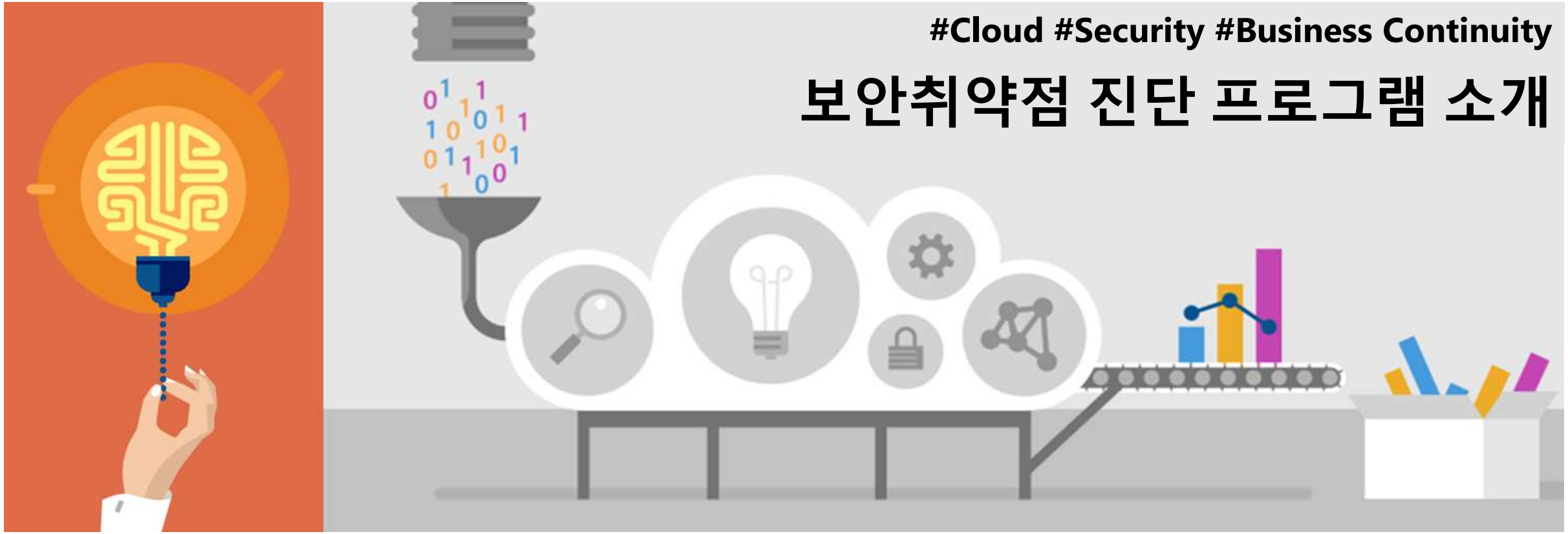


#Cloud #Security #Business Continuity

보안취약점 진단 프로그램 소개

Microsoft

QS solutions

One Commercial Partner
Solution Assessment Team
권은정
ejkwon@microsoft.com

보안취약점 진단 프로그램 개요

보안, 기업의 영원한 숙제

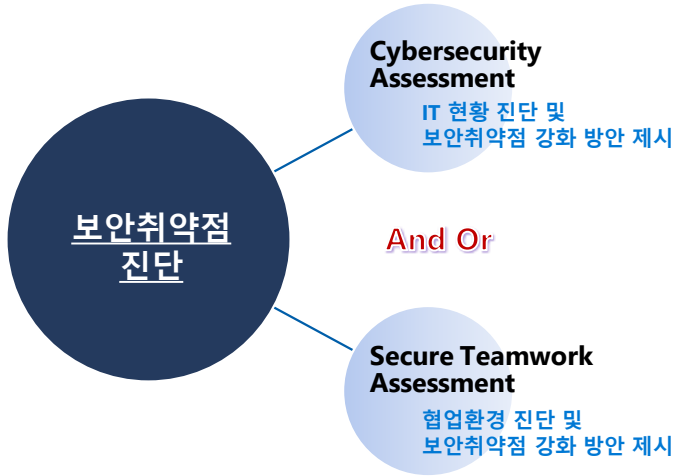
- 고객사의 많은 IT 비용이 보안대책을 수립하고 관련 솔루션을 도입하는데 사용되고 있음과 동시에, 사이버보안 공격은 더욱 지능화 되고 있어, 지속적인 보안취약점에 대한 대비가 필요합니다.
- 사이버보안 공격은 보안 강화된 방화벽을 공격하는 대신, 관리되지 않는 사용자 계정, 쉽게 설정된 암호, 최신 업데이트 되지 않은 소프트웨어, 관리되지 않는 서버 등 자주 간과되는 백도어를 통해 보안 침입이 발생합니다.
- 개인정보보호 및 기업주요정보 누출 등 사용자 Fault 로 인한 기업의 피해도 증가되고 있습니다.

온라인 협업, 재택 업무환경 주요 인프라

- COVID-19 확산으로 인해 최근 비즈니스 연속성 준비의 필요성이 대두되고 있습니다.
- 이에 대한 대비로 재택 혹은 원격근무를 위한 온라인 협업환경 도입 및 확대를 검토하는 기업이 늘어나고 있습니다.
- 안전한 원격업무 환경을 위해 최근 많은 보안전문가 혹은 관련 단체에서 사용자 및 IT 담당자가 지켜야 할 보안 수칙이 제시되고 있습니다.
- 증가된 온라인 협업환경에서는 사용자로 인한 기업의 정보유출, 맬웨어 감염 등 사이버보안 취약점도 함께 증가할 수 있어 이에 대한 대비도 함께 고려되어야 합니다.

보안취약점 진단, 보안위협 대비에 필수

- Microsoft에서 제공되는 "**보안취약점 진단 프로그램**"은 IT 인프라 및 협업 환경에 대한 보안취약점을 진단하고, 이를 기반으로 보안강화 방안에 대한 제언을 제공해 드립니다.
- 진단을 위한 IT 현황 수집 및 질의 인터뷰 결과를 기반으로 전체 **보안 성숙도 평가 및 보안 취약점 현황에 대한 조치방안을 권장** 하며, 실제 사이버보안 취약점으로 외부 공격의 타겟이 될 수 있는 상세 항목 제시하여 조치할 수 있도록 가이드 드립니다.
- 보안취약점 진단은 QS Solutions 사의 CSAT (Cyber Security Assessment Tool)을 활용하여 Microsoft에서 제공하는 **무료프로그램** 입니다.



참조: CSAT 소개동영상 (영문)

보안취약점 진단 절차 및 소요일정

0 프로그램 소개 및 진행방식 설명회 — 0일

고객사 준비사항
- ✓ 진행 담당자 미팅 참석

1 진단툴 준비 — 1일

고객사 준비사항
- ✓ CSAT Server (Windows Server or VM)
- ✓ Administrator Account
- ✓ Firewall Rules

2 데이터수집 및 질의 인터뷰 수행 — 3일차

고객사 준비사항
- ✓ 질의사항 리뷰
- ✓ 질의내용 Interviewee 담당자

3 진단결과 리포트 작성 — 7일차

고객사 준비사항
- ✓ NA

4 리포트 공유 및 제언 — 10일차

고객사 준비사항
- ✓ 최종리포트 리뷰
- ✓ Action Item 협의를 위한 IT/보안 담당자

- 고객사 Needs 및 일정에 따라 두 종류의 진단을 **동시 혹은 선택적으로 진행**가능

- 고객의 참여시간 및 리소스 최소화를 위해, 글로벌 차원에서 입증된 전문 진단툴을 활용하여 단기간에 데이터 수집이 가능
- **진단툴은 고객사 환경 내에 설치**되며 외부 유출되지 않음
- 언택트 방식으로 원격에서 수행 가능

- 국내 보안전문 파트너사와 함께 진단결과에 대해 사이버보안 취약점 강화방안에 대한 제언을 함께 제공

- 진단을 위한 환경 준비 및 본 진단과제를 함께 수행할 고객 담당자의 질의 인터뷰 일정에 따라 유동적이나, 리포트 공유 및 제언까지 **평균 2주 정도 소요**

Cyber security Assessment

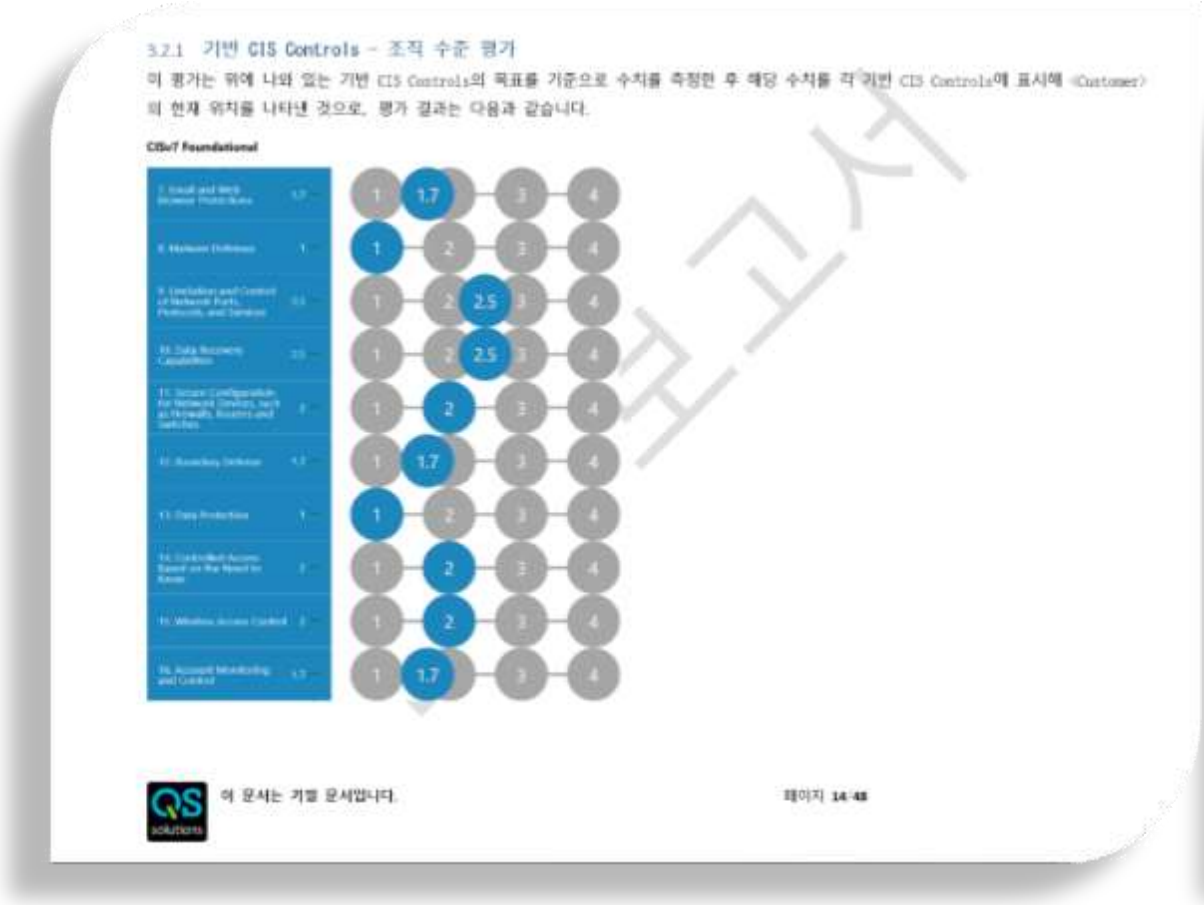
IT 현황 진단 및 보안취약점 강화 방안 제시

Secure Teamwork Assessment

협업환경 진단 및 보안취약점 강화 방안 제시

Cybersecurity Assessment – 진단항목 및 결과(예시)

- "사이버보안 진단 리포트"는 Center for Internet Security (CIS Controls v7.1) 기반으로 작성된 질의 인터뷰 결과를 기반으로 보안수준 평가 결과 및 개선을 위한 권장 사항을 제시합니다.



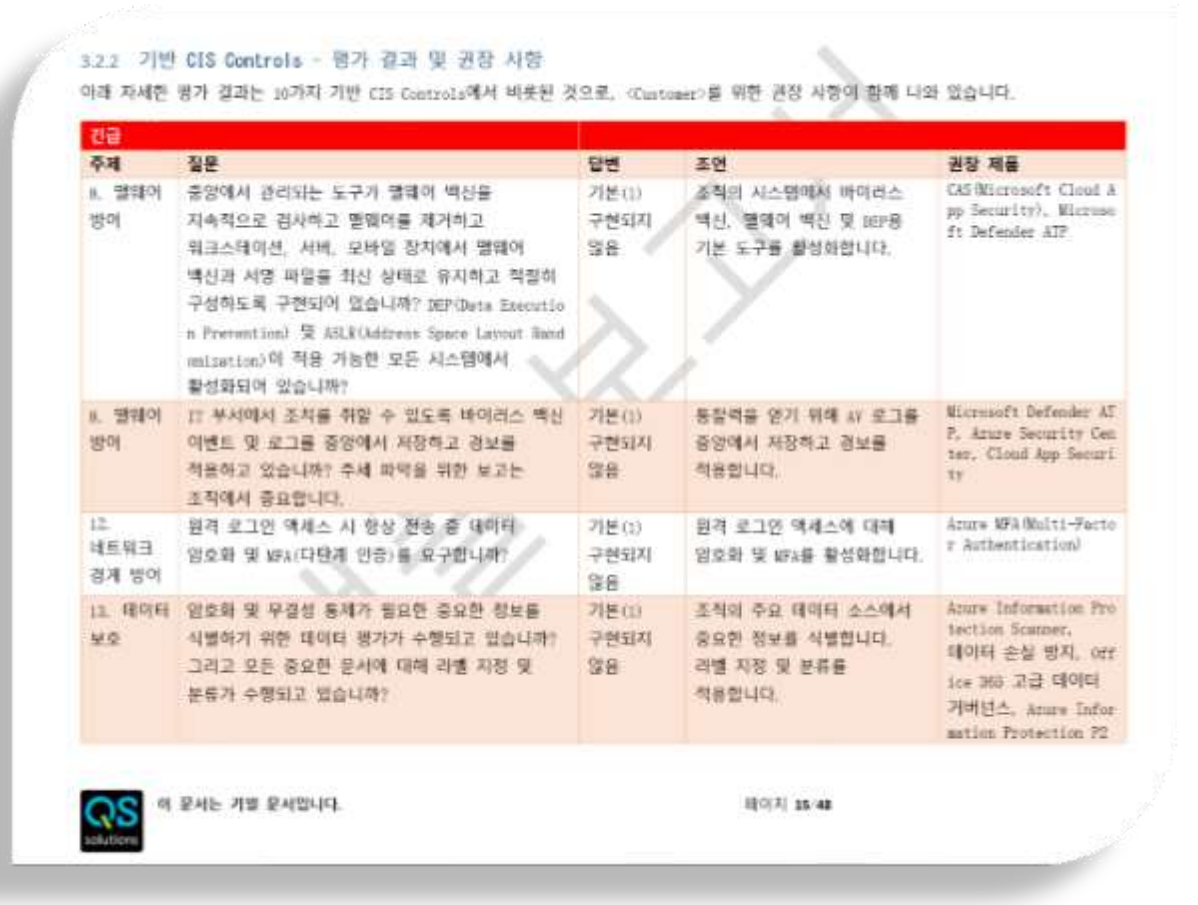
3.2.1 기반 CIS Controls - 조직 수준 평가

이 평가는 위에 나와 있는 기반 CIS Controls의 목표를 기준으로 수치를 측정한 후 해당 수치를 각 기반 CIS Controls에 표시해 〈Customer〉의 현재 위치를 나타낸 것으로, 평가 결과는 다음과 같습니다.

CISv7 Foundational

이 문서는 기밀 문서입니다.

페이지 14/48



3.2.2 기반 CIS Controls - 평가 결과 및 권장 사항

아래 자세한 평가 결과는 10가지 기반 CIS Controls에서 비롯된 것으로, 〈Customer〉를 위한 권장 사항이 함께 나와 있습니다.

긴급				
주제	질문	답변	조언	권장 제품
8. 멀웨어 방어	중앙에서 관리되는 도구가 멀웨어 백신을 지속적으로 검사하고 멀웨어를 제거하고 워크스테이션, 서버, 모바일 장치에서 멀웨어 백신과 서명 파일을 최신 상태로 유지하고 적절히 구성하도록 구현되어 있습니까? DEP(Data Execution Prevention) 및 ASLR(Address Space Layout Randomization)이 적용 가능한 모든 시스템에서 활성화되어 있습니까?	기본(1) 구현되지 않음	조직의 시스템에서 바이러스 백신, 멀웨어 백신 및 DEP용 기본 도구를 활성화합니다.	CAS(Microsoft Cloud App Security), Microsoft Defender ATP
8. 멀웨어 방어	감사 부서에서 조치를 취할 수 있도록 바이러스 백신 이벤트 및 로그를 중앙에서 저장하고 정보를 적용하고 있습니까? 추세 파악을 위한 보고는 조직에서 중요합니다.	기본(1) 구현되지 않음	통찰력을 얻기 위해 AV 로그를 중앙에서 저장하고 정보를 적용합니다.	Microsoft Defender ATP, Azure Security Center, Cloud App Security
12. 네트워크 경계 방어	원격 로그인 액세스 시 항상 전송 중 데이터 암호화 및 MFA(다단계 인증)를 요구합니까?	기본(1) 구현되지 않음	원격 로그인 액세스에 대해 암호화 및 MFA를 활성화합니다.	Azure MFA(Multi-Factor Authentication)
13. 데이터 보호	암호화 및 무결성 통제가 필요한 중요한 정보를 식별하기 위한 데이터 평가가 수행되고 있습니까? 그리고 모든 중요한 문서에 대해 라벨 지정 및 분류가 수행되고 있습니까?	기본(1) 구현되지 않음	조직의 주요 데이터 소스에서 중요한 정보를 식별합니다. 라벨 지정 및 분류를 적용합니다.	Azure Information Protection Scanner, 데이터 손실 방지, Office 365 고급 데이터 거버넌스, Azure Information Protection P2

이 문서는 기밀 문서입니다.

페이지 15/48

Cybersecurity Assessment – 진단항목 및 결과(예시)

- **"사이버보안 진단 리포트"는 수집된 IT 현황을 기반으로 전체 보안 취약점 현황을 분석하며 이에 대한 조치방안을 권장 합니다.**
  실제 사이버보안 취약점으로 외부 공격의 타겟이 될 수 있는 아래 항목들이 포함됩니다.

✓ **ID/PW 사용 및 관리현황**
: 90일 이상 로그인 하지 않은 장비, 관리 되지 않고 있는 Admin 권한

✓ **안전하지 않은 어플리케이션 설치 현황**
: 의심스러운 Publisher로 부터 배포된 어플리케이션

✓ **OS 현황 및 최신 업데이트 현황**
: 기술지원 종료 및 최신 업데이트 되지 않은 소프트웨어

✓ **엔드포인트의 보안 구성**
: 보안강화를 위한 보안 기술 적용 여부

✓ **맬웨어 방어를 위한 이메일 및 웹브라우저 보호**
: Antivirus의 최신 버전으로 업데이트 되지 않은 디바이스

✓ **개인정보 보호 포함된 파일 관리 현황**
: PII 정보가 포함된 파일의 위치

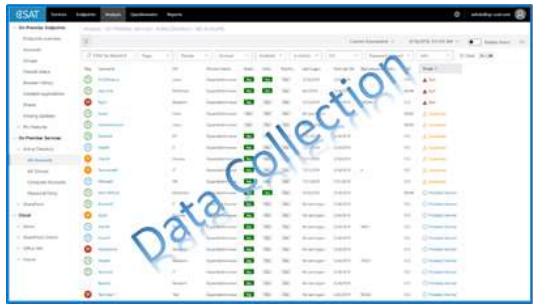
✓ **외부 공유된 사이트 현황**
: 협업을 위해 제3자와 공유중인 사이트 및 디렉토리

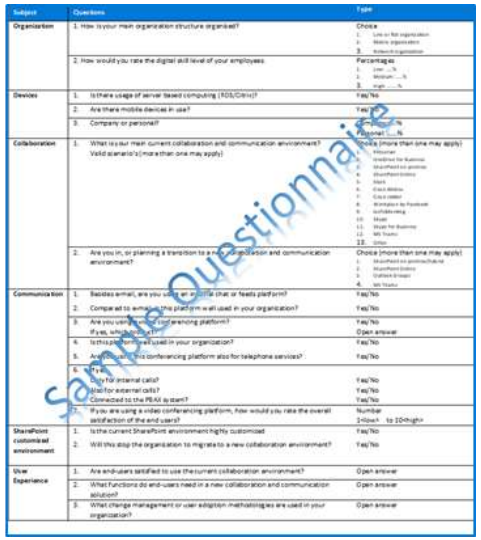
Secure Teamwork Assessment – 진단항목 및 결과(예시)

- **"Secure Teamwork 진단 리포트"**는 수집된 협업환경 현황을 기반으로 **보안 취약점 현황을 분석**하며 **안전한 협업환경 구축을 위한 조치방안을 권장** 합니다.

진단항목

- ✓ *임직원들이 안전하게 사내 인프라에 로그인 하고 있는지?*
- ✓ *임직원들이 내부 및 외부 협력업체들과 어떻게 협업하고 있는지?*
- ✓ *사내 데이터 혹은 자료들이 안전하게 저장 및 관리되고 있는지?*





진단결과 리포트

- ✓ *임직원들이 어떻게 내부 및 외부와 협업하고 있는지 실제 수집된 데이터로 인사이트 제공*
- ✓ *수집된 데이터 및 인터뷰 내용을 기반으로 보안강화에 필요한 조치와 함께 **Microsoft Teams**로 안전한 온라인 협업환경 구축 제언*
- ✓ *제언 내용을 실제 구축하기 위한 **Action plan** 제시*

보안취약점 진단 신청방식

- 저희 마이크로소프트와 국내 전문 파트너사가 함께 무료로 수행해 드리는 보안취약점 진단 프로그램을 담당 Microsoft 영업에게 신청해 주시면 대면 혹은 비대면 형식의 미팅을 통해 진단 범위, 일정, 기대효과 등에 대해 상담 드립니다.

상담
- 프로그램 이해
- 결과기대치 협의

신청
- 진단범위 협의
- LOE 동의 (*)
- 진단신청 (by MS 영업)

진단 Kick-Off
- 파트너사 지정
- Agent 설치
- 데이터수집

(*) Letter of Engagement는 진단목적, 범위, 일정 등이 포함된 문서로 진단진행에 대한 고객사 동의를 받기 위함 입니다.

참고) 보안취약점 진단 프로그램 준비사항

- **CSAT 서버 권장 설치 요구 사양**
  - ✓ 운영체제 : Win 10 Pro 또는 Enterprise 1709 이상 , Win Server 2019 또는 2016
  - ✓ H/W : CPU(4 cores 이상), Memory(16GB 이상), SSD(80GB 이상의 여유공간)
  - ✓ S/W : .NET Framework v4.6 이상

- **네트워크 Port 설정**

Port 번호	TCP, UDP	사용 내역
443	Outbound TCP	Office 365, SharePoint Online 과 Azure AD 스캔
8080	Inbound TCP	배포 서비스, 임시 에이전트(dissolvable agent) 배포에 사용
4432	Inbound TCP	CSAT Portal 용, 발신 트래픽 없음
8018	Inbound TCP	열거 서비스(Enumeration service) 용, 발신 트래픽 없음
8090	Inbound TCP	분석 서비스(Analysis service) 용, 발신 트래픽 없음
8288	Inbound TCP	네트워크 서비스(Network service) 용, 발신 트래픽 없음

- **단말장치(Endpoint, Workstation 및 Laptop) 스캔 가능 사양**
  - ✓ 방화벽 세팅
    (AD 미사용시 - 제공되는 스크립트 배포)

방화벽 규칙 명	그룹	허용 포트 번호
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	139
File and Printer Sharing (SMB-In)	File and Printer Sharing	445
Remote Scheduled Tasks Management (RPC)	Remote Scheduled Tasks Management	RPC Dynamic Ports
Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation	135
Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation	All (only allow svchost.exe)

  - ✓ S/W
    : .NET Framework v3.0 이상(Windows Server 2008 (R2)과 Win 7의 기본 .NET 버전 : 2.0)
    : 안티바이러스 세팅 : C:\windows\temp 에서 CSAT.exe 실행 가능
  - ✓ 관리자 계정 (Local Admin Account) : AD 사용시 - 기본 관리자 계정 (ID & PW) / AD 미사용시 - 제공되는 스크립트 배포

- **클라우드 / Active Directory** : 테넌트의 관리자 계정 (ID & PW) / Active Directory 관리자 계정 (ID & PW)

Microsoft

THANK YOU

Nothing can stop a team.
Work remotely with Microsoft Teams.