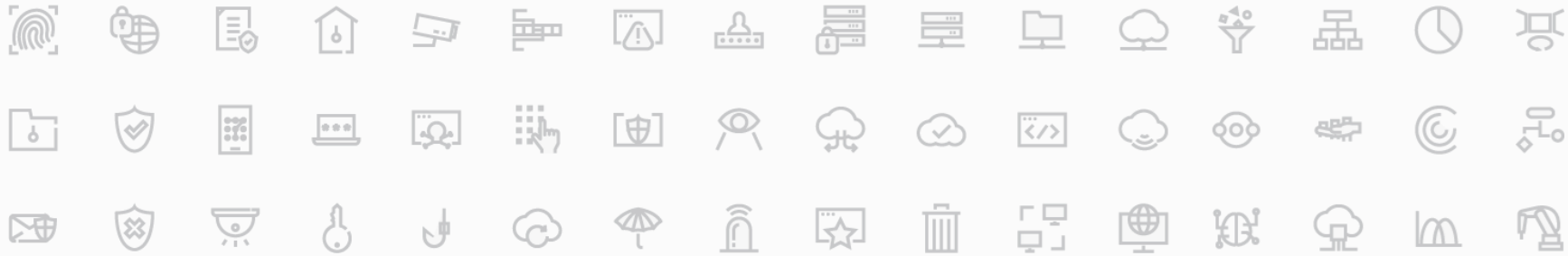
2025

정보보안패키지 서비스

소개자료



KOVA (사) 벤처기업협회

SK shieldus

Global Leading Digital Security Company

Contents

KOVA (사) 벤처기업협회

SK shieldus

I. 정보보안패키지 서비스

01 MDR 서비스

02 ETP 서비스

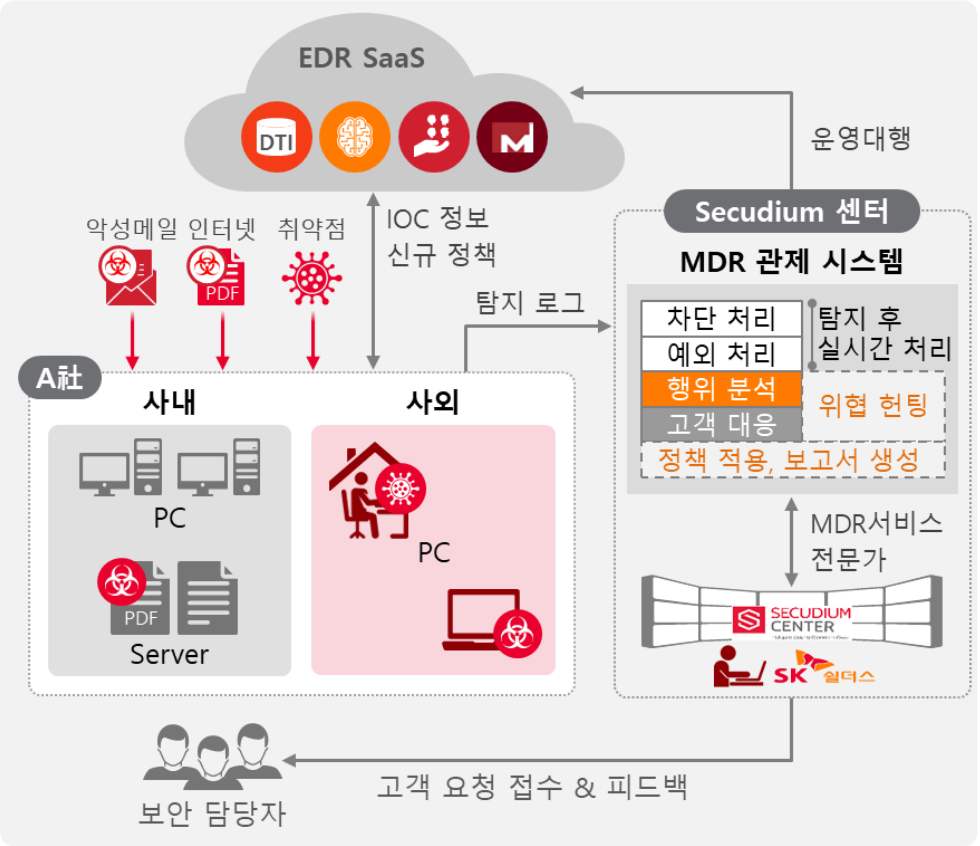
03 사이버가드 서비스

01 MDR 서비스(엔드포인트 위협 탐지 서비스)

PC / 서버 해킹 및 랜섬웨어 방지

MDR 서비스 개요

EDR 보안 구성



EDR 솔루션

Global TOP EDR 솔루션 사용

구분	세부 내용
평판	• "Global T.I" 기반 평판 DB 사용
행위	• 행위 기반 탐지 엔진 - Exploit Guard를 통한 행위 분석 수행 • 신종 공격 탐지 머신런닝 엔진 (Malware Guard)
백신	• 알려진 위협 대응 AV엔진으로 탐지/차단 (Malware Protection)
위협 정보	• 제조사 IoC 및 정책 실시간 반영 • 자체 분석 결과 정책 업데이트 - SK-Defined Rules, IoC를 통한 신속 대응

SK 쉴더스 보안 서비스

MDR 서비스로 공격에 대한 가시성 확보
- 구체적인 행위 파악 및 추가 공격 행위 조사
- 자체 분석 결과를 통한 대응 및 위협 헌팅

운영 대행 및 전문 지원 서비스
- EDR 전문가의 빠르고 정확한 운영 대행
- 이상징후 사후 분석 지원 (침해사고 조사 결과 반영)
- SOC관제 서비스와 연동하여 24 x 7 대응 지원

MDR 서비스 상세 내용

위협 헌팅 서비스

시스템 내부에 침투한 위협을 식별 및 제거하여 피해를 예방하고 보안을 강화
한국 침해사고 IoC 및 자체 수집 정보를 활용 주기적으로 위협 헌팅을 수행

운영 대행 및 정책 설정 서비스

보안 전문가 서비스로 고객사 환경에
최적화하여 운영 관리 대행 서비스

위협 제거 서비스

Agent 설치 이후 Full Scan을 통해
잔존 위협 제거 수행

위협 분석 대응 서비스

고객 요청으로 의심파일에 분석 후
추가 조치 및 대응 방안 제공 서비스

MDR 서비스

침해 흔적 조사 서비스

과거 침해 흔적 및 잔존 위협 조사
신규 IoC, IoA 와 위협 헌팅으로 침해흔적 조사 수행

위협 IoC 정보 제공 서비스

침해사고 및 위협에서 추출한 IOC를 통해,
이기종 보안 장비에서 대응 가능하도록 정보를 제공

침해진단 서비스(ASM)

외부에 노출된 자산을 파악하고 공격자 관점에
서 해킹 포인트를 확인하여 보안강화 방안제공
주간 보고서 제공, 매주 이행점검 수행

긴급 대응 서비스

이상행위 탐지 시 구체적인 행위를 분석하여 위협 경로, 유형, 내부 확산 여부등의 영향도를 파악
프로세스 종료 및 네트워크 차단 등 긴급 조치 수행하고 대응 방안을 제공하는 서비스

SK쉴더스 MDR Service 3가지 특장점

서비스 내용

01 EDR 전문가 운영 대행

Managed

- 24 X 7 관제 요청 접수 및 대응
- IoC 및 SK-Defined Rules 업데이트
- 정책 운영 및 예외처리 반영
- 이벤트 분석 & 대응 조치

02 SK쉴더스 상세 분석 서비스

Detection

- EDR/악성코드 전문가 분석 서비스
- EDR 기능을 통한 악성행위 추적 지원
- 상세분석을 통한 정/오탐 대응
- 주기적 위협헌팅 수행

03 침해사고 관점 통찰력

Response

- 국내 최다 침해사고 분석 및 조사 노하우 적용
- 침해 흔적 점검 진행
- 국내 침해지표(IoC) EDR 우선 적용

EDR 전문가 관제서비스

✓ **EDR 전문 관제 서비스**
- 다수 고객사 서비스 제공 중
- 다양한 산업군별 레퍼런스로 고객 요청 대응 가능

✓ **사용자 만족도 향상**
- 숙련된 운영 전문가 신속한 대응

전문가 서비스 활용

✓ **TOP-CERT 활용 가능**
- 24X7 긴급 로컬 투입
- 국내 최다 사고분석 및 조사 대응

✓ **SK쉴더스 보안 전문가 서비스 활용 가능**
- 분석 전문가 상시 대응
- 보안 전문가 분석 서비스 (악성코드분석가 + CERT)
- 전담 조직 체제로 정확/신속 서비스

국내 최대 보안 수준 대응

✓ **서비스 통한 정보유출 불가**
- 첨부파일 자사 망내 분석
- 당사 전용 분석 환경 보유

✓ **사전 보안위협 대응역량 강화**
- 고객 보안 부서와 협업 위협 확산 선 차단 가능

MDR 서비스 방향성 및 목표

서비스 진행 방향

	도입 2개월		도입 5개월
위협 대응	Full Scan를 통해 잔존 위협 제거 (Cleaning Work)	오탐 및 과탐 최소화	탐지 이벤트 수량 최소화
정책 고도화	침해사고 IoC, IoA 적용	SK쉴더스 Define Rule 적용	위협헌팅, 위협 리서치를 통한 위협 식별
서비스 안정화	보안 및 3rd Party 어플리케이션 예외처리		Host별 운영 정책 설정

- 위협 대응
  - 기존 위협을 제거하고 새롭게 침투하는 이벤트에 신속대응하기 위한 절차
  - 오탐 및 과탐으로 인한 정탐 이벤트 분석 방해 요소 최소화
- 정책 고도화
  - 순차적으로 룰을 적용하며, 주기적으로 위협 헌팅을 수행
  - 한국 기업을 대상으로 공격하는 공격자 위협 파악 및 대응
- 서비스 안정화
  - 예외처리 통한 리소스 사용량 최소화
  - 보안 어플리케이션에 발생하는 충돌 예방

탐지된 위협에 최적화된 대응 체계 구축

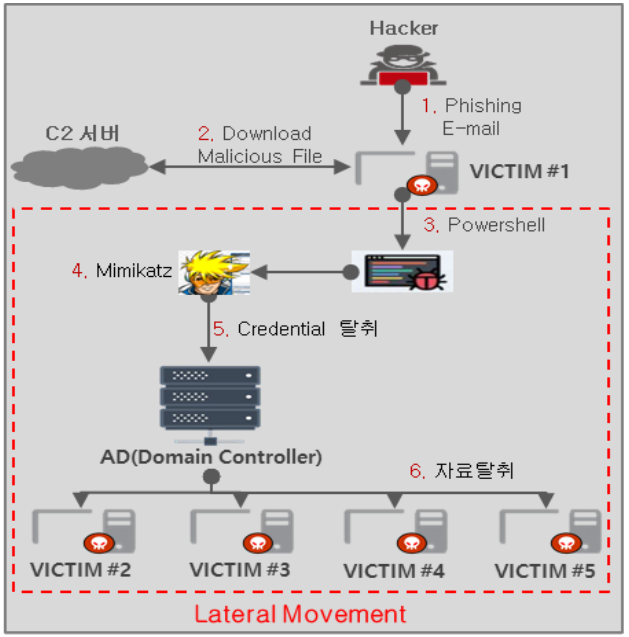
MDR서비스 목표

1. 실시간 위협으로 탐지된 이벤트에 집중
2. 지속적인 정책 고도화를 통한 탐지 성능 향상
3. 서비스 안정성 최우선

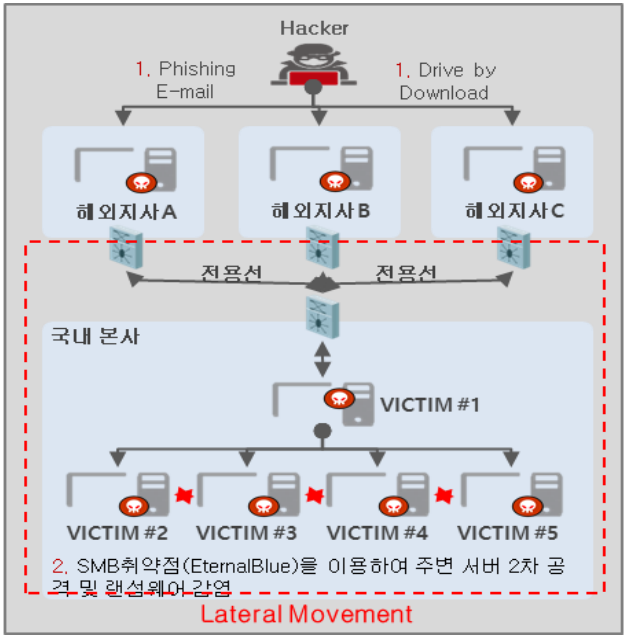
침해사고 관점 대응 서비스(해킹 및 랜섬웨어 방지)

국내 최다 침해사고 분석 및 조사 노하우로 신속/정확한 판단 및 대응

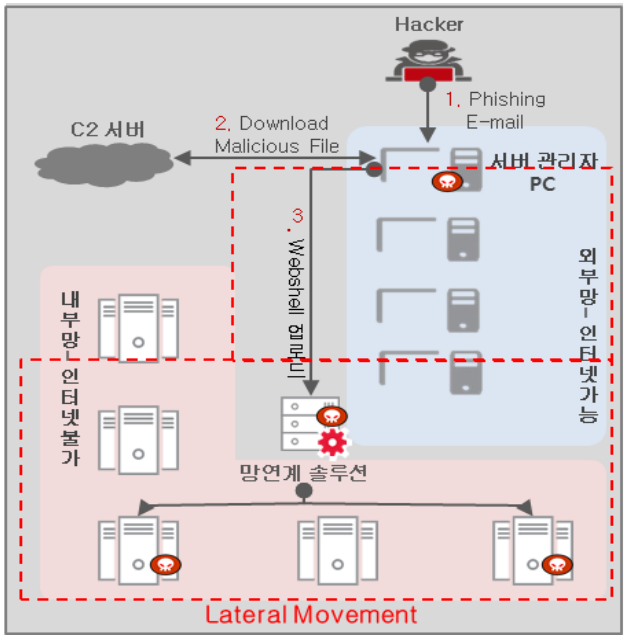
Phase I (AD탈취를 통한 자료 유출사건)



Phase II (해외지사를 이용한 랜섬웨어 감염사건)



Phase III (망연계 솔루션 취약점을 통한 유출사건)



탐지 포인트

- PC를 통한 초기 접근(Initial Access – E-mail)
- AD 계정 탈취(Credential Access – Mimikatz)
- PC/서버간 공격자 행위 (Lateral Movement – 탈취 계정 이용)

- PC를 통한 초기 접근(Initial Access – E-mail, Web)
- SMB 취약점을 통한 권한 탈취 (Execution - Exploitation of Remote Services)
- PC/서버간 공격자 행위 (L/M – SMB 취약점 이용)

- PC를 통한 초기 접근(Initial Access – E-mail, Web)
- 내부 망 연결 서버 권한 탈취(Execution – Webshell)
- PC/서버간 공격자 행위 (Lateral Movement, Credential Access – Mimikatz)

▷해커가 사용하는 주요 명령어 및 툴에 대한 주기적 위협헌팅 수행 ▷▶국내 최근 침해사고 결과 반영 침해흔적 조사

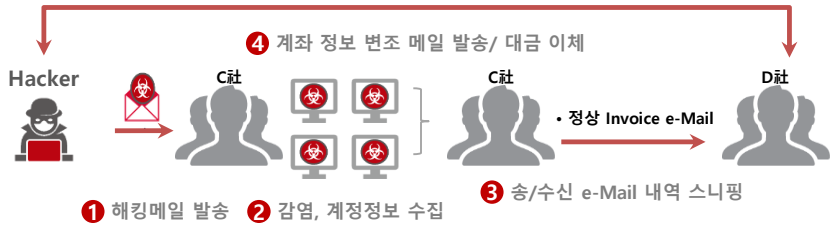
02 ETP 서비스(지능형 공격 탐지 서비스)

E-Mail 해킹 및 스팸/피싱 방지

01 서비스 도입 배경

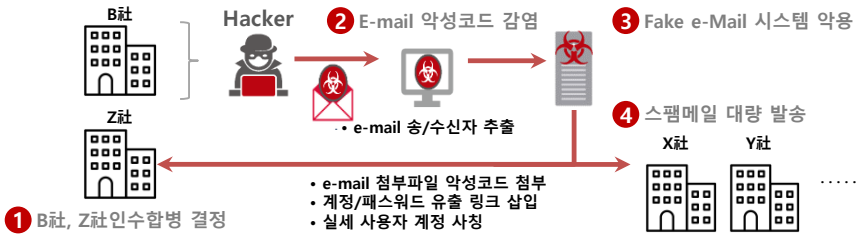
"해킹 92%가 이메일 통한 공격... 공격 성공률 60%이상!!!

01 ('21.9) C社 사례 — "해외 무역 거래 사기 사건"



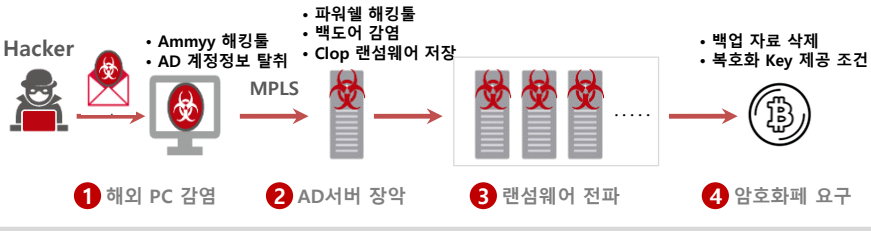
취약점	• 최초 e-Mail 악성코드 유입 미탐지 • 외부 e-Mail 2-factor 인증 부재로 접근 가능 • 계좌 정보 추가(유선, Fax) 확인 없이 대금 송금
피해 규모	• 242억 대금 해커에게 송금, 금전적 손실 발생 • 대외 회사 이미지 실추, 대금 송금 관련 법적 소송
사고 통계	▪ 최근 5년간 2,582건,약 1379억 금전 손실 지속

02 ('20.4) B社 사례 — "B社 Spam Mail 대량 발송 사건"



취약점	• 최초 e-Mail 악성코드 유입 미탐지 • 외부 e-Mail 2-factor 인증 부재로 접근 가능 • 계좌 정보 추가(유선, Fax) 확인 없이 대금 송금
피해 규모	• 242억 대금 해커에게 송금, 금전적 손실 발생 • 대외 회사 이미지 실추, 대금 송금 관련 법적 소송
사고 통계	▪ 최근 5년간 2,582건,약 1379억 금전 손실 지속

03 ('19.7) A社 사례 — "Clop 랜섬웨어 감염 사건"



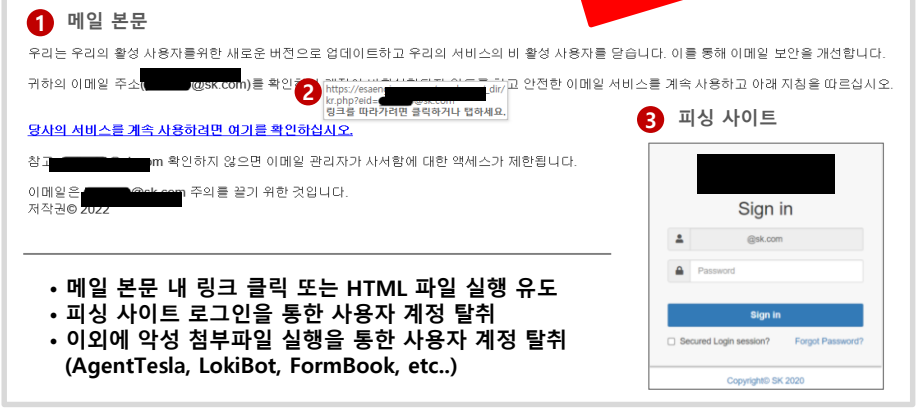
취약점	• 최초 e-Mail 악성코드 유입 미탐지 • 외부 e-Mail 2-factor 인증 부재로 접근 가능 • 계좌 정보 추가(유선, Fax) 확인 없이 대금 송금
피해 규모	• 242억 대금 해커에게 송금, 금전적 손실 발생 • 대외 회사 이미지 실추, 대금 송금 관련 법적 소송
사고 통계	▪ 최근 5년간 2,582건,약 1379억 금전 손실 지속

01 서비스 도입 배경

이메일 해킹 사고 위험

최근 삼성/LG 해킹사고 원인!!!

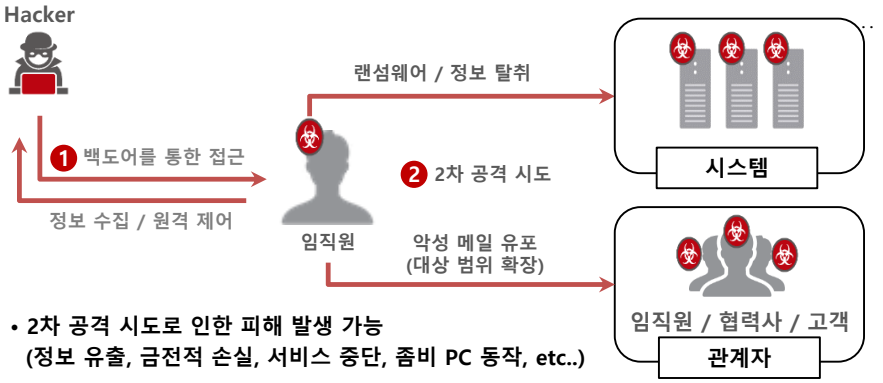
01 메일 계정 탈취 공격



- 메일 본문 내 링크 클릭 또는 HTML 파일 실행 유도
- 피싱 사이트 로그인을 통한 사용자 계정 탈취
- 이외에 악성 첨부파일 실행을 통한 사용자 계정 탈취 (AgentTesla, LokiBot, FormBook, etc..)

02 악성 메일 유포

03 2차 공격 시도



- 2차 공격 시도로 인한 피해 발생 가능 (정보 유출, 금전적 손실, 서비스 중단, 좀비 PC 동작, etc..)

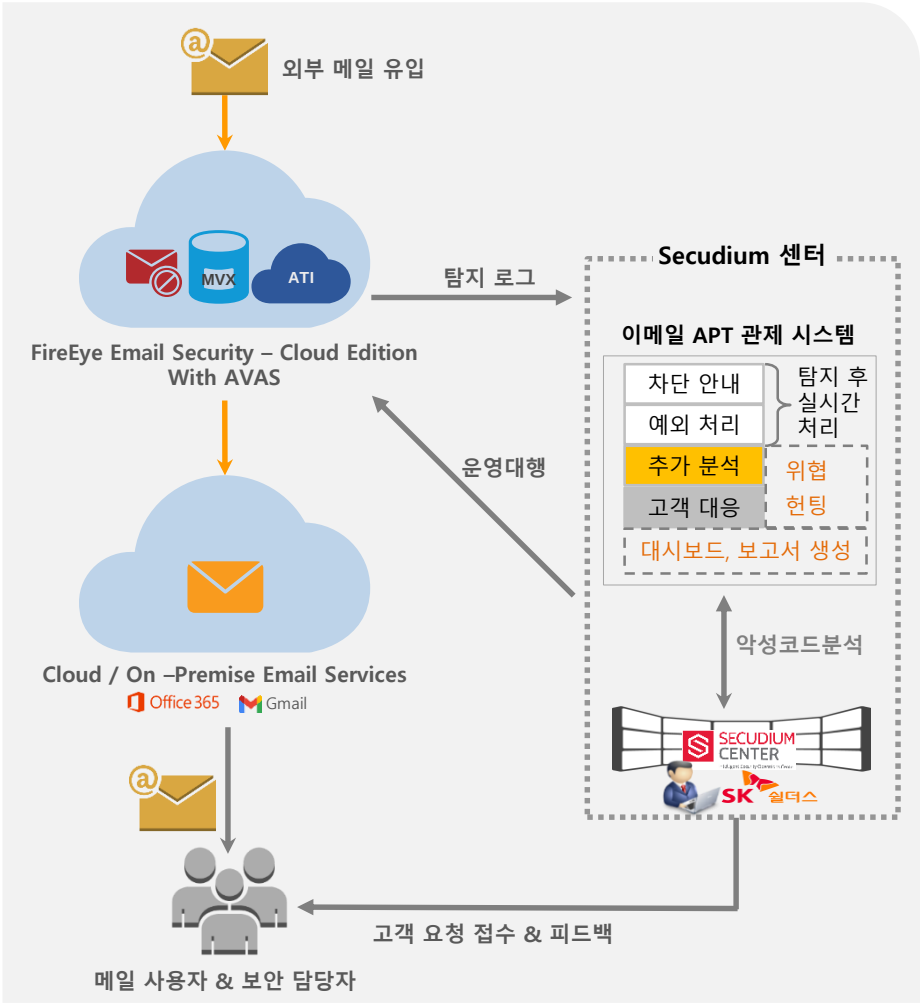
사고 사례 총평

- ✓ A고객사 **계정 탈취 목적의 피싱 공격이 지속 유입**
- ✓ 공격은 1 → 2 → 3 순서대로 진행
- ✓ 공격자는 피싱 메일을 통해 다수의 메일 계정을 탈취한 후, 탈취된 계정의 수·발신 메일 주소를 타겟으로 지정
- ✓ **주고받은 업무 메일에 악성 파일을 삽입**하여 회신 메일을 유포하고, 해당 악성 메일의 수신자로 하여금 악성 파일 클릭 유도
- ✓ **메일 계정 탈취를 통한 2차 공격 피해 주의 요망**

※ 참고기사 : 정부 "삼성·LG 해킹, 기본 보안수칙 간과한 결과"

02 E-mail 관제 서비스

APT 보안 구성



※ 고객사 구축형 서비스도 가능

ETP 서비스

• Global No.1 APT 솔루션 사용

구분	세부 내용
평판	▪ "Global T.I" 기반 평판 DB 사용
행위	▪ 가상 머신 기반 행위분석 환경 – Sandbox를 통한 행위 분석 전수 적용
백신	▪ AV/AS를 통한 탐지/차단
패턴	▪ 글로벌 정책 실시간 적용(15분 간격) ▪ 자체 분석 결과 패턴 업데이트 – YARA를 통한 신속 대응

SK 쉴더스 보안 서비스

• 정탐 및 미탐 파일 /URL Reversing 분석 수행
- 분석 결과 SIEM과 연계하여 위협 분석 및 추이 분석
- 자체 분석 결과를 통한 추가 후속 조치 진행

• 운영 대행 및 전문 지원 서비스
- SOC관제 24 x 7 대응 지원
- e-Mail 보안 훈련 지원 (분석 결과 반영 기반)
- 사내 교육을 통한 보안 의식 강화 지원 (악성메일 신고)

02 E-mail 관제 서비스

국내 유일 이메일 보안 "Managed Service" 제공, SK쉴더스 e-Mail 보안 전문가 분석 서비스를 활용하여 보안 수준 향상

서비스 내용

01 E-Mail 보안 운영 대행

- 24 X 7 메일 사용자 요청 접수 및 대응
  → 격리 해제 및 예외 처리
- 정책 및 패턴 업데이트
- 메일 장애 및 서비스 이슈 대응
- 악성 메일 모의 훈련 지원

02 SK쉴더스 전문가 분석 서비스

- 24 X 7 전문가 분석 서비스
- 상세분석을 통한 정/오탐 대응
- 전담 조직 체제로 정확/신속 서비스

03 정기/비정기 분석보고서 제공

- 고객사 악성 메일 동향 및 대응 방안 제공
- 악성 메일 유형 및 특이사항 보고
- 실시간 악성메일 현황 보고
- 악성메일 분석 후 빅데이터를 통해 추이 분석

국내유일 E-mail APT 관제서비스

- ✓ **E-Mail APT 전문 관제 서비스**
  - 100개社 이상 서비스 제공 중
  - 다양한 산업군별 레퍼런스로 고객 요청 대응 가능
- ✓ **사용자 만족도 향상**
  - 숙련된 운영 전문가 신속한 대응

전문가 서비스 활용

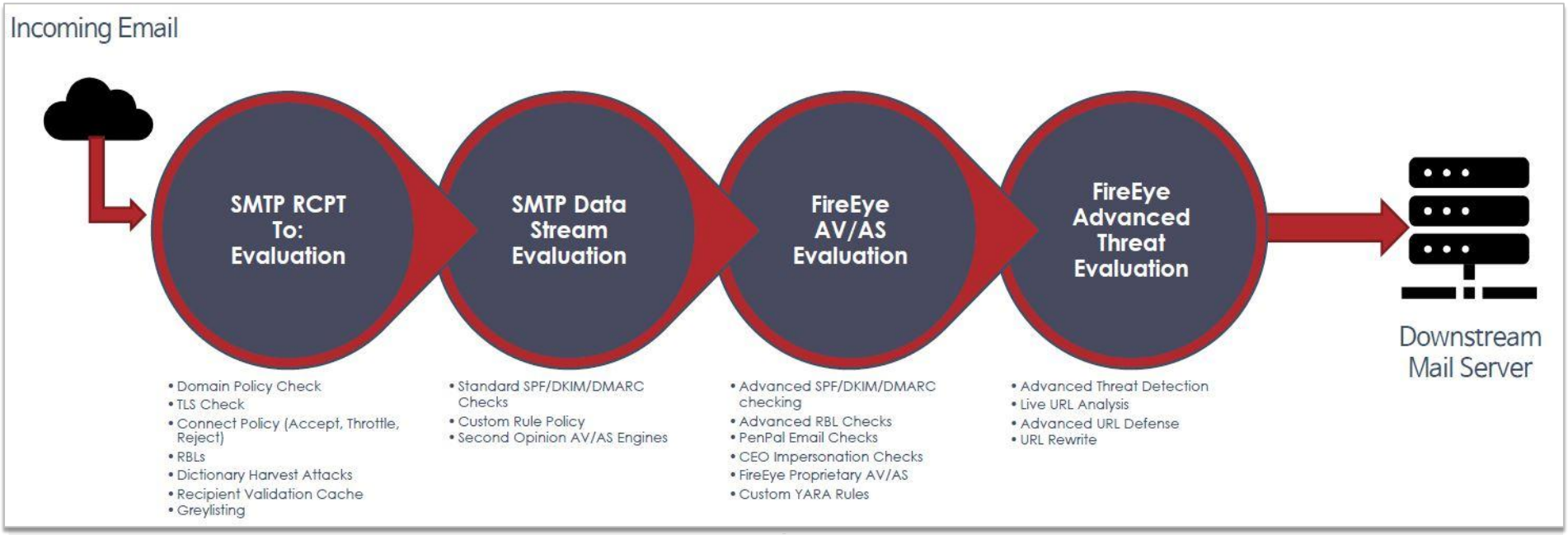
- ✓ **TOP-CERT 활용 가능**
  - 24X7 긴급 로컬 투입
  - 국내 최다 e-mail 사고분석 및 조사 실시
- ✓ **SK쉴더스 보안 전문가 서비스 활용 가능**
  - 분석 전문가 상시 대응
  - 보안 전문가 분석 서비스 (악성코드 분석가 + CERT)
  - 전담 조직 체제로 정확/신속 서비스

국내 최대 보안 수준 대응

- ✓ **서비스 통한 정보유출 불가**
  - 첨부파일 자사 망내 분석
  - 당사 전용 분석 환경 보유
- ✓ **사전 보안위협 대응역량 강화**
  - 고객 보안 부서와 협업 위협 확산 선 차단 가능

02 E-mail 관제 서비스

Trellix(FireEye) ETP 악성메일 탐지 Flow



- 이메일의 첨부파일을 가상머신 환경에서 행위 기반으로 탐지 (알려지지 않은 악성코드 탐지)
- 70+ 파일 타입에 대한 탐지 지원
- 암호가 설정되어 있는 압축파일에 대한 탐지 지원

- FireEye 인텔리전스 기반의 URL 탐지
- 파일 다운로드 유도 링크에 대한 검사
- NX와의 연동을 통한 방어(Option)
- 계정 탈취형 피싱 메일 탐지
- FAUD(FireEye Avanced URL Detection) 엔진에 의한 탐지

03 사이버 가드(정보보안 솔루션 구독서비스)

개인정보보호 및 내부정보유출 방지

1. 사이버가드란?

사이버가드는 개인정보와 영업비밀 등 중요 정보를 보호하고, 외부공격으로부터 PC와 서버 및 네트워크까지 안전하게 보호해주는 정보보안 구독 서비스입니다.

경제성	편리함	맞춤형
전기요금처럼 월 단위 부담 없이! 큰 돈 드는 하드웨어 구축 NO	**클릭 몇 번으로 쉽고, 빠르게 설치!** 어렵고, 복잡한 설치/사용 NO	**고객별, 상황별 맞춤 사용!** 쓸데 없는 상품, 거품 비용 NO

정보보안 담당자 없이도 OK. SK ICT Family 국내 정보보호 1위 기업을 우리회사 정보보안 담당자로!

2. 전체 상품 구성

데이터 및 컨텐츠 보안

01 | 자료유출방지 및 개인정보보호 (DLP)

02 | 문서 암호화 (DRM)

03 | 도면 암호화 (DRM)

04 | PC 백업

05 | 보안USB

06 | 문서중앙화

네트워크 보안

01 | 통합 네트워크 보안 (UTM)

02 | 네트워크 운영/침해 관제

03 | 네트워크 접근통제 (NAC)

04 | 웹 방화벽 (WAF)

기타 및 업무관리 서비스

01 | 근무시간관리 (PC-OFF)

02 | 그룹웨어

03 | 협업 메신저

04 | SW자산관리

05 | 취약점 진단

3. 제품 상세 소개 [1] 자료유출방지 및 개인정보보호(DLP)

DLP(Data Loss Prevention)는 PC 내 중요 정보자산을 안전하게 보호해 내부자에 의해 외부로 유출되는 것을 방지합니다.
업무 외 웹사이트 사용 차단, 메신저/메일을 통한 파일 전송 차단 등을 통해 중요정보과 개인정보보호까지 지원합니다.

제품 형태 및 구성

PC와 노트북에
DLP 보안프로그램 설치

자료를 유출하려
해도 모두 차단!

특징 및 장점

- **Multi-OS & 안전모드 통제**
  : Windows, macOS 지원 / Windows 안전모드 통제 지원
- **강력한 매체통제와 시스템 보안**
  : 다양한 매체 통제
  : Windows 보안 강화(화면보호기 강제화, 로그인 암호 강제화 등)
- **네트워크 유출 차단**
  : 메일 및 메신저를 통한 파일전송 차단 / 악성사이트 및 비업무 사이트 차단

주요 기능

매체 및 시스템 통제

- USB메모리, 외장HDD, 블루투스 등 매체사용 통제
- 매체 차단 정책 하에서 특정 장치만 허용 가능
- Windows 화면보호기, 비밀번호 설정 강제화 및 화면캡처 방지

네트워크 및 출력 통제

- **악성 사이트 및 비업무 사이트 접속 차단 (국내 최다 카테고리 및 DB 지원)**
- 메일 파일 첨부 및 메신저 파일 전송 차단
- 출력 차단 및 특정 프린터/프로세스만 예외 출력 지원 / 출력물 워터마킹 강제화

개인정보보호

- PC 내 개인정보 포함 파일 검사 (고유식별정보, 이메일 등 기본 패턴 제공)
- 커스텀 정규식, 키워드 설정 및 검출 지원
- 개인정보 검출 파일 암호화 지원(복호화 결재 지원)
- 개인정보 검사 내역 및 보유 현황 조회 지원

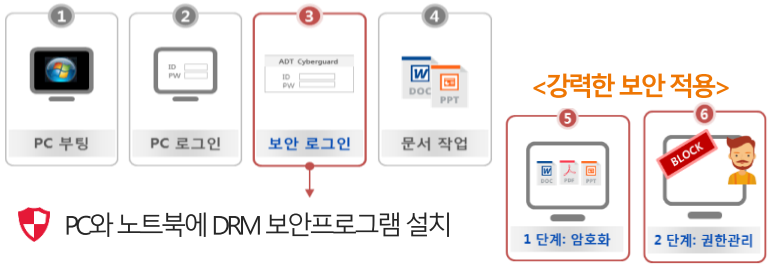
보안 결재 및 관리

- DLP에이전트 설치 현황 및 관리
- 매체 사용, 파일 반출, 워터마크 예외 등 승인 결재(자가승인, 다단 결재 등)
- 모든 보안정책 공통적용 혹은 부서/개인별 적용 지원
- 제공하는 보안기능에 대한 감사로그 증적 및 조회

3. 제품 상세 소개 [2] 문서암호화(DRM)

DRM(Digital Rights Management)은 PC 내 문서파일을 암호화하여 관리합니다. 암호화된 문서파일이 실수나 사고로 외부에 유출되더라도 암호 없이는 열람이 불가능해 정보를 안전하게 보호할 수 있습니다.

제품 형태 및 구성



특징 및 장점

- **우수한 보안성**
  : 국정원 검증필암호모듈 탑재 / GS 인증 획득
- **안전한 협업환경 지원**
  : 내/외부 협업환경에서 안전한 문서유통 체계 지원
- **효율적인 통합 관리**
  : 유연한 정책 설정/적용 및 문서사용 이력관리로 현황파악/사후 감사
- **기본 이미지, 개인정보보호 포함**
  : 이미지(jpg, bmp, png, gif, tif 등), 개인정보 탐지/삭제/격리 기능

주요 기능

문서보안

- 문서 강제 암호화 지원 (보안문서 완전 폐기)
- 접근 권한에 따른 열람/편집/출력 제어
- 복사 & 붙여넣기 제어
- 워터마크 지원

강력한 암호화 제공

- AES 암/복호화 알고리즘 사용
- 수동 및 강제(자동) 암호화 지원
- 파일 및 폴더 암호화 지원

보안정책 및 모니터링

- 그룹 및 사용자별 권한 설정
- 문서 사용 이력에 대한 모니터링 및 감사
- 이벤트별/권한별 검색 통한 일괄 모니터링

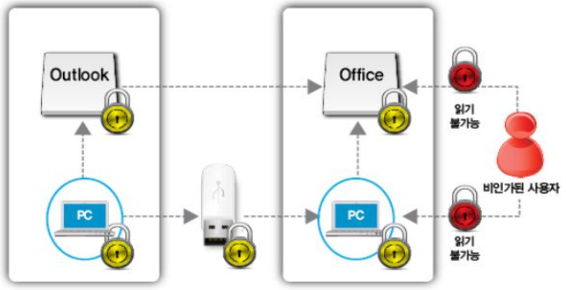
다양한 업무 환경 지원

- 다양한 어플리케이션 지원 (MS Office, 한컴 오피스 등)
- 다국어/유니코드를 통한 글로벌 업무 환경 지원

3. 제품 상세 소개 [3] 도면암호화(DRM)

도면 DRM(Digital Rights Management)은 높은 보안성을 가진 암호화 기술을 통해 다양한 도면 파일을 암호화합니다.

제품 형태 및 구성



암호화된 파일의 비인가자 접근 차단

특징 및 장점

- Kernel Mode 자동 암/복호화
- 인가자와 인가된 애플리케이션만 복호화 허용
- 암호화된 파일의 비인가자 접근 차단
- 일반도면(2D, Autocad), 전문도면(3D) 선택 가능

주요 기능

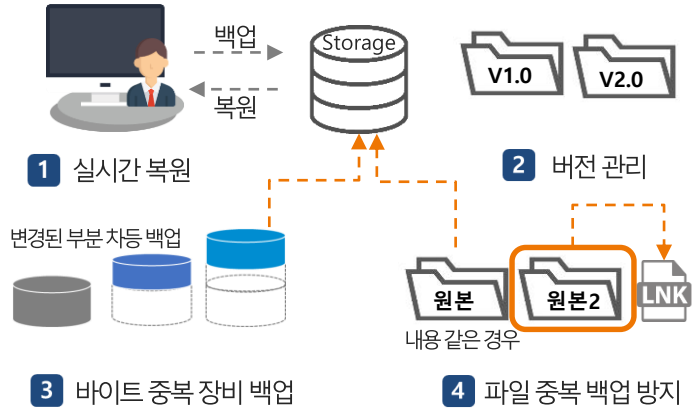
도면 DRM 라인업	지원 범위
일반도면	Auto CAD, Inventor, Revit, UNICAD
전문도면	Auto CAD, Inventor, Revit, UNICAD, SolidWorks, CATIA, Creo(pro/E), Solid Edge, UG-NX 등

구분	분류	기능설명
사용자PC 주요기능	기본	지원범위 내 파일 열람 후, 종료 시 파일 암호화
	트레이 아이콘	보안/인쇄/자가승인 정책 등 정보보기
	암호화 파일	문서 복호화 요청
		임시정책 관리
		암호화 파일 권한 변경
		암호화 파일 속성
		자가승인 정책 허용 시, 자가승인 복호화 지원

3. 제품 상세 소개 [4] PC 백업

PC 백업은 안티-랜섬웨어와 함께 사용을 권장합니다. 파일 저장과 동시에 실시간으로 파일을 PC 내 자동 백업해 데이터 손실 없이 최신 정보 유지를 지원합니다. 또한 사용자 설정을 통해 원하는 파일 혹은 드라이브만 백업해 효율적인 용량 관리가 가능합니다.

제품 형태 및 구성



특징 및 장점

- **실시간/스케쥴(분/일/주/월 단위) 암호화 보안 백업**
- **변경된 파일의 실시간 즉시 백업**
- **폴더(디렉토리) 백업, 파일 확장자 별 백업**
- **데이터 중복제거/증분 백업(변경된 내용분만 별도 저장)**

주요 기능

백업 주기

- 사용자가 얼마나 자주 백업을 해야 하는가?
  → **파일 저장과 동시에 실시간 자동 백업**

백업 정보

- 백업된 정보는 최신 정보인가?
  → **백업정보는 항상 최신 데이터 상태 유지**

백업 설정

- 원하는 파일 혹은 드라이브만 백업 할 수 있는가?
  → **파일 필터링 및 소스폴더 설정을 통해 사용자 백업 설정 가능**

백업 데이터

- 백업한 데이터는 랜섬웨어로부터 안전한가?
  → **ARIT 기술을 통해 랜섬웨어로부터 백업 데이터 보호**

※ ARIT(아리트)는 데이터 보안기술 기반의 파일별 캡슐화와 가상 보안영역 생성으로 데이터를 보호하고, 데이터 백업 기술을 기반으로 실시간 백업과 파일별 이력관리를 수행.

3. 제품 상세 소개 [5] 보안 USB

보안 USB는 매체제어 기능과 다양한 보조기억매체를 중앙에서 관리하는 보안기능을 제공합니다. 보안USB S/W와 메모리(32GB, 64GB, 128GB) 선택을 통해 사용 가능합니다.

제품 형태 및 구성

특징 및 장점

- **분실/도난 시 저장된 데이터의 보호를 위한 삭제, 중앙관리 (보안정책, 로그조회 등)**
- **사용자 식별/인증, 저장 데이터 암/복호화, 저장된 자료의 임의 복제 방지**

주요 기능

매체제어

- 중요(개인) 정보가 매체를 통해 저장/전달/공유/유출되는 일련의 정보 유출 행위를 사전 차단하거나 사후 로그를 통해 감사하는 기능 제공
- 다양한 매체제어 (USB, 테더링, MTP, CD-ROM, E-SATA, SD Card, 외장 HDD)

저장 데이터 암/복호화

- 크립토칩(Crypto-Chip) 기반의 강력한 데이터 암호화로 정보유출 방지
- 분실/도난 시 보안칩의 자동 암호화로 소유자 이외의 열람 차단

저장된 자료의 임의 복제방지

- 보안 USB 전용 탐색기 방식으로 데이터 접근통제 및 복제방지 보안 기능 제공
- 보안 USB Read/Write 허용 및 차단 시, 양방향 사용 로그 기록 제공

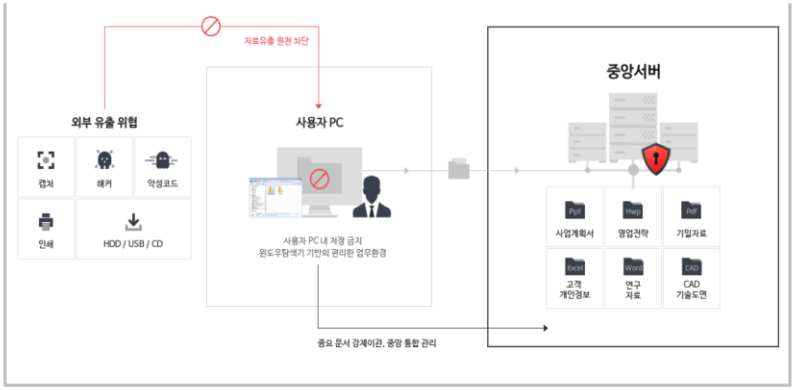
분실/도난 시 저장 데이터 보호를 위한 삭제

- 분실/도난 시 관리자에 의한 실시간 원격 사용금지 또는 데이터 완전삭제
- 보안 USB 분실/도난 시 중앙관리서버로 분실 신고 및 추적 로그 저장

3. 제품 상세 소개 [6] 문서중앙화

문서중앙화는 사용자 PC에 자료 저장을 금지시켜 내부자료 유출을 원천 차단함과 동시에 문서중앙화와 업무효율성을 보장하는 전사적 파일보안 서비스입니다.

제품 형태 및 구성



특징 및 장점

- **자료유출 원천차단**
  : 기업 내부 자료는 문서중앙화 서버에만 저장
- **문서중앙화 환경**
  : 모든 문서는 중앙 서버로 통합해 유실을 방지하고, 업무의 연속성 보장
- **업무 효율성 보장 환경**
  : 윈도우 탐색기 인터페이스와 편리한 반출 프로세스를 통한 편리한 업무환경

주요 기능

내부자료 유출 원천 차단

- 사용자 PC 자료를 중앙 서버로 자동 이관 및 저장
- 내부 자료의 로컬 저장 금지

서버 및 전송 구간 암호화

- 물리적인 디스크 유출 또는 해킹에 의한 데이터 유출 방지
- 전송 구간 및 서버에 저장된 파일 암호화

문서 버전 관리 및 복원

- 실수 또는 변경/삭제된 파일의 복원
  (비인가 프로세스인 랜섬웨어 접근 차단)

다양한 협업 디스크 구성

- 인사 DB와 연동된 조직도 기반의 조직디스크 생성
- 필요에 따라 특정 그룹의 프로젝트 디스크 생성

3. 제품 상세 소개 [1] 통합네트워크보안(UTM)

통합네트워크보안(UTM; Unified Threat Management)은 방화벽, 침입방지시스템(IPS), 가상 사설망(VPN) 등 다양한 보안 솔루션 기능을 하나로 통합, 제공합니다. 복합적인 네트워크 위협 요소를 효율적으로 방어할 수 있는 네트워크 보안 장비입니다.

제품 형태 및 구성

특징 및 장점

- **논리적 가상화**
  : 1대의 장비로 여러 대의 방화벽/가상사설망 보안서비스 제공
- **사용자 인증 · Zone 기반 보안정책**
  : 사용자 계정 기반의 접근 제어, Zone(그룹별, 개인별 차별화 보안정책)
- **성능 저하 없는 고성능 제품**
- **NLB(네트워크 로드밸런싱) · VPN**
  : 인터넷 구간의 다양한 회선 사용 시, 대역폭 통합을 통해 트래픽 보장

주요 기능

- 국가정보원으로부터 CC인증(EAL 4) 획득
- Good Software 인증 1등급 획득
- 전용 OS 기반의 H/W 일체형
- 전원 이중화 (일부 제품)
- 방화벽
- VPN
- SSL-VPN
- IPS
- Anti-DDos (1,300 이상 장비부터 지원)
- QoS
- Contents Filtering (Web URL Filtering / Web Editor Filtering)
- 가상화

3. 제품 상세 소개 [1] 통합네트워크보안(UTM) : 라인업 사양

		(Pro) VPN전용 : ~10대, 40D	(Pro) VPN전용 : ~30대, 80D	(Pro) UTM : ~50대, 90	(Pro) UTM : ~100대, 200	(Pro) UTM : ~150대, 300S	(Pro) UTM : ~200대, 1300S	(Pro) UTM : ~400대, 2300S
Appearance								
CPU		2 Core	2 Core	2 Core	4 Core	4 Core	4Core	4Core
Main Memory		512 MB	1 GB	2 GB	2 GB	4 GB	4GB	16GB
Flash Memory		8 GB	8 GB	8 GB	8 GB	8 GB	8GB	4GB
HDD		N/A	N/A	500GB	500 GB	500 GB	1TB	1TB
NIC	10/100/1000-TX	6	8	8	6	6	6	8
	1000B-SX	-	-	-	2 (Combo)	-	4	4
	10GF	-	-	-	-	-		
	Bypass (Copper/Fiber)	-	-	-	-	(2/0)	(2/0)	(1/0) Option
Power		Single	Single	Single	Single	Single	Single	Redundant
F/W Throughput (Max)		990 Mbps	4.5 Gbps	4.7 Gbps	7.3 Gbps	6 Gbps	10G	16G
IPS Throughput (Max)		-	450 Mbps	450 Mbps	1.6 Gbps	1.9 Gbps	1.9G	2.5G
VPN Throughput (Max)		530 Mbps	1 Gbps	1 Gbps	3.3 Gbps	2 Gbps	2G	2.7G
VPN Tunnel (Max)		5,000	5,000	10,000	10,000	20,000	20,000	40,000
Concurrent Sessions(Max)		50,000	300,000	1,000,000	800,000	2,000,000	2,000,000	5,000,000
Dimensions (WxHxD mm)		260 x 44 x 150	246 x 44 x 172	316 x 44x 265	315 x 44 x 260	430 x 44 x 310	430 x 44 x 310	443 x 44 x 405
Weight (kg)		1.3	1.5	2.7	2.7	4.4	4.8	7.2
OS		AOS	AOS	AOS	AOS	AOS	AOS	AOS

3. 제품 상세 소개 [2] 네트워크 운영/침해 관제

정보보안 1위 기업의 전문 인력을 통해 24시간, 365일 보안 관제 및 실시간 대응 체계를 구축합니다.

서비스 개요

- 24시간 365일 보안 관제
- 고객 개입 최소화 '능동형 관제서비스' 제공

운영 관제 Value

- 보안 장비 On/Off 상태 신속 알림
- 장애처리 진행 상황 공유
- 장비 상태 모니터링

침해 관제 Value

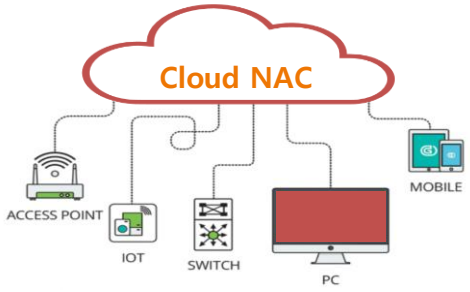
- 해킹 대응 → 공격 위협 차단
- 실시간 위협 모니터링 및 알림
- 월간 리포트 서비스

서비스 종류	분류	서비스 내용
운영 관제	사활 모니터링	장비 On/Off 상태 SMS 통보
	Resource 모니터링	장비 상태(Traffic, CPU, Memory) 이상 SMS 통보
	장애 관리	이상 상황 메일 통보 및 장애 처리 조율
	정책 관리	정책 관리(장비 정책 back-up) 보안장비 정책 커스터마이징 초기 1회 제공
침해 관제	로그 보관	로그 보관(1개월)
	모니터링	보안 이벤트 탐지/분석, 알림 서비스
	공격 대응	공격자 IP 차단 서비스 (요청 시)
	리포트	월간 리포트 서비스 제공
공통 서비스	서비스 Portal	대시보드, 침해위협 뷰어, 정책변경 요청, 정보제공 등
	정보제공 서비스	위협정보, 뉴스클리핑 등 정보제공

3. 제품 상세 소개 [3] 네트워크접근통제(NAC)

네트워크접근통제(NAC; Network Access Control)는 네트워크 가시성을 확보하고, 네트워크에 접속하는 사용자나 다양한 기기를 식별/인증/통제함으로써 네트워크를 보호하고 위협을 통제합니다.

제품 형태 및 구성

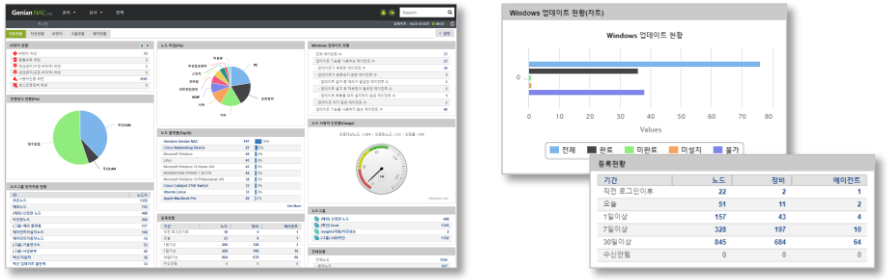


특징 및 장점

- **다양한 DB 연동 통한 정보 자동 등록/관리**
  : ORACLE, MySQL, MSSQL, IBM, DB2, TIBERO, ALTIBASE, PostgreSQL, CSV 등
- **단말 플랫폼 인텔리전스(DPI; Device Platform Intelligence)**
  : Agent 설치 없이도 네트워크 장치에 대한 상세 플랫폼 정보 제공 (주 1회 자동 업데이트)
- **다양한 분석/보고서 제공**
- **MAC OS 지원**

주요 기능

NAC 구성요소	주요 기능
정책서버 (Policy Center)	▪ AWS 환경 지원 ▪ 보안정책 수립 ▪ 단말 현황 및 이력관리
네트워크 센서 (Network Sensor)	▪ 사내 유휴 서버 사용, 대여, 구매 등 다양한 방식 지원 ▪ 유/무선 네트워크 제어 ▪ 네트워크 정보 수립 ▪ DHCP IP 서비스 제공
에이전트 (Agent)	▪ H/W, S/W 정보 수집 ▪ 보안 설정 유무 확인 및 교정 ▪ MS patch
콘솔 (Console)	▪ 관리자 웹 콘솔 ▪ IE, Chrome, FireFox, Safari, Opera 등 다양한 환경 지원 ▪ 유무선 네트워크 통합 관리 지원



[관리자 화면] 대시보드를 통한 네트워크 사용 현황, 관리 로그, 시스템 정보 등 제공

3. 제품 상세 소개 [3] 네트워크접근통제(NAC) : 상세 기능

NW 및 단말 가시성 관리

- 네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인
- 모든 데스크톱의 자동 탐지 및 식별
- 실시간 상세(H/W, S/W, 패치 등) 정보 수집
- '언제, 어디서, 누가, 무엇으로 ' 의 현황 관리

단말 무결성 점검

- 필수 SW(보안SW 등) 설치 점검
- 보안 SW 동작 여부 점검 (악성코드 탐지 기능)
- 단말에 대한 가시성 & 보안성 강화
- 단말의 S/W, H/W 정보 제공
- 단말 무결성 미 확보 시, 단말 NW 격리
- 필수 SW 미 설치 시 강제 배포

IP 관리

- IP 주소 관리 기능 제공
- 인사 DB 연동을 통한 IP 실명제
- DHCP 내장 및 신청/승인 등 업무절차 지원

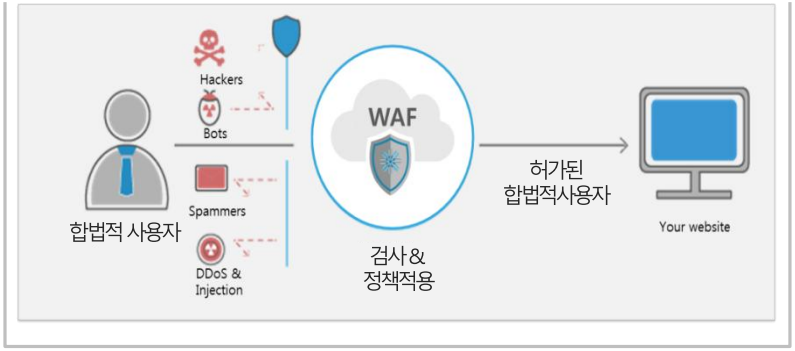
인증 관리

- 사용자 인증 페이지 지원 (CWP , 리다이렉트 페이지)
- 802.1X 지원 및 RADIUS 서버 내장
- 2 Factor 인증 지원 (OTP 등)

3. 제품 상세 소개 [4] 웹방화벽

웹방화벽(Web Application Firewall; WAF)은 하드웨어/소프트웨어 설치, 유지보수, 라이선스가 필요 없으며 다양한 형태의 웹 공격, 비정상적인 접근 차단, 개인정보 유출을 방지합니다. 또한 웹 서버의 성능 저하 없이 외부로부터의 공격을 실시간 탐지/차단합니다.

제품 형태 및 구성



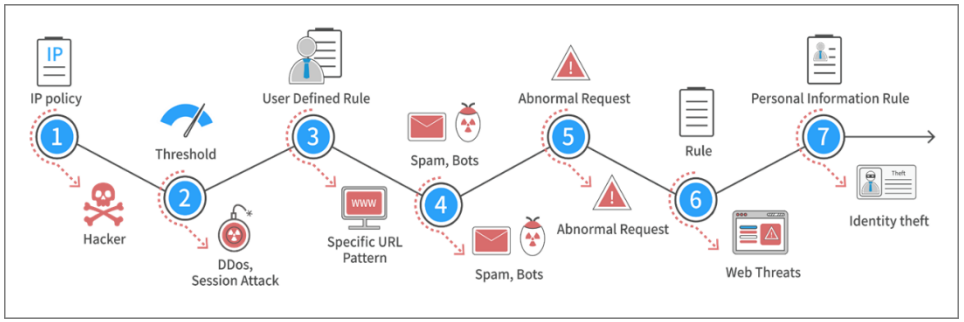
주요 기능

웹방화벽이 방어하는 대표적인 웹 공격 종류

- SQL 인젝션
- 디렉토리 리스트
- 웹 서버 취약성
- 디렉토리 접근
- 악성파일 접근
- 스캐너/스팸봇 탐지
- 시스템파일 접근
- CSRF
- Command 인젝션
- 애플리케이션 취약성

특징 및 장점

- **강력한 보안**
  : 클라우드 기반의 보안 서비스로 강력한 보안 기능 제공
- **간편한 관리**
  : 쉽고 편한 보안정책 설정 및 모니터링
- **용량 별 선택 (30GB / 100GB / 500GB)**



3. 제품 상세 소개 [1] 근무시간관리 (PC-OFF)

근무시간관리 (PC-OFF)는 주 52시간 근무제를 준수하며 임직원들의 근로시간을 효율적으로 관리합니다.

제품 형태 및 구성

- Android / iOS
- 출퇴근 등록
- QR코드 (2단계 인증)
- 근태승인 요청/결재

모바일 App

- Windows / Mac
- 업무시간 외 PC잠금
- 이석 시간 관리
- 근태승인 요청/결재

PC 에이전트

- 출퇴근 등록
- 근태현황 조회
- 근태승인 요청/결재

사용자/결재자 Web

- 조직의 근로기준 설정
- 임직원 근태 현황 조회
- 캡스 근태관리 연동

관리자 Web

특징 및 장점

- **모바일과 PC 연동**
- **다국어(영문) 지원 / Mac OS 지원**
- **퇴직자 지정 기능으로 근태기록 보관(법적으로 3년간 보관 필요)**
- **Good Software(GS) 인증 1등급 획득**
- **사용 중인 인사 및 결제(그룹웨어) 연동 (캡스 근태관리 연동)**

: 서비스형/구축형에 따라 연동 범위 차이

주요 기능

업무시간 외 PC 제어

- 정해진 근무시간 외 PC화면 잠금 / PC 사용 종료 10, 20, 30분 전 알림 제공
- 시작/종료시간, OT 시간 지정(주 12시간 미만 설정 가능)

자리 비움(이석) 시간 관리

- 이석관리 기능 3단 설정으로 회사 내규에 맞는 정책설정 가능

언제, 어디서나 출퇴근 등록

- 재택/출장/외근/현장 등 사무실 밖에서도 모바일 App을 통해 출퇴근 등록
- GPS 기반의 근무지 관리
- PASS 연동, 생체인식(지문, 홍채) 적용을 통한 모바일 개인보안 관리

부정 출퇴근 등록 방지

- 모니터 속 QR 코드를 모바일로 스캔 (이중 보안)

주52시간 근로시간 준수

- 근로기준법에 명시된 주52시간 근무제와 유연근무제 지원

조직의 근무 통계 제공

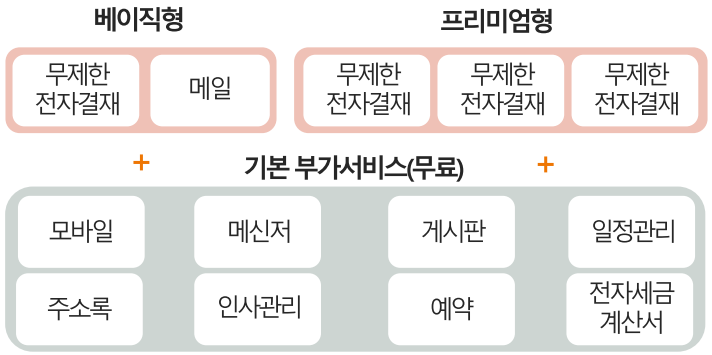
- 설치/미설치 현황, 접속/미접속자 현황, 부서별 근무현황, 일/주/월 별 근무시간 등 근무 통계 제공 (엑셀 다운로드)

3. 제품 상세 소개 [2] 그룹웨어

기타 및 업무관리서비스

그룹웨어는 업무에 필요한 모든 기능을 담아 스마트한 업무환경을 제공합니다. 업무용 메일과 메신저로 소통하고, 회상화의로 협업하고, 전자결재로 품의서 기안 및 일정과 근태를 관리할 수 있습니다.

제품 형태 및 구성



특징 및 장점

- **기업 내 원활한 정보공유, 신속한 의사결정**
  : 사내메일, 메신저 통한 신속한 정보전달 / 전자결재 통한 의사결정 단축 / 게시판, 일정관리 등
- **정보화 수준 향상**
  : 회사 내 정보보안 관리(IP접근제한, 자료 및 정보 접근제한)
- **시공간 제약 없는 업무환경**
  : 출장자, 재택근무 등 시간/장소 제약 없이 업무 진행

주요 기능

기업 메일

- 회사 도메인(@회사명.com)으로 된 메일 사용으로 고객 신뢰도 상승
- 모바일 오피스 앱을 통해 공간 제약 없이 메일 업무 처리 지원
- 송/수신 메일 최대 5년 보관(퇴사자 메일 별도 보관), 법적 용도 및 감사 활용 가능

전자 결재

- 인사관리 및 ERP 결재 연동

인사 관리

- 전자 결재와 연동한 연차/휴가 관리 및 출동경비/근태 시스템과 연동한 출퇴근 관리
- 기업 근태 정책에 따른 군무시간 관리(주52시간)

메신저

- 조직도 기반의 사용자 리스트 세팅

일정관리, 자원예약, 세금계산서

- 공유 캘린더를 이용한 프로젝트 일정 관리, 회의실 등 사내공간 예약,
  국세청과 연동한 무제한 세금계산서 발급

주소록, 게시판

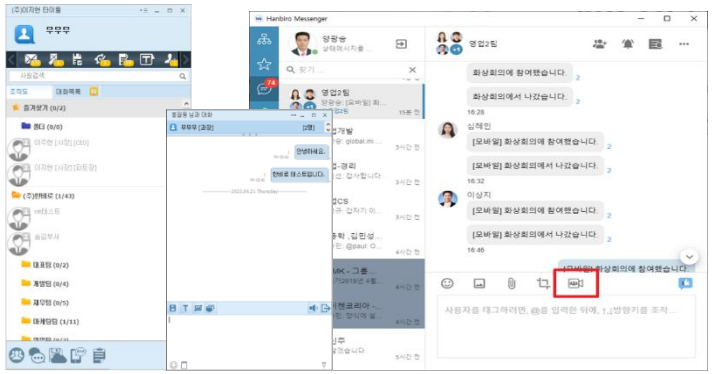
- 개인/공용 주소록 사용, 게시판을 통한 사내 소식 공지/공유

3. 제품 상세 소개 [3] 협업메신저

기타 및 업무관리서비스

협업메신저는 기업의 업무를 더 빠르고, 더 편리하게 하기 위한 협업 솔루션입니다. 모바일 오피스 환경 구축, 실시간 커뮤니케이션 및 파일 공유와 같은 강력한 협업 도구를 통해 기업만의 능동적인 협업 환경을 구축할 수 있습니다.

제품 형태 및 구성



특징 및 장점

- **사용자 최적화 UI/UX**
  : 사용자 사용 빈도에 따른 최적화된 메뉴위치 설정
- **메시지 수신확인 기능**
  : 상용 메신저와 같이 상대방이 메시지 수신여부 확인 가능
- **로그인 디바이스 정보 표시**
  : 다양한 디바이스로 로그인 진행 시 각각 접속 여부를 확인하여 대화 진행 가능

주요 기능

편리한 그룹채팅

- 여러 사람과 실시간 의견 교환 필요시 Drag & Drop으로 대화상대 추가가능

과거대화 검색

- 특정 내용 검색을 위한 키워드 검색 가능

게시판기능

- 대화방 인원과 공유/ 공지가 필요한 경우 게시판 게시 가능 (사진,파일 첨부 가능)
- 새로운 글 게시 시 대화방 알림창을 통해 리마인드 가능

PC원격지원

- 구성원간 상대방 PC에 대한 원격 접속 가능
- 간단한 장애조치나 기술지원시 활용 가능

3. 제품 상세 소개 [4] SW 자산관리

SW 자산관리는 PC에 설치된 S/W 정보를 수집하고, 정품 S/W 현황 관리를 통해 라이선스 문제를 예방합니다.

제품 형태 및 구성

특징 및 장점

- **S/W 관리 자동화를 통한 효율성 향상**
  : 시스템 상의 관리를 통해 수기관리
- **S/W 사용량 측정**
  : 프로세스별/사용자별 S/W 사용량 확인
- **S/W 설치/차단 지원**
  : 부서 및 사용자 별 S/W의 필수설치 및 사용제한 설정

주요 기능

S/W 관리의 자동화

- 사용자, 부서별 사용현황 관리
- 부서별 1차 정책 설정 후, 개인별 정책 설정 가능
- 필수 설치 리스트 관리

자산에 대한 품목 관리

- 품목 분류코드 부여, 분류코드 별 자산 보유 현황 조회

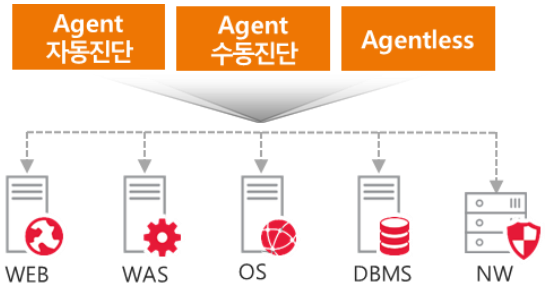
S/W 사용량 관리

- 프로세스/사용자별 사용내역 확인, 프로세스별 시작&종료&총 사용시간 확인
- 사용자별 S/W 사용시간 및 횟수 체크(선택사항)

3. 제품 상세 소개 [5] 취약점 진단

국내 보안 컴플라이언스(전자금융감독규정, 정보통신기반보호법) 규정을 100% 충족하는 원스톱 서비스를 제공합니다.

제품 형태 및 구성



특징 및 장점

- 전문가 수준의 강력한 취약점 점검 및 조치 방안 제공
- 상황에 맞는 진단방법(Agent 수동, Agentless 등) 선택
- 다양한 보고서 제공 및 사용자 편집을 통한 맞춤형 보고서 지원
- 기본 보안규정 템플릿을 이용한 사용자 맞춤형 진단 템플릿 정의
- 주요기반시설/금융기반시설 등 중요 보안규정 템플릿 제공
- 편리하고 직관적인 사용자 인터페이스

주요 기능

자산 관리

- 다양한 분류체계 지원(분류별/물리 논리자산/사용자정의 등)
- 기업 자산 기반, 프로젝트 자산관리 지원

진단/모니터링

- 국내 주요 진단 규정 기본 제공 / 진단 규정 사용자 정의 지원
- 진단 진척율 및 리소스 사용량 실시간 모니터링 지원
- 자동진단, 수동진단, Agentless 진단 지원

조치 관리

- 진단 사전/사후 조치 지원
- 일괄 조치 및 자산별 조치 지원
- 진단 결과에 따른 조치 가이드 제공 및 편집기능 지원

보고서/변경 추적

- 자산별, 프로파일별, 자산그룹별 보고서 제공
- 진단이력조회 및 비교분할창을 통한 진단 결과 비교
- HTML, EXCEL, PDF, HWP 양식의 보고서 출력 지원

II. 추가 바우처 서비스

01 원격보안관제 서비스

02 이메일 모의 훈련

03 외부노출 자산 보안위험진단

01 원격보안관제 서비스

네트워크 보안위협 및 침입 탐지·대응

원격보안관제 서비스

빅데이터 엔진을 기반으로 보안 관제에 필요한 기술, 프로세스, 서비스를 통합하여, 신속한 Data 수집/처리/탐지/대응, 보안관제 업무 및 고객 관리, 취약점 정보 제공, 보고서 작성 등 관제에 필수적인 업무를 효율적으로 운영합니다.

SK쉴더스 보안관제서비스가 해결해드립니다.

6+ Countries	20+ Years Know-how	600+ Experts	2,000+ Customers	8,000+ Sensors	100,000,000+ Treat Event/ 1 Day

최고 최다 전문인력 실시간 모니터링/분석 (Big Data 분석 플랫폼)

21년 노하우/기술력 국내 최대 공격유형 정의 (통합탐지 Rule)

글로벌 최신 위협정보 신속한 수집 및 제공 (한국/중국/일본/베트남/말레이시아 등)

침해사고 최고 전담인력 신속·정확한 분석/지원 (Top CERT)

제공 서비스

Managed 서비스 (기본형)

- 서비스거부공격차단시스템 관제(DDoS)
- 침입차단시스템 관제(FW)
- 지능형지속위협솔루션 관제(APT)
- 웹어플리케이션방화벽 관제(WAF)
- 침입탐지/방지시스템 관제(IDS/IPS)
- EDR 관제, 웹쉘탐지솔루션(W-shield) 관제

전문가 서비스

- 보안 모의훈련 서비스
  (해킹Mail 대응, DDOS 대응, 침해사고 대응)
- 침해사고 흔적 조사
- 다크웹, 해킹탐지 수준진단 서비스

진단 서비스

- 취약점 진단 서비스
  (모의해킹, 모바일진단, 인프라진단)

원격보안관제 서비스_SK쉴더스 센터 소개

Secudium Center는 다년간의 보안관제 경험과 노하우, 통합관제플랫폼 등을 바탕으로 기업의 비즈니스 환경을 24시간 365일 안전하게 보호하고 있습니다.

SECUDIUM CENTER
Intelligent Security Operations Center

국내 1위 보안관제 노하우

- 24X365 무중단 보안관제 서비스 수행
  - 2,000여 고객 / 8,000개 보안장비 대상
- 자체 개발한 통합보안관제플랫폼 보유
- 침해사고대응 전문 인력(Top-CERT) 보유
- 관제 프레임워크 및 방법론(ISMM) 보유

글로벌 사이버위협 공조

- 글로벌 위협 인텔리전스 수집/공유
  - CTA(Cyber Threat Alliance), FIRST 등
- 국내외 유관기관 공조
  - KISA, 국정원, 금융보안원, 美NCSC 등
- 국내 대형 관제 고객 연계
  - SK관계사/SOC, 금융·공공·기업 파견관제

02 이메일 모의 훈련

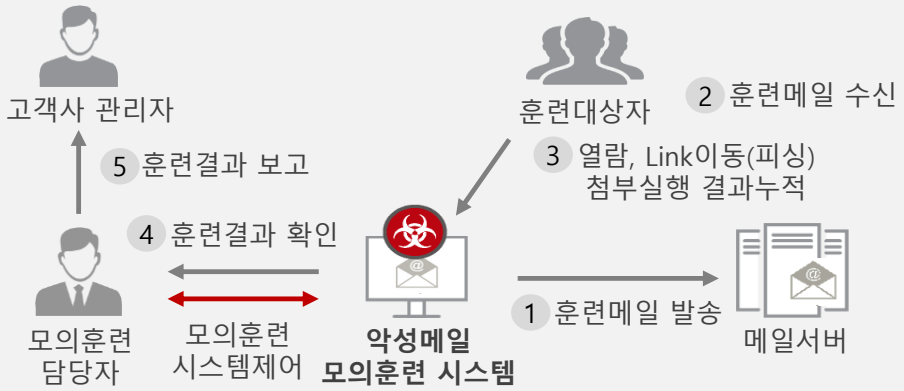
사용자 보안인식 제고 및 메일 보안 강화

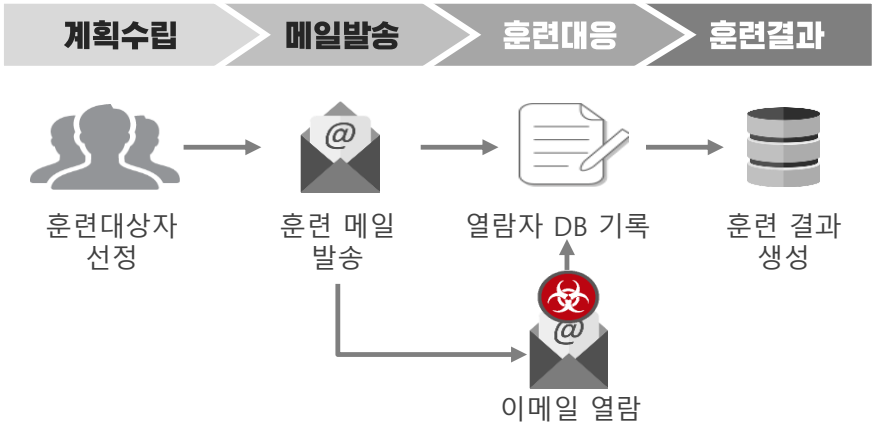
이메일 모의훈련

E-mail을 통한 정보유출사고 및 악성코드 감염으로 인한 피해가 발생하지 않도록 사전에 악성 메일과 유사한 패턴의 모의훈련을 실시하여 피해를 예방하고, 보안인식을 제고할 수 있는 서비스입니다.

E-mail 모의훈련

악성메일 모의훈련 프로세스





기능소개

- **훈련메일 양식 작성, 훈련메일 양식 목록**
- **대상자 관리**
  - 기관/부서등록, 대상자 그룹 생성, 대상자 그룹관리
- **훈련 준비, 훈련 진행, 훈련 완료 등 훈련 관리**
- **발송관리(발송 준비, 발송 진행, 발송 완료)**
- **훈련 결과 조회**
- **시스템 관리**

서비스 특장점

- **최근 악성메일 동향 분석**
  - 최근 발생한 악성메일 유형을 분석하여 악성 메일 시나리오 DB 업데이트
- **고객사 맞춤형 훈련메일 제작 / 훈련**
  - 최근 발생하는 악성메일 유형 및 사회적 이슈 반영한 고객사 맞춤형 훈련 메일 제작
  - 보안 인식 수준을 고려한 훈련 난이도 설정

03 외부노출 자산 보안위험 진단(ASM 서비스)

공격자(해커) 관점 외부침입 진단 및 관리

외부노출 자산 보안위험 진단(ASM 서비스)

주요 기능

주요, 활용 예시

노출된 보안 위협 확인
(공격 시나리오에 활용되는
목표대상 서비스 Scanning 분석 정보)

- 대외 노출된(관리/미 관리) 서비스 확인
- Open된 서비스 및 Port 정보 확인
- 로그인 / 관리자 Page 노출 여부 확인
- SSL 인증 정보 확인

- 불필요한 Open Port 여부 정기적 확인
- 미 관리되는 회사 자산 여부 자동 확인
- 취약한 인증 여부, 만료일 여부 Alert 확인

+

공개/유출된 보안 위협 확인
(직접 공격에 활용되는
OSINT, 딥웹, 다크웹 위협 정보)

- 외부 공개된 OSINT 정보 수집
- Surface Web내 중요 시스템 노출 정보 수집
- 로그인 된 서비스(딥웹) 내, 위협 정보 수집
- 다크웹 내, 유출된 Credential(계정) 정보 수집

- Open된 정보 기반, 노출 취약점 즉시 확인
- 정기적으로 다크웹 내, 회사 유출 정보 확인 및 유효성 자동 테스트 활용

+

취약점 자동 테스트
(확인된 정보기반 자동 테스트 및
관제 모니터링 검증)

- 노출된 Page 로그인 가능 여부 자동 테스트
- 노출된 취약점 확인 CVE(1,359개) 자동 테스트
- 노출된 위험 Port 브루트포스 테스트
- 다크웹 유출 계정 유효성(로그인 가능) 테스트

- 확인된 취약점(이슈)기반 테스트 자동화
- 이슈 상태 관리(조치 여부) 확인
- 조치 후, 이행 점검 시 테스트 자동화
- CVE 자동 공격 테스트 시, 내부 보안 효과성 (관제,모니터링) 검토 활용

외부노출 자산 보안위험 진단(ASM 서비스)

다음과 같이 6단계로 진행됩니다.

1
기본정보 등록
(Setup)

사전 정보수집 범위인 대표 IP
Domain 등록

2
수집정보 범위
방식확인
(Scoping)

서비스 영향도에 따른
수집정보 범위 및 스케줄링 설정

3
공격표면정보 수집
(Discovery)

노출된 관리/미관리 자산정보 수집
유출된 계정정보 수집

4
정보확인 및
검증테스트
(Test)

수집/확인된 정보기준 추가 테스트 요청
요청된 테스트 기준 테스트 결과 제공

5
지속적 모니터링 및
변화 확인
(Monitoring)

이전에 확인된 공격표면정보 변화 모니터링
확인된 이슈 조치 여부 모니터링

6
결과리포팅
(Reporting)

보안전문가의 Review(정/오탐)가
포함된 PDF 리포트

(사) 벤처기업협회

SK shieldus

보안, 그 이상의 믿음

벤처기업협회 08389 서울특별시 구로구 디지털로30길 28 마리오타워 8층
E-mail : lyt@kova.or.kr TEL : 02-6331-7094 FAX : 02-6331-7113

SK쉴더스 13486 경기도 성남시 분당구 판교로 277번길 23 4&5층
E-mail: hjlee85@sk.com TEL : 010-7667-5068 FAX : 02) 6361-9998