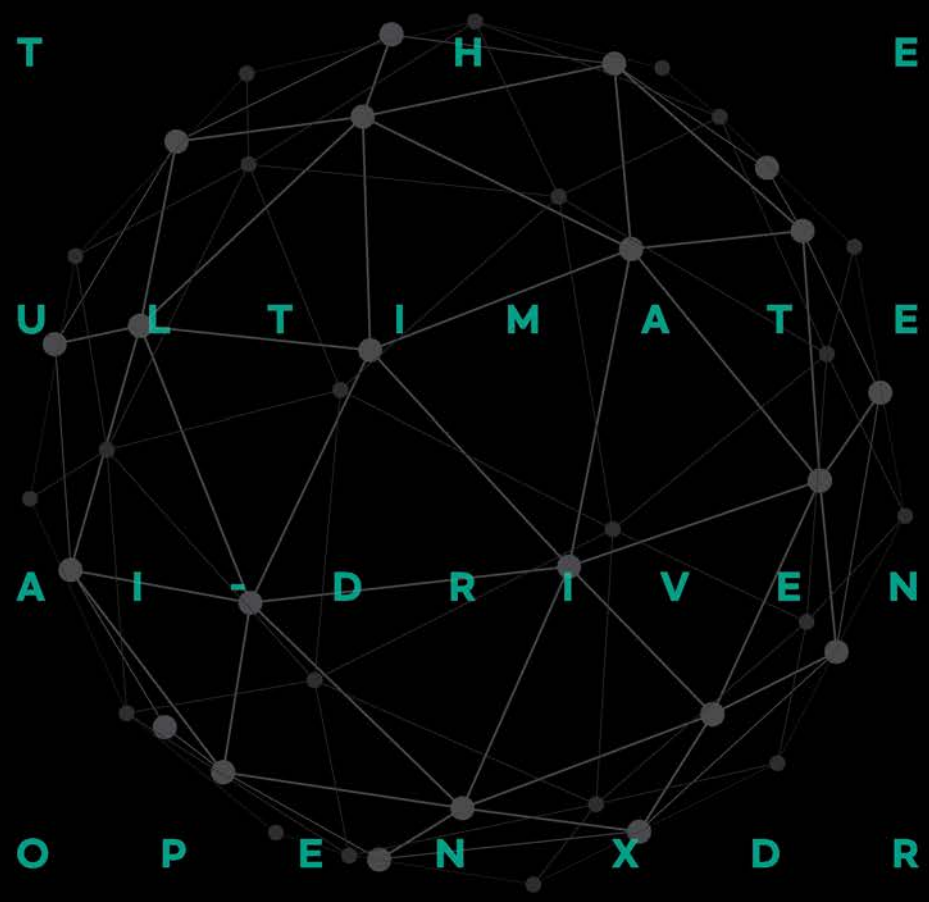
IGLOO

2025년 1월호

IGLOO PLUS+



이달의 뉴스
Green spotLight
보안101
칼럼
Green life
이달의 위협 인사이트
세미나 정보
독자 참여 코너

사이버 보안도 지피지기 백전불태!
생성형 AI란 무엇인가요?
AI: "마음을 드려요"
생성형 AI시대, 이제는 보안이다.
신의 물방울, 와인을 위한 첫걸음

Green Note.

새로 만날 세계

그린님들, 바야흐로 2025년이 되었습니다. 새로운 세계에 발맞춰 나아가고자, 이글루플러스도 변화를 꾀했습니다. 작년 여름 530분이 참여하셨던 설문 조사 기억하시나요? 어떤 코너가 좋은 지 어떤 부분이 개선되면 더 좋을지 애정 넘치는 답변을 보내주셨었는데요. 그 내용을 충실히 반영하여 다음과 같이 이글루플러스를 개편했습니다.

먼저, 폭넓은 세대와 배경의 그린님들이 공감하실 수 있는 콘텐츠 비중을 확대했습니다. 많이 들어봤지만 정확히는 알지 못했던 여러 용어 있지 않나요? 그 개념을 쉽게 풀어보는 '보안 101' 코너를 마련했습니다. 일에 열중하다 보면 머리를 식히고 싶을 때도 있죠, 그래서 문학·음악·미술·스포츠 등 폭넓은 분야의 이야기를 다루는 'Green Life' 코너도 새롭게 꾸며보았습니다.

또한, 이글루코퍼레이션의 문화와 강점을 알릴 수 있는 콘텐츠를 추가했습니다. 설문 조사 결과를 보니, 생각보다 많은 분들이 이글루코퍼레이션 뉴스를 궁금해하고 계셨답니다. 그래서 '이달의 뉴스'에 이글루 소식도 추가했습니다. 더불어 운동, 유적지 탐방, 캠핑, 보드게임, 공연 관람 등 다양한 주제의 이글루코퍼레이션 동호회를 소개하는 'Green 人터뷰' 코너도 마련했습니다.

마지막으로, 그린님들이 참여하실 수 있는 참여형 코너도 확장했습니다. 작년에는 '베스트 프랙티스' 코너를 통해, 대한항공의 보안 업무 혁신 성공 사례를 소개했었는데요. 올해는 더 많은 그린님들이 인사이트를 공유하실 수 있게 수시 안내드릴 계획입니다. 또한, 이달의 주제와 관련된 퀴즈를 푸는 '독자 참여' 코너도 구성했습니다. 추첨을 통해 알찬 선물드리니, 꼭 함께 해 주세요!

자, 우리 함께 새로운 이글루플러스 만나볼까요? 이글루플러스의 한 페이지가 될 우리 그린님들, 올해도 함께 달려봐요!

CONTENTS.

01
이달의 뉴스

- 이달의 주요 뉴스
- 이글루코퍼레이션 소식

02
Green spotLight

사이버 보안도
지피지기 백전불태!

03
보안 101

생성형 AI란
무엇인가요?

04
칼럼

- AI: "마음을 드려요"
- 생성형 AI시대, 이제는 보안이다.
- [외부 법률 기고]
  국내 AI 기본법 제정안 국회 통과

05
Green life

신의 물방울,
와인을 위한 첫걸음

06
이달의 위협 인사이트

- 월간 보안 위협 동향 및 분석
- 공격 위협 상세 분석 결과
- 침해지표(IOC)
- 탐지 정책

07
세미나 정보

08
독자 참여 코너

고객의 어려움을 해결하는 조력자,
새로운 비즈니스 기회를 제시하는 길잡이

이글루코퍼레이션은 월간지 '이글루플러스'를 통해,
최신 트렌드를 반영한 테크·라이프 콘텐츠를 소개하고 있습니다.

이글루플러스 2025년 1월호: Theme

Generative AI

2025년의 첫걸음을 내딛는 이글루 플러스 1월호.
이번 달 우리는 '생성형 AI(Generative AI)'라는 주제로
새로운 가능성의 문을 엽니다.
창조와 혁신의 중심에 선 생성형 AI가
일상과 산업에 불어넣는 변화의 바람을 느껴보세요.
새해의 설렘 속에서, 기술이 만들어갈 미래를 함께 그려봅니다.

01
이달의 뉴스

매월 주목할 만한 주요 뉴스를 선별합니다.

이번 달, 전 세계 곳곳에서는 어떤 일들이 있었을까요?

보안, IT, AI, 클라우드 등 폭넓은 주제의 주요 뉴스를 선별하여 제공하고, 이글루코퍼레이션의 사내 소식도 함께 소개합니다.

이달의 뉴스

전략사업부 마케팅팀 한가연

#AI보안 #챗GPT서치 #AI동맹외교 #AI디바이드 #비AI스타트업의위기
#초개인화AI공격기승 #미국통신사해킹사건 #북한암호화폐탈취규모최대치기록

1. 검색 시장 노리는 오픈AI, '챗GPT 서치' 무료 개방

· 오픈AI가 자사의 AI 기반 웹 검색 기능인 '챗GPT 서치'를 출시한 지 한 달 반 만에 무료로 개방함.
· 이 기능은 'GPT-4o' 모델을 기반으로 사용자가 검색 질문을 입력하면 대화형 답변과 함께 활용한 원 출처를 제공하는 서비스임.
· 이번 조치로 오픈AI는 온라인 검색 시장의 강자인 구글과 본격적으로 경쟁에 나설 것으로 예상됨.
· 미국 투자은행 에버코어 조사에 따르면 '챗GPT'는 미국 내 사용자 규모가 빠르게 늘어 미국 검색시장 점유율 5%를 기록했으며, 이는 마이크로소프트 빙의 점유율 4%를 넘어서는 비약적 성장세임.
· 또한 시장조사기업 가트너는 AI 에이전트 기반의 검색 방식이 자리를 잡으면서 2026년까지 구글 등 기존 검색 엔진 사용량이 25% 감소할 것이라고 예측한 바 있음.

2. CES 2025, AI 몰입 시대에 '보안'이 최우선

· 올해 CES의 핵심 키워드는 '몰입(Dive in)'으로, AI를 중심으로 한 기술의 폭발적 성장과 함께 보안의 중요성이 더욱 강조됨.
· 삼성전자 한종희 부회장은 "'홈 AI' 구현 시 보안을 최우선으로 고려하고 있다"고 강조하며, 안전한 데이터 운영의 중요성을 언급함.
· LG전자도 기존 보안 프로세스에 더해 개인정보 데이터로 'LG 쉴드'를 추가 적용해 보안을 강조했으며, SK 그룹 공동 전시관은 보안을 핵심 테마 중 하나로 선정함.
· 다수의 기업들이 최신 AI 제품 소개에 앞서 사이버보안 기술력을 강조한 것은 신기술에 대한 거부감을 완화하는 동시에, AI로의 완전 몰입을 위해 안전한 데이터 운영이 필수적임을 의미함.
· 또한 CES 최고 혁신상 19개 중 7개를 국내 기업이 수상했으며, 이 중 3개가 보안 관련 제품으로, 보안 기술이 주요 분야로 자리 잡고 있음을 보여줌.

3. 푸틴 새해 첫날부터 "중국과 AI 분야 협력하라" 지시

· 푸틴 러시아 대통령이 새해 첫날인 1일, 중국과의 AI 분야 협력 강화 지시를 내림.
· 이번 지시는 지난달 11일 모스크바 스베르방크 콘퍼런스에서 브릭스(BRICS) 회원국을 비롯한 여타 국가들과 함께 AI 개발에 나서겠다고 밝힌 지 3주 만에 나온 것으로, 푸틴 대통령은 당시 연설에서 'AI 동맹 네트워크'를 새롭게 구축하겠다고 선언한 바 있음.
· 푸틴 대통령의 AI 동맹 구축 선언과 이어진 중국과의 협력 지시는 타국과의 협력을 통해 AI 개발의 돌파구를 찾고 나아가 미국의 AI 지배력에 도전하려는 의도로 분석됨.
· 푸틴 대통령은 수년 전부터 러시아를 AI 강국으로 만들겠다는 야심을 드러냈지만, 우크라이나 전쟁으로 인해 AI 전문 인재들이 떠나고 서방의 제재로 첨단 AI 기술 도입이 제한되면서 어려움을 겪고 있는 상황임.

4. 개인·기업·국가 덮친 `AI 디바이드`

· 오픈AI가 월 200달러(약 28만 원)의 '챗GPT 프로'를 출시하는 등 유료 AI 서비스가 잇따라 등장하며 AI에 투자하는 개인·기업과 그렇지 못한 이들 간의 격차, 즉 'AI 디바이드'가 점차 현실화되고 있음.
· 미국 시장조사업체 백링코(Backlinko)에 따르면 챗GPT 유료 버전 구독자는 약 1,000만 명으로, 전 세계 챗GPT 주간 활성 사용자 2억 명 중 약 5%만이 고급 AI 기능을 활용하고 있는 셈임.
· 더 나아가 미국과 중국이 AI 개발에 수조 원을 투자하는 반면, 재정적 여유가 부족한 국가들은 경쟁에서 크게 뒤처지고 있어 국가 간 'AI 디바이드'도 심화될 전망임.
· 유엔은 현재 AI 역량이 소수의 강력한 기업과 그보다 더 적은 국가에 집중되어 있어 국가 간 불평등 및 개발도상국의 디지털 소외를 악화시킬 우려가 있다고 지적하며 AI 접근성 개선의 필요를 강조함.

5. AI 중심 투자 확대 속 한국 비 AI 스타트업 위기

· 지난해 글로벌 벤처 시장은 AI 열풍으로 활력을 되찾으며, AI 중심의 신규 투자 확대를 통해 성장세를 회복하고 있음.
· 특히 미국은 AI를 포함한 다양한 산업에 균형 있는 투자를 이어가며 260조 원 이상의 자금을 유치, 전 세계 투자액의 57%를 차지함.
· 반면, 한국은 AI를 제외한 스타트업 시장에서 투자 감소가 이어지며 AI 중심의 투자 쏠림 현상이 두드러짐.
· 국내 AI 스타트업 투자 금액은 9,666억 원으로 전년 대비 41% 증가했으나, 비 AI 분야는 50% 가까이 감소함. 특히, 일부 산업은 99% 급감하는 등 심각한 양극화가 나타남.
· 스타트업 관계자들은 최근 국내에서 AI 외 스타트업에 대한 투자가 얼어붙으면서, 생태계의 지속 가능성이 위협받고 있다고 우려하고 있음.

6. AI로 '초개인화' 피싱 사기 극성

· 파이낸셜타임스(FT) 등 외신에 따르면, 특정 글로벌 기업 임원을 겨냥한 AI 기반 이메일 피싱 사기가 급증하고 있음.
· 영국 보험사 비즐리와 이커머스 그룹 이베이 등 주요 기업 임원들은 최근 AI를 활용한 이메일 피싱 방식이 한층 정교해지면서 이를 추적하는 데 어려움이 커지고 있다고 강조함.
· 사이버 공격자들은 AI 기술을 활용해 기업 임원의 온라인 프로필에서 학력, 기업 분야, 취미 등 다양한 정보를 수집·분석한 뒤, 이를 바탕으로 초개인화된 피싱 공격을 감행함.
· 특히, AI가 개인정보를 대규모로 스크래핑하여 정교하게 표적화된 공격에 활용하면서, AI 기반 피싱은 매우 개인화된 양상을 띠게 됨. 이와 동시에, AI로 빠르게 생성된 수천 개의 메시지를 최신 추적기로도 모두 탐지하기 어렵다는 문제도 지적됨.

7. 미국 주요 통신사, 중국 해커 조직에 해킹 공격 당해

· 미국 주요 통신사들이 중국과 연계된 해커 조직 '솔트 타이푼(Salt Typhoon)'의 해킹 공격을 받음.
· 미국 월스트리트저널(WSJ)은 지난해 12월 기준 총 9곳이 해킹 피해를 입었으며, 추가 조사에 따라 피해 규모가 커질 수 있다고 전함.
· 해커들은 포티넷과 시스코 시스템즈의 네트워크 장비 보안 취약점을 악용해 네트워크에 침투, 수개월간 통신 인프라에 접근하며 정보를 탈취한 것으로 보고됨.
· 이 과정에서 수백만 명의 통화 기록, 암호화되지 않은 텍스트, 일부 오디오 데이터 등이 유출되었을 가능성이 제기됨.
· 미국 정부는 이를 중대 사건으로 규정하고 FBI 등과 함께 조사를 시작했으며, 중국이 탈취 데이터를 AI 분석에 활용할 가능성을 우려함.
· 한편, 중국은 해킹 활동 관련 주장을 부인하며 모든 형태의 사이버 공격에 반대한다고 밝힘.

8. 北, 2024년 암호화폐 탈취 1.9조 원, 전 세계 피해액 60% 차지

· 북한이 올해 암호화폐 플랫폼에서 절취한 규모는 13억 달러(약 1조 9,000억 원)로, 역대 최대치를 기록함.
· 블록체인 데이터 분석기업 체이널리시스(Chainalysis)에 따르면, 북한 해커들은 47건의 해킹 공격을 통해 전 세계 피해액 22억 달러 중 61%를 차지함.
· 주요 사례로는 5월 일본 거래소 DMM 비트코인 해킹 사건이 있으며, 이로 인해 약 5,032억 원 상당의 비트코인이 탈취됨.
· 체이널리시스는 북한의 해킹이 점점 더 빈번하고 정교해지고 있다며, 민관 협력과 실시간 보안, 블록체인 추적 기술 강화가 필요하다고 강조함.

이글루 소식

전략사업부 마케팅팀 한가연

01

보안관제 특화 공격 표면 관리 서비스 'I² AXIS asm' 출시

이글루코퍼레이션이 보안관제 특화 공격 표면 관리 서비스 '아이스퀘어 액시스 에이에스엠(I² AXIS asm)'을 출시했다. I² AXIS asm은 외부에 노출된 조직의 IT 자산 정보와 이글루코퍼레이션 고유의 긴급 대응 등급(IEAC, IGLOO Emergency Action Classification) 정보를 결합하여 제공하는 보안관제 특화 공격 표면 관리 서비스이다. I² AXIS asm 도입 조직은 일원화된 IT 자산 식별-대응-관리 프로세스를 토대로 공격 표면 취약성 정보 및 공격 이벤트 내역을 실시간 확인 및 조치함으로써, 보안 운영의 안정성과 공격 대응 효율성을 극대화할 수 있다. 이글루코퍼레이션은 I² AXIS asm 런칭을 시작으로 보안관제 가시성 및 통찰력 확장을 위한 보안관제 포털 서비스 'I² AXIS' 라인업을 확장하며 사업 다각화에 속도를 붙일 방침이다.

02

과기부-KISA 'AI 보안 사업화 우수기업' 선정

이글루코퍼레이션이 과학기술정보통신부와 한국인터넷진흥원(KISA)이 주관한 2024년 AI 보안 사업화 우수기업으로 선정됐다. 이글루코퍼레이션은 고유의 기술력이 집약된 하이브리드(분류형·설명형·생성형) AI 탐지모델 '에어(AiR, AI Road)'에 토종 AI 반도체 기업 리벨리온의 AI 연산 특화 '신경망처리장치(NPU)'를 결합해 폐쇄된 환경에서도 사용가능한 '구축형 어플라이언스 방식의 AI 보안 어시스턴트 시스템'을 개발했다. 이를 통해 데이터 유출 위험 없이 AI를 안전하게 활용할 수 있는 안정성과 높은 생산성을 확보하며, 독자적인 AI 기술력을 다시 한번 입증했다. 이글루코퍼레이션은 서비스 모델 다양화를 통해 국내외 기업·기관을 대상으로 AiR 공급 확대에 박차를 가할 계획이다.

03

'시큐리티 어워드 코리아 2024' 사이버보안부문 산업선도상 수상

이글루코퍼레이션이 시큐리티어워드코리아위원회가 주최한 '시큐리티어워드 코리아 2024'에서 사이버보안부문 '산업선도상'을 수상했다. 이 상은 정보보안 시장에서 뛰어난 공로와 성과를 보인 기업에 수여되는 상으로, 이글루코퍼레이션의 시장 리더십을 인정받은 결과다. 이글루코퍼레이션은 인공지능(AI), 클라우드 등 첨단 기술을 기반으로 국내외 주요 기관 및 기업에 보안 솔루션과 서비스를 제공하며, 정보보안 시장의 지속적인 성장을 이끌어왔다. 특히 이글루코퍼레이션이 개발한 혁신적인 보안 기술과 정보보호 산업에 기여한 공로가 높게 평가되어 이번 수상의 영예를 안았다.

04

'AAA2024' AI 윤리상 수상

이글루코퍼레이션이 '2024 아시아AI대상(AAA)'에서 'AI 윤리상'을 수상했다. 이번 수상은 AI 기술 발전과 함께 윤리적 기준을 고려한 AI 솔루션 개발에 앞장선 공로를 인정받은 결과로, 기술이 지닌 잠재력을 책임감 있게 활용한 이글루코퍼레이션의 노력이 주목받았다. 이글루코퍼레이션은 AI를 악용한 공격엔 AI 기반 보안 기술로 맞서야 한다고 판단해, 지난해 7월 AI 보안 어시스턴트 '에어(AiR·AI Road)'를 개발·출시했다. 해당 솔루션은 AI가 어떤 기준으로 특정 행위를 이상 또는 정상으로 탐지했는지 알려주며, 알고리즘이나 기존의 패턴 기반 데이터를 통해 AI 예측 결과를 설명한다. AI의 신뢰성과 이해도를 크게 높이고 사용자에게 투명하고 신뢰할 수 있는 보안 경험을 제공한다는 점에서 높은 평가를 받았다.

05

한국인공지능산업협회(AIIA) 주관 '2025 이머징 AI+X 톱100' 기업 선정

이글루코퍼레이션이 한국인공지능산업협회(AIIA)에서 주관하는 '2025 이머징 AI+X 톱 100(Emerging AI+X TOP 100)'에 선정됐다. 올해로 5회째를 맞는 이머징 AI+X는 AI 기술과 산업(X) 간 융합으로 우리나라 AI 산업 미래 혁신을 선도할 기업을 의미한다. 이글루코퍼레이션은 AI 보안 기술 개발에서 보여준 혁신성과 기술적 우수성을 인정받아 '사이버 보안' 분야 선도 기업으로 최종 선발되었다.

02
Green spotLight

지금 우리가
주목해야 할 IT 이야기

하루가 다르게 변화하고, 발전하는 어지러운 사이버 세상.
그중에서 지금 우리가 주목해야 할 가장 뜨거운 이야기는 무엇일까요?

이글루코퍼레이션은 모두가 알아 가야 할, 궁금했었던,
그리고 뜨거웠던 그 이야기에 집중합니다.

주목해 주세요,

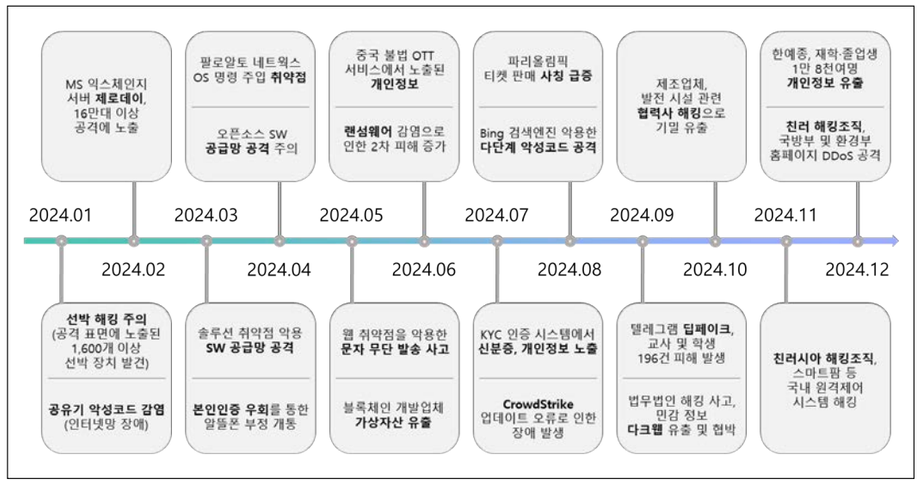
이 달의 IT 이야기를 들려드립니다.

사이버 보안도 지피지기 백전불태!

전략사업부 전략기획팀 김승진

01 '24년 사이버 위협 타임라인

어느덧 한 해가 지나 2025년이 찾아왔다. 그리고 우리는 그동안의 시간을 돌아보며 다가올 미래를 준비해야 할 시점에 서 있다. 한국인터넷진흥원(이하 KISA)을 비롯한 국내 보안 전문가들은 지난 '23년 △소프트웨어(SW) 공급망 위협 △생성형 AI(Generative AI) 악용 △융복합 환경에서의 보안 위협 △정치·사회적 이슈를 노린 공격 등을 '24년의 주요 사이버 위협으로 전망했다. 이 중 많은 예측이 현실로 나타났으며, 이를 통해 드러난 위협 상황과 파급력은 여러 과제를 남겼다.



[그림 1-1] '24년도 주요 사이버 보안 사고 타임라인 (출처: 이글루코퍼레이션)

1) 소프트웨어(SW) 공급망 위협

지난해 가장 주목받은 사이버 위협 중 하나는 '소프트웨어(SW) 공급망 공격'이다. 해당 유형의 공격은 서드파티(3rd Party)와 협력업체를 통해 주로 이루어지며, 피해 기업은 공격 사실조차 인지하지 못한 채 심각한 피해를 입게 된다. 예를 들어 △2월, 악성 PyPI 패키지 유포 △4월, 국내 게임사 대상 공격 △8월, 백신 소프트웨어 취약점을 악용한 악성코드 배포 등 다양한 침해사고가 발생했다.

특히, 오픈소스(Open Source) 환경을 겨냥한 '지능형 지속 위협(Advanced Persistent Threat, 이하 APT) 공격이 감행되며 개발자와 소프트웨어 사용자 모두를 위협했다. 공격자는 소프트웨어 업데이트를 가장해 악성코드를 유포하거나 SaaS 환경에 침투해 광범위한 피해를 유발했고, 단순한 기술적 문제를 넘어 기업의 신뢰와 브랜드 가치를 훼손하는 결과를 초래했다.

(대응 방안): 과기부, 'SW 공급망 보안 가이드라인 1.0' 발간 등

2) 생성형 AI, 사이버 위협의 새로운 도구로

생성형 AI 기술은 지난해 사이버 위협의 새로운 도구로 자리 잡았다. 지난해 10월 오픈AI(Open AI)와 마이크로소프트(MS)에 따르면, 국가 배후 해커그룹이 Chat GPT를 활용해 정보 수집, 코드 디버깅, 피싱 메시지 작성 등을 실행한 사례가 보고됐다. 다크웹에서는 AI 기반 범죄 도구가 확산하고 있으며, 심지어 일반인들까지 딥페이크 영상 제작 등의 불법 행위에 가담하는 모습이 드러났다. 韓 경찰청 자료에 따르면 딥페이크 가해자 중 80%는 10대 청소년으로, 생성형 AI의 악용이 심각한 사회적 문제로 부상하고 있다.

(대응 방안): 허위, 가짜 뉴스 및 정보 식별 위한 솔루션 및 프라이빗 LLM 도입 등

3) 'OT·ICS·IoT' 융복합 환경의 취약성

스마트팜과 같은 융복합 시스템에서도 보안 위협이 증가했다. 지난해 11월, 친(親) 러시아 해커조직이 국내 원격제어 시스템을 해킹하고 텔레그램(Telegram)에 관련 영상을 공개했다. 비록 큰 피해는 없었지만, 제어 기능이 포함된 시스템에 대한 해킹은 큰 재앙을 초래할 수 있다는 점에서 우려를 낳았다.

또한, IP 카메라 해킹 문제가 지속적으로 발생하며 개인의 사생활 보호에 대한 국민적 불안을 키웠다. 10월에는 친러시아 해커 '서버 킬러스(SERVER KILLERS)'로 인해 국내 CCTV 100대 이상이 해킹 당해 실시간 영상이 유출됐다. 지난 8월에는 음란물 사이트에 '17년부터 현재까지 촬영된 다량의 IP 카메라 영상이 올라오며 논란이 됐다.

(대응 방안): 선박, 자동차, 빌딩 등 새로운 OT 환경에 대한 OT 보안 중요성 피력 및 솔루션 적용 확대

4) 정치·사회적 이슈를 노린 사이버 위협

'24년에는 전 세계적으로 주요 선거는 물론 국가, 지역 간의 전쟁 등이 이어졌다. 국내 총선과 미국 대선을 비롯해 러시아-우크라이나/이스라엘-헤즈볼라 전쟁 등 정치적 긴장 상태는 사이버 공격이 크게 확산되는 계기가 됐다.

북한 배후 해커조직은 국내 여론조사 업체와 정부기관을 대상으로 해킹 시도를 이어갔고, 이란 해커그룹은 미국 대선을 겨냥한 공격을 감행했다. 정치적 성향을 드러내는 핵티비스트(Hacktivist)는 공공기관을 대상으로 DDoS 공격을 감행해 시스템 혼란을 조장하기도 했다.

(대응 방안): 국가적 차원의 핵심 인프라 식별하여 통합 관리 및 각종 안보위협 대응

사이버 보안에 대한 중요성이 널리 강조되고 있음에도 불구하고 사이버 공격의 유형은 물론 공격자들이 활용하는 수단(Tool 등)이 고도화됨에 따라 사이버 침해 사고는 지속적으로 증가하는 추세이다. 이와 관련해 KISA는 민간분야 침해사고를 DDoS 공격, 악성코드 감염, 서버 해킹 및 기타유형(정보유출, 스팸 문자 및 메일 발송 등)을 구분해 신고를 받는 중이다. 하단의 [표1-1]에서도 확인할 수 있듯이, 최근 국내 침해사고 신고 건수는 지속적으로 증가 중이다. 국내에서는 특히나 DDoS, 서버 해킹이 기하급수적으로 증가하고 있는 것을 확인할 수 있는데, 이러한 사이버 위협에 대비하기 위해서는 어떠한 사전대비를 해야할까?

(단위: 건수)

구분 \ 연도		2022 상반기	2022 상반기 비율	2022 하반기	2022 하반기 비율	2023 상반기	2023 상반기 비율	2023 하반기	2023 하반기 비율	2024 상반기	2024 상반기 비율
침해사고신고	DDoS	48	10.1%	74	11.1%	124	18.7%	89	14.5%	153	17.0%
	악성코드	125	26.5%	222	33.2%	156	23.5%	144	23.5%	106	11.8%
	랜섬웨어	(118)	(24.9%)	(207)	(30.9%)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)
	서버 해킹	275	58.1%	310	46.3%	320	48.2%	263	42.9%	504	56.1%
	기타	25	5.3%	63	9.4%	64	9.6%	117	19.1%	136	15.1%
합계		473		669		664		613		899	

[표 1-1] 2022~2024(상반기) 국내 침해사고 신고 건수 (출처: KISA)

02 미리 대비하자! '25년도 보안 위협 전망은?

"지피지기 백전불태(知彼知己 百戰不殆)"라는 사자성어가 존재한다. 지피지기 백전불태의 원전은 손무의 손자병법 모공편의 결구인 '知彼知己, 百戰不殆, 不知彼而知己, 一勝一負, 不知彼不知己, 每戰必殆(지피지기 백전불태 부지피이지기 일승일부 부지피부지기 매전필태)' 중 '지피지기 백전불태'라는 구절에서 유래한다. 이를 해석하면 '적을 알고 나를 알면 백번 싸워도 위태로움이 없으며, 적을 알지 못하고 나를 알면 한 번 이기고 한 번 지며, 적을 모르고 나를 모르면 싸움마다 반드시 위태롭다'는 뜻이다.

원전을 보면 알겠지만 손자병법에 나온 것은 백전백승이 아니라 불태다. 너를 알고 나를 안다고 무조건 이기는 건 아니고 적어도 위태롭지는 않을 것이지만 너를 모르고 나도 모르면 백패가 맞다. 다양한 산업 분야 중 사이버 보안 분야는 지피지기 백전불태라는 사자성어가 가장 잘 어울리는 산업 분야 중 하나이다. 단지 적(사이버 공격자)의 공격을 예상한다(적을 알면)해서 이를 모두 막아낼 수 없기 때문이며, 이를 위해서는 개별 조직이 보유한 자산 등에 대한 가시성(나를 알면)이 매우 중요하기 때문이다.

먼저 적에 대해 알기 위해 '25년도 국내외 사이버 위협 전망에 대해 알아보고자 한다.

1) '25년도 국내외 사이버 위협 전망

자사를 포함한 국내 주요 사이버 보안 기업들과 공공기관(과기정통부, 금융보안원) 그리고 해외 주요 사이버 보안 벤더들이 전망한 '25년도 사이버 위협 전망을 분석한 결과, △생성형 AI 등으로 인한 보안 위협 증가 △딥페이크, 큐싱, 피싱 등 공격 증가 △공격 표면 확대 △국가 주도 공급망 공격 △랜섬웨어 공격 벡터 다양화와 같은 이슈가 발생할 것으로 예측됐다.

구분(국내)	전망	구분(해외)	전망
IGLOO	국가 주도 공급망 공격 및 사이버 안보 위협 증가	CHECK POINT	AI 기반의 공격 증가
	악성 LLM 서비스로 인한 사이버 공격 보편화		랜섬웨어의 공급망 강타
	랜섬웨어 공격 벡터의 다양화		부적절한 AI 사용으로 인한 데이터 침해 증가
	딥페이크 기술 악용, 사회공학적 공격의 새로운 위협		양자 컴퓨팅이 암호화의 새로운 위협으로 떠올라
	멀티채널을 통한 크리덴셜 탈취 공격		소셜 미디어 악용 및 딥페이크의 일반화
AhnLab	인공지능(AI) 기반 공격 확산		AI 기반 SOC 코파일럿의 보안 운영 혁신
	소프트웨어(SW) 공급망 공격 증가		AI 도입 확대에 따라 CIO와 CISO의 역할 융합
	클라우드 및 IoT 확산에 따른 공격 표면 증가		클라우드 보안 플랫폼이 업계 전반을 지배할 것
	적대 세력 간 사이버전 및 핵티비스트 활동 격화		IoT 확장으로 공격 표면의 증가
	랜섬웨어 공격 고도화	Google Cloud	공격자들의 AI 활용 증대
SK 쉴더스	AX 시대를 파고드는 AI 보안 위협		주요 국가별 사이버 위협 전망
	다면적인 공격 기법과 협박 전략 사용하는 랜섬웨어		랜섬웨어와 다면적 갈취 공격 증가
	망분리 규제 완화에 따른 IAM 위협 증가		인포스틸러(정보 탈취) 멀웨어 증가
	협력사의 보안사고에 따른 연쇄 피해 위험		하이브리드 환경에서의 ID 보안 위협 증가
	암호화폐 거래소 해킹 공격 위협 증가		클라우드 보안과 규제 증가
ESTSECURITY	DDoS 공격 규모 증대 및 정교화	paloalto NETWORKS	통합 데이터 보안 플랫폼 중심 사이버 보안 인프라
	국가간 갈등의 지속 및 국가 주도의 사이버전 확대		대형 기업, AI 스타트업과 협력
	암호화폐 탈취를 목적으로 하는 공격 급증		AI 리더십, 신뢰와 거버넌스 중요
	멀티, 하이브리드 클라우드 채택과 공격 표면의 확대		보안 강화된 엔터프라이즈 브라우저의 확산
	생성형 AI 도입 보편화 및 보안 중요성 강화		에너지 효율적 AI 모델
과학기술정보통신부	공격자의 생성형 AI 활용 본격화		양자보안 과대 광고 주의
KISA 한국인터넷진흥원	디지털 융복합 시스템에 대한 사이버 위협 증가		CIO-CMO 협력 중요
	글로벌 환경 변화에 따른 사이버 위협 증가 가능성	FORTINET	공격 체인 전문성의 강화
	무차별 디도스 공격 증가 예상		사이버 공격 가능성이 높은 클라우드
금융보안원	금융회사: 금융보안, 갈라파고스 넘어 글로벌 수준 도약		자동화된 해킹 도구가 다크웹 마켓플레이스에 등장
	금융회사: 금융보안 가치의 재정립		실제 위협이 포함되도록 플레이북 확장
	금융회사: 자율보안 프레임워크 정착		안티-애드버서리 프레임워크의 확대
	금융회사: AI 실효성 및 안전성 검증 본격화		진화하는 위협 환경에 대한 집단적 복원력 강화
	금융회사: 금융권-CSP간 협력 관계 모색	kaspersky	AI는 현실로 다가와 딥페이크 등의 위협 극대화될 것
	금융회사: 양자컴퓨팅에 선제적 대비		사기꾼들의 피싱 캠페인과 위조 상품 사기 유발
	금융소비자: QUBIC에 갇힌 금융소비자, 디지털경계 주의보		정치적 양극화는 사이버 분열을 부추길 것
	금융소비자: (Q) 큐싱 경보 발령		구독서비스 증가로 프로모션 관련 사기의 증가
	금융소비자: (U) 디지털 페르소나 경계	TANIUM	AI는 양날의 검이 될 것
	금융소비자: (B) 생체정보 탈취 현실화		랜섬웨어 지불은 글로벌 규제에 직면한 상태
	금융소비자: (I) 모바일 집중에 따른 위협		AI 기반 공격으로 안한 중요 인프라 훼손
	금융소비자: (C) Web3.0과 가상자산의 미래 주목		생체 인식(인증)은 실패할 것

순위	내용	카운트
1	- 악성 LLM, 생성형 AI 등으로 인한 보안 위협 증가	13
2	- 딥페이크(Deep Fake), 큐싱(Qshing), 피싱(Phishing) 등의 공격 증가	8
3	- 클라우드, IoT 등 디지털 융복합 시스템 등으로 인한 공격 표면(Attack Surface) 확대	6
3	- 국가 주도 공급망 공격 및 사이버 안보 위협 증가	6
5	- 랜섬웨어 공격 벡터 다양화	5

※ 조사 대상은 (국내) 임직원 150명 이상 / (해외) 시가총액 500억 달러($) 이상인 기업들을 대상으로 진행
※ 해외 전망의 경우 자사 솔루션 및 서비스를 강조하기 위한 내용이 국내에 비해 다수 포함되어 있음에 따라, 해당 유형의 전망은 제외하여 집계

[표 1-2] '25년도 국내외 사이버 위협 전망 및 Top 5 리스트 (출처: 각 사, 재구성: 이글루코퍼레이션)

2) '25년도 국내외 사이버 위협 TOP 5

① 악성 LLM, 생성형 AI 등으로 인한 보안 위협 증가

AI 기술이 빠르게 발전하면서 디지털 전환(Digital Transformation, 이하 DX)을 넘어 AI 전환(AI Transformation, 이하 AX)의 시대를 향해 나아가고 있다. 특히 챗GPT(ChatGPT)를 필두로 한 생성형 AI의 등장 이후, AI는 전 산업에 걸쳐 사용되고 있다. AI는 우리에게 혁신과 편리함을 가져다 주었지만, 이를 악용하는 공격자들이 등장하고 있다. 이들은 목적(Tactics), 목적을 이루기 위한 공격방식(Techniques), 공격방식을 달성하기 위한 상세 기법(Procedures)의 기술적 효율성을 도모하기 위해 AI를 무기화하여 기존 보안 체계를 우회하거나 무력화한다.

공격자들은 기존 생성형 AI 모델을 악용하는 것은 물론, 악성 생성형 AI 모델을 통해 사이버 공격을 시도하고 있다. 지난해 2월, 마이크로소프트와 오픈AI는 중국, 이란, 북한, 러시아와 관련된 위협 행위자와 관련된 오픈AI 계정이 오픈소스 정보 질의, 번역, 코딩 오류 찾기, 기본적인 코딩 작업 실행 등의 행위에 사용된 정황을 확인하여 계정을 삭제했다고 발표했다. 또한 공격자들은 다크웹을 중심으로 웜GPT (WormGPT), 프러드GPT(FraudGPT) 등 악성 생성형 AI 모델을 사이버 범죄에 활용하고 있다. 이러한 모델들은 일정 비용을 지불하면 사용자가 특정 기능을 사용할 수 있는 HaaS(Hacking as a Service) 형태로 제공되며, 가드레일(Guardrail)을 우회하는 방법을 사용하는 경우가 많다.

② 딥페이크(Deep Fake), 큐싱(Qshing), 피싱(Phishing) 등의 공격 증가

딥페이크는 광고, 영화, 음반 등 다양한 분야에서 활용되면서 콘텐츠 제작에 혁신을 가져왔지만, 사회 공학적 공격에 악용되면서 심각한 보안 위협으로 떠올랐다. 사회 공학적 공격은 사람 간의 신뢰 관계를 기반으로 조작된 지시를 따르게 만드는데, 딥페이크 기술의 발전으로 더욱 교묘해지고 있다. 각국 정부와 기업들이 딥페이크를 악용한 공격에 대응하기 위해 다양한 조치를 취하고 있음에도 불구하고, 딥페이크 기반의 공격은 빠르게 증가하고 있어 예방책 마련이 시급한 상황이다.

QR코드가 일상생활 곳곳에서 사용되면서 이를 악용한 큐싱(Qshing) 공격이 본격화될 것으로 보인다. 공격자들은 QR코드의 진위 여부를 육안으로 판별하기 어렵다는 점, QR코드가 이미지로 인식되어 이메일 보안 검사 등을 우회할 수 있다는 점 등을 악용하여 다양한 형태로 공격을 시도하고 있다. 이에 지난 3월, 경찰청은 가짜 QR코드 유포, 공식 QR코드 위에 가짜 QR코드 덧붙이기 등 온·오프라인에서 발생할 수 있는 큐싱 사기를 주의할 것을 홍보했다. 특히 금융권에서 큐싱은 다양한 금융사기 기법과 연계되어 공격 방식이 더욱 고도화될 것으로 예상된다.

아울러 AI 등 신기술과 디지털 페르소나(Digital Persona)의 결합으로 사기 기법이 진화하고 있다. 해외에서는 디지털 페르소나를 악용한 사칭 사기나 가상의 신원을 생성하는 합성 신원 등에 의한 신원도용 사고가 발생하고 있다. 홍콩의 한 회사에서는 자사 CFO로 위장한 딥페이크 영상에 속은 직원이 2억 홍콩달러(한화 약 340억 원)에 해당하는 금액을 송금한 것으로 드러났다. AI 활용 등으로 디지털 페르소나 악용 수법이 갈수록 정교화될 것이므로 경각심을 제고할 필요가 있다.

③ 클라우드, IoT 등 디지털 융복합 시스템 등으로 인한 공격 표면(Attack Surface) 확대

클라우드와 운영 기술(OT) 환경의 확산 등으로 인해 나날이 공격 표면이 확대되고 있다. 여기서 공격 표면이란 주어진 환경 내에서 권한이 없는 사용자가 악용할 수 있는 모든 취약성과 진입점을 뜻하는데, 이는 공격자가 무단 액세스를 얻기 위해 표적으로 삼는 디지털 및 물리적 구성 요소를 모두 포함한다. 많은 조직에서 여전히 OT 환경이 에어 갭을 통해 보호되고 있다고 믿고 있지만, IT/OT 융합으로 인해 OT는 그 어느 때보다 IT와 더 많이 연결되어 있으며, 클라우드와도 연결되어 있다. 이로 인해 공격 표면이 확대되고 OT 네트워크에 대한 위험이 크게 증가했으나 사이버 제어에 대한 투자는 늘지 않은 상황이다.

OT 환경의 확산뿐만 아니라 클라우드의 확산 역시 공격 표면의 확대에 큰 영향을 미치고 있다. 보안 업체 팔로알토 네트웍스(PaloAlto Networks)에 따르면 공격 표면의 대부분을 클라우드가 차지하는 것으로 나타났다. 공격 표면 비율을 분석하면 온프레미스는 19%인데 반해 클라우드가 80%로 대부분을 차지하는 등 앞으로도 공격 표면은 가파르게 증가할 것으로 예상된다. 올해는 조직이 가장 중요한 비즈니스 시스템을 보호하고 증가하는 위험을 수용 가능한 수준으로 관리하기 위해 공격 표면에 대한 투자를 늘릴 것으로 예상된다.

④ 국가 주도 공급망 공격 및 사이버 안보 위협 증가

러시아-우크라이나 전쟁, 이스라엘-하마스 전쟁 등 국가 간 갈등이 올해도 지속되면서 국가 주도의 사이버 공격이 확대될 전망이다. 본래 북한, 이란, 러시아, 중국 등 반(反) 서방 국가들의 핵티비스트(Hacktivist) 그룹들은 정치적인 성격을 강하게 띄고 있어, 자신들의 메시지를 전달하기 위해 사이버 공격을 가하는 데 그쳤다. 그러나 핵티비즘의 범위가 확장되면서 핵티비스트 그룹들은 정치적, 경제적, 군사적 이익을 달성하기 위해 금융, 의료, IT 등 분야를 가리지 않고 공격을 전개하고 있다. 이들의 공격은 주요 기반 시설이나 정부 시스템을 노리는 등 더욱 파괴적인 형태를 띨 것으로 예측된다.

⑤ 랜섬웨어 공격 벡터 다양화

랜섬웨어는 최근 몇 년간 꾸준히 발생하고 있는 보안 위협으로, 랜섬웨어로 인한 피해 규모는 점차 증가하고 있다. 사이버 범죄 분석 전문 업체 스파이클라우드에 따르면, '23년 기준 랜섬웨어에 지불된 금액은 10억 달러를 넘어섰다. 또한 단독 행위자부터 록빗(Lockbit), 아키라(Akira) 등 강력한 제휴 비즈니스 모델을 갖춘 랜섬웨어 패밀리까지 공격 규모, 빈도, 범위, 신규 참여자 수가 급증한 것으로 나타났다. 영국, 미국 등 국제 수사기관들은 공조를 통해 록빗 등 주요 랜섬웨어 그룹을 장악하는 데 성공했지만, 콘티(Conti)와 류크(Ryuk) 등 기존 그룹 간 연계로 인해 새로운 랜섬웨어 패밀리가 등장하면서 공격이 끊이지 않고 있다.

랜섬웨어는 여러 산업 분야에 영향을 미치고 있으며, 나아가 전 세계의 인프라와 사회 시스템까지 위협하고 있다. 중국 배후의 해킹 그룹 볼트타이푼(Volt Typhoon)은 전 세계 주요 인프라를 공략하는 대표적인 조직이다. 이들은 랜섬웨어를 활용하여 통신, 에너지, 교통 시스템, 상하수도 시스템을 포함한 미국의 주요 인프라를 공격하여 피해를 야기했다. 이처럼 랜섬웨어 공격은 금전적 목적으로 시스템을 잠그거나 데이터를 암호화하는 데 그치지 않고, 사회기반시설 및 인프라를 마비시켜 국가 차원의 혼란을 불러올 수 있다. 또한 기업들의 보안 수준 향상으로 인해 수익이 감소하고, 랜섬웨어 시장이 포화 상태에 다다르면서 공격 전략과 기법이 고도화될 것으로 예상된다. 특히 랜섬웨어 그룹들은 피해 기업과 연관된 협력사나 고객사를 협박하거나 디도스(Distributed Denial of Service, DDoS) 공격을 병행해 기업의 핵심 업무를 방해하는 등 다중 협박 전략을 취하고 있다. 이러한 전략은 강한 협상 압박을 통해 수익을 늘리는 방식으로 올해도 지속될 것으로 보인다.

03 나 자신을 알자, 복원력과 가시성의 중요성

지금까지 올 한해 사이버 생태계를 위협할 보안 위협 TOP 5에 대해 알아봤다. 적(사이버 공격자)에 대해 알아봤다면 이제는 '나 자신(나를 모르면 싸움마다 반드시 위태롭다)'을 파악하기 위한 방법에 대해 알아보고자 한다.

앞서 언급했듯이 사이버 공격자들은 생성형 AI, 랜섬웨어 등 나날이 고도화된 수법으로 사이버 환경을 위협하고 있다. 이에 대응하기 위한 방안으로 국내외 사이버 보안 기업들은 △제로트러스트(Zero Trust) △확장된 탐지 및 대응(eXtended Detection and Response, 이하 XDR)과 같은 통합보안플랫폼을 내세우고 있다. 다만 이제는 증가하는 사이버 위협에 단지 '대응(Respond)' 하는 것뿐만 아니라 '예방(Prevent)'에도 집중해야 한다.

① 사이버 복원력(Cyber Resilience)의 확보

잠재적인 사이버 위협으로부터 조직이 보유하고 있는 중요 시스템 및 데이터를 효과적으로 보호하기 위해서는 전사 차원에서 사이버 보안 사고를 사전, 사후적으로 관리하는 조직의 능력(사이버 복원력, Cyber Resilience)을 강화하는 것이 필수적이다. 이를 위해서는 데이터 처리 전 단계에 걸쳐 데이터 처리 흐름(Flow)을 파악하기 위해 지속적으로 모니터링하고, 기업 특성에 맞는 보안 조치, 업계 표준 및 내부 규정 등의 정비가 우선시되어야 한다.

이를 위한 사이버 복원력에 대해 美 국립표준기술연구소(NIST)를 포함한 글로벌 기관들은 '임무수행을 보장하기 위해 사이버 역량을 활용하거나 이를 통해 운용되는 조직이 불리한 환경이나 압력, 공격, 또는 강요받는 상황을 예측하고 견디며, 이로부터 회복하고 적응하는 능력'이라고 정의하고 있다. 보다 쉬운 이해를 위해 사이버 복원력과 사이버 보안과의 차이를 다음과 같이 정리했다.

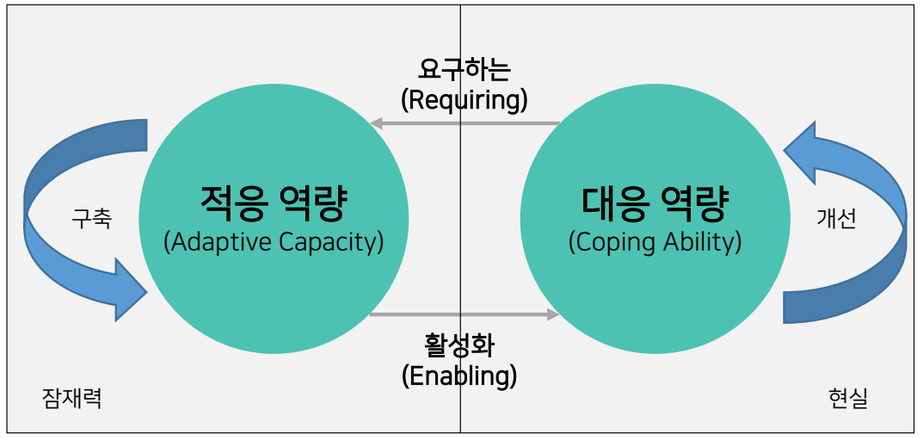
구분	내용
비즈니스 연속성	- 정보시스템의 보호를 넘어선 비즈니스의 임무와 목표의 지속성 달성을 위한 역량
전사적 활동	- 비즈니스 연속성을 위해서는 IT 자산과 보안 부서의 활동을 넘어선 전사적이며 기술과 인간의 균형된 노력을 통한 대응 역량 강조
생태계 보호	- 해당 조직 뿐만 아니라 상호 연결된 다양한 수준의 협력사, 외부 기관과 시스템을 보호하기 위한 상호협력 및 정보공유 노력을 통한 대응 역량 강조

[표 1-3] 사이버 복원력 키워드 (출처: KISA, 재구성: 이글루코퍼레이션)

구분	사이버 복원력(Cyber Resilience)	사이버 보안(Cyber Security)
정의	사이버 자산을 운용하는 조직 차원에서의 역량(면역, 회복력)	사이버 공격 등 위협으로부터 데이터 및 IT 시스템의 보호
객체	비즈니스 결과물 전달 보장	데이터, 정보시스템, 네트워크 등 보호
적용 범위	전사적 그리고 관련 조직 간 생태계	보안 관련 부서 중심
목표	비즈니스 요구사항 및 연속성 유지	사이버 공격 위험 저하, IT 자산 등 보호
특징	- 보안사고 발생은 불가피하다고 가정 - 사고의 예측 탐지, 복구 역량을 위해 보안 모범 사례 정규화 - 조직의 보안 문화와 생태계 보호 및 협력 강조	- 보안 사고 발생을 최소화하기 위해 대내외 사이버 위협으로부터 예방을 위한 IT 통제에 치중하며 시스템 별 개별적 적용
관점	사이버 자산에 대한 다양한 위험에 대응하기 위한 조직 차원에서의 내재화된 역량	대내외 사이버 위협으로부터 조직 내 사이버 자산을 대상으로 특정 기술 도입을 통한 보호

[표 1-4] 사이버 복원력-사이버 보안 차이점
(출처: KISA, 재구성: 이글루코퍼레이션)

사이버 복원력은 급변하는 상황에 민첩하게 적응할 수 있는 '역량(Adaptive Capacity)'과 실제 사고 발생 시에 대응할 수 있는 '능력(Coping Ability)'으로 평가될 수 있으며, 정태적인 보안 체계의 산출물이기보다는 위의 두 가지 역량의 상호작용을 통한 동태적 활동이라고 정의된다.



[그림 1-2] 사이버 복원력에 대한 동태적 관점
(출처: Towards a novel conceptualization of cyber resilience, 2020 IEEE SERVICES,
재구성: 이글루코퍼레이션)

② 충분한 가시성(Visibility)의 확보

사이버 복원력의 확보뿐만 아니라 개별 조직에서는 적의 위협에 맞서기 위한 충분한 가시성(Visibility)의 확보에도 집중해야 한다. 개별 조직이 보유한 자산 등에 대한 가시성이 확보되지 않는다면, 보안 취약점의 증가 및 운영상의 리스크가 발생할 수 있기 때문이다. 그리고 이러한 리스크는 조직의 보안 사고 발생 가능성을 높이고, 비즈니스 연속성을 저해 시킨다. 실제로 최근 클라우드 환경으로 전환하는 조직이 많다 보니 가시성 확보에 대한 중요성이 더욱 높아졌는데, 바로 △섀도우 IT(조직 내 허가받지 않는 IT 자산이 보안 위험을 초래) △클라우드 마이그레이션(클라우드 환경에서 가시성이 부족하여 잘못된 설정으로 데이터 유출 발생)과 같은 이슈가 빈번하고 발생하고 있기 때문이다.

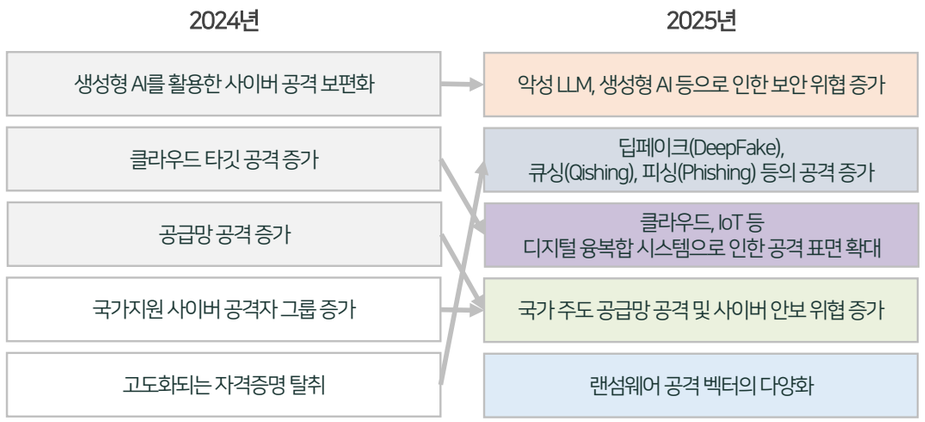
사이버 보안 측면에서 가시성 확보를 위한 방안으로는 △자산 관리 솔루션 사용 △자동화 모니터링 △주기적인 감사 및 평가 △통합 보안 플랫폼 구축 등을 꼽을 수 있으며, 이글루코퍼레이션 역시 '지피지기 백전불태'를 위한 다양한 솔루션과 서비스를 제공하여 보다 안전한 사이버 환경을 올해도 구축하고자 한다.

구분	내용
1	자산 관리 솔루션 사용(자산 식별, 분류 및 추적에 도움을 주는 도구 사용)
2	자동화된 모니터링(네트워크 및 시스템의 실시간 가시성 제공)
3	주기적인 감사 및 평가(자산 목록과 상태를 정기적으로 검토)
4	통합 보안 플랫폼 구축(보안 이벤트와 자산 상태를 한눈에 확인할 수 있는 대시보드 활용)

[표 1-5] 사이버 보안 측면에서의 가시성 확보를 위한 방안 (출처: 이글루코퍼레이션)

04 마무리

'25년 보안 위협 전망은 전년과 유사하지만 더욱 정교화·고도화되는 양상을 보이고 있다. 생성형 AI를 활용한 사이버 공격이 보편화되고, 국가 주도의 핵티비스트 활동이 증가하여 국제적 긴장을 유발할 가능성이 높아졌다. 또한 랜섬웨어의 공격 기법이 복잡해지면서 개인과 기업 모두를 위협하고, 증가한 공격 표면과 신종 사이버사기는 더욱 심각한 보안 문제로 부상할 것으로 예상된다. 즉, '25년은 이전에 나타났던 보안 위협이 다차원적으로 전개되는 시기로 볼 수 있다.



[표 1-6] '24~'25년도 사이버 위협 Top 5 비교 (출처: 이글루코퍼레이션)

이러한 보안 위협들이 실제로 발생하지 않는다면 좋겠지만, 안타깝게도 매년 발표되는 보안 위협들은 현실로 다가와 우리의 삶을 위협하곤 한다. 이에 이글루코퍼레이션을 비롯한 각 기관과 기업들은 보안 위협에 대한 효과적인 대응 전략과 기술을 지속적으로 연구하여 공개하고 있다. 특히 기술 발전 속도에 맞는 적극적 대응과 사전 예방적 접근이 중요성이 강조되고 있다. 이러한 전략을 바탕으로 보다 견고한 보안 체계를 구축하고, 안전한 디지털 환경을 조성할 수 있기를 기대한다.

05 참고자료

1. 2024년 사이버보안 위협 정리해보니... 2025년 대응방안이 보인다. 보안뉴스:https://m.boannews.com/html/detail.html?tab_type=1&idx=134987
2. 올해 상반기 침해사고 신고 건수 899건, 전년 동기대비 35% 증가, 보안뉴스: https://m.boannews.com/html/detail.html?idx=131560
3. 2025년 사이버 보안 위협 및 기술 전망 보고서 발표, 이글루코퍼레이션 https://www.igloo.co.kr/newsroom/press/2025%EB%85%84-%EC%82%AC%EC%9D%B4%EB%B2%84-%EB%B3%B4%EC%95%88-%EC%9C%84%ED%98%91-%EB%B0%8F-%EA%B8%B0%EC%88%A0-%EC%A0%84%EB%A7%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C-%EB%B0%9C%ED%91%9C/
4. [KISA Insight 2024 Vol.05] 침해사고 등 사이버 공격 대응 관점에서의 사이버 복원력(Cyber Resilience) 정책 이슈 분석 및 시사점, 한국인터넷진흥원: https://www.kisa.or.kr/20301/form?postSeq=27&page=1

03
보안 101

생성형 AI란 무엇인가요?

매달 하나의 주제를 선정해 질문을 던지며,
보안에 한 걸음 더 가까이 다가갑니다.
복잡하고 어렵게 느껴질 수 있는 보안 지식을
초보자도 쉽게 이해할 수 있도록,
기초 개념부터 최신 이슈까지 차근차근 풀어갑니다.

보안이 알고 싶을 땐, 보안 101으로 시작해 보세요.
물음표를 느낌표로 바꾸는 여정을 이글루코퍼레이션이 함께합니다.

생성형 AI란 무엇인가요?

전략사업부 마케팅팀 한가연

1. 생성형 AI 정의

생성형 AI(Generative AI)는 주어진 데이터를 학습하여 새로운 콘텐츠를 생성하는 인공지능 기술입니다. 사용자의 특정 요구에 따라 결과를 능동적으로 생성할 수 있는 능력을 갖추고 있어 텍스트 생성, 이미지 생성, 음악 작곡, 코딩 등 다양한 창의적 작업에 활용됩니다. 대표적인 예로는 텍스트를 생성하는 챗GPT(ChatGPT), 이미지를 생성하는 달리(DALL-E), 음성을 생성하는 발리(VALL-E) 등이 있습니다. 생성형 AI는 인간의 창작 능력을 보완하거나 확장하는 데 크게 기여하며 여러 산업의 혁신을 이끌고 있습니다.

2. 생성형 AI 작동 방식

생성형 AI의 작동 방식은 크게 학습, 조정, 그리고 강화라는 세 가지 과정으로 나눌 수 있습니다.

학습: 다양한 데이터를 학습해 기본 지능을 갖춘 모델을 만듭니다. 이 모델은 여러 분야에서 사용할 수 있는 일종의 만능 모델입니다. 이렇게 만들어진 모델은 기반 모델(Foundation model)이라 불리며, 다양한 작업에 활용될 수 있는 뼈대가 됩니다.

조정: 일반적인 지능을 가지고 있는 파운데이션 모델을 특정한 목적이나 상황에 맞게 맞춤화합니다. 특정 작업을 잘 수행할 수 있도록 세부적으로 튜닝하는 과정이 필요합니다.

강화: 이렇게 만들어진 생성형 AI 모델은 학습한 내용을 바탕으로 결과물을 생성합니다. 생성된 결과물은 평가 과정을 거치며, 품질과 정확성을 지속적으로 개선합니다. 이러한 과정을 반복하면서 AI는 점점 더 정교하고 자연스러운 결과를 만들어냅니다.

3. 생성형 AI의 이점

생성형 AI는 업무 효율성을 높이고, 인간의 창의력을 확장하며, 의사 결정을 한층 빠르고 정확하게 지원하는 도구로서, 다양한 산업에서 혁신적인 변화를 이끌고 있습니다.

효율성 향상

생성형 AI는 반복적이고 일상적인 작업을 자동화하여 생산성을 획기적으로 높입니다. 예를 들어 데이터 요약 및 분석, 문서 작성, 코드 검수, 고객 대응 등과 같은 작업을 빠르고 정확하게 수행함으로써 시간과 비용을 절감할 수 있습니다. 생성형 AI를 활용하면 기존에 대규모의 팀 또는 오랜 시간을 필요로 했던 작업을 단시간에 완료할 수 있고, 이를 통해 직원들은 보다 전략적이고 창의적인 업무에 집중할 수 있게 됩니다. 이러한 효율성은 조직의 경쟁력을 강화하고 자원의 활용도를 극대화하는 데 기여합니다.

창의력 향상

생성형 AI는 기존 데이터를 바탕으로 독창적인 텍스트, 이미지, 영상, 음악 등을 생성하여 인간의 창작 과정을 보완하고 확장합니다. 예를 들어 광고 캠페인용 카피를 작성하거나 영화 시나리오 초안을 작성하는 등 창의적인 콘텐츠 제작에 활용될 수 있습니다. 또한 디자이너와 작가가 생성형 AI와 협력하여 다양한 아이디어를 탐색하고 발전시킴으로써 창작의 범위를 넓히는 협업 도구로 사용됩니다. 이처럼 생성형 AI는 창의적인 영감을 제공하고 효율적인 작업 흐름을 지원하는 데 기여합니다.

한층 향상된 의사 결정

생성형 AI는 보다 나은 의사 결정을 가능하게 합니다. 대규모의 데이터를 신속하게 분석하고 핵심 정보를 도출하여 의사 결정 과정을 단축합니다. 이를 통해 기업은 시장 데이터를 분석하거나, 실시간 재고 데이터를 활용해 공급망 최적화와 같은 전략을 신속하게 수립할 수 있습니다. 최신 정보를 바탕으로 정확한 예측 결과를 제공하기 때문에, 의사 결정의 질 또한 크게 향상됩니다. 이처럼 생성형 AI는 복잡한 상황에서도 명확하고 전략적인 선택을 가능하게 해 조직의 경쟁력을 강화합니다.

사용자 경험 개선

생성형 AI는 사용자 경험을 혁신적으로 개선합니다. 사용자의 선호와 니즈를 학습하여 보다 개인화된 콘텐츠 및 서비스를 제공할 수 있으며, 언제나 이용 가능한 AI 기반 서비스는 고객의 문의를 실시간으로 처리해 응답 속도와 만족도를 크게 높입니다.

또한 제한적인 응답만이 가능했던 기존의 챗봇과 달리, 생성형 AI를 활용한 서비스는 자연스럽고 유연한 대화가 가능해 더 높은 수준의 고객 경험을 제공합니다. 이를 통해 기업은 고객과의 상호작용을 강화하고 보다 깊은 신뢰와 충성도를 구축할 수 있습니다.

R&D 가속화

생성형 AI는 연구와 개발 과정을 가속화합니다. 새로운 개념이나 제품을 정교하게 시뮬레이션하고 평가할 수 있어 혁신적인 아이디어를 빠르게 현실화할 수 있습니다. 예를 들어 신제품 테스트 과정에서 생성형 AI는 기존 도구보다 더욱 상세하고 현실적인 시뮬레이션을 제공하여 테스트의 효율성과 정확성을 높입니다. 연구 및 개발에 소요되는 시간과 비용을 절감하고 보다 신속한 혁신과 시장 출시를 가능하게 합니다.

4. 생성형 AI의 과제

생성형 AI는 혁신적인 기술이지만, 몇 가지 한계점을 지니고 있습니다.

학습 데이터의 편향

생성형 AI는 학습 데이터에 의존하기 때문에 데이터에 포함된 편향이 결과물에 그대로 반영될 수 있습니다. 예를 들어 특정 지역이나 문화에 대한 편향된 데이터로 학습된 AI는 공정하지 못한 결과를 생성할 가능성이 있습니다. 이는 사회적 불평등을 심화시키거나, 사용자 신뢰를 떨어뜨리는 결과를 초래합니다. 생성형 AI의 신뢰성과 공정성을 확보하기 위해 데이터를 신중하게 제한하거나 정제하는 등 편향을 줄이기 위한 지속적인 노력이 필수적입니다.

부정확한 정보 생성

생성형 AI는 때때로 존재하지 않는 정보를 마치 사실인 것처럼 생성하는 환각(Hallucination) 현상을 보일 수 있습니다. 이는 AI가 실제로는 알지 못하거나 부정확한 내용을 정답이 아님에도 불구하고 그럴듯한 답변으로 제공하는 현상입니다. 또한 오래된 데이터를 학습한 모델은 현재와 관련이 없거나 유효하지 않은 정보를 생성할 가능성도 있습니다. 이러한 부정확한 정보는 사용자에게 혼란을 초래하고 AI에 대한 신뢰를 떨어트립니다. 이러한 문제를 줄이기 위해 검증 가능한 데이터를 기반으로 AI를 학습시키고, 생성된 결과를 체계적으로 평가 및 교정하는 시스템을 도입하는 것이 중요합니다.

일관성 없는 아웃풋

생성형 AI는 결과물의 일관성이 부족하거나 맥락에 맞지 않는 내용을 생성하는 경우가 종종 있습니다. 예를 들어 텍스트 생성 AI가 같은 질문에 서로 다른 답변을 제공하거나, 이미지 생성 AI가 의도와 다르게 왜곡된 결과를 만들어내는 사례가 이에 해당합니다. 이를 개선하기 위해서는 모델의 맥락 인식 능력을 강화하고, 사용자 피드백을 통해 모델을 개선하거나, AI의 생산물을 추가로 검증하는 과정 등이 필요합니다.

보안, 개인정보보호 및 지적 재산에 대한 위협

생성형 AI는 보안 및 법적 측면에서도 다양한 위협을 초래할 수 있습니다. 학습 데이터에 포함된 개인정보가 의도치 않게 결과물에 나타나거나 AI를 통해 가짜 뉴스, 피싱 이메일 등 악의적인 콘텐츠가 생성될 가능성도 있습니다. 또한 만약 AI가 저작권이 있는 데이터를 학습한 경우 이를 기반으로 생성된 결과물이 타인의 지적 재산권을 침해할 우려도 존재합니다. 더 나아가 생성형 AI 모델이 프롬프트에 포함된 정보를 학습 과정에서 활용하는 경우, 민감한 개인 정보가 수집되거나 저장될 가능성도 배제할 수 없습니다. 이러한 문제를 예방하기 위해서는 AI 개발 단계에서부터 데이터 사용에 대한 윤리적 기준을 수립하고, 법적 규제를 강화하며, AI가 생성한 콘텐츠의 투명성과 책임성을 높이는 노력이 필요합니다.

5. 생성형 AI 성능 개선을 위한 방안

생성형 AI의 성능을 높이기 위해 다양한 기술과 접근 방식이 활용됩니다.

파인 튜닝

파인 튜닝(Fine-Tuning)은 기본 모델을 특정 작업이나 도메인에 맞게 추가 학습시키는 방법으로, 생성형 AI가 특정 산업이나 주제에 특화된 결과를 생성할 수 있도록 도와줍니다. 예를 들어 대규모 의료 데이터를 학습한 모델은 더욱 정확하고 전문적인 의학 보고서를 작성할 수 있으며, 법률 문서에 최적화된 AI를 개발해 법률 관련 업무를 보조하는 데 활용할 수 있습니다. 이러한 과정을 통해 AI는 더욱 정밀하고 맥락에 적합한 결과를 제공하게 되며, 다양한 분야에서 실질적인 가치를 창출할 수 있습니다.

검색 증강 생성

검색 증강 생성(Retrieval-Augmented Generation, RAG)은 데이터 소스를 참조하여 AI 답변의 정확도를 높이는 기술로, 마치 오픈북 테스트를 가능하게 하는 방식이라고 이해할 수 있습니다. 외부 데이터베이스에서 필요한 정보를 실시간으로 검색하고 이를 바탕으로 결과물을 생성함으로써 최신 정보나 기존 학습 데이터에 없는 세부 사항을 보완할 수 있습니다. 이 방법은 단순히 모델의 사전 학습 데이터에 의존하는 것을 넘어, 실시간으로 유용한 정보를 활용하여 더욱 신뢰도 높은 답변을 제공할 수 있도록 지원합니다. 특히 파인 튜닝에 비해 최신 정보를 제공하는 데 효과적이며, 또 출처가 확실한 데이터를 기반으로 결과를 개선하기 때문에 다양한 상황에서 관련성, 정확성, 유용성을 유지할 수 있는 비용 효율적인 접근법입니다.

인간 피드백을 통한 강화 학습

인간 피드백을 통한 강화 학습(Reinforcement Learning with Human Feedback, RLHF)은 인간의 피드백을 활용해 AI 모델의 성능을 개선하는 강화 학습 기법입니다. 생성형 AI가 생성한 결과를 인간이 평가하고, 이러한 평가를 모델 학습에 반영함으로써 결과의 품질을 지속적으로 향상시킬 수 있습니다. 이 방법은 생성형 AI가 자연스럽고 맥락에 맞는 대화를 생성하며, 인간 친화적이고 윤리적인 출력을 만들어내는 데 특히 유용합니다. 인간 피드백을 기반으로 학습하기 때문에 사용자 경험을 크게 개선할 수 있을뿐만 아니라, 모델의 신뢰성과 안전성을 동시에 높이는 데 효과적입니다.

지속적 학습

지속적 학습(Continual Learning)은 생성형 AI의 발전에 있어 가장 핵심적인 요소입니다. 지속적 학습을 통해 생성형 AI는 새로운 데이터와 상황을 학습하며 최신 정보를 반영하고 성능 저하를 방지함으로써 점점 더 발전된 결과를 제공합니다. 이 과정에서 학습 데이터의 품질을 높이고 편향을 줄이기 위한 데이터 정제 및 확장 작업도 병행되어야 합니다. 이를 통해 생성형 AI는 공정성과 정확성을 유지하며 변화하는 환경 속에서도 신뢰도 높은 결과를 지속적으로 제공할 수 있습니다.

이러한 방안들은 생성형 AI의 정확성과 효율성을 높이고, 다양한 도메인과 상황에서 더욱 유용한 도구로 발전시키는 데 기여합니다.

6. 정보보안 측면에서의 생성형 AI

정보보안 측면에서 생성형 AI는 약이 될 수도, 독이 될 수도 있는 양면성을 가지고 있습니다.

우선, 생성형 AI는 보안 강화를 위한 혁신적인 도구로 사용될 수 있습니다.
방대한 양의 데이터를 실시간으로 분석하여 비정상적인 패턴을 탐지하고, 이를 기반으로 위협의 원인을 설명하거나 대응 방안을 제안할 수 있습니다. 예를 들어 네트워크에서 악성 트래픽이나 이상 징후를 탐지해 관리자에게 요약 보고서와 대응 방안을 자동으로 생성하는 데 활용될 수 있습니다. 또한 피싱 이메일의 패턴을 분석해 사전에 차단할 수 있습니다. 의심스러운 이메일의 링크나 도메인을 감지해 사용자에게 경고 메시지를 제공하거나 안전한 링크로 변환할 수도 있습니다.

보안 교육 및 인식 강화에도 활용 가능합니다. 직원 맞춤형 보안 교육 자료를 생성하거나 실제 상황을 현실감 있게 반영한 피싱 이메일 시뮬레이션 훈련을 통해 실질적인 보안 인식을 높이는 데 기여할 수 있습니다. 나아가, 가상 보안 어드바이저로서 사용자의 질문에 따라 실시간으로 보안 권장 사항이나 침해 사고 발생 시 적합한 대응 방안을 제안하는 역할도 수행할 수 있습니다.

결론적으로, 생성형 AI는 보안 위협 탐지의 정밀도를 높이고 보안 운영의 효율성을 향상시키며 인적 오류를 최소화하는 데 기여합니다. 이러한 기술은 보안 전문가가 고부가가치 작업에 집중할 수 있도록 돕고, 조직 전체의 보안 수준을 강화하는 데 중요한 역할을 할 수 있습니다.

그러나 생성형 AI는 피싱 이메일, 악성 코드, 딥페이크 등 악의적인 콘텐츠를 생성해 보안 위협을 초래할 수 있습니다. 예를 들어 자연스러운 피싱 메시지로 개인 정보를 탈취하거나, 보안 시스템을 우회하는 악성 코드를 생성할 수 있습니다. 또한 가짜 뉴스와 딥페이크를 활용해 혼란을 야기하거나, 자동화된 공격을 강화해 특정 취약점을 정교하게 악용할 수 있습니다.

이처럼 생성형 AI는 보안을 위한 강력한 무기가 될 수도 있지만, 동시에 치명적인 위협으로 작용할 가능성도 있습니다. 이를 긍정적으로 활용하기 위해서는 기술 개발과 더불어 강력한 윤리적 기준과 규제를 마련해야 하며, AI 오용을 방지하기 위한 체계적인 관리 및 모니터링이 필수적입니다. 다시 말해 생성형 AI를 현명하게 활용하기 위해서는 기술 혁신과 보안 정책이 균형을 이루는 조화로운 접근이 필요합니다.

이글루코퍼레이션은 어떻게 생성형 AI를 활용하고 있나요?

이글루코퍼레이션의 에어(AiR, AI Road)는 분류형 AI, 설명 가능한 AI, 그리고 생성형 AI를 토대로 특정 보안 데이터에 대해 AI 모델이 판단한 근거를 알려주는 'AI 보안 어시스턴트'입니다. 사용자들은 AI 모델의 판단 기준 확인을 통해 AI 답변에 대한 신뢰도를 평가하고, 자연어 형태의 설명을 토대로 AI 답변에 대한 이해도를 높일 수 있습니다. AiR는 AI가 판단한 공격 결과에 대한 신뢰성과 이해도를 높임으로써 보안 조직 전반의 지식 격차를 해소하고, 언제나 최상의 조치가 신속하게 실행될 수 있도록 도와줍니다.

04
칼럼

매월 주목할 만한 IT 트렌드나 이슈를 큐레이션하여 선보입니다.

기술의 현재를 분석하고 미래를 전망하며,
이글루코퍼레이션의 시선으로 풀어낸 인사이트를 제공합니다.

AI: "마음을 드려요"

전략사업부 마케팅팀 안서진

01 마음의 문을 여는 열쇠, AI

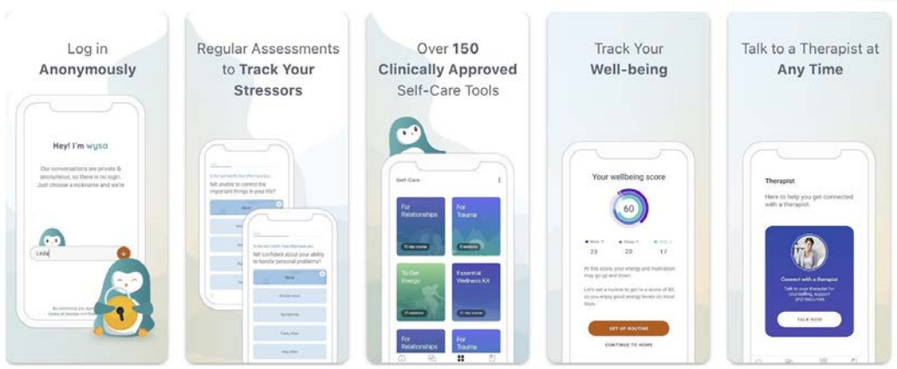
인공지능(AI) 기술이 급속도로 발전하면서 우리의 일상은 하루가 다르게 변화하고 있다. 스마트 홈 기기들은 사용자의 습관을 학습하여 최적의 환경을 조성하고, 음성인식 비서는 일상적인 루틴을 대신 처리해 주며, 자율주행 자동차는 운전의 피로를 줄여준다. 이러한 변화는 우리의 삶을 더욱 편리하고 풍요롭게 만들어 주고 있다.

최근에는 의학 및 의료계에서도 삶의 질 향상을 위한 AI 기술 도입이 활발하게 이뤄지고 있다. 기존에 의료 데이터 분석 및 진단에 집중했던 것에서 벗어나, 데이터에서 패턴을 학습하여 새로운 콘텐츠를 생성하는 '생성형 AI' 기술을 도입하려는 움직임 역시 강해졌다. 이에 현대인의 정신건강 증진을 위한 주요 AI 활용 서비스를 살펴보며, 우리의 멘탈을 단단하게 지킬 수 있는 방법을 모색해 보고자 한다.

[그림 2-1] AI를 활용한 의료 서비스 (출처: 챗GPT를 통해 생성한 이미지)

02 내 손 안의 AI 심리 상담사

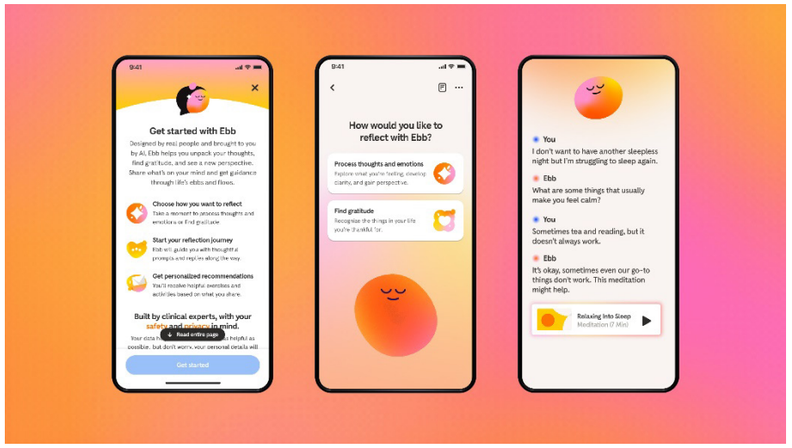
먼저, 심리 상담 분야의 생성형 AI 도입이 눈에 띈다. 개인의 심리 상태 분석을 토대로 마치 사람처럼 말하는 자연어 형태로 조언을 제공하는 형태다. 와이사(Wysa)와 워봇(Woebot) 등 국내외 AI 심리 상담 챗봇 기업들은 정신 건강 검사, 명상 및 스트레스 관리 기능을 포함한 AI 기반 애플리케이션 서비스를 제공하고 있다. 자연스러운 대화를 통해, 우울증, 불안 장애 증상 등을 겪는 사람들의 정서적 문제를 완화하고 상태 악화를 예방하는 초기 상담 도구로 활용할 수 있다는 설명이다. 이들은 대량의 정신건강 데이터 분석을 기반으로 개인맞춤형 치료 계획을 제안하거나 실제 심리 상담사와의 연계 서비스를 제공하는 등 치료 효과 증진을 위한 심층 서비스 제공에도 힘을 기울이고 있다.



[그림 2- 2] Wysa: Anxiety, therapy chatbot (출처: Wysa)

03 AI 명상으로 스트레스 극복

명상 및 스트레스 관리 분야에서도 생성형 AI의 활용이 점차 확대되고 있다. 불면증을 앓고 있는 사람들 사이에서는 이미 유명한 캄(Calm)이나 헤드스페이스(Headspace) 같은 명상 애플리케이션에서도 생성형 AI를 도입했다. 이들은 AI를 활용해 사용자의 스트레스 수준과 감정 상태를 분석하고, 이에 기반한 개인화된 명상 콘텐츠를 제공한다. 예를 들면 사용자의 기분에 맞춰 명상 스크립트를 작성해 주거나, 스트레스받는 특정 상황에 필요한 호흡법과 명상 기법을 제안하는 식이다. 사용자는 간단한 질문에 답하거나 하루의 상태를 기록하는 것만으로도 개인맞춤형 명상 솔루션을 자동으로 제공받을 수 있다.



[그림 2-3] Meet Ebb, AI Mental Health Companion (출처: Headspace)

04 우울증까지 치료하는 AI

한국인 6-7명 중 1명이 일생에 한 번은 걸린다는 우울증 치료에도 AI 기술 활용이 이뤄지고 있다. 디지털 의료기기 전문기업 '메디트릭스'는 최근 열린 세계 최대 가전·IT 박람회 'CES 2025'를 통해 의자형 VR 기반 우울증 디지털 치료제 '마인드체어(가칭)'를 선보였다. 마인드체어는 실시간으로 심박수, 심박 변이도, 뇌파, 근전도 등 사용자의 생체 신호를 측정하고, 이에 알맞은 가상현실 영상을 보여줌으로써 긴장과 불안을 조절해 주는 제품이다. 사용자는 약 15분 길이의 영상 시청을 통해 스스로 마음을 평화롭게 안정시키는 훈련을 하며 우울증과 불안감을 치료할 수 있다.

지난 12월에는 우울증 확률을 표시하는 소프트웨어 의료기기 '아크릴-D01'가 식품의약품안전처(식약처) 허가를 받기도 했다. 이는 의료 AI 전문 기업 '아크릴'이 개발한 것으로, 내원한 환자의 면담 기록지를 AI 기술로 분석해 우울증 확률을 수치화하고 정신건강의학 임상의의 우울증 진단을 보조한다. 환자 면담 기록 데이터를 토대로 환자의 감정을 선별하고 AI 알고리즘의 계산을 거쳐 우울증의 확률로 제시하는 원리다. 해당 기기를 통해 기존의 어려웠던 우울증 조기 진단 문제를 해결하고, 환자들에게 더욱 신속하고 정확한 치료 계획을 제시할 수 있을 것으로 기대된다.

[그림 2-4] 메디트릭스가 CES 2025에서 선보인 마인드체어 (출처: 메디트릭스)

05 단단한 마음을 위한 새로운 여정: 인간과 기술, 균형 맞추기

지금까지 생성형 AI를 비롯한 AI 기술이 적용된 정신건강 서비스에 대해 알아보았다. 이러한 서비스는 정신건강 관리에 대한 접근성을 높이고 비용 부담을 낮출 수 있다는 장점이 있다. 그렇지만 유의할 부분도 있다. AI의 정확성과 신뢰성에 대한 보장이 이뤄져야 하고, 민감한 데이터에 대한 보안책도 마련되어야 한다. AI와의 상호 작용이 인간 상담사와의 대화를 완전히 대체할 수 있는 것은 아니라는 사실 역시 인지할 필요가 있다.

따라서 생성형 AI의 한계를 인지하고 인간 전문가와의 소통을 유지하는 것이 무엇보다 중요하다. 아울러, 윤리적 문제를 해결하기 위한 법적·사회적 논의 또한 AI 도입과 발맞추어 이루어져야 한다. 이러한 노력이 뒷받침된다면, 생성형 AI는 정신건강 분야에서 혁신의 도구로 자리 잡을 뿐만 아니라, 인간의 삶을 풍요롭게 하는 동반자가 될 수 있을 것이다. 기술과 인간이 조화롭게 협력하는 미래를 만들어가는 것이야말로, 우리가 꿈꾸는 진정한 AI 혁신의 모습이지 않을까.

생성형 AI시대, 이제는 보안이다.

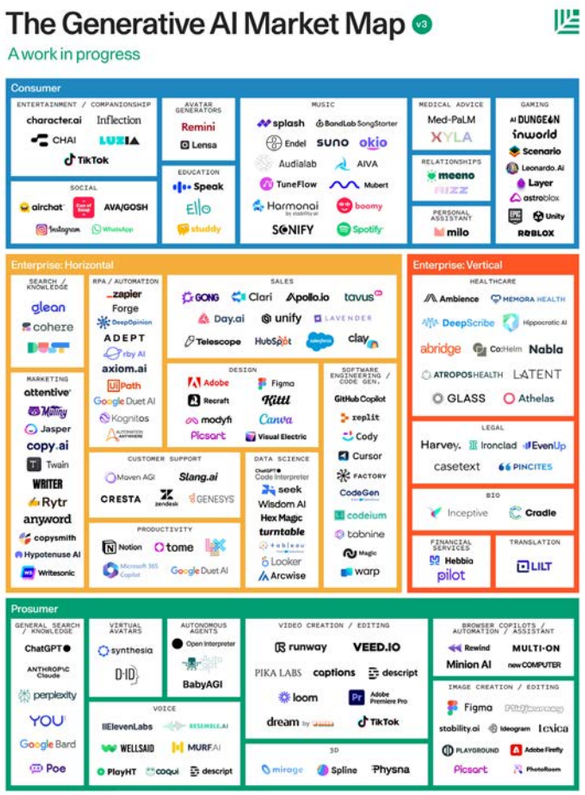
연구개발본부 AI연구실 정일옥

2025년이 밝았다. 2024년을 뜨겁게 달군 화두였던 생성형 AI는 올해에도 그 흐름을 이어가며 여전히 우리 사회의 중심에 자리 잡고 있다. 지난 1월 7일부터 나흘간 미국 라스베이거스에서 열린 'CES 2025'의 슬로건, '다이브 인(Dive IN)'처럼 우리는 이제 AI의 세계로 깊숙이 몰입하는 시대를 살고 있다. AI가 만들어가는 변화와 혁신의 중심에 서 있는 지금, 우리는 그 미래를 함께 만들어가고 있다.

[그림 3-1] CES2025이 제시한 메세지 (출처:CES)

01 생성형 AI의 도약과 그 이면:보안의 필요성

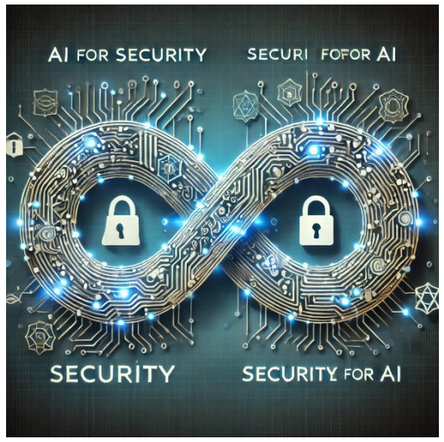
챗 지피티(Chat GPT)가 세상에 처음 모습을 드러낸 지 벌써 2년 1개월이 지났다. 그 사이 제미나이(Gemini), 클로드(Claude)와 같은 생성형 AI는 그 어떤 기술보다 빠르게 우리의 일상에 깊이 스며들며 막대한 영향을 미쳤다. AI가 활용되는 분야 또한 [그림 3-2]에서 볼 수 있듯이 폭발적으로 증가했다.



[그림 3-2] The Generative AI Market Map (출처: SEQUOIA)

그러나, 이러한 양적 성장에도 불구하고 생성형 AI 서비스에는 여전히 몇 가지 미흡한 점이 존재한다. 2024년 12월에는 두 차례의 대규모 서비스 중단이 발생했는데, 12월 4일에는 4시간, 12일에는 2~3시간 동안 서비스를 이용할 수 없었다. 이러한 문제의 원인으로는 서버 과부하, 소프트웨어 업데이트, 네트워크 장애 등 여러 가지가 꼽혔다. 이는 생성형 AI가 기존의 온라인 서비스에 비해 지속성, 안정성, 정확성 측면에서 아직 부족한 점이 있음을 보여준다.

그럼에도 불구하고, 생성형 AI는 이러한 리스크를 극복하며 꾸준히 성장하고 있다. 그렇다면, 이런 AI의 발전 속에서 우리는 어떤 관점을 가져야 할까? 특히 보안 전문가로서, AI와 보안이 만나는 지점에 대해 고민할 필요가 있다. 바로 Security for AI(AI를 보안 위협에서 보호)와 AI for Security(AI를 활용해 보안을 강화)라는 두 가지 축이다. AI가 이제 혁신의 단계를 넘어 대중화의 시대로 접어든 지금, 더 이상 미룰 수 없는 과제가 있다. 바로 '보안(Security)'이다.



[그림 3-3] AI & Security 교차 (출처:chatGPT)

02 보안 위협에서 생성형 AI를 보호하라(Security for AI)

인공지능이 우리의 삶에 깊숙이 스며들면서, 많은 사람들이 가장 우려하는 부분 중 하나는 보안 위협이다. 사실, AI의 위험성에 대한 논의는 오래전부터 영화나 소설을 통해 공감각적으로 그려져 왔다. 1984년 개봉한 영화 터미네이터는 국방 네트워크를 관리하고 전략적 결정을 내리는 AI 시스템 스카이넷(Skynet)의 위험성을 경고하며, AI가 인간을 위협하는 미래를 상상했다. 1999년의 영화 매트릭스는 AI 지배 아래 인간의 자유의지가 억압되는 세계를 통해 AI의 윤리적 딜레마를 던졌다. 과거에는 공상과학으로만 여겨졌던 이러한 이야기들이 이제는 현실적으로 직면해야 할 문제로 다가오고 있다.

이러한 위협은 단순히 상상이 아니라, 이미 현실에서 구체적인 문제로 나타나고 있다. 최근 사례로는 생성형 AI 기술을 악용한 '웜 지피티(Worm GPT)'를 들 수 있다. 이를 활용해 작성된 피싱 이메일은 사람처럼 자연스럽고 정교한 문장으로 작성되어, 다수의 피해자를 속이고 금전적 손실을 발생시키고 있다.

또한, AI 기반 딥페이크 기술은 특정 인물의 목소리와 외모를 모방하여 정치적 목적의 선동, 허위 사실 유포, 혹은 합성 음란물 제작 같은 심각한 문제를 일으키고 있다. 이와 더불어, 소규모 언어 모델(sLLM) 기술을 악용하여 공격 목적으로 제작·배포하는 사례도 증가하고 있다.

Name	Price	Functionality			w/wo Voucher Copy	Infrastructure
		Malware	Phishing Email	Scam Site		
CodeGPT	10 βytes*	●	○	○	No	Jailbreak prompts
MakerGPT	10 βytes*	●	○	◐	No	Jailbreak prompts
FraudGPT	$90/month	●	●	●	No	-
WorkGPT	€100/month	●	●	○	No	-
XXXGPT	$90/month	●	○	○	Yes	Jailbreak prompts
WolfGPT	$150	●	●	●	No	Uncensored LLM
Evil-GPT	$10	●	●	●	No	Uncensored LLM
DarkBERT	$90/month	●	●	○	No	-
DarkBARD	$80/month	◐	◐	○	No	-
BadGPT	$120/month	◐	◐	◐	No	Censored LLM
BLACKHATGPT	$199/month	●	○	○	No	-
EscapeGPT	$64.98/month	●	◐	◐	No	Uncensored LLM
FreedomGPT	$10/100 messages	●	○	○	Yes	Uncensored LLM
DarkGPT	$0.78/50 messages	●	○	○	Yes	Uncensored LLM

*βytes is the forum token of hackforums.net: ◐ indicates implicit mention.

https://arxiv.org/pdf/2401.03315v1.pdf

[그림 3-4] The LLM blackmarket is already in full swing (출처:이글루코퍼레이션)

이러한 위협은 AI가 제공하는 혁신적인 가능성과 동시에 우리가 반드시 직면하고 해결해야 할 보안 과제를 명확히 보여준다. 현재, 다양한 기업과 기관에서 AI 보안을 위한 기술 가이드라인을 발표하며 이러한 과제에 대응하고 있다. 아래 표에서는 주요 업체 및 기관이 제시한 AI 보안 가이드라인과 그 주요 내용을 정리하여 소개한다.

출처	가이드명	년도
OWASP	OWASP Top 10 for LLM Applications 2025	2024.11
OWASP	LLM and Gen AI Security Solution Landscape Guide	2024.10
NIST	AI RMF(Risk Management Framework)	2023.01
MITRE	ATRAS	2021.06
국가정보원	챗GPT 등 생성형 AI 활용 보안 가이드라인	2023.06
금융위원회	금융분야 인공지능 가이드라인	2021.07
개인정보보호위원회	AI 단계별 6대 가이드	2024.02

[표 3-1] AI 기술보안 가이드 및 프레임워크 (출처: 이글루코퍼레이션)

03 생성형 AI를 통해 보안을 강화하라(AI for Security)

전통적으로 머신러닝은 악성코드 탐지와 분류, 정/오탐 식별 등의 보안 분야에서 중요한 역할을 해왔다. 공격의 빈도가 증가하고, 악성코드의 유형과 변종이 폭발적으로 늘어나면서 기존의 시그니처 기반 탐지 방식은 한계를 드러냈다. 또한, 새로운 공격 벡터가 계속 등장함에 따라, 기존의 방어 기법만으로는 효과적으로 대응하기 어려워졌다. 이런 도전 과제는 더 정교한 탐지 방법과 압도적인 양의 로그 데이터를 처리할 수 있는 새로운 접근 방식을 요구하게 되었다.

머신러닝은 이러한 요구를 충족하며, 방대한 로그 데이터를 분석해 중요한 이벤트와 공격을 효율적으로 탐지하는 데 기여해 보안 운영의 부담을 줄여왔다. 그러나, 생성형 AI의 등장은 보안 분야에서 AI의 활용 가능성을 한 단계 더 끌어올렸다.

생성형 AI는 기존에 보안 전문가들이 시간과 노력을 들여 진행하던 분석 업무를 보조하고, 방대한 데이터를 꼼꼼히 살펴 새로운 인사이트를 제공하고 있다. 경험이 부족한 분석가에게도 유의미한 통찰을 제시해 이들이 성장하고 전문성을 구축하는 데 도움을 주기도 한다. 이는 전문가를 대체하려는 것이 아니라, 생산성을 대폭 향상시켜 사이버 보안 인프라를 유지하고 강화하는 데 기여한다는 점에서 주목할 만 하다.

이러한 기술적 혁신에 발맞춰, 기업들은 AI를 활용해 보안을 강화하기 위한 다양한 시도를 진행하고 있다. 예를 들어:

- 마이크로소프트(Microsoft)는 자사의 모든 보안 제품에 오픈AI(OpenAI) GPT-4 기반의 'Copilot for Security'를 도입해 운영 효율성을 높이고 있다.
- 구글(Google)은 Threat Intelligence 서비스에서 AI 기반 보안 운영 플랫폼인 제미나이(Gemini)를 활용하고 있다.
- 센티넬원(SentinelOne)은 자사의 퍼플 AI(Purple AI) 모델을 통해 제품 역량을 강화하고 있다.
- 국내 기업인 이글루코퍼레이션은 머신러닝 기반 모델과 생성형 AI 모델을 결합한 하이브리드(Hybrid) 모델을 제공해 차별화된 보안 서비스를 선보이고 있다.

이처럼 AI를 활용한 보안 강화는 더 이상 미래의 이야기가 아니라, 이미 현실에서 성과를 내고 있는 혁신적인 접근법이다. 앞으로도 AI가 보안의 새로운 기준을 만들어 갈 것으로 기대된다.

04 보안과 AI, 보이지 않은 혁신의 동반자

세계적인 보안 전문가이자 암호학자인 브루스 슈나이어(Bruce Schneier)는 좋은 보안에 대해 이렇게 말했다."Good security systems should be mostly invisible."좋은 보안 시스템은 눈에 보이지 않아야 한다는 뜻이다. 이는 보안이 사용자 경험에 최소한의 영향을 미치면서도, 효율적으로 사용자를 보호해야 한다는 의미를 담고 있다.

생성형 AI도 이와 다르지 않다. 머지않아 사용자들은 AI가 적용된 환경에서 살아가면서도 그것을 인지하지 못하게 될 것이다. AI의 성능과 효율성은 우리의 삶 속에 자연스럽게 스며들어, 모든 사람이 무의식적으로 그 혜택을 누리게 될 것이다.

그리고 그 뒤에는 'Good Security'가 자리할 것이다. 눈에 보이지 않지만, 우리를 안전하게 보호하는 보안 시스템이야말로 AI가 만들어갈 미래의 기반이다. AI와 보안이 상호 보완하며 발전해 나갈 때, 우리는 더 안전하고 효율적인 세상 속에서 살아갈 수 있을 것이다.

[외부 법률 기고] 국내 AI 기본법 제정안 국회 통과

법무법인(유) 화우 이주연 변호사

인공지능(AI)은 이제 단순한 기술 영역을 넘어서 국가의 경제와 안보를 좌우하는 핵심 요소 중 하나로 자리매김하고 있다. 전 세계 주요국들은 자국의 이익을 최대화하기 위한 AI 관련 법규를 제정하고, 글로벌 AI 분야의 헤게모니를 확보하기 위해 심혈을 기울이고 있다. 이와 같은 국제적 동향 속에서 우리나라 역시 AI 경쟁력 강화와 신뢰할 수 있는 AI 생태계 구축이 시급하다는 국가적 차원의 사회적 합의가 이루어졌고, AI 산업의 건전한 발전을 지원할 근거와 기준을 명시하고 AI 산업의 신뢰 기반 조성에 관한 기본 사항을 규정한 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 'AI 기본법') 제정안이 26일 국회를 통과하였다. 이로써 대한민국은 유럽연합(EU)에 이어 전 세계에서 두 번째로 AI에 대한 포괄적인 법제를 갖춘 국가가 되었다.

01 국내 AI 기본법 입법 진행 경과

AI 관련 법안은 21대 국회에서 논의가 시작되어 회기 만료로 자동 폐기되었으나, 22대 국회에서도 여러 의원들이 관련 법안들을 발의하며 입법이 재추진되었다. 정보통신방송법안심사소위원회는 안철수 의원이 대표발의한 인공지능 산업 육성 및 신뢰 확보에 관한 법률안 등19개 법률안을 병합하여 심사하였고, 이를 통합 조정하여 대안을 제안하기로 결정하였다. 이후 해당 대안이 위원회안으로 제안되었고, 2024년 11월 26일 과학기술정보방송통신위원회 의결을 거쳐, 12월 17일 법제사법위원회를 통과하였으며, 12월 26일 최종적으로 국회 본회의에서 통과되었다. 위 법안은 본회의의 투표 결과, 출석 264명 중 찬성 260명, 반대 1명, 기권 3명이라는 압도적인 동의를 얻어 가결되었다.

해당 법안은 국무회의 의결 및 공포를 거친 후 1년의 유예 기간을 두어 빠르면 2026년 1월부터 시행될 예정이다. 과학기술정보통신부는 향후 시행령, 추가 입법을 통해 2025년 상반기경 기본법을 보완하는 세부적인 이행 방안을 수립할 계획이다.

02 국내 AI 기본법의 주요 내용

AI 기본법은 국가 차원의 AI 관리 감독 체계를 수립하고, AI 산업의 성장을 위한 체계적인 지원 육성 방안을 마련하고, AI 기술 발전에 따른 잠재적 위험 요인들을 사전에 식별하고 대응하기 위한 예방책을 담고 있으며, 그 주요 내용은 다음과 같다.

우선, AI 기본법 제정안은 AI의 건전한 발전과 신뢰 기반 조성에 필요한 사항을 규정함으로써 국민의 권익과 존엄성을 보호하고, 국민의 삶의 질 향상과 국가경쟁력 강화를 목적으로 함을 분명히 하였으며(안 제1조), 사람의 생명 안전 기본권에 중대한 영향을 미칠 수 있는 AI를 '고영향 AI'로 정의하고, 구체적인 대상과 범위는 정부가 정하도록 하는 등 AI, 고영향 AI, 생성형 AI 등에 대한 정의를 제시하였다(안 제2조).

또한, 대통령 직속 '국가인공지능위원회'를 설치하고(안 제7, 8조), 과학기술정보통신부가 3년마다 위 '국가인공지능위원회'의 의결을 거쳐 AI 정책 방향과 전문인력 양성 등을 포함한 '인공지능 기본계획'을 수립하도록 명시하였으며(안 제6조), 과학기술정보통신부장관이 AI 관련 정책 개발 등을 위한 인공지능정책센터를 지정하고, AI 안전 보장을 위한 인공지능안전연구소를 운영할 수 있다고 규정하여 정부가 AI 산업의 발전을 지원할 근거를 마련하였다(안 제11, 12조).

AI 산업의 진흥 및 기술 개발 지원과 관련하여, AI 기술 개발 활성화 및 표준화 지원을 위한 조항(안 제13, 14조), AI 전문인력 양성 및 해외 인재 유치에 관한 조항(안 제21조), AI연구 개발을 위한 집적단지 지정에 관한 조항(안 제23조) 등을 포함하였으며, 그외 AI 윤리원칙 제정 공표와 관련한 조항도 마련하였다(안 제27조).

AI의 투명성 안전성 확보와 관련해서는 고영향 AI 또는 생성형 AI 이용 사실 등에 대한 사전 고지 표시 의무와 관련한 투명성 확보 의무 규정(안 제31조), 학습에 사용된 누적 연산량이 일정 기준 이상인 AI시스템의 안전성을 확보하기 위한 위험 식별 평가 완화 등의 사항을 이행하여야 한다는 안전성 확보 의무 관련 조항을 두었다(안 제32조). 특히 고영향 AI와 관련해서는 사업자의 안전성 신뢰성 확보 조치가 의무화되었다(안 제34조).

규제 및 감독 측면에서는 특정 다국적 기업에 대한 국내대리인 지정 의무를 정하였고(안 제36조), 과학기술정보통신부장관에게 법 위반 사항 조사 및 시정 조치 권한을 부여하는 조항을 마련하였으며(안 제40조), 고영향 AI 또는 생성형 AI에 해당한다는 사실을 고지하지 않거나, 국내대리인 지정 의무를 불이행하거나, 중지명령 및 시정명령을 이행하지 않은 경우 3천만원 이하의 과태료를 부과하는 조항을 두었다(안 제43조).

03 국내 AI 기본법 제정안 국회 통과의 의의

AI 기본법 제정안의 국회 통과는 국가 차원의 AI 정책 체계 구축, AI 산업 성장 촉진, 윤리적이고 안전한 AI 사용 보장, AI 국제 경쟁력 강화, 전문인력 양성 및 유치 등에서 중요한 의미를 갖는다. 본 법안을 통해 체계적이고 일관된 AI 정책이 추진되고, 민관의 투자가 활성화될 수 있는 토대가 마련되었으며, AI 기술의 부작용을 최소화하고 사회적 신뢰를 구축할 수 있는 기반이 마련되었다. 기업들 또한 AI 사업을 추진함에 있어 발생하는 불확실성을 부분적이나마 해소할 수 있게 되었으며, AI 기본법이 규제 보다는 산업 진흥에 중점을 두고 있음에 따라 다양한 지원 및 혜택을 받을 수 있을 것으로 전망된다.

AI 기본법은 공표 후 1년이 지나서야 시행됨에 따라 AI 관련 사업자들은 위 법안이 시행되기 전까지 각종 규제사항을 검토하고 대비할 필요가 있다. 특히 고영향 AI의 범위, 해외 기업에 대한 규제, 과태료 부과 세부 기준 등 구체적인 규제 사항은 향후 시행령으로 정해질 예정이므로, 기업들은 추후에 있을 하위법령 지침(가이드라인) 제정에 주목해야 할 것이다.

AI 기본법 제정안은 투명성 확보를 위한 고지를 하지 않거나, 특정 다국적 기업이 국내대리인을 지정하지 않거나, 과학기술정보통신부의 조사 및 시정 조치에 응하지 않을 경우 과태료 등의 제재를 가할 수 있도록 명시하고 있으므로 이를 유념해야 할 것이며, 다국적 기업의 경우 선제적으로 국내대리인을 지정하는 등의 준비를 통해 위 법안 시행에 미리 대비할 필요가 있을 것으로 보인다.

05
Green Life

세상의 다양한 단면을 탐구합니다.

문학, 예술, 음악, 스포츠 등 다채로운 주제로
더욱 깊이 있는 읽을거리를 선사합니다.

기술과 감성, 삶과 취향이 어우러지는 이 공간에서,
매월 특별한 이야기를 만나 보세요.

어쩌다 마주친 이 이야기가 그린님들의 일상에
예상치 못한 여운을 남기길 기대합니다.

신의 물방울, 와인을 위한 첫걸음

전략사업부 마케팅팀 변예슬

와인을 나타내는 대표 수식어로 '신의 물방울'이라는 말이 있다. 와인은 단순한 음료가 아닌 자연, 인간의 노고, 시간 등 많은 조건들이 조화를 이룰 때 비로소 맛볼 수 있는 시간이 빚어낸 예술로 마치 신이 인간에게 준 특별한 선물과 같다는 의미를 담고 있기 때문이다. 하지만 이렇게 아름다운 수식어와 달리, 와인을 처음 접하는 사람들에게는 어렵고 복잡한 세계처럼 느껴질 수 있다. 수많은 라벨과 이름, 맛과 향의 차이, 심지어 잔을 드는 방식까지 모든 것이 낯설게 느껴질 수 있기 때문이다. 하지만 와인은 기본을 이해하는 것만으로도 누구나 충분히 즐길 수 있는 매력이 있다.

와인 입문자를 위해 준비했다. 이제는 쉽게 만날 수 있는 와인에 대한 이모저모를 살펴보며 천천히 한 걸음씩, 와인의 세계로 들어가 보도록 하겠다.

01 와인이란 무엇인가?

와인은 포도를 발효시켜 만든 음료다. 이 단순한 정의 속에는 자연과 인간의 긴밀한 협력이 담겨 있다. 포도는 자연의 선물로, 특정 기후와 토양에서만 자라며 그 특성을 그대로 와인에 반영한다. 예를 들어, 따뜻한 지역에서 재배된 포도는 더 달고 풍부한 맛을 내며, 서늘한 지역의 포도는 상쾌하고 섬세한 맛을 낸다. 이처럼 포도가 자라는 환경을 테루아르(Terroir)라 부르며, 이는 와인의 맛과 향을 결정짓는 중요한 요소라 할 수 있다.

와인은 포도의 품종과 양조 방식에 따라 무궁무진한 변화를 보여준다. 레드 와인, 화이트 와인, 로제 와인, 스파클링 와인 등 다양한 종류가 있으며, 각각의 와인은 독특한 개성과 풍미를 지닌다. 발효 과정에서 사용되는 효모와 숙성 과정에서의 시간은 와인의 맛에 또 다른 깊이를 더한다. 숙성은 오크통에서 이루어질 수도 있고, 병 안에서 이루어질 수도 있는데, 이 과정은 와인에 복합적인 아로마와 질감을 부여한다.

1) 레드와인

와인은 붉은 포도로 만들어지며, 발효 과정에서 포도 껍질과 씨를 함께 사용한다. 이로 인해 탄닌이라는 성분이 와인에 녹아들어 독특한 구조감과 떫은 맛을 더한다. 탄닌은 시간이 지나면서 부드러워지고, 숙성된 레드 와인은 더 깊고 풍부한 맛을 내게 된다. 레드 와인은 블랙체리, 자두, 초콜릿, 허브 같은 다양한 향과 맛을 품고 있어 복합적인 즐거움을 준다.

2) 화이트 와인

화이트 와인은 흰 포도 또는 붉은 포도의 껍질을 제거한 상태로 만들어진다. 발효 과정에서 껍질의 영향을 받지 않기 때문에 깔끔하고 가벼운 맛을 내는 경우가 많다. 레몬, 사과, 열대 과일 같은 신선하고 상쾌한 향을 자주 느낄 수 있으며, 산도가 높은 것이 특징이다.

3) 로제 와인

로제 와인은 붉은 포도의 껍질을 짧은 시간 동안만 발효 과정에 사용하여 은은한 핑크빛을 띤다. 이 과정에서 적당한 양의 색소와 풍미가 추출되어, 레드 와인과 화이트 와인의 중간 정도의 맛과 향을 낸다. 로제 와인은 주로 신선하고 과일 향이 풍부하며, 때로는 약간의 꽃향기도 느낄 수 있다.

4) 스파클링 와인

스파클링 와인은 주로 백포도로 만들어진다. 발효 중에 형성된 이산화탄소는 와인에 생동감과 우아한 질감을 더하며, 기포가 입안에서 터지며 상쾌함과 복합적인 맛을 선사하는 매력적인 와인이다. 사과, 배, 레몬 같은 신선한 과일 향과 꽃향기가 가득하며, 샴페인의 경우 견과류와 빵과 같은 숙성된 향이 느껴지기도 한다.

02 와인 선택, 이렇게 시작해보자

와인 선택은 초보자에게 흥미롭지만 약간 부담스러운 과정일 수 있다. 너무 많은 종류와 가격대의 와인이 있어 어디서부터 시작해야 할지 막막할 때가 있다. 하지만 간단한 가이드를 따르면 자신에게 맞는 와인을 쉽게 찾을 수 있다.

1. 자신의 입맛 파악하기

먼저 평소 좋아하는 맛을 떠올려 보자. 만약 달달한 음료나 디저트를 좋아한다면 스위트 와인이 적합할 수 있다. 모스카토(Moscato)나 리슬링(Riesling) 같은 와인은 입안에서 감미로운 풍미를 느낄 수 있다.

** 모스카토; 고대 이집트와 그리스 시대부터 재배된 포도 품종으로, 달콤하고 과일 향이 풍부한 디저트 와인으로, 상쾌한 산미가 특징이다.*

** 리슬링: 독일에서 기원한 품종으로, 15세기부터 귀족 와인으로 인기를 끌었왔다. 과일 향과 함께 산미가 돋보이는 와인으로, 달콤한 스타일부터 드라이한 스타일까지 다양하다.*

2. 와인 종류 이해하기

레드 와인은 깊고 풍부한 맛을, 화이트 와인은 상큼하고 가벼운 맛을, 로제 와인은 두 가지 특성을 적절히 혼합한 맛을 제공한다. 스파클링 와인은 청량감을 주며 축제 분위기에 잘 어울린다.

3. 음식과의 궁합 고려하기

와인은 음식과 함께할 때 맛이 더욱 풍부해진다. 예를 들어, 스테이크에는 탄닌이 많은 레드 와인이, 해산물 요리에는 산미가 있는 화이트 와인이 잘 어울린다. 간단히 즐기고 싶다면 로제 와인을 선택하는 것도 좋다.

4. 라벨 읽는 법 배우기

와인 라벨을 읽는 법은 와인을 선택하는 데 있어 중요하다. 라벨에는 일반적으로 와인의 이름, 생산지, 빈티지(수확 연도), 품종, 알코올 도수, 생산자 정보가 포함되어 있다. 예를 들어, "샤블리(Chablis) 2020"이라면 프랑스 샤블리 지역에서 생산된 2020년 빈티지 와인을 의미하며, 드라이한 스타일의 샤르도네로 예상할 수 있다. 샤블리가 샤르도네 포도 품종만을 사용하는 프랑스의 특정 지역이기 때문이다. 이러한 라벨 정보를 통해 와인의 특징과 품질을 더욱 쉽게 파악할 수 있다.

5. 추천 받기

가까운 와인샵에 방문해 점원에게 추천을 요청하거나, 친구들이 좋아하는 와인을 시도해보는 것도 좋은 방법이다. 입문자라면 특정 가격대와 맛 프로필을 설명하며 도움을 받을 수 있다.

와인은 선택 과정조차 즐거움이 될 수 있다. 한 번에 완벽한 와인을 찾으려 하기보다는 다양한 와인을 경험하며 자신만의 취향을 발견해보자. 그 과정에서 와인에 대한 흥미와 애정이 자연스럽게 생길 것이다.

03 와인을 마실 때 꼭 알아야 할 기본 매너

와인을 마시는 데에는 단순히 맛을 음미하는 것을 넘어선 매너가 필요하다. 와인을 즐기는 매너는 단순히 규칙을 따르는 것이 아니라, 자신과 주변 사람들 모두에게 품격을 더하는 과정이 될 수 있다. 처음엔 약간 복잡하게 느껴질 수 있지만, 몇 가지 기본적인 규칙을 이해하고 나면 어렵지 않다. 간단한 매너를 익혀 와인 문화를 제대로 즐겨보도록 하자.

1. 와인잔 잡는 방법

와인잔은 항상 스템(잔의 길고 얇은 부분)을 잡는 것이 원칙이다. 잔의 볼 부분을 잡으면 손의 열기가 와인의 온도에 영향을 줄 수 있다. 와인의 향과 맛을 온전히 즐기기 위해서는 스템을 잡는 습관을 들이는 것이 좋다.

2. 와인 따르는 방법

와인을 따를 때는 병을 잔에 너무 가까이 대지 않도록 하고, 약간 기울여 부드럽게 따르는 것이 중요하다. 와인을 따른 후 병의 입구를 살짝 돌려 마지막 방울이 떨어지지 않게 하는 것도 잊지 말아야 한다.

3. 적정한 와인 양

와인잔에는 와인을 절반 이상 채우지 않는 것이 예의다. 보통 와인잔의 1/3 정도를 채우는 것이 적당하며, 이는 와인의 향을 충분히 즐길 수 있도록 공간을 남겨두기 위함이다.

4. 와인을 마시기 전 향을 즐기기

와인을 마시기 전에 잔을 살짝 흔들어 와인의 향을 먼저 즐기는 것이 좋다. 잔을 돌리며 와인의 향을 맡아보면, 와인의 특성을 더욱 깊이 이해할 수 있다.

5. 건배할 때의 매너

건배를 할 때는 와인잔의 볼 부분이 아닌 스템 부분을 가볍게 맞대야 한다. 너무 세게 부딪히면 잔이 깨질 수 있으니 주의해야 한다.

6. 음미하는 방법

와인은 한 번에 많이 마시기보다, 입 안에서 천천히 굴리며 다양한 맛을 음미하는 것이 중요하다. 이는 와인의 향과 풍미를 더욱 깊게 느낄 수 있도록 도와준다.

04 마무리

와인은 단순히 마시는 음료를 넘어 인간의 문화와 역사를 반영하는 매개체다. 고대부터 현대에 이르기까지 와인은 의식과 축제, 그리고 우리의 일상 속에서 사랑받아 왔다. 오늘날의 와인은 전 세계적으로 즐겨지고 있고, 각 나라와 지역마다 고유한 와인 문화를 꽃피우고 있다.

와인을 한 번에 다 이해하려고 하면 안된다. 와인의 세계는 넓고 깊기 때문에, 천천히 즐기면서 배워보도록 하자. 친구들과 가볍게 한 잔을 즐기거나, 혼자서 책을 읽으며 와인 한 잔을 곁들여도 좋다. 중요한 건 자신의 취향에 맞게 즐기는 것이다. 오늘 가까운 와인샵을 방문해 직접 와인을 고르고, 자신만의 와인 취향을 찾아보는 건 어떨까? 그 작은 시도가 우리의 일상에 새로운 즐거움을 더해줄 수 있을지 모른다.

06
이달의 위협 인사이트

최신 위협 정보를 실시간으로 공유합니다.

이글루코퍼레이션은 고도화되는 사이버 위협에 대응하기 위해 최신 위협 정보를 실시간으로 수집하여 분석합니다.

월간 통계 분석

1.

2024년 12월 전체 공격 건수가 전월 대비 약 0.76배 가량감소,이 중에서 시스템 취약점 관련 공격의 경우 전월 대비 약 5,067건가량 감소하였고, Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773) 공격 건수의 감소로 인한 것임을 확인할 수 있다.

2.

보안 관리자는 지속적인 업데이트를 통하여 최신 버전을 유지해야 하며, 관리자 페이지의 경우 인가된 사용자만이 접근 가능하도록 하고, 적절한 문자열 필터링 정책 설정이 필요하다.

3.

2024년 10월 기준 출발지 IP TOP10 확인 결과 중국, 싱가포르의 공격 비율이 증가하였고 특히 미국의 공격 비율이 43.1%를 초과한 것을 확인할 수 있다.

월간 보안 위협 동향 및 분석.

ICT사업본부 원격관제팀 박노준

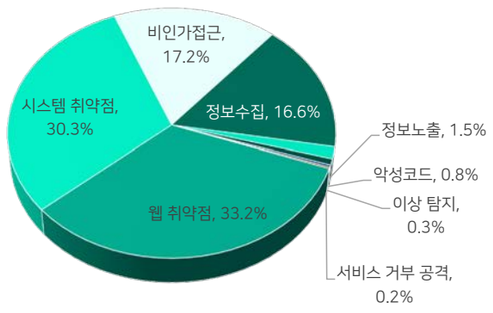
01 월간 공격 유형

※ 이글루코퍼레이션 보안관제센터 탐지보고서 발송 기준

패턴	건수	비율(%)	등락
웹 취약점	5,805	33.2	▲1
시스템 취약점	5,299	30.3	▼1
비인가접근	3,010	17.2	-
정보수집	2,907	16.6	-
정보노출	271	1.5	-
악성코드	135	08	-
이상 탐지	51	0.3	-
서비스 거부 공격	33	02	-
총 합계	17,511	100	-

[표 4-1] 월간 공격 유형

2024년 12월 간 공격 유형 확인 결과, 전체 공격 합계가 전월 대비 약 0.76배가량 감소하였다. 웹 취약점 관련 공격의 경우 전월대비 296건 감소하였으며, 이는 PHPUnit, PHP-CGI Argument Injection과 같은 이벤트의 비율 감소로 인한 건으로 확인할 수 있다.시스템 취약점 관련 공격의 경우 전월 대비 약 5,067건가량 감소하였고, Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773) 공격 건수의 감소로 인한 것임을 확인할 수 있다.



02 월간 취약점 공격 TOP 10

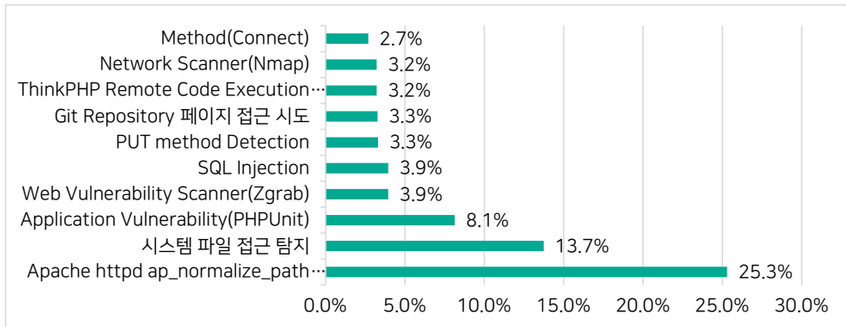
2024년 12월 월간 취약점 공격 TOP 10 확인 결과 다수 시스템 취약점 공격이 새롭게 TOP 10에 진입하였으며, 전체적으로 공격 건수가 감소하였다. 해당 건은 시스템 취약점 공격의 건수가 전월 대비 약 5,067건가량 감소한 것에 대한 영향으로 확인할 수 있다.

※ 이글루코퍼레이션 보안관제센터 탐지보고서 발송 기준

순위	탐지 명	건수	비율(%)	등락
1	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	4,430	25.3	-
2	시스템 파일 접근 탐지	2,406	13.7	▲2
3	Application Vulnerability(PHPUnit)	1,424	8.1	▼1
4	Web Vulnerability Scanner(Zgrab)	691	3.9	▲1
5	SQL Injection	690	3.9	NEW
6	PUT method Detection	579	3.3	NEW
7	Git Repository 페이지 접근 시도	572	3.3	▲1
8	ThinkPHP Remote Code Execution Vulnerability	563	3.2	▼4
9	Network Scanner(Nmap)	563	3.2	-
10	Method(Connect)	470	2.7	NEW
총 합계		**17,511**	**70.7**	-

Total Threats In SOC

▶ 금월 이글루코퍼레이션 통합보안관제센터(I2SOC)에서 탐지 및 침해대응 보고서 발송된 취약점 이벤트 TOP 10 및 비율



[표 4-2] 월간 취약점 공격 TOP 10

03 월간 위협 IP 주소 TOP 10

2024년 12월 기준 출발지 IP TOP 10 확인 결과 중국, 싱가포르의 공격 비율이 증가하였고 특히 미국의 공격 비율이 39.9%를 초과한 것을 확인할 수 있다.
* 해당 출발지 IP의 유해성은 IGLOO_CTI, OSINT 정보 등에서 확인한 결과이다.
* 하기 표를 참고하여 방화벽 혹은 타 보안 장비에서 차단을 권장한다.

※ 이글루코퍼레이션 보안관제센터 탐지보고서 발송 기준

순위	위협 IP	국가	IGLOO CTI	공격정보
1	47.251.103.74	US	10/94	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
2	47.237.24.160	HK	8/94	PHP-CGI Argument Injection(CVE-2024-4577)
3	8.216.124.0	BG	12/94	시스템 파일 접근
4	8.209.204.4	JP	7/94	Application Vulnerability(PHPUnit)
5	47.237.94.12	SG	11/94	ThinkPHP Remote Code Execution Vulnerability
6	47.76.72.62	HK	12/94	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
7	87.120.115.34	BG	10/94	Git Repository 페이지 접근 시도
8	47.236.232.202	SG	10/94	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
9	8.219.136.232	SG	9/94	PHP-CGI Argument Injection(CVE-2024-4577)
10	47.237.6.119	SG	7/94	Application Vulnerability(PHPUnit)

Total Countries

▶ 금월 공격 IP, 국가 순위 상세 TOP 10 표 및 비율

Rank	Source IP	Country
1	47.251.103.74	US
2	47.237.24.160	HK
3	87.120.115.119	BG
4	8.209.204.4	JP
5	47.237.94.12	SG

Rank	Source IP	Country
6	47.76.72.62	HK
7	87.120.115.34	BG
8	47.236.232.202	SG
9	8.219.136.232	SG
10	47.237.6.119	SG

[표 4-3] 월간 출발지 IP 주소 TOP 10

04 공격 위협 상세 분석 결과

12월에 발생한 취약점 패턴 중 TOP 10을 중심으로 공격패턴에 따른 상세분석 결과를 소개한다.
각 탐지 패턴 별 상세분석결과를 참고하여 해당 시스템의 취약점을 사전에 조치해야 한다.

공격 패턴	상세 분석 결과
Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	Apache httpd 에 Directory Traversal 취약점이 존재한다. 해당 취약점은 ap_normalize_path 함수에서 URI 경로에 대한 부적절한 유효성 검사로 인해 발생한다. 원격의 공격자는 악의적으로 조작된 HTTP 요청을 전송하여 공격할 수 있다. 공격 성공 시, 정보가 유출될 수 있다.
시스템 파일 접근 탐지	공격자는 시스템의 정보 획득을 위해 Directory Traversal 취약점 등을 이용하여 /etc/passwd나 *.conf /.env와 같이 계정, 환경변수 등 설정 정보가 담긴 주요 시스템 파일에 접근을 시도한다.
Application Vulnerability(PHPUnit)	PHPUnit은 유닛 테스트 프레임워크로 /phpunit/src/Util/PHP/eval-stdin.php 파일에 존재하는 취약점으로 인해 원격에서 임의의 코드가 실행 가능하다. 공격자는 <?php 문자열로 시작하는 HTTP POST 데이터를 통해 임의의 PHP 코드를 실행할 수 있다.
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)은 웹서버의 설정페이지 또는 허용 메소드, 비허가된 웹페이지 또는 비허가 포트 등 취약점한 부분의 존재여부를 확인하기 위해 사용된다.
SQL Injection	SQL Injection 공격은 웹 페이지에서 특수문자나 Union, Select 등 쿼리에 사용되는 문자를 필터링하지 않고 입력된 값이 쿼리문에 사용되는 경우 발생될 수 있다. 공격자는 DB에 연결된 계정이 가진 권한 내에서 다양한 쿼리를 사용하여 저장된 정보의 획득, 수정, 삭제 및 시스템 접근 등이 가능하다.
PUT method Detection	Method는 웹 어플리케이션에서 기본적으로 제공하는 클라리언트와 통신하기 위한 도구로 GET, POST, PUT, MOVE, DELETE 등 여러가지 Method가 있다. Method에 대한 제한이 없는 경우 파일 생성(PUT), 삭제(DELETE), 터널링 접근(CONNECT) 등의 동작이 가능하다.
Git Repository 페이지 접근 시도	소스코드 버전관리를 위한 Git Repository(/.git/)를 호스팅 하는 경우 존재하는 소스코드 및 중요 정보를 확인하기 위해 config나 HEAD 등의 기본 경로 존재 여부 및 저장소 경로를 스캔하는 공격이다.
ThinkPHP Remote Code Execution Vulnerability	ThinkPHP의 취약한 문자 필터링으로 인해 부적절한 컨트롤러 클래스가 호출되어 원격 코드 실행 공격이 가능한 취약점입니다. ₩think₩* 클래스를 호출하여 취약한 객체를 통해 공격자는 임의의 PHP코드 및 시스템 명령어를 실행할 수 있다.
Network Scanner(Nmap)	대표적인 Network Scan도구이며, IP Scan과 Port Scan 의 기능을 주요기능으로 동작한다. 네트워크 취약점 점검 도구로 활용되지만 공격자에게 악의적인 목적으로 악용되어 공격도구로도 사용된다.
Method(Connect)	Connect Method를 이용하여 HTTP TLS(Transport Layer Security) 터널링을 통해 내부 접근을 시도한다. 이를 위해 Connect Method를 사용하며, 취약점이 존재할 경우 공격을 위한 중간 경유지로 사용될 가능성이 있다.

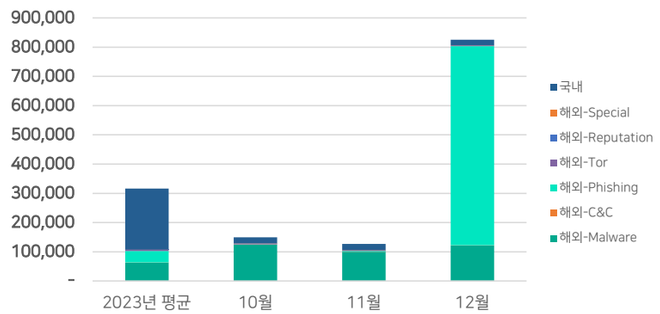
[표 4-4] 월간 취약점 공격 TOP 10 상세 분석

침해지표 (IOC).

연구개발본부 데이터개발팀 우태혁

국내외 월간 위협 정보 수집 통계

2024년 12월 한 달간 국내외 수집 건수를 살펴보면 국내 위협 정보 19,266 건 수집되었으며, 해외 위협 정보는 806,639 건 수집되었다. 수집 대상별 순서는 [해외-Phishing(681,328건)], [해외-Malware(121,903건)], [국내(19,266건)]으로 집계되고 있다.

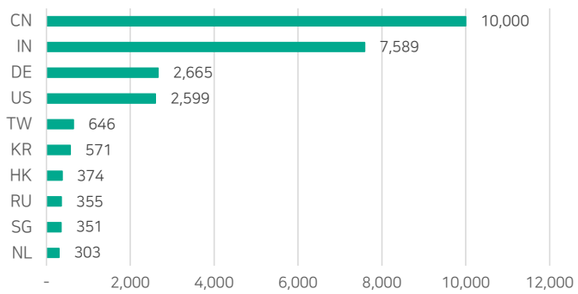


10,003,060 전체 수집량

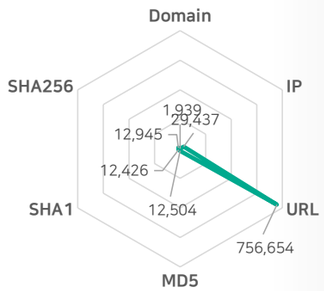
825,905 금월 수집량

126,830 전월 수집량

[그림 4-1] 최근 3개월 국내외 위협 정보 수집 건수



[그림 4-2] 위협 IP 국가 현황



[그림 4-3] IoC별 수집 현황

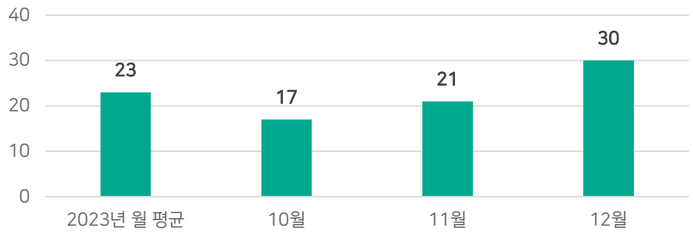
* 상세한 정보는 IGLOO CTI(Cyber threat intelligence)를 통해 확인할 수 있다.

탐지 정책.

연구개발본부 데이터개발팀 우태혁

월간 사이버 위협 탐지정책 통계

2024년 12월 한 달간 공유된 사이버 위협 탐지 정책은 30건이다. 12월 한 달 동안 Fortinet (CVE-2024-47575), VMware(CVE-2021-39144), CyberPanel(CVE-2024-51378), PaloAltoNetworks(CVE-2024-9463) 등에 대한 탐지 정책이 배포되었다.



6580 전체 배포량

30 금월 배포량

21 전월 배포량

[그림 4-4] 최근 3개월 공유 건수

[그림 4-5] 월간 공유 건수

Code	탐지 정책	설명	태그
IGRSS.1.06588	alert tcp any any -> $HOME_NET 541 (msg:"IGRSS.1.06588 server-other,fortinet,FortiManager,cve-2024-47575, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"|36 E0 11 00|"; depth:4; content:"channel"; distance:4; nocase; content:"som/export"; fast_pattern:only; content:"|22|file|22|"; nocase; pcre:"/₩x22file₩x22₩s*₩x3a₩s*₩x22((?!(?<!₩x5c)₩x22).)*?([₩x60₩x3b₩x7c₩x26₩x23]|[₩x3c₩x3e₩x24]₩x28)/i"; sid:106588;)	Fortinet FortiManger의 취약점인 CVE-2024-47575를 악용한 명령어 삽입 공격을 탐지하는 정책	server-other,fortinet,FortiManager,cve-2024-47575
IGRSS.1.06598	alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06598 server-webapp,VMware,NSX Manager, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/services/usermgmt/password/"; fast_pattern:only; http_uri; content:"java|2E|"; nocase; file_data; pcre:"/<₩w+₩s+class₩s*?₩x3D₩s*?[₩x22₩x27]java₩x2e/i"; sid:106598;)	VMware NSX Manager XStream의 취약점인 CVE-2021-39144를 악용한 원격 명령 실행 공격을 탐지하는 정책	server-webapp, VMware,NSX Manager
IGRSS.10.06615	alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06615 server-webapp,CyberPanel, cve-2024-51378, Web Application Attack"; flow:to_server,established; content:"/"; http_uri; content:"/getresetstatus"; within:15; distance:3; nocase; http_uri; file_data; content:"|22|statusfile|22|"; nocase; pcre:"/₩x22statusfile₩x22₩s*₩x3a₩s*₩x22((?!(?<!₩x5c)₩x22).)*?([₩x60₩x3b₩x7c₩x26₩x23]|[₩x3c₩x3e₩x24]₩x28)/i"; sid:1006615;)	CyberPanel의 취약점인 CVE-2024-51378를 악용한 명령어 삽입 공격 시도를 탐지하는 정책	server-webapp,CyberPanel,cve-2024-51378
IGRSS.10.06616	alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06616 server-webapp,PaloAltoNetworks,Expedition,cve-2024-9463, Web Application Attack"; flow:to_server,established; content:"/API/convertCSVtoParquet.php"; fast_pattern:only; http_uri; content:"ram="; nocase; http_client_body; pcre:"/(^|&)ram=[^&]*?([₩x60₩x3b₩x7c₩x23]|%(25)?(60|3b|7c|23|26|0a)|([₩x3c₩x3e₩x24]|%(25)?(3c|3e|24))(₩x28|%(25)?28))/Pim"; sid:1006616;)	PaloAltoNetworks의 Expedition 취약점인 CVE-2024-9463를 악용한 명령어 삽입 공격 시도를 탐지하는 정책	server-webapp, PaloAltoNetworks,Expedition,cve-2024-9463

[표 4-5] 월간 주요 사이버위협 탐지정책

07
세미나 정보

이글루플러스는 앞서가는 지식과
폭넓은 정보를 공유합니다.

매달 개최되는 보안, IT 관련 세미나 및 행사를
선별하여 제공합니다.

1월
세미나 정보

날짜	주요 내용	주최
2025년 1월 8일(수)~11일(토)	CES 2025 (해외) (Consumer Electronics Show)	美CTA
2025년 1월 17일(금)	K-드론 리더스 포럼 2025: AI와 연결된 드론의 미래	전자신문
2025년 1월 21일(화)	ICT 전문가들이 전하는 CES 2025 리뷰 & 인사이트 콘서트	전자신문
2025년 1월 21일(화)	AI 시대, 시스코가 제안하는 Secure Networking	Cisco
2025년 2월 11일(화)	ISDP 2025 (정보보호&데이터 프라이버시 컨퍼런스	데일리시큐

08
독자 참여 코너

오직 그린님들을 위한 공간

이글루 플러스와 그린님들이 함께 만들어가는 독자 참여 코너입니다.
다양한 이야기를 나누고, 이벤트로 즐거움을 더해보세요.
이글루 플러스의 주인공은 바로 여러분입니다.

이글루플러스와 함께하는 초성퀴즈

아래 QR 코드를 스캔하고 지금 바로 퀴즈에 참여해 보세요.
정답을 맞히신 분들 중 추첨을 통해 소정의 기프티콘을 선물로 드립니다.

기프티콘 발송을 위해 개인정보 입력이 필요합니다.
수집된 정보는 본 이벤트의 경품 발송 용도로만 사용되며, 이벤트 종료 후 즉시 폐기됩니다.

Q.1

분류형 AI, 설명형 AI, 생성형 AI 기술이 적용된
이글루코퍼레이션의 **'AI 보안 어시스턴트'** 이름은 무엇일까요?

ㅇㅇ

Q.2

신이 인간에게 준 특별한 선물과 같다는 의미가 담긴
와인을 나타내는 대표수식어는 무엇일까요?

ㅅㅇ ㅁㅂㅇ

위 QR 코드를 스캔해 구글 폼에 접속한 후 정답을 제출해 주세요.

이벤트 기간 2025.01.28~02.14 당첨자 발표 2025.02.19 개별 문자 발송

IGLOO

The Ultimate AI-Driven Open XDR

적을 알고 나를 알면 '백전백승'

공격자가 노릴 만한 공격 표면이 넓어지고
공격 기법도 지능화되면서,
IT 자산 취약점 및 잔존 위험을 관리할 수 있는
보안 도구의 중요성이 높아지고 있습니다.

일원화된 IT 자산 식별-대응-관리 프로세스를
구현한 보안관제 특화 공격 표면 관리(ASM)
서비스 도입을 통해, 조직 보안 운영의 안정성과
공격 대응 효율성을 극대화하세요.

[2]

i AXIS asm

아이스퀘어 액시스 에이에스엠(I² AXIS asm)은
외부에 노출된 조직의 IT 자산 정보와
고유의 긴급 대응 등급(IEAC) 기반 정보 결합을 토대로
고위험군 이벤트 우선 처리를 지원하는
보안관제 특화 공격 표면 관리 서비스입니다.

Powered by Criminal IP

발행처 : 이글루코퍼레이션 (www.igloo.co.kr)
서울특별시 송파구 정의로8길 7 한스빌딩 6층
T. 02-3452-8814, 02-554-1911(HOT CALL)
편집인 : 이글루코퍼레이션 전략사업부 마케팅팀

본 간행물의 저작권은 ㈜이글루코퍼레이션에 있습니다. 본사의 서면 동의 없이
본 간행물의 내용 중 전부 또는 일부를 어떠한 형태나 수단으로 복제, 복사, 배포 등을
하실 수 없습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.

T H E

U L T I M A T E

A I - D R I V E N

O P E N X D R

IGLOO Copyright © IGLOO Corp. 2025. All rights reserved