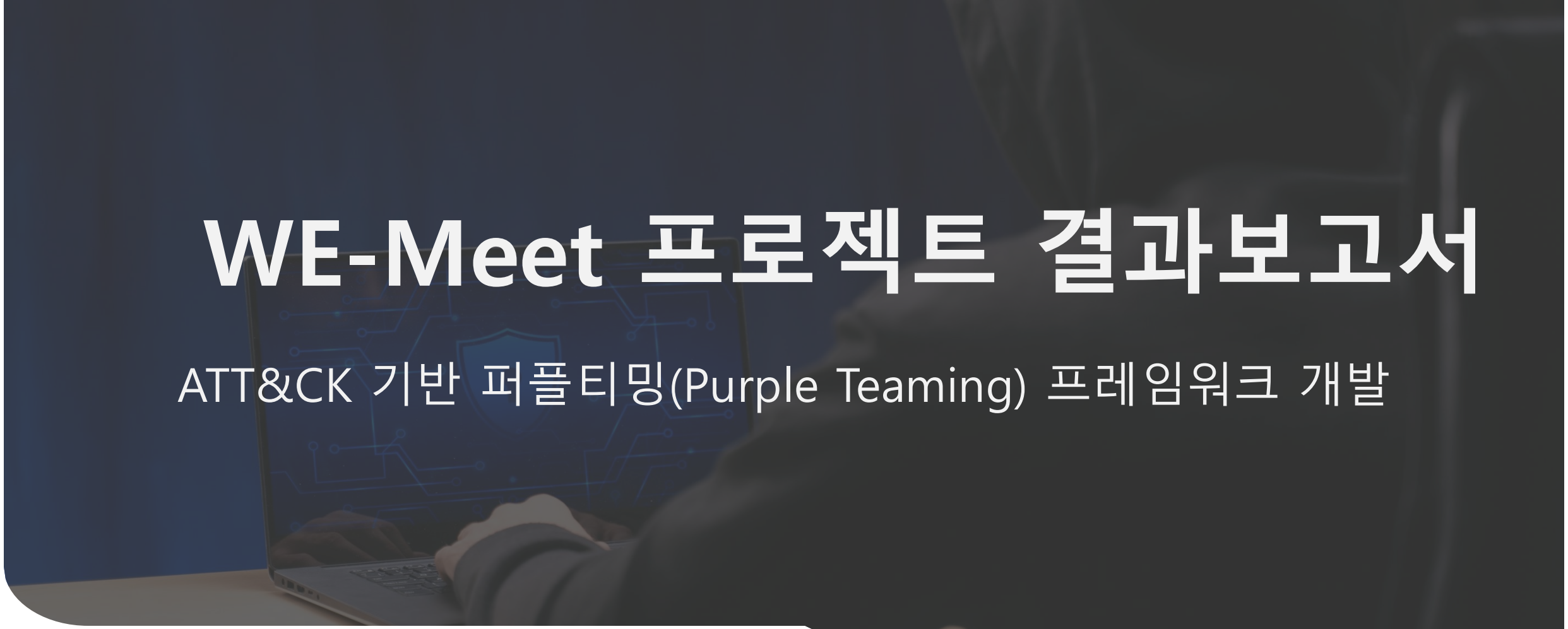


WE-Meet 프로젝트 결과보고서

ATT&CK 기반 퍼플티밍(Purple Teaming) 프레임워크 개발

참여 프로젝트 | ATT&CK 기반 퍼플티밍(Purple Teaming) 프레임워크 개발_C
멘토/지도교수 | 이철호, 최창진 (기업멘토), 김상형 (지도교수)
팀 명 | 정찬이가좋아하는블루베리
팀 원 | 나소진 (팀장), 이정찬, 이현재, 진건승 (팀원)

WORK EXPERIENCE PLATFORM
WE·Meet

CONTENTS

목차

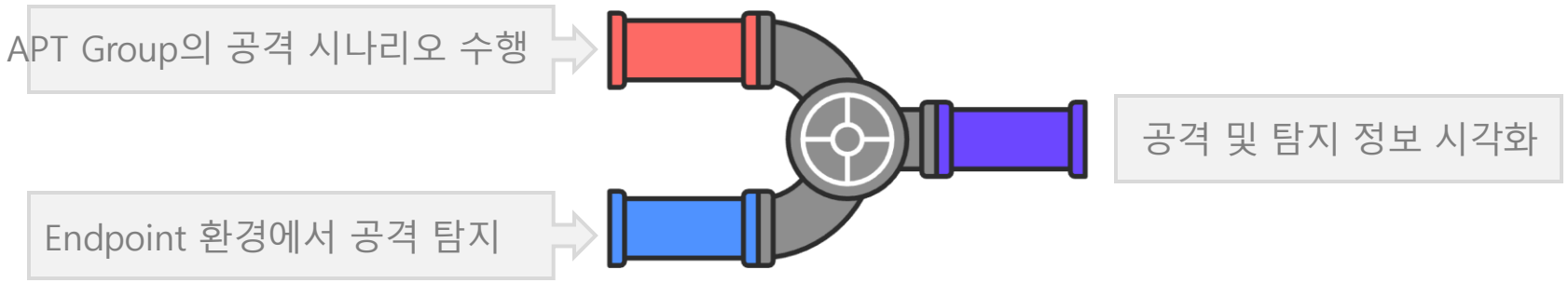
CHAPTER
01

프로젝트 개요

프로젝트 소개 및 추진 배경

프로젝트 개요

- 프로젝트 소개
  - ATT&CK 기반 Purple Teaming 프레임워크
    - Red Team(공격팀)과 Blue Team(방어팀)을 통합한 보안 평가 접근법인 Purple Teaming 서비스를 자동화한 프레임워크를 개발



프로젝트 개요

- 프로젝트 목표
  - 서비스의 기능을 RED, BLUE, PURPLE로 구분하여 아래와 같은 목표를 수립

Analytics	RED TEAM	BLUE TEAM	PURPLE TEAM
MITRE의 ATT&CK Matrix 학습	공격 Simulation 환경 구축	Endpoint 악성 행위 탐지 환경 및 SIEM 구축	BAS와 SIEM 데이터 ATT&CK 기반 TTPs 시각화
APT 그룹의 공격 TTPs 분석	APT 그룹의 공격 시나리오 재연	Sigma rule을 응용하여 단일 공격 및 복합 공격(APT 등) 탐지	

프로젝트 개요

- 프로젝트 배경

현대 사이버 보안의 한계

- 복합적 공격에 대한 단일 관점 방어
- 분리된 Red/Blue Team 구조로 인한 정보 공유 지연
- 탐지 불가한 공격에 대한 실시간 대응의 어려움

+

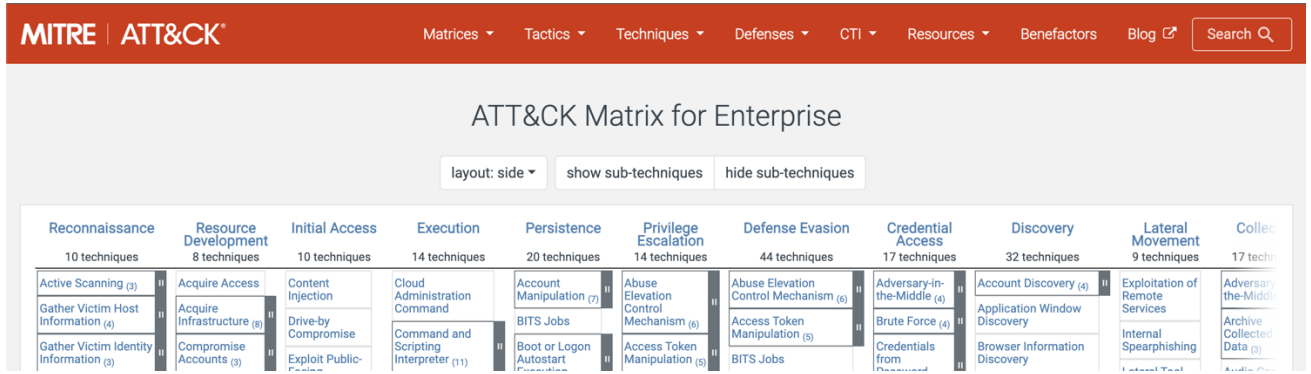
Purple Teaming의 장점

- Red Team과 Blue Team의 통합적 접근
- 공격팀 – 방어팀 간의 표준화된 커뮤니케이션
- 예방, 탐지, 대응 메커니즘을 사전에 개선 가능

표준화된 ATT&CK 프레임워크를 이용하여 Purple Teaming으로 협력적인 사이버 보안 환경 조성

프로젝트 개요

- 프로젝트 배경
  - 관련 용어 및 기술
    - TTPs
      - 공격자가 사용하는 전술(Tactics), 기술(Techniques), 절차(Procedures)
    - ATT&CK
      - MITRE에서 제작한 사이버 공격자들의 전술과 기술을 체계적으로 정리한 프레임워크



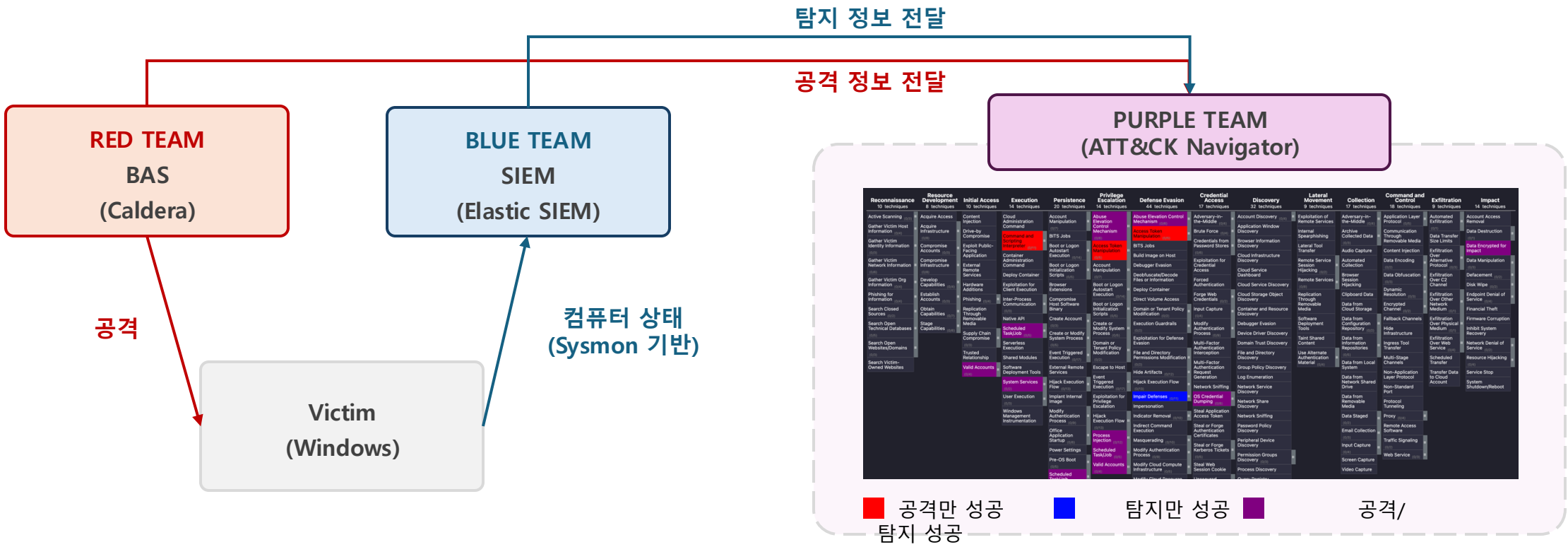
[그림. MITRE의 ATT&CK Homepage]

프로젝트 개요

- 프로젝트 배경
  - 관련 용어 및 기술
    - BAS (Breach and Attack Simulation)
      - 실제 사이버 공격을 모방하여 조직의 보안 태세를 평가하는 자동화된 도구
      - 프로젝트 내에서 RED TEAM의 형태로 사용
    - SIEM (Security Information and Event Management)
      - 다양한 보안 이벤트를 중앙에서 수집, 분석하여 위협을 탐지하는 보안 관리 시스템
      - 프로젝트 내에서 BLUE TEAM의 형태로 사용
    - Sigma
      - 다양한 SIEM 시스템에서 사용할 수 있는 로그 기반의 탐지 규칙을 작성하기 위한 오픈 표준

프로젝트 개요

- 프로젝트 예상 결과물
  - Windosw 환경에서 오픈소스를 이용한 Purple Teaming Framework



프로젝트 개요

- 프로젝트 예상 결과물
  - 특징
    - Promox 서버를 사용한 TEAM별 Virtual Machine 생성 및 관리
    - RED TEAM
      - Kali Linux 환경 기반 Caldera 환경 구축
      - Caldera(Cyber Adversary Language and Decision Engine for Red Team Automation)
        - BAS(Breach and Attack Simulation)의 일종
        - MITRE에서 개발한 오픈소스 침투 테스트 자동화 시스템
        - 실제 공격자의 행동을 모방하여 공격 시나리오 생성 및 실행

프로젝트 개요

- 프로젝트 예상 결과물
  - 특징
    - BLUE TEAM
      - Ubuntun Server 환경 기반 Elastic SIEM 환경 구축
      - Elastic SIEM
        - Elastic Stack(Elasticsearch, Logstash, Kibana)을 기반으로 한 오픈소스 보안 정보 및 이벤트 관리 솔루션
        - 실시간 데이터 수집 및 분석과 규칙 기반 알림 생성 기능 지원
        - 파일 전송 플러그인 Winlogbeat의 Sysmon 모듈을 이용한 Windows 이벤트 수집 가능
      - SIGMA rule 기반 탐지

프로젝트 개요

- 프로젝트 예상 결과물
  - 특징
    - PURPLE TEAM
      - MITRE의 ATT&CK Framework 기반
      - Caldera와 Elastic SIEM에서 받은 정보를 기반으로 공격 및 탐지 여부 판별
      - 탐지 결과를 TTPs에 따라 ATT&CK Navigator 형태로 시각화

CHAPTER
02

프로젝트 수행 과정

업무분장 및 수행 과정

프로젝트 수행 과정

- 업무분장

프로젝트 수행 과정

- 프로젝트 수행 일정

항목	9월				10월				11월				12월				진행도
	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주	
프로젝트 세부 목표 수립																	✓
프로젝트 세부 목표 구체화																	✓
ATT&CK 프레임워크 분석 및 BAS 시스템 구축																	✓
BAS를 이용한 공격 시나리오 구성 및 재연																	✓
Sysmon, Sigma, elasticsearch 기반 엔드포인트 공격탐지 시스템 구축																	✓
BAS 및 엔드포인트 공격탐지 시스템 기반 단일공격 탐지																	✓
ATT&CK 및 Sigma를 응용한 복합공격 탐지																	🔼
공격 및 탐지 정보 Navigator 시각화																	✓
최종 점검 및 보고서 제출																	🔼

프로젝트 수행 과정

- 프로젝트 수행 중 발생한 문제 및 해결 과정
  - Caldera Operator 설정 문제
    - 초기 상황 및 구성 환경
      - Kali Linux 환경에서 apt를 통한 CALDERA 설치 후 Adversary 프로필 생성 및 저장 불가 문제 발생

프로젝트 수행 과정

- 프로젝트 수행 중 발생한 문제 및 해결 과정
  - Caldera Operator 설정 문제
    - 문제 해결 과정
      - apt로 설치되는 CALDERA(v4.2.0)를 Github에서 직접 다운로드 후 소스코드를 빌드
      - 공식 문서로 확인되는 지원 가능한 Python 버전별로 모두 검증
        - Python 3.9: 라이브러리 deprecated 문제 발생
        - Python 3.8: 동일한 라이브러리 호환성 문제
        - Python 3.7: 모든 라이브러리 정상 작동 (문제 해결)

프로젝트 수행 과정

- 프로젝트 수행 중 발생한 문제 및 해결 과정
  - Caldera Operator 설정 문제
    - 최종 해결
      - Python 3.7 가상환경에서 CALDERA 설치
      - Adversary 프로필 생성 및 저장 기능 정상 작동 확인

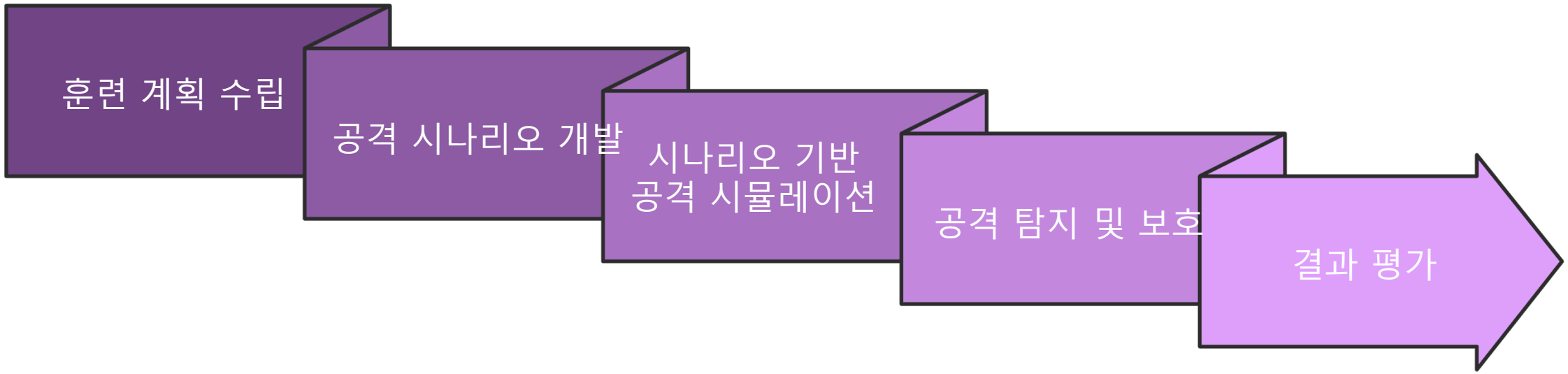
CHAPTER
03

프로젝트 수행결과

프로젝트 결과 산출물 및 시연 영상

프로젝트 수행 결과

- Purple Teaming Process 도출

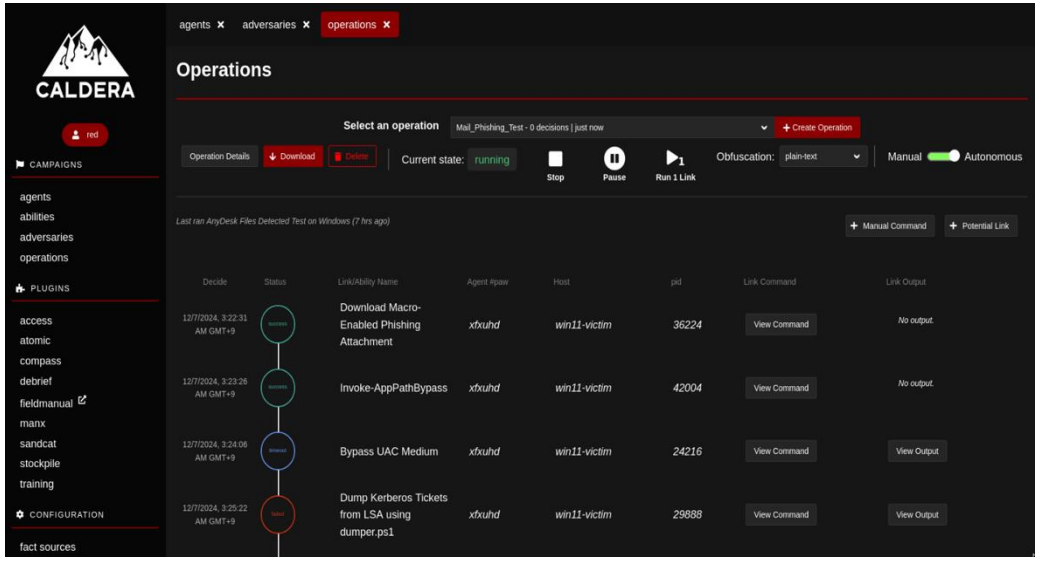


프로젝트 수행 결과

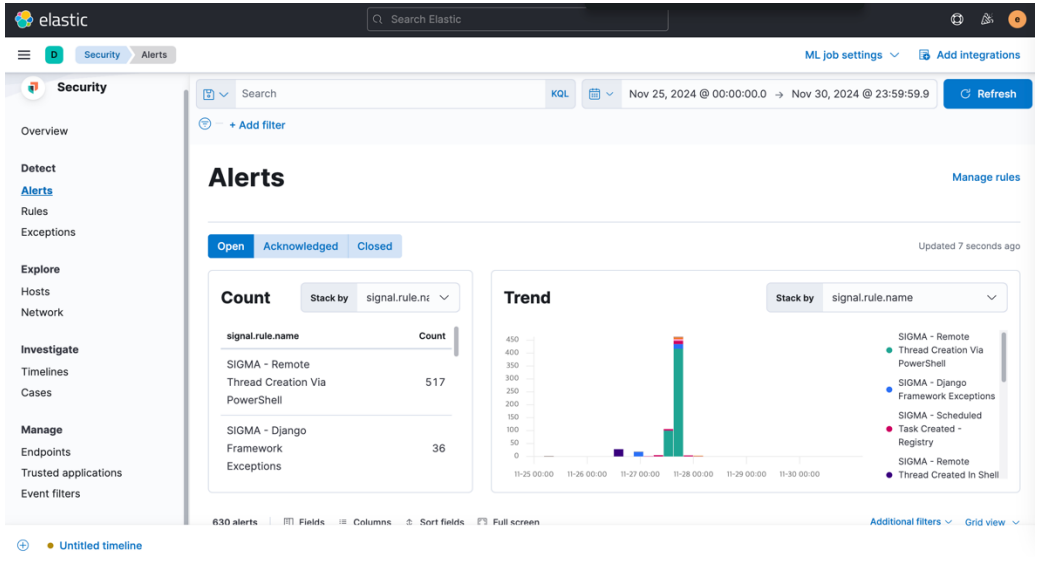
- 주요 기능
  - Caldera를 이용한 시나리오 기반 침투 테스트 자동화
  - ELK SIEM의 Winlogbeat 모듈을 통한 Windows 환경에서의 이벤트 수집
  - SIGMA Rule 기반 ELK SIEM의 공격 탐지
  - 공격 정보 및 탐지 정보를 결합하여 MITER ATT&CK 기반 공격의 TTPs 시각화

프로젝트 수행 결과

- 공격 및 탐지 환경 구축



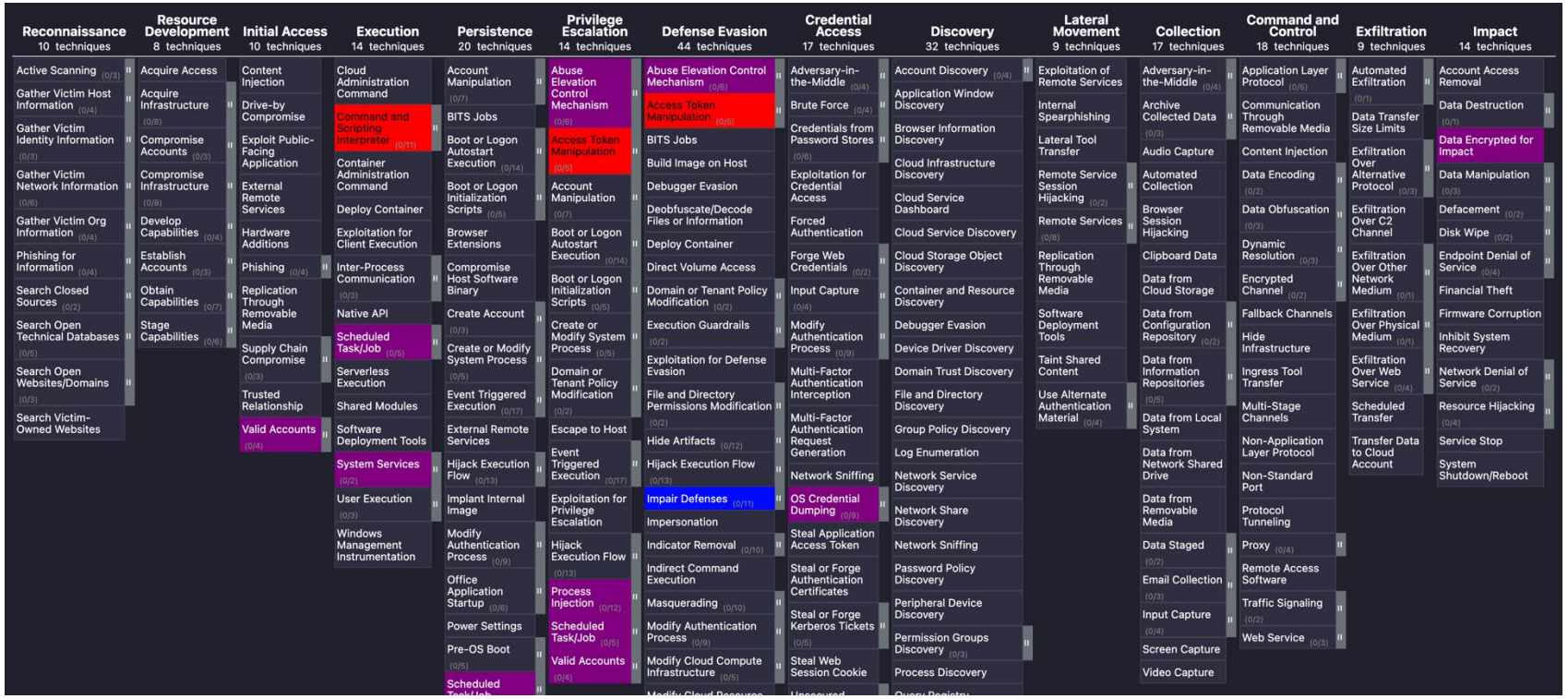
[RED TEAM 역할의 Caldera 테스팅 환경]



[BLUE TEAM 역할의 Elastic SIEM 테스팅 환경]

프로젝트 수행 결과

- Purple Teaming Navigator 제작



프로젝트 수행 결과

Demo video (바로 가기)

URL : https://youtu.be/deRVwHO_B_8

Purple teaming Navigator (바로 가기)

URL : https://github.com/bellaria19/attack-navigator.git

CHAPTER

04

예상 효과

기대효과 및 활용 분야

예상 효과

- 기대효과

보안 체계 강화

> TTPs 기반 체계적 위협 분석

> 공격-방어 과정 반복 수행을 통한 보안
개선 프로세스 수립

> 실제 공격 사례를 기반한 시나리오 훈련을 통한 보안 솔루션 평가

비용 절감

> 현재 사용 중인 보안 솔루션 평가에 적용하여 기능 개선을 통한 사고 예방

> 자동화된 보안 테스팅을 통한 비용 감소

> RED TEAM, BLUE TEAM 개별 서비스 환경 구성 대비 시간 단축

예상 효과

- 활용 분야

침투 테스트

자동화된 모의해킹 및 APT 시나리오 검증

취약점 진단 자동화

보안 관제

실시간 위협 탐지 및 보안 이벤트 분석

대응 체계 고도화

침해사고 대응

위협 탐지 규칙 검증 및 분석 자동화

대응 절차 훈련

교육 및 연구

신규 공격 기법 연구 및 방어 전략 수립

탐지 규칙 개발

Reference

[1] MITRE ATT&CK, https://attack.mitre.org/#
[2] Elastic, https://www.elastic.co/kr/elasticsearch
[3] MITRE ATT&CK Navigator, https://mitre-attack.github.io/attack-navigator/
[4] Promox, https://www.proxmox.com/en/
[5] "Red Teaming: The Art of Ethical Hacking", Joshua Pennell, ISSA, 2003
[6] "Continuous Security: Implementing the Critical Controls in a DevOps Environment", SANS Institute, 2016
[7] Purple Teaming: A comprehensive and collaborative approach to cyber security, Erik Van Buggenhout, Cyber Security: A Peer-Reviewed Journal, 7 (3), 207-216 (2024)
[8] SigmaHQ/sigma, https://github.com/SigmaHQ/sigma