SNI system

PHISHING SHIELD v1.0

“사이버 보안 모의훈련 시스템”제안

전자우편을 통한 랜섬웨어 감염 등의 악성코드 피해를 예방하고 정보보안 의식 향상을 위해 ‘사이버 보안 모의훈련 시스템-피싱쉴드‘ 를 제안합니다.



SNI system

Contents

01 사이버 침해사고 현황 및 대응방안

- 사이버 침해사고 현황 및 위협 전망
- 모의훈련의 필요성

02 사이버 보안 모의훈련 시스템“ PHISHING SHIELD”

- PHISHING SHIELD 소개
- 프로세스, 주요 기능
- 핵심 포인트 1,2,3,4,5
- 기대효과

03 기타사항

- 기능요건
- 교육사항
- 지원사항
- 고객사례

사이버 침해사고 현황 및 위협 전망 #1

2020년 대비 공격건수는 최소 102%이상 증가

2020년 3분기부터 50% 이상씩 공격 횟수 증가

전세계 랜섬웨어 피해액 200억달러(22조원)을 넘을 것으로 예측

국내 랜섬웨어 피해 신고 3배 이상 증가



[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 공격 확대
▶ 내부 정보 유출부터 파일 암호화까지, 협박수단 강화

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 침투 시도

사이버 침해사고 현황 및 위협 전망 #2

■ 2023년 상반기 국내 과학기술정보통신부(한국인터넷진흥원) 침해사고 신고 건수

[출처 : 2024년 하반기 사이버 위협 동향보고서 (KISA)]

[단위 : 건수]

구분 \ 연도	2021년		2022년		2023년	
	상반기	하반기	상반기	하반기	상반기	하반기
건수	298	342	473	669	664	613
합계	640		1,142		1,277	

■ 2023년 상반기 국내 과기정통부(한국인터넷진흥원) 침해사고 유형별 현황

[단위 : 건수]

구분 \ 연도		2022 (상반기)	비율	2022 (하반기)	비율	2023 (상반기)	비율	2023 (하반기)	비율
침해사고 신고	DDoS 공격	48	10.1%	74	11.1%	124	18.7%	89	14.5%
	악성코드	125	26.4%	222	33.2%	156	23.5%	144	23.5%
	(랜섬웨어)	(118)	(24.9%)	(207)	(30.9%)	(134)	(20.2%)	(124)	(20.2%)
	서버 해킹	275	58.1%	310	46.3%	320	48.2%	263	42.9%
	기타	25	5.3%	63	9.4%	64	9.6%	117	19.1%
합 계		473		669		664		613	

* 악성코드 감염의 90% 이상 랜섬웨어

* 기타 : 직원 문자 및 메일을 통한 개인, 경영정보 유출 건수

여전히 침해사고 유형 중 **악성코드(랜섬웨어)**의 비율이 높음

사이버 침해사고 현황 및 위협 전망 #3

해킹그룹	발생월	사칭메일내용	주요Target	피해내용
Kimsuky(북한)	05월	북한정책관련기자, 학계인사 등 사칭	북한정권 관련자	PC내 외교전략 및 북한 관련 정보수집
미상	05월	KISA 스팸 대응센터 사칭	불특정 다수 개인	악성코드 설치 후 내부 침투 경로로 활용
미상	04월	채용사이트(리멤버) 포인트 적립 위장	불특정 다수 개인	악성코드 설치 후 내부 침투 경로로 활용
미상	04월	금융위원회, 네이버관리자 사칭	불특정 다수 개인	네이버/카카오 계정정보 탈취
미상	03월	한국무역협회 사칭	불특정 다수 개인	악성코드 설치 후 내부 침투 경로로 활용
APT43(북한)	02월	북한관련 연구 분야 소속 전문가로 위장	대북 안보 관련 기관 & 전문가	PC내 외교전략 및 북한 관련 정보 수집
미상	02월	가비아 서비스 연장 결제 요청 위장	불특정 다수	네이버/카카오 계정정보 탈취
북한 해커그룹 추정	02월	신년인사 '남북미 정상에게 드리는 메시지' 로 위장	북한 관련 인사	악성코드 설치 후 내부 침투 경로로 활용
미상	01월	화물 통관 서류 제출 위장	불특정 다수 개인	DHL계정정보 탈취
미상	01월	'전자세금계산서 발급 및 세무조사 출석요구' 안내 위장	불특정 다수	네이버/카카오 계정정보 탈취
미상	01월	네이버 마이박스 서비스 위장	불특정 다수	네이버/카카오 계정정보 탈취

사이버 침해사고 현황 및 위협 전망 #4

※ 최신위협

→ 국정원을 사칭하여 유포중인 이메일!(2024년 5월)

2024-05-02 (목) 오전 3:37
국가정보원(한국) [redacted]
경찰 보고서
받는 사람 [redacted]
메시지 국가정보원(한국).pdf

안녕하세요

첨부 파일은 경찰 보고서입니다. 첨부파일을 읽어보시고 즉시 회신해 주시기 바랍니다.

조태용

국가정보원 원장

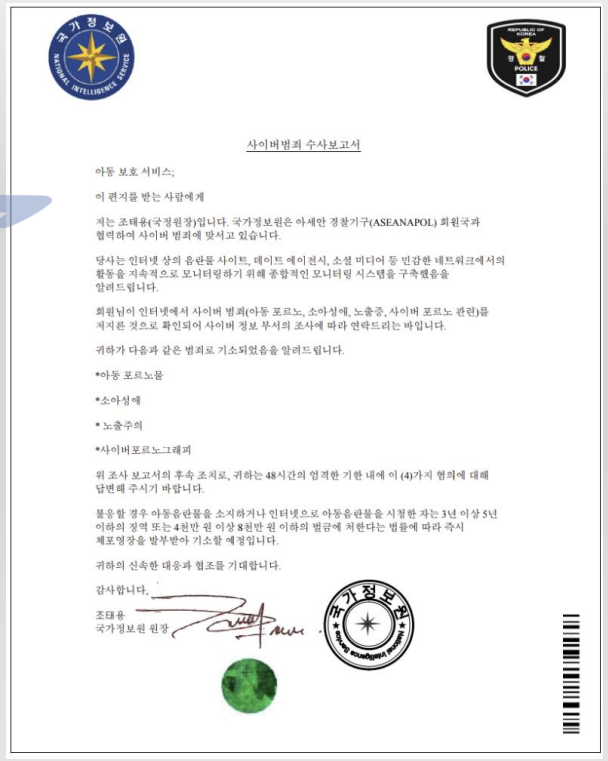
2024-05-15 (수) 오전 8:32
국가정보원(한국) [redacted]
경찰 보고서
받는 사람 [redacted]
숨은 참조
메시지 국가정보원(한국).pdf (587 KB)

안녕하세요

첨부 파일은 경찰 보고서입니다. 첨부파일을 읽어보시고 즉시 회신해 주시기 바랍니다.

조태용

국가정보원 원장



사이버범죄 수사보고서

아동 보호 서비스;

이 편지를 받는 사람에게

저는 조태용(국정원장)입니다. 국가정보원은 아세안 경찰기구(ASEANAPOL) 회원국과 협력하여 사이버 범죄에 맞서고 있습니다.

당사는 인터넷 상의 음란물 사이트, 데이트 에이전시, 소셜 미디어 등 민감한 네트워크에서의 활동을 지속적으로 모니터링하기 위해 종합적인 모니터링 시스템을 구축했음을 알려드립니다.

회원님이 인터넷에서 사이버 범죄(아동 포르노, 소아성애, 노출증, 사이버 포르노 관련)를 저지른 것으로 확인되어 사이버 정보 부서의 조사에 따라 연락드리는 바입니다.

귀하가 다음과 같은 범죄로 기소되었음을 알려드립니다.

*아동 포르노물

*소아성애

* 노출주의

*사이버포르노그래피

위 조사 보고서의 후속 조치로, 귀하는 48시간의 업격한 기한 내에 이 (4)가지 혐의에 대해 답변해 주시기 바랍니다.

불응할 경우 아동음란물을 소지하거나 인터넷으로 아동음란물을 시청한 자는 3년 이상 5년 이하의 징역 또는 4천만 원 이상 8천만 원 이하의 벌금에 처한다는 법률에 따라 즉시 체포영장을 발부받아 기소할 예정입니다.

귀하의 신속한 대응과 협조를 기대합니다.

감사합니다.

조태용
국가정보원 원장

[국정원 사칭하여 첨부파일 경찰보고서 확인 유도! → 메일 수신자 위협!]

모의훈련의 필요성

사전예방 중심 정보보안 체계

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

정보보호교육 및 모의훈련

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

전자우편 보안대책

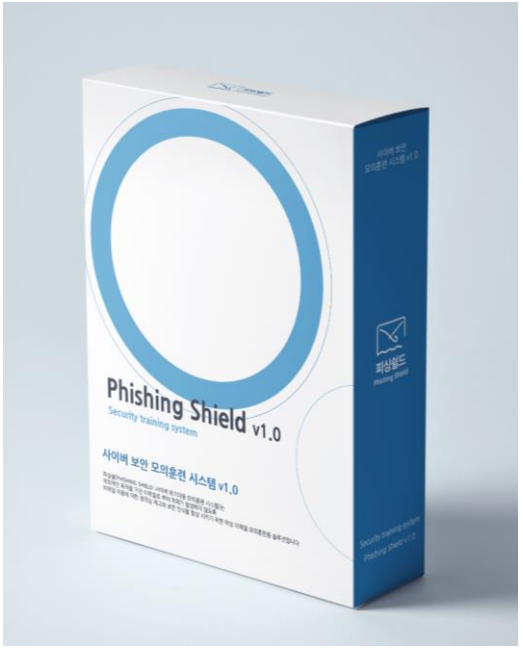
해킹메일에 첨부된 피싱 사이트 및 악성코드에 대하여 보안 및 신고절차 수립 요구



피싱쉴드 (PHISHING SHIELD)

사이버 보안 모의훈련 시스템

피싱쉴드(Phishing Shield)는 임직원들을 대상으로 실제 악성 메일과 유사한 '모의 악성 이메일'을 발송한 후 대응 결과를 수집하여 평가하고 보안교육을 통해 위반한 임직원의 보안 인식을 향상 시키기 위한 솔루션입니다.



◆ 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

프로세스

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
컨텐츠 교육 참여
평가관리

훈련결과 수집

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

전반적인 훈련계획 설정에 따라 훈련 발송 및 확인, 수집 정보의 분석 결과, 자동화된 보고서까지 완전한 프로세스 제공

주요기능

"매스피어링"과 같은 악성메일과 유사한 훈련용 이메일을 발송하여 임직원의 정보보안 의식을 향상시키고 보안수준 향상을 통해 정보 유출과 같은 피해 예방을 지원합니다.

훈련 관리

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

훈련 대상자 관리

엑셀 일괄 업로드
개별 대상자 등록
훈련 이력관리

교육,훈련,컨텐츠 관리

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

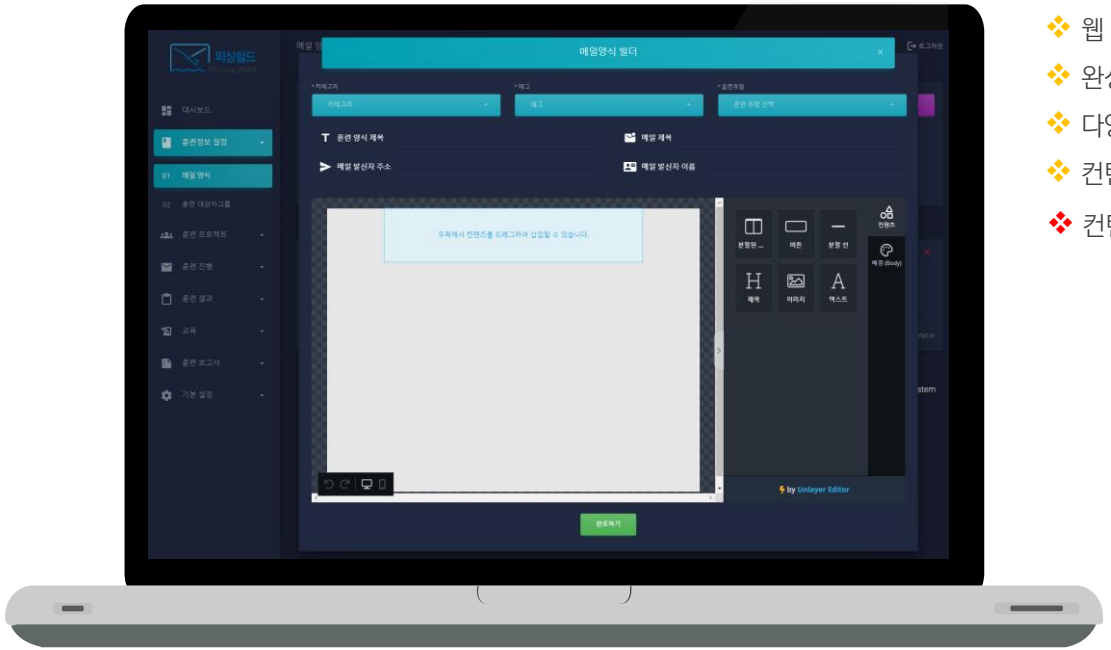
결과 관리

다양한 검색 필터 지원
누적 통계 확인
훈련부터 교육까지 전체 과정의 종합 상세 결과 엑셀 리포트 제공
다양한 포맷의 리포트 출력 가능-*옵션 (한글/PDF/PPT 등)

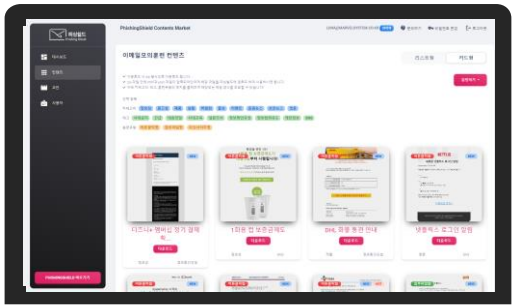
POINT #1

훈련 컨텐츠

컨텐츠 게시판 지원(피싱쉴드 컨텐츠 마켓)을 통해 언제든지 다양한 최신 훈련 시나리오를 지원 받으실 수 있습니다.



- 웹 에디터 형태의 훈련 컨텐츠 셀프 제작
- 완성된 훈련 컨텐츠의 손쉬운 수정 작성
- 다양한 형태의 컨텐츠(HTML)을 업로드하여 사용 가능
- 컨텐츠별 훈련 대상자 설정
- 컨텐츠 게시판 지원을 통한 최신 트렌드 컨텐츠 적용



▲ 훈련 컨텐츠의 자유로운 다운로드

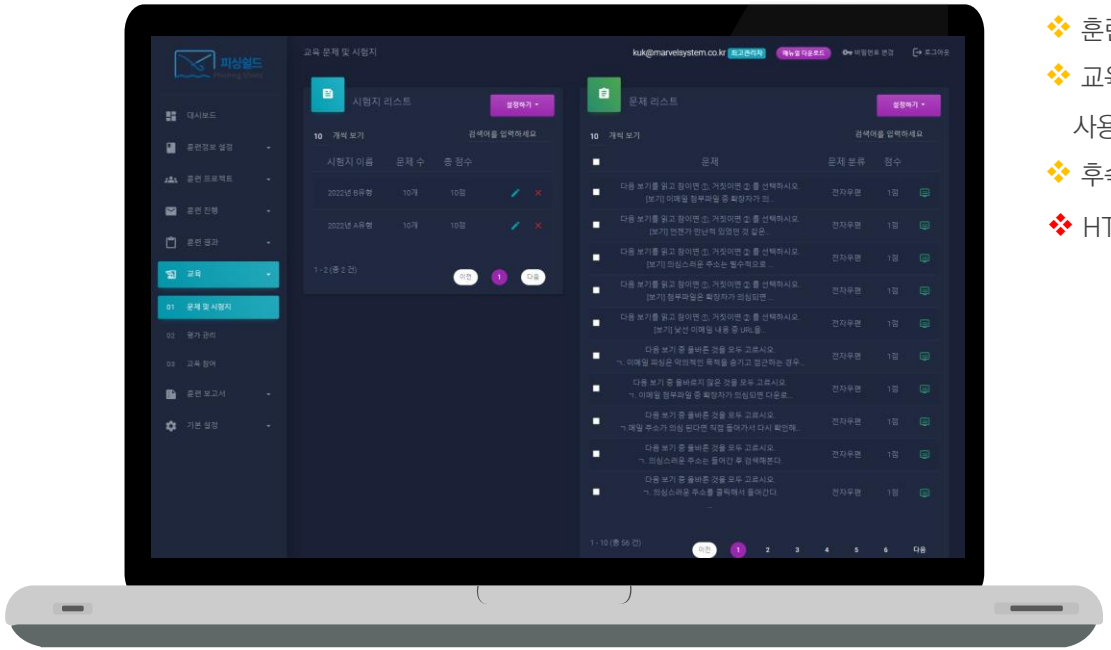
훈련 시나리오는 상시 70~100여개를 유지하며, 모두 최신 트렌드를 반영하고 있습니다. (반기 기준 컨텐츠는 50%이상 변경/수정)

원하시는 시나리오가 없으실 경우 당사 Tech팀으로 시나리오 샘플을 전달해주시면 마켓을 통한 익일 지원이 가능합니다.

POINT #2

교육 관리

후속조치 대상자 및 전체 훈련대상자를 기준으로 보안 교육 교안을 제공하고, 교육을 지원합니다.



- 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
- HTML형태의 참여형 보안인식교육 교안 제공

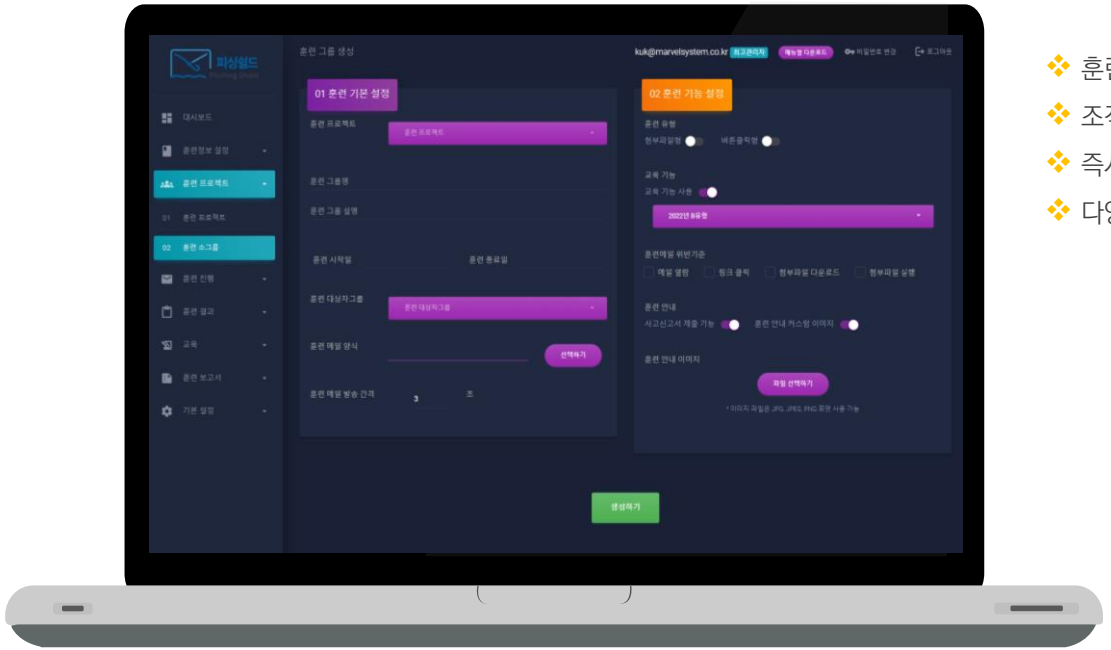


▲ 보안 교육 컨텐츠 제안 예시

POINT #3

계획 실행

다양한 옵션을 한 화면에서 설정하고, 훈련 일정에 맞추어 훈련을 자동으로 실행, 수집할 수 있습니다.



- 훈련목적, 기간, 사전공지, 보안교육 등 단계별 훈련 시나리오 관리
- 조직별, 사용자별 다양한 훈련 유형 선택 가능
- 즉시발송, 예약발송 선택
- 다양한 훈련관련 설정을 한 화면에서 설정

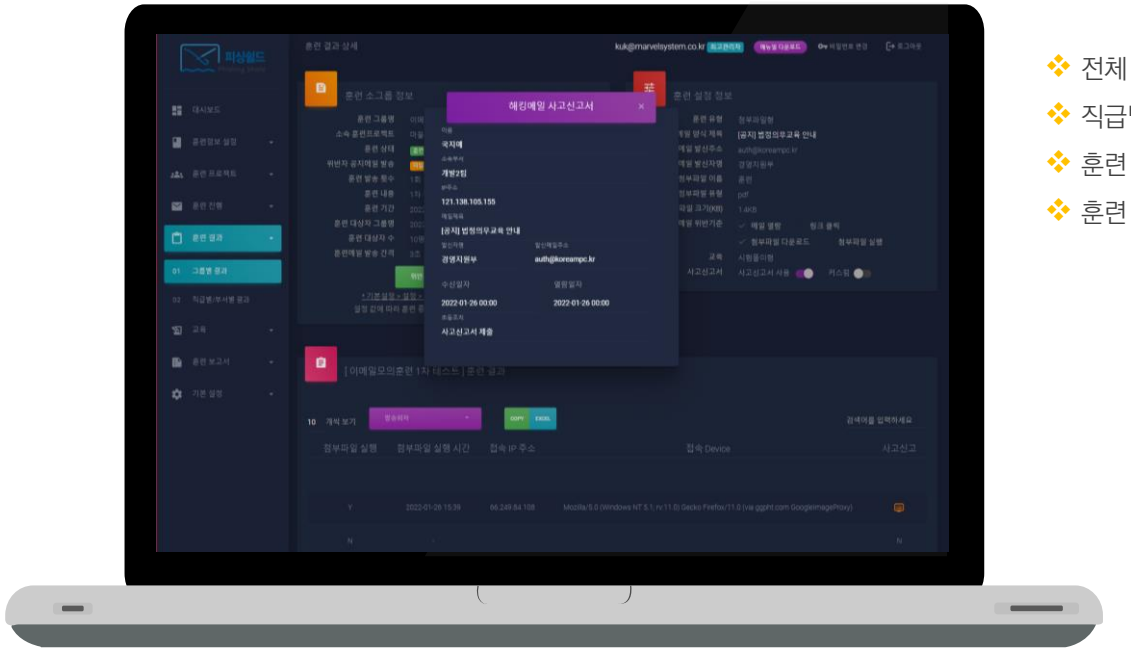


▲ 훈련 그룹 예시

POINT #4

결과 관리

그룹별, 직급별, 부서별, 개인별 상세 결과를 조회 할 수 있습니다.
또한 다양한 통계 정보를 이용해 훈련 결과에 대한 자동 보고서를 제공합니다.



- 전체 프로젝트 내 소그룹별 상세 결과 조회
- 직급별, 부서별, 개인별 상세 결과 조회
- 훈련 결과 상세 차트 및 리스트 시각화 제공
- 훈련 종합 상세결과를 바탕으로 자동화 된 리포트 지원(EXCEL, PPTX)

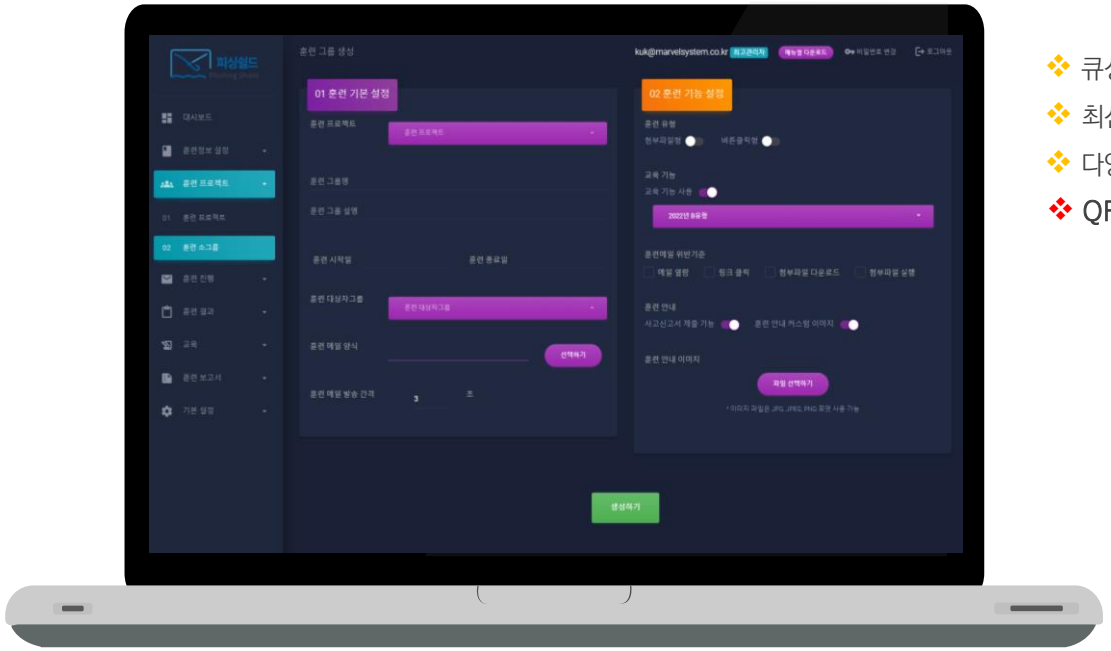


▲ 훈련 결과 리포트 예시

POINT #5

훈련의 다양성

최신 공격 위협과 관련한 훈련 설정 및 다양한 훈련 세팅 옵션을 통해 적용할 수 있습니다.



- 큐싱(Qshing) 위협이 높아짐에 따라 새로운 형태의 QR코드 훈련 유형 제공
- 최신 공격 유형에 맞춘 다양한 훈련 형태를 적극적으로 기능 수용
- 다양한 훈련 셋팅을 수용할 수 있도록 유연하게 설계
- **QR코드 공격 유형까지 총 4가지 유형의 훈련 시나리오를 다양하게 제공**



▲ QR유형 훈련 예시

기대효과



법/규제 대응

법, 규제 내용의 모의훈련, 전자우편 대책 등에 대한 대응 가능



인식 및 역량 강화

훈련과 교육을 통한 정보보안 인식 향상과 위협대응 역량 강화



정보보안 사고감소

임직원 의식 향상을 통한 실제 사고 감소 기대 및 위협 신고율 향상



수준 관리

지속적인 훈련과 교육지수 관리를 통한 보안수준 관리 및 사전 대책 수립

반복적이고 **지속적인** 훈련과 교육으로 보안 인식을 **강화**하는 것이 가장 중요합니다



감사합니다