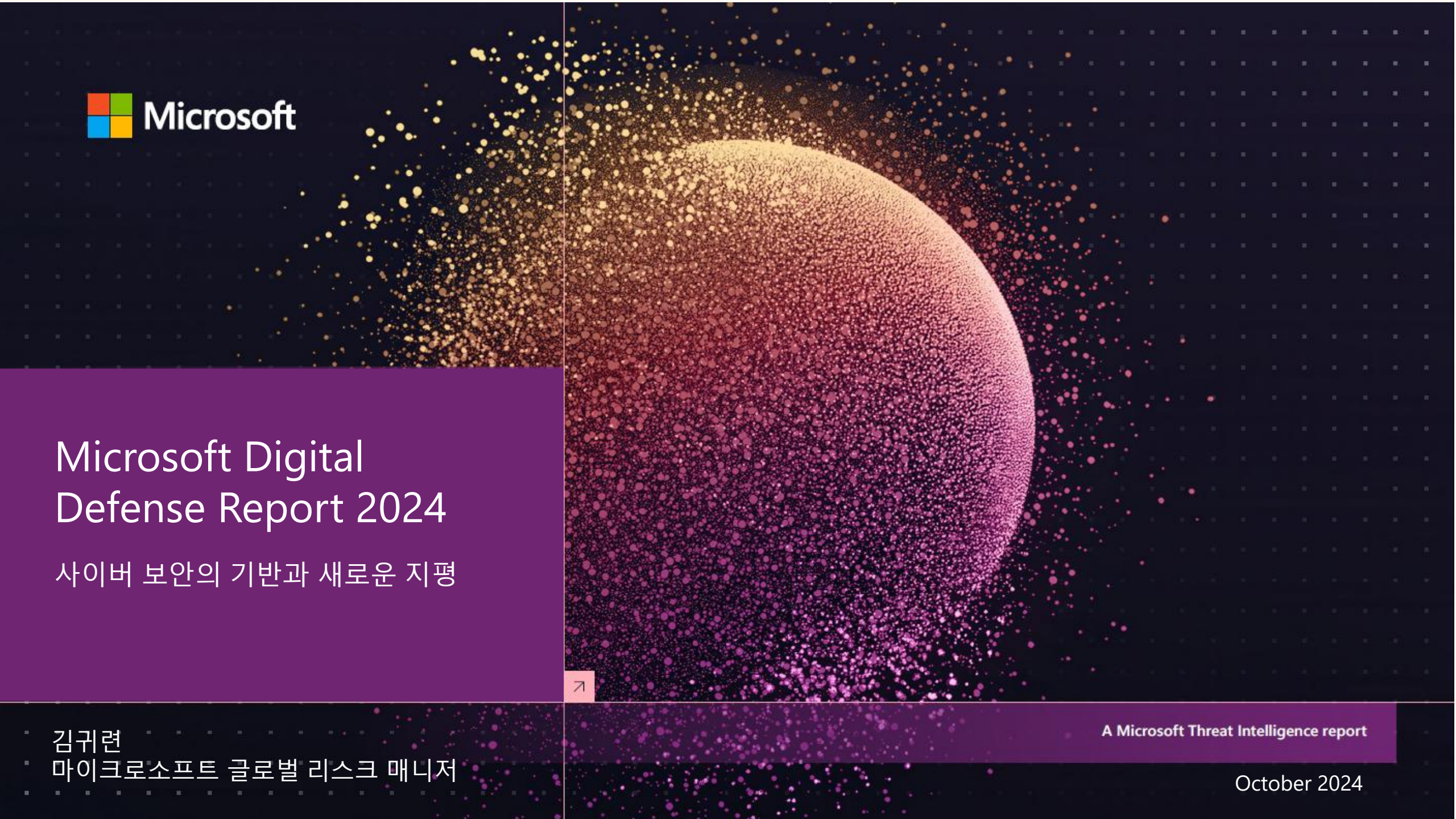


Microsoft Digital Defense Report 2024

사이버 보안의 기반과 새로운 지평

김귀련
마이크로소프트 글로벌 리스크 매니저

A Microsoft Threat Intelligence report

October 2024

디지털 생태계에서의 입지를 바탕으로 사이버 보안의 주요 동향을 관찰할 수 있습니다. 사이버 보안에 대한 Microsoft의 관점은 50년간의 경험과 인사이트를 통해 구축되었습니다.

사회 | Microsoft 이해 관계자 | Microsoft 고객

Microsoft의 고유한 관점

Microsoft는 전 세계적으로 수십억 명의 고객에게 서비스를 제공하므로 광범위하고 다양한 기업, 조직 및 소비자의 보안 데이터를 집계할 수 있습니다.

매일 13조 건의 보안 신호 추가 처리

2023: 65조, 2024년: 78조

디지털 위협과 범죄 사이버 활동을 이해하고 보호하기 위해 클라우드, 엔드포인트, 소프트웨어 도구, 파트너 에코시스템에서 발생하는 비용입니다.

1,500개의 고유 위협 그룹 추적

Microsoft Threat Intelligence는 현재 600개 이상의 국가 위협 행위자 그룹, 300개 사이버 범죄 그룹, 200개 영향력 운영 그룹 및 기타 수백 개를 포함하여 1,500개 이상의 고유 위협 그룹을 추적하고 있습니다.

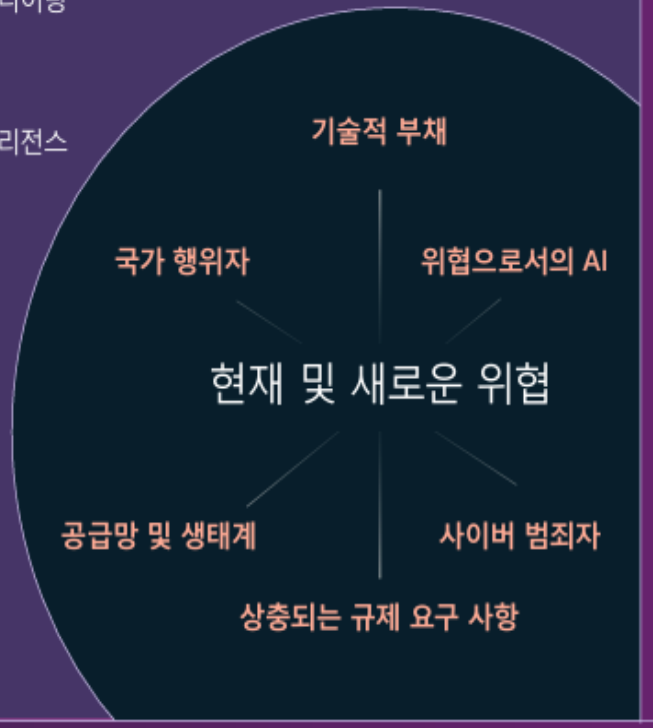
Microsoft의 사이버 보안 접근 방식

Microsoft 보안 투자

- AI 레드 팀
- 민주주의 수호
- 감지 및 대응
- 디지털 범죄
- 디지털 안전
- 인시던트 대응
- 국가 안보
- 물리적 보안
- 대중 인식 및 교육
- 책임 있는 AI
- 보안 엔지니어링
- 보안 운영
- 위협 분석
- 위협 인텔리전스

34,000명의 전담 보안 엔지니어

디지털 기술 역사상 최대 규모의 사이버 보안 엔지니어링 프로젝트에 풀타임으로 투입된 인원의 수입니다.



복잡하고, 도전적이며, 점점 더 위험해지는 상황

- 매일 6억 건 이상의 공격
- 도전에 맞서기 위해: 개별 사용자부터 경영진까지 사이버 방어에 대한 집중과 철저한 실천
- 사이버 공격을 억제하기 위해 정부 조치와 병행
- AI 기반 사이버 보안의 발전으로 방어 균형 제공
- "모두가 참여하는" 과제

"This is a consequential time."

Satya Nadella, Microsoft CEO

The 2024 Microsoft Digital Defense report

Chapter 1
진화하는 사이버 위협 환경

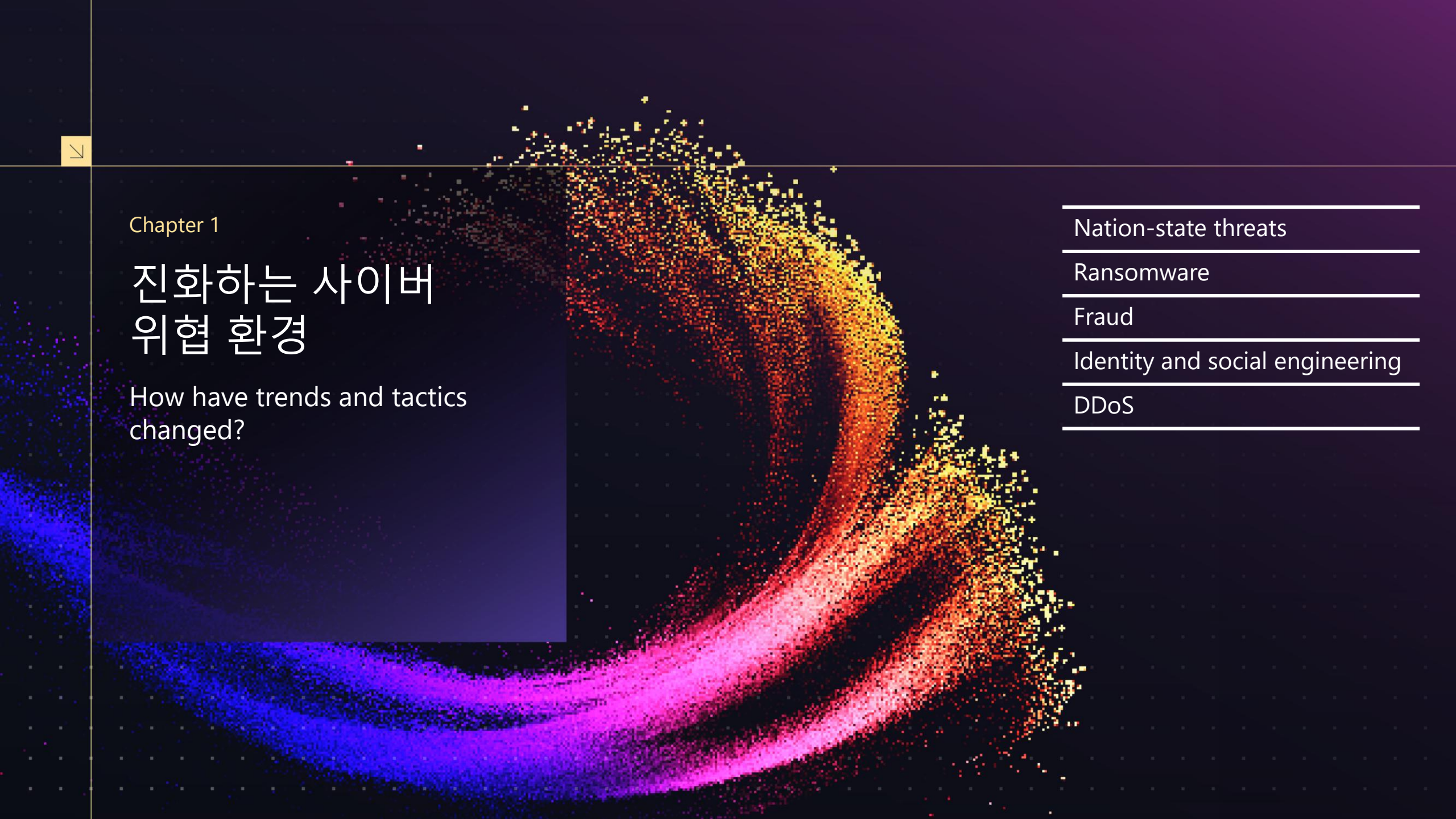
- Nation-state threats
- Ransomware
- Fraud
- Identity and social engineering
- DDoS
- Space

Chapter 2
보안 중심 기반

- Secure Future Initiative
- Strategic cybersecurity
- Incident response
- Critical environments

Chapter 3
AI가 사이버 보안에 미치는 영향

- Key insights
- Emerging attack techniques
- Nation-state threat actors and AI
- AI for defense
- Security operations efficiencies
- Governments and industries advancing global AI security



Chapter 1

진화하는 사이버 위협 환경

How have trends and tactics changed?

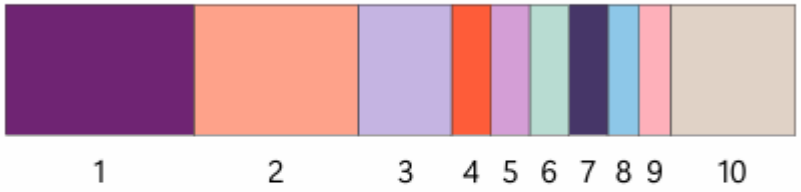
- Nation-state threats
- Ransomware
- Fraud
- Identity and social engineering
- DDoS

숫자로 보는 국가 간 위협 활동

- 국가와 연계된 위협 행위자들은 광범위한 지정학적 분쟁에서 지속적인 지원 역할을 수행했다.
- **교육 및 연구** 부문은 국가 위협 행위자 가운데 두 번째로 가장 많은 표적이 되었습니다.
  : 실제 타겟을 공격 하기 전에 테스트 장소로 사용

러시아, 중국 이란, 북한의 위협 행위자들은 정부 및 기타 민감한 조직에 대한 공급망 공격을 수행하기 위해 IT 제품 및 서비스에 대한 액세스를 추적했습니다.

전 세계 상위 10개의 표적 부문



분야		백분율
1	IT	24%
2	교육 및 연구	21%
3	정부 기관	12%
4	싱크탱크 및 NGO	5%
5	운송	5%
6	고객 소매유통업	5%
7	재무	5%
8	제조업	4%
9	통신	4%
10	그 외 기타	16%

Source: Microsoft Threat Intelligence

국가 조직 위협 행위자들: 러시아, 중국

Russia

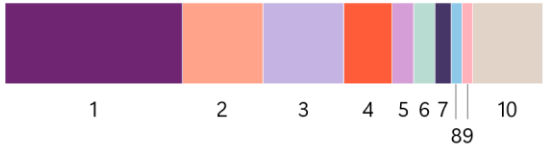
Nation-state threat actor activity

Targeting by region

Sector		Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Approximately 75% of targets were in Ukraine or a NATO member state, as Moscow seeks to collect intelligence on the West's policies on the war. Ukraine remains the country most targeted by Russian actors.

Most targeted sectors



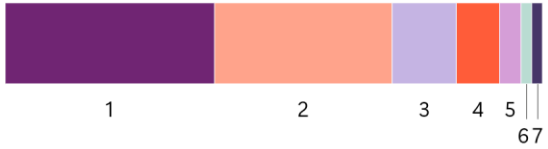
Sector		Percentage
1	Government	33%
2	IT	15%
3	Think tanks and NGOs	15%
4	Education and Research	9%
5	Inter-governmental organization	4%
6	Defense Industry	4%
7	Transportation	3%
8	Energy	2%
9	Media	2%
10	All others	13%

Russian actors focused their targeting against European and North American government agencies and think tanks, likely for intelligence collection related to the war in Ukraine. Actors like Midnight Blizzard also targeted the IT sector, suggesting it was in part planning supply-chain attacks to gain access to these companies' client's networks for follow-on operations.

China

Nation-state threat actor activity

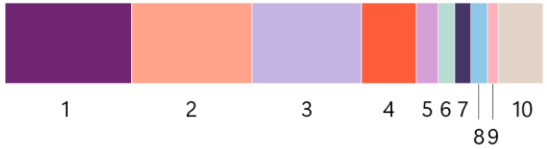
Targeting by region



Sector		Percentage
1	East Asia & Pacific	39%
2	North America	33%
3	Europe & Central Asia	12%
4	Latin America & Caribbean	8%
5	South Asia	4%
6	Middle East & North Africa	2%
7	Sub-Saharan Africa	2%

Chinese threat actors' targeting efforts remain similar to the last few years in terms of geographies targeted and intensity of targeting per location. While numerous threat actors target the United States across a wide variety of sectors, targeting in Taiwan is largely limited to one threat actor, Flax Typhoon.

Most targeted sectors



Sector		Percentage
1	IT	24%
2	Education and Research	22%
3	Government	20%
4	Think tanks and NGOs	10%
5	Manufacturing	4%
6	Defense Industry	3%
7	Communications	3%
8	Finance	3%
9	Transportation	2%
10	All others	9%

Most Chinese threat activity is for intelligence collection purposes and was especially prevalent in ASEAN countries around the South China Sea. Granite Typhoon and Raspberry Typhoon were the most active in the region, while Nylon Typhoon continued to target government and foreign affairs entities globally.

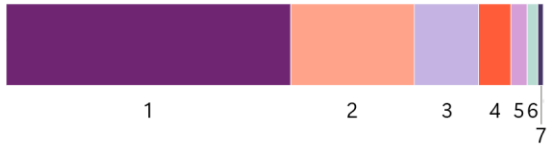
Source: Microsoft Threat Intelligence

국가 조직 위협 행위자들: 이란, 북한

Iran

Nation-state threat actor activity

Targeting by region



	Sector	Percentage
1	Middle East & North Africa	53%
2	North America	23%
3	Europe & Central Asia	12%
4	South Asia	6%
5	East Asia & Pacific	3%
6	Latin America & Caribbean	2%
7	Sub-Saharan Africa	1%

Iran placed significant focus on Israel, especially after the outbreak of the Israel-Hamas war. Iranian actors continued to target the US and Gulf countries, including the UAE and Bahrain, in part because of their normalization of ties with Israel and Tehran's perception that they are both enabling Israel's war efforts.

Most targeted sectors

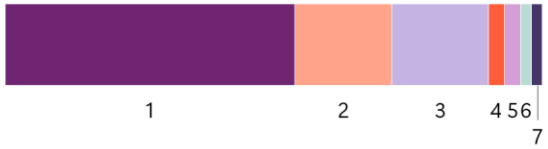
	Sector	Percentage
1	Education and Research	19%
2	IT	11%
3	Government	7%
4	Transportation	6%
5	Finance	4%
6	Communications	4%
7	Energy	3%
8	Commercial Facilities	3%
9	Manufacturing	3%
10	All others	42%

Iranian targeting focused on education, IT, and government as part of strategic intelligence collection. Iranian actors often target the IT sector to gain access to downstream customers, including those in government and the defense industrial base (DIB). "Other" includes media and think tanks or NGOs, which Iran often targets to gain insights into dissidents, activists, and persons who can impact policymaking.

North Korea

Nation-state threat actor activity

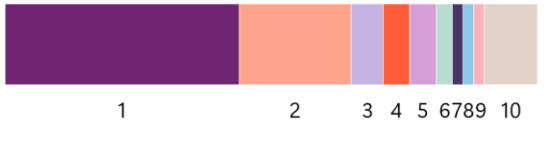
Targeting by region



	Sector	Percentage
1	North America	54%
2	East Asia & Pacific	18%
3	Europe & Central Asia	18%
4	Latin America & Caribbean	3%
5	Middle East & North Africa	3%
6	South Asia	2%
7	Sub-Saharan Africa	2%

The United States remained the most heavily targeted country by North Korean threat actors, but the United Kingdom rose up the ranks this year to second place. The "Other" category comprised 44 other countries targeted by North Korean threat actors.

Most targeted sectors



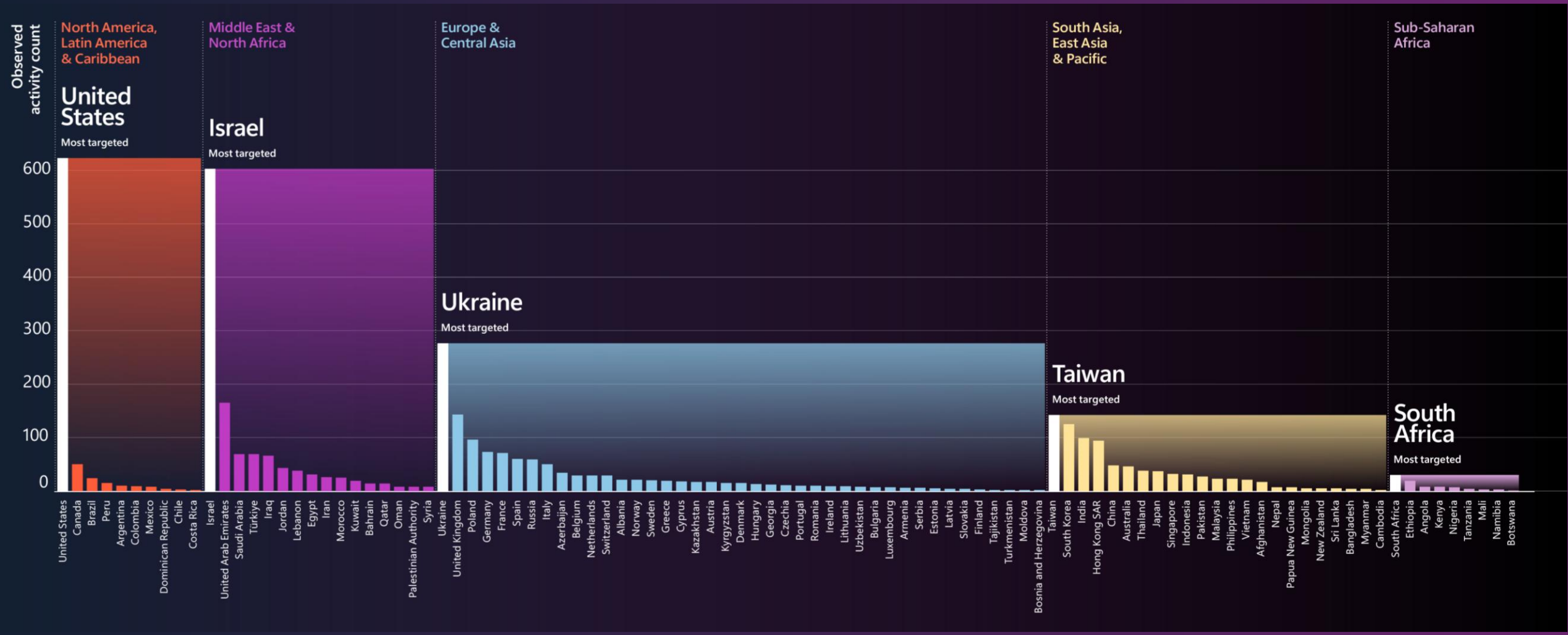
	Sector	Percentage
1	IT	44%
2	Education and Research	21%
3	Manufacturing	6%
4	Consumer Retail	5%
5	Finance	5%
6	Think tanks and NGOs	3%
7	Communications	2%
8	Government	2%
9	Health	2%
10	All others	10%

North Korean threat actors targeted the IT sector the most, particularly to conduct increasingly sophisticated software supply chain attacks. They also continued to heavily target experts in the education sector for intelligence collection. The "Other" category comprised seven other sectors.

Source: Microsoft Threat Intelligence

국가 주도 위협 행위자들의 주요 표적이 된 국가들

Regional sample of activity levels observed



Source: Microsoft Threat Intelligence data

선거 개입

러시아:
- Pro-Trump, Anti-Ukraine 콘텐츠
- 미국 선거 관련 뉴스 사이트들이 콘텐츠 생성에 AI를 활용

이란:
- AI를 활용해 분열을 조장하는 콘텐츠를 배포하는 은밀한 뉴스사이트 네트워크 운영
- 대통령 선거 캠페인을 표적으로 삼아 영향력을 행사하고 비방 정보를 유출하려는 작전 수행

중국:
- 트럼프와 해리스/바이든 모두를 비판
- 미국 대중을 분열적인 정치 이슈에 끌어들이려는 활동

Election-related influence operations timeline

China (December 22, 2023)
PRC-linked influence actor Taizi Flood uses AI-generated audio files to allege then Taiwanese Democratic Progressive Party presidential candidate was an informant in the 1980s.

China (January 13, 2024)
Taizi Flood promotes faked AI-generated audio recording of former presidential candidate and Foxconn founder Terry Gou endorsing then Taiwanese Nationalist Party presidential candidate Hou Yu-ih.

Russia (February 23, 2024)
Russia-affiliated actor Ruza Flood registers a series of US election-themed news websites. The websites are amplified over social media by inauthentic accounts using website redirect networks to mask the actors' infrastructure and likely use AI tools to generate content.

Russia (April 19, 2024)
Russia-affiliated influence actor Storm-1516 produces fake video that attempts to frame Ukraine for interference in the 2024 US presidential election.

China (May 2024)
Sophisticated PRC-linked sockpuppet accounts position on new social media platforms to spread divisive messaging, particularly surrounding protests on US college campuses ahead of the US presidential election.

Iran (June 15, 2024)
Iran sends spear phish to presidential campaign, likely in preparation stage for influence operations targeting the US elections. (Source: Microsoft data)

China (July 2024)
July 10: Deceptively edited short-form video from PRC-linked sockpuppet account masquerading as US conservative voter reaches 1.5 million views.

July 13: PRC state media foment speculation of "deep state involvement" in Trump attempted assassination.

Presidential elections
Taiwan
Jan 2024

Presidential elections
US
Nov 2024

On the right are key elections the influence actors were likely seeking to influence.
The flags represent the nation-state affiliation of observed influence actors.

Source: Microsoft Threat Analysis Center

랜섬웨어 트랜드와 인사이트

2.75x

사람이 운영하는 랜섬웨어 관련 사건의 연간 증가율

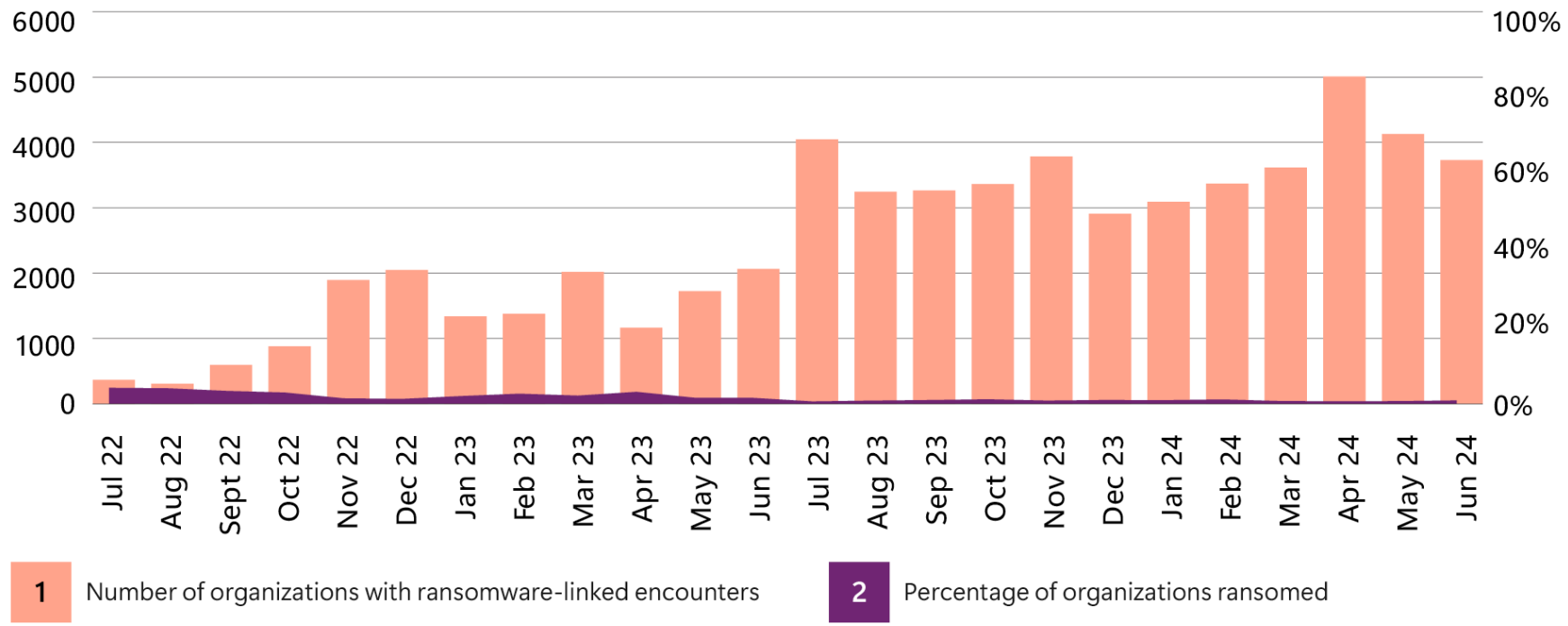
92%

의 성공한 랜섬웨어 공격은 네트워크에 연결된 관리되지 않은 디바이스 이용

3x

지난 2년 동안 랜섬웨어 공격이 암호화 단계에 도달한 비율은 3분의 1로 감소

랜섬웨어 관련 사건을 경험한 조직의 수는 계속 증가하고 있지만, 실제로 랜섬웨어 피해를 입은 조직의 비율은 감소하고 있다.(2022년 7월 ~ 2024년 6월)



랜섬웨어 관련 사건을 경험하는 조직의 수는 계속 증가하고 있지만, 실제로 랜섬웨어에 의해 암호화 단계까지 이른 조직의 비율은 같은 기간 동안 3배 이상 감소했습니다.

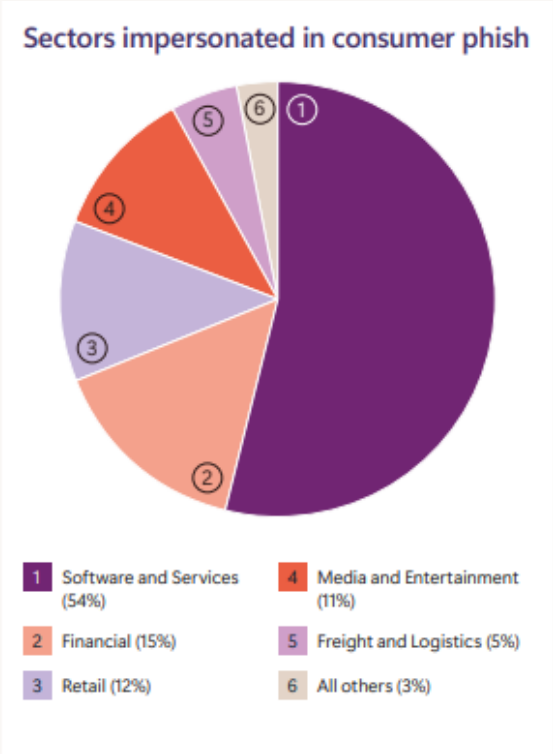
Source: Microsoft Defender for Endpoint

사기 수법과 동향: 사칭

Deepfakes

딥페이크가 비즈니스 환경에서 더 흔해짐에 따라, 조직들은 거래 시 추가적인 인증을 요구하는 등의 대응책을 도입해야 할 것입니다

Corporate impersonation



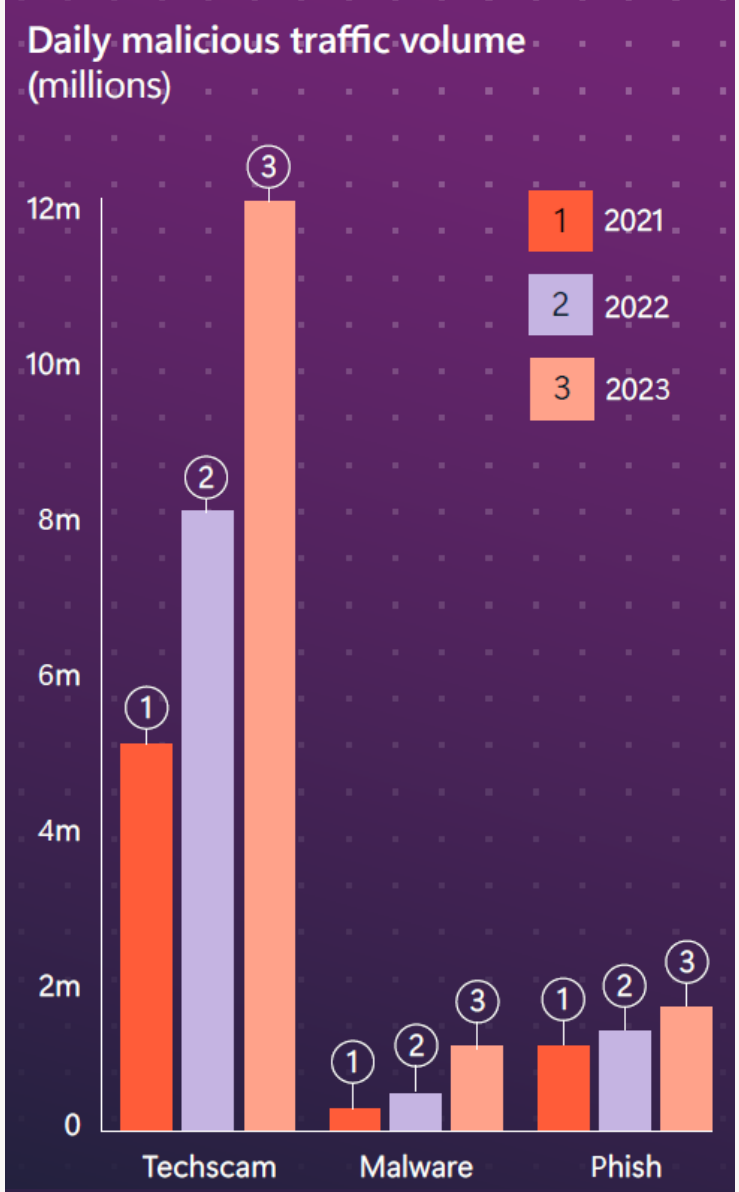
Account takeovers(ATO)

대부분의 계정 탈취(ATO)는 여전히 패스워드 스프레이, 키로깅, 웹에서 발견된 이전 공격의 비밀번호를 사용하는 등 단순한 방법으로 발생되고 있습니다.

Techscam*

>70% 이상은 2시간도 채 활동하지 않으며, 이는 탐지되기 전에 사라질 수 있다는 것을 의미합니다.

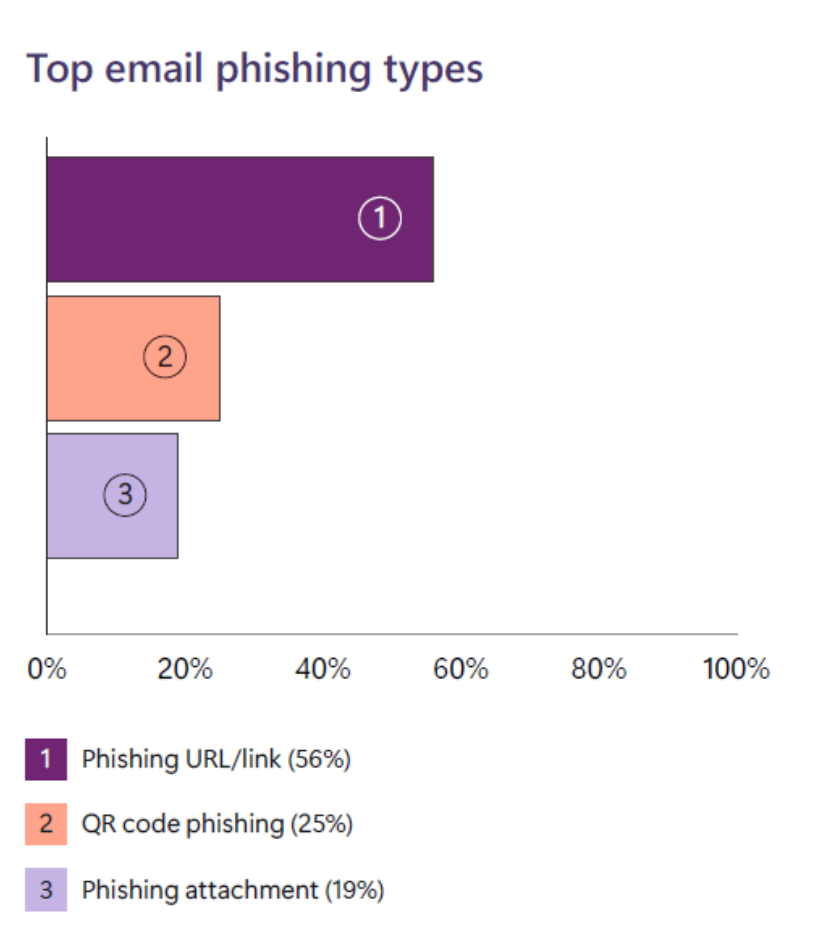
*Techscam은 유명한 기술 회사의 지원 서비스를 사칭하여 고객의 민감 정보 탈취 및 비용 지불을 유도, 피싱보다 10배 더 재정적 영향을 미침.



Techscam 트래픽의 일일 볼륨이 2021년 이후 급격히 증가하며, 같은 기간 동안의 악성 코드와 피싱 트래픽과 극명한 대조를 보임.

Source: SmartScreen log data

사기 수법과 동향: 피싱

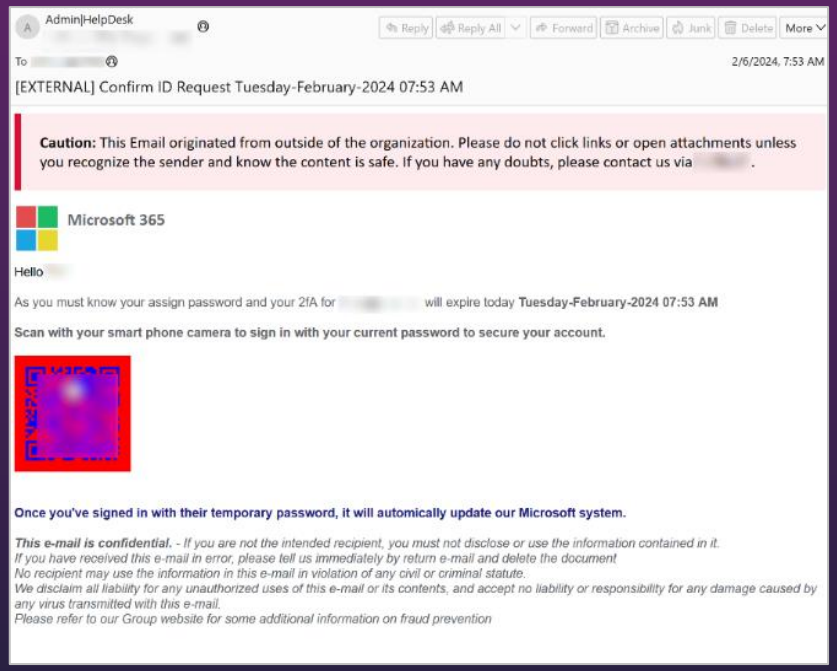


775 million

email messages contained malware

QR code phishing(Quishing, 쿼싱)

QR 코드의 특성상 사용자에게 목적지를 숨기기 때문에 보안에 있어 과제가 될 수 있다.



신원 공격의 관점

패스워드 기반 공격이 여전히 주를 이루고 있지만, 강력한 인증 방법을 사용하면 이를 차단할 수 있습니다.

신원 공격의 99% 이상이 패스워드 공격입니다.

Breach replay

Password spray

Phishing

추측하기 쉬운 암호 선택, 여러 웹사이트에서 암호 재사용, 피싱 공격의 희생양이 되는 등 예측 가능한 인간의 행동에 의존합니다.

<1% 미만

공격 비율

MFA 공격

SIM 스와핑
MFA 피로
AiTM(Adversary-in-the-middle)

인증 후 공격

토큰 도용
동의 피싱

인프라 성능 저하

Source: Microsoft Threat Intelligence

7,000

패스워드 공격 수 / 초

39,000

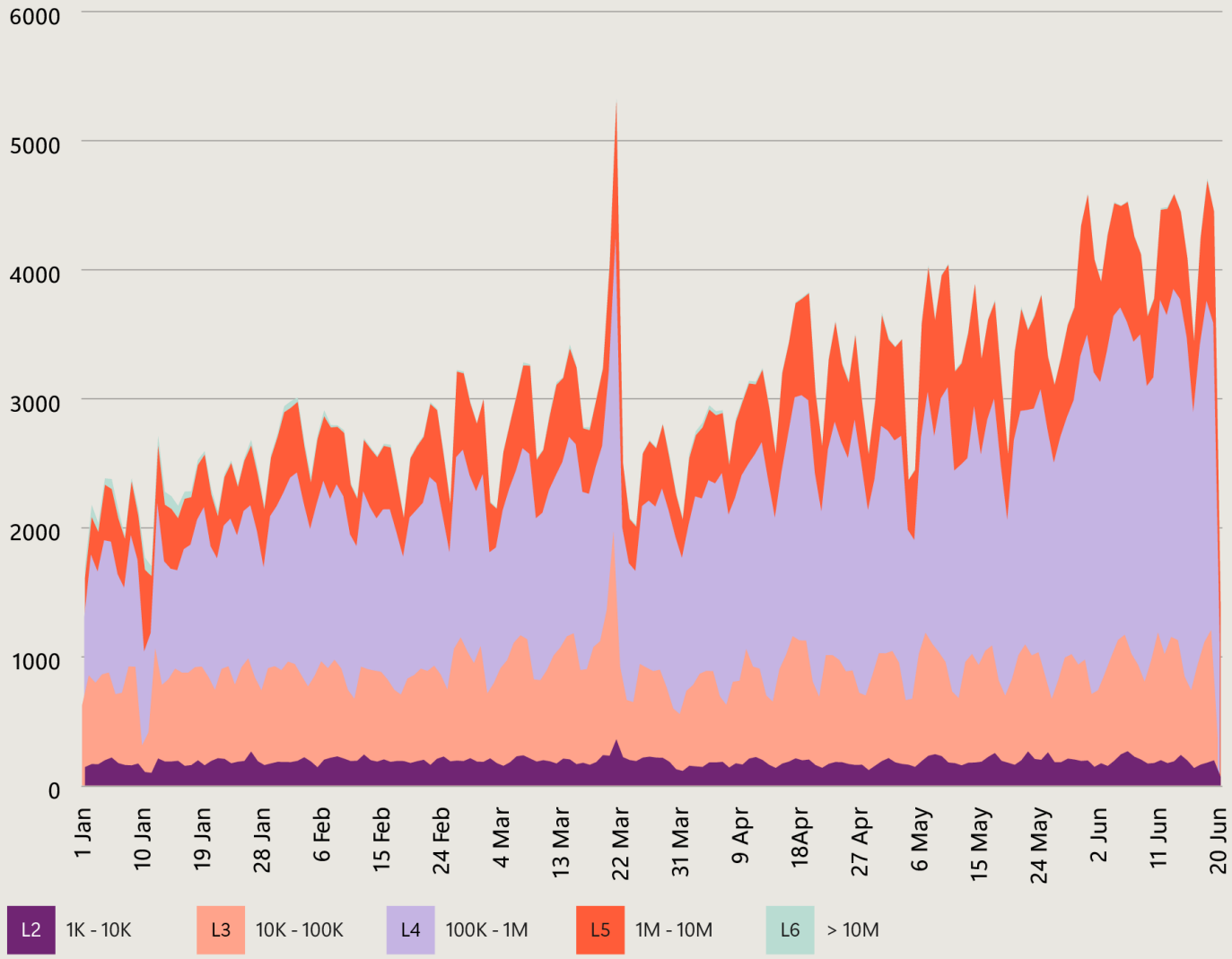
토큰 탈취 건수 / 일

146%

AiTM 피싱 공격 증가

DDoS:
은밀한 위협 등장

DDoS 공격이 **애플리케이션 레이어에 더욱 집중**되면서 비즈니스 가용성에 미치는 위험이 증가하고 있습니다.



The number of DDoS attacks mitigated continues to increase, with a notable surge layer 4 (L4, application layer) attacks. Application layer attacks are more stealthy, sophisticated, and difficult to mitigate than network-level attacks. Layers in the key are in "packets per second (pps)".

Source: Microsoft Global DDoS Mitigation Operations

Chapter 2

보안 중심 기반

What is the path forward to improve resilience?

- Secure Future Initiative
- Strategic cybersecurity
- Incident response
- Critical environments

보안을 최우선으로 생각

Microsoft SFI(Secure Future Initiative)는 가능한 한 최고 수준의 보안 표준을 달성할 수 있도록 제품 및 서비스를 **설계(Secure by Design), 기본적인 보안(Secure by Default) 및 안전한 운영(Secure Operations)**하는 방식을 발전시키기 위한 다년간의 이니셔티브입니다. 이는 끊임없이 진화하는 위협 환경에서 회사와 고객 모두를 보호하기 위한 Microsoft의 장기적인 약속입니다.

73만 개

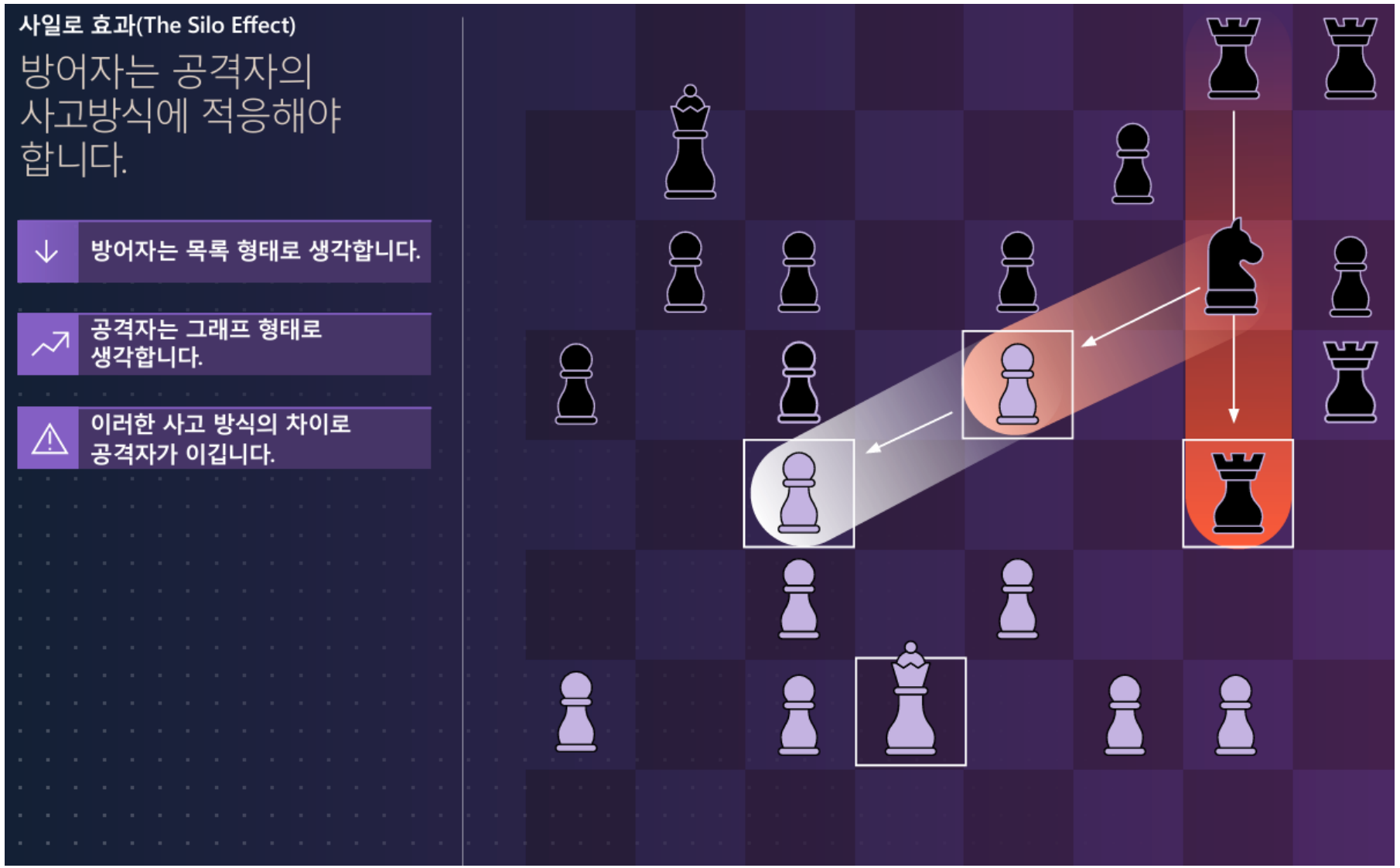
제거된 SFI 비준수 앱의 수

575만 개

제거된 비활성 테넌트의 수로 잠재적인 사이버 공격 표면을 대폭 줄였습니다.

위협 정보 기반 방어

위협 대응을 위한
색다른 사고



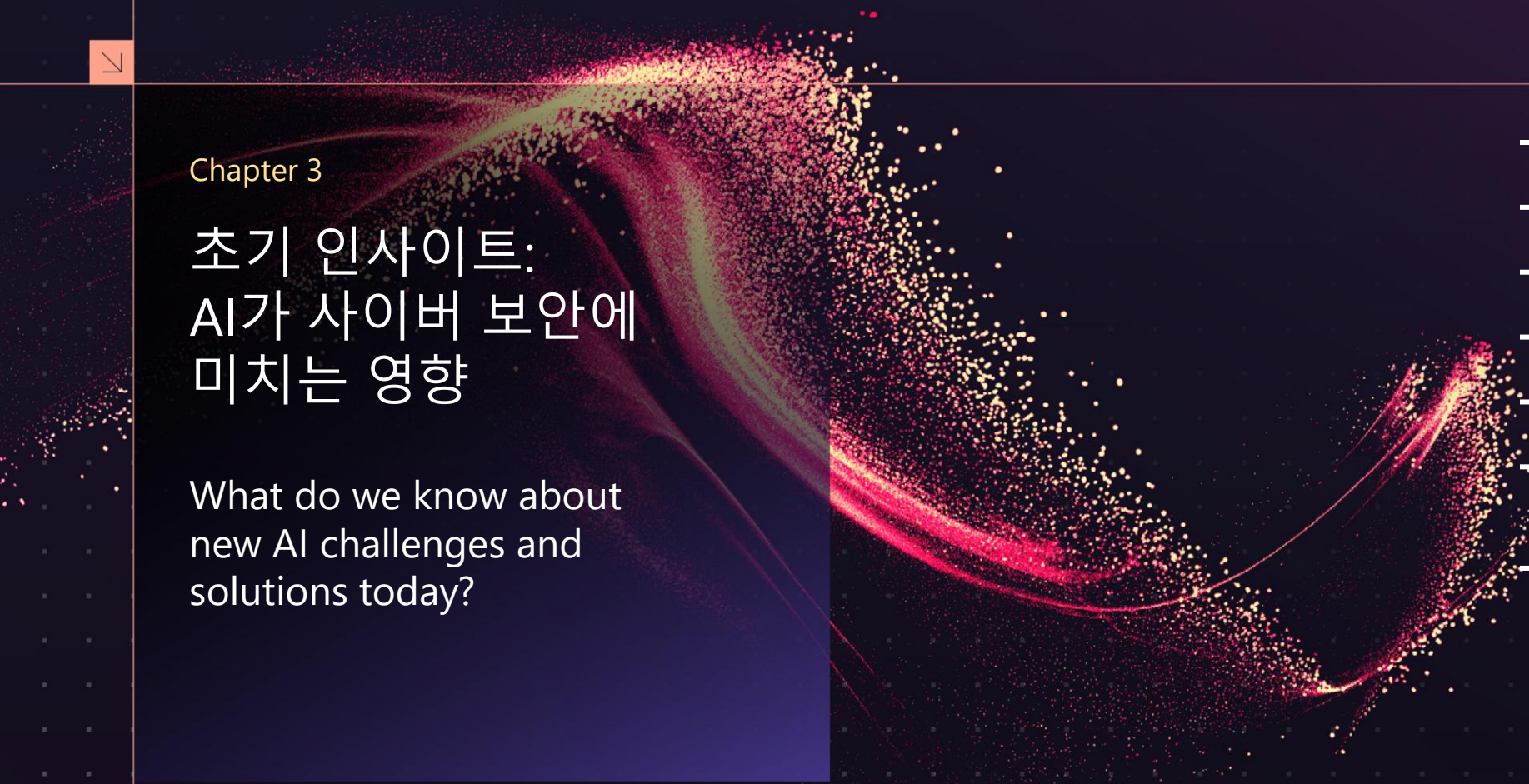
침해 전 공격 경로 분석

- ✓ 단일 창구
- ✓ 중요 자산 관리
- ✓ 공격 경로 관리

Chapter 3

초기 인사이트: AI가 사이버 보안에 미치는 영향

What do we know about new AI challenges and solutions today?



생성형 AI 보안에 대한 두 가지 주요 인사이트

1. 구축은 쉽지만, 테스트는 어렵다.

시스템 테스트 및 조정:

- 흔치않은(Uncommon) 입력
- 적대적인(Adversarial) 입력
- 개발자와 다른 사고방식을 가진 사용자로부터의 입력

2. 생성형 AI보안은 결과가 일정하지 않다.

- 같은 말을 두 번 반복해도 동일한 결과를 보장하지 않는다.
- 표현 방식의 미묘한 변화가 결과를 바굴 수 있다.
- 이는 전통적인 보안 취약성에 대한 “패칭(Patching)” 방식과는 다르다.

새로운 AI기반 공격 기술

위협 행위자들은 머신 러닝이 지원하는 AI 기반 타겟팅을 활용하여 **중요한 인물들을 타겟**으로 삼고 있습니다. 이러한 인물들은 영업 비밀, 금융 시스템, 핵심 전략, 기타 민감하고 독점적인 지적 재산에 접근할 수 있는 사람들입니다.

AI기반 스피어 피싱 및 웨일링

- AI와 결합된 맬웨어; 공격 타겟을 식별할 때까지 휴면 상태로 있다가 대상이 확인되면 활동 시작
- 위협 행위자들은 고도록 특정화된 타겟에 공격을 집중하고, 가장 유용한 정보만 탈취
- 사용자 모르게 AI가 디바이스 카메라, 스피커, GPS등을 사용하여 타겟 확인
- 발견된 시점에는 맬웨어가 이미 타겟 정보를 탈취한 상태

'이력서 스워밍'과 스테가노그래피

- AI를 활용해 구인 공고에서 키워드와 자격 정보를 수집하고 완벽한" 이력서를 생성
- 수천 개의 고도로 자격을 갖춘 가상의 후보자 이력서를 생성해 공개된 채용 공고에 지원
- 이 이력서는 자동 심사 도구를 통과하도록 보이지 않는 정보를 포함하는 스테가노그래피 기술 활용
- 지원자가 면접에 선정되고 결국 채용됨. 이를 통해 위협 행위자들은 조직 내에 내부자를 배치하여 영업 비밀, 정보, 또는 기타 민감한 데이터 탈취

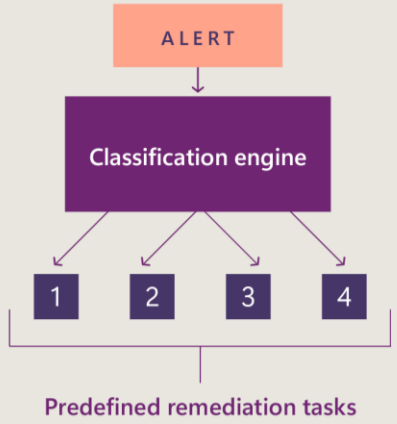
> *When it comes to AI-enabled human targeting, threats will be more difficult to detect and defend against—even with AI tools assisting defensive strategies.*

방어를 위한 AI

AI 혁신에 대한 Microsoft의 상당한 투자는 사이버 보안 방어자에게 방어 영역에서 공격자에 대한 비대칭적인 이점을 제공하는 것을 목표로 합니다.

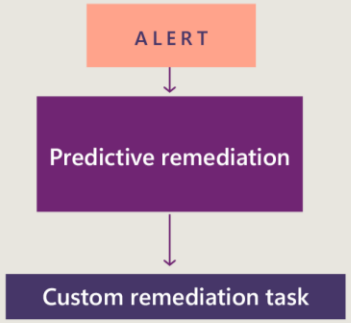
생성형 AI를 활용해 사이버 공격을 이해하고 맞춤형 대응 방안 마련하기

Rules-based approach



전통적인 규칙 기반 방어 접근법은 사전에 정의된 작업으로만 옵션이 제한됩니다.

With generative AI



생성형 AI를 활용하면, 경고와 관련된 특정 사실에 기반하여 다음 단계를 예측하고 그에 따른 고유한 대응책을 마련할 수 있습니다.

사이버 공격 탐지 및 차단을 위한 AI 활용

AI를 활용한 숨겨진 공격 탐지

Hands-on-keyboard attacks, 사이버 범죄자가 손상된 시스템과 직접 상호작용하는 이러한 공격은 탐지가 어렵습니다.

- **LLMs** 의심스러운 활동을 식별하도록 정밀 조정
- **맥락 및 의미를 학습**하여 잠재적 위협을 식별하고 플래그 설정

엔드포인트 탐지와 AI를 결합한 공격 차단 및 대응

AI모델은 hands-on-keyboard attack을 탐지할 때 경고합니다.

MDE는 자동으로 다음을 수행합니다:

- 영향을 받은 디바이스 격리
- 손상된 사용자 계정을 일시적으로 비활성화

사이버 보안 전반에 AI 확장

AI 모델은 네트워크 로그, 이메일 커뮤니케이션, 웹 트래픽, 소셜 미디어와 같은 방대한 복합 데이터를 분석하여 악성 활동을 탐지합니다.

글로벌 AI 보안을 발전시키기 위해 노력하는 정부 및 산업

- AI의 개발, 배포, 활용에서 안정성과 보안의 중요성에 대하 공감대가 형성되어 있습니다.
- 정부들은 보안 요구사항을 구현하는데 있어 다양한 접근 방식을 취해왔습니다.

정책 접근 방식의 범위와 규모

정보의 정책 이니셔티브의 차이는 다음을 반영합니다:

- 정부 지도부의 핵심 가치
- 각국의 법적 및 헌법적 체계
- 기술 산업의 현재 상태와 미래 성장 가능성

국제 표준

국제 표준은 AI 보안 규제의 단편화를 완화하는데 도움을 줄 수 있습니다.

- AI 보안과 관련된 두 개의 ISO 표준 (42001 및 27090) 이 있습니다.
- 미국 정부의 NIST(국립표준기술연구소)는 AI와 보안에 대한 요소들을 Risk Management Framework와 crosswalk을 보유하고 있습니다.

Microsoft Digital Defense Report

https://microsoft.com/mddr

감사합니다

Microsoft