<파란학기-기업제안 프로그램 진행 절차>

※ 참여 희망학생 필독

① 제안1~5의 기업제안 프로그램을 살펴보고 2026-1학기 파란학기로 참여할 과제를 선정
& 프로젝트를 같이 진행할 팀원 모집

⇩

② 신청 계획서 작성 전 기업 담당자와 면담을 진행하여 프로젝트의 세부내용에 대해 논의하고 협의하는 과정 (제안서상 기업담당자 연락처로 직접 일정 조율하여 프로젝트에 대해 상의, 일정 조율에 어려움이 있을 시 아래 문의사항 연락처로 도움 요청)

⇩

③ 기업담당자와 조율한 내용을 바탕으로 팀별, 개인별 신청서 작성

⇩

④ 신청서 작성 완료 후 해당 지도교수님께 계획서 검토 요청, 지도교수 서명을 받은 후 교육혁신팀으로 최종 신청서 제출 (~12/31(수) 11시까지)

⇩

⑤ 2026-1학기 파란학기제 운영이 확정되면, 파란학기제 활동 시작
(기업 담당자 멘토링을 받으면서 진행)

⇩

⑥ 파란학기제 종료 후 해당 기업의 현장실습 참여(권장 사항)

<문의사항>

T : 031-219-3383/3387
E : ajouparan@ajou.ac.kr

2026-1학기 아주대학교 파란학기제 기업제안 프로그램 목록

NO	프로그램명	학점	연계기업명	지도교수	페이지
1	CCTV활용 중소제조 산재 분석 및 산재 예방 AI 모델 개발	3	빈공간 테크놀러지	박재일 (산업공학과)	p3
2	거대언어모형을 이용한 교통안전 의사결정 지원 체계 개발	3	엠큐닉	박성호 (미래자동차 혁신융합대학사업단)	p8
3	사이버 위협 시뮬레이션 자동화	3	주)쏘마	곽진 (사이버보안학과)	p12
4	END TO END AI Agent 보안 가시화 기술 개발	3	쿤텍	곽진 (사이버보안학과)	p17
5	Zero Trust 기반 네트워크 경계 위협탐지 및 대응 모델 개발	3	프라이빗 테크놀로지	곽진 (사이버보안학과)	p.22

※ 기업제안 프로그램은 복수의 팀이 지원 및 참여할 수 있으며, 각기 다른 접근과 방식으로 과제를 수행할 수 있습니다.

[제안1]

회사명	빈공간테크놀러지
분야	산재예방 인공지능
프로젝트명	CCTV활용 중소제조 산재 분석 및 산재 예방 AI 모델 개발
지도교수(소속)	박재일 (산업공학)

1. 멘토 소개

이름/소속/직위	황상훈/빈공간/대표
소개글	당사는 CCTV와 4족보행 로봇을 융합한 피지컬AI 기반 산업안전 솔루션을 개발하고 있습니다. AI 영상분석과 로봇 자율주행 기술을 결합하여, 중소 제조현장에서의 산업재해를 사전에 감지하고 예방할 수 있는 지능형 시스템을 구축하고 있습니다. 특히, 위험 구역 내 로봇 순찰 및 실시간 상황 인식, 작업자 이상행동 감지, 비상 상황 대응 자동화를 통해 안전관리 인력의 한계를 보완하며, 중소기업 맞춤형 산재예방 플랫폼으로 확장하고자 합니다. 또한 본 기술은 사회적 가치 실현을 지향합니다.
연락처 (학생공지용)	-내선번호 : 010-7712-2776 -이 메 일 :hwangsh@ajou.ac.kr

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	AI 영상인식: CCTV 영상에서 작업자·장비·위험요소를 실시간 인식 (YOLO, Mask R-CNN 등) 피지컬AI 융합: AI의 인지·판단 기능 결합한 현장 대응 시스템 산재사고 분석 및 보고서: 산재 사례를 분석하고 AI용 정형화된 보고서 생성
함양 경험·역량	작업 현장의 CCTV 영상 데이터을 분석하여, 위험 행동·장비 이상·환경 변화 등의 이상 징후를 자동으로 탐지하고 대응할 수 있도록 AI 영상 기술을 설계중입니다. 이를 위해 YOLO·Mask R-CNN 등의 객체 인식 모델을 활용해 작업자와 장비의 위치 및 동작을 정밀하게 추적하고, 또한 AI 학습 데이터셋 구축, 실시간 스트리밍 처리 등의 과정을 직접 수행하며 CCTV 영상 데이터을 분석 기술 실무 역량과 안전 데이터 분석 능력을 함양합니다.

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	산업공학 (안전공학), 소프트융합
	필 요 역 량 (프로그래밍언어 등)	AI 영상 딥러닝 기술 이해, AI용 산재 분석 및 예방보고서
멘티에게 하고 싶은 말		"기술은 사람을 대신하는 것이 아니라, 사람을 **더 안전하게 만드는 것**이라 믿습니다. 우리 프로젝트는 로봇과 AI를 결합해 산업 현장의 안전을 지능화하는 일입니다. 배움과 실험을 두려워하지 않고, '이 기술이 현장에 어떤 변화를 줄 수 있을까'를 함께 고민하는 동료를 기다립니다. 단순한 코드보다, '사람의 안전'이라는 가치를 기술로 실현하고 싶은 분이라면 누구든 환영합니다."

5. 도전과제 주요내용

도전과제 목표	CCTV 활용 AI 기반 행동 인식을 적용한 '중소제조 산재예방 스마트 안전관리 시스템'을 개발하고자 함 - CCTV 영상으로 작업자 행동·보호구 착용 여부 실시간 감지 - TS-LSTM 기반 시퀀스 인지 → 위험행동·근골격계 부담 동작 판별 - 관리자 대시보드와 모바일 연동 → 실시간 알림, 보고서 자동 생성
종 산출물	1. CCTV 영상과 AI 행동인식 모델:실시간 작업자 행동 모니터링, 보호구 착용 여부 자동 판별, 위험행동 감지 기능 2. 과거 산재사고 데이터를 수집·분석하여 사고 유형, 원인, 재발 가능성을 자동 분류 및 AI가 이해할 수 있도록 정형화된 보고서 템플릿으로 출력

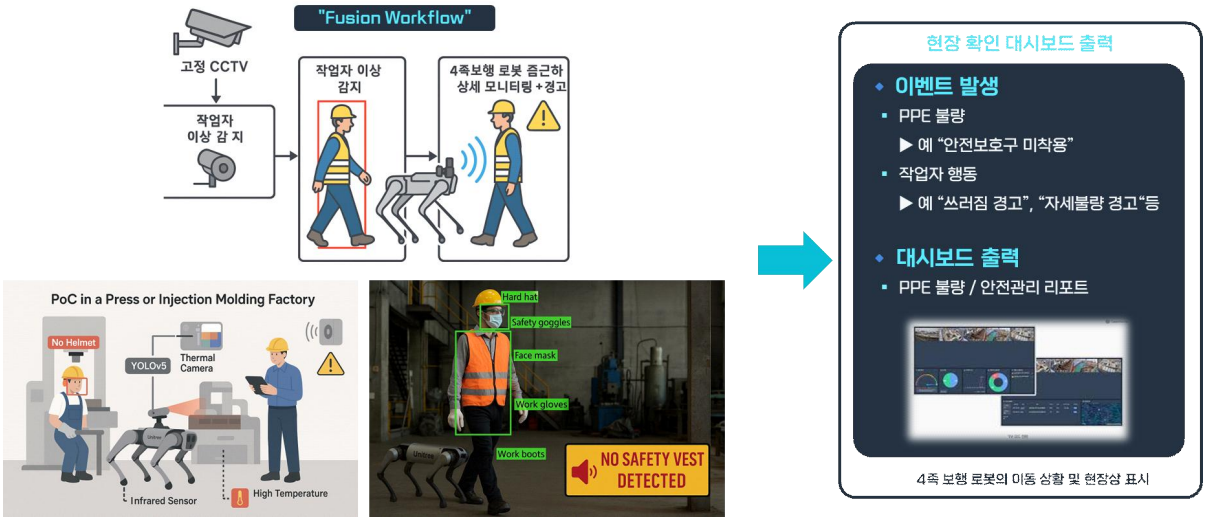
운영인원	4명
예상 투입시간	한 주당 약 10시간 * 주8~10시간 소요 시 3학점으로 인정
주요업무	
역할	**역할 세부내용**
1.AI 비전 모델 개발	CCTV 영상 기반으로 작업자·장비·위험요소를 인식하는 YOLO·Mask R-CNN 모델 개발 및 성능 고도화
2.행동 인식 알고리즘 연구	TS-LSTM 기반 시퀀스 분석을 통해 근골격계 부담 동작 및 위험 행동을 자동 판별
3.데이터 수집 및 통합관리	현장 CCTV·로봇 센서 데이터를 수집·정제하여 학습 및 분석용 데이터셋 구축
4.AI 기반 산재사고 분석 보고서 자동 생성 시스템	산재사고 데이터를 자동으로 분석하고, 표준화된 형식의 AI 학습용 보고서를 생성
도전과제 세부내용	
❍ 중소 제조업 현장은 인력 부족, 작업환경 제약으로 인해 **산업재해 예방체계가 미흡** - **보호구 미착용, 부주의 행동, 반복 동작으로 인한 근골격계 질환** 빈번 - CCTV 단독 모니터링은 **인력 의존적이고, 조명·사각지대에 취약**	

- 센서 기반 안전장비는 착용 불편·운영비용 부담으로 확산 저조
- 실시간 대응 및 사전 예방이 어려워 **재해 발생 후 조치 위주 관리**에 머무름

⇒ 따라서, 본 과제를 통해 영상인식·로봇·AI 분석을 결합한 통합 안전관리 시스템을 개발함으로써 **①산업재해 사전 예방 체계 확립, ②작업자 안전 및 생산성 향상, ③중소제조업 맞춤형 스마트 안전 솔루션 보급을 달성**하고자 함

❍ 당사는 **CCTV와 AI 기반 행동 인식을 적용한 '중소제조 산재예방 스마트 안전관리 시스템'을 개발**하고자 함

- CCTV 영상으로 작업자 행동·보호구 착용 여부 실시간 감지
- TS-LSTM 기반 시퀀스 인지 → 위험행동·근골격계 부담 동작 판별
- 멀티센서(열화상, 3D, LiDAR 등) 융합으로 조명·사각지대 취약점 보완
- 관리자 대시보드와 모바일 연동 → 실시간 알림, 보고서 자동 생성



❍ 기대효과

- 중소 제조업의 산재 비용 절감 및 안전관리 효율성 향상
- 멀티스트림 기반 위험행동 인식 원천기술 확보, 국산화된 로봇·AI 융합 솔루션 개발
- 제조·건설·물류 등 고위험 산업으로 확장 가능, 안전관리 시장 경쟁력 강화

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	중소 제조현장 안전관리 실태조사, 산재사례 데이터 수집 및 분석 체계 수립	10
2주차	CCTV 영상·근골격계 관련 데이터 수집 및 라벨링 기준 확립	10
3주차	YOLO 기반 객체 인식 모델 설계 및 초기 학습 수행	10
4주차	TS-LSTM 기반 시퀀스 분석 모델 설계 및 위험행동 분류 실험	10
5주차	보호구(안전모·장갑 등) 착용 여부 자동 판별 알고리즘 개발	10
6주차	보호구(안전모·장갑 등) 착용 여부 자동 판별 알고리즘 개발	10
7주차	CCTV 영상 스트리밍 파이프라인 구축	10
8주차	CCTV 영상 스트리밍 파이프라인 구축	10
9주차	CCTV 영상 스트리밍 파이프라인 구축	10
10주차	관리자용 대시보드 설계 및 실시간 알림·이상상황 시각화 기능 개발	10
11주차	모바일 연동형 안전관리 UI/UX 디자인 및 테스트	10
12주차	통합 플랫폼 프로토타입 완성 및 기능 통합 테스트	10
13주차	중소 제조현장 실증 환경 구축 및 시스템 설치·운영	10
14주차	실증 결과 기반 AI 모델 정확도 향상 및 데이터 고도화	1.0
15주차	산재사고 분석 및 AI용 정형화 보고서 자동 생성 기능 개발	10
16주차	최종 통합 시연, 결과보고서 작성, 기술이전·확산 계획 수립	10

7. 지도교수

이름/소속 박재일 / 산업공학과
이 메 일: jipark@ajou.ac.kr

<파란학기-기업제안 프로그램 협약서>
※ 파란학기 최종결과물의 귀속 및 이익금 분배에 대해 아래와 같이 표준협약이 되었습니다.
※ 파란학기 기업제안 프로그램 신청 전 아래 사항을 숙지하여 주시고, 기업 담당자 면담 시 아래 내용에 대해 다시 한 번 확인 부탁드립니다.

제1조 (목적)
본 협약은 “아주대(=파란학기 참여학생)”와 “회사” 양 기관의 상호간 협력을 바탕으로 파란학기-기업제안 프로그램 최종 결과물을 활용함에 있어서 양 당사자의 권리 및 의무를 규정하는 것을 목적으로 한다.

제2조 (귀속 및 이익금 분배)
① 파란학기-기업제안 프로젝트의 최종 결과물은 “아주대(파란학기=참여학생)”에게 귀속된다.
② 회사가 파란학기-기업제안 프로젝트 최종 결과를 회사 운영에 활용하거나 이윤을 남기는 경우 그 이익금의 분배에 대하여는 “아주대(=파란학기 참여학생)”와 협의하여 결정한다.

제3조 (협약기간)
본 협약의 협약 기간은 협약일로부터 파란학기 종료 이후 “프로젝트 결과물”의 유효 존속 기간까지로 한다.

제4조 (협약의 변경)
본 협약의 내용은 "아주대(=아주대 참여학생)"와 "회사"의 서면합의에 의하여 유효하게 변경될 수 있다.

제5조 (신의성실의 의무)
본 협약이 목적하는 바를 상호 충족시키기 위해 필요한 제반 사항에 대하여 "아주대"는 신의, 성실을 다하여 "회사"에게 적극 협조하여야 하며, "회사" 또한 본 협약을 성실히 이행하여야 한다.

제6조 (협약의 효력)
본 협약의 효력은 쌍방이 서명 날인한 날부터 유효하다.

제7조 (해석)
본 협약에 명기되지 아니하거나 본 협약상의 해석상 이의가 있는 사항에 대하여는 쌍방의 합의에 의하여 결정한다.

[제안2]

회사명	엠큐닉
분야	모빌리티, 인공지능, 빅데이터
프로젝트명	거대언어모형을 이용한 교통안전 의사결정 지원 체계 개발
지도교수(소속)	아주대학교 미래자동차 혁신융합대학사업단 박성호 연구교수

1. 멘토 소개

이름/소속/직위	장양중
소개글	위 본인은 교통·모빌리티 분야의 정밀도로지도, 자율주행 SW, 데이터 표준화 및 디지털트윈 구축 관련 업무에서 활동하고 있습니다. 또한 교통빅데이터 관련 연구에도 다수 참여하고 있습니다. 위 본인은 엑큐닉에서 기술개발업무 총괄을 맡고 있으며, 첨단교통 분야 소프트웨어 개발 관련 10년 이상의 경력을 보유하고 있습니다.
연락처 (학생공지용)	- 내선번호 : 02-521-7723 (회사 대표 번호) - 이 메 일 : tring@mqnic.com

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☐ 가능 ☑ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	파이썬 등 컴퓨터 프로그래밍, 챗GPT 등 거대언어모형
함양 경험·역량	교통공학, S/W, 교통안전 등 다양한 전공자의 참여가 가능하며, 기본적으로 문제의 공학적 정의, 문제 해결을 위한 기술 대안 탐색 그리고 대안 구현을 위한 프로그래밍 기초 지식 등을 갖춘 인재의 참여를 요구하며, 프로젝트 수행에 필요한 거대언어모형 개념 및 프로그래밍은 지도교수가 별도 교육 실시할 예정임

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	교통공학, 파이썬 프로그래밍, 거대언어모형
	필 요 역 량 (프로그래밍언어 등)	파이썬 프로그래밍, 거대언어모형 기초 지식, 교통공학 기초 지식
멘티에게 하고 싶은 말		거대언어모형 최적화 과정을 거쳐서 교통분야 의사결정을 지원할 수 있는 모형을 개발하는 경험을 쌓도록 할 예정임

5. 도전과제 주요내용

도전과제 목표	거대언어모형 최적화(파인튜닝 또는 검색 증강 생성 적용)를 통한 교통안전 의사결정 체계 개발
최종 산출물	교통안전에 대한 의사결정을 지원하는 거대언어모형 거대언어모형 파인튜닝 방법 기술서 거대언어모형 검색 증강 생성 방법 기술서

운영인원	2~4
예상 투입시간	한 주당 약 8시간 * 주8~10시간 소요 시 3학점으로 인정
주요업무	
역할	**역할 세부내용**
모형 기획	전체적인 모형의 개발 방향, 개발 방법 그리고 활용 계획을 수립함
거대언어모형 구축	소규모로 구축 가능한 거대언어모형을 선정하고, 의사결정을 위한 입력 및 출력 체계를 기획함
파인튜닝	거대언어모형의 파라메터을 파인튜닝하여 교통안전 분야 의사결정을 지원하도록 고도화 함
검색 증강 생성	거대언어모형에 검색 증강 생성 방버을 적용하여 활용하는 별도의 전문 데이터셋을 구축하여 교통안전 분야 의사결정을 지원하도록 고도화 함
도전과제 세부내용	

본 연구의 목표는 거대언어모형(LLM, Large Language Model)을 기반으로 교통안전 분야의 의사결정을 지능적으로 지원할 수 있는 특화형 언어모형을 개발하는 것이다. 최근 교통안전 데이터는 사고 이력, 도로 특성, 기상·교통량 등 다양한 비정형 데이터를 포함하고 있으며, 이를 통합적으로 이해하고 분석할 수 있는 고도화된 언어모형의 필요성이 커지고 있다. 본 과제에서는 교통사고 예방과 정책 의사결정 지원을 목적으로, 기존 범용 LLM 중 언어 이해력과 추론 성능이 우수한 모형을 선정하고, 이를 교통안전 도메인에 맞게 파인튜닝(fine-tuning) 및 검색 증강 생성(RAG, Retrieval-Augmented Generation) 기법을 결합하여 개발할 계획이다. 우선, 후보 모형으로는 오픈소스 기반의 GPT 계열, LLaMA, 또는 Mistral 계열 모델을 비교 평가하여, 한국어 및 기술적 전문 문서 처리 성능이 우수한 모델을 선정한다. 이후, 교통사고 통계, 한국도로교통공단의 사고 원인 분석 자료, 정책 보고서, 연구논문 등 신뢰성 있는 데이터셋을 수집·정제하여 파인튜닝을 수행하고자 한다. 이를 통해 모델이 교통사고 발생 요인, 안전 대책, 위험 예측 등 도메인 특화 지식을 학습하고자 한다. 또한 단순 언어생성 한계를 극복하기 위해 RAG 구조를 적용하고자 한다. 이는 모델이 질의 시 외부의 최신 교통데이터베이스나 정책문서를 검색하여, 관련 근거를 기반으로 응답을 생성하도록 하는 방식이다. 이를 통해 모델은 사실 기반(reasoning-grounded) 의사결정 지원을 수행할 수 있으며, 정책 입안자나 연구자가 사고 예방 대책을 수립할 때 신뢰도 높은 인사이트를 제공할 수 있다. 최종적으로 구축되는 모형은 "교통안전 의사결정 지원 LLM"으로, 교통사고 원인 진단, 정책 시나리오 분석, 안전시설 투자 우선순위 평가 등 다양한 응용에 활용될 수 있다. 본 연구는 LLM의 도메인 특화 가능성을 실증함과 동시에, 데이터 기반의 과학적 교통안전 의사결정을 지원하는 혁신적 지능형 도구를 제시하는 것을 목표로 한다.

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	연구 착수 및 기획 회의를 통해 연구 목표, 범위, 추진 절차를 확정하고, 팀별 역할과 세부 일정표를 수립한다.	8
2주차	거대언어모형(LLM) 후보군을 선정하기 위한 기준을 마련하고, 성능, 비용, 한국어 지원력, 기술 확장성 등을 종합적으로 검토한다.	8
3주차	GPT, LLaMA, Mistral 등 주요 공개·상용 모델을 비교 평가하고, 교통안전 관련 데이터에 대한 파일럿 테스트를 수행하여 적합한 기본 모델을 결정한다.	8
4주차	교통안전 도메인 데이터(교통사고 통계, 정책 보고서, 논문, 기술문서 등)를 수집하고, 활용 가능한 데이터셋의 범위와 출처를 체계적으로 정리한다.	8
5주차	수집한 데이터에 대해 정제 및 전처리 작업을 수행하여 품질을 확보하고, 라벨링, 중복 제거, 포맷 통합 등 학습용 데이터셋을 구축한다.	8
6주차	파인튜닝(fine-tuning) 전략을 설계하고, 학습 파이프라인 및 하이퍼파라미터를 구성하여 실험 환경을 구축한다.	8
7주차	교통안전 도메인 데이터로 1차 파인튜닝을 수행하고, 모델의 언어 이해 및 사고 원인 분석 정확도를 내부적으로 점검한다.	8
8주차	중간 점검(Mid-term Review)을 실시하여 현재까지의 진행 현황, 데이터 품질, 모델 성능 등을 평가하고, 향후 일정 및 보완 방향을 조정한다.	8
9주차	검색 증강 생성(RAG) 구조를 설계하고, 외부 교통데이터베이스 및 정책문서 검색 기능을 모델에 연동하기 위한 시스템 아키텍처를 구현한다.	8
10주차	RAG 기반 검색·생성 통합 기능을 시험하여 모델이 교통안전 관련 질의에 대해 근거 기반의 응답을 생성할 수 있는지 검증한다.	8
11주차	모델의 응답 품질 향상 및 오류 보정을 위해 추가 파인튜닝을 수행하고, 검색 인덱스 및 문서 임베딩 구조를 최적화한다.	8
12주차	실제 의사결정 지원 활용을 위한 시나리오(정책평가, 사고원인 진단, 안전대책 도출 등)를 설계하고, 평가 지표를 정의한다.	8
13주차	설계된 시나리오를 바탕으로 모델의 성능을 실험적으로 평가하고, 교통안전 의사결정 지원 능력과 설명력(Explainability)을 분석하고 파란학기 성과평가 보고 준비를 한다.	8
14주차	평가 결과를 분석하여 개선이 필요한 부분을 도출하고, 최종 성능 향상을 위한 모델 재학습 및 응답 품질 개선을 수행한다.	8
15주차	연구성과를 종합하여 보고서 초안을 작성하고, 모델의 주요 기능과 응답 예시를 포함한 시연 자료를 준비한다.	8
16주차	최종보고(Final Presentation)를 진행하여 전체 연구 결과, 모델 성능, 한계 및 향후 고도화 계획을 발표하고 과제를 종료한다.	8

7. 지도교수

이름/소속 박성호 / 미래자동차 혁신융합대학사업단
이 메 일: fenix3339@ajou.ac.kr

<파란학기-기업제안 프로그램 협약서>

※ 파란학기 최종결과물의 귀속 및 이익금 분배에 대해 아래와 같이 표준협약이 되었습니다.
※ 파란학기 기업제안 프로그램 신청 전 아래 사항을 숙지하여 주시고, 기업 담당자 면담 시 아래 내용에 대해 다시 한 번 확인 부탁드립니다.

제1조 (목적)
본 협약은 “아주대(=파란학기 참여학생)”와 “회사” 양 기관의 상호간 협력을 바탕으로 파란학기-기업제안 프로그램 최종 결과물을 활용함에 있어서 양 당사자의 권리 및 의무를 규정하는 것을 목적으로 한다.

제2조 (귀속 및 이익금 분배)
① 파란학기-기업제안 프로젝트의 최종 결과물은 “아주대(파란학기=참여학생)”에게 귀속된다.
② 회사가 파란학기-기업제안 프로젝트 최종 결과를 회사 운영에 활용하거나 이윤을 남기는 경우 그 이익금의 분배에 대하여는 “아주대(=파란학기 참여학생)”와 협의하여 결정한다.

제3조 (협약기간)
본 협약의 협약 기간은 협약일로부터 파란학기 종료 이후 “프로젝트 결과물”의 유효 존속 기간까지로 한다.

제4조 (협약의 변경)
본 협약의 내용은 "아주대(=아주대 참여학생)"와 "회사"의 서면합의에 의하여 유효하게 변경될 수 있다.

제5조 (신의성실의 의무)
본 협약이 목적하는 바를 상호 충족시키기 위해 필요한 제반 사항에 대하여 "아주대"는 신의, 성실을 다하여 "회사"에게 적극 협조하여야 하며, "회사" 또한 본 협약을 성실히 이행하여야 한다.

제6조 (협약의 효력)
본 협약의 효력은 쌍방이 서명 날인한 날부터 유효하다.

제7조 (해석)
본 협약에 명기되지 아니하거나 본 협약상의 해석상 이의가 있는 사항에 대하여는 쌍방의 합의에 의하여 결정한다.

[제안3]

회사명	주식회사 쏘마
분야	APT 위협 시뮬레이션
프로젝트명	사이버 위협 시뮬레이션 자동화
지도교수(소속)	곽진/사이버보안학과

1. 멘토 소개

이름/소속/직위	노용환/주식회사 쏘마/대표이사
소개글	25년 이상 보안 업계에서 다양한 정보보호 솔루션을 개발했습니다. - Firewall (방화벽개발) - IDS (네트워크 침입 탐지 시스템) - ESM (Enterprise Security Management) - 게임 보안 솔루션 - 커널기반 가상머신 - 클라우드 기반 안티바이러스 탐지 및 분석 엔진 (안랩 ASD) 현재는 엔드-포인트 행위 기반 위협 탐지 플랫폼과 사이버위협 시뮬레이션 솔루션 (BAS)를 개발하고 있는 주식회사 쏘마를 운영하고 있습니다.
연락처 (학생공지용)	- 이 메 일 : somma@somma.kr

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	MITRE ATT&CK 에 대한 이해, APT 공격기술에 대한 이해 프로그래밍 능력 (PowerShell, Python, 등)
함양 경험·역량	최신 공격 기법에 대한 이해, 악성코드 분석

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	컴퓨터 공학, 사이버 보안 관련 전공
	필 요 역 량 (프로그래밍언어 등)	공격 도구 제작을 위한 프로그래밍 능력 - 파워쉘 스크립트 작성 - 파이썬 스크립트 작성 - C/C++
멘티에게 하고 싶은 말		공개된 APT 공격/오퍼레이션 관련 정보를 수집하고, 수집된 정보를 바탕으로 실제 동작하는 공격코드를 작성하는 과정을 통해 레드팀 오퍼레이션 능력과 공격 기술에 대한 이해를 바탕으로 방어 전략을 수립하는 과정(TID, Threat Informed Defense)을 배울 수 있습니다.

5. 도전과제 주요내용

도전과제 목표	자사가 보유한 상용BAS 솔루션을 기반으로 최근 발생한 사이버 위협 (BPFDoor 같은)의 초기 침투부터 데이터 유출, 백도어 설치등의 공격 전체 생명주기를 시뮬레이션 하고, 각 공격기법에 대한 팀지 전략을 수립한다.
최종 산출물	실제 공격과 유사한 형태의 공격 코드와 각 공격들을 탐지하는데 필요한 탐지 룰

운영인원	4명
예상 투입시간	한 주당 약 8시간 * 주8~10시간 소요 시 3학점으로 인정
주요업무	
역할	**역할 세부내용**
레드팀	공격 모듈 개발
레드팀	공격 모듈 개발
레드팀	공격 모듈 개발
블루팀	공격 탐지 룰 개발

도전과제 세부내용

실제 발생한 APT 공격 사례를 조사하고, 공격 전체 생명주기에 대한 공격코드를 작성하여 전체 공격을 자동화하는 것을 목표로 합니다.

[산출물에 대한 예시]

[*] 공격그룹: Wizard Spider

[*] Operations Flow

Wizard Spider는 원래 Trickbot 뱅킹 맬웨어로 알려진 러시아 기반 전자 범죄 그룹입니다. 2018년 8월 Wizard Spider는 Trickbot 소프트웨어에 Ryuk 랜섬웨어 배포를 가능하게 하는 기능을 추가했습니다. 이로 인해 높은 랜섬웨어 복호화 비용 지불을 위해 대규모 조직을 표적으로 삼는 "big game hunting" 캠페인이 발생했습니다. 주목할만한 Ryuk 공격에는 Universal Healthcare System 병원, 미국 조지아 및 플로리다 주 정부 행정 사무소, 중국 기업이 포함됩니다.

... 생략 ...

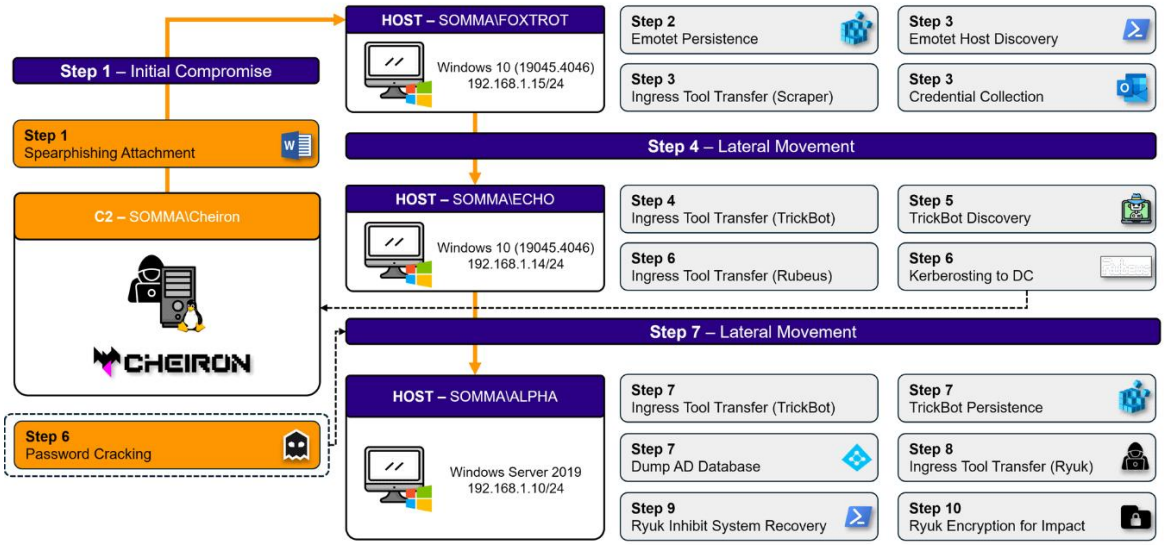
[*] Attack Phase

Phase Number	Summary
Phase 1	**피싱 이메일**을 통해 첨부된 악성 **Word** document 파일은 **매크로** 실행을 통해 사용자 PC에 침투합니다. 실행된 매크로는 **C2** 서버를 통해 추가 페이로드를 다운로드 받고 **cscript.exe** 및 **rundll32.exe** 프로세스를 활용하여 공격자 Command를 실행합니다. rundll32.exe를 통해 실행된 **Emotet(adb.dll)** 악성코드는 사용자 시스템 정보 **수집(조회)** 및 **지속성**을 유지하고 **Outlook scraper**를 통해 사용자 메일 박스에서 **Credential** 정보를 탈취합니다. 탈취된 Credential 정보를 통해 같은 도메인 네트워크 호스트로 **WinRM**을 통한 **측면 이동**을 수행하고 **Trickbot(uxtheme.exe)** 악성코드를 실행합니다.
Phase 2	실행된 Trickbot 악성코드는 주요 시스템 정보를 수집(조회)하고 **Rubeus** 공개도구를 통해 **Kerberoasting** 공격을 수행합니다. Kerberoasting 공격 수행을 통해 탈취된 **Kerberost Ticket** 정보를 바탕으로 구성된 NTLM 해시값을 **Brute Forcing**하고 **도메인 컨트롤러**에 대한 계정 정보를 탈취합니다. 탈취된 계정정보를 통해 도메인 컨트롤러로 WinRM을 통한 **측면 이동**을 수행합니다. 기타 볼륨 쉐도우 복사본, SAM 데이터 베이스 덤프를 통한 계정 정보 탈취도 수행합니다.
Phase 3	DC로 측면이동된 Trickbot은 지속성 유지 및 **Adfind** 도구 활용을 통한 도메인에 대한 모든 정보를 조회합니다. 조회된 정보를 바탕으로 가입된 도메인 호스트들의 랜섬웨어 감염을 위해 다운로드 받은 **Trickbot(uxtheme.exe)** 악성코드를 실행하여 주요 서비스 종료 및 복원 지점 삭제를 수행합니다. 마지막으로 **Process Injection**을 통해 **방어 회피**를 수행한 **Ryuk** 랜섬웨어가 **RSA-2048** 및 **AES-256** 알고리즘 방식을 통해 시스템 구성 파일을 제외한 호스트의 모든 파일을 **암호화**합니다.

[*] Infrastructure

HostName	OS	Role	IP
CHEIRON	Amazon Linux2	Linux Workstation(Attacker)	cheiron.somma.kr
FOXTROT	Windows 10 Pro - 10.0.19045.2965	Windows Workstation(DU)	192.168.1.15
ECHO	Windows 10 Pro - 10.0.19045.2965	Windows Workstation(DU)	192.168.1.14
ALPHA	Windows Server 2019 Datacenter - 10.0.17763.3650	Windows Server(DC)	192.168.1.10

[*] Operation Flow



[*] Emulation Plan

Script	Description	HostName	Source ID
Disable Windows Defender	각 Step별 주요 악성코드 정상 실행을 위해 MS Windows Defender를 비활성화 합니다.	FOXTROT ECHO ALPHA	1
Install Microsoft Office 2013	피싱 이메일 첨부파일이 악성 매크로가 포함된 Word 문서이므로 정상 실행을 위해 MS Office 365 버전 Word를 설치합니다.	FOXTROT	2
Windows Remote Management	Lateral Movement를 수행하기 위해 WinRM 초기 설정을 세팅합니다.	FOXTROT ECHO ALPHA	3
Microsoft Word, Outlook Security Settings	Microsoft Word와 Outlook에 대한 보안 설정을 세팅합니다.	FOXTROT	4
.NET Framework 3.5	Rubeus 도구 사용을 위해 .NET Framework 3.5를 설치합니다.	ECHO	5
SPN Settings	Kerberoasting을 위해 SPN을 설정합니다.	ALPHA	6
Wizard Spider Setup	Wizard Spider 시나리오에서 사용하는 Setup 스크립트입니다.	CHEIRON FOXTROT ECHO ALPHA	7

[*] 단계별 공격코드

1.B T1204.002 | User Execution: Malicious File

FOXTROT 192.168.1.15

Somma의 User Foxtrot는 메일함에서 악성 문서를 다운로드 받고 실행합니다.

```
Add-Type -AssemblyName UIAutomationClient
Add-Type -AssemblyName UIAutomationTypes
Add-Type -AssemblyName System.Windows.Forms

Start-Sleep 3

$outlookID =  (Get-Process -Name "outlook").Id
$loopcondition = $false
while (-not $loopcondition) {
    $root = [Windows.Automation.AutomationElement]::RootElement
    $condition = New-Object Windows.Automation.PropertyCondition([Windows.Automation.AutomationElement]::ProcessIdProperty, $outlookID)
    $outlookUI = $root.FindFirst([Windows.Automation.TreeScope]::Children, $condition)
    $condition = New-Object Windows.Automation.PropertyCondition([Windows.Automation.AutomationElement]::ControlTypeProperty, [Windows.Automation.ControlType
    $dataItems = $outlookUI.FindAll([Windows.Automation.TreeScope]::Descendants, $condition) | Select-Object -First 5
    foreach ($item in $dataItems) {
        if ($item.Current.Name -like "*#{ATTACKER_SENDER_NAME}*") {
            $x = $item.Current.BoundingRectangle.X + 100
            $y = $item.Current.BoundingRectangle.Y - 5
            [System.Windows.Forms.Cursor]::Position = New-Object System.Drawing.Point($x, $y)
            Start-Sleep 1
            $item.GetCurrentPattern([Windows.Automation.InvokePattern]::Pattern).Invoke()
            $loopcondition = $true
        }
    }
    if (-not $loopcondition) {
        Start-Sleep 5
    }
}
```

6. 도전과제 세부일정 (1.8. 수정)

주차	도전과제 목표 및 활동	투입시간
1주차	프로젝트 세부 내용 파악, 추진 일정 수립, 역할 분담	8
2주차	MITRE ATT&CK 에 대한 이해	8
3주차	상용 및 오픈소스 BAS 플랫폼에 대한 이해 및 실습	8
4주차	Hands-On-Lab 방식의 공격 시뮬레이션 실습 (1)	8
5주차	Hands-On-Lab 방식의 공격 시뮬레이션 실습 (2)	8
6주차	Hands-On-Lab 방식의 공격 시뮬레이션 실습 (3)	8
7주차	APT 공격 사례 조사 및 분석 (1)	8
8주차	APT 공격 사례 조사 및 분석 (2)	8
9주차	APT 공격 코드 제작 (1)	8
10주차	APT 공격 코드 제작 (1)	8
11주차	APT 공격 코드 제작 (1)	8
12주차	APT 공격 코드 제작 (1)	8
13주차	프로젝트 PT평가	8
14주차	공격 코드 생성 자동화 방안/아이디어 도출/토론	8
15주차	공격 탐지 방안 아이디어 도출/토론	8
16주차	방어자 관점(Blue team)에서의 공격 시뮬레이션 기술 적용 방안 도출/토론	8

7. 지도교수

이름/소속 곽진 / 사이버보안학과
이 메 일: security@ajou.ac.kr

<파란학기-기업제안 프로그램 협약서>
※ 파란학기 최종결과물의 귀속 및 이익금 분배에 대해 아래와 같이 표준협약이 되었습니다.
※ 파란학기 기업제안 프로그램 신청 전 아래 사항을 숙지하여 주시고, 기업 담당자 면담 시 아래 내용에 대해 다시 한 번 확인 부탁드립니다.

제1조 (목적)
본 협약은 “아주대(=파란학기 참여학생)”와 “회사” 양 기관의 상호간 협력을 바탕으로 파란학기-기업제안 프로그램 최종 결과물을 활용함에 있어서 양 당사자의 권리 및 의무를 규정하는 것을 목적으로 한다.

제2조 (귀속 및 이익금 분배)
① 파란학기-기업제안 프로젝트의 최종 결과물은 “아주대(파란학기=참여학생)”에게 귀속된다.
② 회사가 파란학기-기업제안 프로젝트 최종 결과를 회사 운영에 활용하거나 이윤을 남기는 경우 그 이익금의 분배에 대하여는 “아주대(=파란학기 참여학생)”와 협의하여 결정한다.

제3조 (협약기간)
본 협약의 협약 기간은 협약일로부터 파란학기 종료 이후 “프로젝트 결과물”의 유효 존속 기간까지로 한다.

제4조 (협약의 변경)
본 협약의 내용은 "아주대(=아주대 참여학생)"와 "회사"의 서면합의에 의하여 유효하게 변경될 수 있다.

제5조 (신의성실의 의무)
본 협약이 목적하는 바를 상호 충족시키기 위해 필요한 제반 사항에 대하여 "아주대"는 신의, 성실을 다하여 "회사"에게 적극 협조하여야 하며, "회사" 또한 본 협약을 성실히 이행하여야 한다.

제6조 (협약의 효력)
본 협약의 효력은 쌍방이 서명 날인한 날부터 유효하다.

제7조 (해석)
본 협약에 명기되지 아니하거나 본 협약상의 해석상 이의가 있는 사항에 대하여는 쌍방의 합의에 의하여 결정한다.

[제안4]

회사명	쿤텍 ㈜
분야	인공지능, 사이버보안, AI 에이전트
프로젝트명	END TO END AI Agent 보안 가시화 기술 개발
지도교수(소속)	곽진(사이버보안학과)

1. 멘토 소개

이름/소속/직위	방혁준/쿤텍/대표
소개글	- 2016.01~현재 : 쿤텍(주) 대표이사 - 2008.05~2015.12 한컴MDS테크 보안사업팀장 - 2024년 고려대학교 이학석사 (수리데이터과학)
연락처 (학생공지용)	- 내선번호 : 010-2715-7138 - 이 메 일 : joon@coontec.com

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	1. LLM 기반 AI 에이전트 기술 2. SaaS 기반 플랫폼 개발 사용 기술 3. 웹 개발 및 시각화 기술
함양 경험·역량	1. 사이버 보안 기술 이해 2. LLM 기반 AI Agent 기술 이해 3. 프로그래밍 및 데이터 시각화 경험 4. LLM 프롬프트 엔지니어링

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	사이버보안학, 전산학, 컴퓨터공학 관련 전공
	필 요 역 량 (프로그래밍언어 등)	- LLM 프롬프트 및 API 또는 MCP 등 사용 경험 - 오픈소스를 이용한 시스템 구축 경험 - 웹기반 프로그래밍 언어 1개 이상 사용 가능
멘티에게 하고 싶은 말		LLM을 이용한 어플리케이션의 보안 기술을 개발 하고 학습합니다. 실제 산업 현장에서 꼭 필요한 기술을 중심으로 MVP 기능을 구현해 봅니다.

5. 도전과제 주요내용

도전과제 목표	LLM을 기반의 최신 AI Agent Application의 보안을 테스트하고 강화하며 시각화할 수 있는 솔루션의 MVP를 개발합니다.
최종 산출물	AI Application을 위한 보안 도구

운영인원	3~5명
예상 투입시간	한 주당 약 10시간
주요업무	
역할	**역할 세부내용**
설계 및 구현	AI 에이전트 보안 도구 설계
시나리오 및 구현	보안 위협 시나리오 및 프레임워크 구현
시각화 구현	AI Agent 가시화 기술 개발
테스트 시나리오 및 구현	AI Agent의 테스트 프로브 연구 및 개발
도전과제 세부내용	
- AI 에이전트 어플리케이션을 위한 보안 도구의 설계 및 구현을 목표로 하며, 지능형 에이전트의 행위 추적, 위협 탐지, 방어 로직 설계를 합니다. - 학생들은 실제 보안 위협 상황을 모델링하여 AI 에이전트의 취약점 분석 및 공격·방어 시나리오를 작성하고, 이를 프레임워크로 개발합니다. - 에이전트 간의 상호작용, 의사결정 흐름, 보안 이벤트를 실시간으로 시각화하는 AI Agent 가시화 기술을 개발합니다. - AI 에이전트의 보안성 및 신뢰성을 평가하기 위한 테스트 프로브(Test Probe) 모듈을 설계·개발하여 자동 진단 및 검증 체계를 구축합니다.	

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	교육 목표, 산출물, 팀 구성과 실무 요구사항(기업 사례)을 정의합니다.	10시간
2주차	AI 에이전트 아키텍처 기초와 위협 모델, 에이전트 구성 요소와 공격면(데이터·모델·통신·연결성) 식별	10시간
3주차	위협 시나리오 작성, 현실적 공격 케이스(데이터 중독, 명령 주입, 정보유출 등) 상세화	10시간
4주차	연구 가설 설정과 측정지표 정의: 각 위협에 대한 가설(취약성/영향)과 검증용 정량/정성 지표 수립	10시간
5주차	테스트베드 및 프레임워크 설계 프롬프트를 통한 평가 및 검증 후 설계보정	10시간
6주차	테스트베드 및 프레임워크 설계 프롬프트를 통한 평가 및 검증 후 설계보정	10시간
7주차	가시화 요구사항 식별 및 대시보드 설계	10시간
8주차	테스트 시나리오 개발 및 테스트 환경 구축	10시간
9주차	기본 프로토타입 구현 (점검 및 수시 피드백)	10시간
10주차	기본 프로토타입 구현(점검 및 수시 피드백)	10시간
11주차	기본 프로토타입 구현(점검 및 수시 피드백)	10시간
12주차	기본 프로토타입 구현(점검 및 수시 피드백)	10시간
13주차	시나리오 기반 중간 평가	10시간
14주차	피드백 추가 구현	10시간
15주차	종합 테스트 및 버그 수정	10시간
16주차	최종 시험 평가	10시간

7. 지도교수

이름/소속 곽진/사이버보안학과
이 메 일: security@ajou.ac.kr

<파란학기-기업제안 프로그램 협약서>
※ 파란학기 최종결과물의 귀속 및 이익금 분배에 대해 아래와 같이 표준협약이 되었습니다.

※ 파란학기 기업제안 프로그램 신청 전 아래 사항을 숙지하여 주시고, 기업 담당자 면담 시 아래 내용에 대해 다시 한 번 확인 부탁드립니다.

제1조 (목적)
본 협약은 “아주대(=파란학기 참여학생)”와 “회사” 양 기관의 상호간 협력을 바탕으로 파란학기-기업제안 프로그램 최종 결과물을 활용함에 있어서 양 당사자의 권리 및 의무를 규정하는 것을 목적으로 한다.

제2조 (귀속 및 이익금 분배)
① 파란학기-기업제안 프로젝트의 최종 결과물은 “아주대(파란학기=참여학생)”에게 귀속된다.
② 회사가 파란학기-기업제안 프로젝트 최종 결과를 회사 운영에 활용하거나 이윤을 남기는 경우 그 이익금의 분배에 대하여는 “아주대(=파란학기 참여학생)”와 협의하여 결정한다.

제3조 (협약기간)
본 협약의 협약 기간은 협약일로부터 파란학기 종료 이후 “프로젝트 결과물”의 유효 존속 기간까지로 한다.

제4조 (협약의 변경)
본 협약의 내용은 "아주대(=아주대 참여학생)"와 "회사"의 서면합의에 의하여 유효하게 변경될 수 있다.

제5조 (신의성실의 의무)
본 협약이 목적하는 바를 상호 충족시키기 위해 필요한 제반 사항에 대하여 "아주대"는 신의, 성실을 다하여 "회사"에게 적극 협조하여야 하며, "회사" 또한 본 협약을 성실히 이행하여야 한다.

제6조 (협약의 효력)
본 협약의 효력은 쌍방이 서명 날인한 날부터 유효하다.

제7조 (해석)
본 협약에 명기되지 아니하거나 본 협약상의 해석상 이의가 있는 사항에 대하여는 쌍방의 합의에 의하여 결정한다.

[제안5]

회사명	프라이빗 테크놀로지
분야	인공지능
프로젝트명	Zero Trust 기반 네트워크 경계 위협탐지 및 대응 모델 개발
지도교수(소속)	곽진 교수/ 사이버보안학과

1. 멘토 소개

이름/소속/직위	김영랑/프라이빗테크놀로지/대표
소개글	2018년에 설립된 '제로 트러스트' 기반의 통신 보안 솔루션을 개발하는 기업의 대표입니다. 김영랑 대표는 네트워크 중심의 제로 트러스트 통합을 전문으로 하며, 특히 온프레미스와 클라우드를 함께 고려한 보안 서비스인 '프라이빗 커넥트'를 주력 제품으로 삼고 있습니다. 이 기업은 한국인터넷진흥원(KISA) 주관 'DPG 통합플랫폼 대상 국가망 보안체계(N2SF) 실증 사업'의 주관기업으로 선정되기도 했습니다.
연락처 (학생공지용)	- 내선번호 : 010-6449-8521

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	※ 본 프로젝트 진행 시 사용하는 핵심기술 역량 등 - 보안 대상이 되는 네트워크 망의 경계에서 보안 로그, 시스템, 네트워크, 엔드포인트의 데이터를 수집-분석-학습-탐지-대응하는 보안시스템 개발
함양 경험·역량	※ 본 프로젝트에 지원하기 위해 필요한 경험 및 역량 기술 다음 항목의 경험 중 하나 이상의 경험 필요 - 위협 행위 수행 : 테스트 환경 등에서 보안 위협에 해당하는 알려진 악성행위를 수행 또는 분석해 본 경험 - 위협 분석 : 악성코드 또는 악성 네트워크 패킷 분석 등 보안 위협에 해당하는 행위를 식별해 본 경험 - 데이터 분석 : 구조화(또는 비구조화)된 데이터를 수집-정제-분석하여 시각화해 본 경험

4. 이런 Fellow를 찾습니다

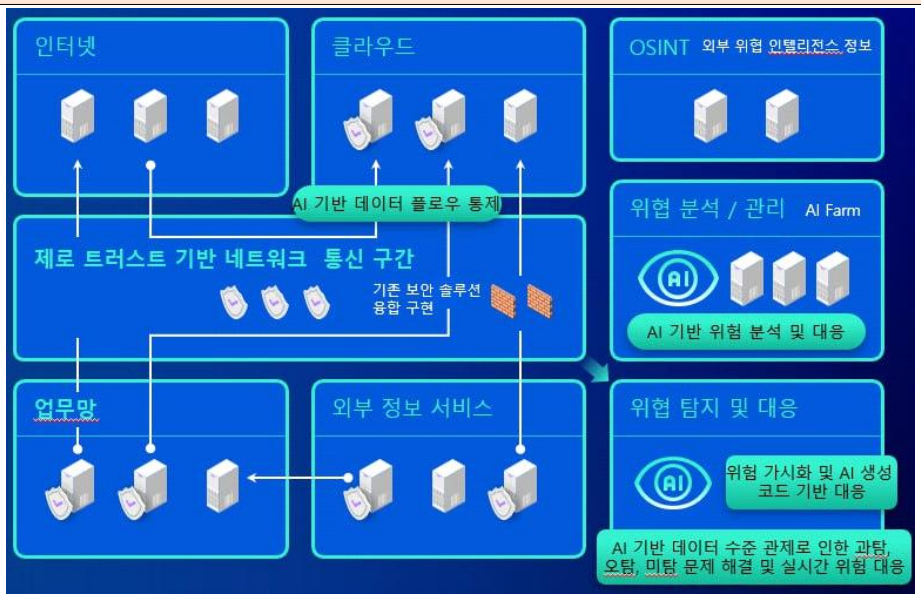
희망 멘티	**전공분야**	정보보호, 인공지능, 데이터 분석
	필 요 역 량	위협 행위 수행 및 분석 : metasploit, WireShark, Scrapy, Burp suite 등 위협 분석 : Burp suit, Fiddler, WireShark, Yara, 등

	(프로그래밍언어 등)	데이터 분석 : python, SQL/NoSQL, Docker/K8s, ELK 등

5. 도전과제 주요내용

도전과제 목표	가상의 네트워크 인프라망 내에서 발생하는 각종 이벤트의 수집-분석-탐지-대응을 자동화하고 분석-탐지 기준을 판단할 수 있는 AI 모델 개발
최종 산출물	- 1. 이벤트 수집-분석 시스템 - 2. AI 기반 데이터 분석-탐지 모델

운영인원	4명
예상 투입시간	한 주당 약 10시간
주요업무	
역할	**역할 세부내용**
위협 관리자	알려진 위협행위를 모사 및 위협 검증 위협행위 발생 시 탐지 근거 마련 및 개발 산출물 성능 검증
위협 분석가	각종 이벤트 수집 및 분석 정상, 위협데이터 수집 및 주요 위협 정보 식별
데이터 분석가	위협 탐지 엔진 개발 및 대응 수집 데이터 분석 및 라벨링을 통한 AI 학습 및 대응 근거 마련
어플리케이션 개발자	탐지 및 대응 현황 가시화 페이지 개발 및 대응 기능 개발
도전과제 세부내용	



맥락 관리
- 사용자, 시스템, 네트워크 간의 흐름을 파악하여 전체 맥락을 기반으로 위협 판단

AI 위험 평가
- AI가 위험도를 자동으로 분석하고 대응이 필요한 위협 선별

공격 표면 관리
- 내*외부 통신 경계에서 모든 디지털 자산을 탐지하고 구성 취약점, 노출 포트, 잘못된 접근 rnjgsk 등을 지속적으로 점검

로그 기반 행위 추적
- 공격자의 행위 단서를 추적하고 침입 경로와 피해 범위 규명

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	Zero-Trust 개념 & 아키텍트 이해	8
2주차	네트워크 세분화 & SD-WAN 환경 구성 - 소규모 네트워크 환경 구성	8
3주차	인증·인가·액세스 관리 - 인증 관련 로그 수집 및 위협 분석	8
4주차	디바이스 보안 & Health Check - 엔드포인트 이벤트 수집 및 위협 분석	8
5주차	네트워크 모니터링 & 로그 수집 - 네트워크 이벤트 수집 및 위협 분석	8
6주차	위협 인텔리전스 & IOC 자동화 - 위협정보 식별 및 수집 로그 비교	8
7주차	Zero-Trust Threat Hunting - 인증상태, 엔드포인트, 네트워크 이벤트 기반 상관분석	8
8주차	실시간 이상 탐지 모델 개발 - 수집 및 분석된 데이터 분석 및 학습	8
9주차	보안 정책 자동화 개발 - 보안 위협 차단 정책(YARA,suricata 등) 자동화	8
10주차	사고 대응 자동화 - 이벤트 수집-위협탐지-위협분석-대응 자동화	8
11주차	탐지 및 대응 현황 가시화 - 이벤트 수집-위협탐지-위협분석-대응 가시화	8
12주차	Zero-Trust SOC prototype 검증 - 개발 산출물 데모 및 성능 검증	8
13주차	개발 산출물 PT 평가	8
14주차	탐지 및 대응 기술 고도화 - 탐지 가능한 위협 행위 고도화 및 탐지, 대응 기술 추가 학습	8
15주차	탐지 및 대응 기술 고도화 - 탐지 가능한 위협 행위 고도화 및 탐지, 대응 기술 추가 학습	8
16주차	최종 시험 평가	10시간

7. 지도교수

이름/소속 곽진/사이버보안학과
이 메 일: security@ajou.ac.kr

<파란학기-기업제안 프로그램 협약서>

※ 파란학기 최종결과물의 귀속 및 이익금 분배에 대해 아래와 같이 표준협약이 되었습니다.
※ 파란학기 기업제안 프로그램 신청 전 아래 사항을 숙지하여 주시고, 기업 담당자 면담 시 아래 내용에 대해 다시 한 번 확인 부탁드립니다.

제1조 (목적)

본 협약은 “아주대(=파란학기 참여학생)”와 “회사” 양 기관의 상호간 협력을 바탕으로 파란학기-기업제안 프로그램 최종 결과물을 활용함에 있어서 양 당사자의 권리 및 의무를 규정하는 것을 목적으로 한다.

제2조 (귀속 및 이익금 분배)

① 파란학기-기업제안 프로젝트의 최종 결과물은 “아주대(파란학기=참여학생)”에게 귀속된다.

② 회사가 파란학기-기업제안 프로젝트 최종 결과를 회사 운영에 활용하거나 이윤을 남기는 경우 그 이익금의 분배에 대하여는 “아주대(=파란학기 참여학생)”와 협의하여 결정한다.

제3조 (협약기간)

본 협약의 협약 기간은 협약일로부터 파란학기 종료 이후 “프로젝트 결과물”의 유효 존속 기간까지로 한다.

제4조 (협약의 변경)

본 협약의 내용은 "아주대(=아주대 참여학생)"와 "회사"의 서면합의에 의하여 유효하게 변경될 수 있다.

제5조 (신의성실의 의무)

본 협약이 목적하는 바를 상호 충족시키기 위해 필요한 제반 사항에 대하여 "아주대"는 신의, 성실을 다하여 "회사"에게 적극 협조하여야 하며, "회사" 또한 본 협약을 성실히 이행하여야 한다.

제6조 (협약의 효력)

본 협약의 효력은 쌍방이 서명 날인한 날부터 유효하다.

제7조 (해석)

본 협약에 명기되지 아니하거나 본 협약상의 해석상 이의가 있는 사항에 대하여는 쌍방의 합의에 의하여 결정한다.