

보도시점

2023. 10. 12.(목)
행사 종료 후

배포 2023. 10. 12.(목) 12:00

윤 대통령, '청년 화이트해커들과의 대화' 시간 가져

- 국내외 해킹 대회를 휩쓸고 있는 청년 화이트해커들의 열정과 노력 격려 -
- 사이버안보 경쟁력의 핵심인 「사이버 10만 인재 양성」의 중요성 강조 -
- 「사이버보안 유니콘 기업」이 탄생할 수 있는 성장 기반 조성 의지도 밝혀 -

과학기술정보통신부(장관 이종호, 이하 '과기정통부')는 윤석열 대통령이 오늘 낮 12시, 청와대 영빈관에서 청년 화이트해커들과 산·학·연 관계자들이 참석한 가운데, 「청년 화이트해커와의 대화」 시간을 가졌다고 밝혔다.

오찬과 함께 진행된 이번 행사는 최근 세계 최고 권위의 데프콘(DEF CON) 국제 해킹방어대회 2년 연속 우승 등 국내·외 해킹 대회를 휩쓸고 있는 우리 청년 화이트해커들의 노력과 우수한 성과를 격려하고, 화이트해커 등 사이버 인재 양성 현장의 다양한 목소리를 듣기 위해 마련되었다.

이날 행사에는 국내·외 주요 해킹 방어대회* 수상자, 국내 중고교·대학교의 정보보호학과 등에 재학 중인 학생, 군·검·경 등 주요기관 및 기업 재직자 등 청년 화이트해커 88명을 비롯해 과기정통부 장관, 국가안보실장, 사이버작전사령관, 국정원 3차장 등 정부 및 유관기관 관계자 총 110여명이 참석하였다.

* 데프콘(DEFCON), 사이버공격방어대회, 코드게이트, 나토 락드실드 해킹방어대회 등

본격적인 행사에 앞서, 윤 대통령은 이종호 과기정통부 장관 등과 함께 주요 기반시설인 스마트시티의 모사 환경에 대한 해킹·방어 시연 현장을 참관하고 사이버 공격에 대응하는 화이트해커의 역할과 중요성을 확인하였다.

< 해킹·방어 시연 주요내용 >

- **시연내용** : 스마트시티 교통신호, 전력망 등 주요 기반시설에 대한 사이버 공격에 따른 피해 발생, 화이트해커의 긴급 대응·복구 등을 통해 시스템이 정상화되는 과정 시연

<시연물>

- **시연절차**

- ① (블랙해커 공격) 사이버 공격 개시
- ② (사이버공격탐지) 이상 징후 탐지·알람
- ③ (화이트해커 방어) 사이버공격 대응 및 복구·정상화



이어서 진행된 ‘청년 화이트해커와의 대화’에서 윤 대통령은 청년 화이트해커들의 경험과 고민, 미래에 대한 포부를 청취하였으며, 최정예 사이버 인재 양성과 경쟁력 있는 산업 생태계 조성을 위한 다양한 방안에 대해 참석자들과 의견을 나누었다.

참석자들은 △세계 최고 수준의 해킹대회 우승 경험과 △사이버보안 스타트업 창업 경험, △민간 우수 인재의 軍 유입과 경력 관리, △화이트해커의 성장과 진로 등 다양한 경험과 고민을 나누었으며, 사이버위협 패러다임 변화에 대응하여 글로벌 역량을 갖춘 사이버 인재 양성과 사이버보안 시장 확대를 위해 정부의 지속적인 관심과 지원을 요청하였다.

과기정통부 이종호 장관은 “이번 대화를 통해 화이트해커분들의 생생한 경험과 고민에 대해 다시 한번 생각 할 수 있는 기회가 되었으며, 사이버보안 인재 양성에 대한 막중한 책임감을 느낀다”고 밝히며, “정부는 지난해 발표한 **「사이버 10만 인재 양성방안」**을 체계적으로 실행해 나가는 한편, 국내 보안 산업의 혁신과 글로벌 진출을 위해 국내 최초의 **「사이버보안 유니콘」**이 탄생할 수 있도록 뒷받침해 나가겠다”고 말했다.

아울러, “민·군 협력을 통해 **「사이버 탈피오트 제도」**를 도입하여 軍 보안 인재들이 지속적으로 역량을 키우고, 전역 후 창업을 통해 경쟁력 있는 기업으로 성장할 수 있도록 지원할 것이며, 중소기업, 개인 등 보안 사각지대에 대한 맞춤형 보안서비스·제품 제공, 보안 취약점 점검 활성화를 통해 디지털 시대 보안성 강화를 위해 적극 노력하겠다”고 말했다.

한편, 정부는 우수한 사이버 인재 양성과 정보보호산업 역량 강화를 위해 다양한 정책을 추진하고 있으며, 주요 내용은 다음과 같다.

① 「사이버 10만 인재 양성 방안」의 이행

사이버안보 경쟁력의 핵심 원천인 우수 인재 확보를 위해 지난해 발표한 「사이버 10만 인재 양성 방안」을 체계적으로 실행해 나간다.

먼저, 보안 제품 개발부터 사고대응에 이르는 소 주기에서 잠재력 있는 인재가 최정예 인재로 성장하도록 맞춤형 교육과정을 신설하여 운영하고, 정보보호특성화대학과 융합보안대학원을 지속 확대한다.

< 전주기 최정예 인재 양성 과정 >

교육 대상	중급 과정	고급 과정
개발자(제품 개발자)	(SW 등 IT개발 인력 선발)	⇒ 'S-개발자' ('23년 신설)
화이트해커(사고대응)	'화이트햇 스쿨' ('23년 신설)	'차세대 보안리더(BoB)' (기존)

※ 정보보호특성화대학('23년 5개 → '26년 10개) : 고려대(세종), 세종대, 성신여대, 충남대, 전남대
 융합보안대학원('23년 10개 → '26년 12개) : 강원대, 고려대, 부산대, 성균관대, 순천향대, 전남대, 충남대, KAIST, 경희대, 중앙대

국내 유망한 젊은 연구자가 우수 연구자로 성장할 수 있도록 미국 카네기 멜론대학교, 독일 헬름홀츠연구소 등 사이버보안 분야 세계 최고 대학, 연구기관에 전문인력을 파견*하고, 미국·독일·핀란드 등 글로벌 선도국과의 국제공동연구도 확대한다.

* △해외 우수대학 및 연구소 등에 박사후 연구원 파견, △국내 석·박사 재학생 연구자의 해외 기술연수, 인턴십 등 지원 추진('24~, 신규)

軍의 보안 인재들이 군 복무 중에 지속적으로 역량을 개발하고, 전역 후 보안 기업 창업 등을 통해 산업 성장을 이끌 수 있도록 「사이버 탈피오트 제도」 도입을 추진한다.

※ (단기, '23년~) 군 사이버전문인력 대상 특화 교육 지원, (중장기) 사이버전문사관 임관경로 다양화 및 R&D 수행 지원 등

② 사이버보안 유니콘 육성을 위한 산업 기반 조성

국내 사이버보안 기업의 경쟁력 강화를 위한 「정보보호산업의 글로벌 경쟁력 확보 전략」을 마련('23.9월)하여 국내 산업이 '27년까지 시장규모 30조원, 세계 5위권 시장으로 성장할 수 있도록 적극 추진한다.

먼저, 제로트러스트, SW공급망보안 등 새로운 보안체계의 적용과 미래 산업의 보안 내재화를 통해 신시장을 창출하고, 국산 신기술 적용확산을 통해 지능형 CCTV 등 물리보안을 차세대 성장산업으로 육성한다.

- (신보안체계) 제로트러스트 및 SW공급망보안(통신, 금융 등) 실증 시범사업 추진 확대
- (융합보안) 전략산업 분야(스마트공장, 헬스케어, 로봇, 스마트선박 등) 융합서비스 보안 내재화 지원
- (물리보안) 국산 신기술을 적용한 지능형 CCTV 및 생체인식, 무인점포 분야 수출강화

「K-시큐리티 얼라이언스」 등 기업 간 협력을 기반으로 한국형 통합보안 모델을 구현하고, 중동·동남아 등 신흥시장을 전략적으로 공략하여 글로벌 시장 경쟁력을 확보한다.



민·관 합동의 「사이버보안 펀드 조성」(~'27년 총 1,300억원 규모), 「K-시큐리티 클러스터 벨트*」 등 글로벌 시장 진출 가속화를 위한 산업 생태계를 확충하고, 미래 산업 성장에 필수적인 차세대 사이버보안 전략기술**을 선제적으로 확보한다.

* (판교) 보안 스타트업 육성('17~), (부울경) 지역 보안산업 강화('23.11월~), (송파) 글로벌 클러스터('28~)

** △미래도전(AI·클라우드·ZT 등), △기술산업선도(양자내성, 프라이버시), △안보투자(능동대응기술)



담당 부서	정보보호네트워크정책관 정보보호기획과	책임자	과 장	김경우 (044-202-6440)
		담당자	사무관	임재현 (044-202-6441)
			사무관	임수연 (044-202-6448)
			사무관	최고석 (044-202-6446)
협조 부서	정보보호네트워크정책관 정보보호산업과	책임자	과 장	정은수 (044-202-6450)
		담당자	사무관	김성환 (044-202-6451)
	정보보호네트워크정책관 사이버침해대응과	책임자	과 장	허진우 (044-202-6460)
		담당자	사무관	김승열 (044-202-6461)

□ 화이트해커 개념

- ‘화이트해커(White Hat Hacker)’는 공격자의 관점에서 사이버공간과 정보통신시스템의 보안 취약점을 연구·발견하고 취약점 보완 및 해킹방어 지원 등 보안성 향상을 지원하는 정보보안 전문가
- 사이버 공간을 공격해 중요한 기밀·개인정보를 훔치거나 국가 주요 시설을 마비시키는 목적으로 해킹 기술을 악용하는 블랙해커(Black Hat Hacker)와 구분

< 화이트해커의 주요 업무 >

- (모의해킹·보안컨설팅) 기업·정부기관의 서비스·시스템 분석을 통한 보안 취약점 진단 등
- (관제) 네트워크·시스템에 대한 모니터링을 통해 이상행위 탐지·대응
- (침해대응) 공격이 발생한 시스템·서비스 분석을 통해 피해 규모, 경위 조사 및 추가 피해 방지 등
- (디지털포렌식) 시스템 공격에 대한 증거 분석으로 숨겨진 정보 파악 및 소실 자료 복구 등

□ 화이트해커 양성 현황

- 화이트해커 양성을 위한 초·중·고급의 전문교육과정을 운영* 중이며, 차세대보안리더(BoB) 과정을 통해 ‘리더급’ 화이트해커 양성(‘12~ , 1,648명)

* (초급) 사이버가디언즈(청소년) → (중급) 화이트햇스쿨(청년층) → (고급) 차세대보안리더(고교생·대학생)

- BoB 과정을 통해 양성된 화이트해커의 취·창업률 88%로 공공(국방부, 경찰, 연구기관 등) 및 민간(보안, IT, 금융 등) 분야에서 활동
- 교육 중 수행한 프로젝트를 바탕으로 스타트업 창업(4개 기업 운영)

- 화이트스캔(4기) 대표, 미국 포브스 ‘아시아 글로벌 리더 300인(‘20년)’ 선정
- 테이텀(8기), 2022 대한민국 산업대상, ‘보안솔루션 대상’ 수상(‘22년)
- 트리링(9기), 2021년 예비창업패키지 ‘데이터·네트워크 분야’ 선정(‘21년)
- 레이버훗(10기), 2022년 소셜벤처 경연대회 전국대회 청소년 부문 대상(‘22년)

- 해킹방어대회 입상 및 취약점 제보, 보안기술·논문발표 등 성과창출

대회입상	취약점 제보	기술 발표	논문 발표	기타	합계(‘12~‘22)
895건	1,702건	353건	369건	32건	3,351건

※ DEFCON(‘18, ‘22, ‘23), 코드게이트, 화이트햇콘테스트 등 국내외 주요 해킹방어대회에서 우승 달성

□ 개요

- (목적) ‘해킹 올림픽’으로 불리며, 전 세계 보안전문가와 해커들이 모여 실력을 겨루는 세계 최고 권위의 해킹방어대회
- (대회 개요) '93년 유명 해커인 제프모스(Jeff Moss)에 의해 설립된 세계에서 가장 큰 해커들의 축제로 전 세계 해커들이 참가하여 경연

◇ 개최시기 : 연 1회

※ 개최기간 : 예선 5월(온라인), 본선 8월 개최

◇ 경시분야 : 단일분야 / 팀 단위 참가(국적 및 연령 제한 없음)

◇ 출제유형

- (예선) Jeopardy(문제풀이), Live CTF(토너먼트)
- (본선) Attack & Defense(공방전), King of the Hill(점령전), Live CTF(토너먼트) 등

◇ 시상방식 : 본선 후 당일 1위팀 시상

- 블랙 배지(데프콘 평생 무료 참여 가능) 제공, 차년도 본선 출전권 부여

□ 한국 출전팀 주요 성과

개최연도	팀명	참가성적	국적
2015	DEFKOR	1위	한국
2018	DEFKOR00T	1위	한국
2022	MMM	1위	한국, 미국, 캐나다
	StarBugs	3위	한국
2023	MMM	1위	한국, 미국, 캐나다
	HypeBoy	4위	한국

참고3

해킹·방어 시연 주요내용

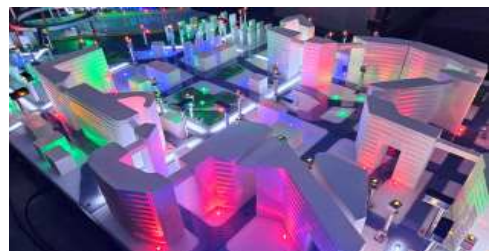
□ 개요

- 스마트시티(세종) 모사 환경에서 주요 기반시설의 해킹 시연을 통해 사이버 공격의 위험성을 보여주고, 국가 안보와 사회 안전을 지키는 화이트해커 역할의 중요성을 강조

□ 시연내용

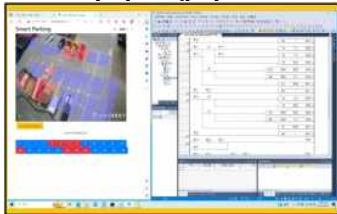
- 스마트시티 주요 기반 시설에 대한 해킹 (블랙해커) 및 방어(화이트해커) 시연
 - ▲ 신호등 체계, ▲ 주차관리 시스템, ▲ 전력망 시스템 작동 오류 및 복구

<시연물>



※ 시연업체 : (주)옵시아(취약점 점검, 모의해킹 및 보안솔루션 제공 기업)

< 시연 절차 >

시연 절차	블랙 해커 공격	■ 블랙해커가 도시 주요 기반시설 사이버 공격 개시 → 도로 교차로 내 신호등 교란으로 교통 혼란 발생 → 주차관리시스템 장애로 차량 입·출차 불가 → 전력 배전설비 이상으로 전력망 마비	
	공격 탐지	■ 스마트시티 보안관제 모니터링 을 통해 실시간으로 주요 기반시설과 네트워크 에 대한 이상 징후 탐지 및 알람	
	화이트 해커 방어	■ 화이트해커가 출동 하여 사이버 공격에 대한 긴급 대응 을 통해 공격 차단 및 복구 , 사이버 공격 재발 방지 를 위한 시스템 취약점 점검 등을 수행	
화면 표시 내용	블랙해커 PC 	보안관제 PC 	화이트해커 PC 
	■ 공격코드가 실행되는 화면, 공격 성공 메시지 등 표현	■ 네트워크 트래픽 등 급증, 오류 메시지 등 표현	■ 주요 기반시설 시스템 복구 및 기능 정상화 표현

I. 추진 배경

- 사이버위협은 중소기업, 융합산업 등 보안이 취약한 분야를 시작으로 디지털 혁신의 가속화에 따라 사회 전 영역으로 확대
 - 주요기업의 해킹, 러시아-우크라이나 사이버전 확대 등 사이버 위협이 국민 일상, 기업 경제활동, 국가안보를 직접적으로 위협
 - 사이버 역량은 사이버보안 제품·서비스를 신속하게 개발하고 잘 활용하는 것이 중요하며 이는 보안인력의 역량이 좌우
 - 인공지능을 활용한 사이버위협 등으로 사이버 전문인력의 중요성은 미래에도 지속될 전망이며, 미(美) 등 주요국은 인력양성을 위해 노력
- * 2022년 유망 직업 1위로 정보보안 분석가 선정(US News & world Report 2022)
 * 미 바이든 대통령은 사이버안보 강화 대책회의 개최, 사이버보안 일자리 50만개 신규 창출 계획 발표

II. 사이버 인력 현황 및 전망

(사이버 인력) 정보 자산을 보호하기 위한 보안 제품·서비스 개발, 보안 정책수립·관리, 사고대응 등 사이버 공격에 대응하는 활동을 하는 인력



- (현황·전망) 산업성장 등을 감안, 사이버 인력은 12.4만명('21년) → 16.3만명('26년) 확대되어 약 4만명의 신규 인력 수요 발생 전망

< 직무별 인력 수요 전망 >

직무별	'21년	'26년	신규수요
제품 개발	1.3만명	1.7만명	0.4만명
보안 관리	9.5만명	12.4만명	3.0만명
사고대응	1.3만명	1.8만명	0.5만명

* 최근 5년의 사이버 인력(7.0%) 및 보안산업인력(5.6%) 증가율 반영

Ⅲ. 비전 및 추진전략

비전	최정예 사이버인력 양성으로 안전한 디지털 강국 구현		
목표	실전형 사이버 인력 10만명 양성	최정예 전문 인재 2,000명 육성	우수 보안 스타트업 25개 창업 지원

추진과제

[전략1] 사이버보안 **초주기 최정예 인력 양성체계** 구축

- ① **대학·대학원의 사이버보안 정규교육 지원 확대**
 - ▶ 융합보안대학원 확대('22년 8개 → '26년 12개) 석·박사 과정 신설
 - ▶ 정보보호특성화대 확대('22년 3개 → '26년 10개)
- ② **보안 특화 교육을 통한 최정예 사이버 인재 육성**
 - ▶ 최정예 보안 SW 개발인력 육성 'S-개발자'(50명)
 - ▶ 화이트해커 육성 강화(^{신규}화이트햇 스쿨 도입 300명)
- ③ **사이버보안 산업 연계를 강화하는 실무형 인재 육성**
 - ▶ 기업 주도형 '시큐리티 아카데미' 과정 도입(200명)
 - ▶ '사이버보안 일자리 플랫폼' 구축

[전략2] **상시 육성 체계와 글로벌 연계** 기반 마련

- ① **온라인 기반 실전형 사이버보안 훈련 체계 강화**
 - ▶ 실전형 사이버훈련장 확대(지역 기반 구축, 훈련과정(3종→9종))
- ② **사이버보안 교육의 지역 확산을 위한 기반 마련**
 - ▶ 권역별 클러스터 내 지역정보보호교육센터 구축
- ③ **글로벌 사이버 인력 네트워크 구축**
 - ▶ ^{가칭}'K-사이버 글로벌 인력 네트워크' 추진

[전략3] **민·관·군 유기적 협력으로 사이버 戰·범죄 대응**

- ① **민·관·군 협력을 통한 공공↔민간의 인력 선순환 구조 마련**
 - ▶ 사이버 부서관 양성을 위한 전문대학 신설
- ② **민간 인적 자원을 활용하는 탈피오트, 사이버예비군 도입**
 - ▶ '사이버 탈피오트' 도입(우수인력 선발→軍 사이버안보 분야 복무→취(창)업)
 - ▶ 민간 사이버 전문인력을 '사이버 예비군'으로 조직·운영
- ③ **침해대응기관(KrCERT) 사이버 인력 역량 강화 지원**
 - ▶ 사이버 보안 재직자 역량 강화 프로그램((가칭)K-Shield/Public) 운영

붙임

10만 사이버 인재 양성 방안('22년~'26년)

분야	과정	양성 방안
신규 인력 공급 (4만명)	정규 과정 (1.0만명)	[고급] 대학원(0.1만명) (확대) 융합보안대학원 확대 (8개교 → 12개교, 석사 → 석·박사) [중급] 대학(0.4만명) (확대) 정보보호특성화대 확대(3개교→10개교) [초급] 특성화고·전문대학(0.4만명) (신규) 사이버부서관 특화 정보보호 전문대학
	특화 교육 (3.9만명)	[고급] 최정예 우수 인력 확보(0.1만명) (신규) 최정예 보안제품 개발과정 'S-개발자'(50명) - 정예 화이트해커(Best of Best, BoB) 양성(200명) [중급] 실무형 인재 양성(3.6만명) (확대) 구직자 대상 K-Shield Jr.(300명→1000명) (신규) 중급 화이트해커(화이트햇 스쿨) 양성(300명) (신규) 시큐리티 아카데미 도입(200명) [초급] 보안관리 인력 공급 확대(0.2만명) (확대) ICT 융합 보안교육 확대(400명→600명)
재직자 역량 강화 (6만명)	사이버 훈련장 (2.5만명)	'디지털 실전형 사이버훈련장' 구축(25만명) [고급] 실전형 사이버 공격·방어 훈련 실시 [중급] 침해사고 대응 등 해킹방어 기본기술 습득 [초급] 동영상 강의, 실습 등 기초역량 교육
	지역 교육 (2.6만명)	'지역 정보보호교육센터' 설립(2.6만명) [중·고급] 악성코드 분석·탐지 등 실무형 교육 [초급] 사이버보안 소양, 보안제품 실습 등 기초 직무 교육
사이버보안 산업 종사(2.5만명)		- 사이버보안 제품·서비스 개발·공급 - 보안 취약점 진단 - 보안제품 설치 및 유지보수
일반기업·기관 보안관리(7.5만명)		- 기업·기관의 보안 관리 및 운영 - 보안정책 수립 및 적용

1 추진배경

- 사이버공격의 양적 증가* 뿐 아니라 AI 활용 등으로 고도화되고, 전쟁수단화** 되면서, 각국은 정보보호산업 육성을 안보와 직결된 문제로 인식, 경쟁력 확보에 주력***

* 사이버공격으로 인한 글로벌 경제피해는 '15년 3조 달러에서 '22년 6조 달러로 2배 이상 증가('22, PwC)

** 러시아는 우크라이나 침공 시 악성코드와 랜섬웨어를 활용한 사이버 전면전을 감행 (MS, '22)

*** 미국(국가안보전략, '22.10), EU(사이버방어전략, '22.11), 영국(국가사이버전략, '22.12)등 관련 정책 발표

- 또한, 디지털심화 및 원격근무 확산 등을 계기로, 고성장 중인 글로벌 보안시장을 선점하려는 기업들의 주도권 경쟁도 본격화

※ 글로벌 정보보호 시장규모는 '23년 3,019억 달러(약 393.9조), '26년까지 연평균 8.5% 성장 전망(Markets&Markets, '22)
시장의 성장세 속에 벤처캐피탈의 집중 투자로 글로벌 사이버 보안 유니콘도 급증('19년 13개 → '23년 58개)

⇒ 정보보호산업을 미래 전략산업으로 육성하여, 우리 힘으로 사이버 안보를 실현하고, 고성장 중인 글로벌 보안시장 주도권 확보 추진

- (문제점) 국내 산업은 그간 양적으로 성장*하고 있으나, 내수·공공 편중**, 보안 투자 부족, 기업 간 공조문화 미흡 등으로 질적 성장 한계

* '18년 시장규모 10조에서 '22년 16.2조로(정보보호산업협회, '23.8) 4년 만에 60% 이상 고성장 달성

** '22년 정보보안 매출액(5조 6,171억 원)중 수출은 2.76%(1,552억 원), 국내 보안 기업 기술개발 및 성장 애로사항 1위(40.8%)는 자금조달 (정보보호산업협회, '22.9)

- (시사점) 우리산업의 경쟁력 강화를 위해서는 ①딥테크·신기술시장 개척, ②기업 간 협업활성화, ③신흥시장 공략, ④투자촉진으로 정책방향 집중 필요

국내 산업 문제점 분석과 시사점

국내시장 분석		시사점
전통적 보안분야(관계 등)에 안주하는 시장문화 (23, CTA 국가별 혁신순위에서 F학점(최하점))	 기술혁신성	ZT, SW공급망, AI 및 융합보안 등 딥테크·신기술 시장 개척
단일제품 위주의 시장, 기업 파트너십 부재로 글로벌 시장점유율 정체	 시장점유율	대·중·소 기업 간 전략적 파트너십을 통한 경쟁력 확보
내수·공공 중심 시장(年 약 5조)으로 단일기업 가치 1조원 이상 도달 어려움	 시장규모	신흥국 등 해외시장 진출로 국내시장의 한계 돌파
경직된 시장으로 민간 투자매력도 하락 (국내 보안기업의 애로사항 1위는 자금조달)	 투자기반	정부주도 정책펀드 조성을 통해 투자 활성화 기반마련

② 목표 및 추진전략

비전	글로벌 정보보호산업 강국 도약		
목표	'27년까지 정보보호산업 세계 5위권 진입	'27년까지 정보보호산업 시장규모 30조원 달성	'27년까지 보안 유니콘 육성
추진 전략	1 보안패러다임 전환 주도권 확보 및 新시장 창출 2 협업기반 조성을 통한 신흥시장 진출 강화 3 글로벌 공략을 위한 단단한 산업 생태계 확충 4 차세대 정보보호 기술 경쟁력 확보		

□ 보안패러다임 전환 주도권 확보 및 新 시장 창출

새로운 보안체계 적용과 미래산업의 보안내재화를 통해 新시장을 창출하고, 융합보안 및 물리보안 산업 강화를 통해 글로벌 보안시장 진출 확대

① 사이버보안 패러다임 전환에 따른 新기술시장 주도권 확보

- (제로트러스트) 기존 경계보안의 한계를 해소하기 위한 '제로트러스트 단계별 모델 및 전환 로드맵'을 수립하고, 신속한 도입·확산 추진('24~)
 - * 산업 분야별 최적의 ZT 모델 구현 및 확산에 필요한 가이드라인 고도화('23.7, 가이드1.0→ '24. 가이드 2.0)
- 통신·금융·의료 등 기반 분야를 중심으로 기존 경계 모델을 ZT 보안 모델로 적용·확산하는 시범사업 추진('24~'27)
- (SW공급망 보안) SW 공급망 공격에 능동적으로 대응하고, 해외 SW 무역장벽에 대비하기 위한 SW 공급망 보안점검·대응 인프라* 구축('24~)
 - * SW 자산식별, 보안취약점 점검 및 컨설팅, 실시간 모니터링 및 상황전파, 보안패치 등 공급망 전반의 보안대응 지원

② 유기적 협력·선제적 보안내재화로 미래형 융합보안 시장 개척

- (융합보안 내재화) 스마트헬스케어, 자율차 등 주요 분야 보안 내재화 프로세스*를 마련하고, 미래 전략산업(로봇, 우주 등) 등 융합보안 신분야 개척
 - * (스마트헬스케어 예시) 서비스 취약점 점검 → 취약점 보완 → 시험결과 확인 → 스마트 의료기기 (HW/SW) 인증·허가 심사시 보안성 항목은 시험결과 확인으로 인증
- (융합보안 협력체계 구축) 자율차·스마트선박 등 산업별 보안요구사항*에 전략적으로 대응하기 위한 유관부처·기관 '융합보안 협력체계' 구축('24~)
 - * (국토부) EU의 자율차 사이버 보안관리체계 준수 규제, (해수부) 국제해사기구의 스마트선박 사이버보안 요구사항 규제 등
 - * 국제규제 대응을 위한 공동연구, 신규 인증제도 마련에 필요한 인증기준 수립, 법령 재정비 등 협력 추진

③ 국산 신기술 적용·확산을 통해 물리보안을 차세대 성장산업으로 육성

- (지능형 CCTV 수출확대) 정부 R&D로 국산화된 핵심부품^{CCTV SoC}의 보급을 확산(10개社→40개社)하고, 해외수출 가속화('24~)

※ 물리보안 분야 CCTV 관련 수출규모 '21년 1.6조에서 '27년 3조원까지 확대 추진

- 2세대 국산 지능형 SoC칩* 개발·양산을 추진하여(~'24), 우리 제품의 글로벌 시장점유율 확대를 연계('22, 3%→'27, 10%)

* 2세대 SOC칩(EN677): CPU 등 성능개선 및 보안성 강화, 영상이미지·화질개선 및 보정기능 탑재 반도체 설계·제조 전 과정 국산화 통해 미·독·일 등 주요국에 수출 확대 기대('24년 1분기 출시 예정)

- (생체인식 기반강화) 지문·안면 중심 생체인식 성능평가 분야를 확대(2종→ 6종, 정맥, 홍채 등)하여 생체인식 물리보안 시장확대('24~)

- (스마트 안심점포 확산) 국내 보안기술*을 집약시킨 '한국형 무인 점포'를 구현하고, 실증을 통해 상용화 추진('~'24)

* AI(객체인식, 모션인식)인지, 자동인증·결제, 성인인증 기술 등 기존 외산기술(클라우드픽(중국), AIFI(미국)) 대체

- 개발된 우수 무인기술·제품을 소상공인 무인점포에 지원하여 범죄 등 사회문제 해결을 지원하고, 무인보안 시장 확대 추진

※ 경찰청 및 지자체와 협력, 출입통제장치 및 지능형 CCTV 등 지원 후 범죄발생을 등 성과 추적('23, 총 120개소)

□ 협업 기반 조성을 통한 신흥시장 진출 강화

기업 간 협력을 기반으로 한국형 통합보안 모델을 구현하고, 신흥시장을 전략적으로 공략하여 글로벌 시장 경쟁력 확보

① 통합보안 모델 구축을 위한 「K-시큐리티 얼라이언스」 추진

- (통합보안 협업체계 강화) 혁신적인 통합솔루션·서비스 개발을 위한 민간주도형 전략적 협업 체계 강화 추진('24~)

- 민간주도 공동·협업 통합보안 사업화모델, 표준화 및 상호운용성 확보 등을 유도하고, 판로·투자·해외진출시 우선지원

- (통합보안 시범사업) 현장수요 기반 우수 통합보안 모델*을 우선 선정하고, 시범사업을 통해 개발하여 협업 활성화 마중물로 활용('24~, 年 5개)

* 통합보안 모델 예시: 이벤트 로그(SIEM) + 엔드포인트 보안(EDR) + 자동화된 통합관제(SOAR)가 결합된 단일 통합 솔루션 등

※ 협업성과공유회, 성과사례집 및 협업추진 가이드 발간(연 1회), 우수 상호운용성 표준제정 등 추진('24~)

② 국제협력 기반의 신흥시장 진출 가속화

- (전략거점 재편·확대) 중동·동남아 등 신흥시장 집중공약을 위해 중동거점을 사우디로 재편하고(‘23.7~), 베트남 거점을 신설(‘23.12~), 6대 거점 중심 진출 지원 강화

※ 現 해외 5대 전략거점: 미국(실리콘밸리), 동남아(인니), 중동(오만), 아프리카(탄자니아), 중남미(코스타리카)

- (민·관 협력 글로벌 조달수주) 중동·동남아 기금·공공조달 사업 프로젝트 수주를 위한 민·관 협력형 ‘시큐리티 팀 코리아’ 구성·지원(‘24~)

※ (우수사례) ASEAN Cyber Shield Project: 한아세안 경험기금 사업으로, KISA가 프로젝트 제안 및 대표 계약자로 사업수주 후 공개입찰로 국내 보안기업을 수행사업자로 선정(‘23~’25, 총 120억 규모)

□ 글로벌 공약을 위한 산업 생태계 확충 및 차세대 보안기술 확보

우리 보안기업의 글로벌 시장진출 가속화를 위해 시설확충·펀드조성 미래전략 기술 확보 등 지속성장 환경 조성에 집중 투자

① 보안 스타트업 육성^{판교} 및 지역 보안산업 강화^{부울경}, 글로벌 시큐리티 클러스터^{송파}로 구성된 「K-시큐리티 클러스터 벨트」 조성(‘28)

- ※ △ (판교) 입주공간 지원, 테스트베드, 사이버훈련장, 교육프로그램, 기업 간 네트워킹 등 창업·스케일업 지원
- △ (지역) 지역 전략산업(스마트조선·항만·시티 등)에 특화된 기업육성 및 인력양성, 훈련 인프라 지원
- △ (송파) 기업 성장 및 차세대 기술 개발(R&D), 세계수준의 보안인력 양성, 민·관·군 협력을 통한 사이버 공격 대응

② 「사이버보안 펀드」를 조성하여 민간투자의 마중물로 활용

- (펀드조성) 기업의 안정적 기술개발 및 민간투자 활성화를 위해 민·관 합동 「사이버보안 펀드」 조성(‘27, 총 1,300억 원 규모)

- (투자활용) AI 및 제로트러스트 등 유망 분야 스타트업 지원 및 기업 간 M&A를 통한 스케일업 지원에 집중 투자 유도(펀드결성액의 50%이상)

- ※ △ 스타트업 분야 유망신기술(AI, ZT, 양자 등) 및 원천분야(네트워크, 5G, 암호 등) 제품·서비스 개발 및 사업화
- △ M&A분야 중소·중견 사이버보안 기업의 인수합병을 통한 통합 제품·서비스 개발 및 사업화

③ 국내·외 기술·시장 분석 통해 ①미래 도전, ②기술·산업 선도, ③안보투자 등 주요 R&D 영역을 도출하고, 전략적 투자 추진(‘24~)

* △ 미러도전(AI·클라우드·ZT 등), △ 기술산업선도(양자내성, 프라이버시), △ 안보투자(능동대응기술)

④ 국제 공동연구를 통한 글로벌 보안기술 경쟁력 확보

- (선도국 협력연구) 미국·독일·핀란드* 등 사이버보안 분야 강점을 지닌 선도국과 공동 연구를 통해 글로벌수준 기술 확보(‘24~)

* 협력연구(예시): △ 미국(가상자산 불법행위 추적, AI 영상보안 등 美DHS 협력), △ 독일(스마트공장·자율차 보안 등 獨 CISA 협력), △ 핀란드(6G 등 이동통신 보안)

- (신흥국 지원연구) 동남아·중동 등 주요 신흥시장을 전략적으로 공략하기 위한 현지 시장 수요기반 보안기술 모델 공동개발(‘24~)

* 협력연구(예시): △ 동남아전문인력 양성체계, PKI 등 인증제도, △ 중동(스마트시티보안, 통합관제 등)