사이버 보안 모의훈련 시스템

PHISHING SHIELD v1.0

WINCNS

MARVEL SYSTEM

Contents

WINCNS

MARVEL SYSTEM

사이버 침해사고 현황 및 대응방안

위협 동향

2021년 주요 보안위협 트렌드 톱5

[안랩]

2021년 주요 보안위협 트렌드 톱5

[이스트시큐리티]

2021년 주요 보안위협 트렌드 톱5

[이글루시큐리티]

사이버 침해사고 현황 및 대응방안

사이버 침해사고 현황

[KISA 2021년 사이버 위협 전망]

표적형 공격 랜섬웨어의 확산과 피해규모 증가

- 정부 및 기업 등 특정 대상을 표적한 공격
- 서비스 및 제조, 의료 등 다양한 산업 분야로 랜섬웨어 공격확대
- 내부 정보 유출부터 파일 암호화까지, 협박수단강화

고도화된 표적형 악성 이메일

- 맞춤형 악성 이메일과 대량 피싱이 결합한 매스피어링 등장
- Emotet 악성코드를 활용하여 스팸 메일 생성 및 배포 증가
- 유출된 기업 데이터에서 특정 대상의 전자 메일, 계약정보 등을 활용한 맞춤형 공격

코로나-19 사이버 공격 팬데믹

- 악성 웹사이트, 악성 첨부파일을 포함한 이메일 등으로 재택근무자 공격 증가
- 재택근무 증가로 엔드 포인트 장치에서의 기업 정보 유출 우려
- 취약한 VPN(가상사설망) 등 원격 네트워크 환경을 통한 기업 네트워크 침투시도

사이버 침해사고 현황 및 대응방안

사이버 침해사고 현황

2020년 대비 공격건수는 최소 102%이상 증가

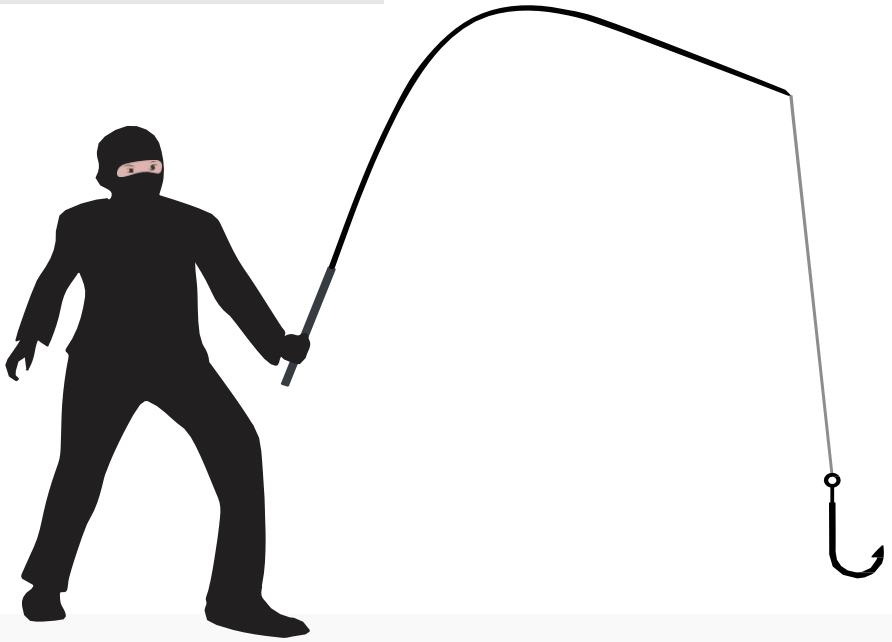
2020년 3분기부터 50%이상씩 공격횟수 증가

전세계 랜섬웨어 피해액 200억달러(22조원)을 넘을 것으로 예측

국내 랜섬웨어 피해 신고 3배 이상 증가

사이버 침해사고 현황 및 대응방안

피해 사례



글로벌 피해 현황

서비스 장애 및 중단

미국 IT 서비스 기업 카세야(Kaseya)가 랜섬웨어 공격으로 고객사 수백 개 기업의 서비스가 장애... 일부 기업은 비즈니스 중단 ...

기반 시설 피해

미국 최대 송유관 운영사 콜로니얼 파이프라인에 랜섬웨어 공격 ...휘발유 값이 7년 만에 최고수준... 국가 시설 공격 간주

막대한 비용 지출

세계 최대 육류 회사 JBS홀딩스 해킹 공격을 받고 1100만달러의 몸값을 지급

매스피어링(Masspearing)

스피어 피싱이 날로 정교해지고 있다. 최근에는 대상 맞춤 형태의 공격이 발생하고 있으며 맞춤형 공격은 더욱 발전할 것이다. 해커는 다크 웹이나 소셜 네트워크, 언론 등을 통해 특정 대상의 내부정보를 얻고 이를 활용하여 정밀하고 신뢰성 있는 공격을 진행한다. 또한 유출된 기업 재무, 계약정보를 통해 기업 거래처나 고객에게 대량으로 악성 메일을 발송하여 공격을 확대하고 있다. 이렇게 맞춤형 이메일과 대량 피싱이 결합된 매스피어링(Masspearing)이 등장했다. 여기에 Emotet 악성코드 공격이 증가 하면서 악성 메일 전파가 더욱 가속화되고 있다. Emotet 악성코드는 뱅킹 악성코드로 시스템에 설치된 이후 추가 모듈 또는 악성코드를 다운로드 시키는 트로이목마다. Emotet 악성코드를 첨부한 악성 메일을 보내고 감염된 계정의 주소록에 해당 계정으로 악성 메일을 보내 감염을 전파시키고 있다. 이러한 공격은 랜섬웨어 감염, 정보 유출 등 2차 공격의 기반이 되고 있어 더욱 주의가 당부 된다.

사이버 침해사고 현황 및 대응방안

규제 및 대응방안

-점검을 통해 공격 진행 단계를 탐지하여 선제적으로 무력화

- 점검포인트 : 시스템 관리자PC 악성코드 감염 여부, 주요 서버 비정상 접근시도 여부, 주요 서버 악성코드 설치 여부 등

점 검

- 점검단계에서 특이사항이 발견되면 단편적 조치가 아니라 후속대응이 매우 중요
- 침투경로와 해커의 활동 범위를 식별하여 조치

대 응

대 응

- 랜섬웨어 감염 사고를 가정하고 데이터 복구 훈련 실시
- 사업의 연속성을 저해할 수 있는 서비스 장애에 대한 고민과 준비
- 백업 데이터를 감염시킬 수 있는 경로 파악
- 사회공학적 기법을 이용해 점점 교묘해지는 랜섬웨어 공격에 대한 임직원 대응 교육
- 기본 정보보안인식 재고 및 사고대응절차 훈련

훈 련

▶ KISA에서 발표한 랜섬웨어 대응 핵심전략 3가지를 바탕으로 작성된 내용입니다.

사이버 침해사고 현황 및 대응방안

규제 및 대응방안

국정원	국가사이버안전관리규정 제9조의 2 사이버위기 대응훈련 국가 정보보안 기본지침 제 12조 모의훈련
과학기술정보통신부	제13조 민간분야 침해사고 모의훈련 계획 수립 및 실시에 관한 사항 제43조 모의훈련 계획 수립 및 실시
교육부	제10조 사이버분야 위기대응 훈련 계획의 수립·시행 제68조 훈련 계획 수립·시행
행정안전부	제27조 기술지원 및 모의훈련의 시행 제39조 사이버 침해사고 대응에 대한 기술지원 및 모의훈련의 수행
국민안전처	제9조 매년 정기 또는 수시 대응 모의훈련을 실시
외교부	제32조 사이버 위협으로부터 정보유출 예방을 위한 사이버보안 업무(신설 2015.11.06) 정보화 및 정보보안 교육(일부개정 2015.11.06)

사이버 침해사고 현황 및 대응방안

모의훈련의 필요성

사전예방 중심 정보보안 체계

사후에 발생하는 막대한 복구비용을 미연에 방지하기 위해
국가 정보보안 정책이 예방중심으로 변환됨

정보보호 교육 및 모의훈련

정보보안 보호지침을 준수하기 위한 교육 및 훈련 준수 근거
자료로서 가장 효율적인 모의훈련

전자우편 보안대책

해킹메일에 첨부된 피싱 사이트 및 악성코드에 대하여 보안
및 신고절차 수립 요구


사이버 보안 모의훈련 시스템
PHISHING SHIELD v1.0

개요

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

피싱쉴드(PHISHING SHIELD : 사이버 위기대응 모의훈련 시스템)는 악의적인 목적을 가진 이메일로 부터 피해가 발생하지 않도록 이메일 이용에 대한 경각심 제고와 보안 인식을 향상 시키기 위한 악성 이메일 모의훈련용 솔루션입니다.

피싱쉴드
Phishing Shield

피싱쉴드는 다양한 형태의 악의적인 공격으로부터 임직원과 개인의 피해를 줄여줄 수 있는 기본적인 방패입니다.

구분	권장 사양
CPU	Quad Core 2.5GH 이상
Memory	8GB이상
HDD	SATA 300G 이상
OS/DBMS	Linux or Windows / MySQL
비고	어플라이언스 제품으로 제공 가능

구성

임직원들을 대상으로 실제 악성메일과 유사한 '모의 악성 이메일' 을 발송한 후 대응결과를 수집하여 평가하고 위반된 임직원은 보안교육을 통해 보안 인식을 향상 시킬 수 있는 모의훈련을 반복합니다.

훈련대상 선정

훈련대상자/기간/훈련 컨텐츠 선정

메일발송

발송

훈련대응

대응 결과 수집

훈련결과

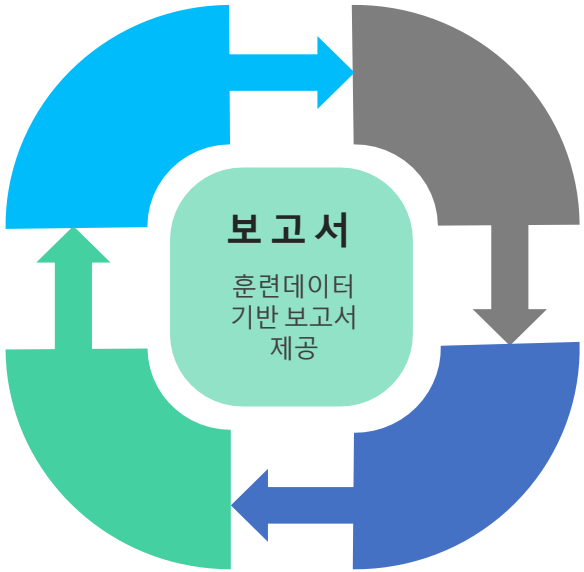
결과 리포트

프로세스

전반적인 훈련계획 설정에 따라 훈련 발송 및 확인, 수집 정보의 분석 결과, 자동화된 보고서까지 완전한 프로세스를 제공합니다.

훈련계획

전체 훈련일정 설정 훈련 대상자 설정 훈련 컨텐츠 설정
컨텐츠에 따른 회치 설정



훈련실시

계획된 내용에 따른 훈련 메일 발송
발송 상태 확인
컨텐츠에 따른 회 차별 훈련 확인

보안교육

시험지, 보안교육 콘텐츠교육 참여
평가관리

훈련결과수집

훈련 결과 확인
개인/조직 등 그룹별 행위 분석 컨텐츠 및 훈련환경 별 행위 분석

주요기능

유형별 훈련관리, 유연한 대상자 관리, 다양한 컨텐츠 사용, 다각화된 결과보고 등 악성 이메일 위협에 대응할 수 있는 모의훈련에 필요한 모든 기능을 보유하고 있습니다.

훈련관리

전체 훈련 관리(대시보드)
개별 훈련 회치 관리
훈련 목적,기간, 공지, 교육 등
단계별 훈련관리 기능
즉시발송, 예약발송 설정

훈련대상자관리

엑셀 일괄 업로드
개별 대상자 등록
훈련 이력관리

교육,훈련,컨텐츠관리

웹 에디터 형식 컨텐츠 편집
기능 제공
최신 악성 이메일 트렌드 적용
후속조치 대상자 교육 공지 안내
교육 결과 평가기능

결과관리

다양한 검색 필터 지원
누적 통계 확인
훈련부터 교육까지 전체 과정의
종합 상세 결과 엑셀 리포트 제공
한글, PDF, PPT등 다양한
포맷의 리포트 출력가능(옵션)

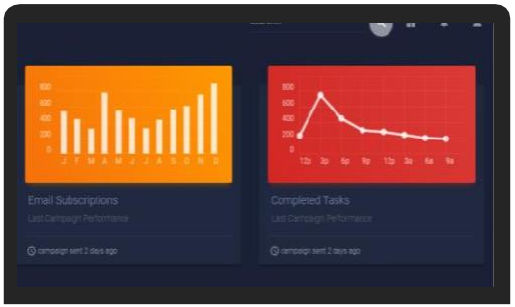
유형별훈련관리 | 유연한대상자관리 | 다양한컨텐츠관리 | 다각화된결과보고

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

메인 대시보드 : 메인 대시보드를 통해 전체 모의훈련의 결과 및 진행사항을 한눈에 볼 수 있습니다

- 실시간 진행 상황 파악
- 전체 훈련 통계 및 차트확인
- 팀별/그룹별 등 지수화 된 내용 한눈에 파악 가능

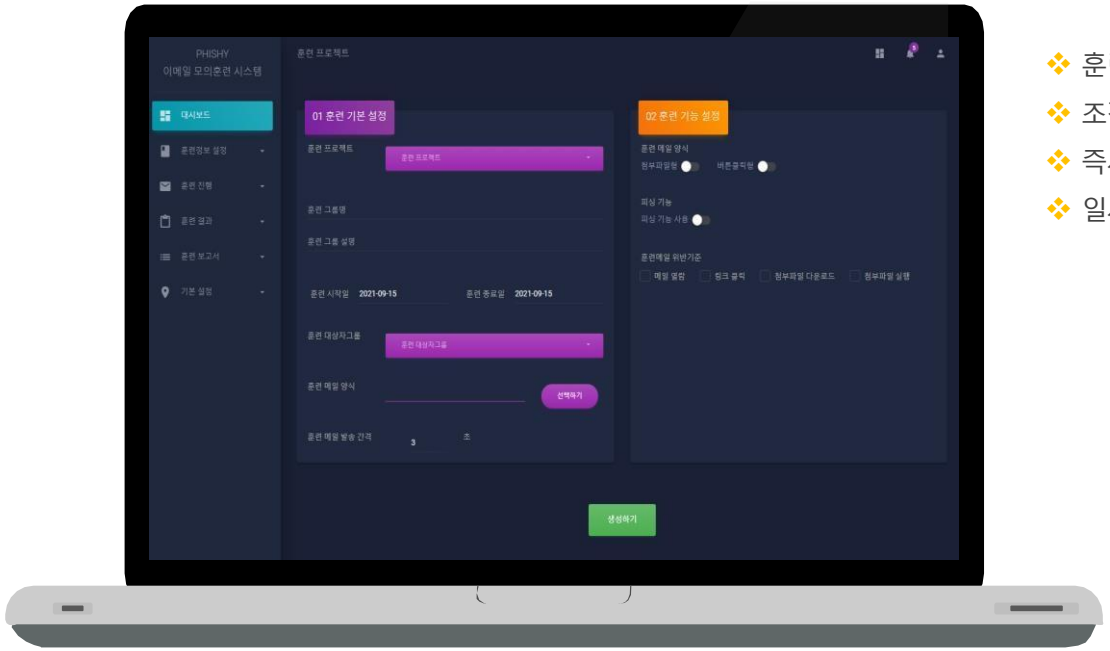


▲메인 대시보드 예시

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

훈련그룹 관리 : 훈련명 및 훈련 기간, 발송 기간 및 발송 시간대 등의 설정이 가능하며, 훈련 대상별 다양한 컨텐츠를 활용한 훈련 설정이 가능합니다.



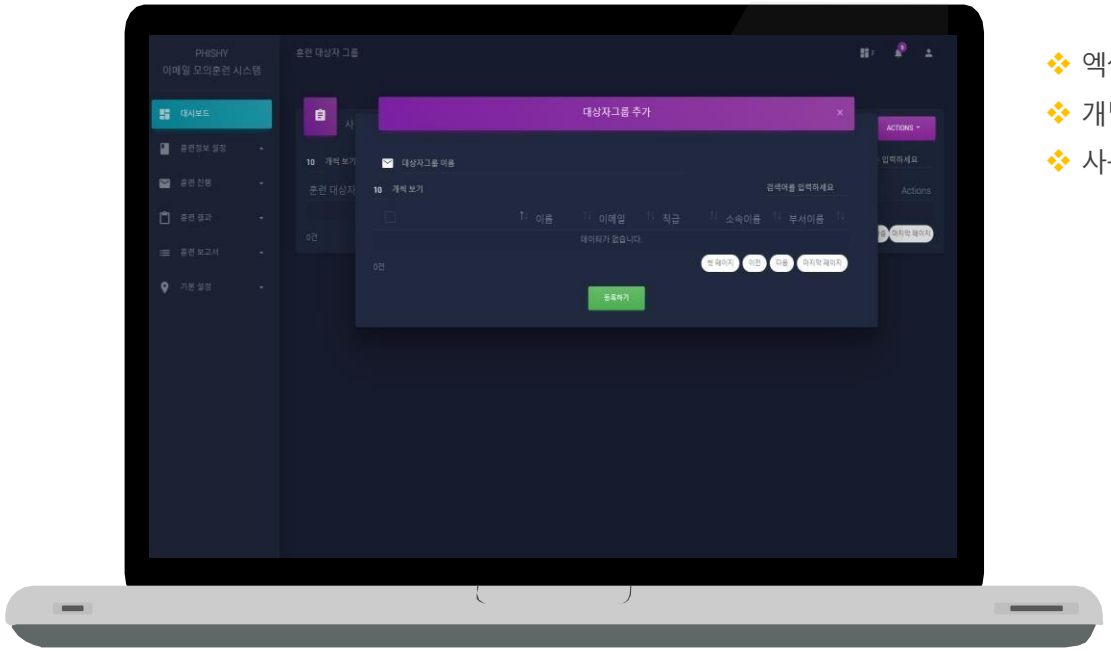
- 훈련목적, 기간, 사전공지, 보안교육 등 단계별 훈련 시나리오 관리
- 조직별, 사용자별 다양한 훈련 유형 선택 가능
- 즉시발송, 예약발송 선택
- 일시정지 등 발송관련 내용 확인 및

▲훈련그룹예시

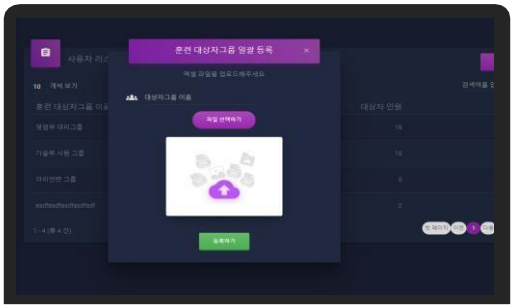
주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

훈련 대상자 관리 : 엑셀파일로 훈련대상자를 편리하게 업로드할 수 있는 기능과 사용자 정의 태그 기능을 사용하여 유연하게 훈련 대상자를 선정할 수 있습니다.



- 엑셀 일괄 업로드 기능 지원
- 개별 사용자, 조직, 훈련 대상자 설정
- 사용자 정의 태그 기능 활용

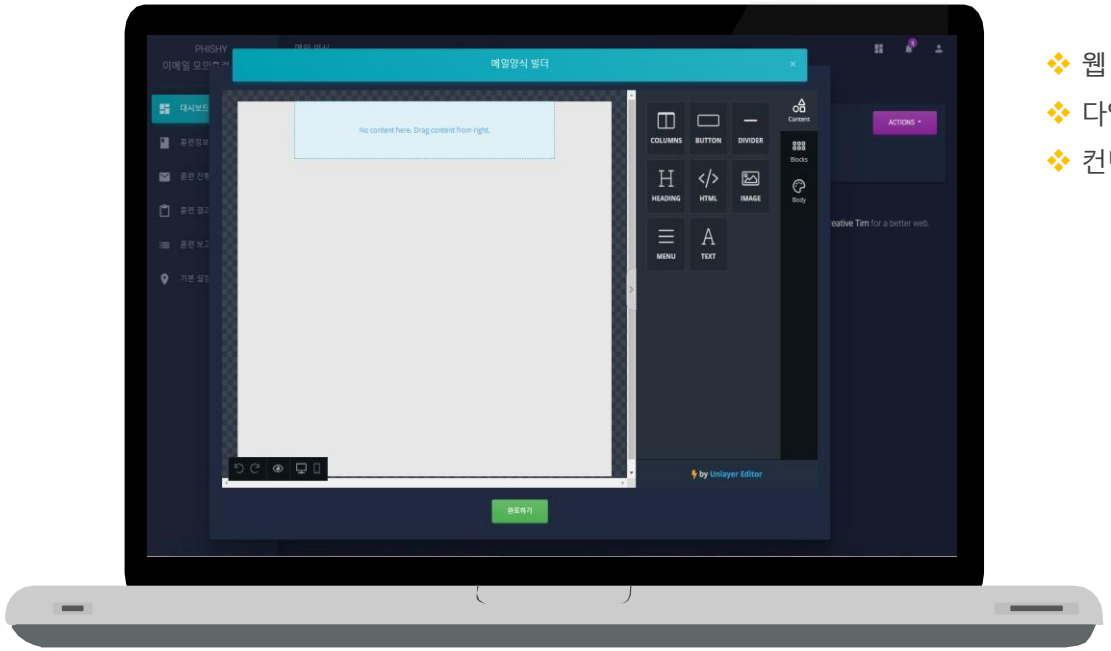


▲훈련대상자 일괄 등록 기능 예시

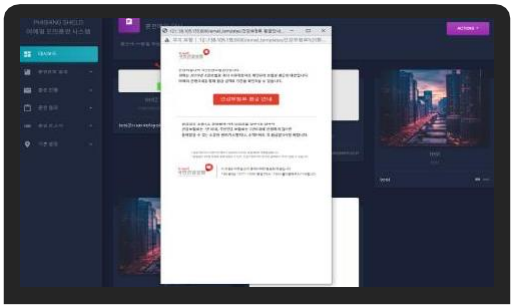
주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

훈련 컨텐츠 관리 : 웹 에디터 형태의 훈련 컨텐츠 셀프 제작이 가능합니다. 다양한 형태의 컨텐츠(HTML)를 업로드하여 사용 가능하며, 다양한 컨텐츠별 훈련 대상자 설정이가능합니다.



- 웹 에디터 형태의 훈련 컨텐츠 셀프제작
- 다양한 형태의 컨텐츠(HTML)을 업로드하여 사용 가능
- 컨텐츠별 훈련 대상자 설정

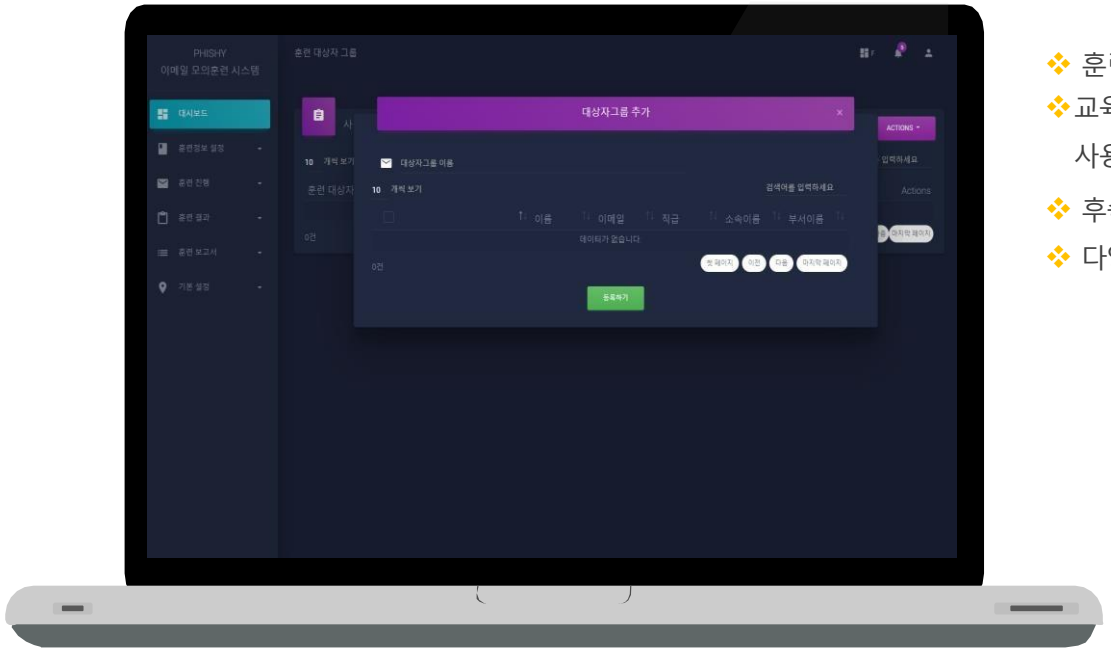


▲훈련 컨텐츠 샘플 관리

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

교육 관리 : 후속조치 대상자를 기준으로 교육 안내 및 교육 콘텐츠 제공이 가능합니다.



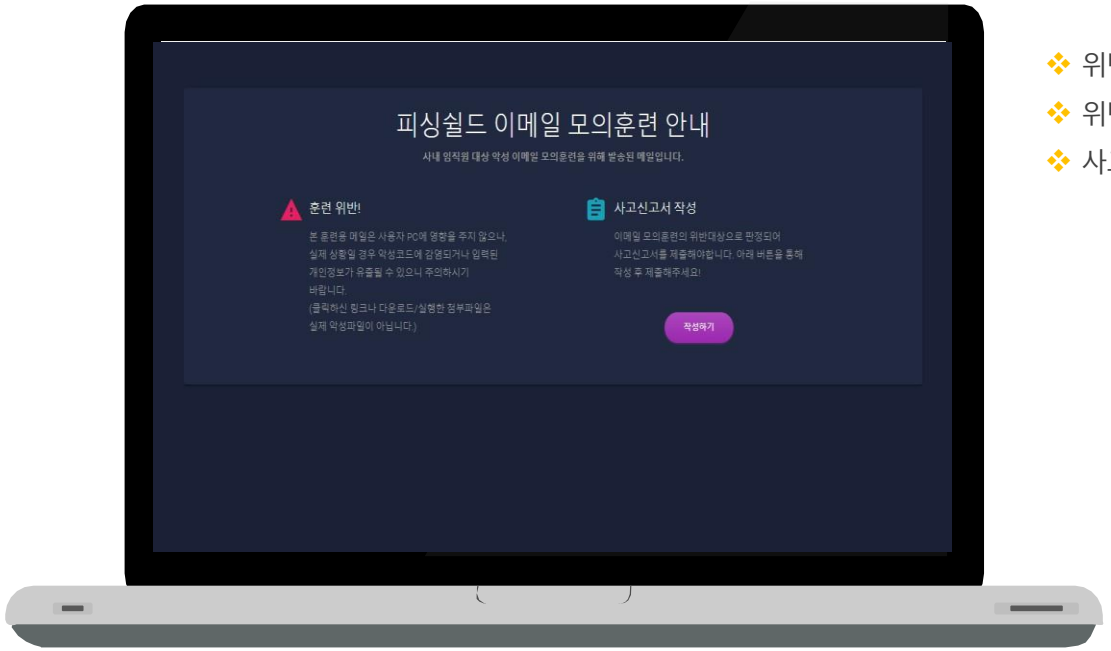
- 훈련 대상자별 교육훈련, 상태, 점수, 배점 등 평가정보 제공
- 교육훈련자에게 훈련 메일을 발송하여 교육 참여를 유도하고 교육 미 참여 사용자를 실시간으로 확인
- 후속조치 필요 대상에게 교육참가 안내메일 발송
- 다양한 교육 컨텐츠 제공(유료)

▲보안 교육 컨텐츠 제안 예시

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

신고 관리 : 훈련용 메일에 대한 신고기능을 제공하며 사고 신고서 기능을 통해 대상자 리스트 확보 및 신고 정보에 대한 확인이 가능합니다.



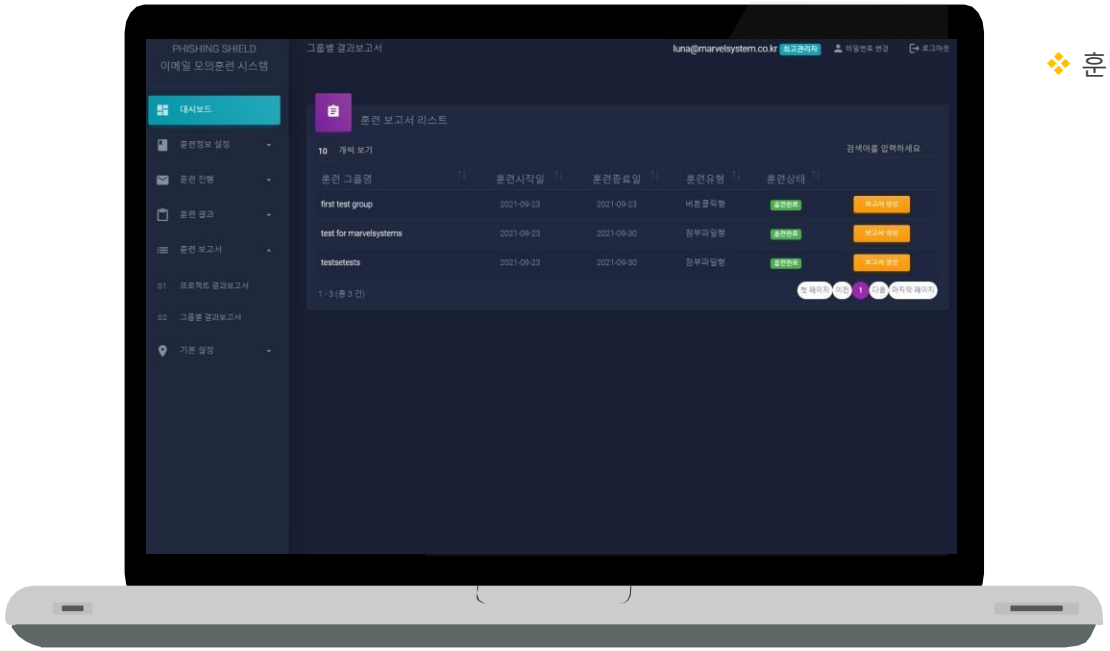
- 위반자 기준 훈련 위반 안내메시지 제공
- 위반자 사고신고서 안내 및 작성
- 사고신고서 등록 결과 및 내역 관리

▲보안 교육 컨텐츠 제안 예시

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

결과 관리 : 다양한 통계 정보를 이용해 훈련 결과에 대한 Excel 형태의 보고서를 제공합니다.



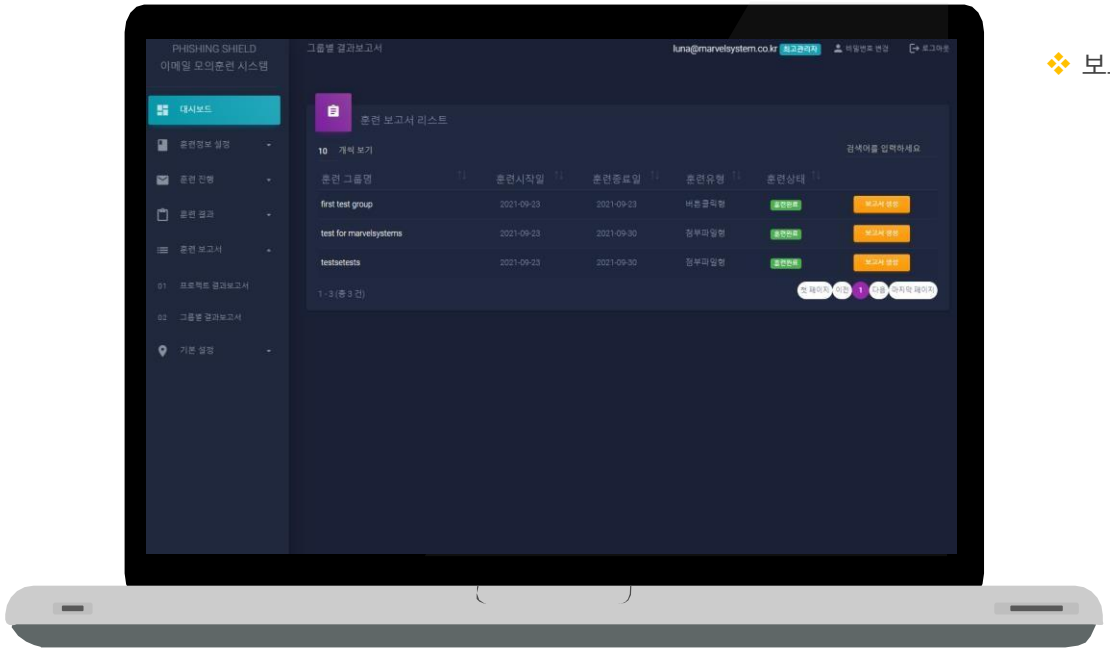
❖ 훈련 종합 상세결과를 바탕으로 자동화 된 리포트 지원(EXCEL)

▲훈련 결과 EXCEL 리포트 예시

주요기능

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

결과 관리 : 한글, PPTX, PDF, 점자 리포트 등 다양한 형태의 보고서 커스터마이징이 가능합니다.(옵션)



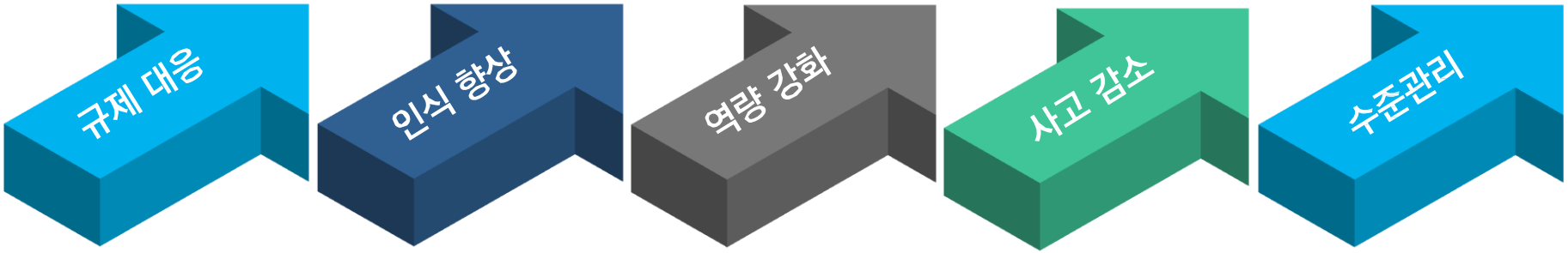
❖ 보고서 전문 제품과 협업을 통한 다양한 보고서 커스터마이징 기능 제공

▲표준 리포팅 솔루션 CLIP report

기대효과

피싱쉴드 (PHISHING SHIELD : 사이버 보안 모의훈련 시스템)

피싱쉴드를 통해 당장 직면한 규제대응부터 실제 악성 이메일을 통한 보안사고감소 효과를 기대할 수 있습니다. 또한 임직원 보안수준관리 및 역량을 강화로 전반적인 전사 보안수준을 향상시킬 수 있습니다.



법/ 규제대응

법, 규제 내용의 모의훈련, 전자우편 대책 등에 대한 대응 가능

보안인식향상

훈련과 다양한 교육 활동을 통해 정보보안 인식 향상

보안위협대응역량강화

모의훈련 및 사고 신고훈련 등을 통해 사이버 보안위협 대응 역량을 강화

실제 사고감소

보안인식 향상 및 역량강화를 통해 실제 사고 감소 기대 및 위협 신고율 향상

임직원보안수준관리

지속적인 훈련과 교육지수 관리를 통해 보안수준 관리 및 사전 예방대책 수립

라이선스형태

구축형(납품형)

Appliance 납품형(H/W+S/W) Software 납품형(S/W)

서비스형

클라우드 서비스를 활용한 1회성 훈련
분기별,반기별 연간 구독 훈련 서비스

BASIC
PS_1000 : 1000USER

ENTERPRISE
PS_3000 : 3000USER

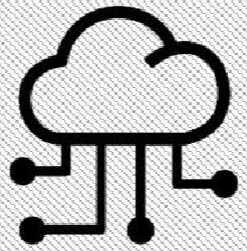
OPTION
PS_USER_추가 USER
PS_REPORT_추가리포트모듈

구축형(납품형)

단일고객사 기준 일반적인 납품형 모델 그룹관리 및 권한분리로 고객사 최적화

서비스형

보안 클라우드 서비스를 이용한 1회성 악성메일모의훈련



SERVICE
PSSV_200 : 200USER

ENTERPRISE
PSSV_1000 : 1000USER

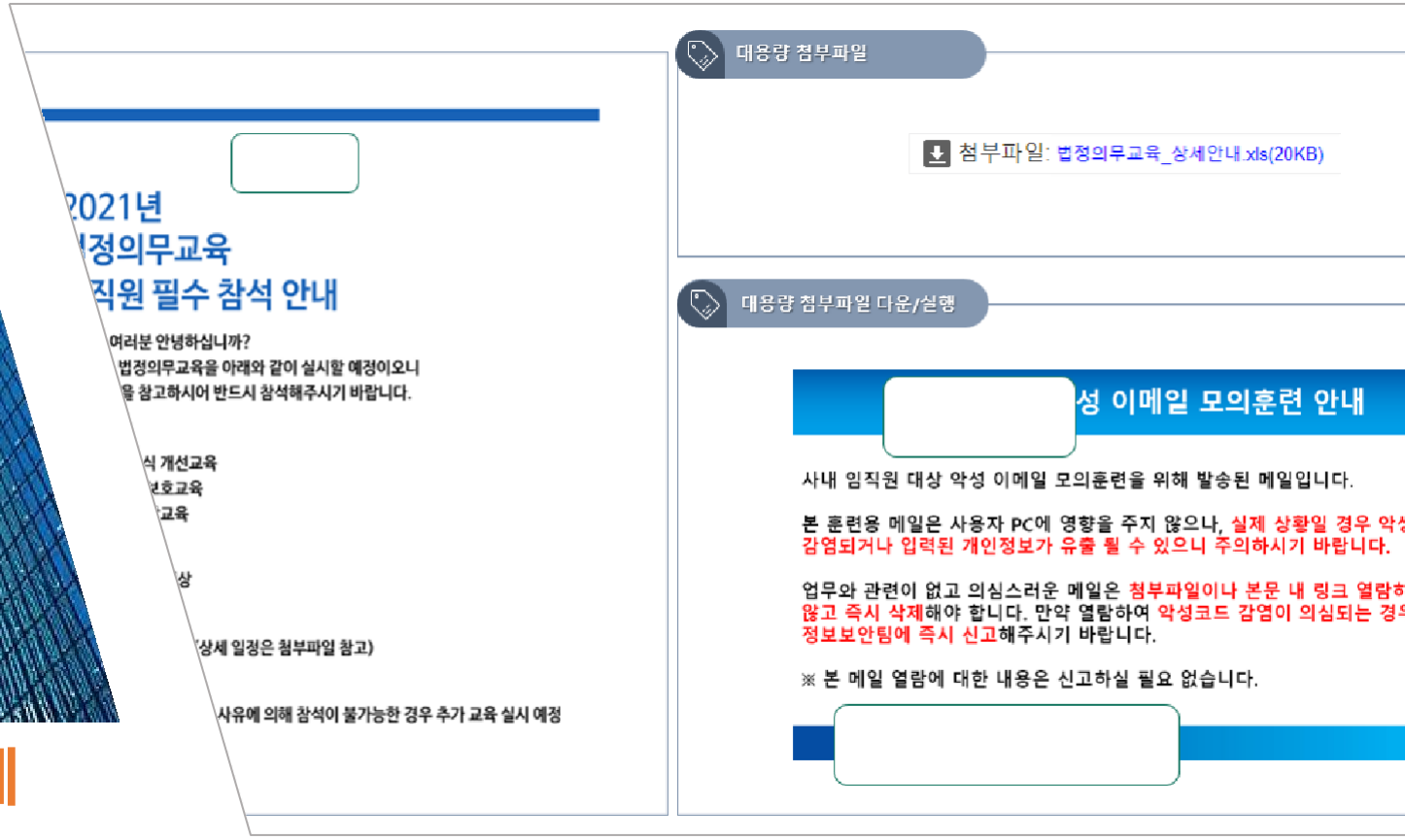
OPTION
PS_USER_추가 USER
PS_CONTENT_추가콘텐츠

훈련사례

Y금융사

- 훈련 대상자 : 1600명
- 훈련 템플릿 : 버튼(링크) 클릭형, 개인정보 입력형, 첨부파일형(파일 다운로드 및 실행)
- 훈련 특징 : 고품질의 양식사용으로 위기대응모의훈련의 강도가 높은 편이며, 사후 교육을 통해 보안의식 고취 (매년 정기 진행)

▼실제 훈련 양식 예



감사합니다

제품소개 및 데모 시연 문의

주식회사 윈씨엔에스 기술영업부 : 김 영 균 부장

담당 직통 : 010-8929-7637

이메일 : sales@wincns.co.kr

서울시 금천구 가산디지털2로 169-16, 914호(가산동, 하우스디가산퍼스타)