글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션5) 사이버보안

사이버보안 정부정책 및 국가R&D 추진방향

정현철 보안블록체인PM, IITP

주최 과학기술정보통신부 Ministry of Science and ICT
특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency
TTA IITP KEA kisto ETRI

Index

01 사이버보안 패러다임 변화

공격 위협 확대

**사이버공격으로 인한 피해가 개인, 기업 → 국가로 확대,
사회 혼란, 국가간 분쟁 유발 등 국가 안보 위협**

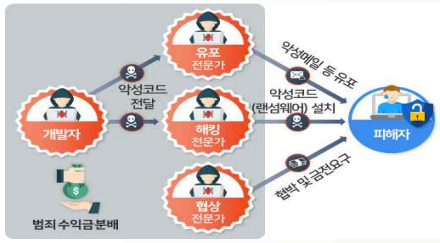
- '23년 세계경제포럼(WEF) **'사이버범죄 및 불안 확산'**을 글로벌 10대 리스크로 선정

①기후변화 완화실패, ②기후변화 적응실패, ③자연재해와 이상기후, ④생물다양성 손실, ⑤난민, ⑥천연자원 위기, ⑦사회결속력 약화, **⑧사이버범죄 및 불안 확산**, ⑨지정학적 대립, ⑩환경피해

- 선진국 중심 **'사이버보안'을 주요 국가안보전략 요소**로 선정
- **美**, 주변 동맹국들 간 주요 협력 분야에 **'사이버보안' 포함**

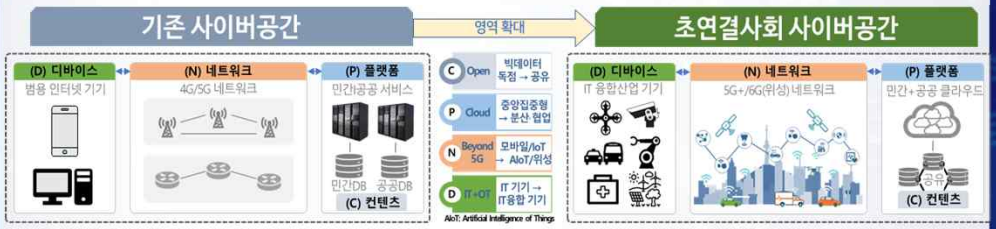
공격방식의 고도화 · 산업화

**(고도화) 탐지·방어가 어려운 최신 AI(ChatGPT 등)기반 공격
(산업화) 서비스형 랜섬웨어(RaaS) 등 해킹 서비스 제공**



공격 대상 확대

**디지털 대전환, 팬데믹 상황 지속 등으로
사이버공간 확장, 확장된 공간 = 공격 대상**

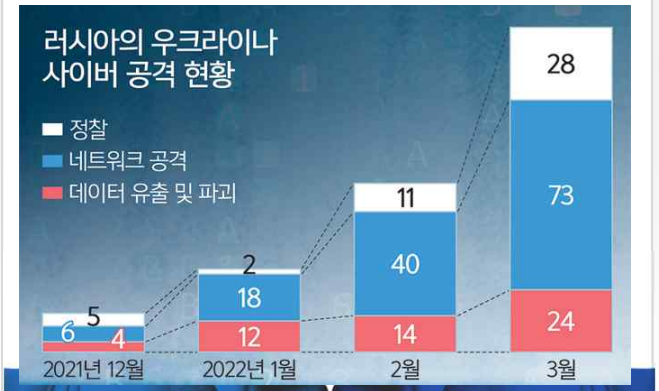


01 사이버보안 패러다임 변화

국가 안보, 경제를 위협하는 사이버보안

러시아-우크라이나 전쟁

우크라이나 침공 전초전은 '사이버 공격'
'22년 2월 24일, 러시아가 우크라이나 침공



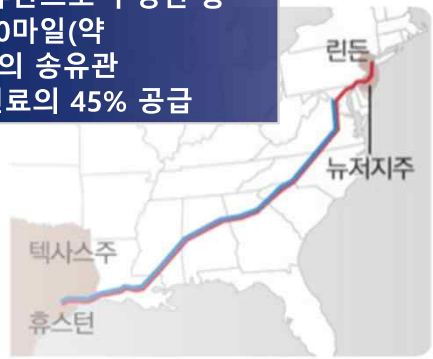
물리공격보다 앞선 사이버 공격
막강한 해킹능력으로 막강한 전투력 발휘

국가 기반시설 대상 사이버공격

미 최대 석유제품 송유관 운영사
'콜로니얼 파이프라인' 랜섬웨어 공격피해

러 해커집단 '다크사이드'이 **랜섬웨어 공격**('21.5)
→ 수일간 미 일부 지역에 송유 지급 중단
→ 해커집단에 몸값으로 $440만 지급 후 복구

- 2개의 송유관으로 구성된 총 길이 5,500마일(약 8,800km)의 송유관
- 미 동부 연료의 45% 공급



북한 해킹

2009년	7.7 디도스 대란
2010년	외교, 안보, 통일 관련 부처 해킹
`12~`15년	신문사, 은행, 언론사, 육군히 등 해킹
2016년	정부 주요 인사 스마트폰, 민간기업 해킹 방글라데시 중앙은행 8,100만달러 해킹
2017년	빗썸 등 가상화폐거래소 사이버공격
2018년	정부기관 및 대북단체 사이버공격
2022년	가상자산 2조원 해킹 (전체 가상자산 해킹의 44%)

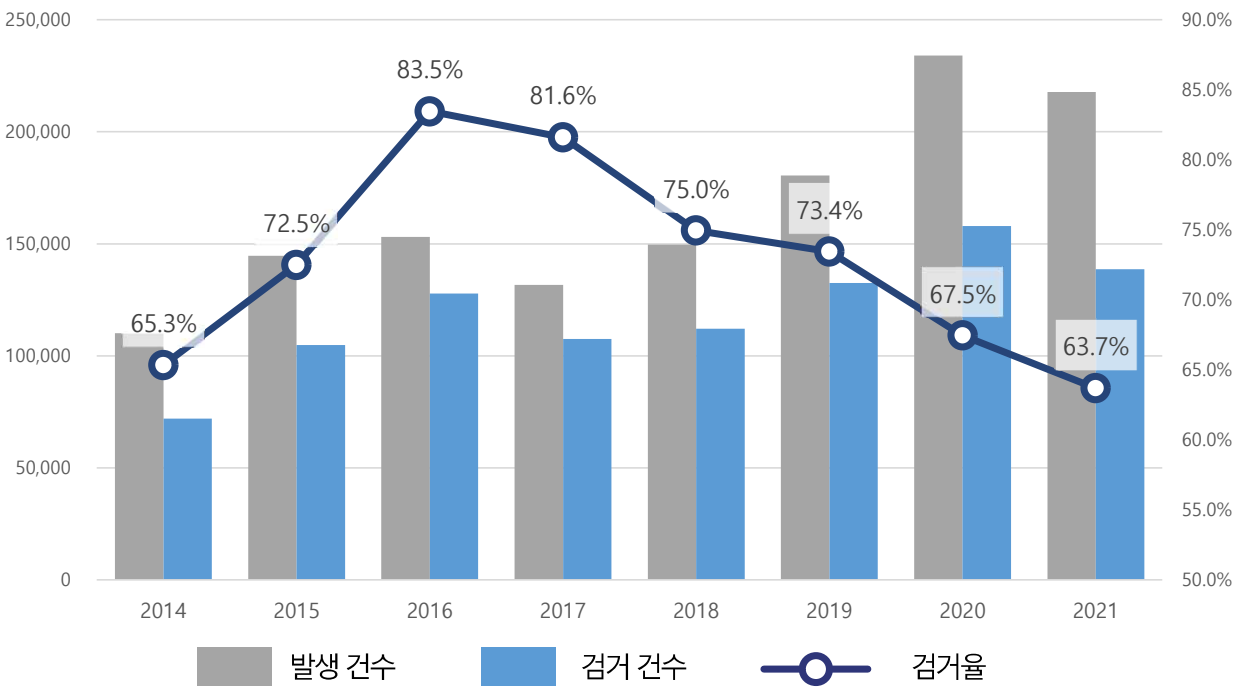
UPI뉴스 2019.2.20.

북한 해킹능력, 러시아 이어 세계 2위

北, 2시간 20분만에 네트워크 침투해 정보 탈취 1위
露, 해킹으로 19분 안에 원하는 정보를 빼내

※ 출처 : 북한의 사이버공격 사례, 서울경제, `19

8개년(`14~`21년) 간 국내 사이버범죄 발생 건수 급증
사이버범죄 발생 대비 검거율 지속 하락 中

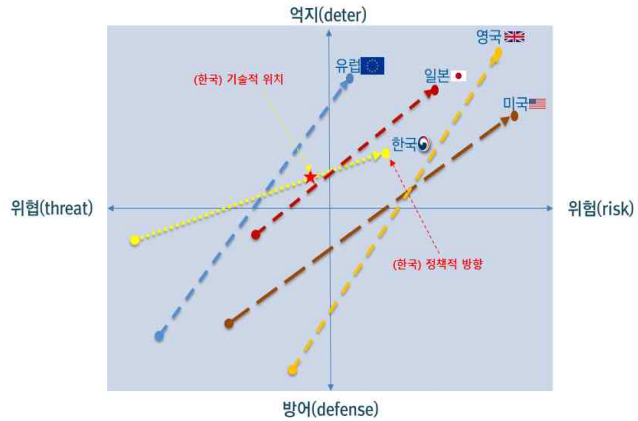


※ 출처 : `14~`21년 경찰청 사이버수사 통계자료 등

02 글로벌 사이버보안 정책 및 시장

주요국 적극적 사이버방어 (Active Cyber Defense) 로 변화
– 위협 행위자의 식별 및 사전 예방적 차원의 조치 등

국가	계획명	주요 키워드
미국	국가사이버보안 전략 (`23.3)	▪ 공격자에 대한 적극적 대응, 주요기반시설 보호, 글로벌협력
	국가안보전략(`22.10)	▪ 글로벌 협력, 통합억제, 복원력 확보, 국제협력
	CISA 전략계획 2023~2025(`22.09)	▪ 사이버 공간의 방어 및 복원력 향상
	연방 사이버보안 R&D 전략계획 실행 로드맵(`21.12)	▪ 억제, 보호, 탐지, 대응
	국가 사이버 전략(`18.09)	▪ 사이버범죄, 침해사고 대응, 사이버공간 안전성 확보
	사이버 보안 프레임워크(CSF)(`18.04)	▪ 주요 인프라 및 레질리언스 제고
	사이버보안 국가 행동계획(CNAP)(`18)	▪ 사이버 공격 대응 방법 구상, 통합형 사이버 보안 체계 구축
영국	국가 사이버 전략 2022('21.12)	▪ 회복력/복원력, 사이버 공격자의 탐지/억제/방해, 경찰력 강화
	사이버보안 지침(`20.05)	▪ 사이버위협 사전 예방, 복구
	최소사이버보안기준(`18.06)	▪ 적극적 사이버 방어
일본	차기 사이버보안 전략(`22.09)	▪ 사이버공간 확보, 다자간 사이버안보 협력 지향
	사이버보안에 관한 행동계획(`22.06)	▪ 사이버공격 대비 의무화
	新 사이버보안 전략('21.9)	▪ 보안 내재화, 글로벌협력, 경찰력강화
	국가 사이버안보 전략(`18)	▪ 주요기반시설의 사이버보안 역량 강화, 위협 대응 방어



[주요국의 사이버 안보 전략 방향성 전환]

※ 출처 : "국가 사이버안보 전략 패러다임 변화에 대한 주요국 비교분석 연구", KANIS, 유지연, '21.6

참고 한미동맹, “전략적 사이버안보 협력 프레임워크(2023.4월)

사이버공간의 악의적 행위자에 대한 “능동 대응 협력의지” 강조

한-미, 전략적 사이버안보 협력 프레임워크 주요 내용

- **(협력 범위) 한미 협력을 사이버공간까지 확장하고, 사이버위협 정보의 공유를 포함한 사이버안보 기술, 정책, 전략에서 협력을 증진하며 신뢰를 구축**
  - (차단 및 억지) 악의적인 행위자들의 활동을 차단하고 억지하기 위해, 방어 및 위협 감소 수단을 포함한 다양한 종류의 대응수단을 개발하고 실행
  - (정보 공유) 자금세탁, 가상자산 탈취 등 사이버공간의 악성활동을 탐지·억지·와해하기 위해 협력, 다양한 원천으로부터 정보공유 지속

    ⋮
  - (역량 강화) 사이버안보 역량 강화를 위해 사이버훈련에 적극적으로 참여, 핵심 기반시설 보호를 위한 핵심기술 연구·개발에 협력

    ⋮
  - (민·관·학 협력) 사이버안보 사고관리, 사이버 위협정보 실시간 공유 등 사이버 복원력 확보를 위한 정부·민간·학계간 협력체계 구축
  - (국제 협력) 모든 국가가 개방-상호운영 가능-신뢰할 수 있고, 안전한 인터넷과 사이버공간을 장려하기 위해 사이버역량 구축 협력 촉진

EU 집행위원회 「 사이버복원력법안 」 발표('22.9.)

• 제조. 유통, 수입업체 등 공급망에 포함된 기업들 대상 의무사항 부여

목적

사이버 보안 제품에 대한 공통 표준 수립

- EU 시장에 출시된 제품 및 소프트웨어 안전성 확보
- 디지털 제품 수명주기 전반의 사이버 보안 강화

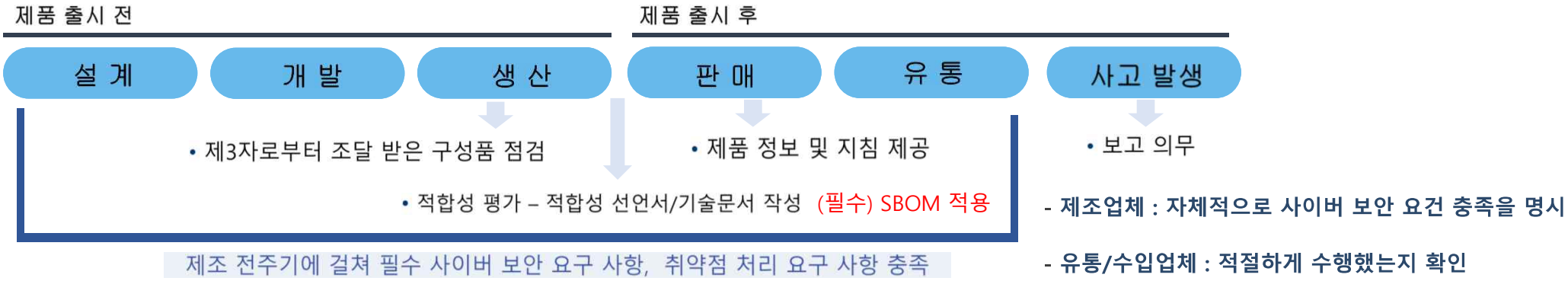
적용대상

직간접적으로 타 기기 또는 네트워크에 연결될 수 있는 디지털 요소가 포함된 모든 제품(HW, SW 등)

기존 EU법에 의해 규제되는 제품 적용 제외

ex) 의료제품, 자동차, 항공, 군사 제품 등

주요 내용



제조 전주기에 걸쳐 필수 사이버 보안 요구 사항, 취약점 처리 요구 사항 충족

- 제조업체 : 자체적으로 사이버 보안 요건 충족을 명시
- 유통/수입업체 : 적절하게 수행했는지 확인

02 글로벌 사이버보안 정책 및 시장

보안/프라이버시 규제 강화, 기술장벽으로 확장

01 데이터	EU GDPR 시행과 국내 데이터 3법 시행
02 스마트홈	지능형 홈네트워크 보안강화 고시 개정 시행 (2022년 7월 1일)
03 의료기기	IMDRF, 의료기기 사이버 보안 지침 개정 (2020년) 식약처, 의료기기 사이버보안 허가 심사 가이드라인 (2018년)
04 자동차	UNECE 자동차 사이버보안 규정 * 2022년 7월부터 모든 신차에 의무 적용
05 선박	국제해사기구(IMO) 2021년부터 선박 사이버위협 안전관리 요구 * 국제선급협회 2024년 조선 건조시 사이버보안 요건 준수 요구 예정

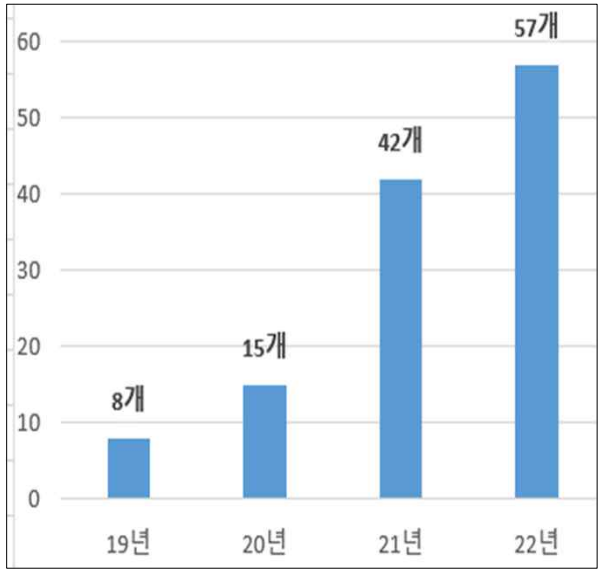
참고 GDPR 위반 벌금 부과 사례

순위	기업명	벌금	사유
1	Meta	$1.3 billion	data transfers between the E.U. and the U.S.
2	Amazon	$781 million	not getting consent from its users
3	Instagram	$427 million	violating children's privacy online
4	Facebook	$275 million	Facebook's personal data was found on an online hacking forum
5	WhatsApp	$247 million	not properly explaining its data processing practices in its privacy notice
6	Google LLC	$99 million	difficult for users to refuse cookies on Google and YouTube
7	Google Ireland	$66 million	difficult for users to refuse cookies on Google and YouTube
8	Facebook	$66 million	not obtaining proper cookie consent from users
9	Google	$55 million	not being transparent with its users about how data was being collected and used for targeted advertising
10	H&M	$41 million	illegal monitoring of its employees

출처 : https://www.enzuzo.com/blog/biggest-gdpr-fines

02 글로벌 사이버보안 정책 및 시장

<사이버보안 유니콘 기업 수, 출처 : CB Insights>



국가	유니콘 기업수
미국	44개
이스라엘	7개
캐나다	3개
중국	1개
스위스	1개
리투아니아	1개

- VC 투자, 대규모 M&A를 통한 대형화, 통합 보안화
- AI, 클라우드, 블록체인 등 신기술 적용을 통한 혁신 기술 개발 중

<사이버보안 유니콘 기업 57개 중 Top 10>

순번	기업명	사업 분야	세부 사업 분야	기업 가치 (단위:10억달러)
1	Wiz	클라우드 보안	클라우드 환경 침입 탐지 대응 시각화 솔루션	$10
2	Tanium	엔드포인트 보안	엔드포인트 관리 및 보안 플랫폼	$9
3	Lacework	클라우드 보안	클라우드 데이터 관리 및 개발 보안 플랫폼	$8.3
4	StarkWare	암호응용 SW	영지식 증명을 이용한 익명성 기반 블록체인 개발	$8
5	Netskope	통합 보안 관리 시스템	보안 접근 서비스 에지(SASE)	$7.5
6	Snyk	AI 보안	AI 기반 소프트웨어 보안 개발 플랫폼	$7.4
7	1Password	권한인증 관리	암호 관리 솔루션	$6.8
8	Coalition	사이버 보험	사이버 보험	$5
9	Socure	권한인증 관리	디지털 신원 확인 솔루션	$4.5
10	Arctic Wolf Networks	통합 보안 관리 시스템	통합 보안 관리	$4.3

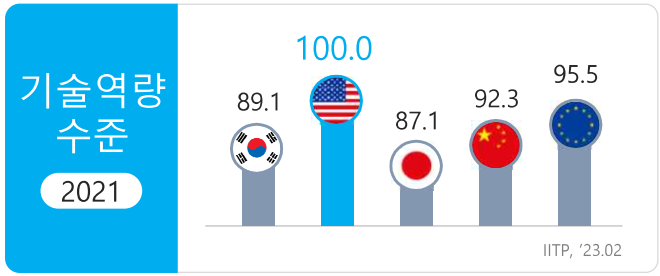
03 국내 사이버보안 정책 및 시장

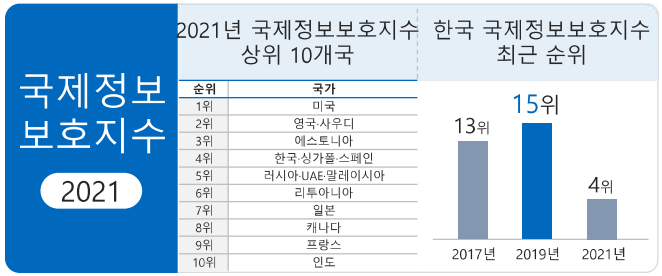
양적 성장은 이루었으나, 분야별 전문화 및 기업 대형화 등 질적성장 필요

출처 : 2022년 국내 정보보호 산업실태조사, 과기정통부, 2023.9월

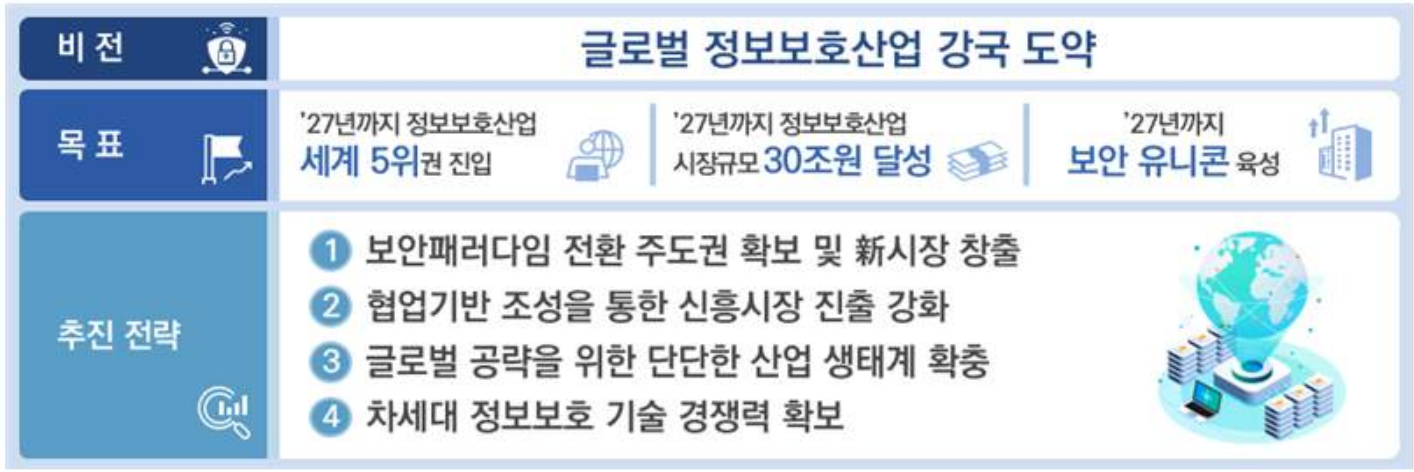
출처 : 안랩 한달새 30명퇴사...사이버보안인력 생태계 붕괴위기, 한국경제, 2023.9.3일

국내 기술 수준 및 현황





과기정통부, 「정보보호산업의 글로벌 경쟁력 확보 전략」 발표 (제30차 비상경제차관회의, 2023.9.5일)



- '27년까지 시장규모 30조원 달성을 목표로 관련 예산 총 1조 1천억 원 투입
- '27년까지 총 1,300억원 규모의 「사이버보안 펀드」 조성을 통해 보안유니콘 기업 본격 육성
- 제로트러스트 전환로드맵 수립 및 제로트러스트 가이드라인 2.0 배포, 통신·금융·의료 등 주요 기반 분야 보안 패러다임 전환 시범사업 추진
- 신 통합보안 모델 개발을 위한 「K-시큐리티 얼라이언스」 추진을 통해 글로벌 수출지원 확대

국내 사이버보안 정책 및 시장 -12대 국가 전략기술

- 사이버보안 기술은 **디지털사회 필수 안전장치**
- 경제 · 안보 인프라 보호를 위해 **자립화가 필수적인 기술분야**

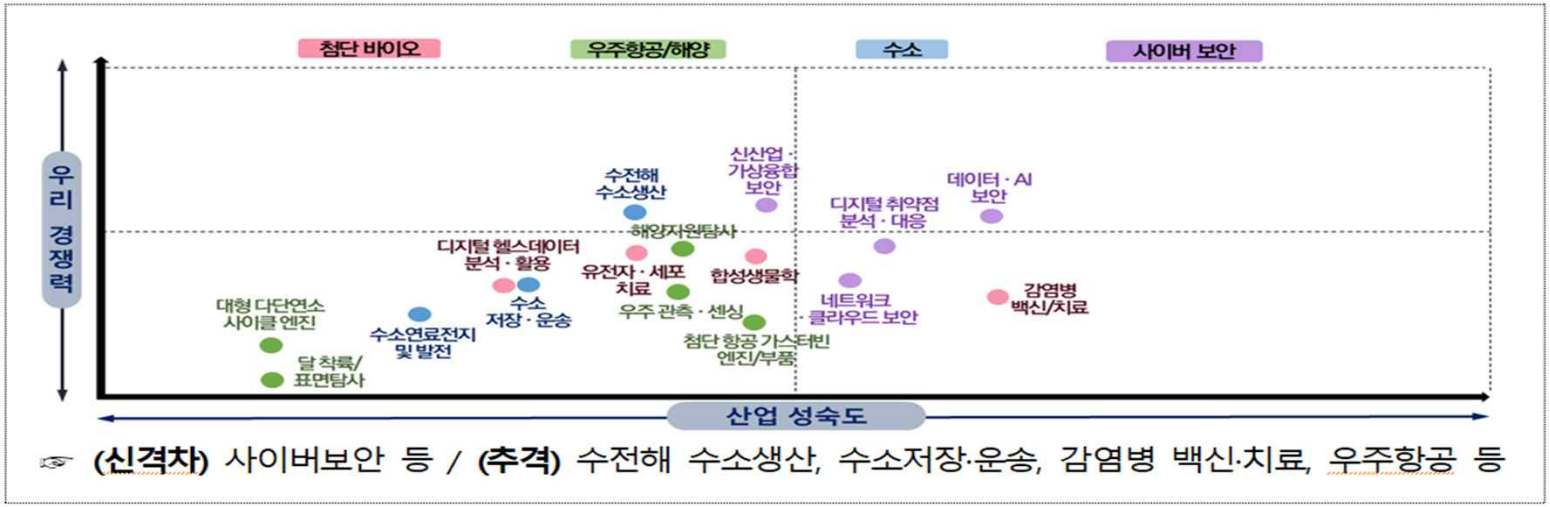
8 사이버보안

단기(~5년)
- **AI기반 보안관제 · 자동대응** 등 **원천기술 개발**
- **ICT** 장비 · SW **취약점**(펌웨어 등) **산속 분석 · 대응기술**

→

중장기(5~10년)
- **미래 디지털 인프라**(모빌리티, 클라우드, 6G 등) **사이버보안 체계 자립화**

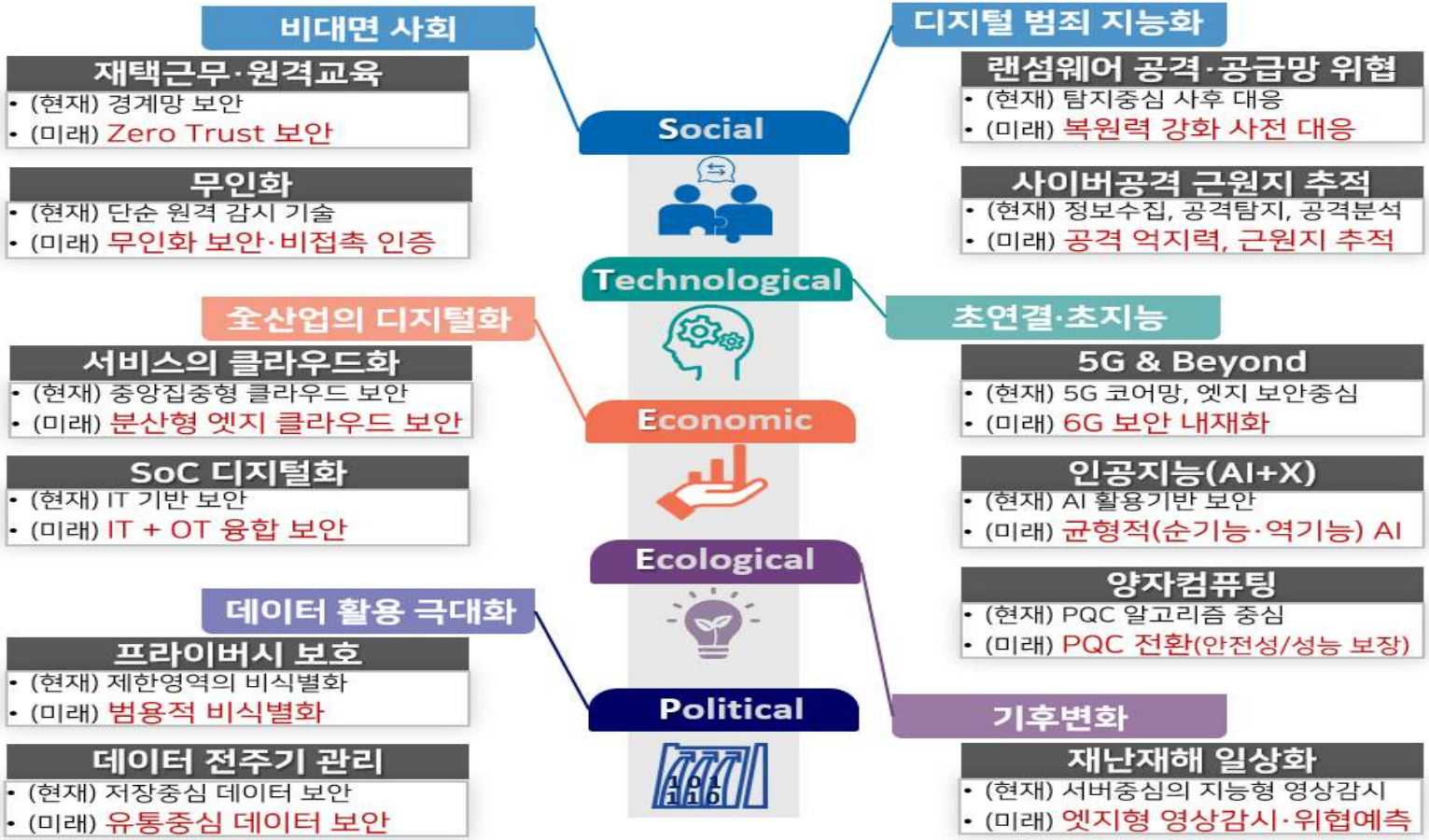
- 데이터·AI 보안
- 네트워크·클라우드 보안
- 디지털 취약점 분석·대응(공급망 보안)
- 신산업·가상융합 보안



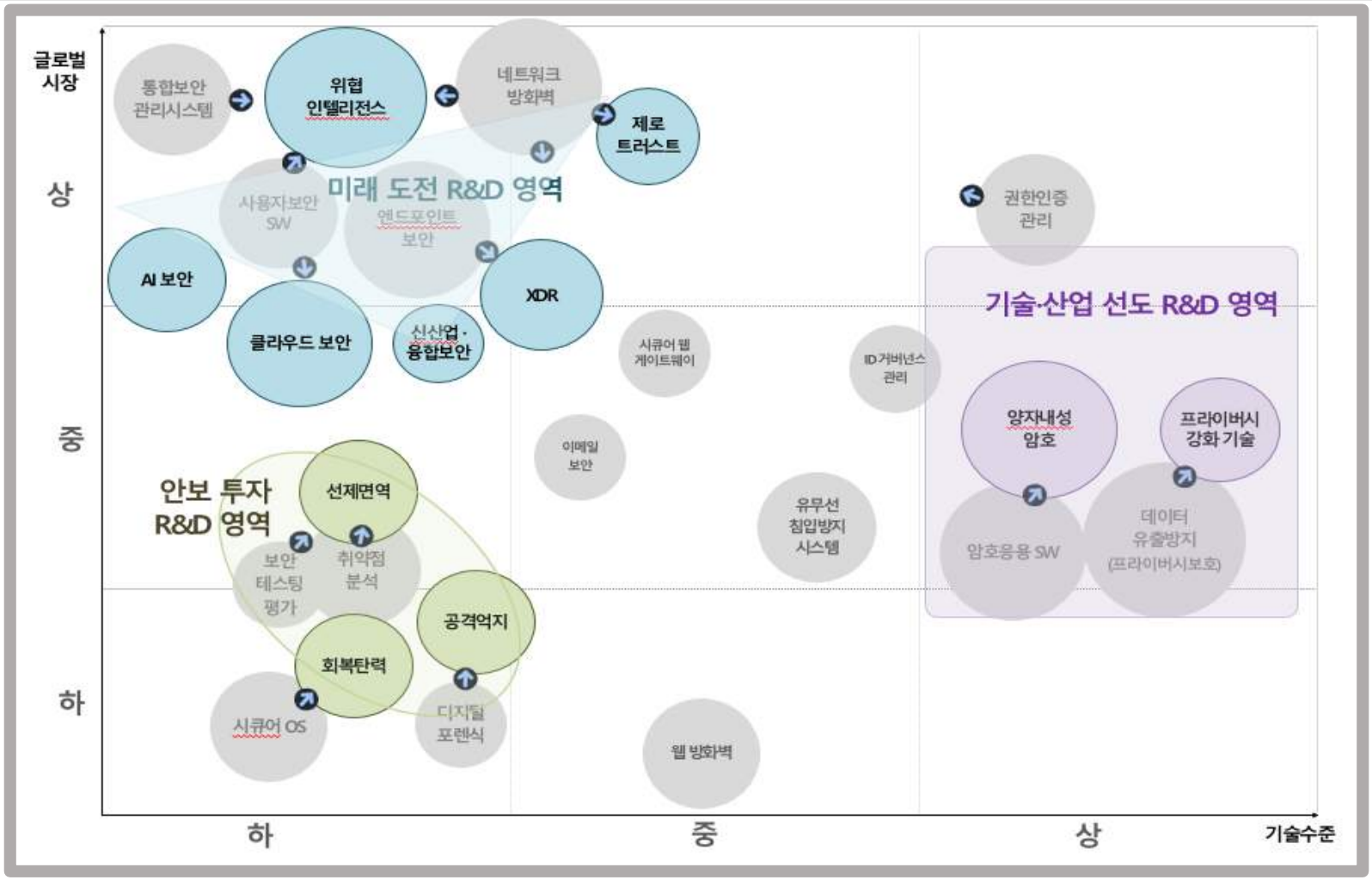
☞ **(신격차)** 사이버보안 등 / **(추격)** 수전해 수소생산, 수소저장·운송, 감염병 백신·치료, 우주항공 등

04 사이버보안 기술개발 방향 - 환경변화

STEEP 트렌드 분석 → 정보보호 이슈 → 현황/니즈 도출



04 사이버보안 기술개발 방향 - 시장, 기술수준 분석



05 주요 보안 이슈① 생성형 AI : 누구나 정교한 해커가 될 수 있다.

[DEF CON AI RedTeam Challenge, 2023.8]

그림 : https://www.airedteam.org/

05 주요 보안 이슈① 생성형 AI : AI 공격은 AI로 방어!

01 사이버공격 악용

02 개인/기밀 정보 유출

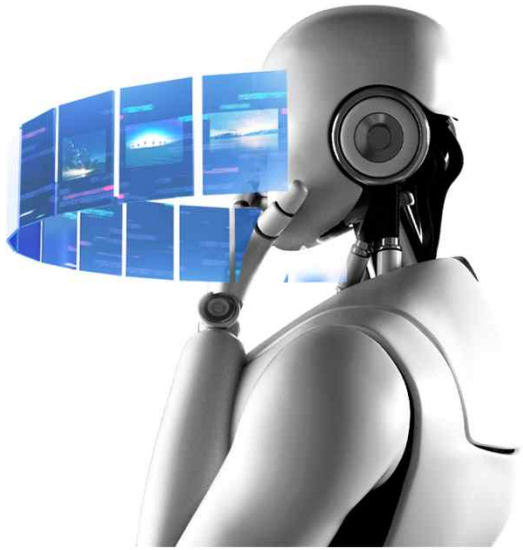
03 결과물 정확성 결여

04 지식재산권 침해

05 AI모델 공격

생성형 AI 보호 기술

- 생성형 AI 활용시 정보유출 방지
- 생성형 AI 학습 데이터 추출, 모델 복제 등 적대적 공격 방어
- 공개 sLLM 백도어 탐지
- 생성형 AI 신뢰성 검증



생성형 AI 활용 보안기술

- 사이버보안에 특화된 소규모 언어모델(sLLM) 개발
- 생성형 AI 기반 사이버위협 자동생성 및 방어기술
  - 공격 전단계 위협 벡터 자동생성 및 증강
  - AI 악성 생성물 탐지/분류 및 위협 인텔리전스 기술
- 생성형 AI 기반 사이버인텔리전스 분석/이해/요약/의사결정지원

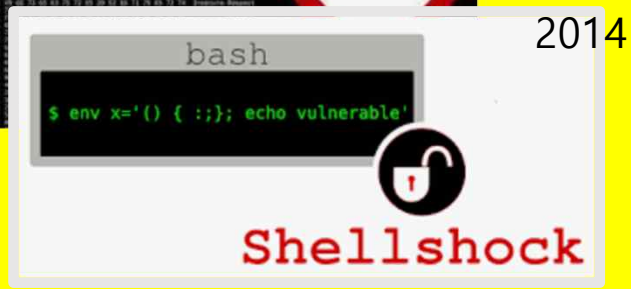
05 주요 보안 이슈② 공급망보안 : 3rd Party 제품 신뢰하십니까?

2020

2022

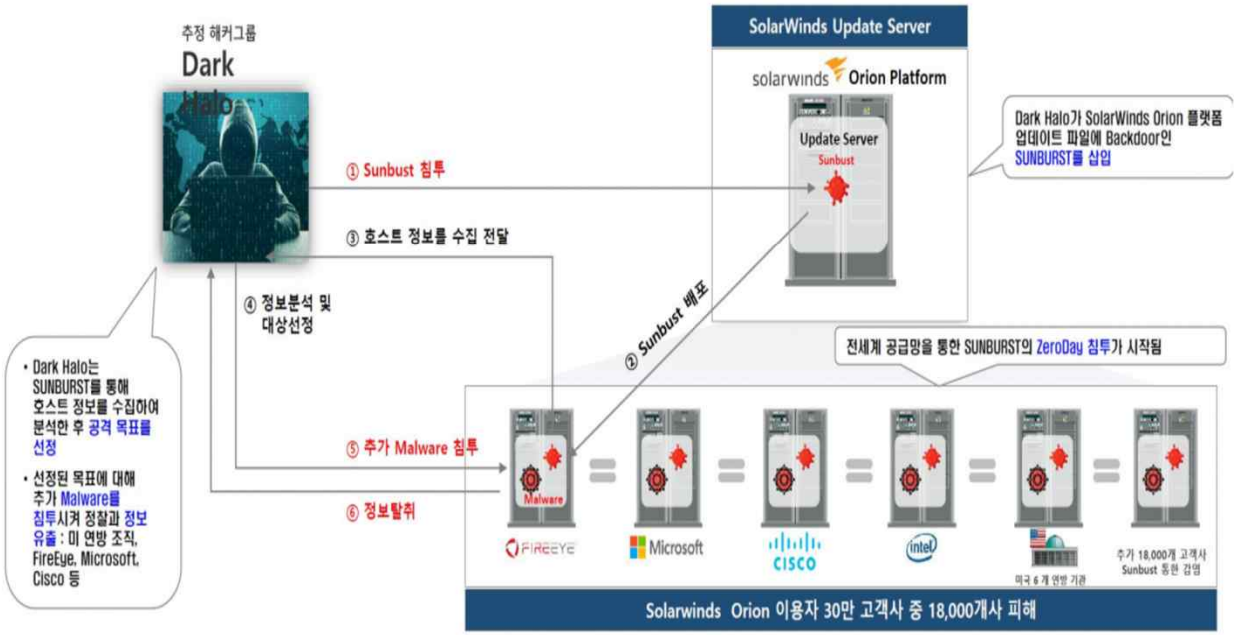
2019

2014



2014

SolarWinds의 SUNBURST 보안침투 상세



자료 :데일리시큐, 2020.12월

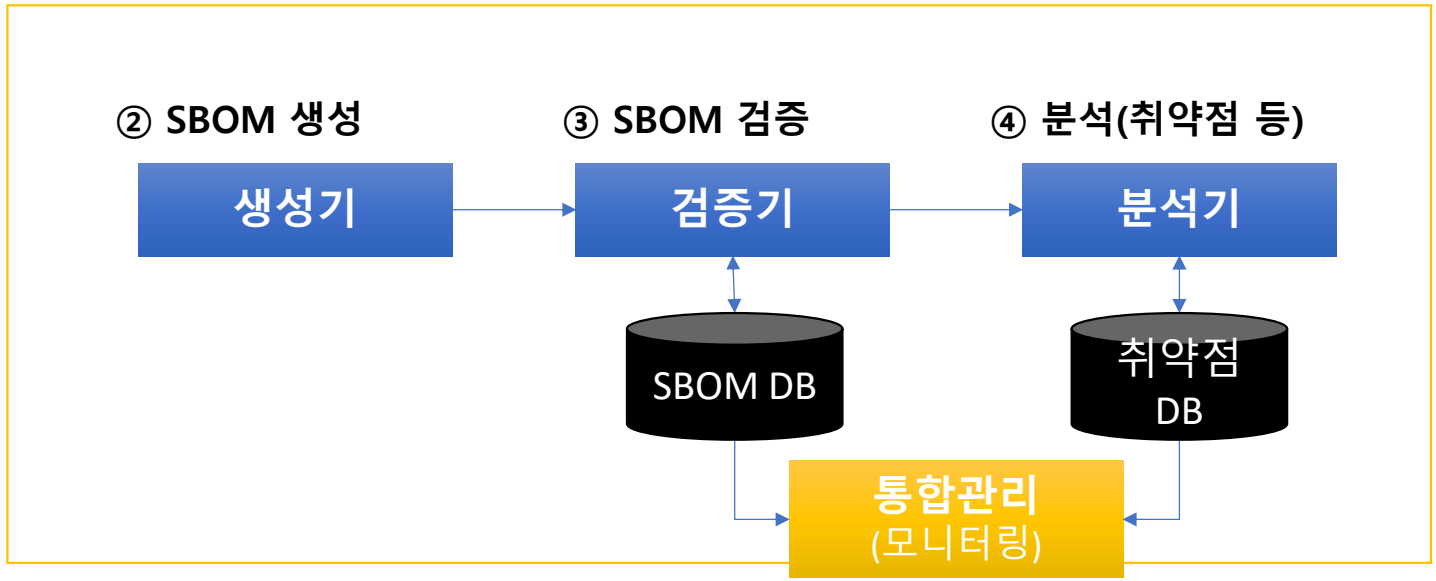
05 주요 보안 이슈② 공급망보안 : 소프트웨어 명세서(SBOM)

명세서(Bills of Material)

자동차 부품 명세서

부품명	제조자	모델명	부품특성	인증규격

SW 공급망 보안 절차

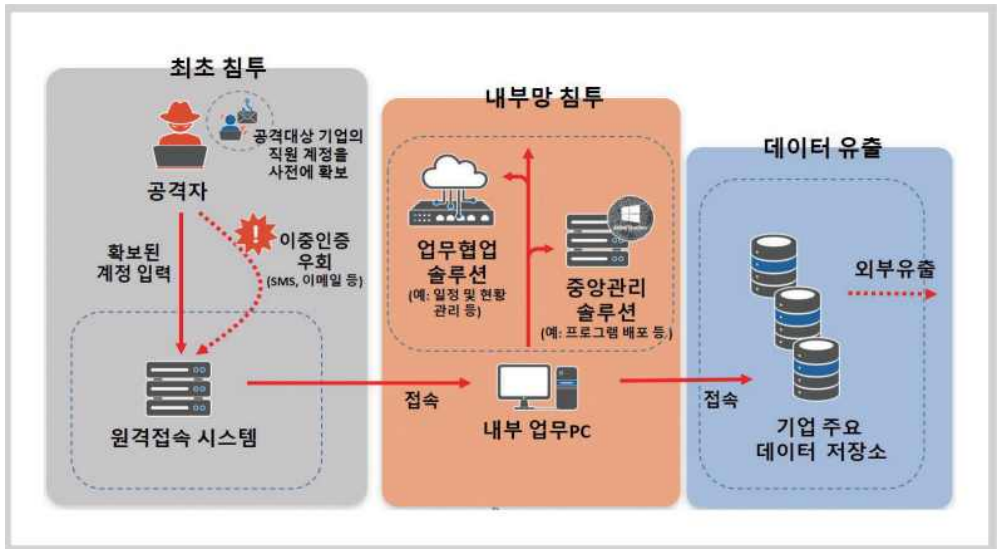


05 주요 보안 이슈③ 제로트러스트 : 어디까지가 내부인가? 내부는 안전한가?

경계망 보안

그림 : https://www.cloudflare.com/

사이버공격 단계별 침투방법

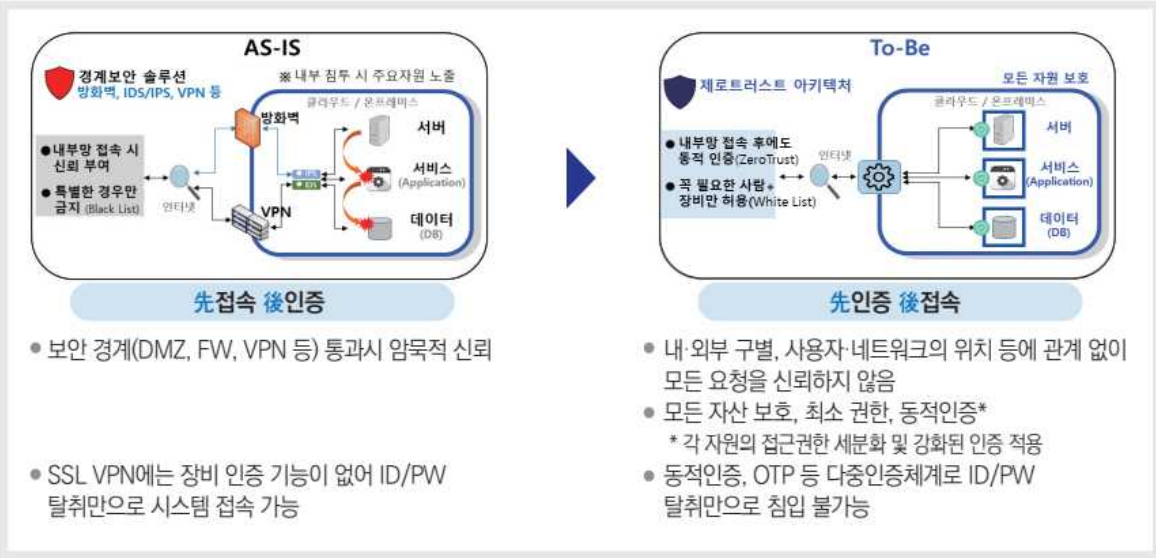


출처 : 제로트러스트 가이드라인 1.0, 과기정통부, 2023.6월

05 주요 보안 이슈③ 제로트러스트 : Never Trust. Always Verify.

Never trust.

Always verify.



- 보안 경계(DMZ, FW, VPN 등) 통과시 암묵적 신뢰
- SSL VPN에는 장비 인증 기능이 없어 ID/PW 탈취만으로 시스템 접속 가능

- 내·외부 구별, 사용자·네트워크의 위치 등에 관계 없이 모든 요청을 신뢰하지 않음
- 모든 자산 보호, 최소 권한, 동적인증*
  * 각 자원의 접근권한 세분화 및 강화된 인증 적용
- 동적인증, OTP 등 다중인증체계로 ID/PW 탈취만으로 침입 불가능

출처 : 제로트러스트 가이드라인 1.0, 과기정통부, 2023.6월

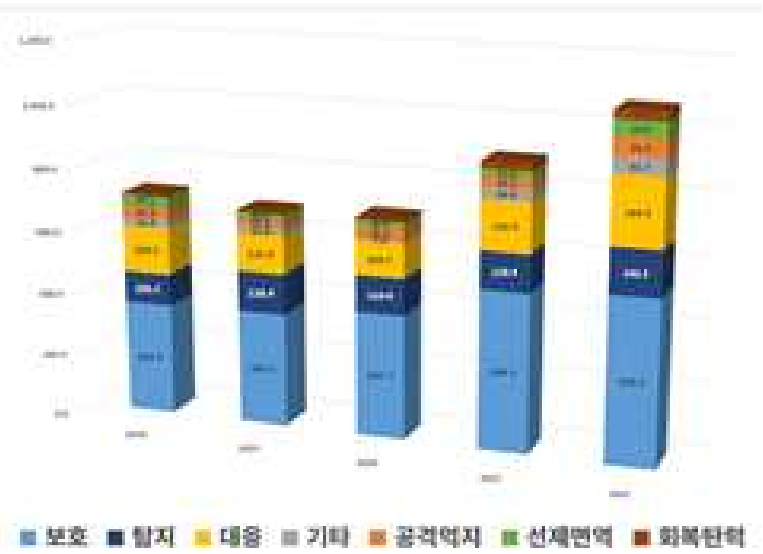
제로트러스트 기본철학

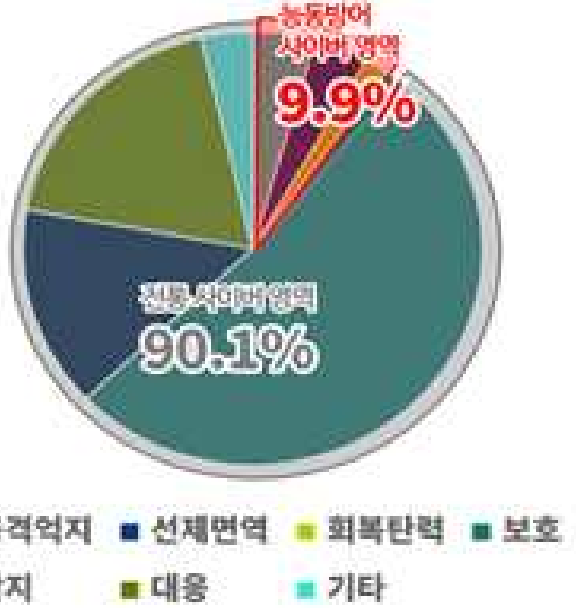
① 모든 종류의 접근에 대해 신뢰하지 않을 것(명시적인 신뢰 확인 후 리소스 접근 허용)
② 일관되고 중앙집중적인 정책 관리 및 접근제어 결정·실행 필요
③ 사용자, 기기에 대한 관리 및 강력한 인증
④ 자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
⑤ 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
⑥ 모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증·제어

05 주요 보안 이슈④ 능동 방어

[국내] 능동적/선제적 방어기술 분야의 연구개발 투자 부족

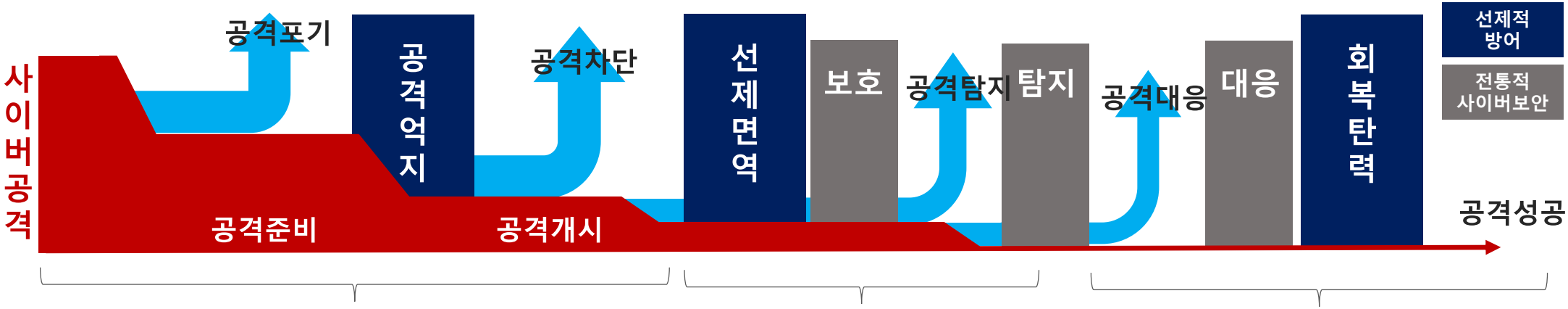
- 능동 방어 : 위협을 미리 예측하여 대비하고 차단
  - "Make it EXPENSIVE, Make it DANGEROUS, Make it WORTHLESS" (영국 통신기업 BT의 선제적 방어 원칙)





사이버공격 패러다임 변화에 유기적으로 대응하고 국가 사이버안보 역량 강화를 위해
능동적/선제적 방어 기술개발 투자에 보다 집중하는 것이 필요

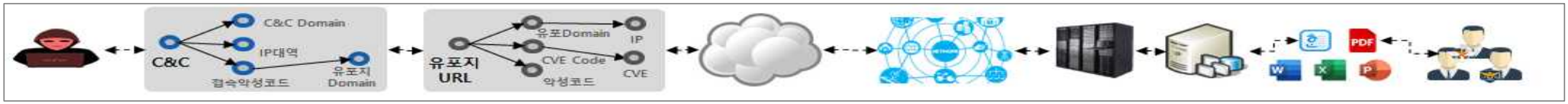
05 주요 보안 이슈④ 능동 방어



공격행위가 발생되지 않도록 능동적 사전 차단

공격이 발생될 경우를 대비한 능동적 사전보호

공격이 지속되는 상황을 대비한
능동적 임무수행 (비즈니스 연속성) 보장



사이버공간

공격자 (해킹조직)	공격 인프라				인터넷	ICT환경				방어자 (전문인력, 이용자)
	데이터	단말	시스템	네트워크		네트워크	시스템	단말	데이터	

기존 사업	공격	VS.	방어
예타 사업	공격	VS.	방어

감사합니다.

정현철 보안블록체인PM, IITP
hcjeong@iitp.kr