기업 및 직무 분석

팀 명 밥 풀 이 들

팀 장 김 신 아 20231773

팀 원 조 승 민 20231801

팀 원 이 승 진 20231788

목차

Ⅰ.목표 기업 선정 배경

1. 정보보안의 선도적인 기업

SK 쉴더스는 정보보안 분야에서 선도적인 기업으로, 다양한 보안 솔루션과 서비스를 제공하고 있습니다. 팀원 모두 정보보안학과 출신으로, 이 분야에서의 전문성과 진로 목표가 일치하여 자연스럽게 SK 쉴더스를 선택하게 되었습니다.

2. 4 차 산업의 중심 기술

SK 쉴더스는 AI, 빅데이터, 클라우드 등 최신 기술을 활용하여 보안 문제를 해결하고 있습니다. 이러한 혁신적인 접근은 정보보안 분야의 미래를 선도하고 있으며, 저희 팀은 이러한 기술적 발전에 대한 이해를 깊이 있게 다루고자 합니다.

3. 산업 내 영향력

SK 쉴더스는 국내외 다양한 기업과 협력하여 보안 생태계를 구축하고 있습니다. 이는 저희 팀이 정보보안 분야에서 영향력을 미치는 기업 문화를 이해하는 데 큰 도움이 될 것이라 생각하였습니다.

4. 사회적 책임

정보보안은 기업뿐만 아니라 사회 전반에 걸쳐 중요한 문제입니다. SK 쉴더스는 사이버 안전을 강화하기 위한 다양한 사회적 책임 활동을 진행하고 있어, 이를 통해 정보보안 분야의 사회적 가치를 느끼고자 합니다.

5. 진로 탐색

저희 팀은 SK 쉴더스에서 제공하는 인턴십 및 채용 기회를 통해 실제 업무 환경을 경험하고, 정보보안 분야에서의 진로를 구체화할 수 있는 기회를 얻고자 합니다.

이러한 이유들로 SK 쉴더스를 기업 분석의 대상으로 선정하게 되었으며,
정보보안 분야에서의 실질적인 경험과 지식을 쌓아가고자 합니다.

Ⅱ.산업 분석

1. 정보보안 산업 현황

▶ 정보보안 산업의 개념과 역할

정보보안 산업은 기업과 개인의 정보 자산을 보호하기 위한 제품과 서비스를 제공하는 분야를 말합니다. 정보보안 산업은 기업과 개인의 정보자산 보호 뿐만이 아니라 국가 차원의 사이버 안보에도 중요한 역할을 합니다. 관련 기술 발전과 새로운 위협 대응을 위해 지속적인 연구개발과 투자가 필요한 분야라고 할 수 있습니다.

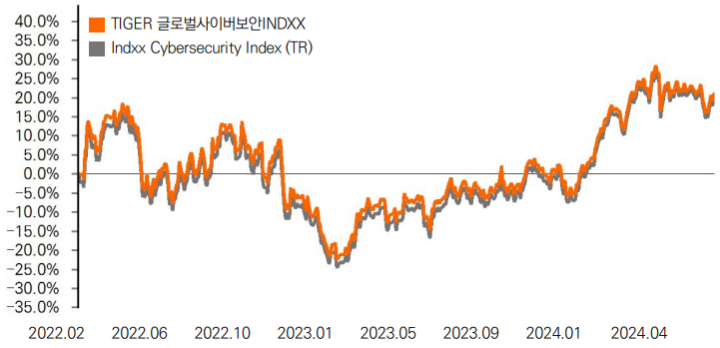
▶ 시장 규모 및 성장 추이

운용성과 (%)

구분	1M	3M	6M	1Y	3Y	YTD	설정이후	변동성
TIGER 글로벌사이버보안ND	**-1.25**	**-2.85**	**28.32**	**36.20**	**-**	**3.89**	**21.25**	**22.04**
Indxx Cybersecurity Index	-1.45	-2.93	29.34	37.94	-	4.36	19.97	22.53

* 위의 수익률 정보 및 아래 그래프는 운용기간 중 발생한 분배금 재투자를 가정하였음.
변동성 : 최근 1년간 일간수익률 기준 표준편차 연환산 (운용기간 1년 이내인 경우 전체 운용일수 기준)

누적성과 그래프



정보보안 산업의 시장 규모는 지속적인 성장세를 보이고 있습니다. 작년 국내 보안산업 매출 규모는 16.8 조원으로 전년 대비 4% 증가한 것으로 나타났습니다. 또한 한국거래소에 따르면 국내에 상장된 'TIGER 글로벌사이버보안 IND'는 4 월 기준으로 1 개월 이내의 운용성과는 -1.25%를 기록하였으나, 지난 1 년 운용성과는 36.20%에 달하였습니다. 이처럼 정보보안 산업은 새로운 기술 발전과 보안 위협 증가에 따라 시장 규모가 지속 적으로 확대될 것으로 전망됩니다.

2. 정보보안 산업 최근 이슈

▶ 사이버 위협 증가와 보안 이슈

최근 기업의 디지털 전환과 인공지능(AI) 기술 발전에 따라 새로운 유형의 사이버 공격이 늘어나고 있습니다. 딥페이크 기술을 이용한 사기 사례나 AI 기반 지능형 공격 등 신종 사이버 위협이 증가하고 있습니다. 이에 따라 차세대 AI 기반 보안 솔루션에 대한 수요가 높아지고 있습니다. 또한 클라우드, IoT(사물인터넷), 모바일 등 신기술 도입이 확대되면서 관련 보안 이슈도 부각되고 있습니다. 유럽연합은 차량 사이버보안 관리체계 인증을 의무 화하는 등 신기술 보안 규제가 강화되는 추세를 보이고 있으며, 국내 기업들은 클라우드 보안, 모바일 보안 등 신기술 보안 분야에서 대응 역량 강화가 시급한 상황입니다. 대형 기업의 데이터 유출 사고도 지속적으로 발생하고 있어 데이터 보안 강화가 필요한 실정입니다.

▶ 신기술 도입에 따른 개인정보 유출 문제

클라우드, IoT(사물인터넷), 모바일 등 신기술 도입이 가속화되면서 새로운 유형의 사이버 위협도 증가하고 있습니다. 특히 클라우드 환경에서의 데이터 보안과 개인정보 유출 방지가 주요 과제로 대두되고 있습니다. GDPR(개인정보보호법) 등 데이터 보안 규제가 강화되면서 기업들의 컴플라이언스 부담이 커지고 있습니다 국내 기업들은 클라우드 보안, 모바일 보안 등 신기술 보안 분야에 대한 대응 역량을 키워 나가야 할 것입니다. 정보보안 전문가들은 기업의 디지털 전환과 신기술 도입에 발맞춰 지속적인 투자와 기술 개발이 필요하다고 강조하고 있지만 중소기업의 경우 신기술 보안 분야 대응을 위한 재원과 인력 확보가 어려워 정부 차원의 지원 대책이 필요하다며 요구되고 있습니다.

3. 정보보안 산업 전망

▶ 시장 성장 전망

최근 기업의 디지털 전환이 가속화되고 인공지능, 클라우드, IoT 등 신기술이 확산되면서 사이버 공격도 지능화, 고도화되고 있습니다. 이에 따라 글로벌 정보보안 시장의 성장세는 가파를 것으로 전망됩니다. 미국 시장조사기관 Gartner 에 따르면 글로벌 정보보안 시장 규 모는 2023 년 1700 억 달러에 이를 것으로 예상되며, 2027 년에는 2500 억 달러를 넘어설 전망이라고 발표했습니다. 특히 신기술 관련 보안 분야의 수요가 크게 증가할 것으로 예상됩니다. 2022 년 국내 시장 규모는 19 조 원 수준으로 추정되며, 연평균 6% 이상의 성장세를 보일 것으로 전망됩니다. 다만 중소 기업 위주인 국내 업체들은 대규모 투자가 어려워 AI 등 차세대 기술 분야에서 글로벌 기업에 비해 뒤처질 가능성이 있습니다.

▶ 기술 발전 및 신규 서비스 분야 예측

1) 정보보안 기술은 신기술 발전에 따라 지속적으로 진화할 것으로 예상됩니다. AI 기술 고도 화로 인한 새로운 유형의 사이버 공격 증가에 대응하기 위해 차세대 AI 기반 위협 탐지 및 대응 솔루션 수요가 높아질 전망입니다. 또한 기업의 클라우드 환경 도입 확대에 따라 클라우드 보안 솔루션과 관리 서비스 분야도 성장할 것으로 보입니다.

2) IoT 기기 보안 이슈도 주목받고 있습니다. 자율주행차, 스마트 팩토리, 스마트홈 등 IoT 기술이 적용되는 분야에서 사이버 위협 대응을 위한 보안 솔루션 및 서비스 수요가 증가할 것입니다.

3) 데이터 유출 및 프라이버시 이슈, 신기술 보안 규제 강화 등에 따라 관련 컴플라이언스 서비스에 대한 수요도 늘어날 전망입니다. 보안 진단, 모의 해킹, 취약점 분석 등의 정보 보호 관리 체계 구축 서비스 수요도 지속적으로 증가할 것으로 예상됩니다.

이에 따라 정부와 기업은 신기술 기반의 정보보안 R&D 투자와 전문 인력 양성에 힘써야 할 것입니다. 정보보안 산업의 지속 성장을 위해서는 기술력 확보와 글로벌 경쟁력 제고가 관건이 될 것이라 예측합니다.

Ⅲ.기업 분석

1. 기업 현황

▶ 기업 정보

기업정보		2023 년말 기준
기업명	에스케이쉴더스 주식회사	
대표이사	홍원표	
설립일	2021 년 3 월 5 일(통합법인) (구. SK 인포섹 2000 년 6 월 26 일, 구. ADT 캡스 1971 년 1 월 22 일)	
본사 소재	경기도 성남시 분당구 판교로 227 번길 23(삼평동)	
임직원	7,031 명(집행임원 3 인 제외)	
사업영역	1. 물리보안	AI 기반 CCTV 및 센서를 활용한 무인경비 및 영상관제, 출입보안, 무인매장, 홈세이프티, 시설관리 서비스 등
	2. 사이버보안	정보보안 관제 및 컨설팅, 솔루션 구축, 클라우드 보안, Mobile Care 솔루션 등

	3. 융합보안	지능형 융합보안 플랫폼을 기반으로 하는 서비스, 산업시설·생산설비에 대한 보안을 제공하는 OT(Operational Technology) 보안 등
자회사	주식회사 캡스텍, Infosec Information Technology(Wuxi)Co., Ltd., SK shieldus America, Inc., SK shieldus Hungary Kft.	

▶ 연혁 및 기업 규모

년도	주요 연혁
1970 년 대	- 한국보안공사(현 ADT 캡스) 설립 - ISO 9001 인증획득
2000 년 대	- 국내 최초 이중 관제 시스템 구축(CMS Back-up System) - 한국인터넷진흥원(KISA) 정보보호관리체계 인증 획득 - 보안업계 최초 ISO27001 인증 획득
2010 년 대	- 인포섹, 2010 년 정보보호 대상 정보보호산업분야 우수상 수상 - 대한민국 브랜드 가치 보안경비 부문 1 위 수상 - 아시아 최초, Global Cyber Threat Alliance 가입 - 국내 최초 일본 현지 대상 웹진단 컨설팅 프로젝트 및 모의해킹 수행
2020 년 ~ 현재	- 'AWS Security Competency' 인증 획득 - ADT 캡스-SK 인포섹 합병, 보안전문기업 출범 - 제 1 금융권에 양자암호 기반 보안 솔루션 최초 구축 - AWS 경계보안 MSSP 자격 획득 - 한국에서 가장 존경받는 기업 정보보안 부문 3 년 연속 1 위

2. 주요 사업 및 핵심 기술

▶ 주요 사업

물리 보안			
사업 유형	**제공 서비스**		**서비스 내용**
물리 보안	상업용 보안	AI CCTV	고화질 CCTV 와 AI 지능형 영상 분석 기술로 실시간 침입탐지,경보 및 통계 분석 서비스

		출동 경비	센서와 영상기기를 통해 사고 신호를 실시간으로 감지하여 출동요원의 긴급 대처와 유관기관 신고 등을 수행하는 보안 서비스
		출입 보안	출입부터 근대관리까지 사업장 맞춤형 통합 출입 관리 서비스
	스마트 매장	무인매장	점주가 24/365 안심하고 원격으로 매장 운영을 할 수 있도록 도움을 주는 platform 기반 무인 매장 전 용 통합 서비스
		매장 관리	상품 도난 방지, 방문 고객 분석 등 고도화된 매장 관리 솔루션 서비스
	가정용 보안		현관문 밖 상황 및 방문자 확인 , 얼굴인식 출입기능, 택배 감시, 비상시 24 시간 보안 요원 출동서비스까지 제공하는 서비스

사이버 보안			
사업 유형	**제공 서비스**		**서비스 내용**
사이버 보안	정보보안	컨설팅	고객사의 보안 환경을 고려하여 정보보호체계를 수립하고 정보보안 방안을 제시해주는 서비스
		Solution/SI*	국내 및 글로벌 업체의 정보보안 솔루션을 공급·구축하고 유지보수를 제공하는 서비스
		보안관제	고객사의 보안 시스템에 대한 운영 및 관리를 전문적으로 지원해주는 서비스
		ISAC**	IT 기술 지원·장애 대응 서비스
	클라우드 보안		클라우드 환경에서 데이터, 애플리케이션, 인프라 등을 보호하는 서비스로 컨설팅, 솔루션 구축·운영 및 모니터링 등 통합 서비스
	가정용 보안		Mobile 스미싱과 악성 App. 탐지 및 가족 위치 알림 서비스 등 백신 및 Care 서비스 제공

융합 보안		
사업 유형		**서비스 내용**
융합 보안	융합보안 SI	다양한 솔루션 간 통합을 통해 보안서비스의 가치를 제고하는 서비스

SUMITS 산업안전	제조 및 건설 등 고위험군 산업현장의 영상 분석과 IoT 센서를 활용한 산업재해의 위협요인을 모니터링하는 서비스
SUMITS OT**	산업제어망 및 제어시스템의 Cyber 공격에 대응서비스
SUMITS FM	시설운영시스템인 BAS***와 보안시스템 간 연동을 통해 편의성과 보안성을 제공하는 통합관리서비스

▶ 핵심 기술

1) AI 기반 위협 탐지 및 대응

SK 쉴더스는 인공지능(AI) 기술을 활용하여 사이버 공격을 실시간으로 탐지하고 분석하는 시스템을 구축하고 있습니다. 머신러닝 알고리즘을 통해 정상 트래픽을 학습하고, 비정상적인 패턴을 신속하게 식별함으로써 빠른 대응이 가능합니다. 이러한 기술은 공격자의 행동을 예측하고, 사전 예방 조치를 취하는 데 큰 도움을 줍니다.

2. 보안 관제 서비스 (SOC)

SK 쉴더스의 보안 관제 센터(SOC)는 24 시간 상시 모니터링을 통해 고객의 IT 환경을 보호합니다. 전문 보안 인력이 연중무휴로 로그를 분석하고, 이상 징후를 탐지하여 즉각적인 대응을 합니다. 이를 통해 잠재적인 위협을 조기에 발견하고, 사고 발생 시 신속한 복구를 지원합니다.

3. 데이터 암호화 및 보호

데이터 보안은 SK 쉴더스의 중요한 축입니다. 민감한 정보에 대한 강력한 암호화 기술을 적용하여 데이터 유출 및 변조를 방지합니다. 또한, 데이터 접근 권한 관리 및 감사 기능을 통해 기업의 정보 보호 수준을 한층 강화하고 있습니다.

4. 네트워크 보안 솔루션

SK 쉴더스는 다양한 네트워크 보안 솔루션을 제공하여 외부 공격으로부터 기업의 네트워크를 보호합니다. 방화벽, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS) 등이 포함되어 있으며, 지속적으로 업데이트되어 최신 공격 기법에 대응할 수 있도록 설계되었습니다.

5. 클라우드 보안

SK 쉴더스는 클라우드 기반 데이터 보호 솔루션을 제공하여 클라우드 서비스의 보안성을 높이고, 데이터 무결성을 유지합니다. 클라우드 환경에 최적화된 보안 정책과 가시성을 제공하며, 클라우드 내 사용자 행동 분석을 통해 잠재적인 위협을 식별합니다.

3. 재무 현황 및 경쟁사

▶ 재무 현황

2023 년 자료/백만원(단위)

재무 현황	매출액	1,873,477
	영업이익	46,379
	당기순이익	- 15,130
	지분순이익	- 15,130
	주당순이익	- 148

▶ 경쟁사

1) SK 쉴더스의 SWOT

Strength	Weekness
- sk 텔레콤의 통신 인프라와 보안기술 보유 - sk 텔레콤 등 그룹사 용역 등 수주 용이 - 사업 분야의 다각화로 매출 구조 확대	- 전체 매출 25%를 차지하는 특수 관계자 매출 - 지속적인 합병과 매각으로 기업 및 브랜드 이미지 혼란 - 사업분의 다각화로 인한 전문성 부족 우려
Opportunity	**Threat**
- 사이버보안 시장의 지속적인 확대 - IOT 등과의 접목 통한 다양한 서비스 확장 - 사업분야별 매출 비중 분산	- 에스원, KT 텔레캅 등 - 타 경쟁 기업과의 가격 및 서비스 경쟁 - 글로벌 사이버 보안 기업과의 경쟁 심화

2) 에스원의 SWOT

Strength	Weekness
- 오랜 업력으로 쌓은 인지도 - 업계 매출 1 위 - 삼성전자 등 그룹사 용역 등 수주 용이 - 양질의 데이터 확보와 전문인력 육성	- 전체 매출의 36%가 특수 관계자 매출 - 지속해서 증가하는 특수관계자 매출 비중 - 타 경쟁 기업에 비해 정보보안 분야 약세 - 매출액 대비 연구개발비 투자 미흡
Opportunity	**Threat**
- 중대재해처벌법, 수술실 CCTV 설치 - 무인매장 증가 등 솔루션 및 제품적용 시장 확대 - IOT 등과의 접목을 통한 다양한 서비스 확장	- SK 쉴더스, KT 텔레캅 등 타 경쟁 기업과의 가격 및 서비스 경쟁 - 정보보안 분야에 대한 서비스 수요 증가 - 지속되는 물리보안과 정보보안의 융합

3) SK 쉴더스와 에스원

<시장 점유율 및 위치>

SK 쉴더스	사이버 보안 시장에서의 점유율이 높으며, 특히 기업 고객을 대상으로 한 맞춤형 솔루션 제공에 강점을 보이고 있습니다. SK 그룹의 지원으로 인한 자원과 네트워크를 활용해 안정적인 성장을 이어가고 있습니다.
에스원	국내 물리적 보안 시장에서 오랜 역사를 가지고 있으며, 다양한 산업군에 걸쳐 안정적인 고객 기반을 확보하고 있습니다. 특히 보안 인력 관리 및 통합 보안 시스템에 강점을 가지고 있습니다.

<서비스 및 제품 포트폴리오>

SK 쉴더스	주로 사이버 보안 및 IT 서비스에 중점을 두고 있으며, AI 기반의 보안 솔루션, 클라우드 보안 서비스 등을 포함하고 있습니다. 고객 맞춤형 솔루션 제공으로 차별화를 두고 있습니다.
에스원	물리적 보안 시스템과 정보 보안을 통합한 종합 보안 서비스를 제공하고 있습니다. 또한, 스마트 빌딩 및 IoT 기반의 솔루션으로 서비스 포트폴리오를 확장하고 있습니다.

<기술 혁신 및 연구개발>

SK 쉴더스	사이버 보안 관련 최신 기술 개발에 많은 투자를 하고 있으며, AI 및 머신러닝 기술을 활용한 보안 솔루션 혁신에 집중하고 있습니다. 또한 R&D 부서의 강화로 빠른 기술 발전을 이루어 내고 있습니다.
에스원	기술 혁신의 속도가 상대적으로 느리지만, 기존 물리적 보안 시스템의 개선 및 IoT 기술을 접목한 서비스 개발에 힘쓰고 있습니다. 그러나 사이버 보안 분야에서는 상대적으로 뒤처져 있는 경향이 있습니다.

<경쟁 환경 및 전략>

SK 쉴더스	경쟁이 치열한 사이버 보안 시장에서 기술 혁신과 글로벌 진출 전략을 통해 시장 점유율을 높이려 하고 있습니다. 또한, 파트너십을 통한 생태계 구축에 집중하고 있습니다.
에스원	물리적 보안 시장에서의 안정성을 바탕으로 스마트 시티 및 IoT 관련 시장으로의 확장을 모색하고 있습니다. 또한, 고객 맞춤형 솔루션을 통해 다른 기업들과 차별화를 두고 있습니다.

4. 비전 및 핵심가치, 복리 후생

▶ 비전 및 핵심 가치

SK 쉴더스는 '고객의 물리자산과 가상자산 전반에 걸친 최고 수준의 디지털 보안 서비스를 제공하는 리더가 되겠다'는 미래 비전 마스터플랜 '5-STAR'을 수립하였습니다. 이는 첨단 기술과 혁신을 바탕으로 고객의 안전과 보안을 최우선으로 하는 SK 쉴더스의 핵심가치를 반영하고 있습니다.

SK 쉴더스는 지속가능경영 목표를 달성하기 위하여 E·S·G 각 항목의 전략목표를 설정하고, 중대성 평가를 통하여 도출된 이슈별 세부 Action Plan 을 수립 및 실행하고 있습니다.
특히 5-STAR 프로젝트를 통하여 선정된 10 개의 ESG Initiatives 는 2024 년부터 5 개년의 중장기 전략목표를 수립하고, 각 연도별로 구체적인 목표와 일정 그리고 KPI 를 명확하게 설정함으로써 보다 장기적인 관점에서 지속가능경영을 추진하고 있습니다.

▶ 복리 후생

구성원의 행복증진	
산업 안전 보건	- 안전보건경영시스템국제표준인증 - 안전 경영시스템인증 사업장을 확대 위험성 평가 프로그램 - 고위험군 안전관리 프로그램
조직문화	- 수평적 조직문화 - 일과 삶의 균형 보장 - 구성원 평가 및 보상 - 다양성 및 포용성
인재경영	- 우수인재 확보 - 산업전문가 양성 - 산업전문가 영입

Ⅳ.기업의 직무 이해

1. 직무 소개 및 안내

SK 쉴더스 정보보안의 직무 분야			
관제	**취약점 진단**	**컨설팅**	**Cloud**
이벤트를 분석, 판별 이벤트에 따라 적절한 대응을 수행	인프라 진단, 웹/모바일 진단, 소스코드 진단, 모의해킹 등	정보보호체계 점검, 정보보호 Risk 조치 방안 및 보호대책 수립 등	Cloud 서비스 도입을 위한 컨설팅, 설계, 구축, 관제, 운영, 기술지원 등
침해대응	**모의해킹**	**보안운영**	**OT/ICS**

정보보안 공격 분석에 대한 포렌식 기법, 로그분석을 통해 대응 방안 마련	방어기술에 대한 지속적인 연구, 산업/기업별 최적화된 점검 진행	보안 영역별 솔루션 제안/구축, 보안 솔루션과 장비 운영	산업 분야 보안 컨설팅, OT 보안 솔루션 구축, 운영, 관제 등 전 영역 지원

.

▶ 희망 직무 분야

주요 역량	세부 내용
취약점 점검	해킹이라는 것은 결국 취약점으로부터 시작되는 것이기 때문에 다양한 취약점을 찾아내는 것이 중요하다.
시나리오 침투 테스트	찾아낸 취약점이 확실하고 실제 해커가 이 방법을 시도했을 때, 어떠한 일이 일어나는지에 대해 알아야 하기 때문에 찾아낸 취약점을 이용해 실제로 해킹을 하는 시나리오를 구성해 시도하는 능력.
프로그래밍 언어 활동	프로그래밍 언어에는 Python , Java , Java Script , HTML , Ruby, C 등 많은 것들이 있고 취약점이라는 것은 프로그래밍 코드로부터 생기는 것이므로 각종 프로그래밍 언어에 대한 이해도와 활용도가 필수적으로 필요.
Binary Reverse Engineering 및 보안 시스템 우회	해킹을 해서 코드로 된 파일이나 중요 문서가 암호화가 되어있을 때 Binary Reverse Engineering 기술이 있으면 코드에 대해 분석을 할 수 있고 숨겨진 코드를 직접 짜 맞출 수 있기에 필수적으로 요구됨. 보안 시스템 우회 능력은 취약점을 찾았지만 그 취약점이 막혀 있는 상황 또는 알집 반디집과 같은 보안 시스템이 있어 이를 우회할 수 있는 능력 요구.
검증 능력	침투에 성공을 하고 보안 정보를 가져올만한 능력인지 아닌지를 확인해야 함. 검증이 안되면 성공적인 해킹인지 아닌지 모르기 때문에 검증 역량이 필요.

2. 직무의 역할 및 업무

▶ 모의 해킹의 역할

사이버공격은 예측하기 어려운 방향으로 진화하고 있어,
실전과 같은 훈련을 통해 대비해야 하고, 필요시 대응 절차를 개선할 할 수 있으며,
금융회사, 공공기관, 일반기업 등등 이와 관련한 이행 점검을 수행할 수 있다.

▶ 모의 해킹의 주요 업무

모의 해킹	외부에 오픈 된 서비스 (웹,모바일, 시나리오 기반)에 대한 모의 해킹
공공기관	국가 주요 기반 대한 ICS 모의해킹

일반 사업	시스템 모의 해킹, 솔루션 모의 해킹
기타	보안성심의 위탁, 전문가 서비스(연간 모의 해킹 수행 및 insight 제공)

3. 채용 방식

채용 방식	
담당업무	- 점검 결과 위협 분석 및 보안 가이드 제공 - 침투 테스트 시나리오 개발 및 점검 수행 - Web, Mobile, System, C/S 등 취약점 진단 및 모의해킹 수행 - 주요정보통신기반시설 및 금융취약점분석평가 기준 취약점 진단 수행 - 결과 보고서 작성 및 결과 리뷰
자격요건	학력 : 학사 졸업 이상 경력 : 유관 경력 3 년 이상 / 신입 가능
우대사항	- IoT/모의해킹 유경함자 - IT, 정보보안 관련 자격증 소지자 - 원활한 커뮤니케이션 능력 보유자
전형절차	서류전형 → SKST(인성검사) → 실무면접 → 합격자발표 접수방법 : SK 쉴더스 채용사이트(https://skshieldusapply.com) 제출서류 : 이력서 및 자기소개서
근무환경	고용형태 신입 : 인턴(3 개월) 후, 평가에 따른 정규직 전환 경력 : 정규직 근무조건 : 주 5 일(월~금) 근무장소 : SK 쉴더스 판교 본사

V.직무 수행을 위한 역량

1. 보유 역량

팀의 보유역량	
자격증	스크래치 2 급, ITQ 파워포인트 A 급, ITQ 엑셀 A 급
비교과 활동	프레젠테이션 대회, 시사 토론대회, 2024-1 학기 기업 및 직무 분석 공모전
대내외 활동	대전대학교 단과대 학생회 임원, 과학년 대표

수상 기록	진로/직무 탐색 콘테스트 장려상 정보보안학과 CTF 대회 우수상
기타	CCTV 설치 공사 8 개월 근무

2. 필요 역량

필요 역량	보유역량
- 네트워크 보안 이해 - 취약점 분석 능력 - 리포트 작성 능력 - 침투 테스트 기법 숙지 - 스크립트 및 프로그래밍 능력	- 프레젠테이션 능력 - 웹 페이지 개발 능력 - 취약점 분석 능력 - 협동 능력
필요 역량 수행 방법	
- 보안 커뮤니티 활동 - 최신 보안 트렌드 연구 - 멘토링 및 팀워크 훈련 - 관련 교육 및 자격증 취득 - 실제 모의 해킹 프로젝트 참여	

3. 직무 수행 역량

지식	**필요 지식**	**팀의 지식**
	해킹 기법 법적 규제 보안 정책 보안 프로토콜	정보보호론 운영체제 해킹 보안 정보보호 법 제도 정보보안 정책
기술	**필요 기술**	**팀의 기술**
	포렌식 분석 기술 취약점 스캐너 운영 침투 테스트 도구 사용 SSL/TLS 분석	프로그래밍 언어 자바 웹 해킹 기술 유닉스 라즈베리파이
태도	**필요 태도**	**팀의 태도**
	협업과 소통 문제 해결 지향 책임감 있는 행동 지속적인 학습 의지 윤리적 해킹 마인드	윤리적 행동 문제 해결 능력 커뮤니케이션 스킬 끊임없는 학습 의지
필요 준비 사항	**역량**	실습경험

		보안 관련 세미나 참석 팀 프로젝트 경험
	자격증	CEH (Certified Ethical Hacker) CISM (Certified Information Security Manager) OSCP (Offensive Security Certified Professional)

VI.기타

1. 결론 및 시사점

김신아	sk 쉴더스 기업과 모의해킹 직무를 분석하면서 사이버 보안의 중요성을 깊이 이해하게 되었습니다. 특히, 최신 공격 기법과 방어 전략을 배우는 과정에서 실무 능력을 향상시킬 수 있었습니다. 다양한 시나리오를 통해 문제 해결 능력과 팀워크의 중요성을 깨달았고, 실제 상황에서의 대응력을 키웠습니다. 이 경험은 저의 전문성을 높이는 데 큰 도움이 되었으며, 앞으로의 경력에 긍정적인 영향을 미칠 것이라 확신합니다.
조승민	정보보안 산업이 단순히 기술적인 영역을 넘어 사회의 필수 안전망 역할을 한다는 점이 인상적이었다. AI, 클라우드, 빅데이터 등을 활용해 보안 솔루션을 혁신적으로 발전시키는 모습에서, 보안이 단순한 방어를 넘어 선제적 예방과 대응을 강조하는 방향으로 나아가고 있음을 느꼈다. 또한 SK 쉴더스의 사회적 책임감이 눈에 뛰었다. 단순히 사업적 성공에 머무르지 않고, 정보보안을 통해 전체 사회의 안전을 증진하고자 하는 진심 어린 노력에 깊은 인상을 받았다.이 회사를 보며, 정보보안 전문가로서 단순히 기술을 다루는 것을 넘어 신뢰와 책임을 바탕으로 한 사회적 사명감이 필요하다는 깨달음이 있었다.
이승진	SK 쉴더스를 조사하며, 기업이 제공하는 보안 서비스가 단순한 기술적 지원을 넘어, 고객의 비즈니스 안전과 생명 보호를 위한 종합적인 솔루션으로 자리 잡고 있다는 점에 깊은 인상을 받았습니다. 특히, AI 와 빅데이터 기반의 스마트 보안 시스템이 실시간 위협 탐지 및 대응에 중요한 역할을 하며, 보안 환경의 변화에 빠르게 적응하고 있다는 점이 인상적이였고 클라우드 보안, IoT 보안, 사이버 위협 대응 등 다양한 분야에서 혁신적인 기술을 선도하며, 글로벌 시장에서의 경쟁력을 높이고 있다는 사실을 새롭게 알게 되었습니다.

https://naver.me/xmx4LG5P / https://naver.me/xhza42tK /

https://www.skshieldusapply.com/