

G-PRIVACY 2023

2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

임직원 '마인드 셋'을 위한 악성메일 모의훈련 전략

#APT #Security Awareness Training #FAS00 #Mind-SAT

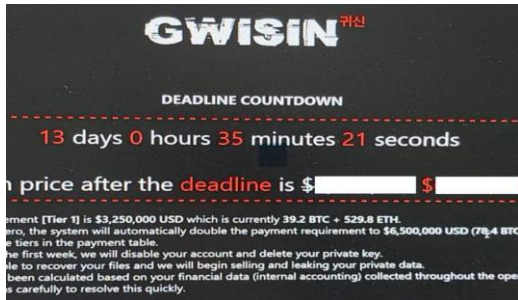
주식회사 파수 | 김은환 컨설턴트

FAS00

국내 사이버 침해 사고 현황

22년 **국내 기업**만을 대상으로 하는 **랜섬웨어** 등 **사이버 침해 사고** 다수 발생, 주 공격 경로는 **피싱**

국내 기업만 노리는 랜섬웨어



- 국내 기업만 특정하여 노리는 귀신(GWISIN) 랜섬웨어
- 22년 국내 다수 기업이 해당 랜섬웨어로 피해 발생

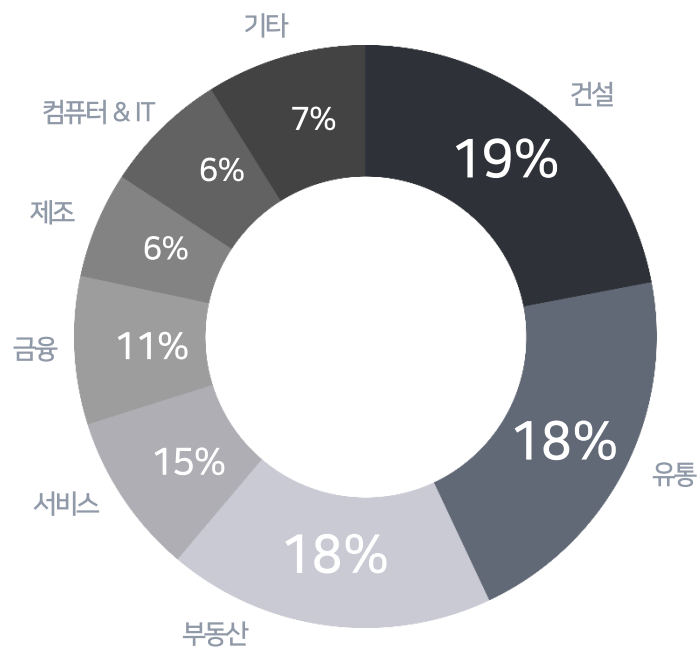
중소기업 대상 랜섬웨어



- 21~22년 배달대행업체, 콜택시 호출업체 대상 랜섬웨어 피해 발생
- 22년 4월 국내 헬스케어 업체 랜섬웨어 피해 발생
- 중소기업 특성 상 보안에 예산 투자가 어렵다는 점을 노린 공격

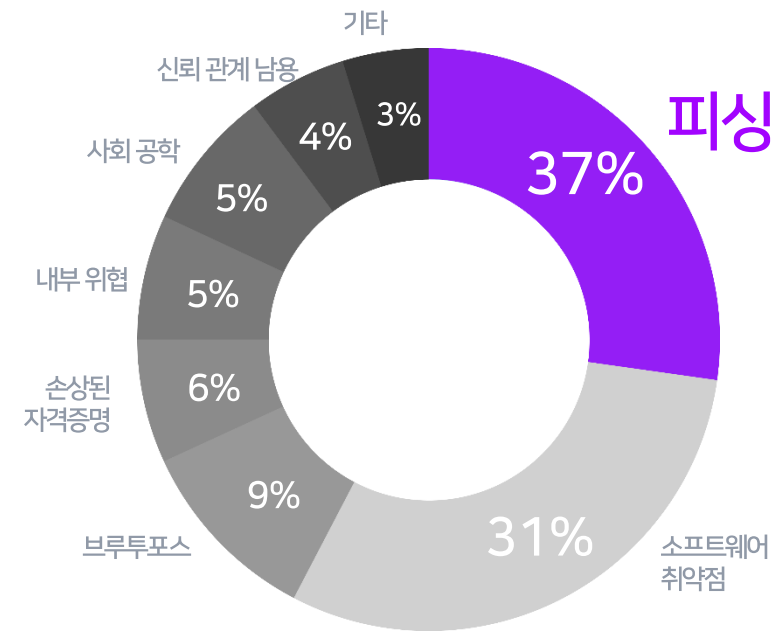
악성메일이란?

악성 코드를 포함하는 링크 또는 첨부파일 등이 삽입된 메일로써, **피싱(Phishing)** 공격의 주요 수단



산업군별 피해 현황

* 출처 : 아크로니스 2022년 하반기 사이버위협 동향 리포트



사이버 침해 사고 경로 현황

* 출처 : 팔로알토네트웍스 침해 대응 연구팀 (연구42)

악성메일은 사이버 침해 사고의 Trigger

보안에 가장 취약한 고리는 **사람**, 그 사람을 공격하는 가장 보편화된 방법은 **Phishing!**



보안에 취약한
사용자



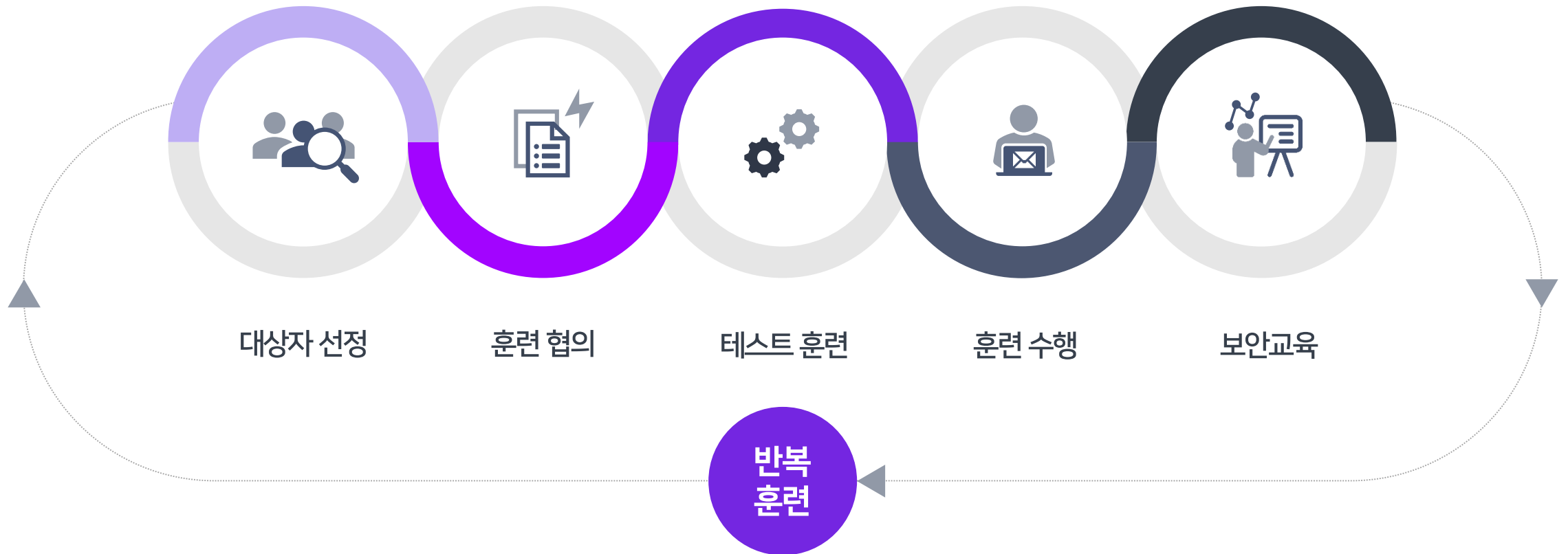
보편화된 공격 방식
Phishing, Whaling...



정보 탈취, 금전 요구 등의
사이버 침해 사고 발생

악성메일 모의훈련이란?

임직원들의 **보안 인식** 제고를 위하여 실제 악성 메일과 매우 흡사한 훈련용 이메일을 활용한 사이버 모의훈련



악성메일 모의훈련 유형

링크 접속 유도형 악성메일 모의훈련

메일 수신

메일 열람

링크 접속

훈련 안내/메일 신고

첨부파일 실행 유도형 악성메일 모의훈련

메일 수신

메일 열람

첨부파일 다운 및 실행

훈련 안내/메일 신고

개인정보 입력 유도형 악성메일 모의훈련

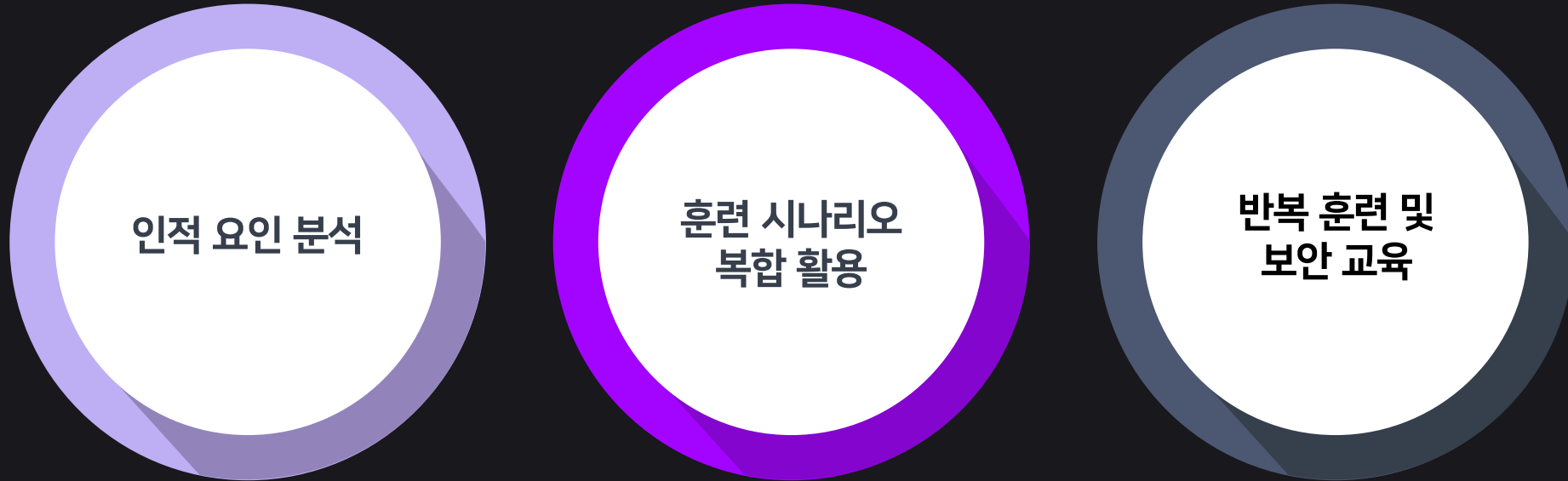
메일 수신

메일 열람

링크 접속 및
개인정보 입력

훈련 안내/메일 신고

악성메일 모의훈련 수행 전략



“ 악성메일 모의훈련 효과 증대 ”

[전략 1] 인적 요인 분석

임직원들에 대한 **인적 요인**을 분석·그룹핑하여 **맞춤 훈련 템플릿** 제작을 통한 **훈련 효과 증대**

인적 요인 분석

직군

직급

성별

연령

메일 테마 선정

경고 안내

이벤트 당첨

채용 공고

견적서

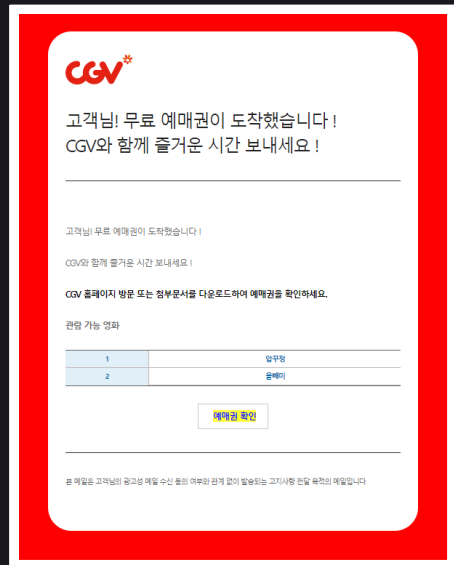
⋮

맞춤 훈련
템플릿 제작

[전략 2] 훈련 시나리오 복합 활용

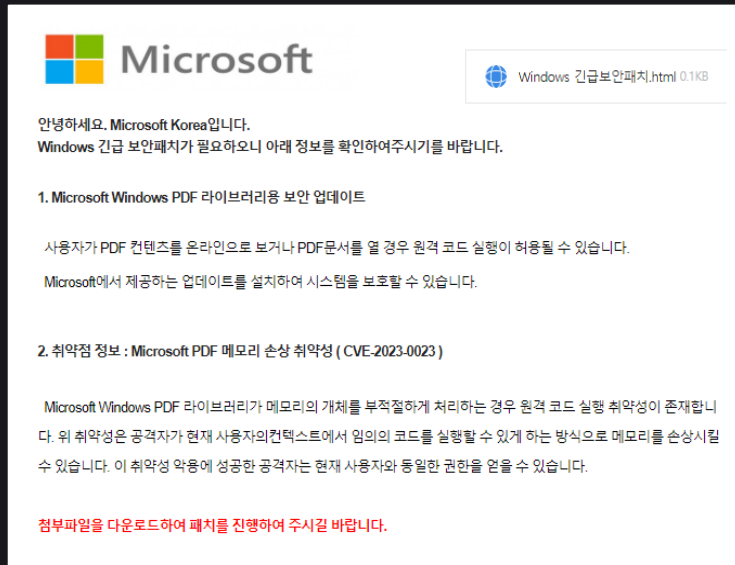
2개 이상의 훈련 시나리오를 활용하여 사내 정보 공유를 줄여 훈련 효과 증대

1



링크 접속 유도형

2



첨부파일 실행 유도형

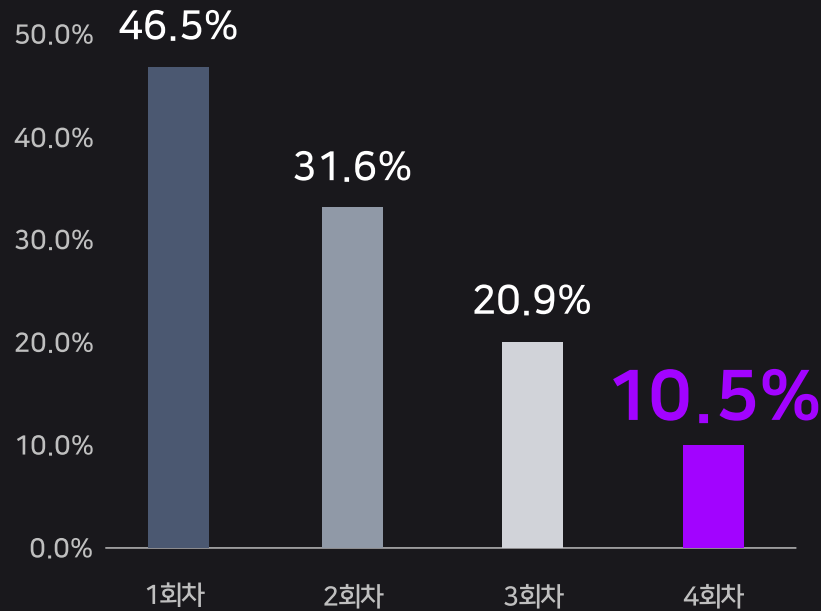
3



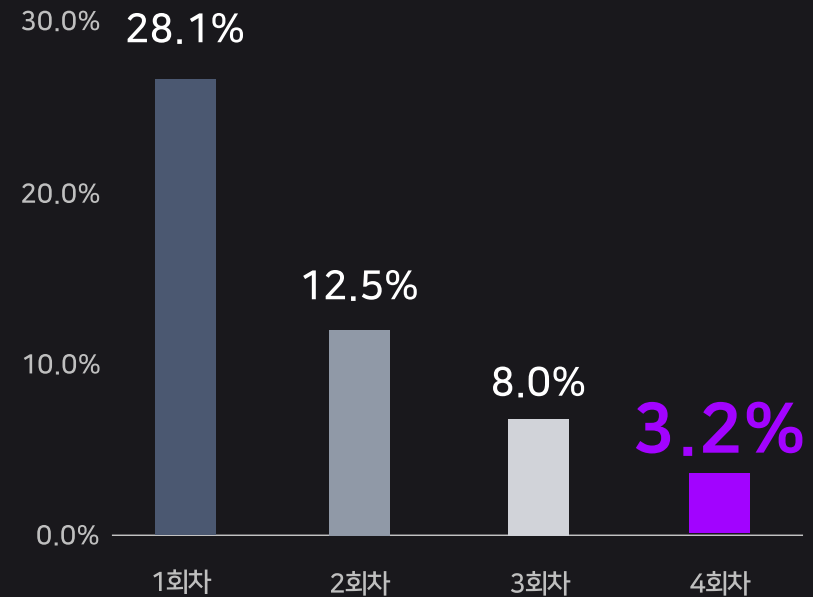
개인정보 입력 유도형

[전략 3] 반복 훈련 및 보안 교육

정기적인 반복 훈련 및 훈련 결과를 기반한 보안 교육을 통한 훈련 효과 증대



링크 접속률



첨부파일 실행율

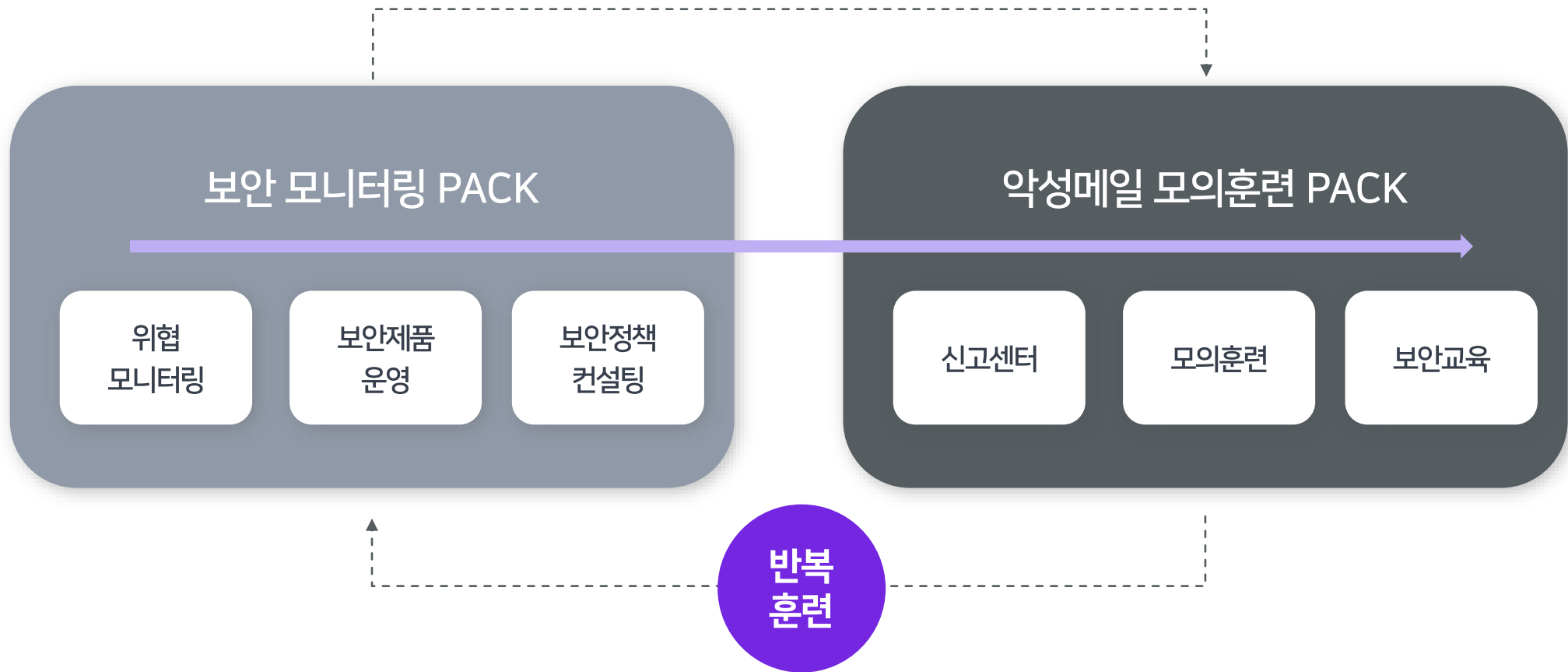
FAS00 악성메일 모의훈련 서비스



FAS00 Security Awareness Training

FASOO 매니지드 서비스

최고 기술력의 정보보안 매니지드 서비스 제공



G-PRIVACY 2023

2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

감사합니다.