관리되는 화장실(범죄율 깨진 유리창 화장실 훨씬 높음)

- 공개된 데이터가 얼마나 많은가?

3) 취약점 파악

- 시스템, 네트워크, 웹, DB, 서버, 엔드포인트 취약점 : 스캔

- 공격 수행 : 스텔스 공격

4) 공격 도구 제작/구매

- 다크웹 구매

- 자동화 생성형 AI 악성코드 생성

- 공격 오픈소스 악용

- 보안 취약점 도구 : 양면성(화이트 해커 vs 크래커)

- 내장 쉘 스크립트 악용(매크로 후킹) - 파일리스

5) 전달(딜리버리)

- 내부 이메일

- USB 침투

- SNS 게시물 클릭 유도

- 피싱/파밍 사이트 클릭 유도

- 워터링홀/DBD 홈페이지 접속 유도

- 압축 암호화, 전송 암호화(https), 파일 암호화

6) 은닉

- 숨어 있는다. (실행되지 않는다.)

- 외부에서 C&C 통신을 연결 (Command & Control)

- 해커 : 실행 시점, 실행 방법 전달

7) 실행 및 설치

- 더블클릭 : 사용자 허가(별도의 악성코드 다운로드, 설치)

- 엑셀 파일(매크로)

8) 파괴 또는 훼손

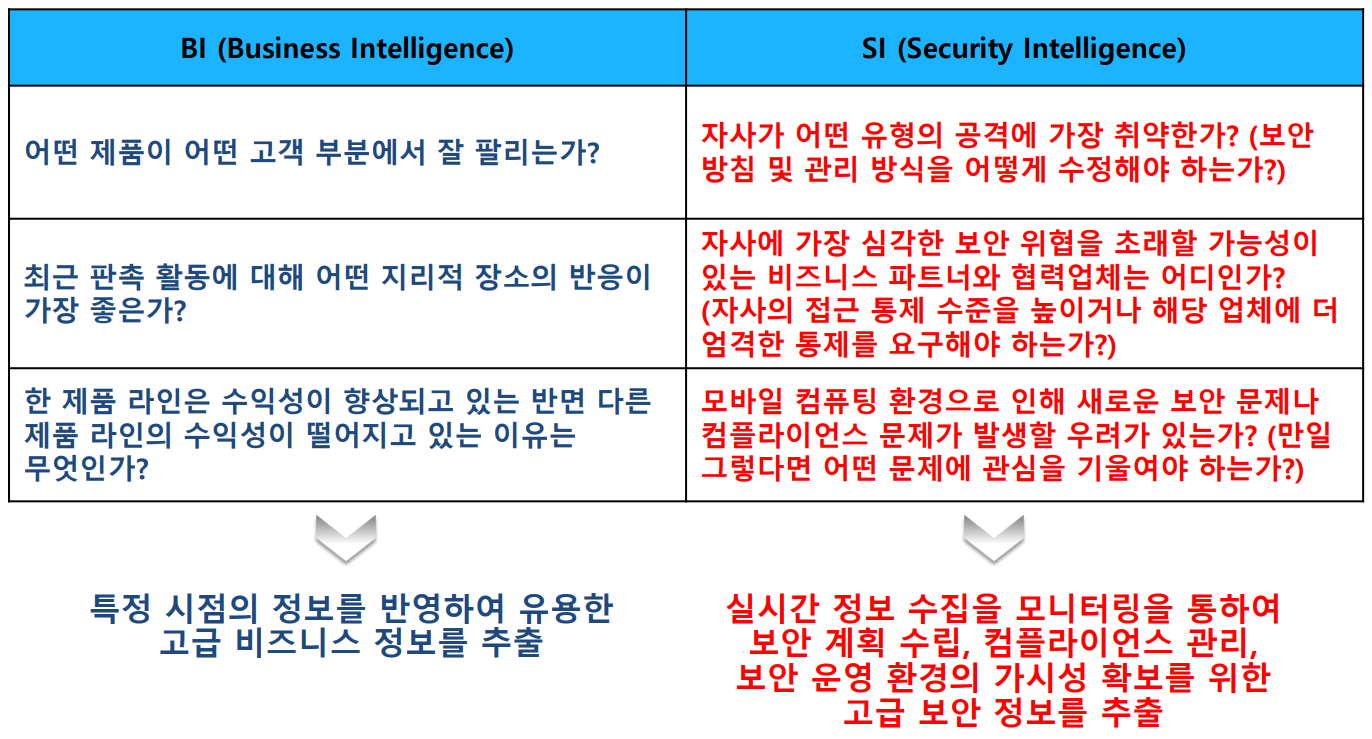
- 데이터

- 쉐도우 볼륨

- 로그 파괴 훼손

- 시간정보 훼손(NTP 서버)

- 마스터 부트 레코드 훼손(MBR)



이상징후탐지를 통한 보안

> 사용자 행위 분석(UBA)

> 이상 금융 거래 탐지 시스템(FDS)

> 배회 : 특정 사람이 좁은 위치에서 왓다갓다함.

>(연구중) 지능형 CCTV : 영상 처리를 활용해 이상 행동을 하는 사람을 탐지해 119 연락 등 대응하는 시스템.

--------------------------------------------------------------------------------

PPT3. "AI의 기술적 한계"는 알아서 보기

--------------------------------------------------------------------------------

실습

--------------------------------------------------------------------------------

실습 1. 침해사고 준비도 가이드 분석

<침해사고 준비도 가이드> 13p~19p

> 디지털 증거 및 기록은 대부분 기록 혹은 로그임.

> 공통 증거 중 활성 데이터는 시스템 종료 혹은 재부팅시 휘발되는 데이터를 의미함.

Step1. 침해사고 준비도 가이드를 읽어보고, 아래의 내용을 생성형 AI를 통해 생성해보고, 분석해보자.

1.1. 악성코드에 의해 시스템 침해 → 어떤 디지털 증거가 남을까? (형식, 경로, 패턴)

1.2. 악성코드에 의해 침해 → 어떻게 증거물을 분석할 수 있을까?

Step2. 생성형 AI 에서 프롬프팅으로 디지털 증거물(File)을 만들고 분석해보자.

2.1. ‘침해사고 유형별 증거 및 기록’에 대해 프롬프팅(침해사고 증거물을 분석하고 싶은데, 아래의 기록을 랜덤하게 생성하고 해당 확장자와 경로를 지정해줘. 다운로드 파일로 만들어줘.)

Ex) 디스크 정보 확인 명령어에 대한 사용 기록(Log)

Ex) CMOS 시간 확인 및 변경 명령어에 대한 사용 기록(Log)

>생성형 AI로 샘플생성, 시나리오기반 자세한 샘플 생성, 분석법, 분석도구

Q. 쉘은 뭐고, 파워쉘은 뭐고, 쉘 스크립트는 또 뭘까요

- 쉘을 딴다. (쉘을 이용해서 내부 원격으로 연결, 명령어 전달, 시스템 핸들링)

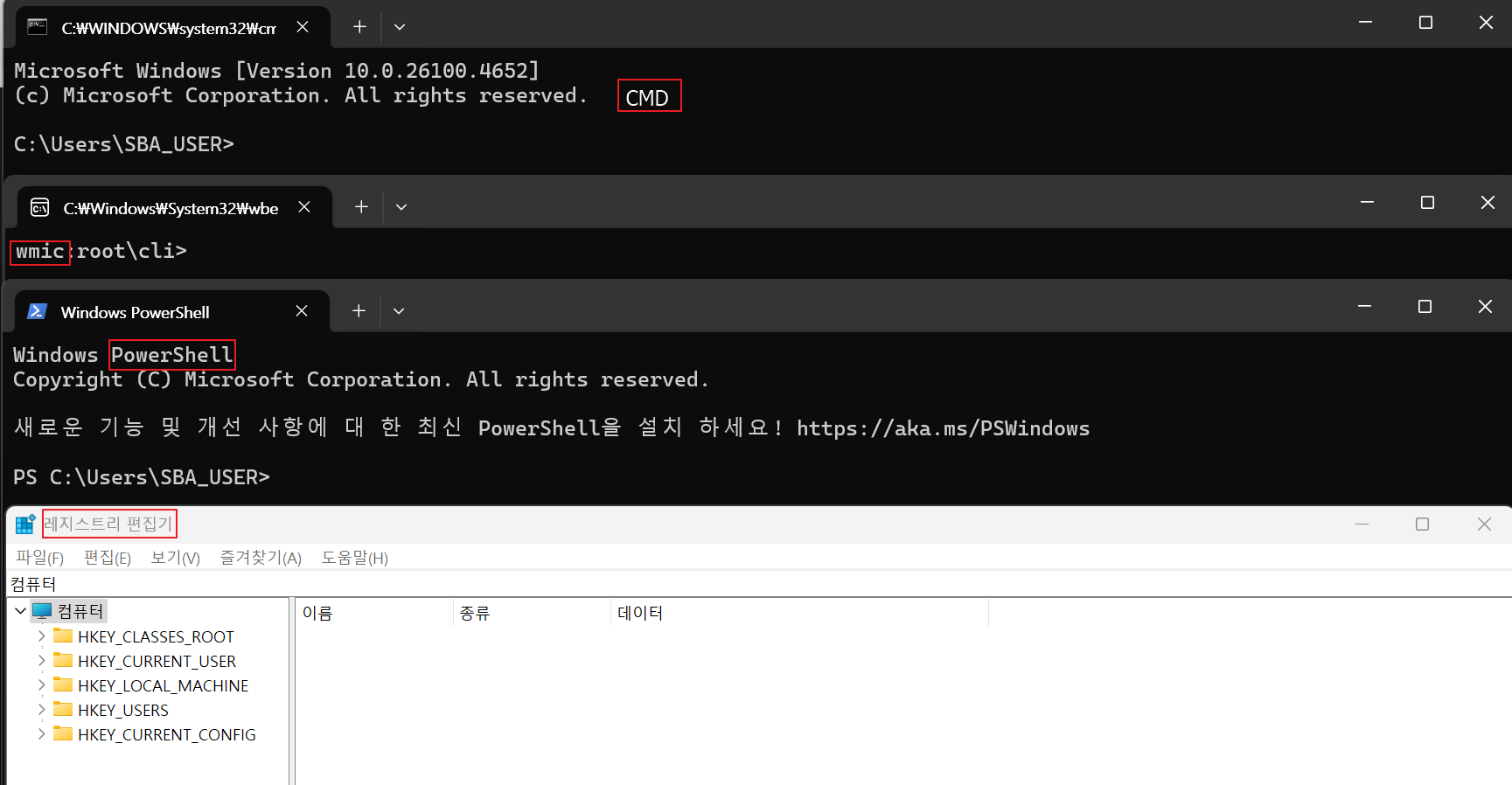
- CTF : 해킹대회 capture the flag(OS 커널, 시스템 메시지, PE 구조) - 스테가노그래피

- 리버싱, 시스템 해킹

- 쉘을 관리 : 내부 실행, 기록, 외부 동작 차단, 백도어 탐지 -> 관리자 권한 제거 (왜? 쉘 관리자 권한)

- 쉘 : 크로스 플랫폼 쉘(윈도우, 리눅스, 유닉스 OS) : CMD, Wmic, powershell(많은 명령어 프로비저닝) (CLI)

> WMIC(Windows Management Instrumentation Command-line) : 윈도우 관리 도구, 기본 내장 CLI 툴



- 쉘 스크립트 : 확장자 빌드(Packaging) .ps1 .bat | 네트워크 전송 할 때 확장자 탐지/차단 zip rar (압축 암호화)

\* 풀리는 암호 : 인증서 보유(Https) 보안서버 Ex) L7 로드밸런서, 웹 방화벽, 웹보안 게이트웨이

\* 안 풀리는 암호 : 압축 암호화, 오피스 암호화, DRM 암호화 (인증서 보유 X) - 악성 메일 주요한 증상

> 회사에서는 PowerShell 실행정책이 설정되어 있음. > .ps1 프로그램 실행이 막혀있음.

MS왈, "VBA는 Copilot으로 점진적 대체 예정임."

(사례) SGI서울보증 랜섬웨어 내용

> "SGI서울보증 랜섬웨어 해킹 공격 요약 보고.txt" 및

"PowerShell 기반 랜섬웨어의 개념적 로직.txt" 참고

2.2. 랜덤하게 생성한 증거물을 분석해보자. (Upload)

Ex) 파이썬 분석 코드를 만듦

Ex) Colab 에 들어가서 파일 업로드(코랩 폴더, 구글 드라이브, 직접 업로드 등) 분석

### [참고사항]

Samples : AD 계정 이상 행위 탐지에 활용할 수 있는 경량화된 샘플로그나 의심스러운 명령어 실행 기록을 랜덤하게 생성하고 싶어. 파일 형식, 파일 저장 경로, 정상과 비정상의 패턴 비교 특징 등을 정리해서 매핑해서 설명하고, 샘플로그는 파일 다운로드가 가능한 형태로 제시해줘. (로그는 200줄을 넘지 말고, 용량은 1MB 를 넘지 않도록 생성해줘.)

> 시트1 확인

Samples : 윈도우 환경의 PC 에서 Clop 랜섬웨어의 탐지와 확산 방지를 위한 분석을 수행하고 싶어. SMB(파일 전송 및 RCE 원격 접근 등) 관련한 탐지 로그와 랜섬웨어의 사전 징후를 포착할 수 있는 샘플로그와 의심스러운 명령어 실행 기록을 랜덤하게 생성해줘. 실제 환경과 유사한 형식으로 구성해주고, 특정 상황을 가정한 예제 데이터로써 파워쉘, WMIC, Batch 스크립트 등의 명령 실행 기록을 알 수 있는 로그 패턴을 포함해줘.

> 시트 및 csv 파일 확인

Samples : Active Directory 중심으로 온프레미스와 클라우드가 연결되어 있는 하이브리드 멀티 클라우드 환경에서 AD 관리자 정보가 유출된 상황을 가정하고 관련된 해킹 행위를 탐지하고 의심스러운 명령 실행 기록을 분석하고 싶어. 관련된 경량화된 샘플로그를 생성해줘.

> 시트 및 csv 파일 확인

Samples : 금융회사의 침해사고 준비도에는 다양한 침해사고 유형별 디지털 증거물과 로그에 대해 설명하고 있어. 생성형 AI를 통해 디지털 증거물을 랜덤하게 생성하고, 분석해보고자 해. 아래의 침해 상황과 증상을 기반으로 랜덤하게 로그를 생성하고, 파일을 다운로드 받을 수 있도록 생성해서 제시해줘.

Samples : 악성 이메일의 첨부파일(파워쉘 기반의 파일리스 악성코드)을 수신함으로써 랜섬웨어에 감염된 PC에 대한 침해상황을 가정하고, 침해상황에 대한 분석을 진행하려고 해. 관련된 샘플 로그를 생성하고, 분석의 포인트를 지정해서 알려줘.

Samples : Active Directory 가 기업의 가장 중추신경을 담당하고 있고, 모든 자산을 중앙집중적으로 관리한다고 들었어. 그리고 보안적인 측면에서 AD 취약점이 많고, AD가 감염되는 경우 전체 기업의 자산이 위험에 처한다고 들었어. AD의 주요 개념으로는 OU, Join, 도메인, LDAP/Kerberos, MAC주소, 동기화 개념에 대해서도 요약해서 알려주면 좋겠어. 우리나라는 망분리 중심으로 네트워크가 구성되어 있는데, AD가 매우 중요한 역할을 하고 있다. 전반적으로 내용을 정리해서 제시해줘. (단, 어려운 용어는 쉽게, 초등학생도 이해할 수 있는 수준으로, 영어 축약어는 full-name 으로 병기해줘.)

> Gemini에서 관련 개념 설명 확인하기.

--------------------------------------------------------------------------------

실습2. 매크로 및 파워쉘 작성 실습(간단)

> 아래의 해당하는 질문을 가지고 생성형 AI(Gemini, ChatGPT 등)을 활용하여 원하는 코드를 얻어보기

[1] 엑셀 매크로 작성

1. 엑셀을 실행시켰을 때, 파워쉘 코드(kisia\_test.ps1)가 실행되도록! (생각해보세요.)

2. 알림창 하나 띄워주세요. ('파워쉘 코드 실행 완료되었습니다.')

3. C:\test 폴더를 하나 생성해주세요.

(주의사항) 매크로는 롤백이 안됨 / 원본 파일 백업하고 실행

[2] 파워쉘 코드(kisia\_test.ps1) 작성

1. '자동으로 표준 시간대 설정'을 '끔'으로 설정하라.

2. 아래의 내용을 포함해서 하나의 텍스트 파일로 저장하고, 지정 경로(C:\kisia\_test)에 저장해주세요.

- 시스템 활성 로그온 정보

- 동작하고 있는 AV(안티 바이러스)가 있는지 확인하고, 있다면 종류와 버전

- 방화벽이 동작 중인지 상태 정보

- 프로세스 목록

3. '화면보호기 설정'을 '없음' 으로 설정하라.

> "레지스트리 변경" 은 반복적인 PC 재부팅의 이유로 실습에서 제외되었음.

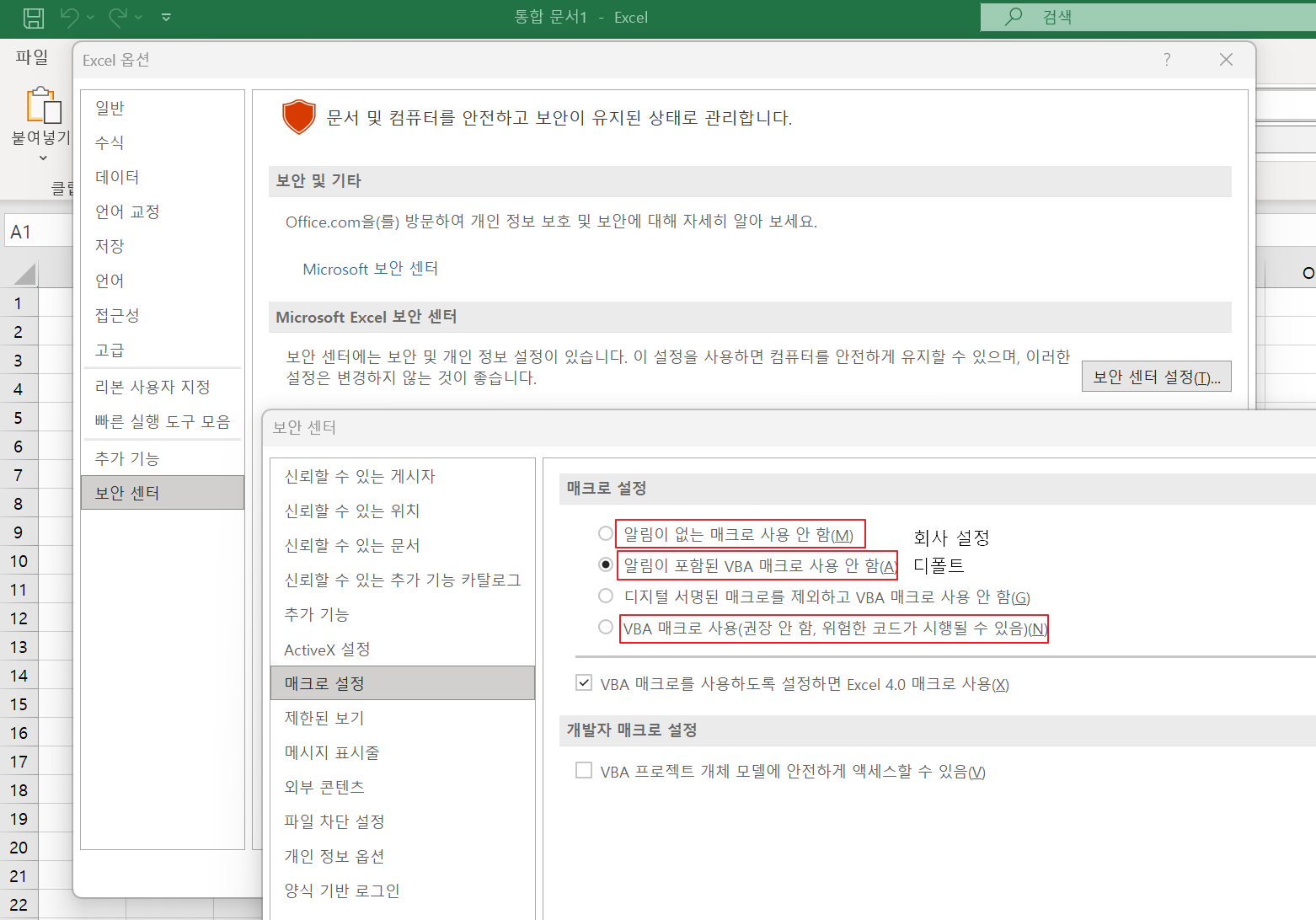
목표로 하는 Flow : 해커 이메일 -> (다운로드) 엑셀 클릭 -> 매크로 동작 -> 파워쉘 동작 -> 정해진 경로 text 생성 -> 정보 수집!

>> 쉐도우 볼륨 : 특정한 시각의 파일, 폴더 또는 특정한 볼륨의 수동 또는 자동 복사본이나 스냅샷을 저장해둔 것을 말함. 복구용 데이터.

>> 킬 스위치 : 비상 정지 장치

>> 특이점 : 차등적 암호화

>> autorun.inf 랜섬웨어 취약점



---------------------------------------------------------------------

[내일을 위한 사전 준비]

- YARA 및 코랩 세팅

1. YARA 설치 및 세팅 : 윈도우 환경, CMD 사용 (환경 변수 설정)\*\*

1. 바이너리 다운로드([Releases · VirusTotal/yara](https://github.com/virustotal/yara/releases/))

2. 전역명령어 - 환경변수 설정(C:\Program Files\yara) sysdm.cpl

3. CMD / Python : 설치 확인

4. 필요한 라이브러리 업데이트, pip 업그레이드 : 호환성, 에러

5. Yara64.exe —help

2. Colab - PE Installer / PEfile 라이브러리 활용

- .ipynb 파일 공유

- PE 구조 더미 파일 생성 / Yara 탐지 룰셋 생성 완료

---------------------------------------------------------------------

시트1.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 특징 | 정상 패턴 예시 | 비정상 패턴 예시 |
| 시간대 | 주로 업무 시간(예: 오전 9시 ~ 오후 6시)에 활동이 집중됩니다. | 특정 사용자가 업무 시간 내에 로그인하고 일반적인 작업을 수행합니다. | 심야 시간이나 주말에 비정상적인 로그인 시도 또는 활동이 발생합니다. |
| 로그인 성공/실패 | 로그인 성공률이 높고, 실패는 주로 오타로 인한 소수입니다. | 사용자가 정상적으로 계정명과 비밀번호를 입력하여 로그인합니다. | 짧은 시간 내에 여러 번의 로그인 실패가 발생하거나, 존재하지 않는 계정으로 로그인 시도가 반복됩니다. |
| 접속 IP 주소 | 주로 내부 네트워크 IP 주소 또는 VPN을 통한 정상적인 외부 IP 주소입니다. | 회사의 고정 IP 주소 대역에서 로그인 시도가 발생합니다. | 이전에 접속한 적 없는 해외 IP 주소나 의심스러운 프록시를 통한 로그인 시도가 감지됩니다. |
| 사용자 계정 활동 | 일반적인 파일 접근, 프로그램 실행, 문서 작업 등입니다. | 사용자가 할당된 그룹 정책에 따라 파일 서버에 접속하여 문서를 열람합니다. | 일반적인 업무와 무관한 시스템 파일 접근, 민감한 정보가 저장된 공유 폴더에 대한 반복적인 접근 시도입니다. |
| 명령어 실행 | 시스템 관리자가 사용하는 정상적인 관리 명령어 또는 일반 사용자가 사용하는 기본적인 명령어입니다. | whoami, ipconfig, net use 등 정보 확인 및 네트워크 설정 관련 명령어 실행입니다. | net user /add, net localgroup administrators, powershell -EncodedCommand 등 권한 상승, 계정 생성, 악성코드 다운로드 관련 의심스러운 명령어 실행입니다. mimikatz와 같은 보안 도구 실행 시도도 포함됩니다. |
| 데이터 전송/유출 | 정상적인 업무 목적의 파일 업로드/다운로드입니다. | 내부 시스템 간의 자료 공유를 위한 파일 전송입니다. | 비인가된 외부 서버로의 대량 데이터 전송, 압축된 민감 파일 전송 시도입니다. |

시트2.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 특징 | 정상 패턴 예시 | 비정상 패턴 예시 |
| SMB 활동 | 파일 공유 및 원격 접근 시도. | 부서 내 공유 폴더 접근, IT 관리자의 원격 지원 세션. | 비정상적인 IP 대역에서 다수의 SMB 세션 시도, 시스템 계정(LocalSystem)을 이용한 SMB 접근, 숨겨진 공유(C$, Admin$) 접근 시도. |
| 로그온 활동 | 주로 업무 시간 내 정상적인 사용자 로그온. | 사용자 계정의 정상적인 인터랙티브/네트워크 로그온. | 비정상적인 시간대의 로그온 시도, 존재하지 않는 계정/만료된 계정으로의 반복적인 로그온 실패 (Brute-force), RDP를 통한 비정상적인 외부 IP 로그인 시도. |
| 프로세스 생성 | 일반적인 응용 프로그램 실행, 시스템 서비스 시작. | explorer.exe, outlook.exe, chrome.exe 등 정상 프로그램 실행. | powershell.exe, cmd.exe, wmic.exe, bitsadmin.exe, certutil.exe 등을 이용한 의심스러운 스크립트/명령 실행, 알 수 없는 프로세스명 실행, vssadmin.exe를 이용한 섀도 복사본 삭제 시도. |
| 파일 시스템 활동 | 업무 관련 파일 생성, 수정, 삭제. | 문서, 스프레드시트 파일 저장 및 수정. | .clop, .onion, .crip 등 랜섬웨어 확장자를 가진 파일 생성 및 대량 암호화 시도, 특정 디렉토리(System32, Program Files) 내 비정상적인 파일 생성/수정, 공유 폴더 내 대량 암호화 파일 생성. |
| 네트워크 연결 | 정상적인 내부/외부 통신. | 웹 브라우징, 내부 서버 접속, 업데이트 서버 연결. | C2(Command & Control) 서버로 의심되는 외부 IP 주소로의 비정상적인 통신, 비표준 포트를 이용한 통신 시도. |
| 서비스 및 작업 스케줄러 | 정상적인 시스템 서비스 시작/중지, 스케줄된 작업 실행. | Windows Update 서비스 시작, 백신 업데이트 작업 실행. | 랜섬웨어 재실행 및 지속성을 위한 새 서비스 등록, 알 수 없는 스케줄된 작업 등록. |

시트3.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 특징 | 정상 패턴 예시 | 비정상 패턴 예시 |
| 로그온 활동 (온프레미스) | 주로 내부 네트워크 IP에서 업무 시간 내 관리자 계정 로그온. | IT 관리자가 내부 시스템에서 ADUC(Active Directory Users and Computers)에 접속. | 비정상적인 시간대/위치에서 관리자 계정의 로그인 시도, 짧은 시간 내 여러 실패 후 성공, 존재하지 않는 관리자 계정 이름으로의 반복 로그인 시도 (Credential Stuffing/Brute-force). |
| 로그온 활동 (클라우드/Azure AD) | 주로 지정된 국가/지역 IP에서 MFA를 통한 클라우드 관리 콘솔 로그인. | 클라우드 관리자가 한국 사무실에서 Azure Portal에 접속하여 사용자 관리. | 이전에 접속하지 않던 해외 IP에서의 클라우드 관리자 로그인 시도, MFA 우회 시도, 서비스 주체(Service Principal)를 이용한 비정상적인 로그인 활동. |
| 디렉토리 서비스 접근 (온프레미스) | AD 관리 도구(ADUC, ADSI Edit)를 사용한 일반적인 쿼리 및 변경. | 관리자가 특정 사용자 계정의 속성을 확인하거나 그룹 변경. | mimikatz와 같은 도구 사용 징후 (LSA 접근, LSASS 프로세스 접근), ntdsutil.exe를 통한 AD 데이터베이스 덤프 시도, dsquery, dsmove 등 비정상적인 대량 쿼리 또는 개체 변경. |
| 프로세스 생성 및 명령 실행 | 정상적인 시스템/AD 관리 명령어 실행. | Get-ADUser, Set-ADUser, repadmin 등 PowerShell/cmdlet 실행. | powershell -EncodedCommand, wmic process call create, certutil.exe -urlcache, bitsadmin, rundll32 등을 이용한 악성코드 다운로드/실행, Invoke-Mimikatz, Invoke-DCSync, PowerView (PowerShell Empire) 등 공격 도구 실행 징후. |
| 계정 및 권한 변경 | IT 관리자의 승인된 사용자/그룹 생성, 수정, 삭제. | 신규 입사자 계정 생성, 부서 이동에 따른 그룹 변경. | 기존 관리자 그룹에 일반 계정 추가, 높은 권한의 계정 생성, 기존 관리자 계정의 비밀번호 변경/재설정. |
| 데이터 유출 징후 | 정상적인 내부 자료 공유, 백업. | 내부 파일 서버로 데이터 이동. | 비인가된 외부 IP/클라우드 스토리지로의 대량 데이터 전송 (AD 데이터베이스, 사용자 정보), 압축 파일 생성 후 외부 전송 시도. |
| 서비스 및 작업 스케줄러 변경 | 정상적인 시스템 유지보수 스케줄. | 백업 스크립트 실행, 시스템 업데이트 스케줄링. | 지속성 유지를 위한 알 수 없는 서비스 등록, 관리자 권한으로 특정 스크립트를 주기적으로 실행하는 작업 스케줄러 등록. |