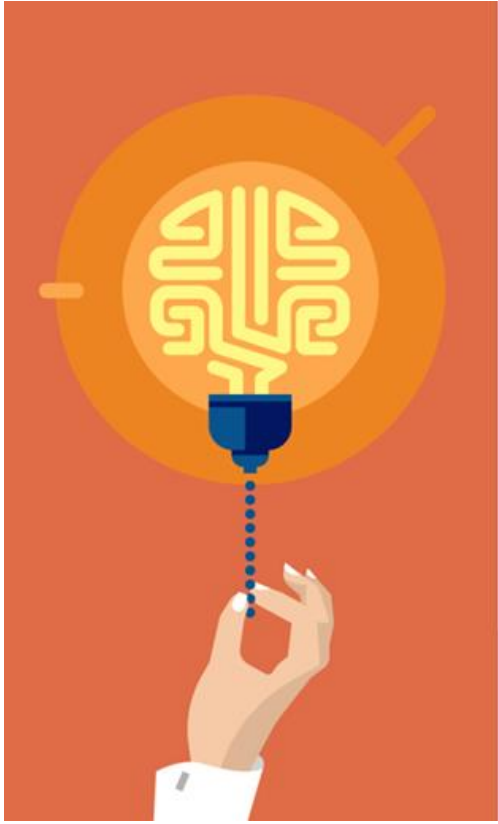
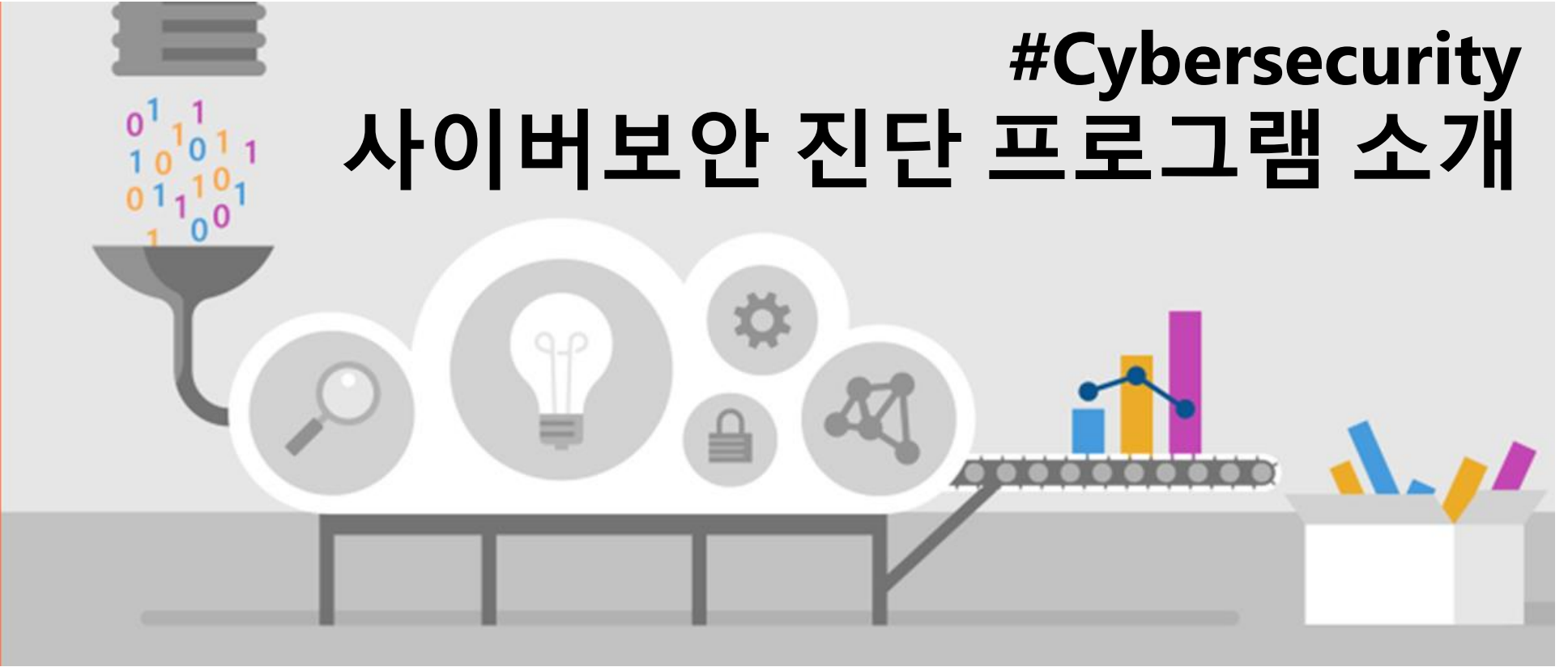




#Cybersecurity 사이버보안 진단 프로그램 소개



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 존재할 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 침입이 이루어 지게 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 인프라 트럭처 및 사용에 대한 정보가 관리되어야 합니다.** 이를 기반으로 **사이버보안 상의 취약점이 어디에 존재하는지를 진단하고, 이에 대한 대응 및 조치를 할 수 있어야 합니다.**”

사이버보안 진단 프로그램



- “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.



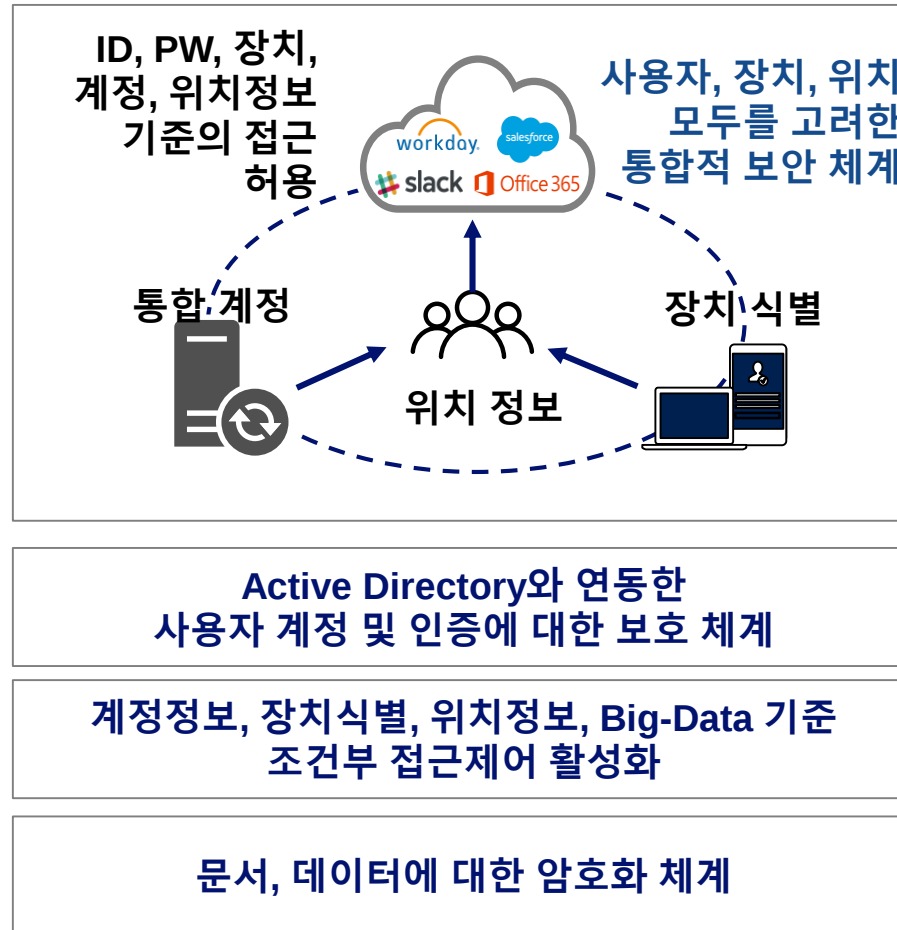
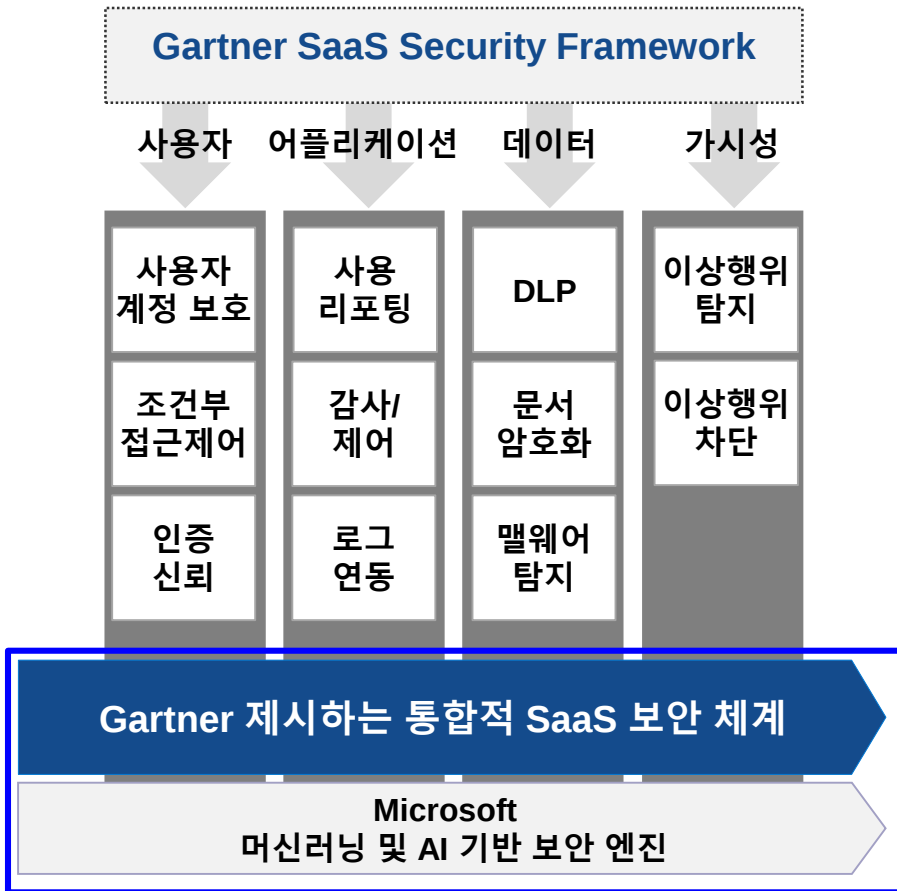
- “사이버보안 진단 프로그램”은 고객의 참여시간 및 리소스 최소화를 위해, 글로벌 차원에서 **인증된 전문 진단툴을 활용**하여 단기간에 데이터 수집 및 결과 리포트를 작성하여, **국내 보안전문 파트너사와 함께** 진단결과에 대해 사이버보안 취약점 강화방안에 대한 제언을 함께 제공해 드립니다.



- 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 Workstation 에 설치되며, 엔드포인트 및 네트워크 접근 체크

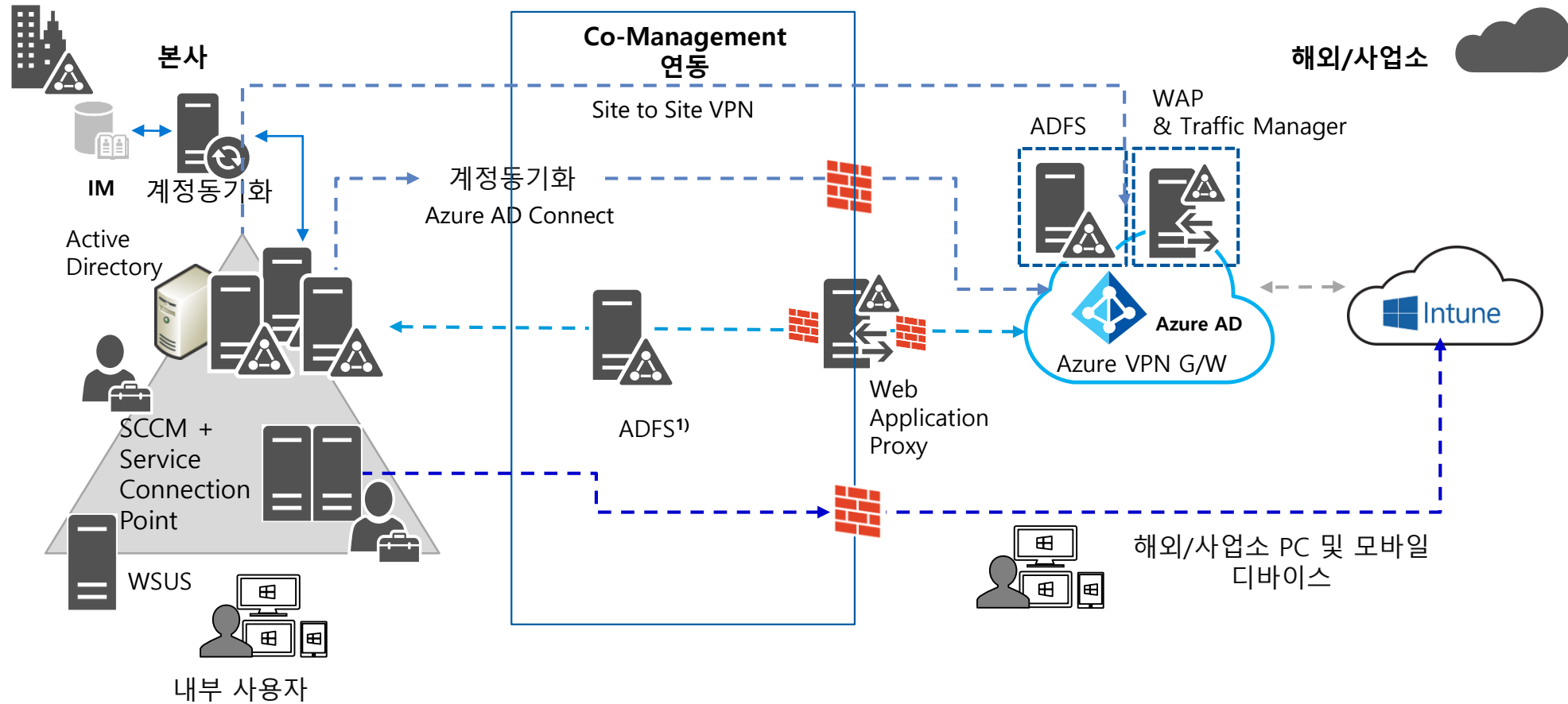
사이버보안 진단 프로그램

가트너에서 제시하는 SaaS 보안 Framework를 토대로 인프라 보안 고도화 방안을 제시합니다.



사이버보안 진단 프로그램

단말의 위치에 관계없이 동일한 통합 보안관리 환경을 구현하기 위한 클라우드 통합 Co-Management 환경 구성은 다음과 같습니다.



*내부 VPN Connector 필요 (Site to Site VPN 지원)

1) ADFS : Active Directory Federation Service (인증 페더레이션)

사이버보안 진단 리포트 예시



- “사이버보안 진단 리포트”는 수집된 IT 현황과 질의 인터뷰 결과를 기반으로 전체 **보안 성숙도 평가 및 보안 취약점 현황에 대한 조치방안**을 권장하며, 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



목차	
1	관리 요약..... 3
1.1	회사 평가..... 3
1.2	조직 수준 권장 사항..... 4
2	사이버 보안 개선을 위한 실행 계획..... 5
2.1	가장 우선해야 할 긴급 조치..... 5
2.2	신속한 결과..... 6
3	사이버 보안 평가 결과 및 권장 사항..... 8
3.1	기본 CIS Controls..... 8
3.2	기본 CIS Controls..... 13
3.3	조직 CIS Controls..... 19
4	기술 데이터 및 분석..... 25
4.2	Microsoft 보안 점수..... 40
5	부록 A - 권장 보안 소프트웨어 제품 개요..... 41
6	부록 B - 수명 종료 제품..... 41
7	부록 C - 평가 범위..... 42
7.1	사이버 보안 평가 목표..... 44
7.2	인벤토리 도구..... 44
7.3	사이버 보안 평가 도구..... 44
8	부록 D - 평가 배경..... 45
8.1	소개..... 45
8.2	컨트롤 프레임워크 배경 (CIS)..... 47
8.3	SOM 모델..... 48

사이버보안 진단 리포트 예시

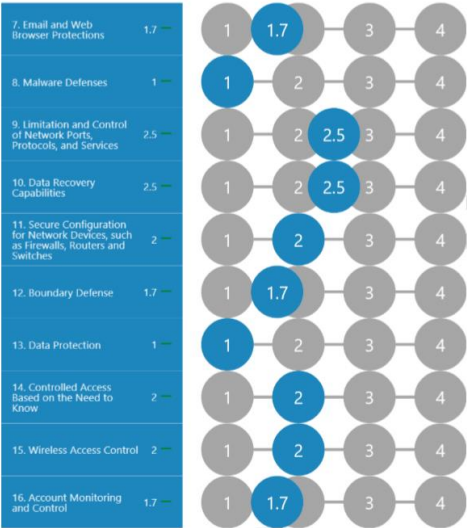


- “사이버보안 진단 리포트”는 보안수준 평가 결과 및 권장 사항을 제시합니다.

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

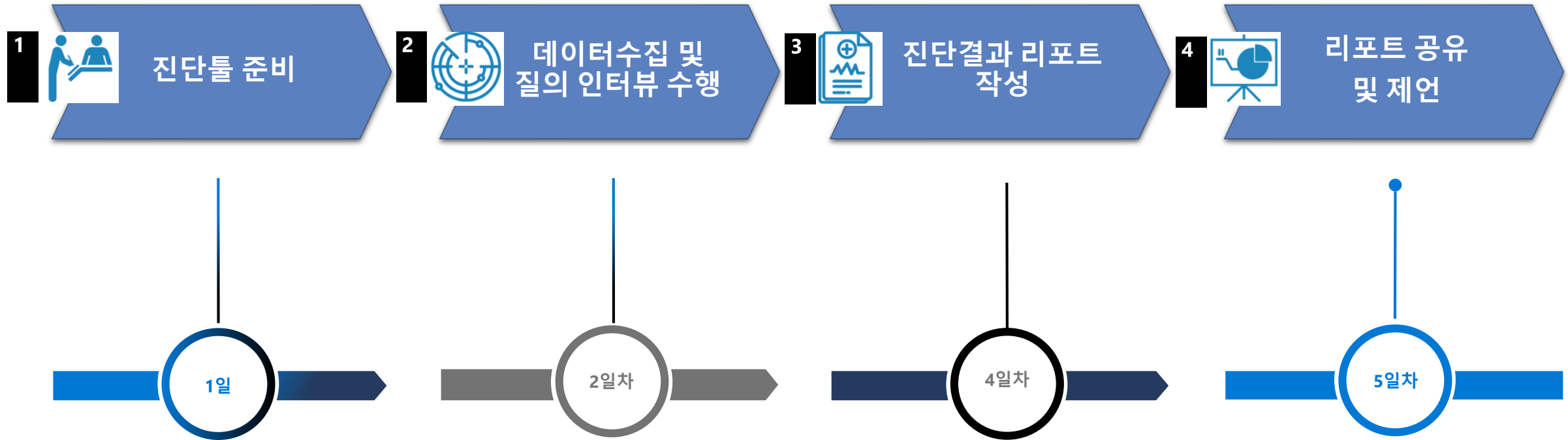
아래 자세한 평가 결과는 10가지 기반 CIS Controls에서 비롯된 것으로, <Customer>를 위한 권장 사항이 함께 나와 있습니다.

진급	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

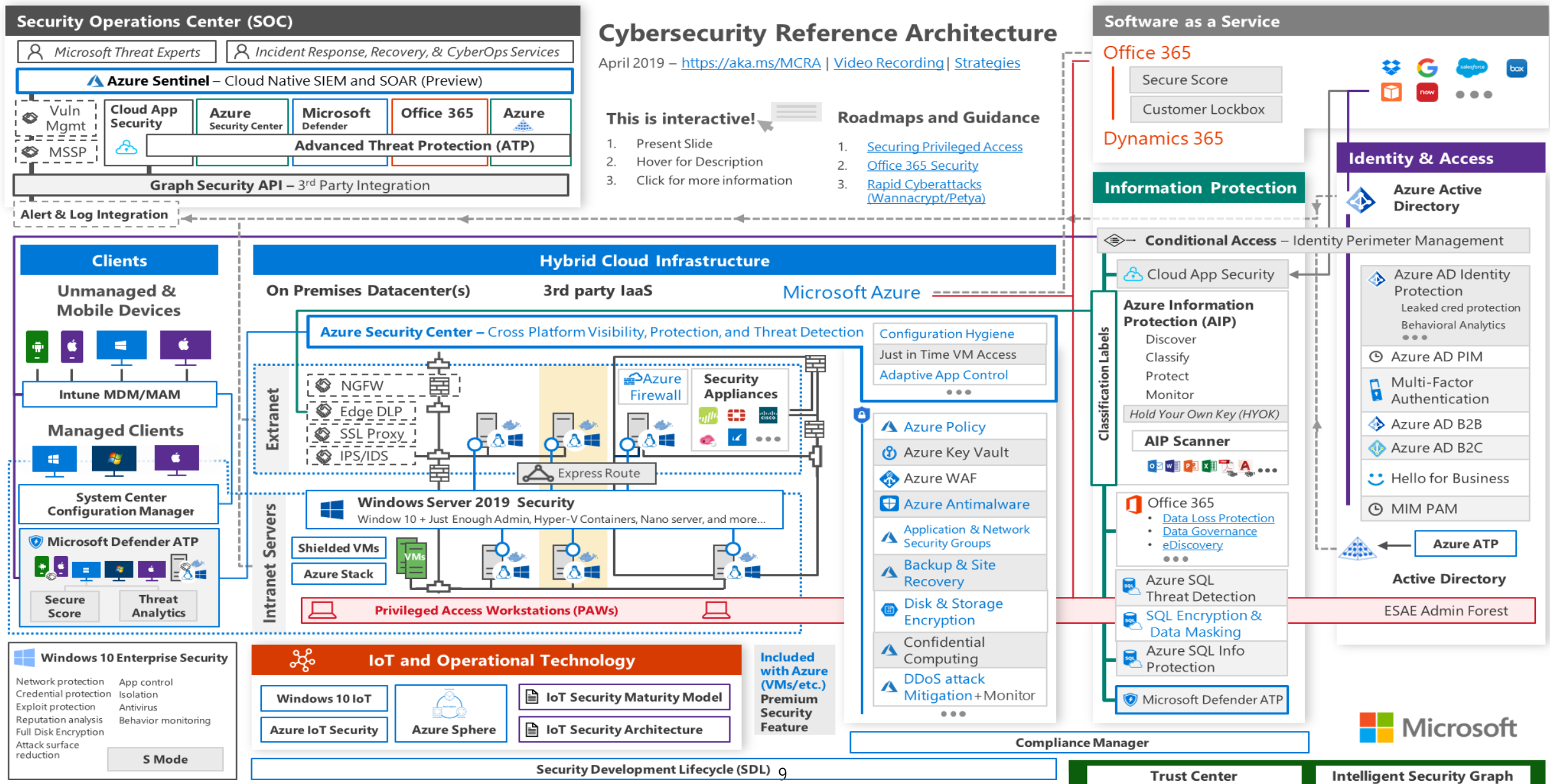
사이버보안 진단 소요일정



- “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.



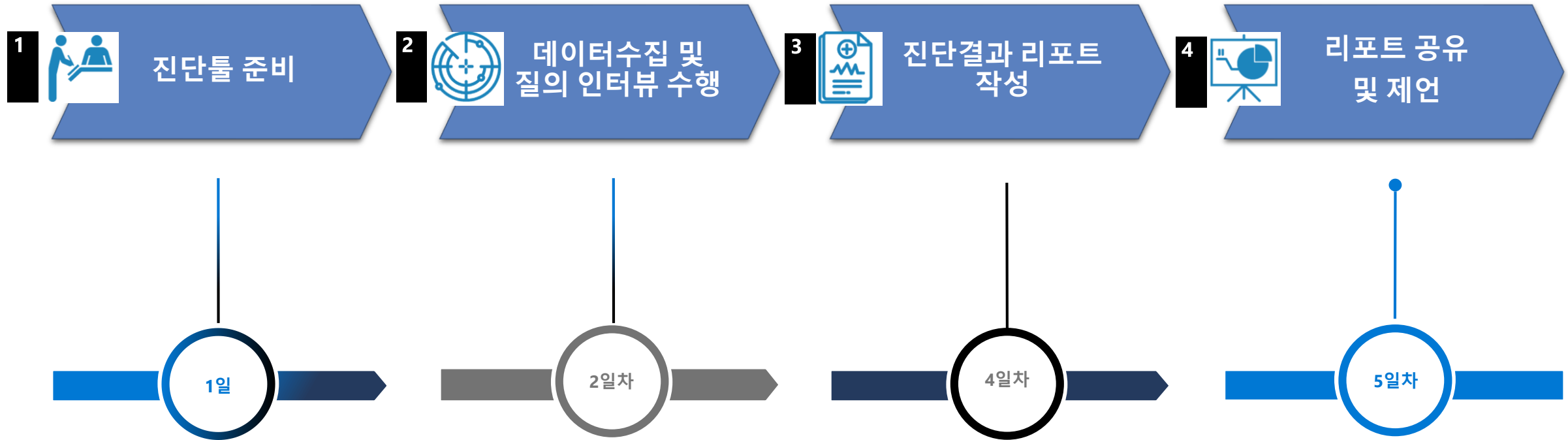
참조) Microsoft Cybersecurity Reference Architecture



사이버보안 진단 소요일정



- “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.



CSAT 정보 수집서버 HW 권장



CSAT 서버 최소 사양

Windows updates	Windows update 최신 버전 적용
CPU	2 CPU cores
Memory	3.5GB
Hard disk	최소 50 GB 이상
.NET Framework	Version 4.6 이상

CSAT 적정 요구 사양

Windows updates	Windows update 최신 버전 적용
CPU	4 CPU cores
Memory	16GB
Hard disk	SSD 80GB 이상
.NET Framework	Version 4.6 이상

CSAT 정보 및 요구사항



CSAT은 보안취약점을 진단 하기 위한 툴로써 Scan 정보는 아래와 같습니다.

Endpoint scan collection

- Endpoints의 정보는 WMI통해 수집
- Endpoints 정보 수집 후 Push된 파일은 제거되어 흔적이 남지 않음
- WMI 서비스가 Endpoints에 올바르게 구성되지 않은 경우 제한된 정보 수집

Network scan collection

- Active Directory 스캔의 경우 직접 AD 및 LDAP 쿼리 통해 수집
- Azure AD, Office 365, SharePoint Online 및 Intune 데이터는 Microsoft API 호출 통해 수집

Network traffic

- CSAT.exe 5MB실행 파일 동시에 30개의 Endpoint에 전송 가능(최대 150MB)
- CPU 사용량 : 1 ~ 5%
- 메모리 사용량 : 40 ~ 70MB
- Network load : 최대 약 100MB

CSAT 정보 및 요구사항 (계속)



CSAT Server Services의 필수 포트 관련 정보입니다.

Port number	TCP, UDP	설명
443	Outbound TCP	Office365, SharePoint Online and AAD Scan
4432	Inbound TCP	For the CSAT Portal
8018	Inbound TCP	Used by the Enumeration service
8080	Inbound and outbound TCP	Used by the Deployment service, used to deploy the dissolvable agent
8090	Inbound TCP	Used by the Analysis service
8288	Inbound TCP	Used by the Network service

CSAT 정보 및 요구사항 (계속)



CSAT와 클라이언트간 방화벽 룰 포트 관련 정보입니다.

Firewall Rule Name	Port	Notes
File and Printer Sharing (NB-Session-In)	139	
File and Printer Sharing (SMB-In)	445	
Remote Scheduled Tasks Management (RPC)	RPC Dynamic Ports (49152 to 65535)	
	1025 to 5000	(*)For Windows Versions older than Windows 7 & Windows Server 2008
Windows Management Instrumentation (DCOM-In)	135	
Windows Management Instrumentation (WMI-In)	ALL ports for svchost.exe	

CSAT 정보 및 요구사항 (계속)



File & Folder Virus and Spyware 예외처리 리스트

%windir%\Temp\csat\csat.exe

%windir%\Temp\csat\cmat_dwnld.exe

%windir%\System32\certutil.exe

%windir%\System32\cmd.exe

Installation Requirements OS

Windows 10 Professional or Enterprise, build 1607 or newer

Windows server 2019

Windows server 2016

Windows Server 2012 R2, though not recommended

CSAT 정보 및 요구사항 (계속)



CSAT 서비스 Active Directory 추가

The screenshot shows the CSAT web interface for managing Active Directory domains. The main table lists existing domains, and a modal dialog is open for adding a new one.

+	새로 만들기	FQDN	계정	모든 도메인 검사	마지막 스캔 상태
☒					
☒	...	softnet.co.kr	softnetdom\snet...	아니요	Complete

정보

Active Directory 도메인 *

softnet.co.kr

☒ 도메인 하나 검사

관리자 계정 *

softnetdom\snetadm

관리자 암호

저장

Active Directory 도메인 명 입력 : Softnet.co.kr
관리자 계정 ID , PW 입력 저장

CSAT 화면 및 기능 소개



CSAT 서비스 Microsoft 클라우드 추가

Office 365 / Azure : 테넌트 이름 – softnet365.onmicrosoft.com

어플리케이션 ID - dbb6ef34-49cb-4317-aa33-dc9f2faac7f3

SharePoint Online : 관리 사이트 URL - <https://softnet365.sharepoint.com>

클라이언트 ID - 797e703b-a0c2-4433-b919-1bb212b50ce7

키워드 입력 (Scan 할 키워드)

CSAT 화면 및 기능 소개



CSAT 서비스 Endpoint 정의 설정

The screenshot displays the CSAT web application interface. The main menu includes '서비스' (Service), '엔드포인트' (Endpoint), '분석' (Analysis), '질문지' (Questionnaire), and '보고서' (Report). The '엔드포인트' section is active, showing a list of endpoints. A modal window titled '정의' (Definition) is open, allowing the user to define a new endpoint. The modal has four radio buttons: '디렉터리' (Directory), 'IP 범위' (IP Range), 'CIDR', and '사용자 지정' (User Designation). The '디렉터리' option is selected. Below this, there are input fields for '디렉터리 서버' (Directory Server) with the value 'SN-INF-DC01' and '그룹 이름' (Group Name) with the value '모든 시스템'. There is also a checkbox for '도메인 하나 검사' (Check one domain). The '보안 정보' (Security Information) section contains a note: '① 검사에 사용할 관리자 자격 증명을 입력하십시오.' (1. Enter the administrator credentials to be used for the check). Below this note are input fields for 'Username' (softnetdom\snetadm) and 'Password'. A '저장 후 닫기' (Save and Close) button is at the bottom right of the modal.

EndPoint 정의 설정 : 디렉터리, IP범위, CIDR, 사용자 지정방법 가능
디렉터리 서버 – Domain 서버 지정
관리자 권한 있는 계정 입력 후 저장 후 검사 진행
Active Directory에 Join 되어있는 computer 모든 개체 Endpoint 검사

CSAT 화면 및 기능 소개



CSAT 서비스 Endpoint 리스트 확인

CSAT

서비스

엔드포인트

분석

질문지

보고서

그룹 추가

Test

FF

엔드포인트

정의

로그 검사

로그 검색

정의

검색

검사

검사 예약

선택 활성화

키워드 필터

엑세스

운영 체제

상태

지우기

190 / 190

시스템/IP	운영 체제	정의됨	재정의	엑세스 ↓	마지막...	마지막 스캔 상태	마지막...	DNS 호스트 이름
... PDCWPARK001 10.10.30.125	Microsoft Windows 10 Enterprise 버전: 10.0.17763	사용자 지정	추가	예		UNKNOWN	2019년 10월	PDCWPARK001.softnet.co.kr
... SN-INF-CSRDB01 172.20.20.18	Microsoft Windows Server 2012 R2 Standard 버전: 6.3.9600	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-INF-CSRDB01.softnet.co.kr
... SN-AZ-DC01 10.250.0.5	Microsoft Windows Server 2016 Datacenter 버전: 10.0.14393	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-AZ-DC01.softnet.co.kr
... SN-BHGO-NP01 10.10.30.97	Microsoft Windows 10 Enterprise 버전: 10.0.18362	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-BHGO-NP01.softnet.co.kr
... SN-WTKIM-NP02 10.10.30.88	Microsoft Windows 10 Enterprise 버전: 10.0.17763	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-WTKIM-NP02.softnet.co.kr
... SN-YJYANG-NP04 10.10.29.202	Microsoft Windows 10 Enterprise 버전: 10.0.17763	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-YJYANG-NP04.softnet.co.kr
... SN-INF-HOST02 172.20.20.89	Microsoft Windows Server 2016 Standard 버전: 10.0.14393	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-INF-HOST02.softnet.co.kr
... SN-INF-DC01 172.20.20.8	Microsoft Windows Server 2016 Standard 버전: 10.0.14393	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-INF-DC01.softnet.co.kr
... SN-INF-DC02 172.20.20.9	Microsoft Windows Server 2016 Standard 버전: 10.0.14393	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-INF-DC02.softnet.co.kr
... JRLEE-WEB01 172.20.20.101	Microsoft Windows Server 2016 Standard 버전: 10.0.14393	디렉터리	추가	예		UNKNOWN	2019년 10월	JRLEE-WEB01.softnet.co.kr
... SN-JHLIM-NP02 10.10.30.237	Microsoft Windows 10 Enterprise 버전: 10.0.17763	디렉터리	추가	예		UNKNOWN	2019년 10월	SN-JHLIM-NP02.softnet.co.kr
... JRLEE-Client01 172.20.20.103	Microsoft Windows 10 Enterprise LTSC 버전: 10.0.17763	디렉터리	추가	예		UNKNOWN	2019년 10월	JRLEE-Client01.softnet.co.kr

EndPoint 리스트 및 상태 확인 가능
개별 리스트 별로 엔드 포인트 스캔하여 체크 가능

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인

CSAT 분석 화면: 방화벽 상태

키워드 필터: 도메인 공개 비공개 지우기 8/8

FQDN	들...	나간...	도메인	공개	비공개	위협 ↑
PDCWPARK001.softnet.co.kr 10.10.30.125	337	393	D B N	D B N	D B N	나쁨
SN-SHKONG-NP01.softnet.co.kr 10.10.28.130	312	277	D B N	E B N	D B N	나쁨
PDCWPARK001.softnet.co.kr 10.10.30.125	337	393	D B N	D B N	D B N	나쁨
SN-CJYANG-NP01.softnet.co.kr 10.10.28.137	507	252	E B N	E B N	E B N	보통
SN-YJYANG-NP04.softnet.co.kr 10.10.29.202	310	203	E B N	E B N	E B N	보통
jaeholee.softnet.co.kr 10.10.28.60	312	246	E B N	E B N	E B N	보통
SN-JHLIM-NP02.softnet.co.kr 10.10.30.237	811	348	E B N	E B N	E B N	보통
SN-HCNAM-N01.softnet.co.kr 10.10.30.178	441	284	E B N	E B N	E B N	보통

CSAT 분석 화면: 설치된 애플리케이션

키워드 필터: 플래그 위협 계시자 지우기 1426/1426

애플리케이션 이름	버전	첫 번째 설치 날짜	계시자	엔드포인트...	위협 ↑
Tools for .Net 3.5	3.11.50727	10/25/2018	Microsoft Corporation	4	보통
Tools for .Net 3.5 - KOR Lang Pack	3.11.50727	10/25/2018	Microsoft Corporation	4	보통
3DP Chip Lite v18.11	v18.11		3DP	1	보통
64 Bit HP CIO Components Installer	22.2.1	03/18/2019	HP Inc.	1	보통
7-Zip 18.01 (x64)	18.01		Igor Pavlov	1	보통
Active Directory Authentication Library for SQL Server	15.0.1300.359	10/19/2019	Microsoft Corporation	1	보통
Active Directory Authentication Library for SQL Server	14.0.1000.169	11/21/2018	Microsoft Corporation	1	보통
Active Directory Authentication Library for SQL Server	14.0.800.90	05/13/2019	Microsoft Corporation	1	보통
AD Replication Status Tool 1.0	2.18.0920.0	06/04/2019	Microsoft Corporation	1	보통
Adobe Acrobat Reader DC - Korean	19.021.20048	10/21/2019	Adobe Systems Inc...	1	보통
Adobe Acrobat Reader DC - Korean	19.021.20049	10/28/2019	Adobe Systems Inc...	1	보통
Adobe Creative Cloud	3.7.0.270		Adobe Systems Inc...	1	보통
Adobe Flash Player 32 PPAPI	32.0.0.270		Adobe	2	보통
Adobe Photoshop CC 2015.5	17.0.0		Adobe Systems Inc...	1	보통
Adobe Refresh Manager	1.8.0	10/17/2019	Adobe Systems Inc...	2	보통

방화벽 상태 확인

설치된 애플리케이션 확인

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인

분석 > 온프레미스: 서비스 > Active Directory > AD 계정

현재 평가 2019년 10월 28일 오전 1:47:03

키워드 필터 플래그 위협 도메인 활성화 관리자 OU 암호가 만료됨 UAC 지우기 175 / 175

사용자 이름	OU	도메인 이름	활성...	IsAd...	암호가...	마지막 로그인	마지막으...	잘못된 암호 시도	UAC	위협 ↑
rachelLee	CN=rachelLee...	softnet	예	아니오	아니오	2015.01.19.			512	나쁨
administrator	CN=Administr...	softnet	아니오	예	아니오	2017.12.02.	2017.01.01.	51607	66050	나쁨
dskim	CN=dskim,OU=...	softnet	예	아니오	아니오	2019.04.08.			512	나쁨
shlee	CN=shlee,OU=...	softnet	예	아니오	아니오	2019.03.29.			512	나쁨
mwlee	CN=mwlee,OU=...	softnet	예	아니오	아니오	2019.07.27.			512	나쁨
myshin	CN=myshin,O...	softnet	예	아니오	아니오	2019.07.22.	2019.05.08.		512	나쁨
PFUP_SN-AZ-DC01	CN=PFUP_SN-...	softnet	예	아니오	아니오	2017.12.19.	2017.12.08.		66048	나쁨
igoh	CN=igoh,OU=...	softnet	예	아니오	아니오	2018.01.03.			512	나쁨
kwlee	CN=kwlee,OU=...	softnet	예	아니오	아니오	2019.03.19.			512	나쁨
kskim	CN=kskim,OU=...	softnet	예	아니오	아니오	2017.12.08.		1	512	나쁨
jhoh	CN=jhoh,OU=...	softnet	예	아니오	아니오	2017.09.19.			512	나쁨
scloud	CN=Softnet Cl...	softnet	예	아니오	아니오	2018.01.22.	2019.04.29.		66048	나쁨
tgshin	CN=tgshin,OU=...	softnet	예	아니오	아니오	2017.05.27.			512	나쁨
mslee	CN=mslee,OU=...	softnet	예	아니오	아니오	2019.03.30.		1	512	나쁨
yjshin	CN=yjshin,OU=...	softnet	예	아니오	아니오	2019.07.26.	2019.05.08.		512	나쁨
tsa	CN=Technical...	softnet	예	아니오	아니오	2017.04.28.	2019.04.29.	1	66048	나쁨
bikang	CN=bikang,OU=...	softnet	예	아니오	아니오	2019.05.29.	2019.05.29.	1	512	나쁨
public	CN=inPHRCare...	softnet	예	아니오	아니오	2018.01.22.	2019.04.29.	1	66048	나쁨

분석 > 온프레미스: 서비스 > Active Directory > 암호 정책

현재 평가

키워드 필터 플래그 위협 지우기 1 / 1

도메인 이름	최소 길이	최소 사...	최대 사...	암호 기록	잠금 기간	관찰 창 잠금	암호 속성	위협 ↑
softnet	7	0	90 일수	1	29 분	29 분	C NA NC L S R	나쁨

AD 계정 보안상태 확인

AD 암호정책 상태 확인

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인

분석 > 클라우드 > Azure > Azure AD 계정

키워드 필터 플래그 위협 활성화... 지우기 192 / 192

표시 이름	활성화됨	AAD 동기...	시작 날짜	사용자 계정 이름	위협 ↑
☐ Azure Connect Service Account	예	예	2019.10.29.	AZURE_CONSVC@Softnet365.onmicros	① 보통인 편
☐ 이철훈	예	예	2019.10.29.	chlee@softnet.co.kr	① 보통인 편
☐ 양철진	예	예	2019.10.29.	cjyang@softnet.co.kr	① 보통인 편
☐ 박철우	예	예	2019.10.29.	cwpark@SOFTNET.CO.KR	① 보통인 편
☐ 용호빈	예	예	2019.10.29.	hbyong@SOFTNET.CO.KR	① 보통인 편
☐ 조훈희	예	예	2019.10.29.	hhcho@softnet.co.kr	① 보통인 편
☐ 한형호	예	예	2019.10.29.	hhhan@softnet.co.kr	① 보통인 편
☐ 황현준	예	예	2019.10.29.	hjhwan@softnet.co.kr	① 보통인 편
☐ 김정겸	예	예	2019.10.29.	jkim@SOFTNET.CO.KR	① 보통인 편
☐ 이종량	예	예	2019.10.29.	jilee@softnet.co.kr	① 보통인 편
☐ 김정태	예	예	2019.10.29.	jtlim@softnet.co.kr	① 보통인 편
☐ 박정우	예	예	2019.10.29.	jwpark@softnet.co.kr	① 보통인 편
☐ 홍경민	예	예	2019.10.29.	kmhong@softnet.co.kr	① 보통인 편
☐ 김민찬	예	예	2019.10.29.	mckim@softnet.co.kr	① 보통인 편
☐ 김만석	예	예	2019.10.29.	mskim@softnet.co.kr	① 보통인 편

분석 > 클라우드 > Azure > Azure AD 그룹

키워드 필터 플래그 위협 지우기 161 / 161

표시 이름	구성원 수	설명	보안 활성화됨	위협 ↑
☐ AZURE EMS CONSULTING	14	AIP	아니요	① 보통
☐ 2팀	10	2팀	예	① 보통
☐ MFA Enable Group	5	이 사용자들은 Intune 정책에서 제외되	예	① 보통
☐ WIP-WIN10	1	WIP-WIN10 세미나	예	① 보통
☐ BCS Admins	1		예	① 보통
☐ 현대다이모스&현대파워텍 도메인 통합	2	현대다이모스&현대파워텍 도메인 통합	아니요	① 보통
☐ ABL 생명 AD/ADEP/SCCM	11	ABL 생명 AD/ADEP/SCCM	아니요	① 보통
☐ Security	3	Network Monitoring Group Mail Accou	예	① 보통
☐ CMSAdmin	2	softnet CMS 관리자	예	① 보통
☐ LG화학 SCCM을 이용한 PMS인프라 구	6	LG화학 프로젝트	아니요	① 보통
☐ DnsUpdateProxy	0	DHCP 서버와 같은 다른 클라이언트를	예	① 보통
☐ 포스코 AD/SCCM 인프라 구축 프로젝트	9	포스코 AD/SCCM 인프라 구축 프로젝트	아니요	① 보통
☐ 헬스케어사업팀	2	헬스케어사업팀-하위포함	예	① 보통
☐ Exchange Recipient Administrators	1	Users in this group can manage Exchan	예	① 보통
☐ Recipient Management	1	Members of this management role gro	예	① 보통

Azure AD 계정 상태 확인

Azure AD 그룹 상태 확인

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인

CSAT
서비스
엔드포인트
분석
질문지
보고서

CISv7 베이직
1. 하드웨어 자산 재...
2. 소프트웨어 자산...
3. 지속적 취약점 관리
4. 관리 권한의 통제...
5. 모바일 기기, 노트...
6. 감사 기록의 유지...

CISv7 기초
7. 이메일 및 웹 브라...
8. 악성소프트웨어 방...
9. 네트워크 포트, 프...
10. 데이터 복구 기능
11. 방화벽, 라우터,...
12. 경계 방어
13. 데이터 보호
14. 알아야 할 필요성...
15. 무선 접속 관리
16. 계정 모니터링 및...

모두 다운로드

요약

CISv7 베이직

1. 하드웨어 자산 재고 및 관리	응답된 질문 2/2
2. 소프트웨어 자산 재고 및 관리	응답된 질문 2/2
3. 지속적 취약점 관리	응답된 질문 2/2
4. 관리 권한의 통제된 사용	응답된 질문 3/3
5. 모바일 기기, 노트북, 워크스테이션, 서버의 하드웨어 및 소프트웨어 보안 설정	응답된 질문 2/2
6. 감사 기록의 유지 관리, 모니터링, 분석	응답된 질문 2/2

CSAT
서비스
엔드포인트
분석
질문지
보고서

현재 상태
파일 템플릿 보고서
템플릿 보고서 다운로드

평가
성숙도 개요
성숙도 세부 정보
성숙도 진행률
권장 사항
내보내기
보안 점수

엔드포인트

검색된 엔드포인트	197
검사된 엔드포인트	12
방화벽이 비활성화된 엔드포인트	5
매우 중요한 업데이트가 누락된 엔드포인트	2
바이러스 백신 정의가 오래된 엔드포인트	0
활성화되지 않은 엔드포인트	2
잘못된 것으로 플러그가 지정된 엔드포인트	0
BitLocker 암호화가 적용되지 않은 클라이언트 엔드포인트	9
BitLocker 암호화가 적용되지 않은 서버 엔드포인트	3

OFFICE 365

PII 문서	0
외부 사용자	18
외부에서 공유된 항목	0

CSAT 보안 취약점 관련 질문지 내역

CSAT질문지

CSAT 보고서 메뉴 화면

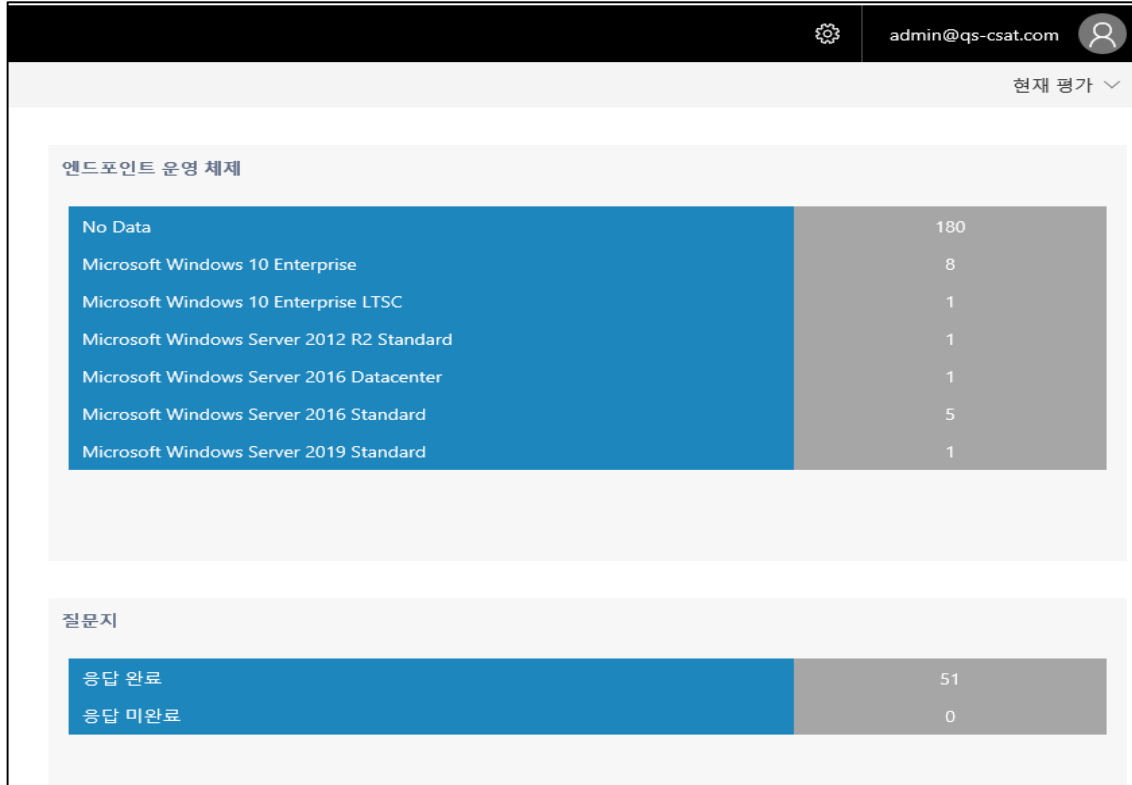
CSAT보고서

23

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인



CSAT 보고서 메뉴 화면

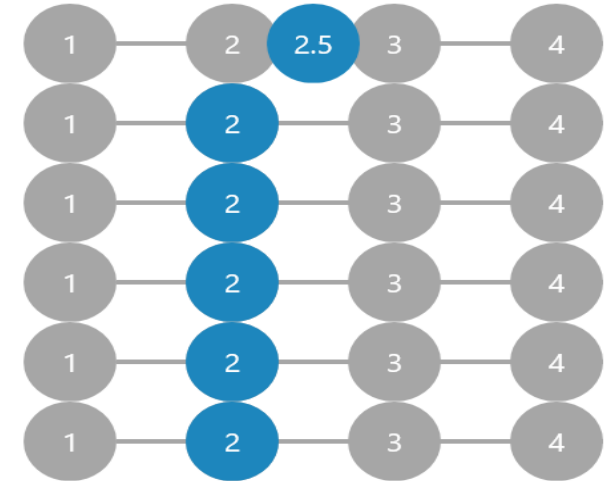
Company Score

Company Score



CISv7 베이직

1. 하드웨어 자산 재고 및 관리	2.5	—
2. 소프트웨어 자산 재고 및 관리	2	—
3. 지속적 취약점 관리	2	—
4. 관리 권한의 통제된 사용	2	—
5. 모바일 기기, 노트북, 워크스테이션, 서버의 하드웨어 및 소프트웨어 보안 설정	2	—
6. 감사 기록의 유지 관리, 모니터링, 분석	2	—

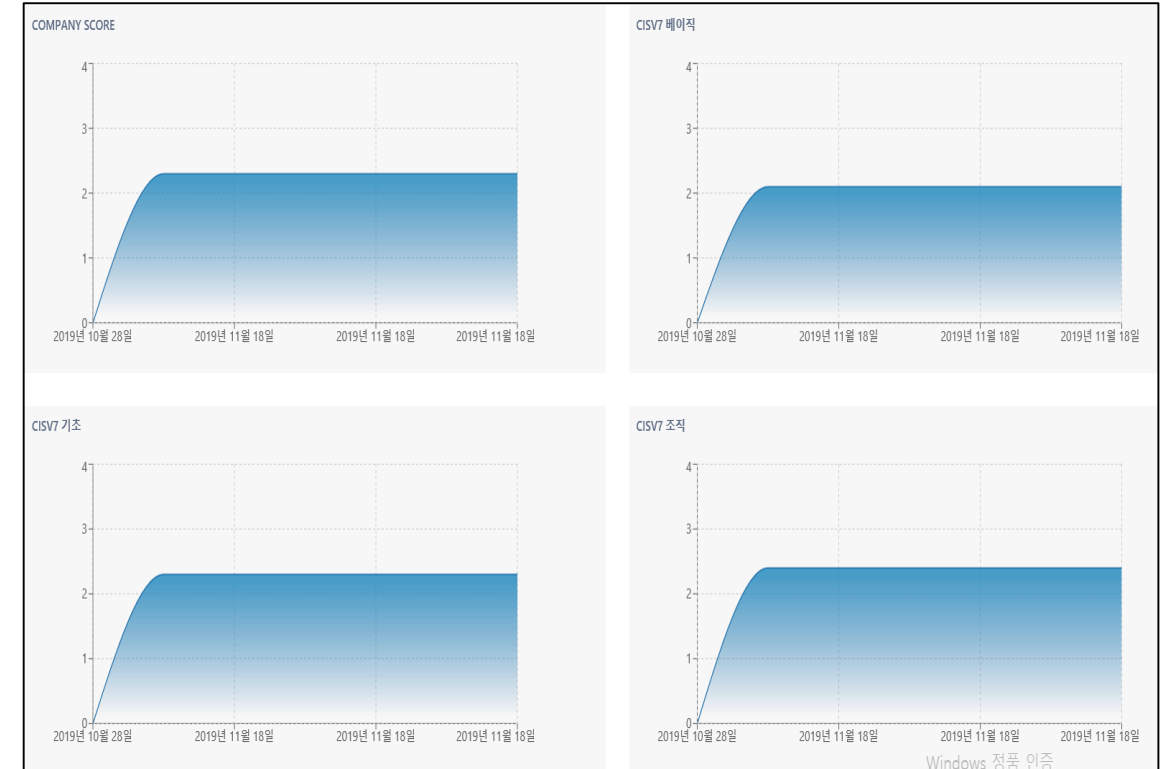


CSAT 보고서 점수 화면

CSAT 화면 및 기능 소개



CSAT 분석 결과 확인



CSAT 보고서 성숙도 세부정보 화면

CSAT 성숙도 진행률 화면

THANK YOU

