<파란학기-기업제안 프로그램 진행 절차>

※ 참여 희망학생 필독

① 제안1~6의 기업제안 프로그램을 살펴보고 2025-2학기 파란학기로 참여할 과제를 선정하고, 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 (~7/1(화) 11시까지)

⇩

⑤ 2025-2학기 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

2025-2학기 아주대학교 파란학기제 기업제안 프로그램 목록

NO	프로그램명	학점	연계기업명	지도교수	페이지
1	인공지능 데이터 보안과 연관된 데이터 가시화 기술과 클라우드 콘텐츠 보안기술	3	나모웹비즈	이원찬 (데이터보안·활용융합 혁신융합단)	p3
4	사이버 위협 시뮬레이션 자동화	3	쏘마	곽진 (사이버보안학과)	p8
5	AI를 활용한 사이버 위협 인텔리전스 프로파일링	3	쿤텍	곽진 (사이버보안학과)	p15
6	제로 트러스트 네트워크 기반 취약점 분석 체계 개발	3	프라이빗 테크놀러지	곽진 (사이버보안학과)	p20

[제안1]

회사명	주식회사 나모웹비즈
분야	인공지능보안, 빅데이터, 마케팅
프로젝트명	인공지능 데이터 보안과 연관된 데이터 가시화 기술과 클라우드 콘텐츠 보안기술
지도교수(소속)	이원찬(데이터보안·활용융합 혁신융합대학사업단)

1. 멘토 소개

이름/소속/직위	진병각/나모웹비즈/대표이사
소개글	- 현) 나모웹비즈 대표이사 - 전) 나모인트랙티브 전무이사 - 전) 나모인트랙티브 기업부설연구소장
연락처 (학생공지용)	- 내선번호 : - 이 메 일 : cyranojin@namowebiz.com

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	- 인공지능 데이터 보안과 연관된 데이터 가시화 기술 - 클라우드 기반 콘텐츠 보안관리 시스템 개발 기술 - 에너지 IoT 보안관제 기술 - 비마커 기반 비전 객체 인식 및 광분석 기술
함양 경험·역량	- 데이터보안의 기초가 되는 IOT 디지털트윈기술에 대한 체계적인 이해 - 비마커 기반 비전 객체 인식 보안 광문석 기술개발 - 클라우드 기반 콘텐츠 관리시스템의 데이터 보안 TOOL개발

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	- 전산학, 컴퓨터공학 관련 전공
	필 요 역 량 (프로그래밍언어 등)	- 클라우드기술에 대한 기초적인 이해 - 오픈소스를 이용한 시스템 구축 경험 - Python 라이브러리 활용 기술
멘티에게 하고 싶은 말		- 분산처리시스템의 데이터 보안기술을 이용해서 클라우드 컴퓨팅의 개념 이해 및 인공지능기반의 클라우드 콘텐츠 보안관리 Tool개발

5. 도전과제 주요내용

도전과제 목표	몰입형(Immersive) 데이터 가시화와 콘텐츠 보안관리 시스템 개발 기술
최종 산출물	인공지능기반의 클라우드 콘텐츠 보안관리 Tool개발

운영인원	5명
예상 투입시간	한 주당 약 40시간 * 주8~10시간 소요 시 3학점으로 인정
주요업무	
역할	**역할 세부내용**
사업기획	몰입형(Immersive) 데이터 가시화를 위한 인공지능기반 콘텐츠 보안관리Tool
인공지능개발	몰입형(Immersive) 데이터 가시화를 위한 콘텐츠 보안관리 시스템 개발
콘텐츠개발	몰입형(Immersive) 데이터 가시화를 위한 콘텐츠 보안관리 시스템 개발
도전과제 세부내용	

-몰입형(Immersive) 디스플레이 환경(VR/AR/MR)에서의 데이터 가시화 기술

-클라우드 기반 콘텐츠 관리 시스템 개발 기술

-에너지 IoT 관제 기술

-비마커 기반 비전 객체 인식 및 광분석 기술

-몰입형 콘텐츠 시스템(Immersive Contents System)과 클라우드 기반 콘텐츠 관리 시스템(CMS),

-IoT 기반 관제 시스템을 개발하는 디지털트윈 소프트웨어 전문가

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	프로젝트 세부내용 파악, 추진일정 수립, 역할 분담	8
2주차	몰입형(Immersive) 데이터 가시화 프레임워크 개념 이해 및 분석(구조, 활용사례 등)	8
3주차	몰입형(Immersive) 데이터 가시화 개념 이해 및 타플랫폼 차이점·장단점 분석	8
4주차	몰입형(Immersive) 데이터 가시화 동작구조 이해 및 스크립트 분석	8
5주차	몰입형(Immersive) 데이터 가시화 시스템 구축 및 실험	8
6주차	몰입형(Immersive) 데이터 가시화 서비스 시나리오 구성 및 실험	8
7주차	콘텐츠 보안관리 시스템 개념 이해 및 분석	8
8주차	콘텐츠 보안관리 시스템 개념 및 클라우드 보안 데이터 수집	8
9주차	콘텐츠 보안관리 시스템을 이용한 디지털트윈솔루션 구축 및 실험	8

주차	도전과제 목표 및 활동	투입시간
10주차	몰입형(Immersive) 데이터 가시화와 디지털트윈솔루션 테스트	8
11주차	몰입형(Immersive) 데이터 가시화의 디지털트윈솔루션 대시보드 개발	8
12주차	콘텐츠 보안관리 시스템을 이용한 디지털트윈솔루션 구축 및 실험	8
13주차	프로젝트 PT평가	
14주차	몰입형(Immersive) 데이터 가시화의 디지털트윈솔루션 대시보드 고도화 아이디어 도출 및 토론	8
15주차	몰입형(Immersive) 데이터 가시화의 디지털트윈솔루션 고도화 실행방안1	8
16주차	몰입형(Immersive) 데이터 가시화의 디지털트윈솔루션 고도화 실행방안2	8

7. 지도교수

이름/소속 이원찬 / 데이터보안·활용융합 혁신융합대학사업단
이 메 일: chanleewon@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	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)	- 내선번호 : - 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 탐지룰

운영인원	4명
예상 투입시간	한 주당 약 8시간
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 ...

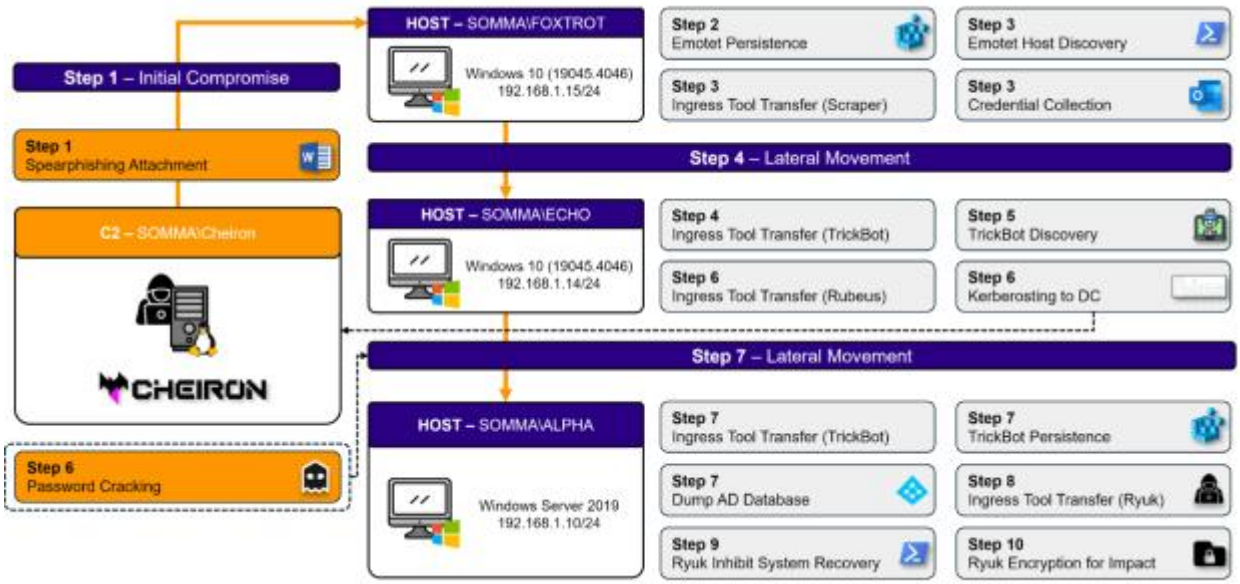
[*] Attack Phase

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(odb.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(Attocker)	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 Word 를 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

주차	도전과제 목표 및 활동	투입시간
1주차	프로젝트 세부 내용 파악, 추진 일정 수립, 역할 분담	8

주차	도전과제 목표 및 활동	투입시간
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

주차	도전과제 목표 및 활동	투입시간
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.

[제안5]

회사명	쿤텍(주)
분야	빅데이터, OSINT 보안
프로젝트명	AI를 활용한 사이버 위협 인텔리전스 프로파일링
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 : - 이 메 일 : joon@coontec.com

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	1. 네트워크 보안 및 데이터 분석 기술 2. SaaS 기반 플랫폼 개발 사용 기술 3. 웹 개발 및 시각화 기술
함양 경험·역량	1. 정보 보안 및 위협 인텔리전스 분석 경험 2. 실시간 데이터 처리 및 분석 능력 3. 프로그래밍 및 데이터 시각화 경험 4. 보안 정책 수립 및 관리 경험

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	전산학, 컴퓨터공학 관련 전공
	필 요 역 량 (프로그래밍언어 등)	- OSINT 및 빅데이터 기술에 대한 기초적인 이해 - 오픈소스를 이용한 시스템 구축 경험 - Python 등 프로그래밍 언어 1개 이상 사용 가능
멘티에게 하고 싶은 말		- OSINT를 이용한 사이버 범죄 및 위협에 대한 수집 방법 이해 - LLM을 이용한 OSINT 데이터 수집 분석 평가 자동화 시스템 개발

5. 도전과제 주요내용

도전과제 목표	공개된 OSINT기법을 활용하여 LLM 추론 기능과 LLM API를 이용하여 사이버 위협 정보 추적, 자동 분류 및 평가 엔진 개발
최종 산출물	LLM OSINT 사어버위협 추적 및 평가 시스템

운영인원	3~5명
예상 투입시간	한 주당 약 10시간
주요업무	
역할	**역할 세부내용**
웹 프레임워크	전체적인 기능을 사용가능한 웹 도구로 개발
OSINT 추적 엔진 개발	LLM을 이용한 위협 추적 도구 개발 (2명)
OSINT 평가 엔진 개발	LLM을 이용한 위협 평가 도구 개발
기획자	전체 프로젝트 리딩 및 총괄
도전과제 세부내용	
- 이미지 등의 OSINT 정보를 기반으로 LLM을 이용한 최종 정보 수집 자동화 시스템 - 정보수집의 단계와 과정에서 추론을 기반한 판단과 평가 기술 개발 - 1차 정보에서 식별 가능한 추가 정보와 메타 정보 등을 기반으로 심화 추적 기술 개발 - 반복적인 시퀀스를 LLM과 OSINT플랫폼으로 프레임워크 자동화 시스템	

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	프로젝트 세부내용 파악, 추진일정 수립, 역할 분담	10
2주차	OSINT 위협 정보 수집 및 개념, 활용 사례	10
3주차	최신 OSINT 플랫폼 기술 이해 및 한계점 분석	10

주차	도전과제 목표 및 활동	투입시간
4주차	최신 OSINT 도구 조사 및 실습 (시나리오 기반 실습)	10
5주차	OSINT 시나리오 기반 LLM을 이용한 수집, 분석, 평가 설계	10
6주차	시나리오 기반 LLM 프롬프트 엔지니링 실험	10
7주차	시나리오를 LLM과 OSINT 알고리즘를 이용한 자동화 설계	10
8주차	OSINT LLM Agent 프로그램 개발 환경 구축	10
9주차	OSINT LLM Agent 프로그램 시험 데이터 수집	10
10주차	OSINT LLM Agent 프로그램 시험 데이터 수집	10
11주차	OSINT LLM Agent 프로그램 개발 및 대시보드 개발	10
12주차	OSINT LLM Agent 프로그램 기반 데이터 자동수집 시험	10

주차	도전과제 목표 및 활동	투입시간
13주차	프로젝트 PT평가	10
14주차	자동 수집 범위 및 추가 연계 OSINT 도구 아이디어 도출 및 토론	10
15주차	OSINT LLM Agent 성능 개선을 위한 아이디어 도출 및 토론	10
16주차	다중 및 대규모 OSINT 프로파일링을 위한 시스템 개선 아이디어 도출 및 토론	10

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.

[제안6]

회사명	프라이빗테크놀로지 ㈜
분야	사이버보안
프로젝트명	제로 트러스트 네트워크 기반 취약점 분석 체계 개발
지도교수(소속)	곽진(사이버보안학과)

1. 멘토 소개

이름/소속/직위	김영랑 / 프라이빗테크놀로지(주) / 대표이사
소개글	- 現 프라이빗테크놀로지 대표이사 및 CTO - 現 한국사이버안보학회 정회원 - 前 N2SF (전 MLS) 아키텍처 설계 위원 - 前 에버스핀 CTO - 前 한국특허정보원 Patent Troll 담당
연락처 (학생공지용)	- 내선번호 : 010-6449-8521 - 이 메 일 : benjamin@pribit.com

2. 현장실습 가능 여부

현장실습 연계 가능 여부	☑ 가능 ☐ 불가능

3. 핵심기술/함양 경험·역량

사용 핵심기술	- MITRE ATT&CK 프레임워크
함양 경험·역량	- 제로 트러스트 샌드박스를 활용하여 스텔스 네트워크로 격리된 대상 자원에 대한 알려져 있는 공격 수행 - 자원에 대한 취약 요소 탐지 및 제로 트러스트 기반 대응 방안 제시

4. 이런 Fellow를 찾습니다

희망 멘티	**전공분야**	-컴퓨터 공학(보안) 전공
	필 요 역 량 (프로그래밍언어 등)	- 공격(해킹) 기술에 대한 기초적인 이해 - Python/Lua 기반 공격 스크립트 개발 경험
멘티에게 하고 싶은 말		- 자원으로 전송되는 명령어 및 각종 데이터 분석 기반 취약점 탐지 - Privilege 획득 기반 자원 내 취약점 탐지 - 네트워크 측면에서의 자원 취약점 탐지

5. 도전과제 주요내용

도전과제 목표	오픈소스 및 알려져 있는 취약점 (심각 수준)을 제로 트러스트 샌드박스를 통해 자원을 모의 공격하고 취약 여부를 판단하는 취약점 탐지 툴 개발
최종 산출물	제로 트러스트 취약점 탐지 툴

운영인원	6
예상 투입시간	한 주당 약 10시간
주요업무	
역할	**역할 세부내용**
레드팀 1	취약점 탐지 스크립트 개발
레드팀 2	취약점 탐지 스크립트 개발
블루팀 1	취약점이 존재하는 시스템 구성
도전과제 세부내용	

- 인터넷 및 네트워크에 상시 연결된 자원의 공격표면 증가 및 공급망 보안, 취약점을 활용한 다양한 공격 및 침투 행위 발생
- 인력 기반의 모의 침투 시험은 빠르게 변화하는 해킹 이코노미 시대에 한계가 존재
- 24 x7 실시간 취약점 탐지 및 침투 시험을 통해 자원에 대한 취약점을 모니터링하고 즉각적으로 대응할 수 있는 보안 체계 확립

6. 도전과제 세부일정

주차	도전과제 목표 및 활동	투입시간
1주차	프로젝트 소개 및 추진일정 수립, 제로 트러스트에 대한 이해	10
2주차	N2SF와 실 업무 시스템 및 네트워크 대한 이해	10
3주차	팀별 제로 트러스트 및 N2SF 이해 및 특장점 발표	10
4주차	세부내용 파악, 역할 분담, 제로 트러스트 샌드박스 소개 및 침투 스크립트 개발 예시	10
5주차	각 팀별 추진 계획 발표	10
6주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
7주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
8주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
9주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10

주차	도전과제 목표 및 활동	투입시간
10주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
11주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
12주차	취약점 탐지 스크립트 개발, 취약점이 존재하는 시스템 구성, 평가	10
13주차	프로젝트 PT평가	10
14주차	제로 트러스트 환경에서 상시 취약점 평가를 위한 개선 아이디어 도출 및 토론	10
15주차	제로 트러스트 환경에서 상시 취약점 평가를 위한 개선 아이디어 도출 및 토론	10
16주차	제로 트러스트 환경에서 상시 취약점 평가를 위한 개선 아이디어 도출 및 토론	10

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.