IBM Security

랜섬웨어 대응을 위한

IBM 솔루션 가이드

요즘 랜섬웨어(Ransomware) 대응에 대한 고민 많으시죠?
IBM은 랜섬웨어 대응 컨설팅부터 탐지/대응을 위한 솔루션까지
포괄적인 해결 방안 제시를 통해 고객 여러분들의 고민을 해결하고자 합니다.

▶ IBM 보안위협 진단 서비스 (랜섬웨어 대응 컨설팅)

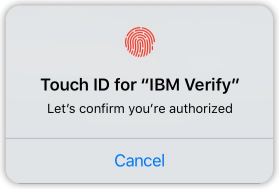
- ✓ 최종 사용자 교육
- ✓ 보안 구성 관리 및 점검

- 보안 정책 검토와 고도화
- 모의해킹, 악성메일 모의훈련, 사용자 PC 점검
- 보안 아키텍처 분석 및 마스터 플랜
- 임직원 보안 인식 교육 등

▶ Verify Access/Govern (인증, 계정 및 권한 관리 솔루션)

- ✓ 다단계 인증 사용
- ✓ 기본/ 초기 비밀번호 변경

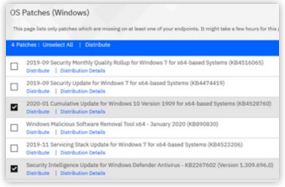
- 다중 요소 인증(모바일 OTP, 생체인증 등) 및 위험 기반 적응형 접근 통제
- 계정, 권한 및 패스워드 라이프사이클 관리



▶ MaaS360 (통합 엔드포인트 관리 솔루션)

- ✓ 패치 관리
- ✓ 최신 패턴의 안티바이러스 유지
- ✓ 플래쉬 삭제

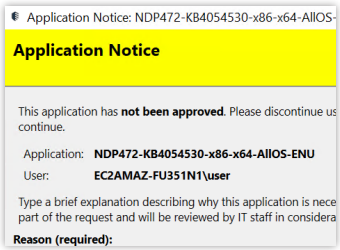
- 모바일, 윈도우, MacOS 운영 체제에 대한 패치 및 어플리케이션 관리
- 모든 엔드포인트 내 안티바이러스 운영 현황 관리
- 플래쉬 및 허용되지 않는 어플리케이션에 대한 일괄 삭제



▶ Verify Privilege Manager (S/W 화이트리스트 솔루션)

- ✓ 이메일 첨부 실행 파일 제거/ 차단
- ✓ Temp 폴더 내 프로그램 실행 제한
- ✓ WSH/플래쉬 비활성화

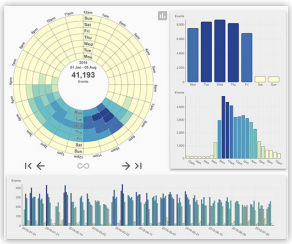
- Administrator 권한 사용 관리 및 통제
- 소프트웨어 실행에 대한 블랙리스트와 화이트리스트 관리
- 파워쉘 및 WSH(자바스크립트, VB스크립트 등) 사용 관리
- 미승인 S/W 실행 필요 시, 승인 절차 및 악성 여부 조사



▶ Verify Privilege Vault (시스템 접근 관리 솔루션)

- ✓ 시스템 접근에 대한 이상 행위 탐지 및 대응
- ✓ 데이터베이스 접근에 대한 이상 행위 탐지 및 대응

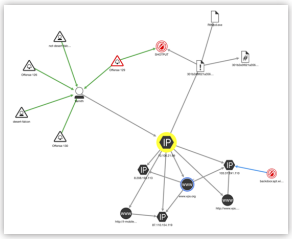
- 머신러닝 기반 시스템 접근에 대한 이상 행위 탐지 및 접근 관리 Guardium Data Protection (DB/Data 접근 관리 솔루션)
- 머신러닝 기반 DB, 파일, 빅데이터 등 Data 접근에 대한 이상행위 탐지 및 접근 관리



▶ QRadar SIEM (통합 보안 관제 솔루션)

- ✓ DNS 가시성 향상
- ✓ 위협 인텔리전스 정보 활용
- ✓ 인공지능 기반 위협 분석 및 대응

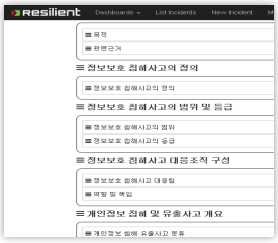
- 네트워크 가시성과 DNS Analyzer를 통한 DNS 위협 분석 및 이상 탐지
- 랜섬웨어 IOC 기반 탐지, 네트워크를 통한 확산, 그리고 의심스러운 행위와 사용자 분석
- 인공지능 기반 위협 분석 및 대응



▶ Resilient (보안 사고 대응 플랫폼)

- ✓ 랜섬웨어 발생 대비한, 업무 협업 채널 및 대응 프로세스 확립

- 기업 표준 및 정보보호 대응 지침 이행으로 랜섬웨어 대응 업무 자동화
- NIST, SANS, SOP 등 글로벌 표준 프로세스 제공
- 진척 및 이행 점검 등 정보보호 업무 형상 관리



랜섬웨어 대응을 위해 IBM의 컨설팅 및 솔루션에 대한 보다 구체적인 상담을 원하신다면,
아래로 연락 주시기 바랍니다.

서비스 및 솔루션 문의

한국IBM마케팅총괄본부 mktg@kr.ibm.com