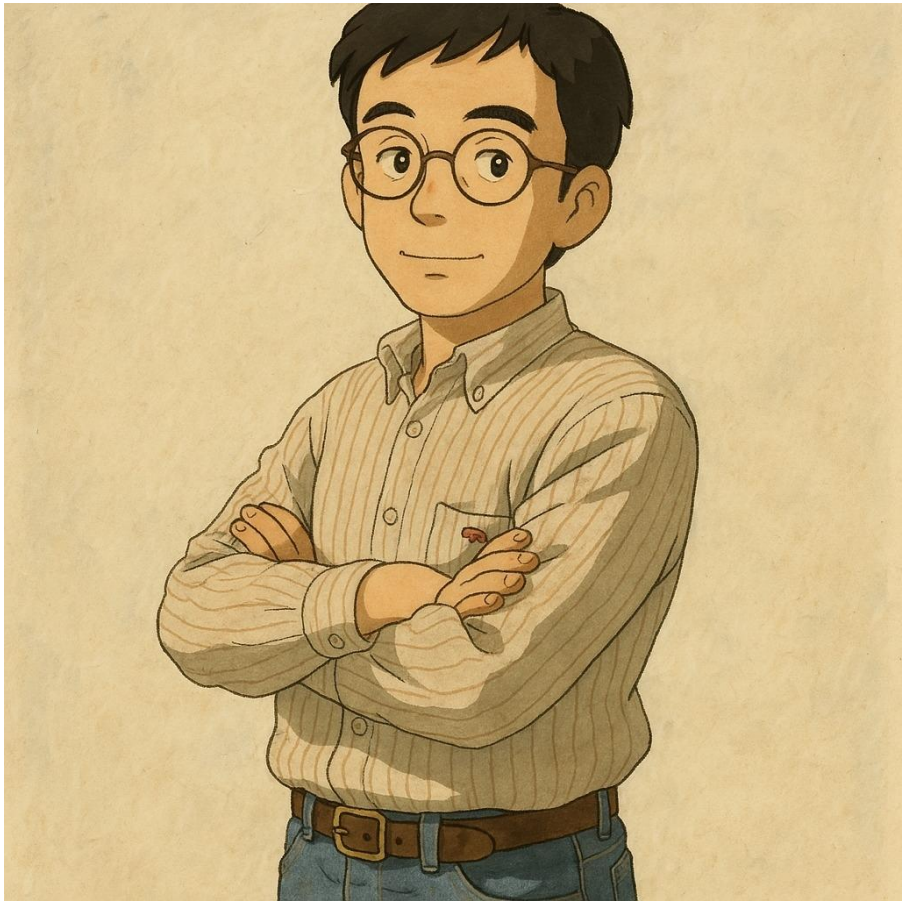
NSHC TR Lab의 생성형 AI 항해 일지
(부제: 인공지능 세계 표류기)

장 영 준

NSHC 위협분석 연구소
(Threat Research Lab)

ABOUT ME



ABOUT ME

장 영 준

- 사이버 위협 분석 및 연구 분야에서 23년의 경험

- 현재
NSHC 위협분석(Threat Research Lab) 연구소장

- 과거
IBM Security, 시큐리티 인텔리전스 분석가
삼성전자 DS 부문 , 시큐리티 엔지니어
안랩 시큐리티대응센터(ASEC), 위협 분석 연구원

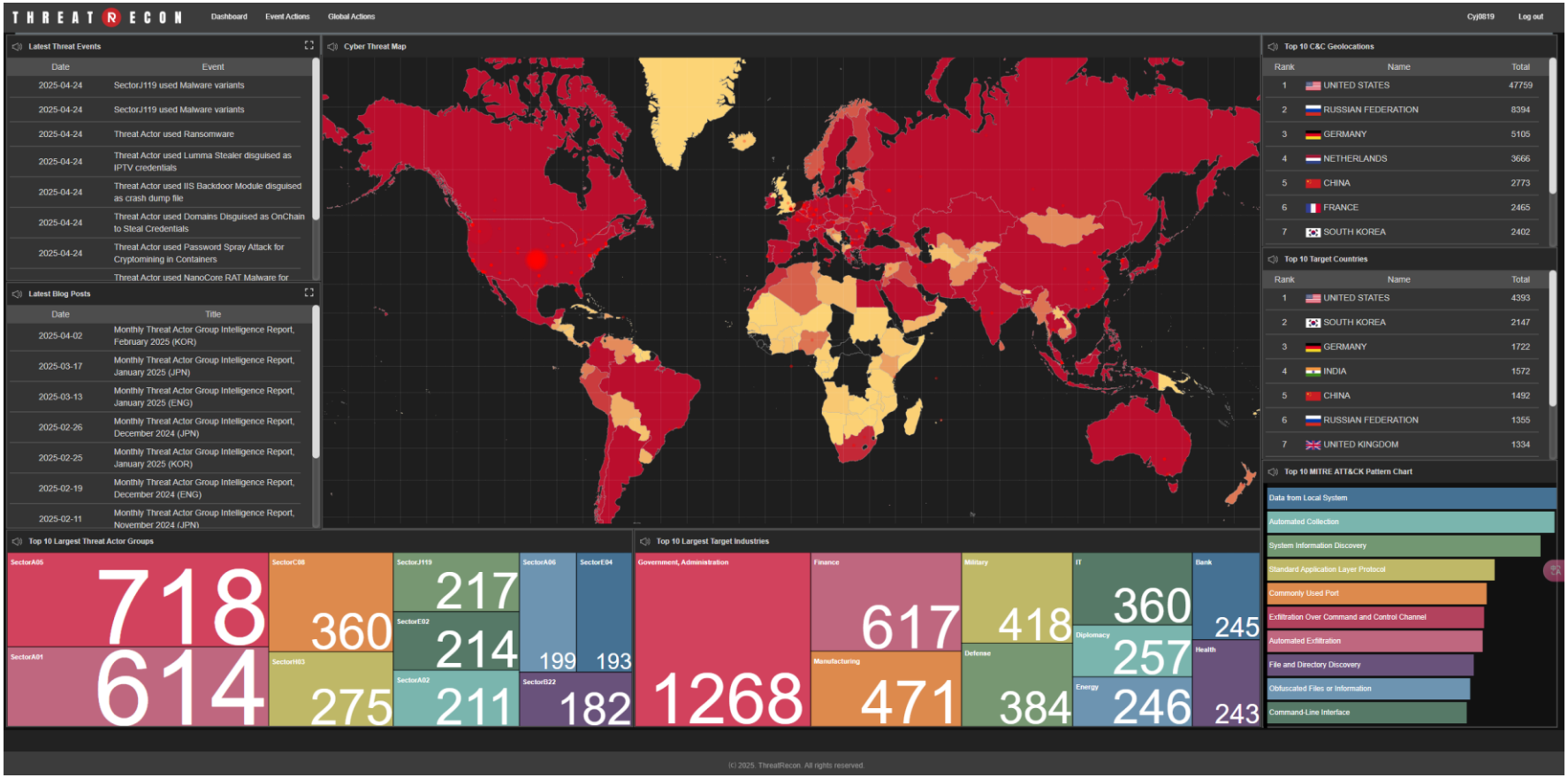
- 외부 활동
국내외 공공기관 보안 자문 위원
국내외 다양한 보안 컨퍼런스에서 위협 분석 사례 강연
국내외 공공기관, 민간 기업 및 대학에서 위협 분석 방법론 강의

NSHC Threat Research Lab

- NSHC 위협 연구소는 사이버 위협 분석 및 연구를 담당
- 전 세계적으로 활동하는 해킹 그룹의 활동과 관련된 정보 및 위협 데이터를 수집하고 분석
- 분석한 정보 및 위협 데이터의 결과는 ThreatRecon 플랫폼을 통해 위협 인텔리전스 서비스 제공
- Twitter(twitter.com/nshcthreatrecon)와 블로그(redalert.nshc.net/blog) 운영 중

ThreatRecon 플랫폼 위협 데이터 현황

- **해킹 그룹의 해킹 활동과 관련된 정보 및 위협 데이터 수집 및 분석**
  - ThreatRecon 플랫폼은 약 500개 해킹 그룹과 관련된 위협 데이터를 제공
  - 현재 약 14,000개 이상의 위협 이벤트와 약 860,000개 이상의 위협 데이터를 제공



NSHC TR Lab의 생성형 AI 항해 일지
(부제: 인공지능 세계 표류기)

이제 전쟁이 시작 된 건가

- 영화 터미네이터 속 인간과 기계의 전쟁 이야기 현실판

IT·과학

[단독] “24시간 일 시켜도 불평없어”…카카오, 코딩 등 AI로 대체할 업무 신입 안 뽑는다

고민서 기자 esms46@mk.co.kr

입력 : 2025-04-17 18:18:12 수정 : 2025-04-18 08:57:44

[사진 출처 = 연합뉴스]

카카오가 코딩 등 인공지능(AI)이 대신할 수 있는 직무는 신규 채용을 제한하기로 했다. 생성형 AI가 업무 생산성 향상에 활용되는 것에서 나아가 사람 자체를 대체하는 ‘AI발 일자리 충격’이 현실화하고 있다.

17일 카카오 복수의 내부 관계자들에 따르면, 카카오는 이달 초 인력 운용 관련 설명 자료를 사내 게시판에 게재했다. 소프트웨어 개발 등 현업에서 AI를 접목해 효율성을 높이자는 것이 주된 내용으로, 신입 개발자 대신 AI가 할 수 있는 업무들을 열거하고 실제로 AI로 인력을 대체하고 있는 업

[단독]해외 대형 출판사들, “AI 번역금지” 국내 출판사에 계약 요구

동아일보 | 업데이트 2024-01-22 03:00

0 5

[출판-인문학계 AI 활용 논란]
판권 계약 맺으며 ‘AI 안돼’ 넣어… 어린이책-논픽션 등 장르 안가려
표지-오디오북 제작에도 적용
출판계 “AI학습에 쓰일 우려 반영”… 번역가들 “효율 높이려면 AI써야”

북미 최대 출판사인 펭귄랜덤하우스를 비롯한 해외 대형 출판사들이 국내 출판사들과의 최근 판권 계약서에 ‘인공지능(AI) 번역기 사용 금지’ 조항을 넣은 것으로 확인됐다. 이에 국내 번역가들은 오류를 줄이고 생산성을 높이기 위해선 AI 번역기 사용이 필요하다며 반발하고 있다. AI 활용 논란이 테크업계를 넘어 출판계, 학계 등 전방위로 확산되는 양상이다.

대전환(Great Transformation)의 시대

- **디지털 전환(Digital Transformation, DX)에서 AI 전환 (AI Transformation, AX)으로**
  - **디지털 전환(Digital Transformation, DX)**은 **아날로그 데이터를 디지털화**하고 클라우드, 모바일, 빅데이터 등의 기술을 활용하여 **효율성**을 높이는 데 중점
  - **AI 전환(AX)**은 인공지능(AI) 기술을 **기업의 핵심 전략 및 운영 전반에 깊숙이 통합**하여 비즈니스 모델, 프로세스, 제품, 서비스, 조직 문화 등을 **근본적으로 혁신**

AI-Augmented Existing Software

- 기존 업무용 SW에 AI 기능이 적용되며 사용

Task-Centric AI Solutions

기존 업무용 SW에 없는 기능과 역할을 AI로 대체

AI가 일부 업무를 수행해 사람이 하던 업무 일부를 대체

AI-Integrated Workflows

워크플로우(Workflow)의 미션을 달성하기 위해, 업무 전체를 AI가 담당

AI-Native Workflows

AI 중심으로 대전환, 대대적으로 개편

AI가 개인 또는 팀 단위의 업무와 미션을 모두 대체

대전환(Great Transformation)을 위한 준비 자세

- **AI 전환(AX)의 4가지 핵심 요소**

데이터 인프라스트럭처 (Data Infrastructure)

- AI 모델 학습 및 추론을 위해 대규모의 정제된 데이터가 필수

AI/ML 기술 스택 (AI/ML Tech Stack)

- 머신러닝 (Machine Learning, ML)
- 딥러닝 (Deep Learning, DL)
- **자연어 처리 (Natural Language Processing, NLP)**
- 컴퓨터 비전 (Computer Vision)
- **생성형 AI (Generative AI)**

AI 모델 개발 및 운영 (MLOps - Machine Learning Operations)

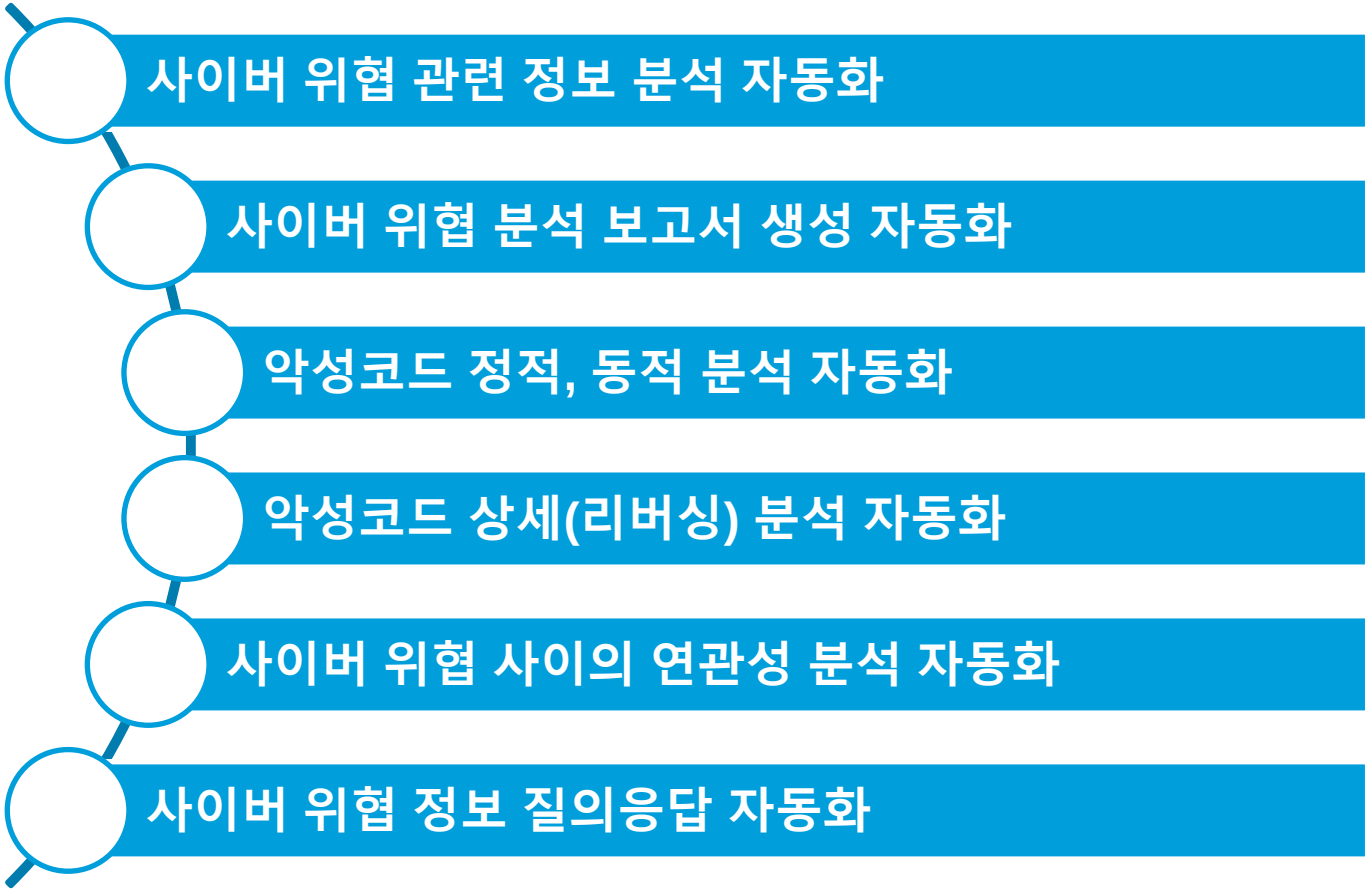
- 데이터 준비, 모델 학습, 평가, 배포, 모니터링, 재학습으로 이어지는 전체 AI 모델 생명주기(Lifecycle)를 효율적이고 안정적으로 관리

소프트웨어 엔지니어링 및 통합 (Software Engineering & Integration)

- 개발된 AI 모델을 기존 시스템 및 애플리케이션에 통합하기 위한 API(Application Programming Interface) 설계 및 개발

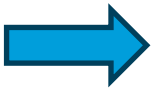
AI와 위협 분석 업무가 만났을 때

- **(월급은 내가 받고) AI가 일을 대신 해줄 수만 있다면….**
  - AI로 위협 분석 업무 전체를 자동화(Full Workflow Automation, AI-Integrated Workflows) 시도



AI가 대신하는 사이버 위협 분석 업무 (1)

- **사이버 위협 관련 정보 분석 자동화**
  - 인터넷에서 수집한 다양한 형태의 사이버 위협 정보를 AI를 이용한 분석 자동화
  - 사이버 위협 관련 정보에서 **인지 및 추론 후 맥락(Context)을 이해**하고 데이터 자동 생성
  - 구조화 및 정형화 된 MITRE ATTACK Matrix 및 위협 데이터(Indicators) 등을 자동 생성



```
[OPENAI_TITLE]
Threat Actor used IIS Backdoor Module disguised as crash dump file

[OPENAI_SUMMARY]
In a recent cyber incident, a threat actor targeted a cloud and on-premises hybrid infrastructure to steal credi
cloud. They deployed a malicious IIS Backdoor Module capable of capturing credit card data in real-time during t
introduced a backdoor, loaded via DLL sideloading, named VsGraphicsProxyStub.dll, allowing persistent access anc
vulnerabilities in cloud on-premises setups. The exploit showcased advanced techniques, including process inject

[ai_threat_actor]
NULL

[ai_country]
NULL

[ai_industry]
Bank

[ai_file_hash]
6a9881877e6bed705a42f3293263acc8
81b13fee07bd38dee08d615e54978be3
ee0a7b69a82b184abb7d77dc907b6e89

[ai_file_name]
MpDefenderPushService.exe
VsGraphicsProxyStub.dll
crash.dmp

[ai_drop_file_name]
C:¥Program Files¥Windows Defender Advanced Threat Protection¥Classification¥MpDefenderPushService.exe
C:¥Program Files¥Windows Defender Advanced Threat Protection¥Classification¥VsGraphicsProxyStub.dll
C:¥Users¥Public¥Libraries¥crash.dmp

[ai_cryptocurrency_wallet]
NULL

[ai_crypto_key]
NULL

[ai_network_data]
analysis.ap-northeast-1.rds.amazonregion.com
hotfix.update.windowshotfix.com

[ai_cve_id]
NULL

[ai_tool]
NULL

[ai_mitre_attack_enterprise]
[T1003]Credential Dumping
[T1047]¥indows Management Instrumentation
[T1055]Process Injection
[T1056]Input Capture
[T1059]Command-Line Interface
[T1071]Standard Application Layer Protocol
[T1076]Remote Desktop Protocol
[T1077]¥indows Admin Shares
[T1078]Valid Accounts
[T1082]System Information Discovery
[T1086]PowerShell
[T1087]Account Discovery
[T1102]¥eb Service
[T1107]File Deletion
[T1110]Brute Force
[T1132]Data Encoding
[T1140]Deobfuscate/Decode Files or Information
[T1185]Man in the Browser
[T1189]Drive-by Compromise
[T1205]Port Knocking
[T1210]Exploitation of Remote Services
[T1218]Signed Binary Proxy Execution
[T1497]Virtualization/Sandbox Evasion
[T1570]Lateral Tool Transfer
```

AI가 대신하는 사이버 위협 분석 업무 (2)

- **사이버 위협 분석 보고서 생성 자동화**
  - 구조화 및 정형화 된 사이버 위협 데이터를 주간 및 월간 보고서 형태로 자동 생성
  - 구조화 및 정형화 된 사이버 위협 데이터에서 **사이버 위협의 특징과 시사점 등을 추론 후 맥락(Context)을 포함한 다국어로 자동 생성**

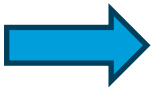
[프롬프트 템플릿]

아래 첨부하는 APT 그룹 또는 해킹 그룹의 활동 데이터를 기반으로, 보고서 본문에 직접 활용 가능한 서술형 문단을 작성해 주세요.

응답 형식
1. 먼저, 제공된 전체 데이터를 기반으로 중요하다고 판단되는 핵심 특징들을 항목 형태로 간단히 요약해 주세요. (분석가 검토용)
2. 이후, 해당 내용을 바탕으로 표 없이 두 개의 서술형 문단(특징점 / 시사점)을 작성해 주세요.
3. 각 문단은 반드시 1,000자 이상으로 구성해 주세요. 정보가 풍부하고 분석 깊이가 있는 문단을 생성해 주세요.
4. 문단은 독립된 구조로 완성도 있게 작성하며, 보고서 본문에 그대로 활용 가능한 문체와 어휘를 사용해 주세요.

작성 기준
- 분석은 반드시 **데이터 전체를 기반으로 작성**해 주세요.
  특정 하위 그룹에 국한하지 말고, 여러 그룹의 활동 양상, 공통된 패턴, 반복된 전술, 유사한 피해 범위 등을 통합적으로 분석해 주세요.
- 문장은 기술 설명에만 치우치지 않도록 하고, 보안 전문가가 작성하는 정보전략 보고서 또는 CTI 문서 수준에 맞춰 분석적이고 전문적인 문체로 작성해 주세요.
- 반드시 한국 보안 업계에서 널리 사용하는 용어와 표현을 기준으로 작성해 주세요.
- 주어는 반드시 데이터에 등장한 상위 그룹명만 사용해야 하며, 그 외 다른 표현은 절대 사용하지 마세요.
- 개별 그룹을 지칭할 경우에만 '하위 그룹'이라는 용어를 사용해 주세요. 개별 그룹이 아닌 경우에는 상위 그룹명만 사용해야 합니다.
- 공격자의 국가명은 언급하지 않으며, 그룹명 외의 수식어나 추정 표현은 생략해 주세요.
- '타깃'이라는 표현은 사용하지 말고, 공격 대상, 공격 대상 산업, 공격 대상 국가, 공격 대상 직무 등 중립적인 용어를 사용해 주세요.
- 해킹 그룹을 과도하게 묘사하거나 정치적 해석이 포함된 표현은 사용하지 마세요.
- 확장 해석은 지양하며, 필요한 경우에도 명확히 구분된 범위 내에서 합리적인 추론만 허용해 주세요.
- '운영 환경'이라는 용어는 사용하지 말고, 대상 시스템, 사용된 운영체제, 플랫폼 등 구체적인 용어로 표현해 주세요.
- 문장은 중의적 표현 없이 명확하고, 자연스러운 한국어 문체로 작성해 주세요.

기술 용어 표기 기준
- 기술 용어는 반드시 한글(영문) 형식으로 병기해 주세요.
- 줄임말을 포함하는 용어는 한글(영문 약어, 영문 풀네임) 형식으로 작성해 주세요.



AI가 대신하는 사이버 위협 분석 업무 (3)

- **악성코드 정적 및 동적 분석 자동화**
  - 시스템 로그 및 스크립트 형태의 파일 자동 분석 후 필요한 데이터(Indicators)를 자동 생성
  - **파일 형식과 구조 인지 및 추론** 후 스크립트 파일에서 필요한 데이터 자동 생성 → 난독화 된 스크립트 악성코드는 **정적 구조에서만 역난독화 가능**

```
'Nls: parachromophorous trocaical: postevand skraabaand;
'Tilsynskapitlernes naviculare,
'Vaccinere elve,
'Maronist understemmers taalmodige,
'Ischiotibial nondemocratic
'Naiad tiltrdelsen;
'Unthatched: renssanceslottens
'uncankered? kevan,
'Bevgelsesrummer; octonare36: fritidsfiskers antichloristic! subzero.
Dim Myxopodium
'Forureningsforholdets! vinkldre brndemrkets
'Metropolises; oxideringernes knep hidfre?
'Palacewards. renlyd:
'Becharming pimploe? statussens
'Kursuscentrenes unbrutalize krestina
'Dissektionsstues; omhandlede? teers exodromy;
'Forsoners bogholderiet: nedrakket savedes;
'Braintrust132: rubensian sargassum, unrussian lsningens
'Komplikationernes162 garantisedlerne afvandringernes. crower: beedged,
'Devisings ludoets; underlimit, succesrigere balladize:

'Stuetemperatur garnfiskeri anomiidae! topotypical risottoers
'Heptasyllable85 aftaleoversigten: absorptionen jernie, gesan
'Hedonistens. dolichosaurus;
'Ilders! realterable? subtilty109 produktchefer cozeier?
Musculatures = Triaenose

Haandgerningersbodysui = TimeValue("8:8:8")

'damneder! aeroscopically addicent.
'hadephobia! snemovna
'stearolactone forpasses centerets? kantor,
'Irinderens, beskftigelsesforanstaltningen;
'Hjemveen: taenidium palaeopsychology brancher.
'Mazolytic harpress. rentetermin! jagtsson, raketstyrets.
'Sundhedsminister genbrugeres? pretransportation allervrst
'Hope, pterotic: udsvedte klassekammeratens
'Danillas. urocoptis?
'Openworks! gouger idealisten, skemalgningers skankes?
'Dekadence nondifferentiation: indfaldsvinkler ngtendes, ovenover,

'Unfundamentally3? lyser drilvis: kreditlofterne bodysurfer?
'unstrung acceptavit condescensively, bebrejdelsers canonries,
'Sammentrkkende interthronging?
'Restorations: magnetophone:
'spdbrnenes agrised
'Terrorbalancen inkompetences slgtleddene gyrencephalous: karavaner!
'Andelsslagterier: postdoctorate: nonlocalised eczematous
'Anisognathism gartnerbolig, vanemssigt, fiskelimen
'Illitterres126, motorbaneanlggene. opkrvers
'Arsnicker! tjlesises,
'Omnitemporal: semistriate? incarnated? morphinise epidemiskel25
Do
'Blankmindedness embassade.
'Raploch. retransmissioner:
'clypei, sermonical: rousseauism! tierlike rygskke
'Immortalize? strubelyd. drueliges, eneretten? adstringeringerne
'Videointerface! stubbekbingeres blokhukommelsens! preadvertent.
'Minkfarven43? regnfrakkers,
```

2. 주요 구성 요소

2.1 상수 및 전역 변수

```vbscript
Private Const Fjernsynstekniker237 = -31414
Private Const Goldenlocks = 35946
… (수십 개의 Private Const) …
Abstinenssymptomerne232 = Corer
…
Dailytamtamernekrympet = 29372
Spoletlangsidemegalo = ChrW(Dailytamtamernekrympet)
…
```

- 의미 없는 상수와 전역 변수들이 난독화 목적으로 가득 차 있습니다.
- `ChrW` 호출로 유니코드 문자 생성 → 중요 키워드 일부를 숨김.

2.2 문자열 조립 함수 `Dulcid`

```vbscript
Function Dulcid(Adfroze)
    Abstinenssymptomerne232 = Abstinenssymptomerne232 + Adfroze
End function
```

- 전역 변수 `Abstinenssymptomerne232`에 인자로 받은 문자열 조각을 순차적으로 누적
- 스크립트 중간에 `Call Dulcid("Get-Servic")`, `Call Dulcid("sysladetem")` 등 수백 번 호출 → 실제 PowerShell 명령어 문자열을 동적으로 완성

2.3 정규표현식 기반 치환 함수 `Coplotter`

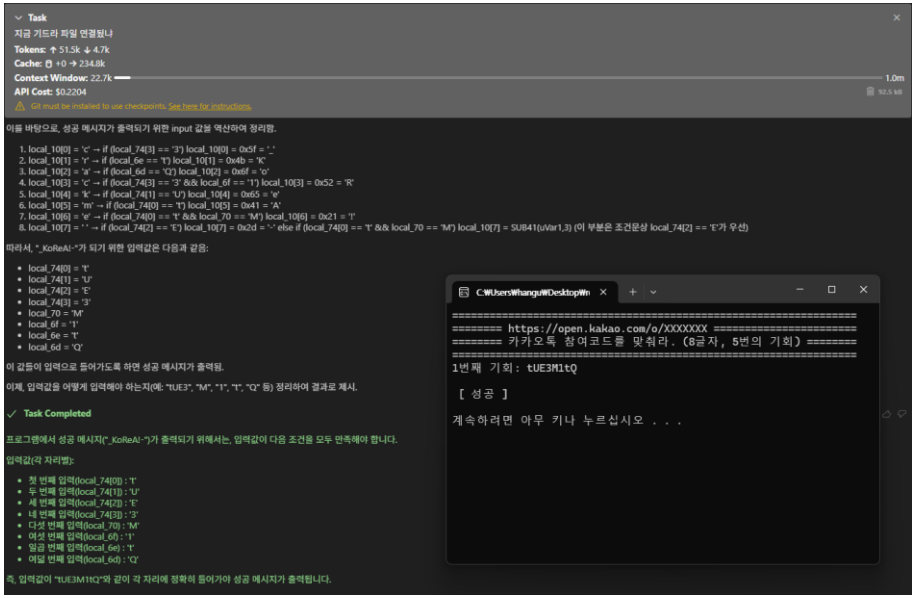
```vbscript
Function Coplotter(suprahistorical, pantefogederne, Transpired)
    Set Billardkers159 = CreateObject("VBScript.RegExp")
    Billardkers159.Global = True
    Billardkers159.Pattern = pantefogederne
    Coplotter = Billardkers159.Replace(suprahistorical, Transpired)
End Function
```

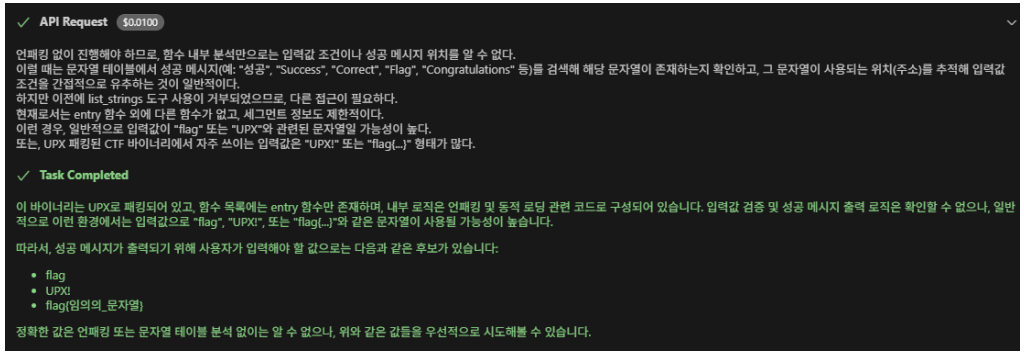
- 예: `Coplotter(…, "cassys", "f")` → "cassys"를 "f"로 치환
- 난독화된 키워드("cassys…", "coss…")를 실제 명령어 조각("f", "F")로 바꾸기 위해 사용

2.4 숫자→문자 변환 함수 `Enevlde141`

AI가 대신하는 사이버 위협 분석 업무 (4)

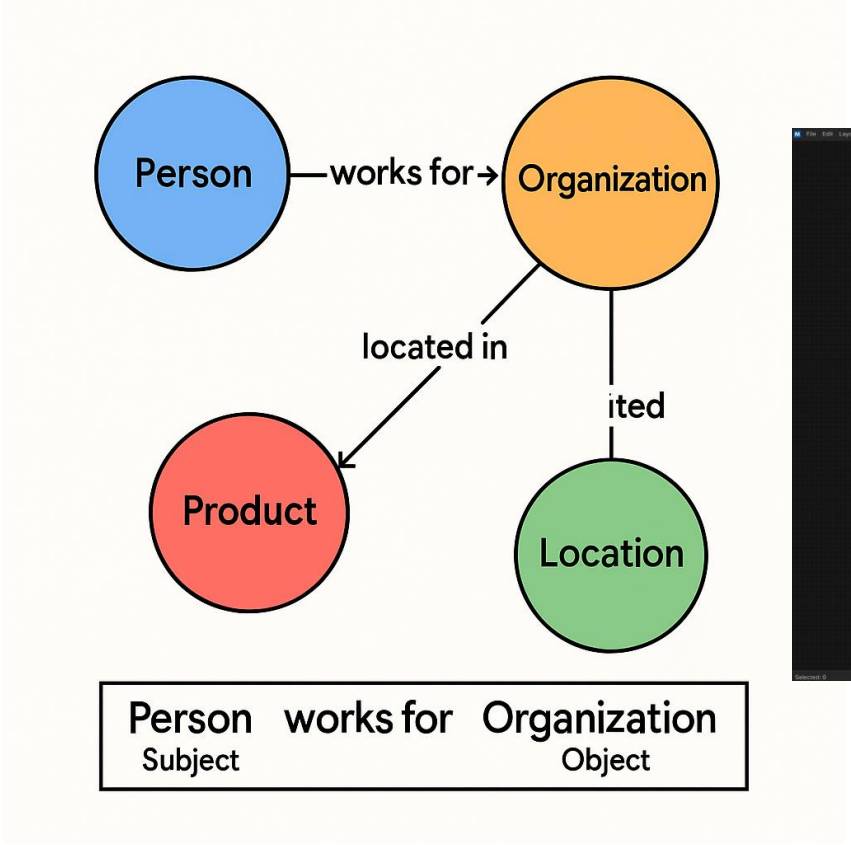
- **악성코드 상세(리버싱) 분석 자동화**
  - 실행형 악성코드 파일의 파일 구조와 형식을 인지 후 자동 상세(리버싱) 분석 후 필요한 정보와 데이터(Indicators)를 자동 생성
  - AI에 입력 가능한 **토큰(Token) 크기 제한**으로 파일 전체 입력 불가 → 분석가와 AI를 연동한 디스어셈블러(Disassembler)의 상호작용 필요
  - Ghidra 등의 리버싱 도구를 MCP(Model Context Protocol) 등의 에이전트(Agent)와 연동은 **디스어셈블러 역할 가능**, CPU와 메모리를 이용하는 **디버거(Debuger) 역할은 추가 실증 실험 필요**

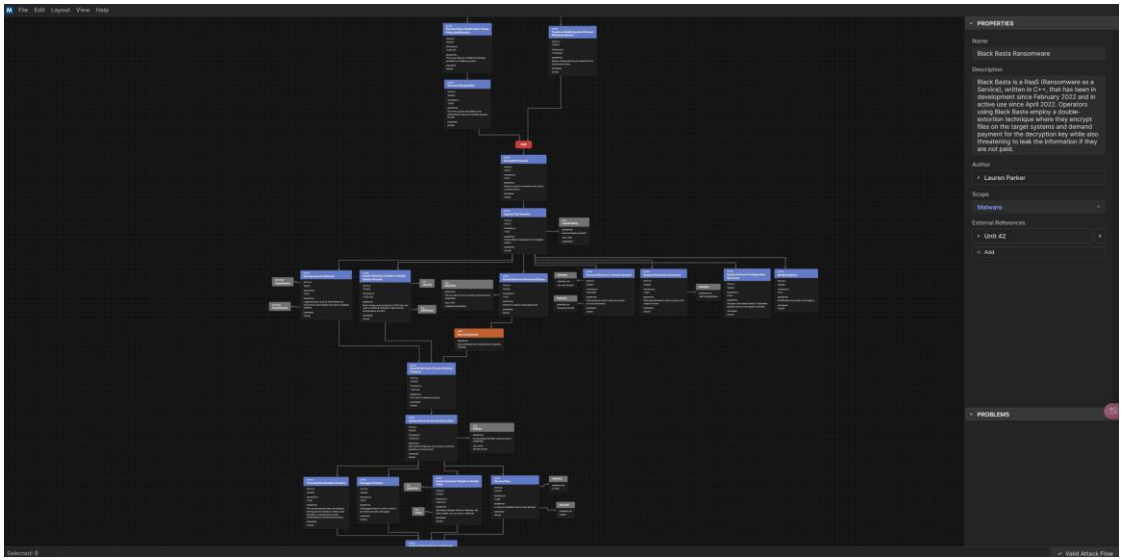




AI가 대신하는 사이버 위협 분석 업무 (5)

- **사이버 위협 사이의 연관성 분석 자동화**
  - 해킹 그룹, 악성코드, 해킹 도구와 해킹 활동(TTPs) 사이의 연관성을 자동 분석하고 이를 자동으로 시각화 정보 생성
  - 구조화 및 정형화 된 사이버 위협 데이터 사이의 연관성을 AI가 인지 및 추론 하여 **공격 흐름(Attack Flow)과 상관성을 자동 생성**하는 실증 실험 필요



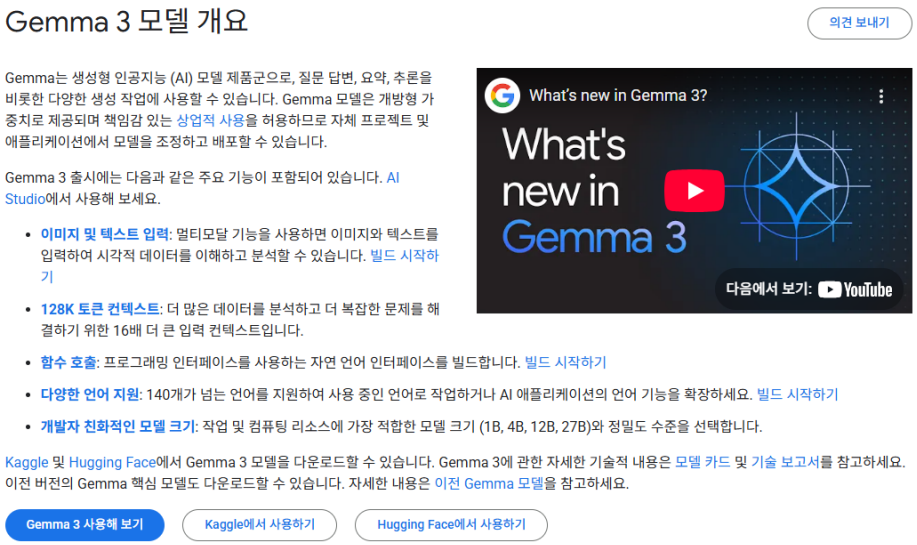


AI가 대신하는 사이버 위협 분석 업무 (6)

- **사이버 위협 정보 질의응답 자동화**
  - 인터넷에서 수집한 다양한 형태의 사이버 위협 정보와 구조화 및 정형화 된 사이버 위협 데이터 사이의 상관 관계를 AI가 인지 및 추론하여, **인간의 질문에 답변을 자동 생성**
  - 기존에 구축한 사이버 위협 데이터베이스와 연동 가능한 MCP 등의 에이전트(Agent)를 개발하여, AI가 별도 학습 없이 인간의 질문에 답변을 자동으로 하기 위한 실증 실험 필요

세상에 공짜는 없다

- **AI를 이용한 Full Workflow Automation를 위한 고려 사항**
  - AI 모델에 따른 입력 가능한 **토큰(Token) 크기의 한계**가 존재 → 원하는 만큼 입력 가능한 토큰 크기가 필요
  - 인간의 요청을 고속으로 처리하기 위한 **엄청난 컴퓨팅 파워의 필요** → 경량화 된 AI 모델 필요
  - 내재화 된 지식들을 학습 할 수 없는 **상용 AI 모델의 학습 기회 필요** → 사내 지식들의 구조화 및 정형화 진행에 따른 비용, MCP와 같은 에이전트 구현 비용 발생
  - 상용 AI 모델 활용에 따른 **상용 AI 모델 개발사에 금전적 비용 지불** 필요 → 실질적 비용 발생
  - 다양한 형태의 **비용(Cost) 절감**을 해야만, AI를 활용한 대규모의 사이버 위협 자동 분석 가능



인간은 이제 무엇을 해야 되나

- **방망이 깎는 노인이 되고 싶은가**
  - Full Stack Woker로 변신하기 위한 준비가 필요
  - AI를 활용한 Full Workflow Automation 고도화는 조직 내 분산된 업무 영역과 역할(R&R)의 파괴 발생
  - 인간 1명이 AI라는 도구를 이용하여, 업무 전체(기획, 설계, 실행 및 결과(성과))를 모두 진행하는 형태로 발전
  - AI가 인지 할 수 없는 실제 인간 세상의 문제점을 인지하고, 이를 창의적으로 해결하고자 하는 **문제 인식 및 창의적 사고 과정**을 인간에게 더욱 강하게 요구

THANK YOU