

#1. 2023년 사이버 보안 직무

2023. 11. 05(일)

이택현

목차

I. 사이버 보안 직무 소개

II. 업무유형

I. 사이버보안직무 소개(1/4)

< 2015년 10대 유망직업 >

순위	유망직업	평균 총점
1위	금융자산운용가	41.92
2위	컴퓨터보안전문가	41.73
3위	하이브리드 동력시스템 개발자	39.19
4위	경영컨설턴트	39.01
5위	마케팅전문가	38.07
6위	유비쿼터스러닝 교수설계자	37.95
7위	태양광발전연구원	37.75
8위	기후전문가	37.71
9위	상담전문가	36.96
10위	실버시터	33.45

* 평균총점 50점 만점 기준

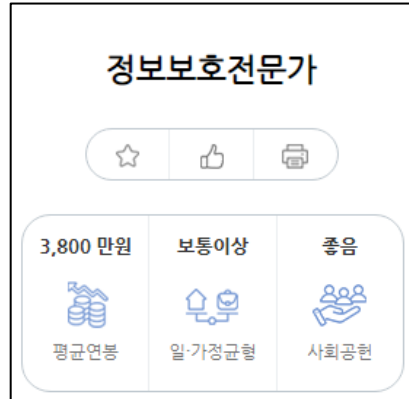
< 자료제공 : 취업포털 커리어 (www.career.co.kr) >

미래 유망직업 15선

1. 사물인터넷 전문가
2. 인공지능 전문가
3. 빅데이터 전문가
4. 가상현실/증강현실 전문가
5. 생명과학 연구원
6. 정보보호 전문가
7. 로봇공학자
8. 자율주행차 전문가
9. 스마트팜 전문가
10. 환경공학자
11. 스마트 헬스케어 전문가
12. 3D 프린팅 전문가
13. 드론 전문가
14. 소프트웨어 개발자
15. 신·재생에너지 전문가

한국고용정보원(2023)

I. 사이버보안직무 소개(2/4)



❓ 관련직업명

컴퓨터보안전문가, 산업보안전문가

❓ 관련학과 및 관련자격

· 관련학과

[스마트정보과](#) [정보통신공학과](#) [정보보호학과](#) [컴퓨터공학과](#) [인터넷정보학과](#) [컴퓨터보안과](#)


· 관련자격

[정보처리기사](#) [정보보안기사](#) [정보시스템관리사](#) [정보시스템감사사\(CISA\)](#) [정보관리기술사](#)

❓ 하는일

- 정보보호전문가는 정보시스템의 보안 정책을 세우고, 시스템에 대한 접근 및 운영을 통제하며, 침입자가 발생했을 때에는 신속하게 발견하고 대응해 시스템을 보호하는 일을 합니다.
- 허가받지 않은 사람이 정보시스템이나 컴퓨터에 불법 접근하여 정보를 탈취, 변조, 파괴하는 등의 공격 행위를 할 때, 이를 방어하거나 예방합니다.
- 각종 컴퓨터바이러스의 발생과 해커의 침입에 대비하여 보안 방법을 만들고, 정보를 보호하는 방화벽의 설정을 변경하거나 관리합니다.
- 정보시스템의 정보가 손상되는 크래킹을 당했을 때 이를 빠르게 복구하고 새로운 보안 방법을 마련합니다.
- 정보시스템의 위험하고 약한 곳을 확인하여 대비를 하고 컴퓨터바이러스 백신 프로그램을 개발하여 보급하거나 바이러스에 감염된 데이터를 살려냅니다.

❓ 핵심능력

 수리·논리력

❓ 적성 및 흥미

· 적성

- 해커들의 최신 해킹 및 크래킹 기법이나 악성 코드나 바이러스 분석을 위해 체계적이고 논리적인 수리·논리력이 필요합니다.

· 흥미

- 평소 최신 IT 기술과 보안기술 장비에 대한 자료를 읽거나 수집하고 깊게 탐구하는 과정을 즐기는 사람에게 적합합니다.
- 기업의 담당자나 임원들을 설득하여 정보보호정책을 실행하도록 해야 하기 때문에 다른 사람을 설득하고 토론 및 논쟁을 즐기는 사람에게 적합합니다.

❓ 분류

표준직업분류 : 정보 보안 전문가 (세분류 2233)

고용직업분류 : 정보보안 전문가 (세분류 1350)

I. 사이버보안직무 소개(3/4)

Q 직업현황

· 직업전망

향후 5년간 정보보호전문가의 일자리 규모는 다소 증가할 전망입니다. 개인정보보호 등 정보보안은 우리 생활과도 아주 밀접한 문제이며, 더욱이 국가기반시설에 대한 보안 문제는 국가안보 또는 국익과도 이어지기 때문에 전문가를 통한 보안 유지의 필요성이 커지고 있습니다. 특히 사물인터넷과 클라우드 컴퓨팅 환경의 확대, 스마트폰 등 모바일기기의 확대 등 초연결 사회로의 변화는 필연적으로 컴퓨터 보안의 수요를 강화하고 있습니다. (자료: 워크넷 직업정보)

· 임금수준 및 직업만족도



평균연봉
3,800 만원

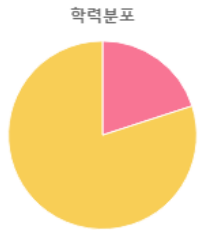
정보보호전문가의 관련 직업인 정보보안전문가의 평균연봉(중앙값)은 3,800만원으로, 조사 대상 전체 직업 평균연봉(중앙값)인 4,072만원과 비교하여 낮은 수준입니다. (자료: 워크넷, 정보보안전문가(2021))



직업만족도
67.1 %

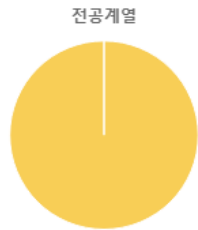
정보보호전문가의 관련 직업인 정보보안전문가의 일자리 증가 가능성, 발전가능성 및 고용안정에 대해 재직자가 느끼는 직업만족도는 67.1%입니다. (자료: 워크넷, 정보보안전문가(2021))

· 학력분포 및 전공계열



중졸이하(0%) 고졸(0%)
전문대졸(20%) 대졸(80%)
대학원졸(0%) 박사졸(0%)

[자료: 워크넷, 정보보안전문가 직업정보(2021)]

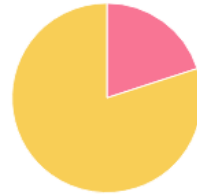


인문계열(0%) 사회계열(0%)
교육계열(0%) 공학계열(100%)
자연계열(0%) 의학계열(0%)
예체능계열(0%)

[자료: 워크넷, 정보보안전문가 직업정보(2021)]

· 학력분포 및 전공계열

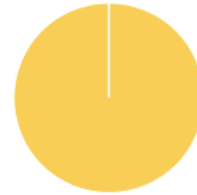
학력분포



중졸이하(0%) 고졸(0%)
전문대졸(20%) 대졸(80%)
대학원졸(0%) 박사졸(0%)

[자료: 워크넷, 정보보안전문가 직업정보(2021)]

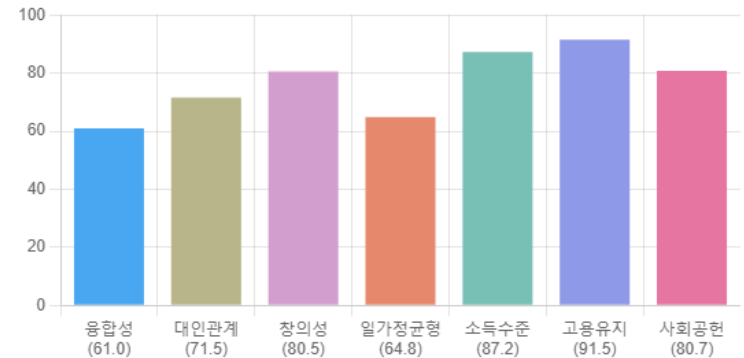
전공계열



인문계열(0%) 사회계열(0%)
교육계열(0%) 공학계열(100%)
자연계열(0%) 의학계열(0%)
예체능계열(0%)

[자료: 워크넷, 정보보안전문가 직업정보(2021)]

Q 한국의 직업지표



[자료: 한국직업능력연구원, 맞춤형취업지원을 위한 직업지표 연구(2020-22)]

I. 사이버보안직무 소개(4/4)

Q 업무수행능력

중요도	능력명	설명
100	가르치기	다른 사람들에게 일하는 방법에 대해 가르친다
97	물적자원 관리	업무를 수행하는데 필요한 장비, 시설, 자재 등을 구매하고 관리한다
97	인적자원 관리	직원의 근로의욕을 높이고 능력을 개발하며 적재적소에 인재를 배치한다
97	공간지각력	자신의 위치를 파악하거나 다른 대상들이 자신을 중심으로 어디에 있는지 안다
94	조직체계의 분석 및 평가	환경이나 조건의 변화가 조직의 체계, 구성, 방식에 어떤 영향을 미칠지 분석하고, 시스템의 효율성을 평가한다
93	기억력	단어, 수, 그림 그리고 철자와 같은 정보를 기억한다
93	범주화	기준이나 법칙을 정하고 그에 따라 사물이나 행위를 분류한다
91	재정 관리	업무를 완료하기 위해 필요한 비용을 파악하고 구체적 소요 내역을 산출한다
90	기술 설계	사용자의 요구에 맞도록 장비와 기술을 개발하여 적용한다
90	장비의 유지	장비에 대한 일상적인 유지보수를 하고 장비를 유지하기 위해 언제 어떤 종류의 조치를 취해야 하는가를 안다

[자료 : 워크넷, 정보보안전문가 직업정보(2021)]

Q 지식중요도

중요도	능력명	설명
98	컴퓨터와 전자공학	컴퓨터의 하드웨어, 회로판, 처리장치, 반도체, 전자장비에 관한 지식
89	통신	전화기, 네트워크, 방송 등의 통신기기를 조작하고 통제하는데 필요한 지식
87	사무	워드 프로세스, 문서처리 및 기타 다른 사무절차에 관한 지식
83	공학과 기술	다양한 물건을 만들고 설계하거나 서비스를 제공하기 위해 필요한 공학적인 원리, 기법, 장비 등을 실제로 적용시키는 지식
79	안전과 보안	사람들과 재산을 보호하기 위해 필요한 지식
70	교육 및 훈련	사람을 가르치고 훈련시키는데 필요한 방법 및 이론에 관한 지식
66	법	법률, 규정에 관한 지식
63	산수와 수학	연산, 대수학, 통계, 기하학의 계산 및 응용에 관한 지식
62	국어	맞춤법, 작문법, 문법에 관한 지식
61	경영 및 행정	사업운영, 기획, 자원배분, 인적자원관리, 리더십, 생산기법에 대한 원리 등 경영 및 관리에 관한 지식

[자료 : 워크넷, 정보보안전문가 직업정보(2021)]

Q 업무환경

중요도	능력명	설명
84	앉아서 근무	앉아서 근무하는 빈도
84	자동화 정도	업무의 자동화 정도
80	이메일 사용하기	업무 수행하면서 이메일 사용하는 정도
76	공문, 문서 주고받기	업무 수행하면서 공문이나 문서를 주고받는 정도
75	반복적인 신체활동, 정신적 활동	지속적이고 반복적인 신체적 활동이나 정신적 활동의 중요성
74	재택근무	재택근무 가능성
70	전화 대화하기	업무 수행하면서 전화로 대화하는 정도
69	사물, 도구, 조종 장치를 다루기 위해 손사용	손으로 사물, 도구 혹은 조종 장치를 다루면서 근무하는 빈도
67	다른 사람과의 상호작용	업무 수행위해 팀/집단으로 함께 일하는 것의 중요성
62	불쾌하거나 무례한 사람 상대	불쾌하거나, 화나거나, 혹은 무례한 사람을 대하는 빈도

[자료 : 워크넷, 정보보안전문가 직업정보(2021)]

II. 업무유형(1/7)

정보보안분야 : “보안정책”, “보안운영”, “보안점검”, “보안모니터링”, “보안컨설팅”, “보안개발”

구분		세부내용	필요스킬
관리 보안	보안정책	<ul style="list-style-type: none"> ●기업 정보 자산에 대한 정책적 보호 조치 수행 - 키워드 : ISMS-P, ISO 27001, PCI-DSS, 국내 법률 	<ul style="list-style-type: none"> - 법률해석 - 컴플라이언스 대응 - 정책, 사업 적합성 검토
	보안운영	<ul style="list-style-type: none"> ●기업 정보 자산에 대한 정책적 보호 조치 수행 - 키워드 : 엔드포인트보안, 네트워크보안, 시스템보안, 클라우드 보안 	<ul style="list-style-type: none"> - 운영체제 운용 스킬 - 보안장비 운영 스킬 - AWS, GWS 솔루션
	보안점검 (모의해킹)	<ul style="list-style-type: none"> ●기업 및 서비스 보안 취약점 분석 및 공격 수행 - 키워드 : 웹 해킹, 시스템 해킹, 리버스엔지니어링, 네트워크 해킹, 0-Day(퍼징 스킬) 	<ul style="list-style-type: none"> - OWASP - 도구 : Web Proxy, IDA, Ollydbg
	보안 모니터링	<ul style="list-style-type: none"> ●보안 모니터링 및 차단, 보안사고 대응 - 키워드 : 보안관제(SIEM), 침해사고대응(CERT) 	<ul style="list-style-type: none"> - 보안 로그 수집 분석 - 이상 탐지 패턴 개발 - 침해사고대응(Forensic)
기술 보안			

II. 업무유형(2/7)

법제처 : <https://www.law.go.kr/>

The screenshot shows the homepage of the Law Commission of Korea. It features a top navigation bar with links like '법령' (Laws), '자치법규' (Local Regulations), '행정규칙' (Administrative Rules), etc. The main content area has a search bar and a list of recent laws. On the left, there are quick links for '기관별 찾기' (Find by Institution), '법분야별 찾기' (Find by Legal Field), and '최신법령' (Latest Laws). The bottom section includes '이번호 시행법령' (This Issue's Enacted Laws) and '주제별 생활법령 정보' (Thematic Living Laws Information).

한국인터넷 진흥원 : <https://www.kisa.or.kr/>

The screenshot shows the KISA website's '가이드라인' (Guidelines) section. It displays a table of security advisories with columns for '번호' (Number), '제목' (Subject), '등록일' (Registration Date), '조회수' (View Count), and '첨부파일' (Attachment). The table lists several advisories related to security patches for various systems.

번호	제목	등록일	조회수	첨부파일
47	실감콘텐츠 보안모델 해설서 및 사례집	2023-03-08	481	
46	자율주행차 보안모델 해설서 및 사례집	2023-03-08	684	
45	스마트공장 보안모델 해설서 및 사례집	2023-03-08	849	
44	디지털헬스케어 보안모델 해설서 및 사례집	2023-03-08	488	

레그테크 : <https://regtech.fsec.or.kr>

The screenshot shows the RegTech website's '연구보고서' (Research Report) section. It displays a table of research reports with columns for '번호' (Number), '구분' (Category), '세부구분' (Sub-category), '제목' (Subject), '등록일' (Registration Date), and '조회수' (View Count). The table lists several reports related to financial security and digital assets.

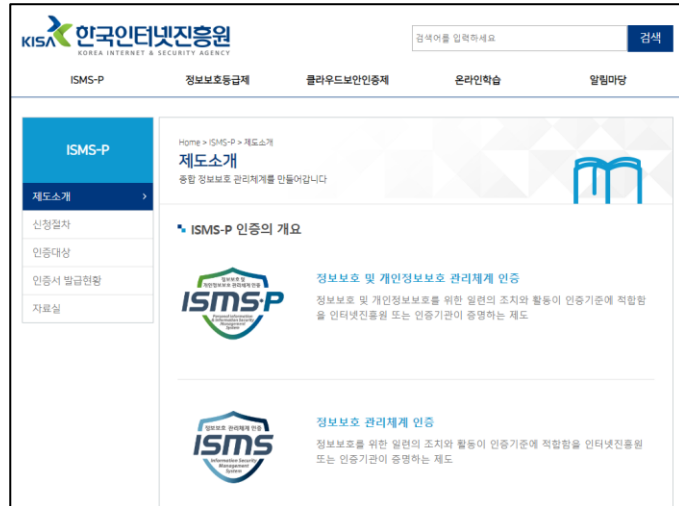
번호	구분	세부구분	제목	등록일	조회수
342	연구 보고서	정책	'23년 3-4월 금융보안 및 디지털자산 국내외 정책동향 요약 보고서	2023.05.15.	51
341	연구 보고서	정책	EU 및 국내 가상자산 관련 법률 제정 동향 검토	2023.05.02.	86
340	연구 보고서	정책	국내외 음성AI(딥보이스) 활용 및 정책 동향 검토	2023.05.02.	72

금융보안원 : <https://fsec.or.kr>

The screenshot shows the Financial Security Agency's homepage. It features a grid of service tiles with icons and text, including '통합보안 관제' (Integrated Security Monitoring), '마이데이터' (My Data), '금융보안 교육' (Financial Security Education), '데이터 전문기관' (Data Specialist Institution), '핀테크 보안' (Fintech Security), and '데이터거래소' (Data Marketplace).

II. 업무유형(3/7)

ISMS-P : <https://isms.kisa.or.kr>



BSI ISO 27001(국제표준정보보호관리체계)



NIST CSF(CyberSecurity Framework)



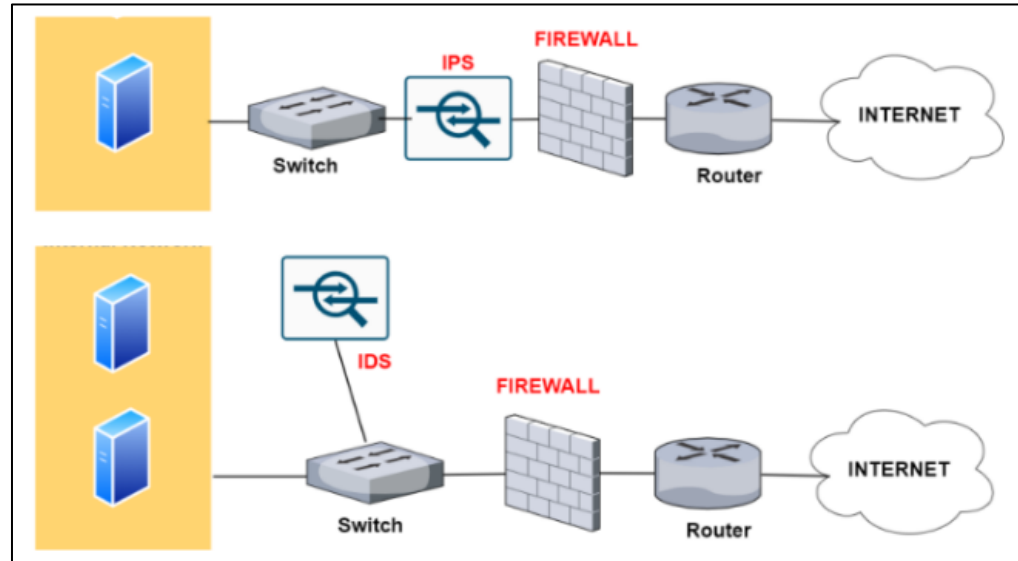
주요정보통신기반시설 보호체계 <https://www.isac.or.kr>



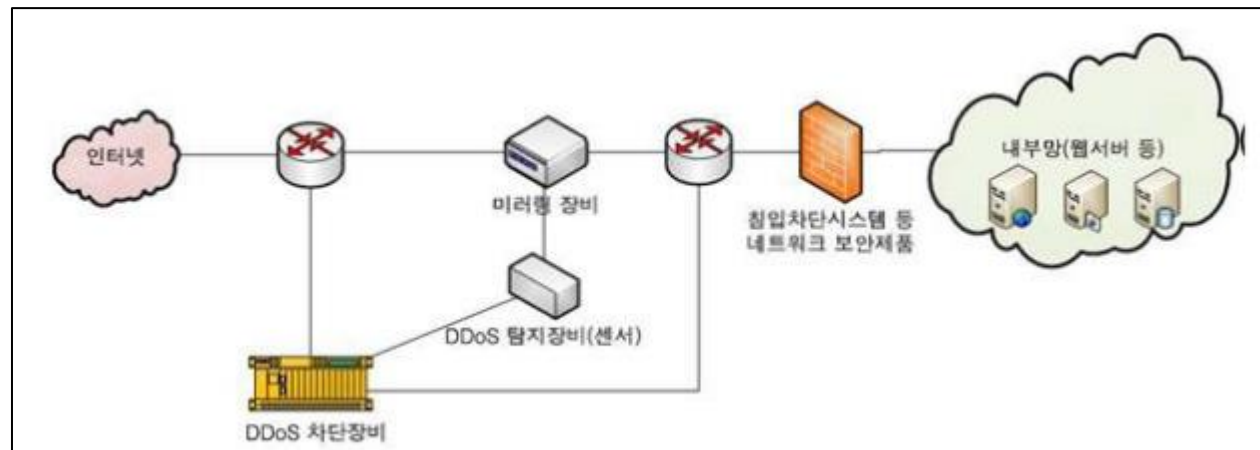
II. 업무유형(4/7)

보안운영

보안장비운영
(IDS, IPS, FW)



DDoS 장비
(탐지, 차단)



보안점검



보안점검(모의해킹) 수행 절차



보안관제센터 운영 (SOC, Security Operation Center)



#2. 2023년 사이버 보안 동향

I. 개요

II. 사이버 보안 위협 동향

III. 사이버 보안 위협 대응 전략

IV. 2030년 사이버 위협 전망

V. 2023년 주요 보안 키워드

Q&A

I. 개요

사회 인프라와 생활 전반의 디지털화가 가속화 되면서, 사이버 보안 위협이 증가하고 있음

개요

- **사회 기반시설과 일상 생활의 ICT 의존도 증가**
 - ✓ 수자원, 원자력, 교통, 에너지 등 사회 인프라에 대한 ICT 의존도 증가
 - ✓ 국내 가구당 인터넷 접속률 99.7%, 국민 이용률 91%
- **디지털 가속화로 인한 사이버 위기 증가**
 - ✓ IT융합 서비스에 대한 보안 리스ٹ 증가
 - ✓ 제조사 장비 백도어로 인한 보안 리스크 증가
 - ✓ 코로나 19로 인한 오프라인 디지털화의 가속화
- **인공지능 기술 발전으로 인한 불확실성 증가**
 - ✓ 사고 발생시 보안, 알고리즘 문제인지 판별 어려움
 - ✓ 전투용 로봇 등장으로 인한 불확실 성 증가

세부내용

- 기술문제 발생 가능성 1위 : CyberSecurity Failure

Social cohesion erosion	27.5%	
Infectious diseases	26.4%	
Mental health deterioration	26.1%	
Cybersecurity failure	19.5%	

※ 출처 : World Economic Forum, "The Global Risks Report 2022 17th"

- 사회 인프라 보안사고 노출 증가



“디지털 의존도가 높을 수록 피해의 규모 더욱 증가”

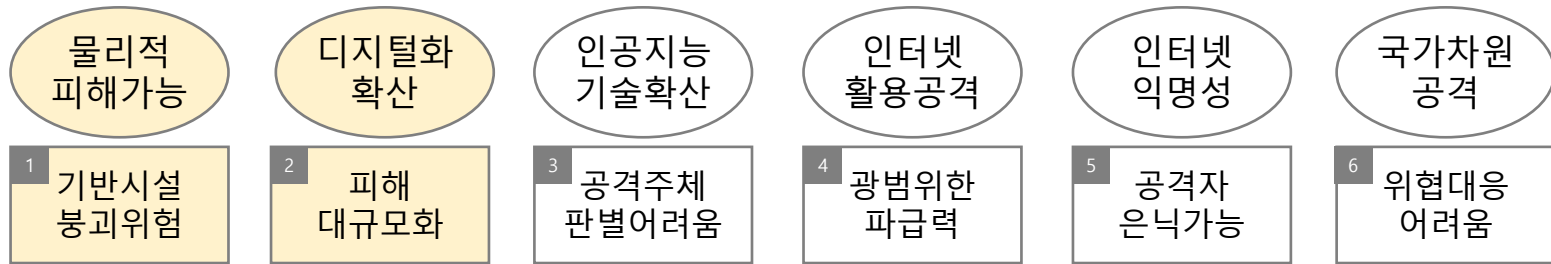
//

디지털화로 발생할 수 있는 사이버 위협을
신속하게 인지하고 관리할 수 있는 노력 필요

II. 사이버 보안 위협 동향(1/3)

사이버 보안 위협은 일반 기업과 정부에서 감당하기 어려운 수준으로 증가하고 있음

사이버 보안 위협의 특징과 예상되는 문제점



1 물리적 피해 가능

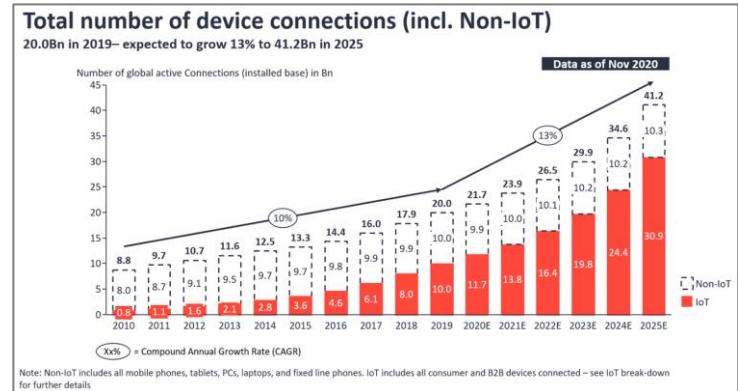
✓ 사이버 공격으로 기반시설 붕괴 가능

- 미국 물관리시스템 해킹(21년) - 인도 핵발전소 해킹(19년)



2 디지털화의 확산 : 초연결사회 진입

✓ IoT/M2M 등 디지털화된 모든 자산 피해 발생 가능

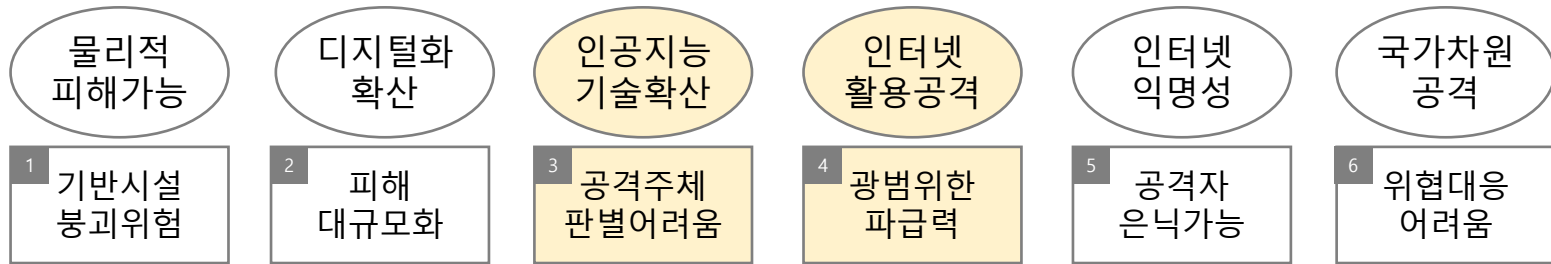


※ 출처: IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker

II. 사이버 보안 위협 동향(2/3)

사이버 보안 위협은 일반 기업과 정부에서 감당하기 어려운 수준으로 증가하고 있음

사이버 보안 위협의 특징과 예상되는 문제점



3 인공지능 기술 확산

✓ 공격 주체 판별이 어려움, 책임소재 판별 어려움



4 인터넷 활용 공격

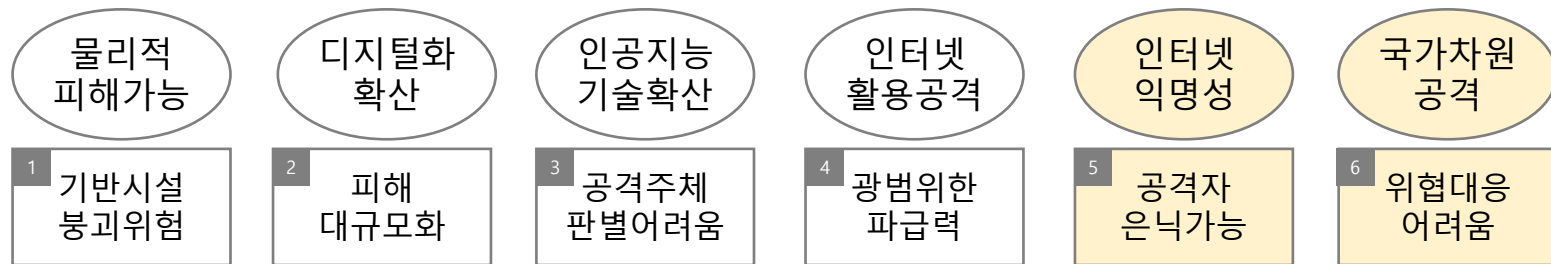
✓ 인터넷을 활용하여 전 세계 공격 피해 가능



II. 사이버 보안 위협 동향(3/3)

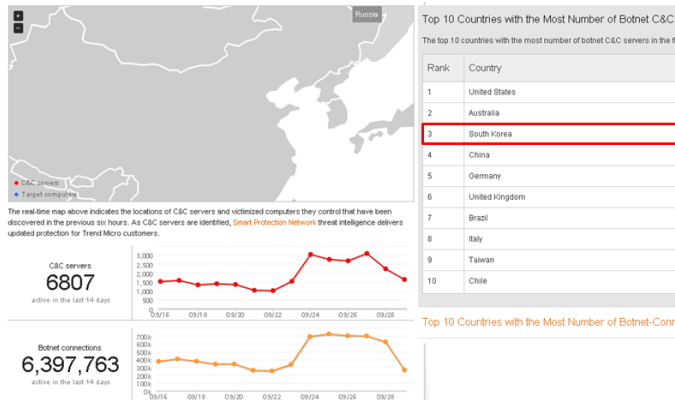
사이버 보안 위협은 일반 기업과 정부에서 감당하기 어려운 수준으로 증가하고 있음

사이버 보안 위협의 특징과 예상되는 문제점



5 인터넷 익명성

✓ 공격지 경유를 통한 실제 공격자 은닉 가능



6 국가 차원의 공급망 해킹 공격

✓ 네트워크 장비 유통 과정에 Firmware 백도어 설치



III. 사이버 보안 대응 전략(1/3)

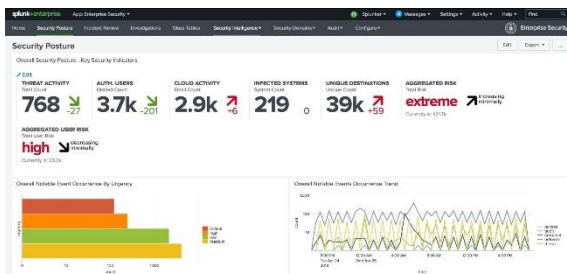
고도화되는 사이버 보안 위협을 대응하기 위해서 다양한 사이버보안 활동을 수행하고 있음

정부와 기업의 지속적인 사이버 보안 위협 대응 노력

보안 활동	1	보안장비운영 (FW, SIEM 등)	2	사이버보안 지수개발관리	3	사이버위협 정보공유체계구축	4	신기술(5G, IoT) 주요보안기술연구	5	AI SecOps연구 (Broadcom, Splunk)
	한계점	보안분야, 서비스 분야 결합 분석 어려움	설문 등을 통한 지수 생성 (비실시간, 주관적)	폐쇄적 운영, 사후 정보 공유	한정된 범위의 기술연구	대중화되지 않음, 단일지표 중심감시				

1 보안장비운영(FW, SIEM 등)

✓ 다양한 보안 장비 모니터링 및 감시 운영



2 사이버 보안 지수 개발 관리

✓ 국가별 사이버 보안 지수 관리를 통한 경쟁 촉발

Belfer Center National Cyber Power Index 2020 "Top 10"			Specific Rankings	
#	Country	Overall score	Capability	Intent
1	United States	50.24	1	2
2	China	41.47	2	1
3	United Kingdom	35.57	3	3
4	Russia	28.38	10	4
5	Netherlands	24.18	9	5
6	France	23.43	5	11
7	Germany	22.42	4	12
8	Canada	21.50	11	9
9	Japan	21.03	8	14
10	Australia	20.04	16	8

III. 사이버 보안 대응 전략(2/3)

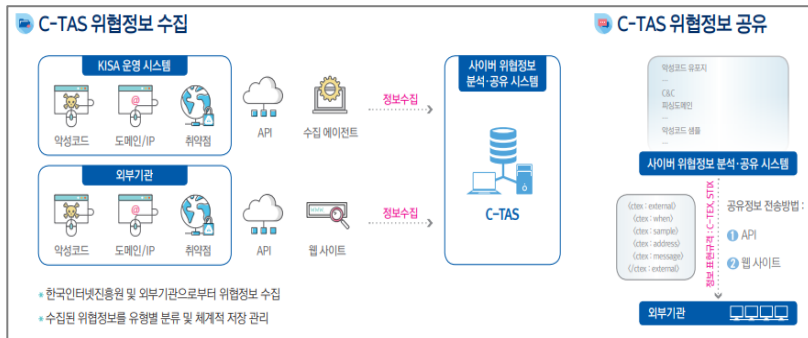
고도화되는 사이버 보안 위협을 대응하기 위해서 다양한 사이버보안 활동을 수행하고 있음

정부와 기업의 지속적인 사이버 보안 위협 대응 노력

보안 활동	1	보안장비운영 (FW, SIEM 등)	2	사이버보안 지수개발관리	3	사이버위협 정보공유체계구축	4	신기술(5G, IoT) 주요보안기술연구	5	AI SecOps연구 (Broadcom, Splunk)
	한계점	보안분야, 서비스 분야 결합 분석 어려움	설문 등을 통한 지수 생성 (비실시간, 주관적)	폐쇄적 운영, 사후 정보 공유	한정된 범위의 기술연구	대중화되지 않음, 단일지표 중심감시				

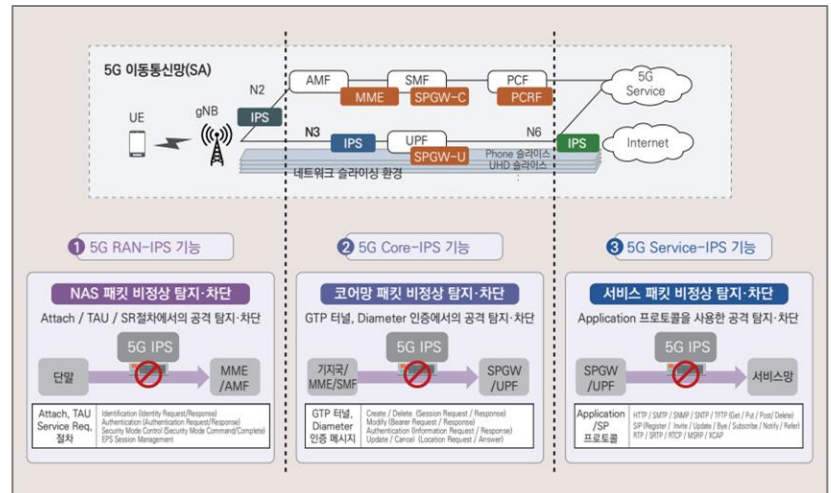
3 사이버 위협 정보 공유 체계 구축

✓ 다양한 보안 장비 모니터링 및 감시 운영



4 신기술(5G/IoT 등) 주요 보안 기술 연구

✓ 핵심 보안 기술 연구 및 기술력 확보 노력



III. 사이버 보안 대응 전략(3/3)

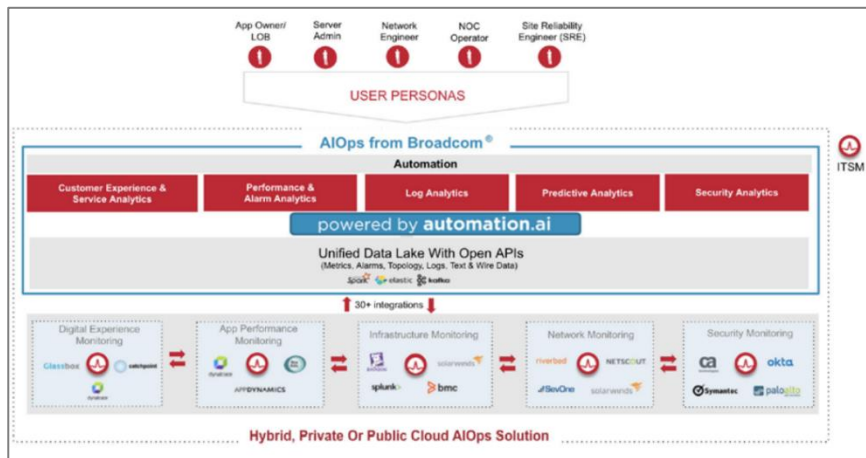
고도화되는 사이버 보안 위협을 대응하기 위해서 다양한 사이버보안 활동을 수행하고 있음

정부와 기업의 지속적인 사이버 보안 위협 대응 노력

보안 활동	1	보안장비운영 (FW, SIEM 등)	2	사이버보안 지수개발관리	3	사이버위협 정보공유체계구축	4	신기술(5G, IoT) 주요보안기술연구	5	AI SecOps연구 (Broadcom, Splunk)
	한계점	보안분야, 서비스 분야 결합 분석 어려움	설문 등을 통한 지수 생성 (비실시간, 주관적)	폐쇄적 운영, 사후 정보 공유	한정된 범위의 기술연구	대중화되지 않음, 단일지표 중심감시				

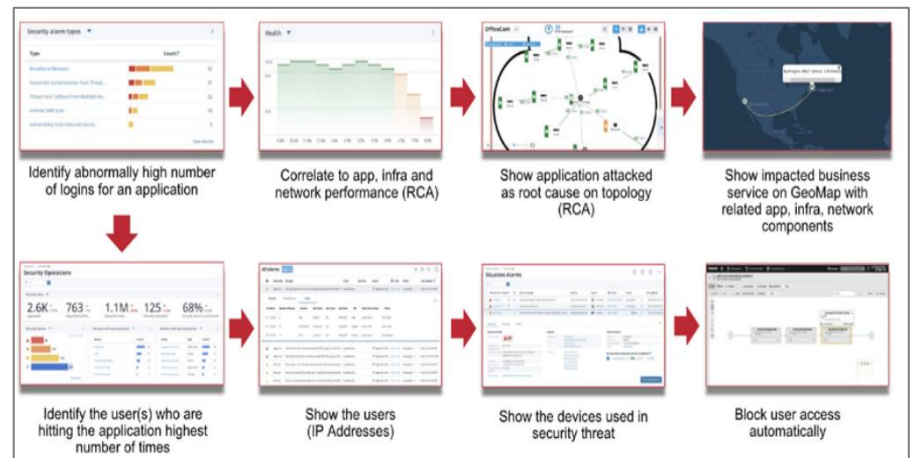
5 AI 기술 정보보안 분야 적용(AI SecOps)

✓ AI기술 보안운영 적용 Framework(예시)



출처 : Broadcom

✓ 이상 징후 탐지 및 원인 분석, 차단 대응 절차(예시)



#3. 2023년 주요 보안 키워드

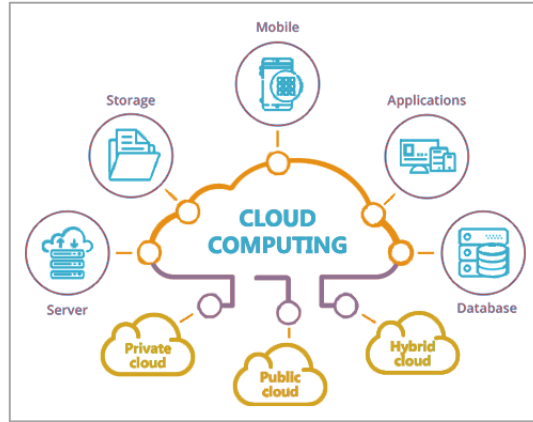
IV. 2023 주요 보안 키워드

ZTA(Zero Trust Architecture)

디지털 대전환 가속화 및 '제로트러스트 아키텍처(ZTA)' 도입 필요성 증대



재택근무 확대



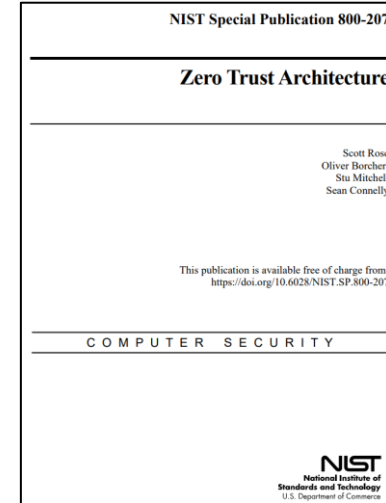
클라우드 컴퓨팅 증대



모바일 기기 활용 확대



IoT 기기 확대



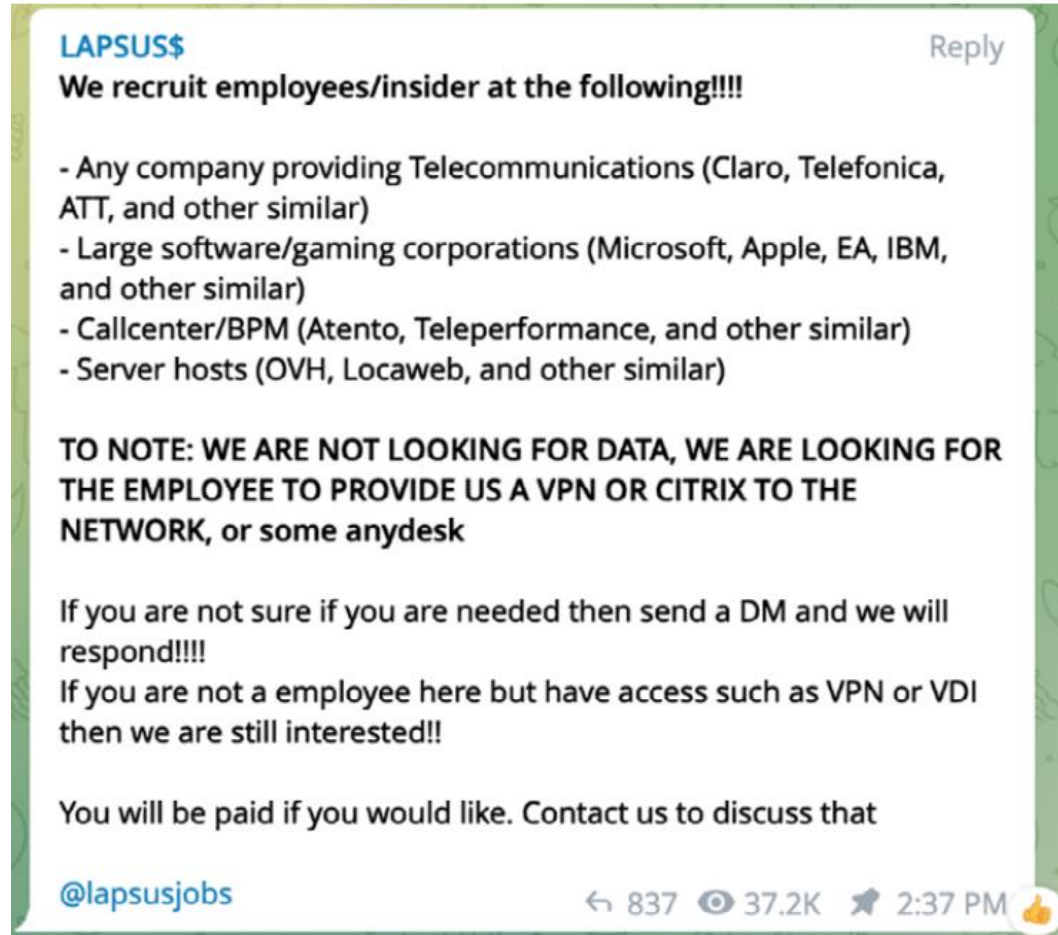
미국 NIST
제로트러스트
아키텍처
(SP-800-207)
'20년 8월



국가 사이버 보안
개선 행정명령

제로트러스트
보안정책 채택
('21년 2월)

‘22년 세계 주요 대기업 Lapsus\$ 공격으로 인한 피해 발생



✓ 기업 내부망 원격접속 정보 구입

- VPN : Virtual Private Network
- VDI : Virtual Desktop Infrastructure
- RDP : Remote Desktop Protocol

✓ 공격절차

Step1) 기업 접속 정보 구입 및 확보

Step2) 내부망 접근 및 주요 권한 획득

Step3) 목표 데이터 유출

Step4) 시스템 계정 및 정보 삭제 등 추적 방지

Step5) 협상

**공격 대상 원격 접속 정보를
공개적으로 구매하는 특이점 존재**

그림 : Microsoft, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction"

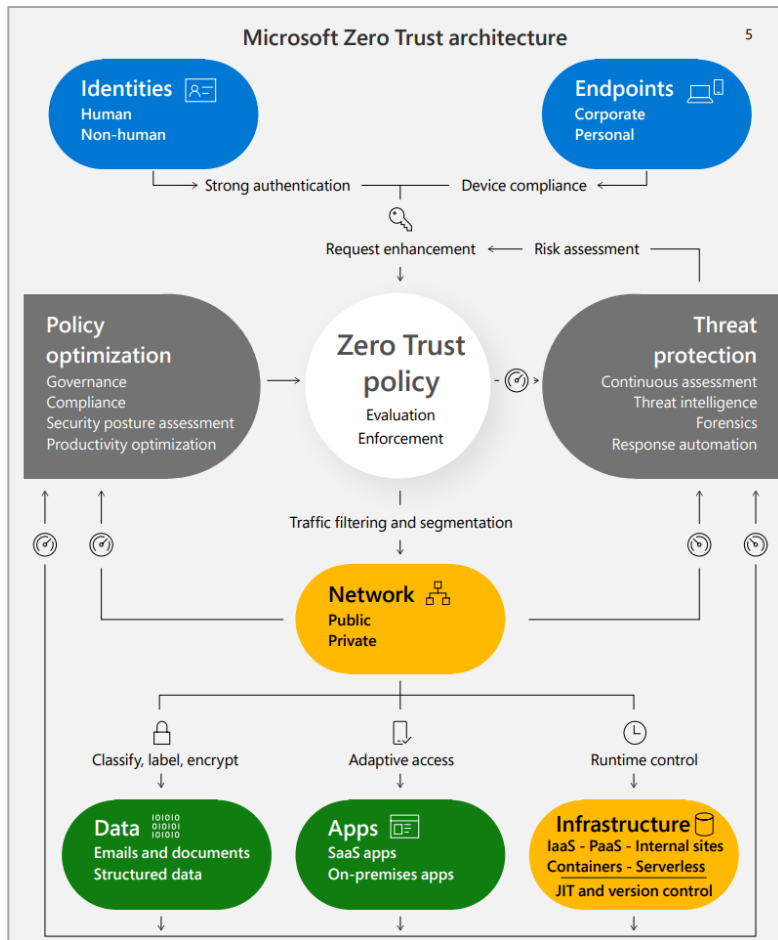
참조 : 한국인터넷진흥원, 상반기 사이버 보안 위협 동향 보고서, 2022

IV. 2023 주요 보안 키워드

ZTA(Zero Trust Architecture)

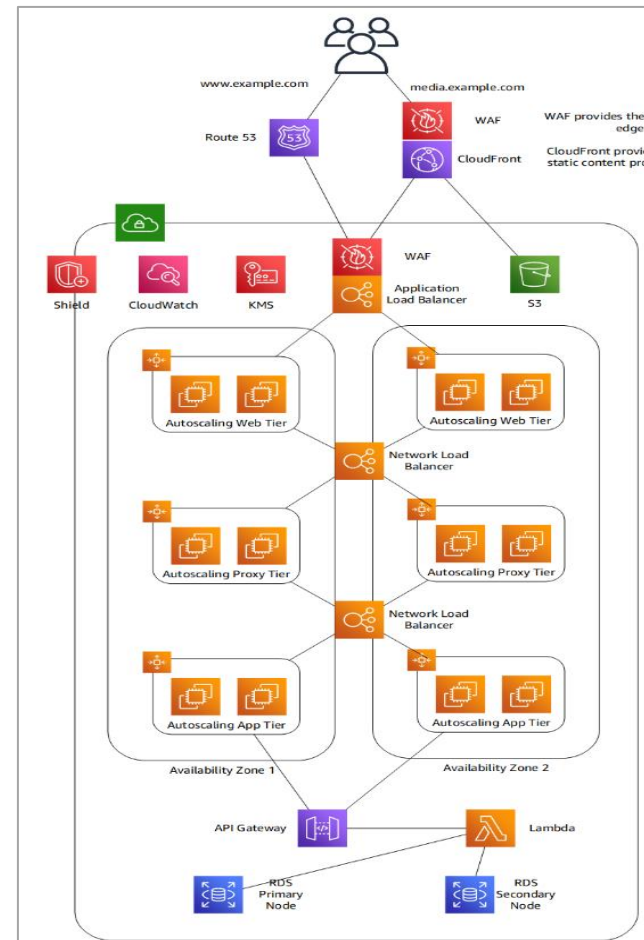
다양한 민간 기업에서 ZTA에 대한 아키텍처를 제안하고 있음

Microsoft Zero Trust Architecture



출처 : Microsoft. The Comprehensive Playbook for Implementing Zero Trust Security, 2022

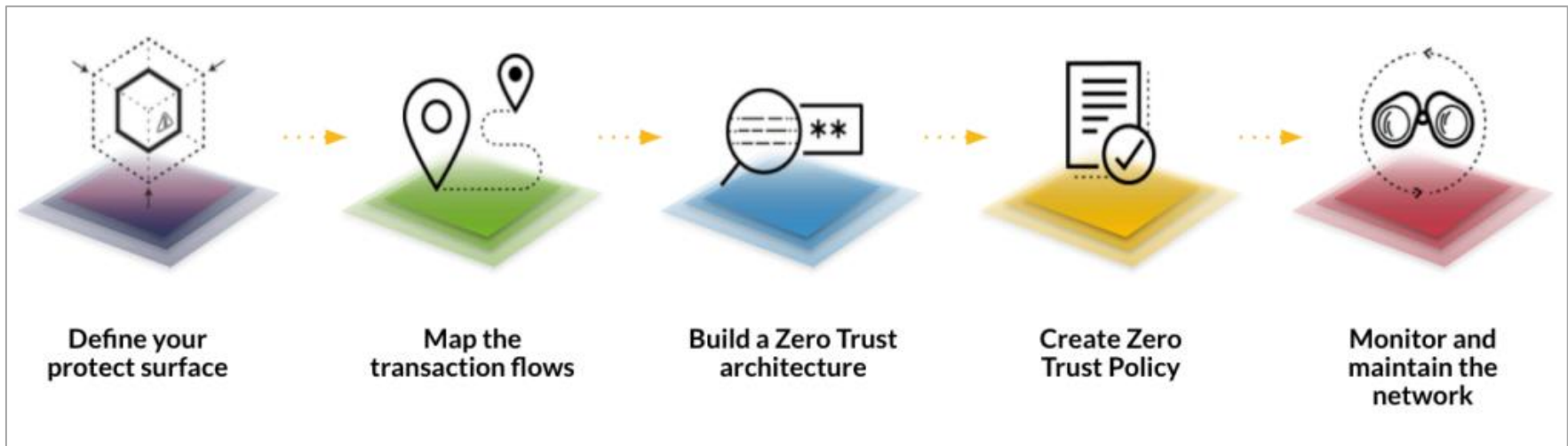
AWS Zero Trust Architecture



출처 : AWS, How to think about Zero Trust architectures on AWS 2020

미국 NSTAC(국가안보통신자문위원회) Zero Trust 구현 계획 발표

- 1) Define your Protect Surface : 주요 보호 대상 및 요소 식별
- 2) Map the transaction flows : 주요 보호 자원 트랜잭션 흐름 매핑 (통제 구간 판단)
- 3) Build a Zero Trust Architecture : Zero Trust 아키텍처 구축
- 4) Create Zero Trust Policy : Kipling Method(5W1H) 기반 Zero Trust 정책 생성
- 5) Monitor and Maintain the Environment : 트래픽 모니터링. 전체 절차 반복 수행



IV. 2023 주요 보안 키워드

오픈소스 활용 리스크(1/2)

디지털 환경 전환 과정에서 오픈소스 활용이 증가하고 있으며, 이 과정에 라이선스 분쟁 발생

구글 Java 소스코드 분쟁('10~'21)



VS



아마존 엘라스틱 유료 사용('15~)



VS



H사 오픈소스코드 미공개('16~'17)
205만(약 25억) 달러 합의





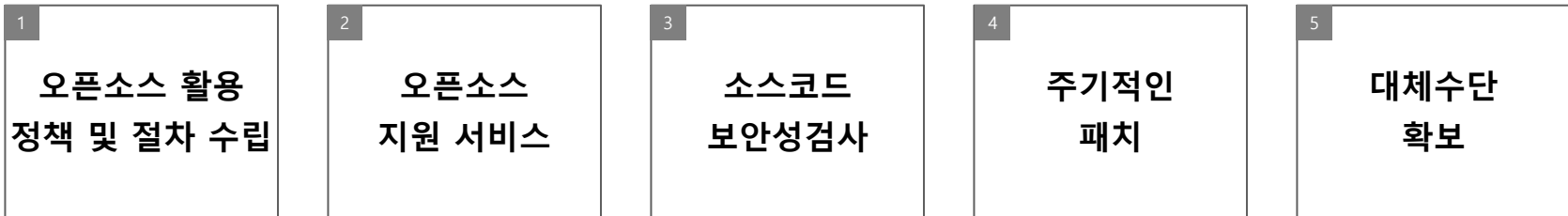
- 주요 오픈소스 라이선스 종류 및 특징 : Apache(28%), MIT(26%), GPL(20%), BSD(7%)

상업적이용	소스코드공개		변경사항 고지	
	의무	선택	의무	선택
GPL, BSD, Apache, MPL, LGPL, GPL	GPL, MPL, LGPL	MIT, BSD, Apache	Apache, LGPL, GPL	MIT, BSD, MPL

참조 : 과학기술정보통신부, 2021년 공개소프트웨어 라이선스 가이드 ([링크](#))

오픈소스 활용 보호 대책을 수립하여, 라이선스 분쟁 및 보안 취약점 노출 관리 필요

- 오픈소스 활용 보호대책



- 오픈소스 분석 점검 도구

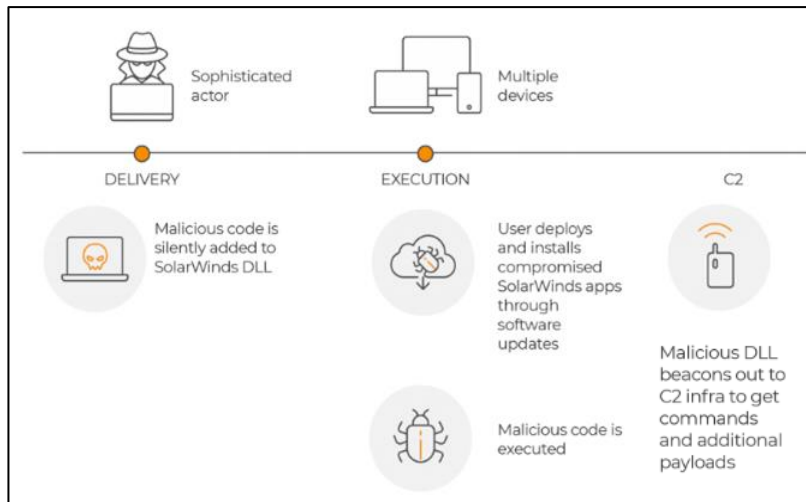
도구명	회사명	라이선스 분석	취약점 탐지	의존성 관리	비용
코드아이	저작권위원회	O	X	X	무료
Black Duck	Synopsys	O	O	O	유료
Sparrow	스패로우	O	O	O	유료
Synk Open source	Synk	O	O	O	유료
WhiteSource	Coontec	O	O	O	유료

IV. 2023 주요 보안 키워드

사이버 복원력(Cyber Resilience)(1/2)

사이버 위협 예측의 어려움으로, 예방 보다는 사고 발생시 효과적으로 대응하는 복원력 중요

- S사 모니터링 솔루션 해킹('20년)



- 유럽 OVH 데이터센터 화재('21)



※ 출처 : <https://www.ebizbank.co.kr/117>

※ 사이버 복원력(Cyber Resilience) : 사이버 자원에 대한 공격과 손상을 예상하고, 적응하거나 빠르게 복구하는 능력(NIST, SP 800-160)

사이버 복원력 확보와 제 3자 리스크 관리를 위한 정책 및 제도 노력



- 운영복원력 강화를 위한 관행 : Sound practices to strengthen operational resilience
- NIST SP 800-160 : Developing Cyber-Resilient Systems



- 디지털 운영 복원력 법안 : Digital Operational Resilience Act, DORA



- 운영 복원력 : 서비스, 아웃소싱 및 타사 위험 관리
(Operational Resilience : Impact tolerances for important business services,
Outsourcing and third party risk management)

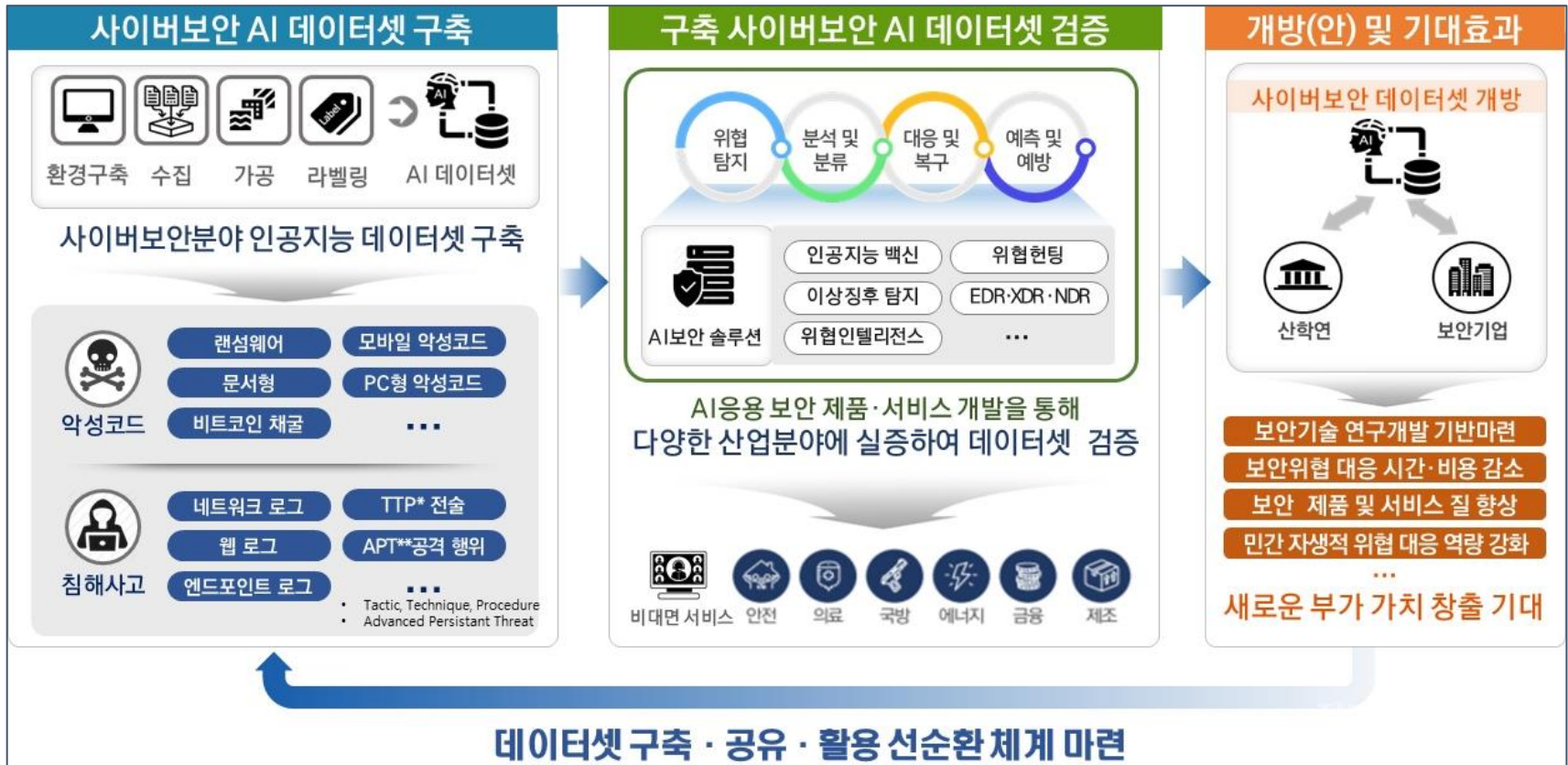


- ISO 22301 : 비즈니스 연속성 경영시스템(BCMS)

사이버 보안 데이터셋을 오프라인으로 제공하고 있으며, 향후 온라인 제공을 준비하고 있음

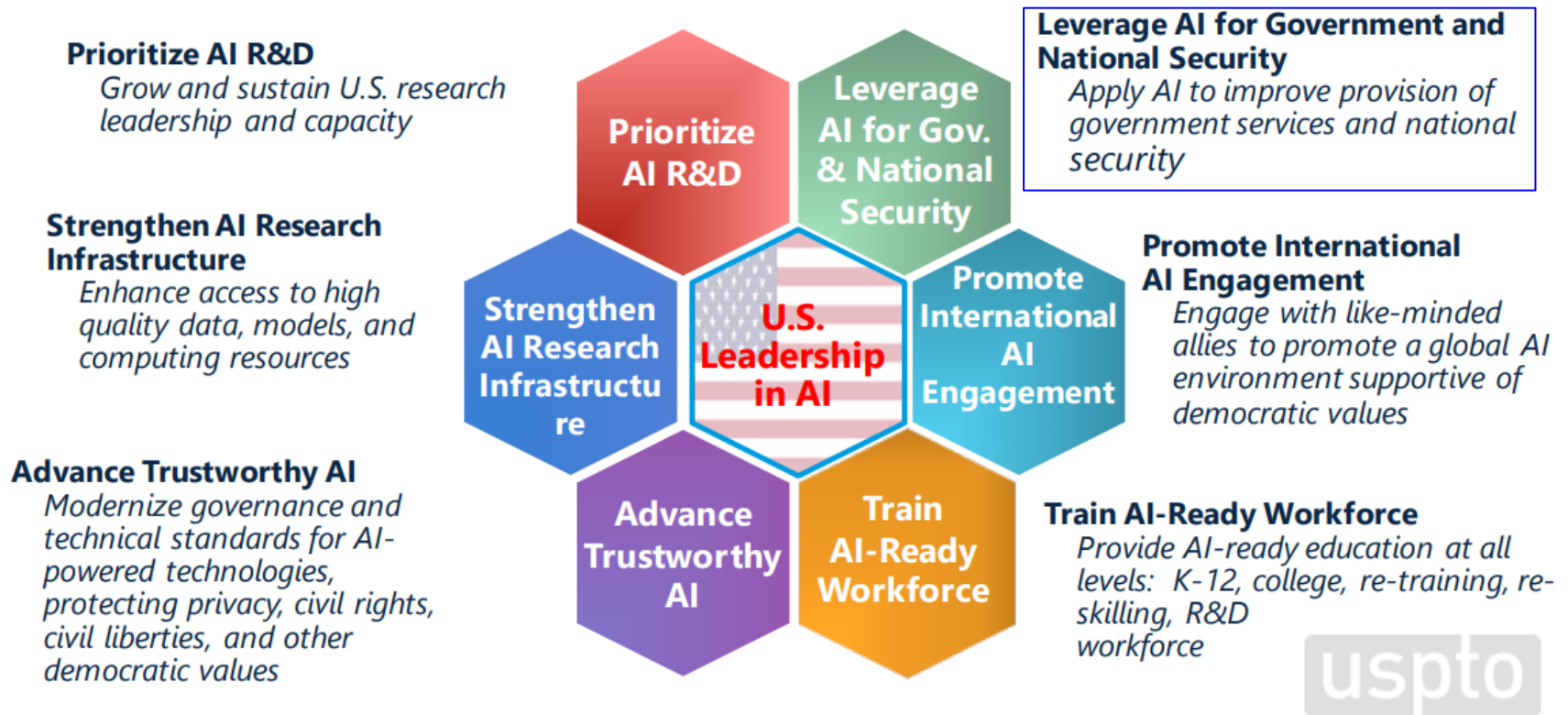
사이버 보안 분야 특화 인공지능 학습데이터(악성코드, 침해사고) 8억건 구축

- ① 악성코드 : 악성코드파일, 속성정보(도구명, 유포지 등), 사회적 관심 키워드 등
- ② 침해사고 : 침해행위(시스템, 네트워크, 장비등), 침해사고 단계별 행위, 침해사고 시나리오 등



AI 전략 추진을 위한 '정부-학계-민간' 연계한 'AI 중심 거버넌스' 구축 노력

- 미국 : 국가 AI 이니셔티브실(National Artificial Intelligence Initiative (NAII))
 - 정부 부처 및 산학연과의 협력을 통한 미국 AI 전략 이행('21년~)



인공지능이 장착된 치명적 자율무기(LAW, 킬러로봇) 신형 병기로 인한 위협

- 인간 개입없이 스스로 목표물을 선택하고 공격하도록 설계 됨. 육지, 하늘, 바다, 우주에서 동작 가능



다이나믹스 보스턴(현대자동차)

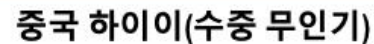


미공군(무인공격기-AI시스템장착)



일본 킬러로봇(KURATAS)

- 인간 개입없이 스스로 목표물을 선택하고 공격하도록 설계 됨. 육지, 하늘, 바다, 우주에서 동작 가능



IV. 2023 주요 보안 키워드

초거대 AI모델(Large Language Model)

AI 분야에서 OpenAI, 마이크로소프트 진영과 구글이 주요하게 경쟁할 것으로 판단됨



VS



2021년 Alphabet Inc.
매출의 81% 광고 수익

IV. 2023 주요 보안 키워드

인공 지능은 “약한, 강한, 초” 수준으로 분류하고 있으며, ChatGPT 기술은 강한 인공지능 초기 버전으로 판단됨

약한
인공지능
(ANI)

한정된 분야에 대하여 문제 해결 능력을 보유하고 있는 AI



- 구글 알파고
- IBM 왓슨
- 카네기멜론대학 딥블루

강한
인공지능
(AGI)

범용적 분야에 대하여 독립적으로 사고하며 문제 해결 능력을 보유한 AI



- 아이언맨 자비스
- HER 영화의 사만다
- OpenAI ChatGPT(?)

초 인공지능
(ASI)

모든 영역에서 인간을 뛰어넘는 인공 지능으로 스스로 목표 지식의 발전 가능



- 어벤저스 비전
- 터미네이터 SkyNet

IV. 2023 주요 보안 키워드

사이버 보안 성숙도(Cyber Security Maturity)

사이버 보안 로드맵 수립 및 지속적인 성숙도 관리를 통한 보안 위협 관리 필요



※ 출처 : 2022 CSO 양성교육 - 사이버 공격 동향, 김영희 교수님

Q & A