사이버 위협
시뮬레이션 자동화

2026-1 파란학기제

이삿짐센터 팀

WORK EXPERIENCE PLATFORM
WE·Meet

목차

01 팀원 소개

02 프로젝트 소개

03 APT 공격이란

04 APT 공격 사례 및 동향

05 사이버 위협 시나리오 소개

06 시연 영상

07 방어 및 탐지 전략

08 결론 및 기대효과

팀원 소개

Blue Team

손윤서
팀장
사이버보안학과 24학번

이정헌
사이버보안학과 24학번

Red Team

김현진
사이버보안학과 24학번

안영진
사이버보안학과 24학번

차진희
사이버보안학과 24학번

진화하는 APT 위협과 정적 보안의 한계

APT
공격의 고도화

소프트웨어를 타고 넘어오는 **공급망 공격**의 증가

해커조차 도입하기 시작한 **AI 공격 자동화**

기존의 사후 탐지·정적 보안으로는 대응 불가

BAS 기반
선제적·상시형
탐지 체계 구축

시나리오 최신 위협 시나리오 설계·생성

시뮬레이션 BAS 플랫폼을 통한 모의 공격 실행

분석 발생한 로그 및 행위 데이터 정밀 분석

방어 탐지 룰 수립 및 방어 전략 고도화

APT 공격이란?

Advanced Persistent Threat
지능형 지속 공격

공격자가 목표 조직내부에 장기간 거점을 확보한 뒤,
지속적으로 내부 시스템과 상호작용하며
정보를 수집하거나 추가 공격을 수행하는 형태의 공격

APT 공격 사례

최근 발생한 지능형 지속 위협(APT)의 실제 유형

- Drop box를 이용한 김수키의 최신 정보 탈취
- Lazarus Group 거짓 채용 APT 공격
- 김수키 AI 딥페이크 기반 군 공무원증 위조 사례
- 김수키 비상계엄 테마 APT

APT 공격 동향

해커가 기업 내부 시스템에 몰래 침투해 숨어 있는 평균 시간은 **280일**입니다.
오늘날의 APT 공격은 단순히 시스템을 파괴하는 것을 넘어,
우측의 **4가지 고도화 전략**을 통해 보안망을 완전히 무력화하며 장기간 정교하게 진행됩니다.

01 신뢰 인프라의 무기화

기업들이 안전하다고 믿고 쓰는 공식 클라우드, 드롭박스, 인증된 소프트웨어 공급망을 해킹의 통로로 악용합니다.

02 AI를 활용한 사회 공학의 고도화

AI 딥페이크로 공무원증을 위조하거나, 완벽한 문장으로 피싱 메일을 써서 담당자를 속입니다.

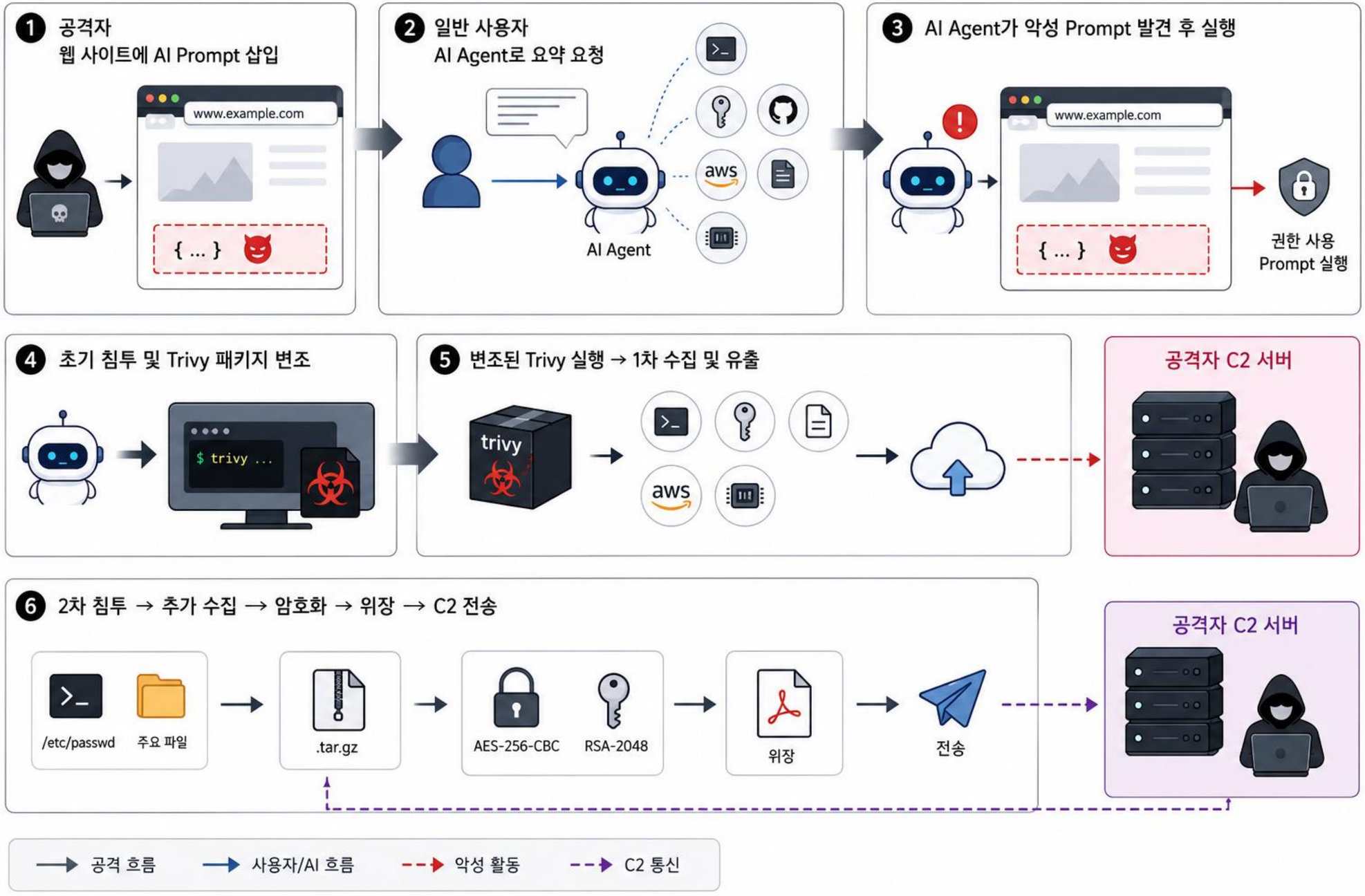
03 관심사 맞춤형 표적화의 분업

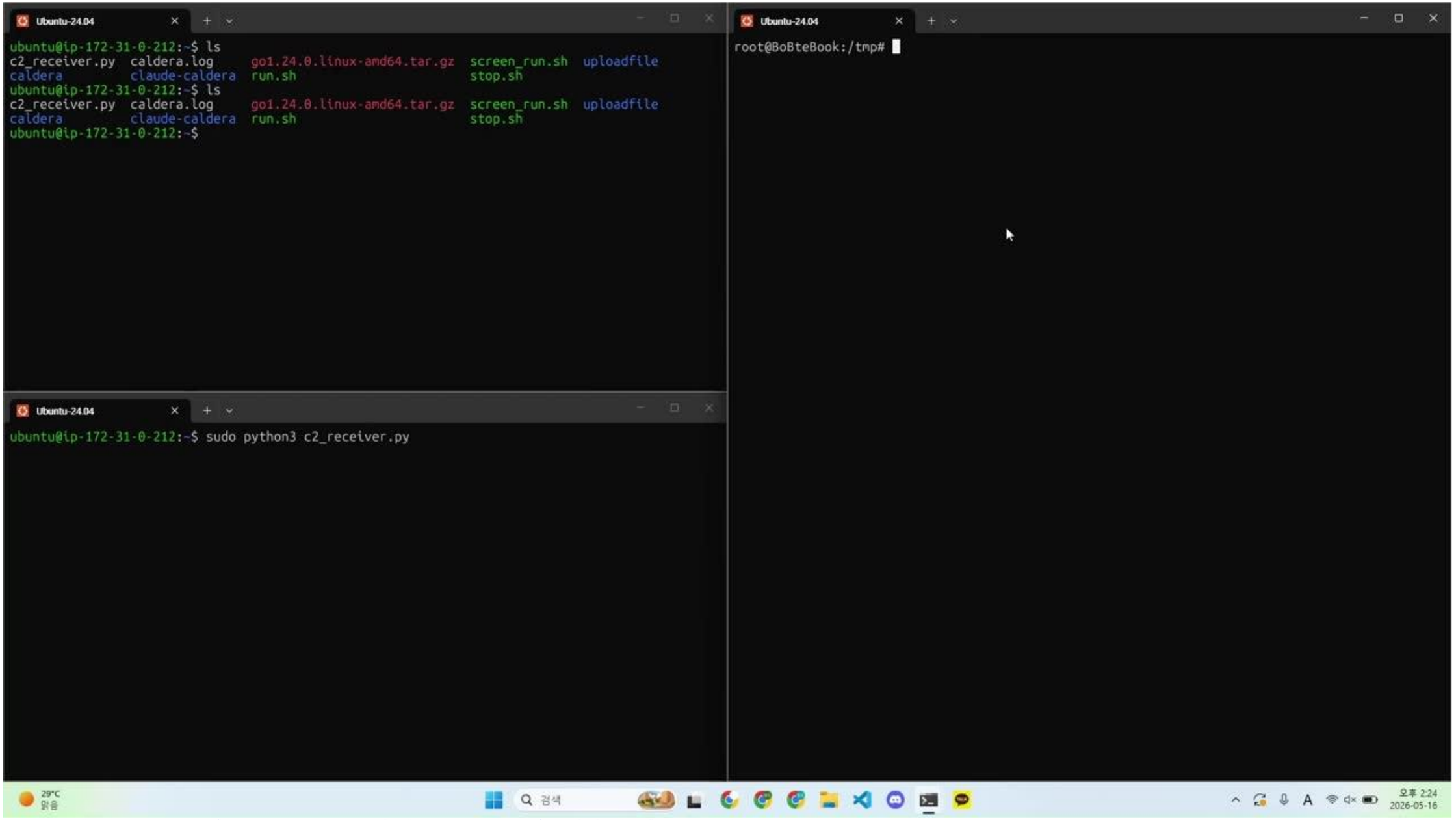
타깃 조직의 최근 이슈를 분석하는 팀과 실제 공격 팀이 기업처럼 철저히 분업화되어 움직입니다.

04 탐지 회피 기법의 다양화

악성 코드를 정상 파일처럼 압축·암호화하여 기존 보안 장비가 감지하지 못하게 교묘히 우회합니다.

만약 기업이 업무 자동화를 위해 도입한
AI Agent를 해커가 속일 수 있다면?


1 공격자
웹 사이트에 AI Prompt 삽입
www.example.com
{ ... }
2 일반 사용자
AI Agent로 요약 요청
AI Agent
aws
3 AI Agent가 악성 Prompt 발견 후 실행
www.example.com
{ ... }
권한 사용
Prompt 실행
4 초기 침투 및 Trivy 패키지 변조
$ trivy ...
5 변조된 Trivy 실행 → 1차 수집 및 유출
trivy
aws
공격자 C2 서버
6 2차 침투 → 추가 수집 → 암호화 → 위장 → C2 전송
/etc/passwd
주요 파일
.tar.gz
AES-256-CBC
RSA-2048
위장
전송
공격자 C2 서버
공격 흐름
사용자/AI 흐름
악성 활동
C2 통신



https://drive.google.com/file/d/1VoMnXEcup58htjNDmY_ToJhqBfhFP6Y3/view?usp=sharing

단계별 공격 시나리오 방어 전략 및 탐지 전략

초기 침투

- 입력 정화 - HTML 숨김 요소 제거
- 인젝션(가중치 룰셋 이용) 탐지
- 명령이 아닌 데이터에 신뢰 경계 태깅
- Agent 프로세스를 parent로 한 shell 실행 탐지
- pip/npm/curl/wget 호출 탐지
- 외부 url 접근 후 실행 흐름 탐지
- PATH 하이재킹 방어
  - 시스템 경로 우선 고정 및 sudo 실행 시 안전한 PATH 강제
  - 호스트 PATH 영향 차단

실행

- 사용자 경로에서의 Trivy 실행 탐지
- Trivy가 bash, python 등을 child로 생성하는 비정상 subprocess 탐지
- 베이스라인 수집 후, 베이스라인과 다른 프로세스 실행 탐지
- 실행 직후 네트워크 통신 탐지

권한 상승

- 허니토큰 발급 후 사용 시 탐지
- 비정상 API 호출 탐지

방어 회피

- 보안 설정 파일 변경 탐지

데이터 수집

- 민감 파일 접근 탐지
- 암호화 바이너리 호출 탐지
- 허니파일 생성 후 접근 탐지
- 압축파일 생성 탐지

정보 유출

- 비인가 도메인 DNS 쿼리 탐지
- outbound 차단 후 싱크홀 서버로 유인
- Trivy 실행 직후 네트워크 통신 탐지
- 외부 통신 제한

결론

STEP 1

학습

- 실제 APT 공격 그룹의 전술·기법·절차 분석
- BAS 플랫폼의 구조와 한계 파악

STEP 2

구현

- 전체 공격 체인을 코드로 구현
- 레드팀과 블루팀이 동일 시나리오를 각자의 관점으로 설계

STEP 3

검증

- 구현한 시나리오를 CHEIRON BAS 플랫폼에 Technique → Group → Action 구조로 등록
- 실제 실행하여 동작 검증

STEP 4

제안

- 기존 BAS의 한계 분석 후 LLM 기반 CTI-to-BAS 자동화 파이프라인 제안
- ASK 2026 논문 게재 승인

APT 공격 흐름을 코드 수준에서 구현하고 BAS 플랫폼에서 검증했으며, 구현한 공격에 대하여 단계별 탐지 룰과 방어 전략을 수립했습니다. 프로젝트 진행 과정에서의 학습 내용을 기반으로 하여 ‘LLM 기반 BAS 자동화 방향’을 학술 논문으로 제안했습니다.

성과

AI 시대,
공격과 방어의 선순환 실증

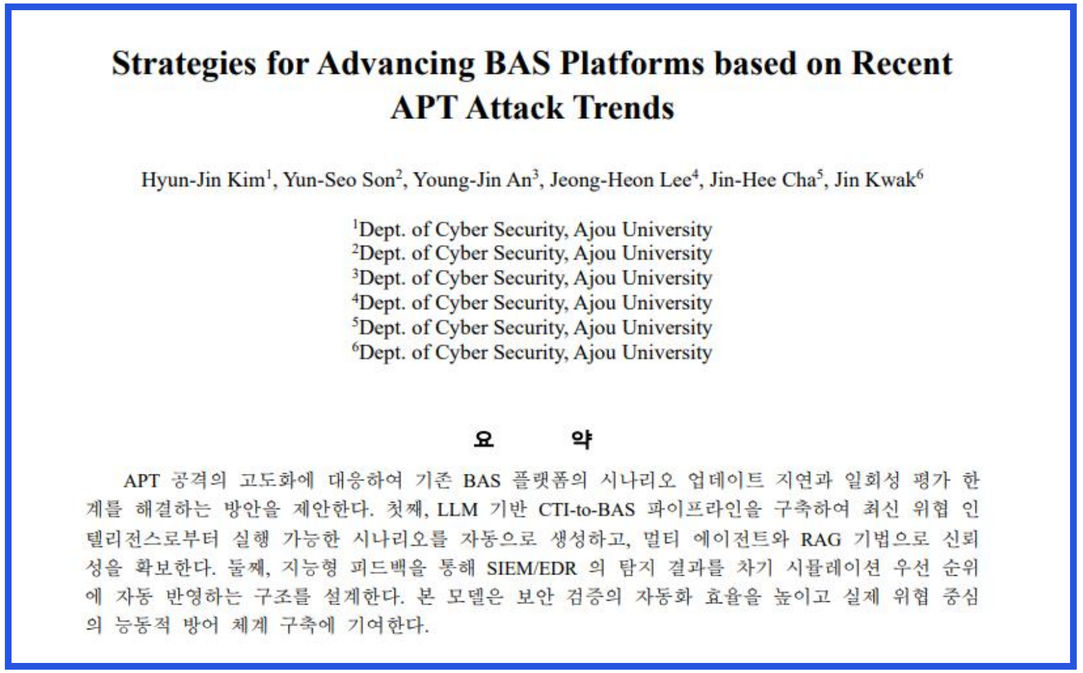
Red팀의 실제 간접 프롬프트 인젝션(IPI) 구현과 Blue팀의 공격 로그 기반 탐지 룰 설계를 통한 실증

기성 플랫폼 공백 보완

1회성 컨설팅 한계를 극복하고 최신 위협을 상시 진단할 수 있는 자동화 가능성 검증

연구 자산화

구현 단계의 문제의식을 학술적 질문으로 발전시켜 실습 경험을 공식 성과로 입증



Strategies for Advancing BAS Platforms based on Recent APT Attack Trends

Hyun-Jin Kim[1], Yun-Seo Son[2], Young-Jin An[3], Jeong-Heon Lee[4], Jin-Hee Cha[5], Jin Kwak[6]

[1]Dept. of Cyber Security, Ajou University
[2]Dept. of Cyber Security, Ajou University
[3]Dept. of Cyber Security, Ajou University
[4]Dept. of Cyber Security, Ajou University
[5]Dept. of Cyber Security, Ajou University
[6]Dept. of Cyber Security, Ajou University

요 약

APT 공격의 고도화에 대응하여 기존 BAS 플랫폼의 시나리오 업데이트 지연과 일회성 평가 한계를 해결하는 방안을 제안한다. 첫째, LLM 기반 CTI-to-BAS 파이프라인을 구축하여 최신 위협 인텔리전스로부터 실행 가능한 시나리오를 자동으로 생성하고, 멀티 에이전트와 RAG 기법으로 신뢰성을 확보한다. 둘째, 지능형 피드백을 통해 SIEM/EDR 의 탐지 결과를 차기 시뮬레이션 우선 순위에 자동 반영하는 구조를 설계한다. 본 모델은 보안 검증의 자동화 효율을 높이고 실제 위협 중심의 능동적 방어 체계 구축에 기여한다.

ASK 2026 학술 논문 게재 승인
학부생 논문경진대회 NSR 소장상 수상
LLM 기반 BAS 자동화 파이프라인 제안

기대효과

APT 테스트 커버리지 확대

· 복잡한 APT 시나리오 자동화로 보안 점검의 범위와 빈도 극대화
· 공격 스크립트 작성 리소스 최소화로 고도화된 타깃형 위협 분석에 집중

인프라 탐지 공백 식별

· 시뮬레이션을 통해 인프라 내 잠재적 사각지대 제거
· 실전 위협 데이터를 기반으로 SIEM / EDR 탐지 룰 개선 근거 확보

BAS 시나리오 지연 해소

· 기성 BAS 플랫폼의 고질적인 '시나리오 업데이트 지연' 한계 극복
· LLM 기반 자동 생성 메커니즘으로 최신 인텔리전스의 실시간 자산화

보안 패러다임 전환: 1회성 보안 컨설팅 의존에서 벗어나, 비용 효율적인 **365일 상시 검증**으로 전환 가능
AI 도입 안전망: 기업들의 AI Agent 도입 시 최대 걸림돌인 **보안 신뢰성 문제에 대한 실질적 기술 솔루션** 제공

감사합니다

Thank you for your
attention.