
11D

**재택 근무 꿀맛?
보안은 쓴맛?!**
-코로나 극복기-

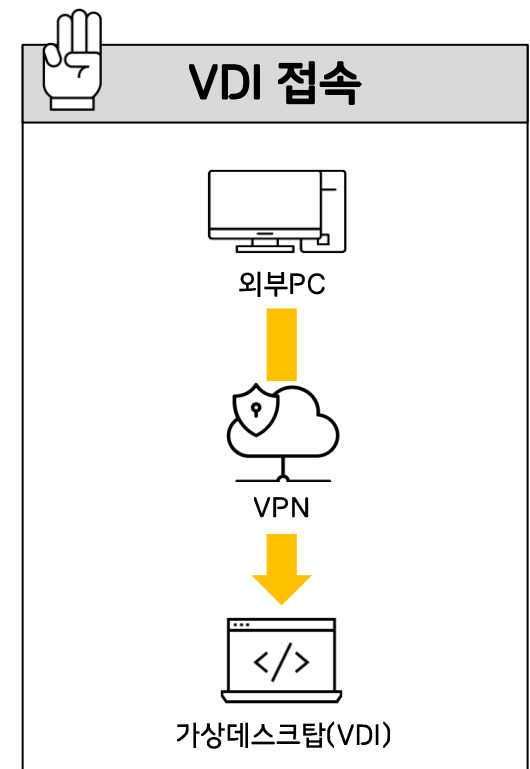
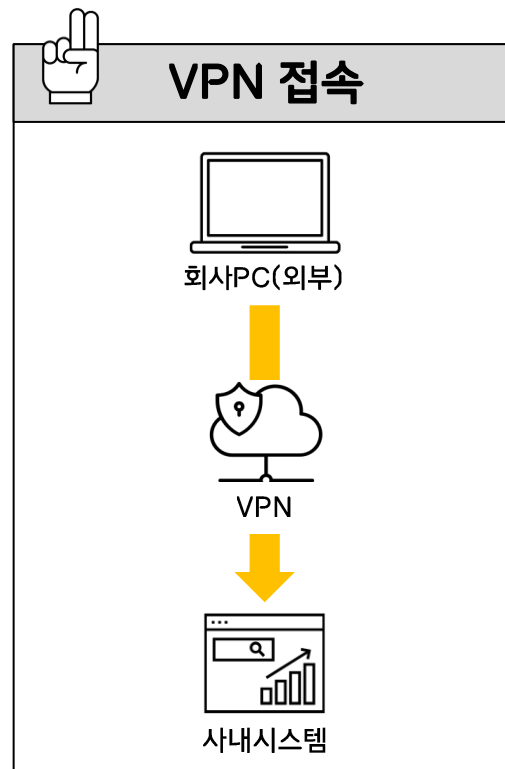
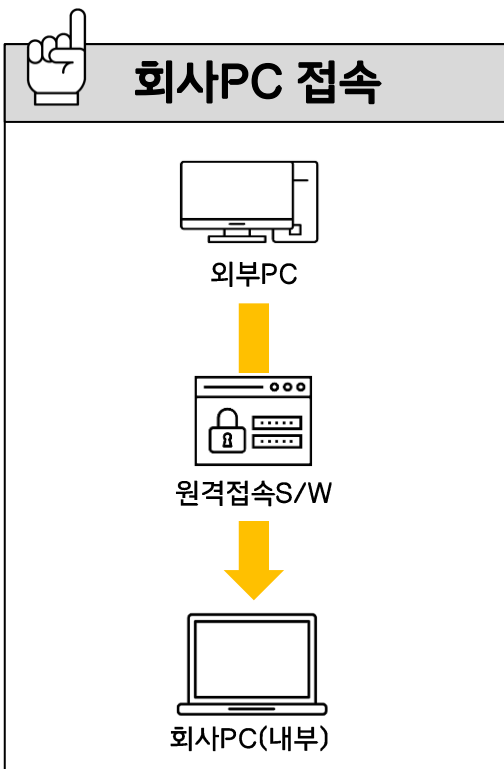
정보보안팀(안호찬)

“코로나 19로 인한 전사 재택 시행“



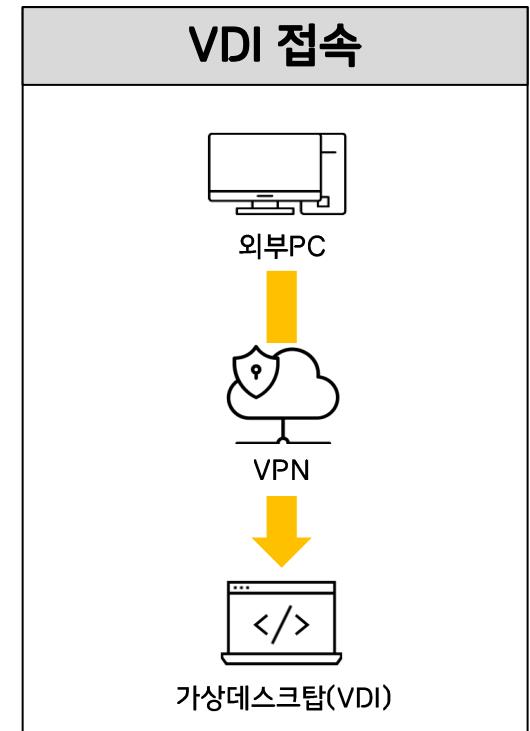
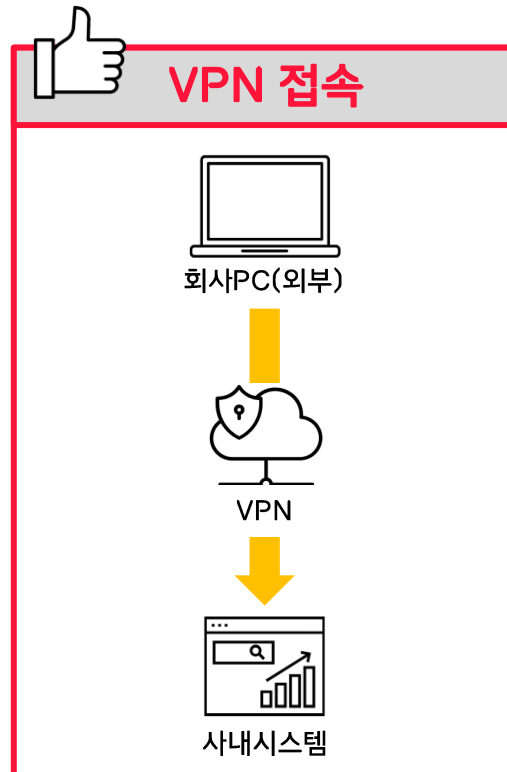
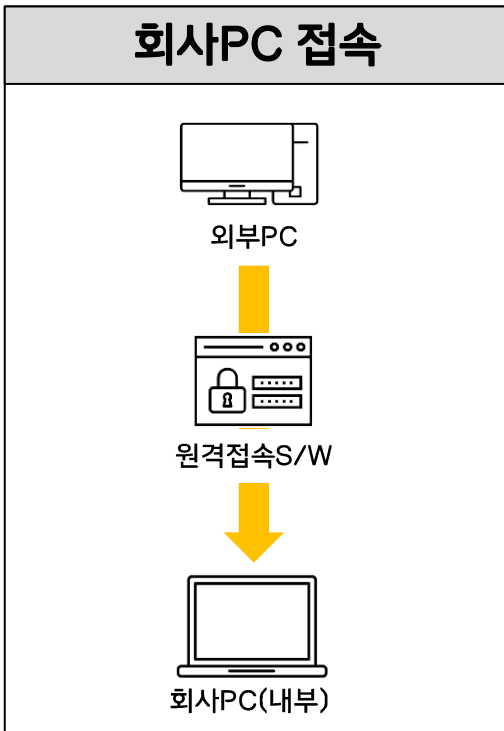
재택 근무 방식을 선택하자

여러가지 방안 중 보안성과 효율성을 고려하여 방식을 선택함



재택 근무 방식을 선택하자

여러가지 방안 중 보안성과 효율성을 고려하여 방식을 선택함



지금 당장 할 수 있는 것을 찾자

매년 1회 정보보호서약서 서약에 추가로 재택근무 보안서약서 징구 시행

항목	2.6.6.원격접근통제
인증기준	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애 대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.

11번가(주)
11번가 임직원 재택근무 보안 서약서 등의안내

재택근무 보안 서약서

나는 11번가 주식회사(이하"회사"라함)의 임직원으로 재택근무를 수행함에 있어, 아래 사항을 충분히 숙지하고 성실히 이행하겠습니다.

1. 나는 재택근무 시 업무 수행에 적합한 독립적인 공간에서 업무를 수행하겠습니다.
2. 나는 회사에서 제공한 업무 단말(PC)은 업무 목적으로만 사용하고 개인적인 용도로 절대 사용하지 않겠습니다.
3. 나는 재택근무 수행 중 열람, 작성, 저장한 문서는 철저히 관리하고, 이를 외부로 유출하지 않겠습니다.
4. 나는 회사로부터 업무 수행을 목적으로 부여된 ID, Password 등 중요 정보가 외부로 유출되지 않도록 철저히 관리하겠습니다.
5. 나는 주요 직무를 수행하는 주요 직무자(개인정보 등 중요정보 취급자)일 경우 위 사항들에 대해 보다 엄격히 준수하며 정보유출 등 보안사고가 발생하지 않도록 보안 의식을 갖고 각별히 주의하도록 하겠습니다.

년 월 일

사 번 :

소 속 :

서 약 자 :

십일번가 주식회사 귀중

서약하기

지금 당장 할 수 있는 것을 찾자

매월 시행 중인 정보보안의 날에 재택 근무 관련 보안 가이드를 지속적으로 안내

2020.02.28 (금) 오후 03:36:07 | 영구 게시글

02월 정보보안의 날 시행(VPN 보안 정책 안내)

안호찬 (정보보안팀) 186 2

★ 즐겨찾기 URL 복사 👍 좋아요

안녕하세요, 정보보안팀입니다.

정보보안팀에서는 매월 마지막주 금요일을 "정보보안의 날"로 지정하고 있습니다.

"정보보안의 날" 시행목적은 우리 회사의 중요 정보 자산을 보호하기 위한 활동으로 정보보호의 중요성을 인식하고 보안 준수를 위한 가이드를 제공함으로써 실질적인 정보보안 수준을 강화하기 위한 전사적인 활동입니다.

정보보안의 날 시행안내

- 시행일 : 매월 마지막 주 금요일(2월 28일)
- 시행목적 : Compliance 규정 준수 및 안전한 보안 문화 정착

이번 2월 정보보안의 날에는 재택근무 시행에 따라 관련 보안 정책 관련 내용을 공유 드립니다.
내용을 참고하셔서 보안강화 실천에 적극적으로 동참해주시길 부탁 드리겠습니다.

[재택 근무 시 보안 대책 안내]

코로나19로 인해 재택 근무가 증가함에 따라 불안감을 악용하는 피싱·스미싱 시도 등의 보안 위협도 증가할 것으로 예상됩니다.

이에 따라 보안 위협에 대한 피해를 줄이기 위해 보안 대책을 공지 드리니 적극 참여를 부탁 드리겠습니다.

[VPN 보안 정책 안내]

2020.03.27 (금) 오후 06:54:24 | 영구 게시글

03월 정보보안의 날 시행(원격근무 보안 가이드)

안호찬 (정보보안팀) 220 0

★ 즐겨찾기 URL 복사 👍 좋아요

안녕하세요, 정보보안팀입니다.

정보보안팀에서는 매월 마지막주 금요일을 "정보보안의 날"로 지정하고 있습니다.

"정보보안의 날" 시행목적은 우리 회사의 중요 정보 자산을 보호하기 위한 활동으로 정보보호의 중요성을 인식하고 보안 준수를 위한 가이드를 제공함으로써 실질적인 정보보안 수준을 강화하기 위한 전사적인 활동입니다.

정보보안의 날 시행안내

- 시행일 : 매월 마지막 주 금요일(3월 27일)
- 시행목적 : Compliance 규정 준수 및 안전한 보안 문화 정착

이번 3월 정보보안의 날에는 재택근무 연장에 따라 관련 보안 정책 관련 내용을 다시 한번 공유 드립니다.
내용을 참고하셔서 보안강화 실천에 적극적으로 동참해주시길 부탁 드리겠습니다.

[원격근무 보안가이드]

코로나19 바이러스 확산으로 원격근무를 진행함에 따라 재택PC로 업무 하는 등 업무장소, PC환경의 변화가 발생하게 됩니다.

원격 근무 기간 동안 내부정보가 안전하게 관리 될 수 있도록 "원격근무 보안 가이드" 안내 드리오니 정보유출이 발생하지 않도록 숙지하여 업무 부탁 드립니다.

[원격근무 보안 가이드]

모의 훈련을 강화하자

최대한 실제와 유사한 콘텐츠로 모의 훈련을 지속적으로 시행

훈련 내용

- 모의훈련 일시 : 00/00 ~ 00/00
- 모의훈련 대상 : 전사구성원 총 0,000명

Scan Data from FX-1C7D2248ECA7



xerox <scandata@gmail.com>

받는 사람: [redacted]

Sent by: [redacted]

Number of Images: 1

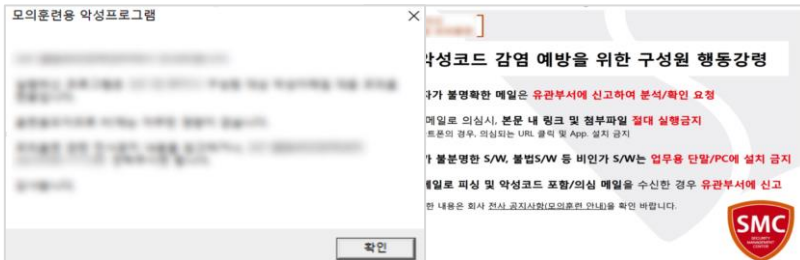
Attachment File Type: PDF

Download Link: [click here](#)

Device Name: Xerox AperosPort-V C3570

Device Location: Document Server

* 링크를 클릭하면 실행파일을 받게 되며, 실행 할 경우 메시지 발생



악성메일 대응



① 의심 메일 신고



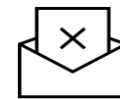
② 보안관제실 검토



③ 메일 열람 여부 확인



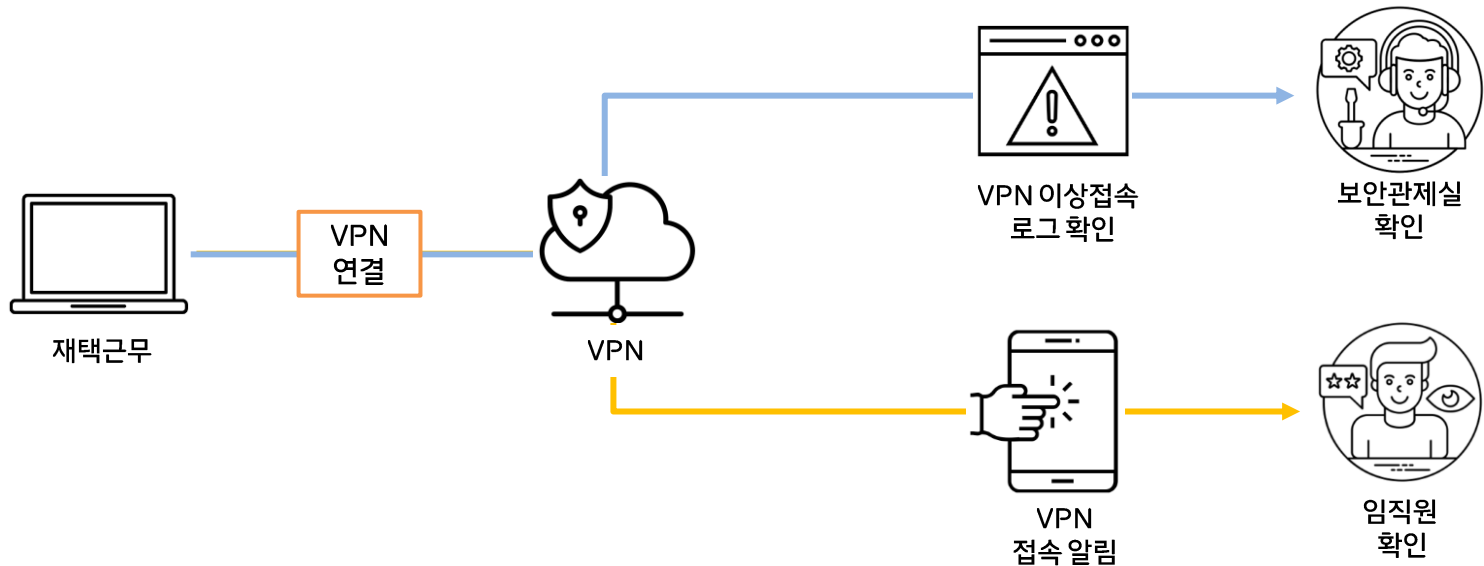
메일 열람



메일 삭제

모든 구성원을 보안 관제 요원으로

보안관제를 통해 이상징후 시나리오에 따른 모니터링을 하던 것에서 전사 구성원이 직접 모니터링 할 수 있도록 개선함



보안알리미 APP 23:25

VPN 접속 이력이 확인되었습니다

접속 결과: 접속 성공

Hostname: [Redacted]

세션 ID: e7c50d36

접속 시간: 2022-11-14 23:24:14

근무 시작: 2022-11-14 09:30

접속 위치: [Redacted] [South Korea]

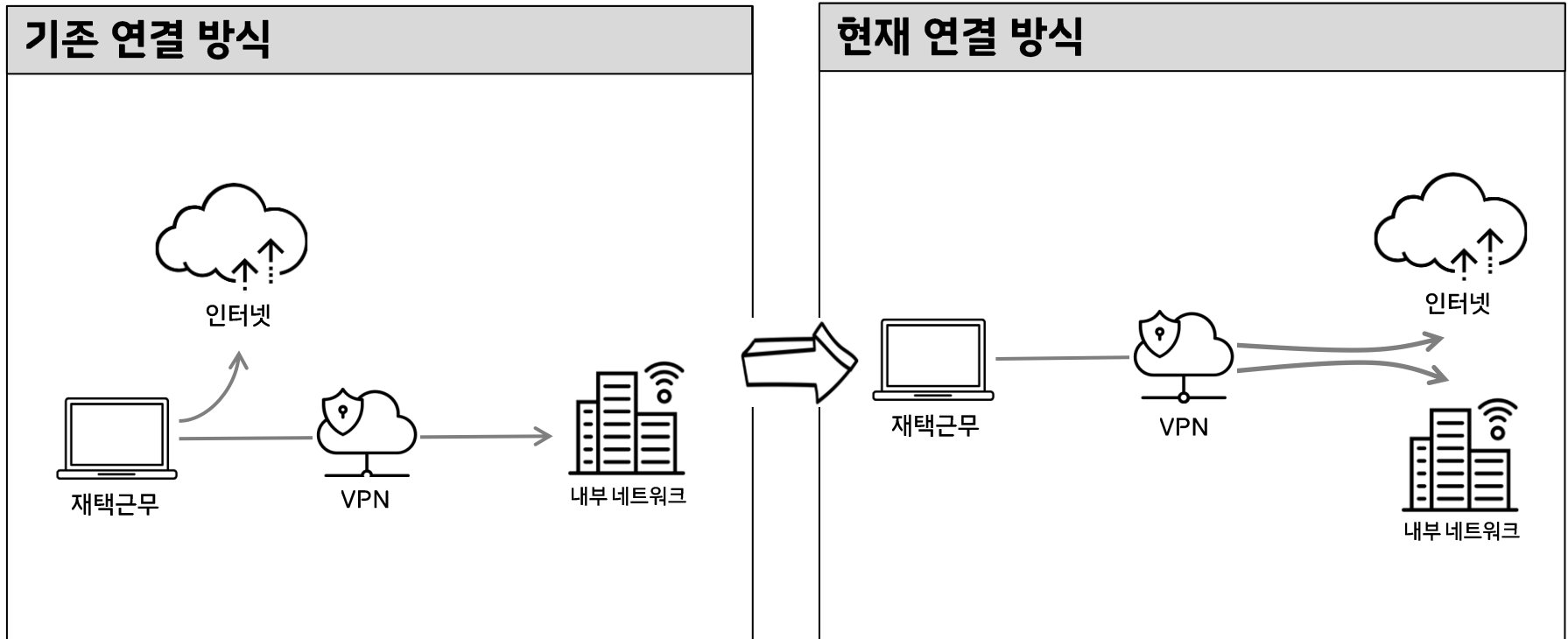
※원격(재택) 근무는 VPN접속 시간을 참고합니다.

본인이 접근한 이력이 아니라면 신고해주세요!

신고하기

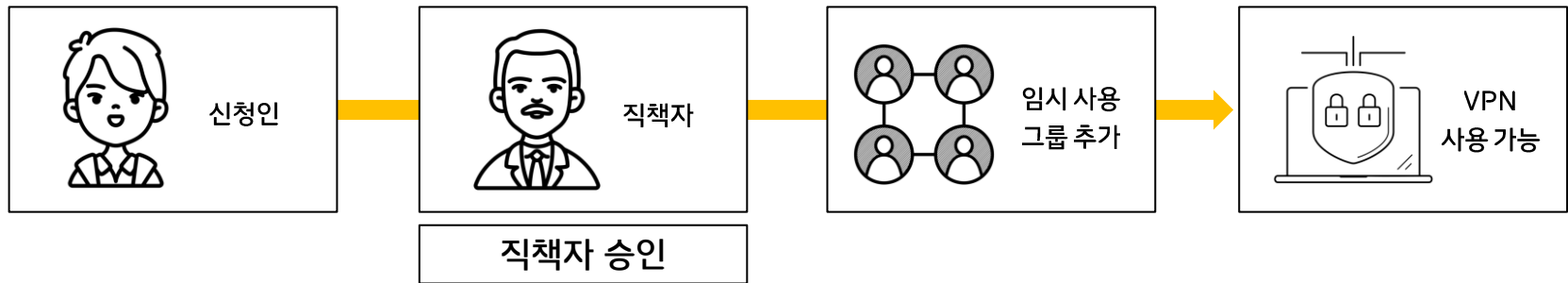
VPN 연결 방식을 전환하자

VPN 연결방식을 Split Tunneling 에서 Full Tunneling 으로 변경



VPN에 승인 기능을 적용해보자

외부에서 긴급하게 VPN 사용이 필요한 경우에는 VPN 사용 신청 시스템을 통해 직책자 승인 후 사용



11번가

VPN 사용 승인 요청 시스템

ID
사번을 입력해주세요

비밀번호
비밀번호를 입력해주세요

로그인

11번가

VPN 사용 승인 요청 시스템

신청기간
2022-11-15 ~ 2022-11-15 00 시 까지 사용됩니다.

신청 시스템
 11번가 VPN
 PAY VPN

신청사유

신청하기

[VPN 사용 신청 시스템]

VPN APPROVE APP 13:26

'조현주'님께서 VPN 사용 요청을 했습니다.

[신청시스템] 11번가 VPN

[신청사유] 업무 테스트 목적으로 신청합니다.

[사용기간] 2022.11.21 ~ 2022.11.21 (PM 2시 까지 사용)

요청일시: 2022년 11월 21일 13시 26분

[신청시스템] PAY VPN

[신청사유] 사용자 문의 이슈 지원

[사용기간] 2022.10.27 ~ 2022.10.27 (PM 3시 까지 사용)

요청일시: 2022년 10월 27일 14시 45분 승인일시: 2022년 10월 27일 15시 17분

[VPN 사용 신청 승인/결과 안내]

내/외부 위협을 보호하자

패턴 방식을 포함한 샌드박스 기반의 악성코드 탐지 방식을 보완하고 즉시 조치 및 분석이 가능한 플랫폼(EDR)을 도입



악성코드 실행
이력에 대한
가시성 부족

악성코드 탐지 전
수행한 실행 이력 및
변경사항에 대한
가시성 확보 불가



알려지지 않은
악성코드
탐지 불가

시그니처 기반의
한계로 알려지지 않은
악성코드
탐지 불가



PC
상세 분석 시
어려움

악성코드 감염
PC 분석 시
해당 장비
미회수 시 분석 불가



실시간 모니터링
및 대응 부재

사내망(VPN)
미 연결 시
사내 자산에 대한
모니터링 및 대응 불가

내/외부 위협을 보호하자

패턴 방식을 포함한 샌드박스 기반의 악성코드 탐지 방식을 보완하고 즉시 조치 및 분석이 가능한 플랫폼(EDR)을 도입



악성코드 실행

이력에 대한
악성코드에
대한 행위
분석 로그 제공

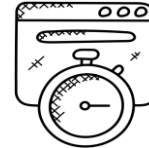
수행한 실행 이력 및
변경사항에 대한
가시성 확보 불가



알려지지 않은

악성코드
정적/동적 SI
기반의 엔진으로
위협 탐지

한계로 알려지지 않은
악성코드
탐지 불가



PC

원격 PC
분석을 위한
기능 제공

PC 분석 시
해당 장비
미회수 시 분석 불가



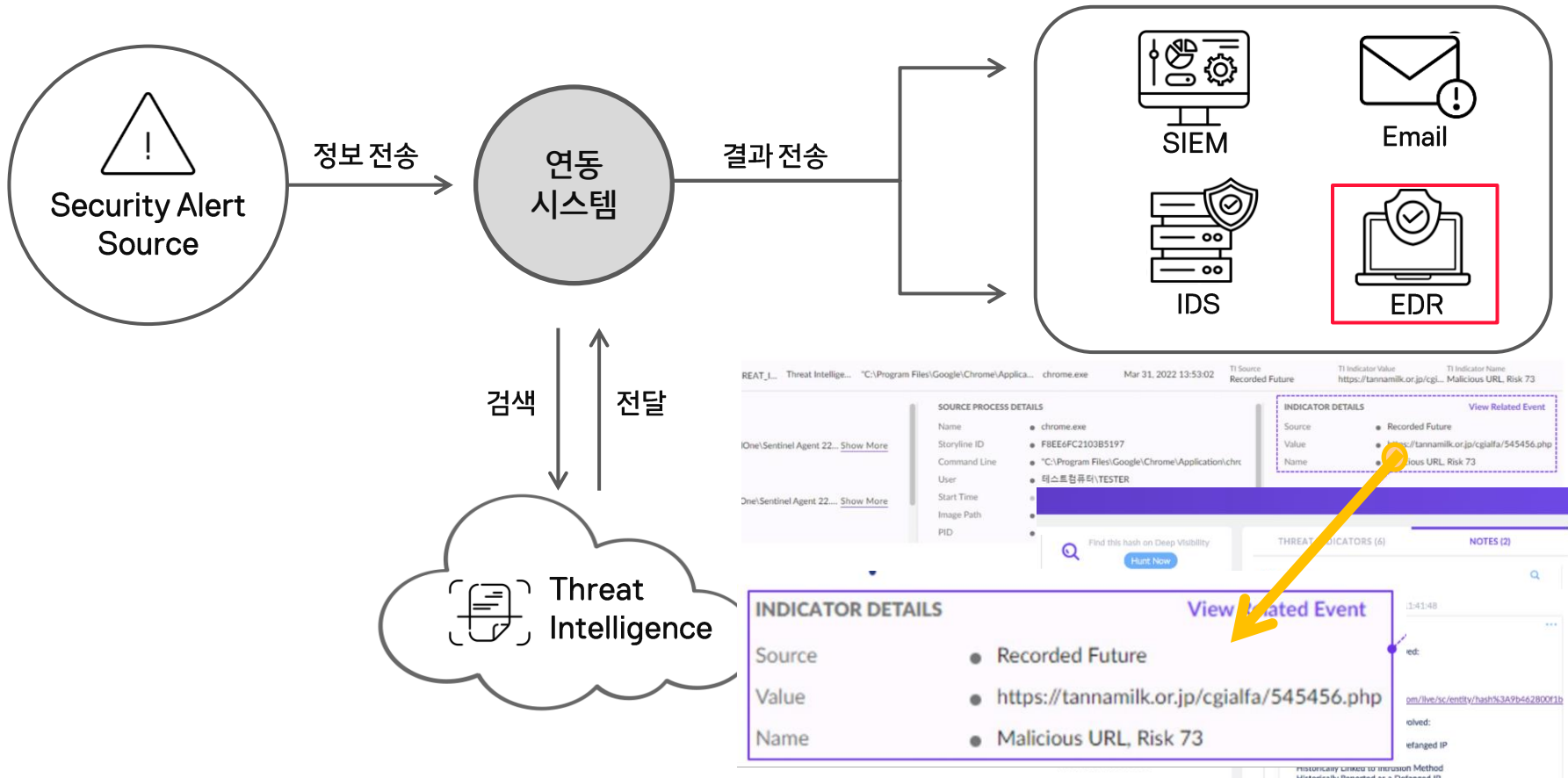
실시간 모니터링

클라우드 기반
운영으로
실시간 로그 수집

미 연결 시
사내 자산에 대한
모니터링 및 대응 불가

내/외부 위협 모니터링의 가시성을 높이자

보안 솔루션에서 발생하는 보안 이벤트에 TI 정보를 연동하여 탐지 로그 내용의 수준을 높임



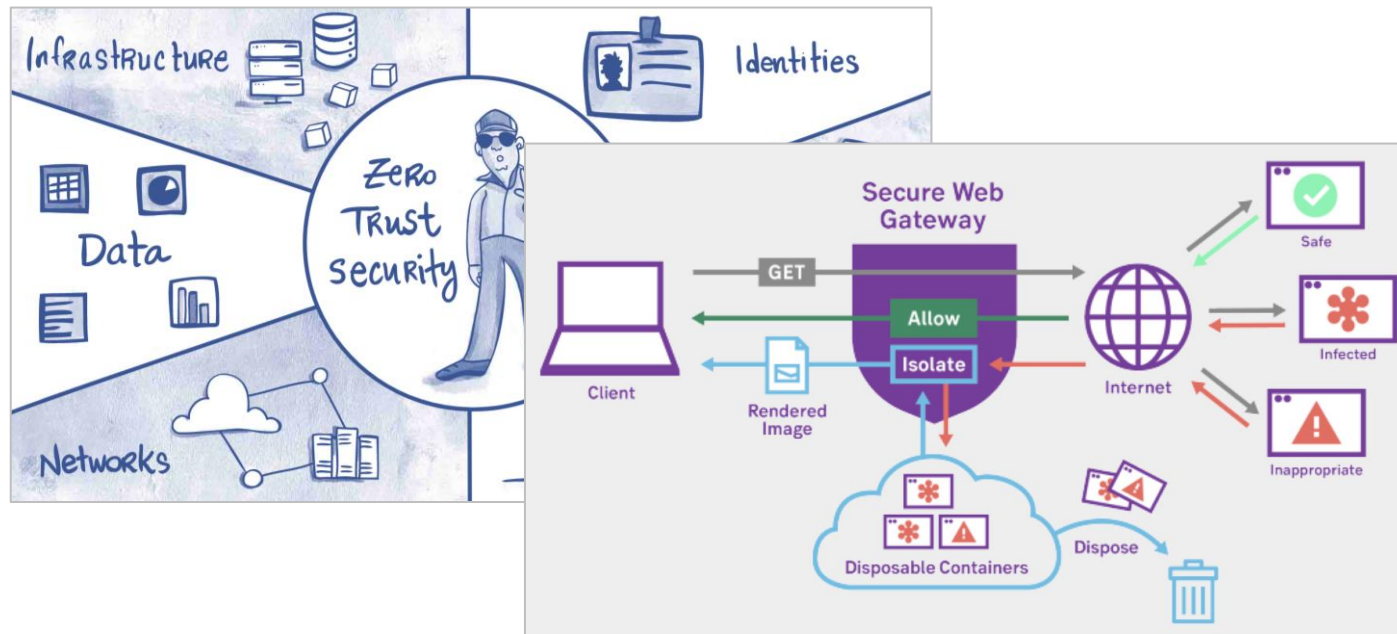
향후 도전 과제

제로트러스트 기반의 외부 접속 보안 수준 향상, 웹격리 보안을 통한 악성코드 유입 차단 등 검토 예정



향후 도전 과제

제로트러스트 기반의 외부 접속 보안 수준 향상, 웹격리 보안을 통한 악성코드 유입 차단 등 검토 예정



Q&A

Thank you