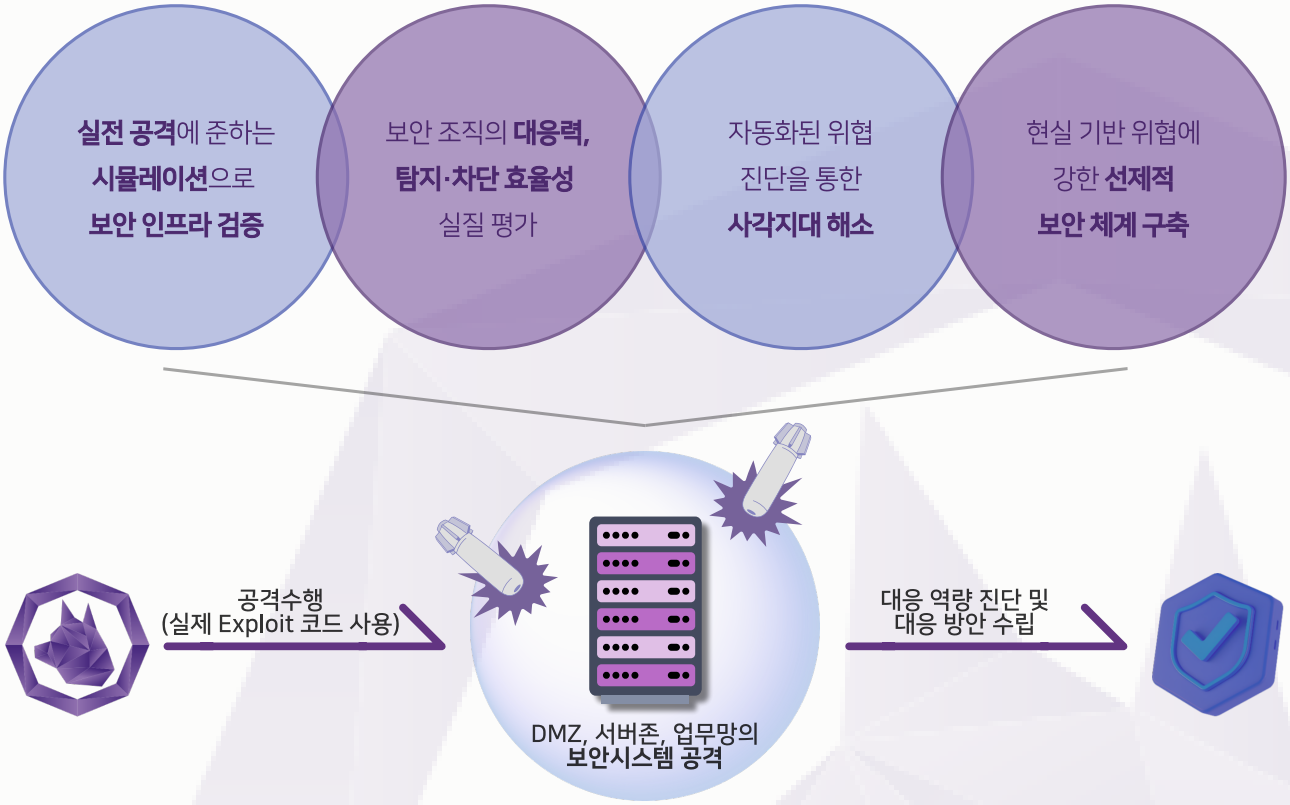

방어의 시작, 공격을 시뮬레이션하라!
PurpleHound

방어의 시작, 공격을 시뮬레이션하라!

"최선의 방어는 공격이다"라는 원칙 아래, PurpleHound는 실제 상황을 가정한 시뮬레이션을 통해 실질적인 대응 역량을 강화합니다. 조직의 보안 시스템(단말/네트워크 보안)이 기존/신규 외부 위협에 효과적으로 대응 하는지를 선제적으로 검증하고 보완하는 체계를 제공합니다.



안전한 가상화 기반 시뮬레이션

1. 실제 공격 수행을 통해 타 솔루션과 차별화
2. 현실적인 공격을 안전하게 재현
3. 가상화 시스템 제어기능 제공

정밀 제어 가능한 공격 단계

1. 각 공격 단계를 세밀하게 분할하여 제어할 수 있는 인터랙티브 모드 지원
2. Breakpoint, Resume, Suspend, Step, Abort 등 직관적 제어

PurpleHound
주요 특징

국내 환경 최적화 지원

1. MITRE ATT&CK 기반 시나리오
2. 한컴오피스(HWP), 알집(ALZIP) 등 국내 환경 고려
3. 주기적 업데이트를 통한 신속한 공격 시나리오 제공

현실성 높은 고도화 공격 구성

1. 최신 비공개 취약점 활용
2. 고객 맞춤형 시나리오 제작
3. 자체 개발 공격코드로 실제 위협 재현
4. 탐지 및 대응 솔루션 포함

사이버 위협을 넘어서는 전략적 '보안시스템' 검증

실제 공격에 앞서 **보안시스템의 취약점을 사전에 발견**하고 **대응할 수 있도록 설계된 선제적 보안 체계를 제공**합니다.
PurpleHound는 단순한 테스트 툴이 아닌, 실전 공격에 강한 조직을 만드는 '모의 침투형 보안 시스템'입니다.

보안 조직의 실전 대응력 강화

1. 실제 해커의 공격을 기반으로 한 시뮬레이션
2. 탐지 → 격리 → 복구 전 과정 정량 측정
3. 랜섬웨어, 정보유출 등 고위험 시나리오 훈련
4. 신규 보안 솔루션 성능 사전 검증

최신 취약점 기반 위협 검증 및 대응

1. 신규 취약점 시나리오 실습
2. 위협 영향 진단 및 대응 우선순위 수립
3. 정밀 분석 보고서 제공
4. 구체적 대응 전략 수립

모의해킹의 한계 보완

1. 자동화·반복 실행 가능
2. 최신 공격 기법 반영
3. 시간·비용 절감, 정량적 보안 평가
4. 신규 취약점에 대한 신속한 위협 테스팅 수행 및 조치 방안 제공

> **PurpleHound와 함께**, 조직의 보안 체계를 실전 수준으로 끌어올리십시오.

PurpleHound 시뮬레이션 시나리오

01
산업별 특화 시나리오

금융권, 공공기관/연구소,
국방/방위산업, 언론사, 대기업(하이테크 기술 유출 방지)

02
공격자 특화 시나리오

APT(Advanced Persistent Threat)그룹, Lazarus(North Korea),
Panda(China), Kimsuky(North Korea), Fancy Bear(Russia) 등

03
TTP 관점 통합 시나리오

스피어피싱, Full Chain 통합 시나리오, 보안 솔루션 우회,
데이터 수집 및 유출, 내부 네트워크 전파 등

04
보안 인프라 특화 시나리오

네트워크 보안(WAF, IDS, IPS), 이메일 보안,
엔드포인트 보안(AV, EDR), 데이터 유출 방지(DLP)

78researchlab
'알파고'를 이긴 '이세돌 9단'의 '78번째 수'
역사적인 신의 한수이자 시스템 보안 취약점 연구로 더욱 안전한 시스템을 만들고자 한다는 의미를 담음

PurpleHound

ResearchLab
78researchlab.com | 02-6952-7809 | contact@78researchlab.com
본사 : 서울시 강남구 봉은사로 114 5F | 기업부설연구소 : 서울시 강남구 봉은사로 114 6F