CLOUDZEN × Microsoft 365

CSAT(Cyber Security Assessment Tool) 소개

powered by ZENITH & COMPANY

CSAT(Cyber Security Assessment Tool) 이란 무엇인가 ?

- "**사이버보안 진단 프로그램**"은 기업의 IT 현황 및 보안성숙도, 보안취약점에 대한 인사이트를 제공함과 동시에 사이버보안 위협을 경감시키고 대체하기 위한 방안추천 및 적용 가능 기술을 제언해 드리는 **무료프로그램** 입니다.

1. 진단툴 준비
2. 데이터수집 및 질의 인터뷰 수행
3. 진단결과 리포트 작성
4. 리포트 공유 및 제언

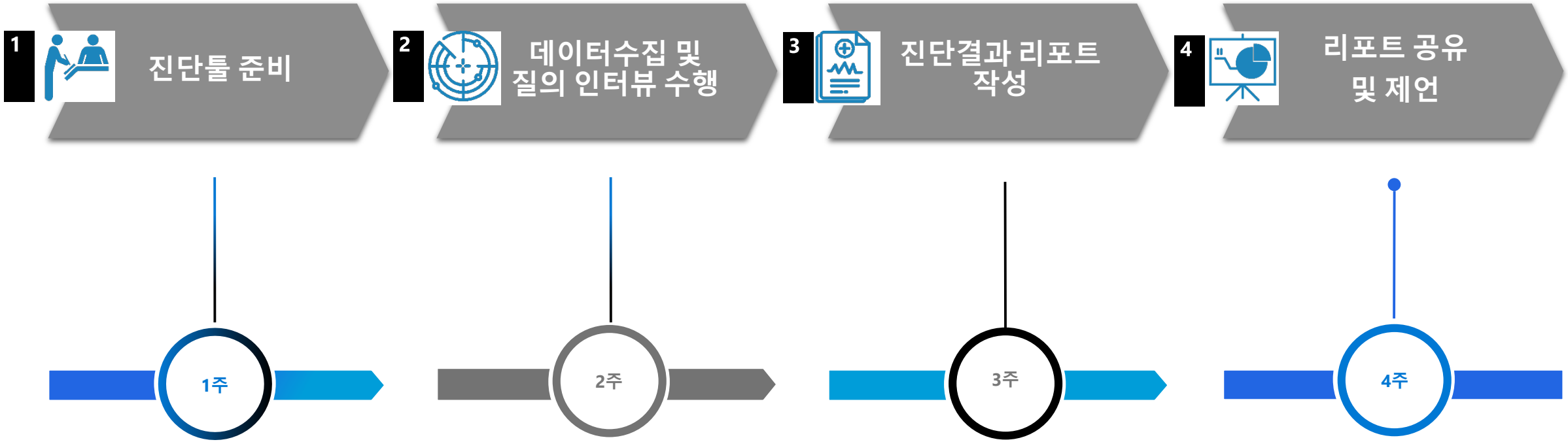
- "**사이버보안 진단 프로그램**"은 고객의 참여시간 및 리소스 최소화를 위해, 글로벌 차원에서 **입증된 전문 진단툴을 활용**하여 단기간에 데이터 수집 및 결과 리포트를 작성하여, **글로벌 보안전문 파트너사와 함께** 진단결과에 대해 사이버보안 취약점 강화방안에 대한 제언을 함께 제공해 드립니다.

1) *사이버보안 진단툴은 QS Solutions 사의 CSAT (Cyber Security Assessment Tool)을 활용하며, 상세한 내용은 소개동영상(영문) 참조*

2) *사이버보안 진단툴은 고객사 내에 Windows Server / Windows Workstation에 설치되며, 엔드포인트 및 네트워크 접근 체크*

CSAT(Cyber Security Assessment Tool) 프로세스

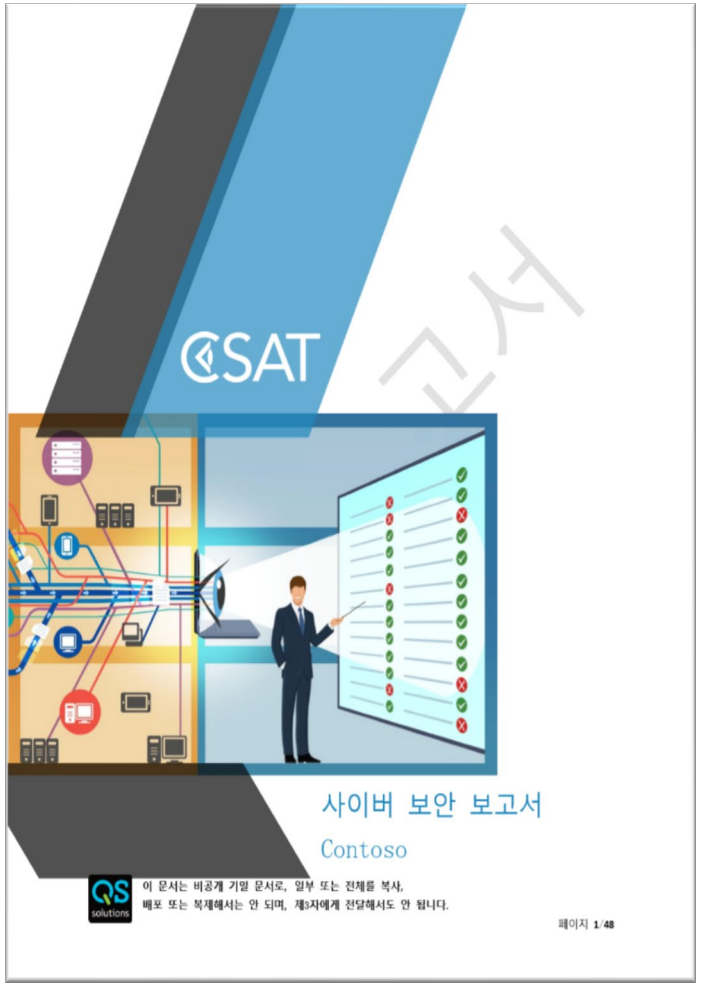
- "**사이버보안 진단**"은 진단을 위한 환경 준비 및 본 진단과제를 함께 수행할 고객 담당자의 질의 인터뷰 일정에 따라 유동적이나, 리포트 공유 및 제언까지 **최소 5일, 최대 2주 정도 소요** 됩니다.

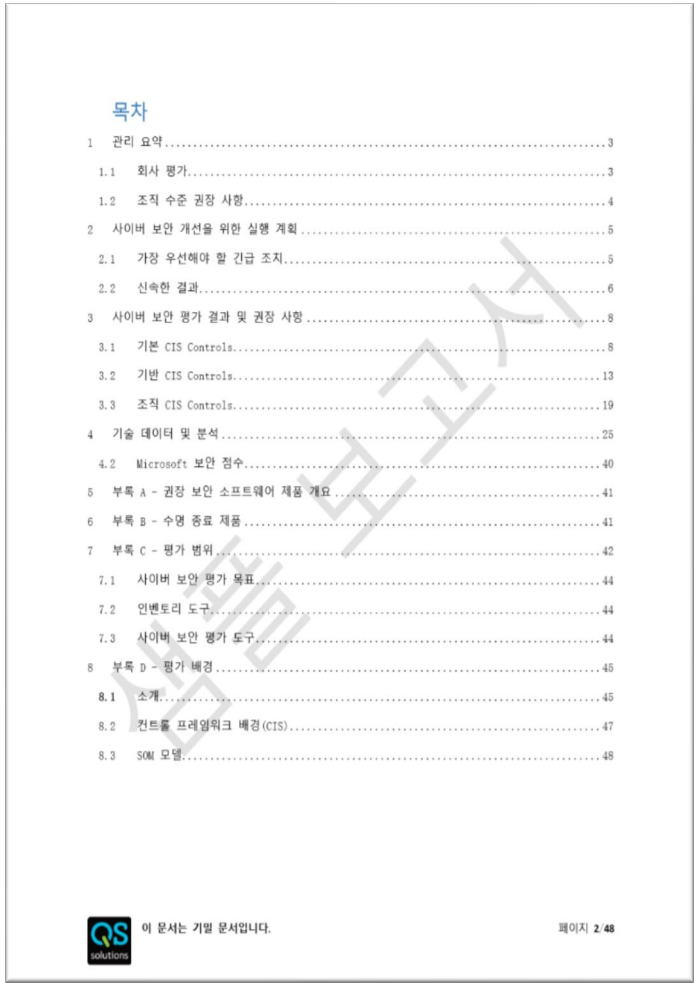


사이버보안 진단 리포트 예시

- "**사이버보안 진단 리포트**"는 수집된 IT 현황과 질의 인터뷰 결과를 기반으로 전체 **보안 성숙도 평가 및 보안 취약점 현황에 대한 조치방안을 권장**하며, 아래 영역의 내용들이 포함됩니다.

✓ 소프트웨어/하드웨어 자산의 인벤토리 작성 및 통제
✓ 지속적인 취약점 관리 (백신 최신 업데이트 현황 등)
✓ 관리 권한 사용 통제
✓ 엔드포인트의 보안 구성
✓ 맬웨어 방어, 이메일 및 웹브라우저 보호
✓ 데이터 보호 및 복구 기능
✓ 계정 모니터링 및 통제
✓ 데이터 거버넌스
✓ 감사 로그 유지관리, 모니터링 및 분석





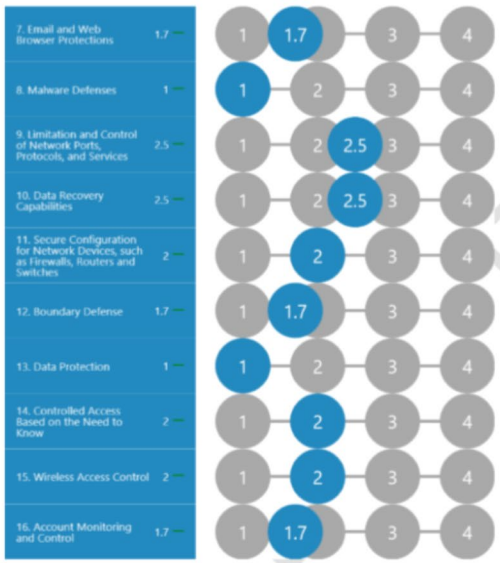
사이버보안 진단 리포트 예시

- "**사이버보안 진단 리포트**"는 보안수준 평가 결과 및 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



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. 맬웨어 방어	중앙에서 관리되는 도구가 맬웨어 백신을 지속적으로 검사하고 맬웨어를 제거하고 워크스테이션, 서버, 모바일 장치에서 맬웨어 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, 맬웨어 백신 및 DEP용 기본 도구를 활성화합니다.	CAS(Microsoft Cloud App Security), Microsoft Defender ATP
8. 맬웨어 방어	IT 부서에서 조치를 취할 수 있도록 바이러스 백신 이벤트 및 로그를 중앙에서 저장하고 경보를 적용하고 있습니까? 추세 파악을 위한 보고는 조직에서 중요합니다.	기본(1) 구현되지 않음	통찰력을 얻기 위해 AV 로그를 중앙에서 저장하고 경보를 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

사이버보안 진단의 필요성

사이버보안 위협에 대처하기 위해 **맬웨어 방지, 방화벽 솔루션, 보안 컨설팅 등에 많은 비용을 소비하고 있음에도 불구하고, 신종 사이버보안 공격 및 관리상의 이슈로 보안적 취약점이 존재**할 수 있습니다.

포비스에 따르면, **2021년까지 전 세계 사이버범죄 피해 규모가 6조 달러**($6 trillion)에 이를 것으로 예상됩니다. 또한 개인정보보호 누출로 인한 기업의 피해도 증가하고 있습니다.

사이버범죄는 보안강화된 방화벽을 공격하는 대신, **지원되지 않거나 승인되지 않은 소프트웨어, 관리되지 않는 사용자 ID, 쉽게 설정된 암호, IT 조직에서 관리되지 않는 서버 등 자주 간과되는 백도어를 통해 보안 침입**이 이루어지게 됩니다.

Source) Harvard Business Review / March 28, 2018

"관리되지 않는 소프트웨어, 서버, ID/PW 등은 보안적으로 보호될 수 없기 때문에, 회사 내에 어떤 솔루션/시스템이 구축되어 누가 어떻게 사용하고 있는지, 최신 버전으로 업데이트 되어 있는지, 개인정보보호가 잘 지켜지고 있는지 등 전반적인 인프라스트럭처 및 사용에 대한 정보가 관리되어야 합니다. 이를 기반으로 사이버보안 상의 취약점이 어디에 존재하는지를 진단하고, 이에 대한 대응 및 조치를 할 수 있어야 합니다."

CSAT(Cyber Security Assessment Tool)의 4가지 포인트

Cybersecurity

사이버 보안 인프라를 포괄적으로 분석하고 사이버 위험 감소를 위한 올바른 프로세스를 수립할 수 있도록 제언합니다.

MS Cloud Security

Microsoft의 뛰어난 Cloud Security서비스를 활용할 수 있는 전략과 방안을 제시합니다.

Security Management

복잡한 보안 환경의 관리를 좀 더 쉽고 명확한 관리를 할 수 있게 전략과 방안을 제시합니다.

Cloud Change Management

클라우드로의 변화 과정에서 발생하는 보안 이슈를 강화된 보안으로의 변화 관리 방안을 제시합니다.

Key Message

현재 수많은 보안 이슈들이 동시 다발적으로 발생하고 이를 처리하기 위해 많은 수의 솔루션들이 도입, 검토되고 있습니다.
MS에서 제공하는 Cyber Security Assessment을 통해 보안 강화와 관리 축소를 하기 위한 전략과 방안을 제시합니다.

감사합니다.

CLOUDZEN

Microsoft Partner
Microsoft

2019 Partner of the Year Winner
Korea

Microsoft Partner
Microsoft

Gold DevOps
Gold Data Analytics
Gold Cloud Platform
Gold Application Development
Gold Small and Midmarket Cloud Solutions

Microsoft Partner
Microsoft

Gold Datacenter
Gold Cloud Productivity
Gold Windows and Devices
Gold Collaboration and Content
Gold Enterprise Mobility Management

고객의 성공을 위한

The right partner, The right solution

클라우드젠

서울특별시 강남구 테헤란로16길17 제니스빌딩 9층-11층 06235
marketing@zenithn.com

powered by ZENITH & COMPANY