#Cybersecurity
사이버보안 진단 프로그램 소개

Microsoft

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 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 인프라스트럭처 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 경감시키기고 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

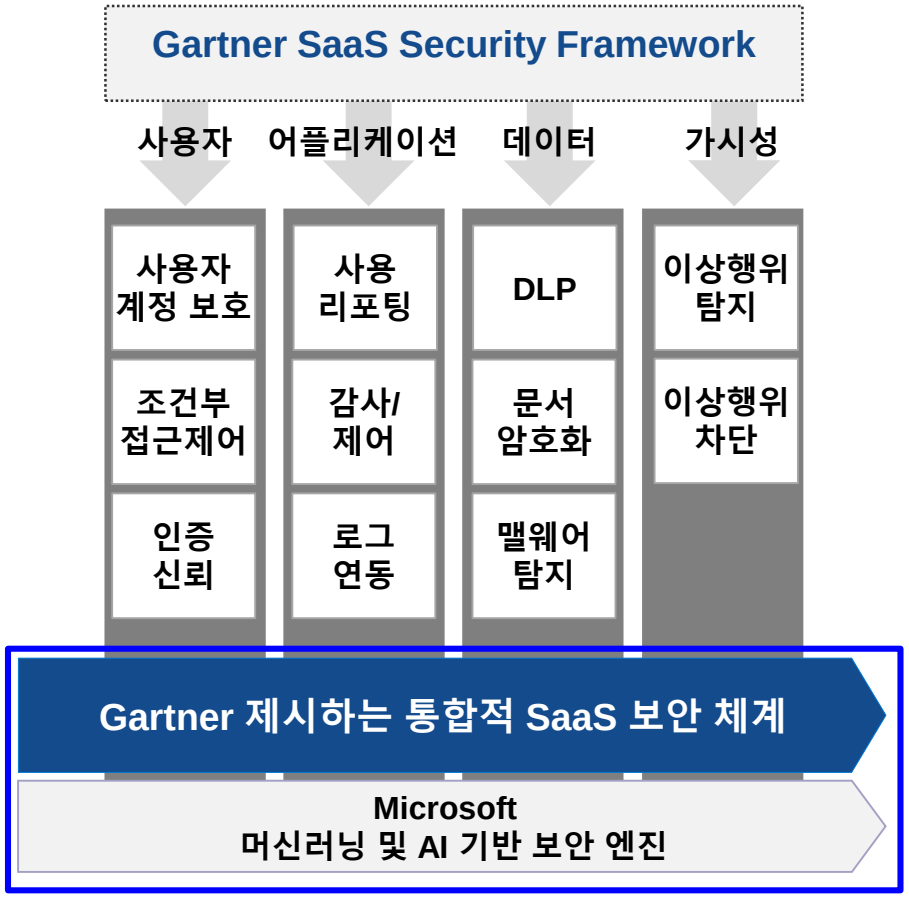
- "**사이버보안 진단 프로그램**"은 고객의 참여시간 및 리소스 최소화를 위해, 글로벌 차원에서 **입증된 전문 진단툴을 활용**하여 단기간에 데이터 수집 및 결과 리포트를 작성하여, **국내 보안전문 파트너사와 함께** 진단결과에 대해 사이버보안 취약점 강화방안에 대한 제언을 함께 제공해 드립니다.

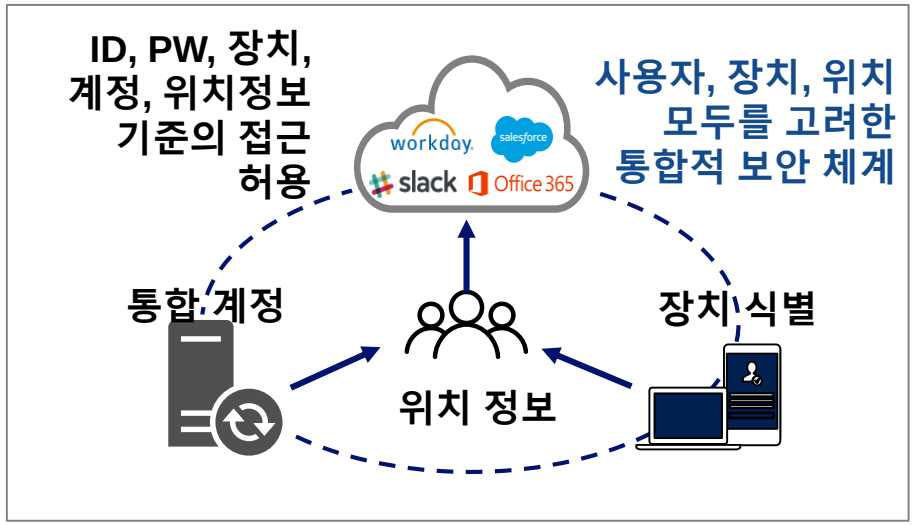
1) *사이버보안 진단툴은 QS Solutions 사의 CSAT (Cyber Security Assessment Tool)을 활용하며, 상세한 내용은 소개동영상(영문) 참조*

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

사이버보안 진단 프로그램

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





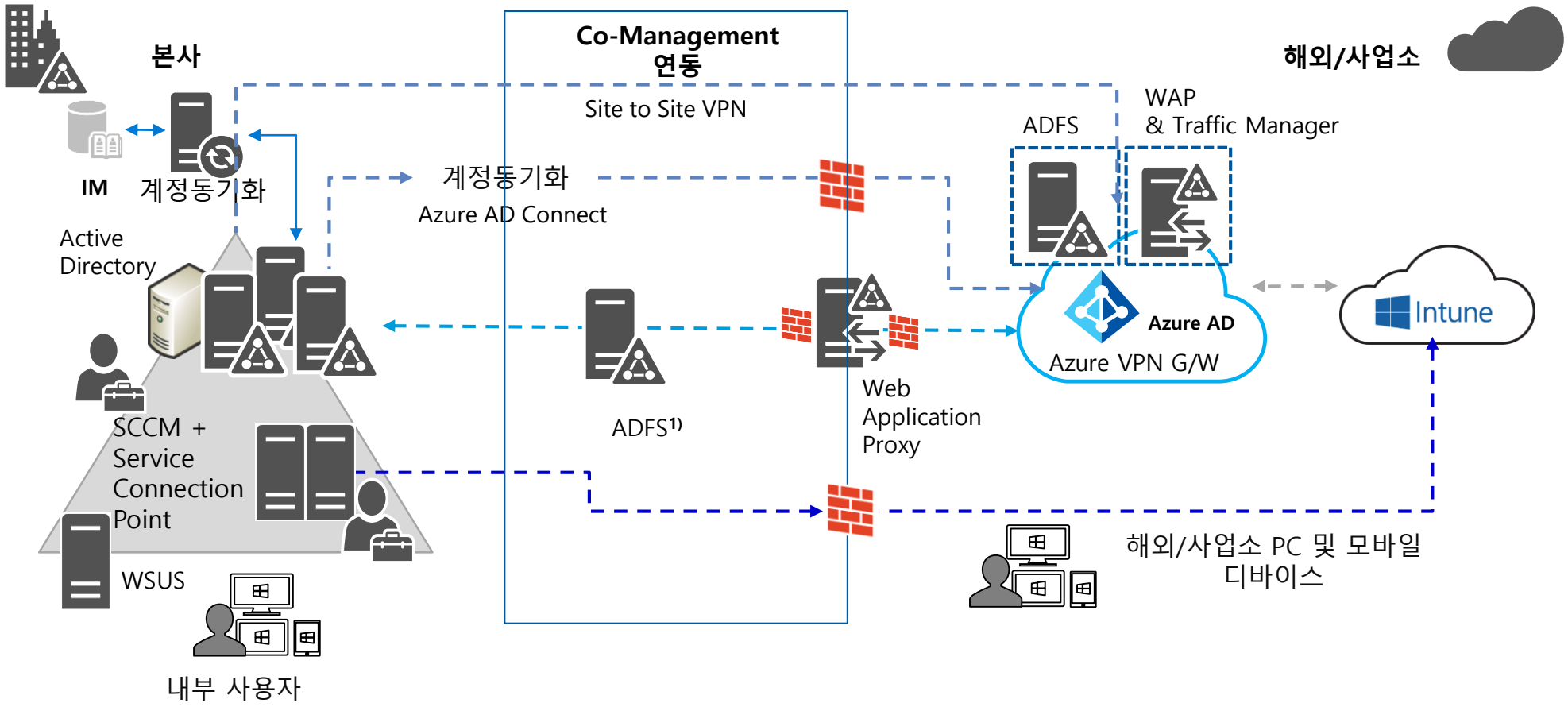
Active Directory와 연동한
사용자 계정 및 인증에 대한 보호 체계

계정정보, 장치식별, 위치정보, Big-Data 기준
조건부 접근제어 활성화

문서, 데이터에 대한 암호화 체계

사이버보안 진단 프로그램

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



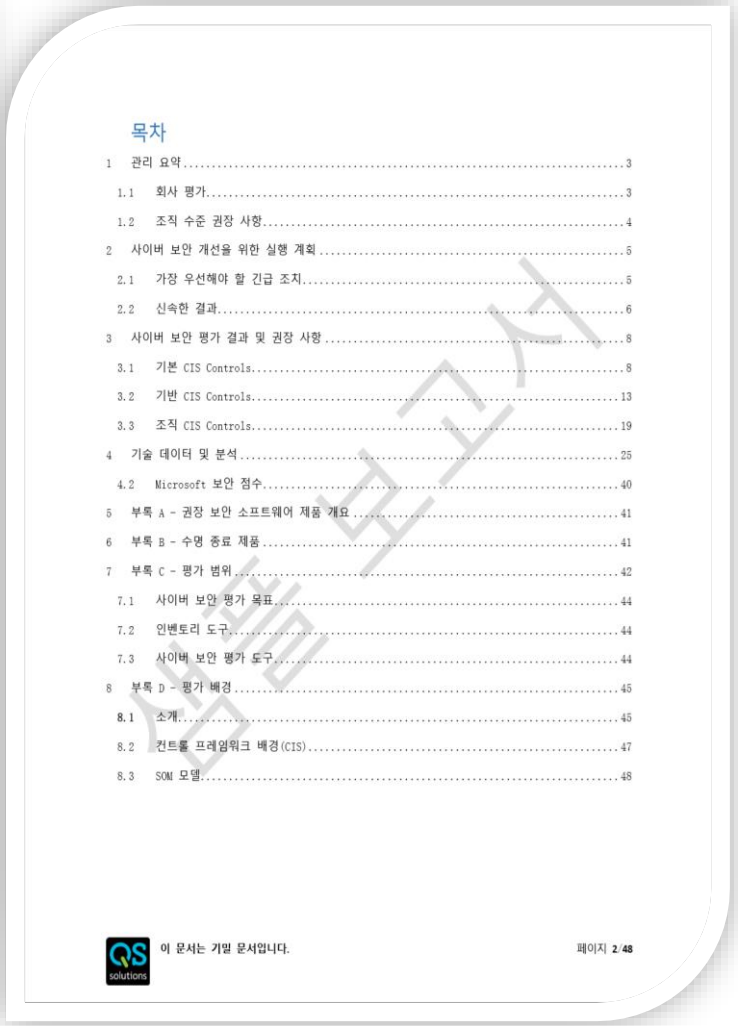
*내부 VPN Connecter필요(Site to Site VPN 지원)

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 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



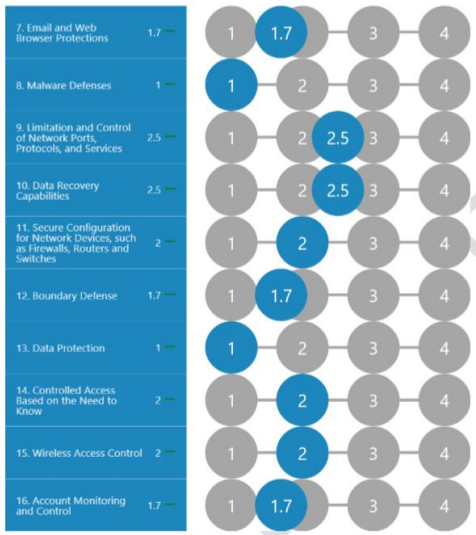
사이버보안 진단 리포트 예시

- "**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



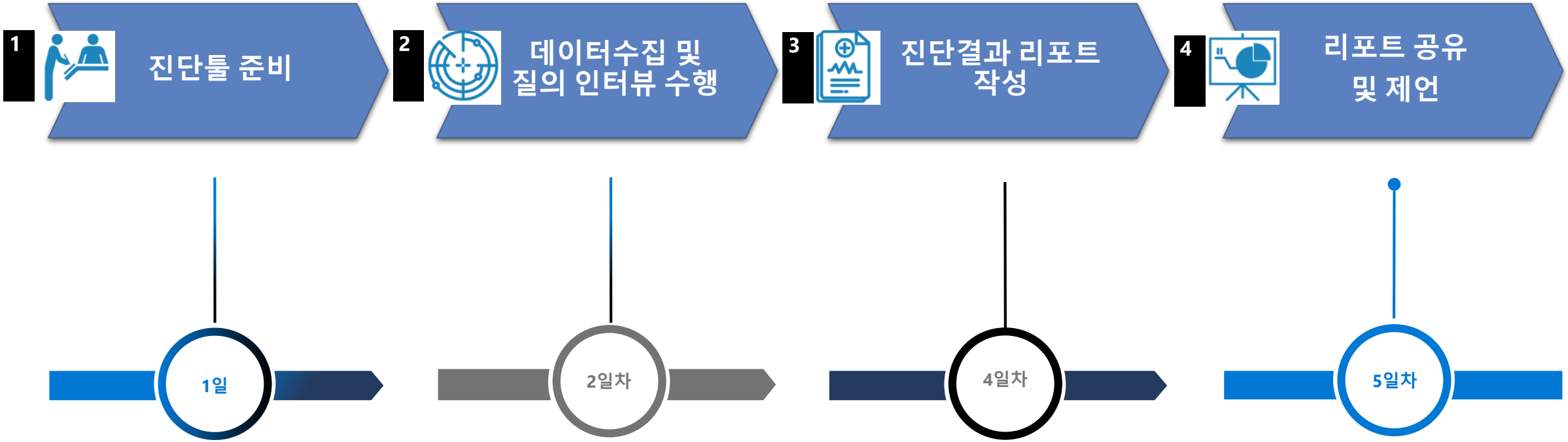
3.2.2 기반 CIS Controls – 평가 결과 및 권장 사항

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 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

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

- Microsoft Threat Experts
- Incident Response, Recovery, & CyberOps Services
- **Azure Sentinel** – Cloud Native SIEM and SOAR (Preview)
- Vuln Mgmt
- MSSP
- Cloud App Security
- Azure Security Center
- Microsoft Defender
- Office 365
- Azure
- Advanced Threat Protection (ATP)
- Graph Security API – 3rd Party Integration
- Alert & Log Integration

Software as a Service

- Office 365
  - Secure Score
  - Customer Lockbox
- Dynamics 365

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Microsoft Defender ATP
- Secure Score
- Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS/IDS
- Azure Firewall
- Security Appliances
- Express Route

Intranet Servers

- **Windows Server 2019 Security**
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs
- Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Information Protection

- Cloud App Security
- **Azure Information Protection (AIP)**
  - Discover
  - Classify
  - Protect
  - Monitor
  - Hold Your Own Key (HYOK)
- AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection
- Microsoft Defender ATP

Identity & Access

- Azure Active Directory
- **Conditional Access** – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring
- S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

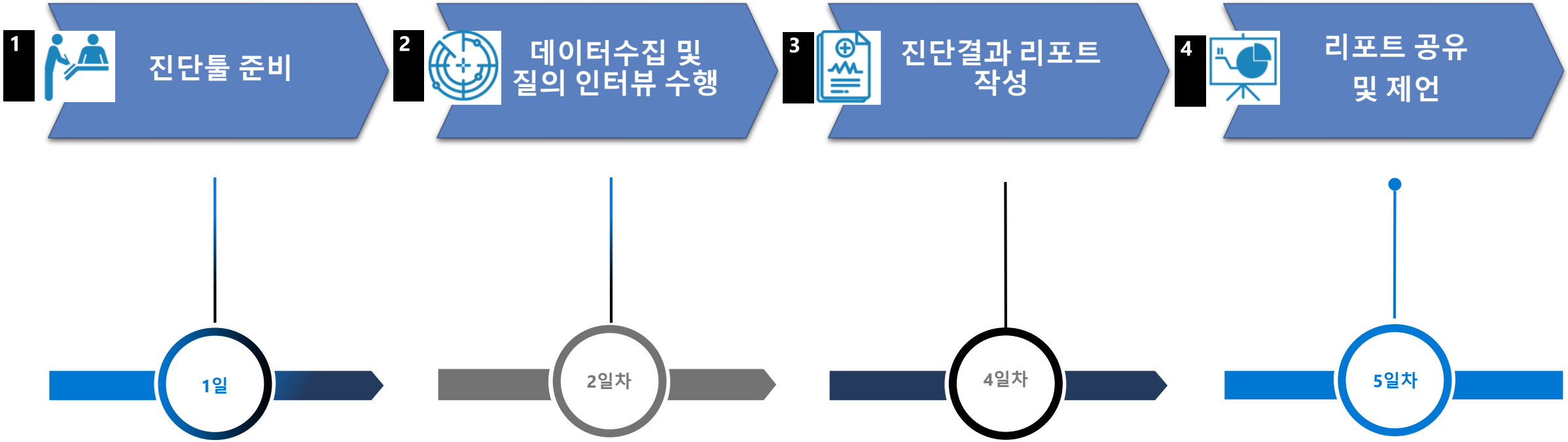
Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

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 버젼 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 버젼 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

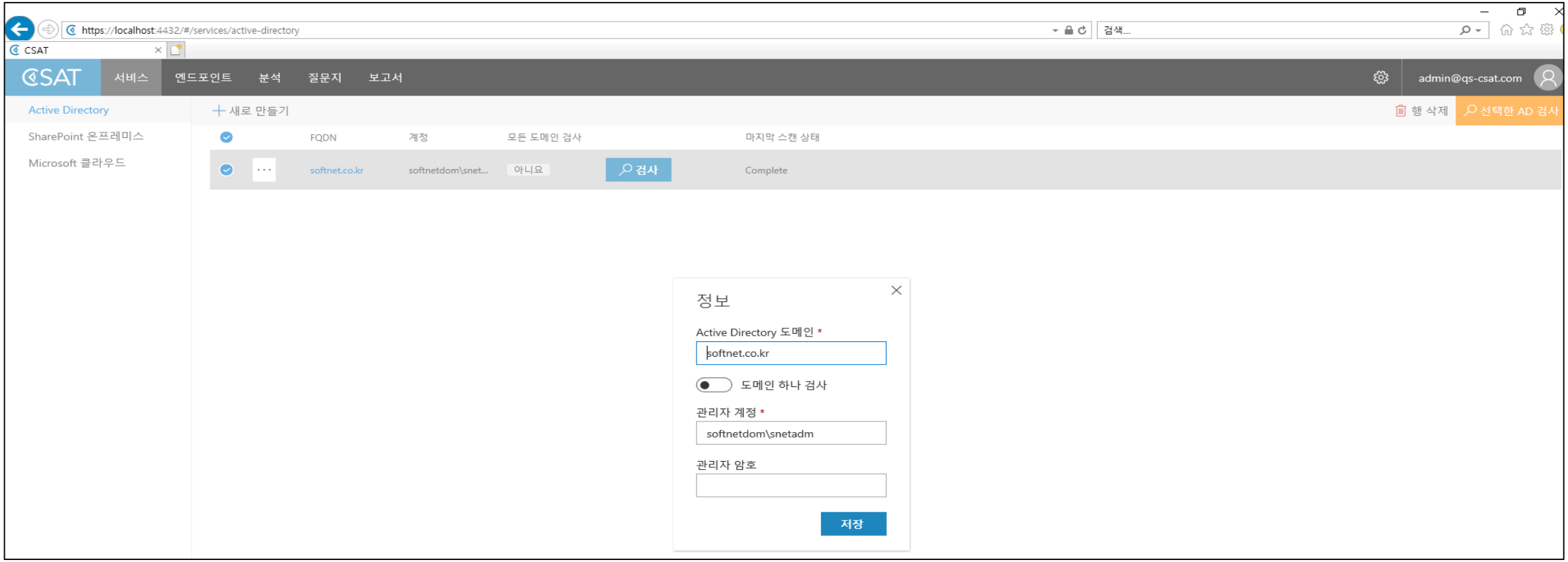
Windows server 2019

Windows server 2016

Windows Server 2012 R2, though not recommended

CSAT 정보 및 요구사항 (계속)

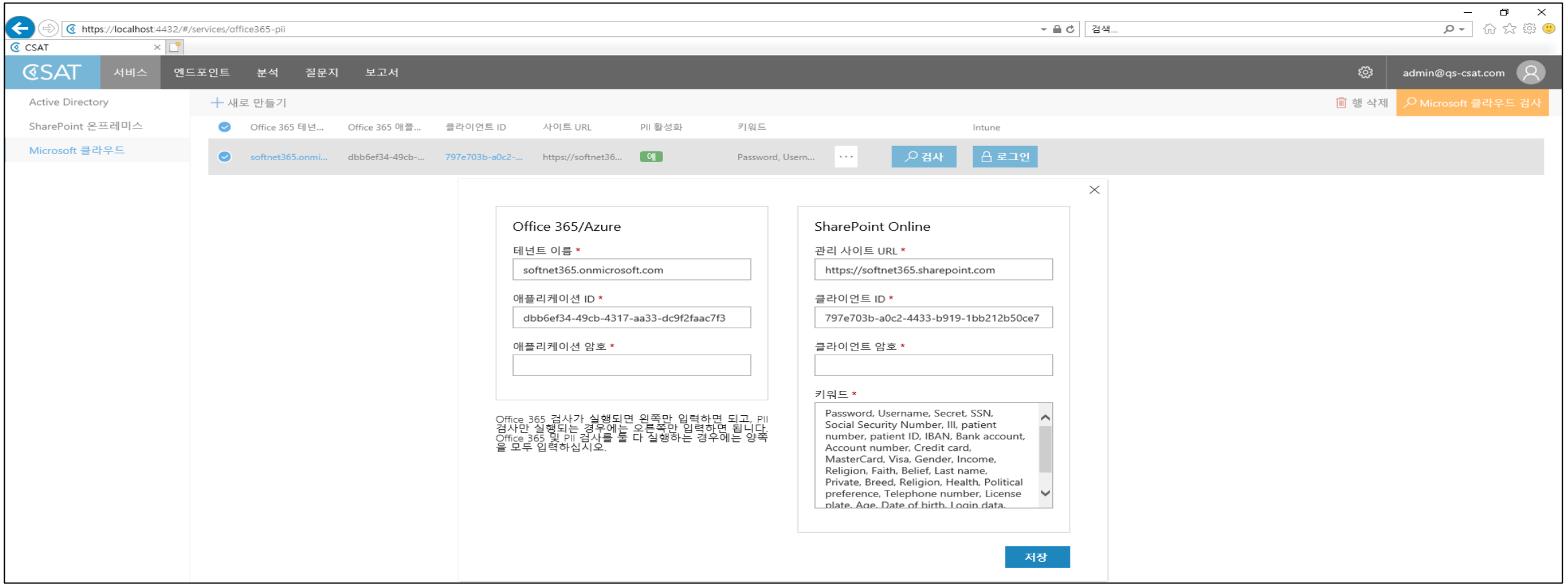
CSAT 서비스 Active Directory 추가



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

CSAT 화면 및 기능 소개

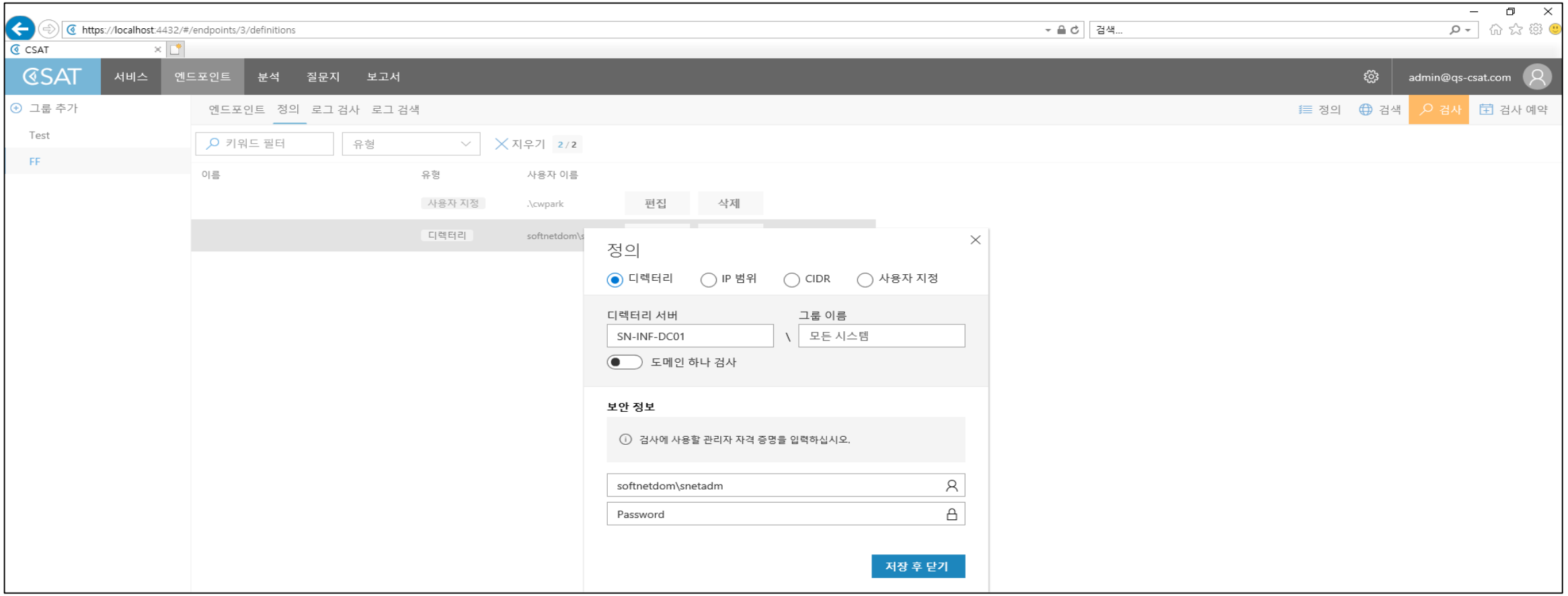
CSAT 서비스 Microsoft 클라우드 추가



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

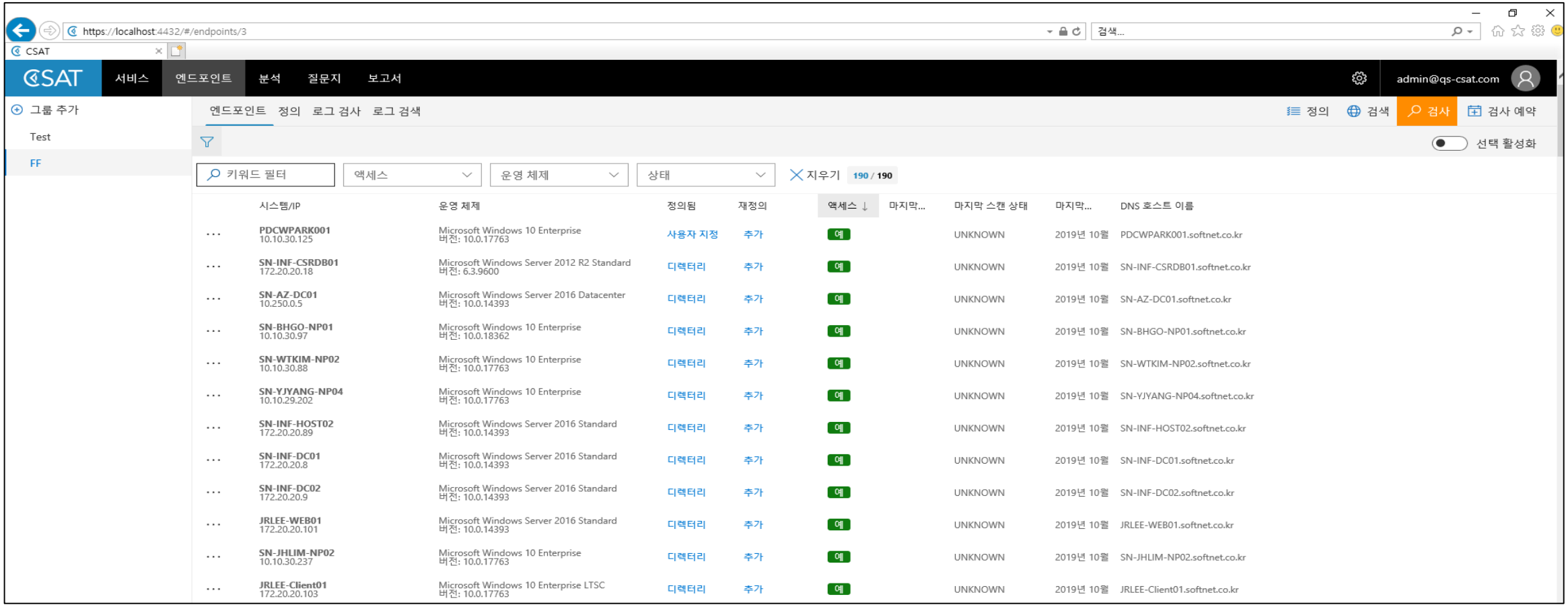
CSAT 서비스 Endpoint 정의 설정



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

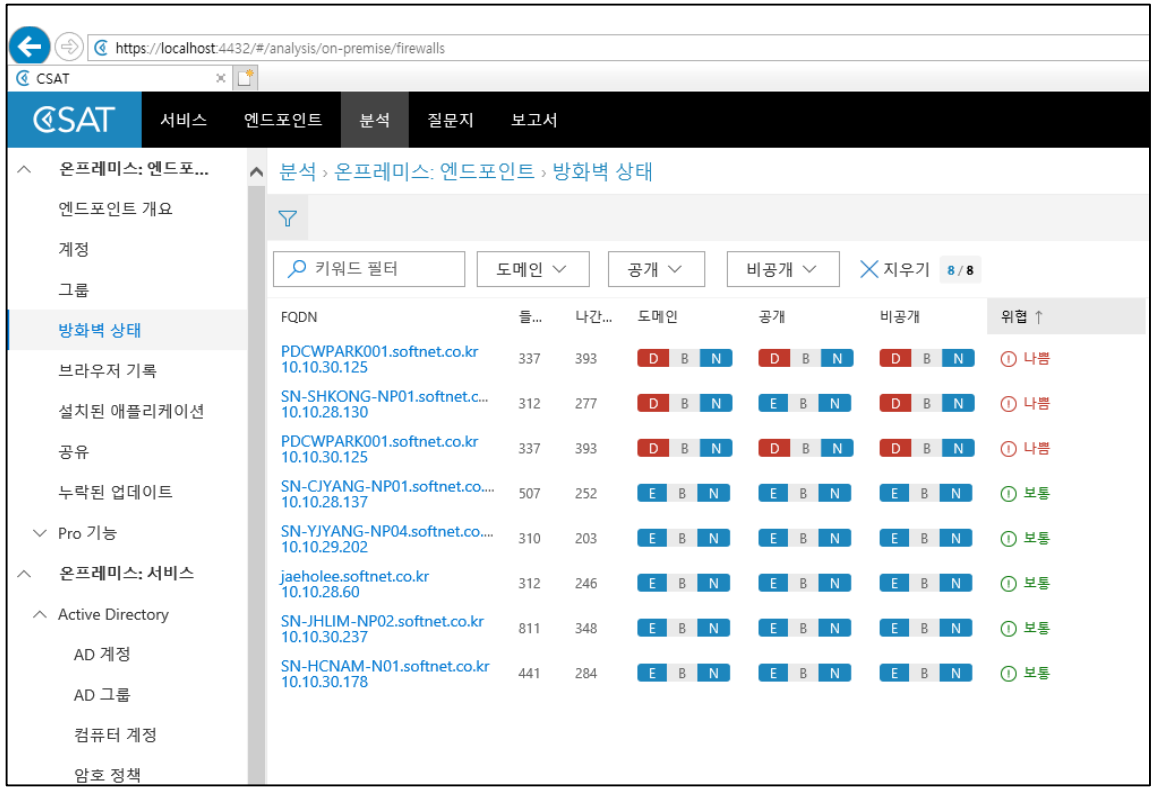
CSAT 서비스 Endpoint 리스트 확인



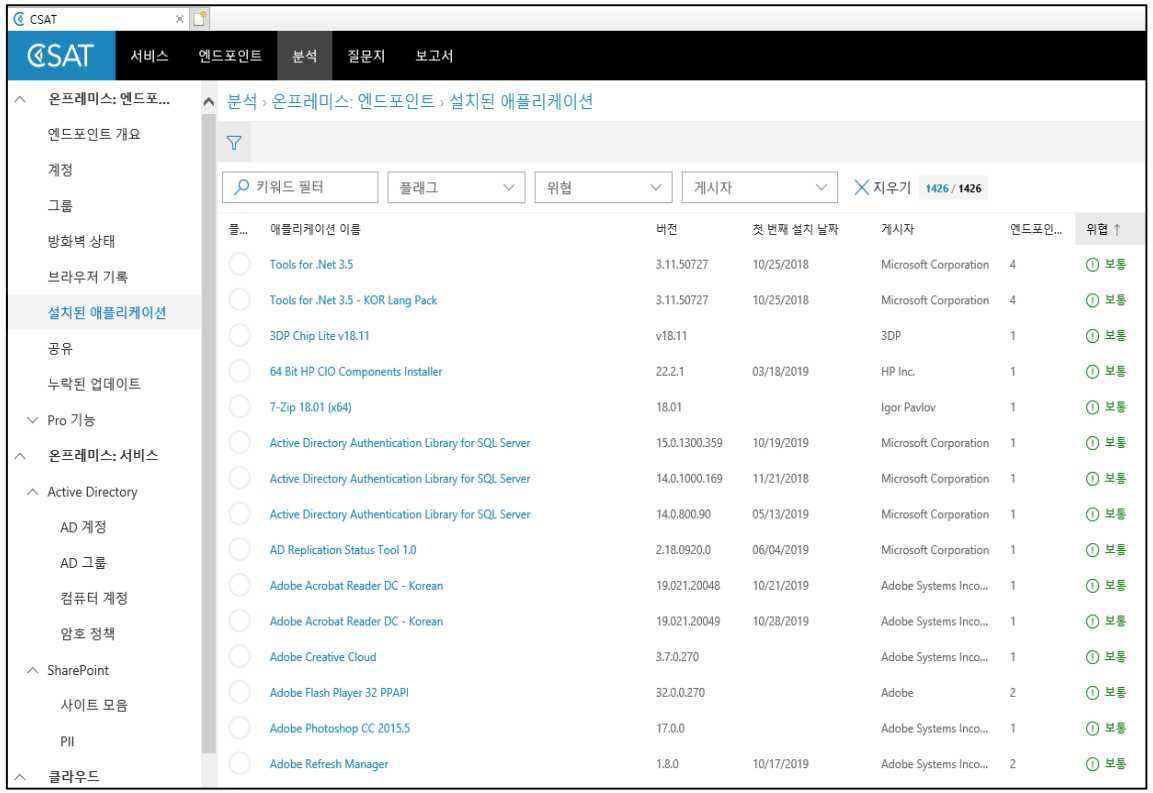
EndPoint 리스트 및 상태 확인 가능
개별 리스트 별로 엔드 포인트 스캔하여 체크 가능

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인



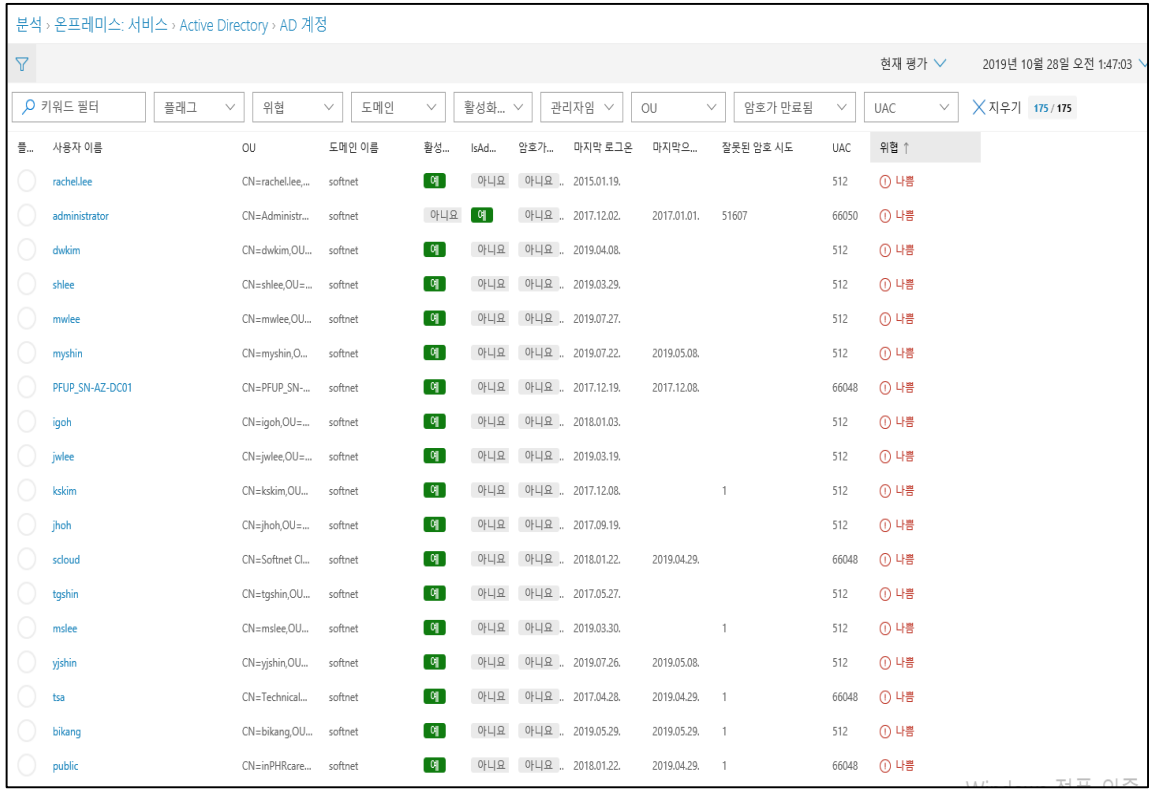
방화벽 상태 확인



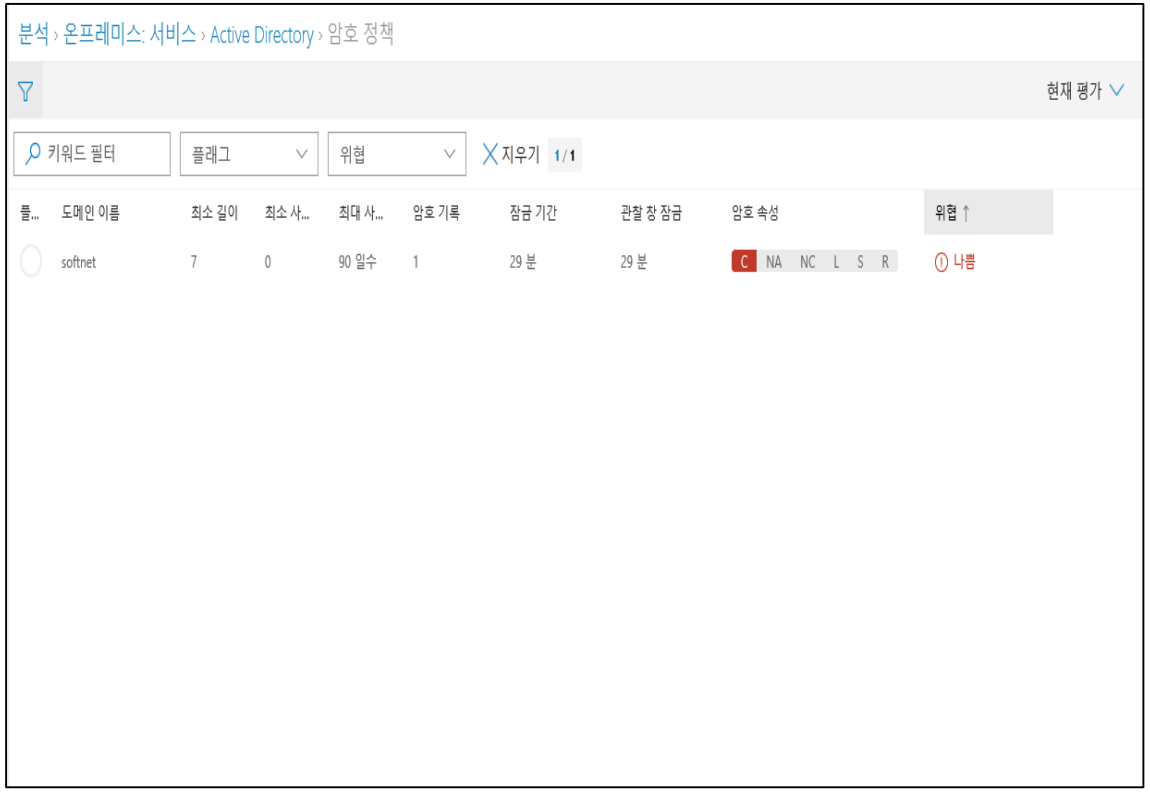
설치된 애플리케이션 확인

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인



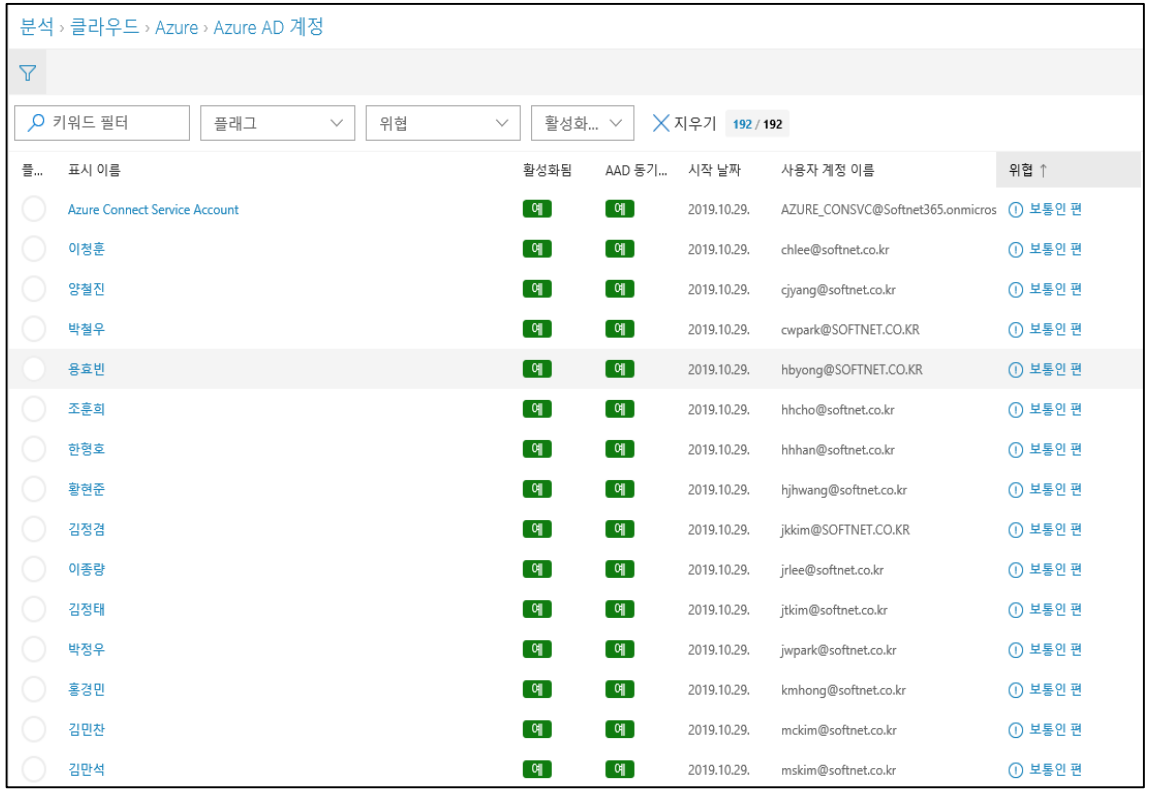
AD 계정 보안상태 확인



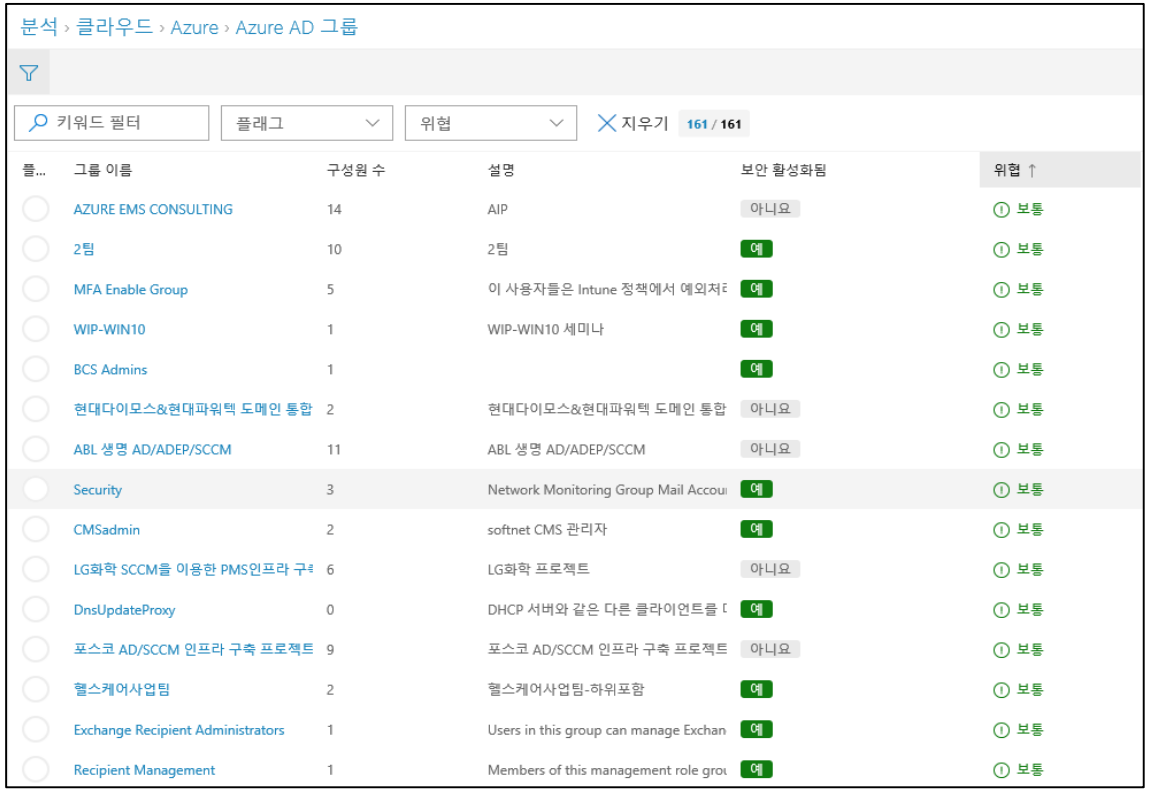
AD 암호정책 상태 확인

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인



Azure AD 계정 상태 확인



Azure AD 그룹 상태 확인

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인

CSAT 보안 취약점 관련 질문지 내역

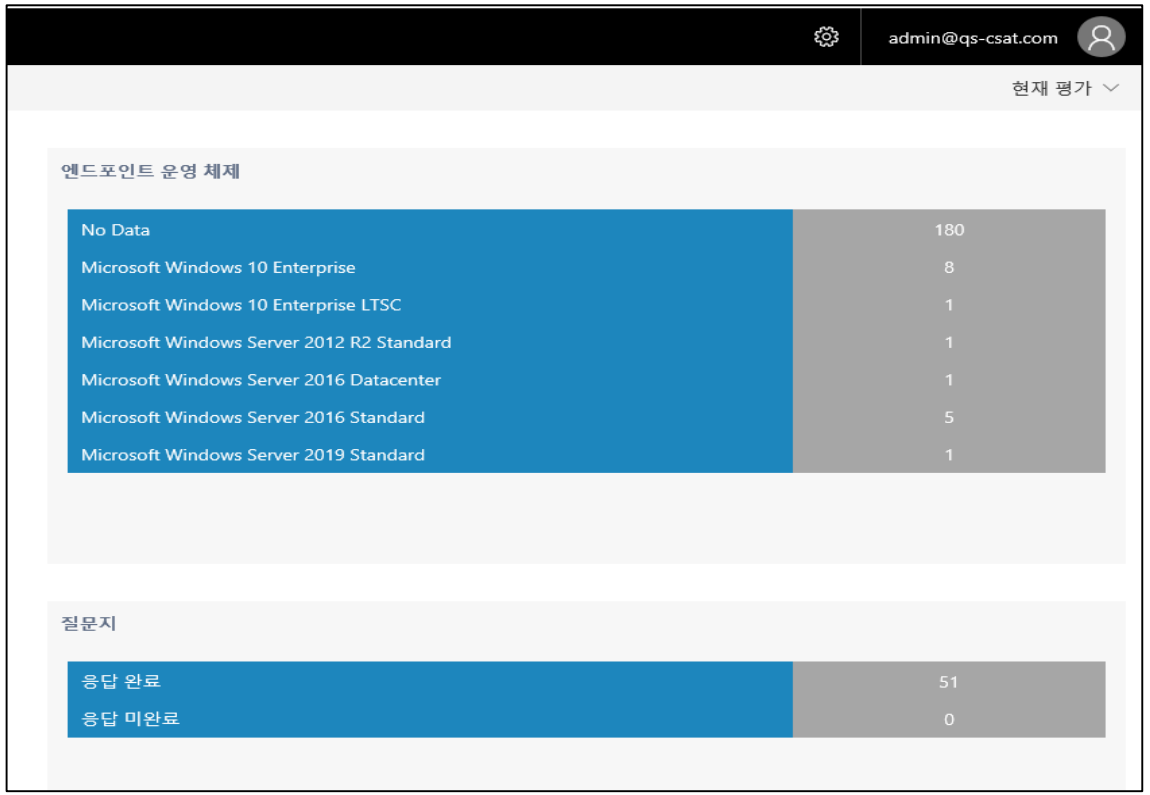
CSAT질문지

CSAT 보고서 메뉴 화면

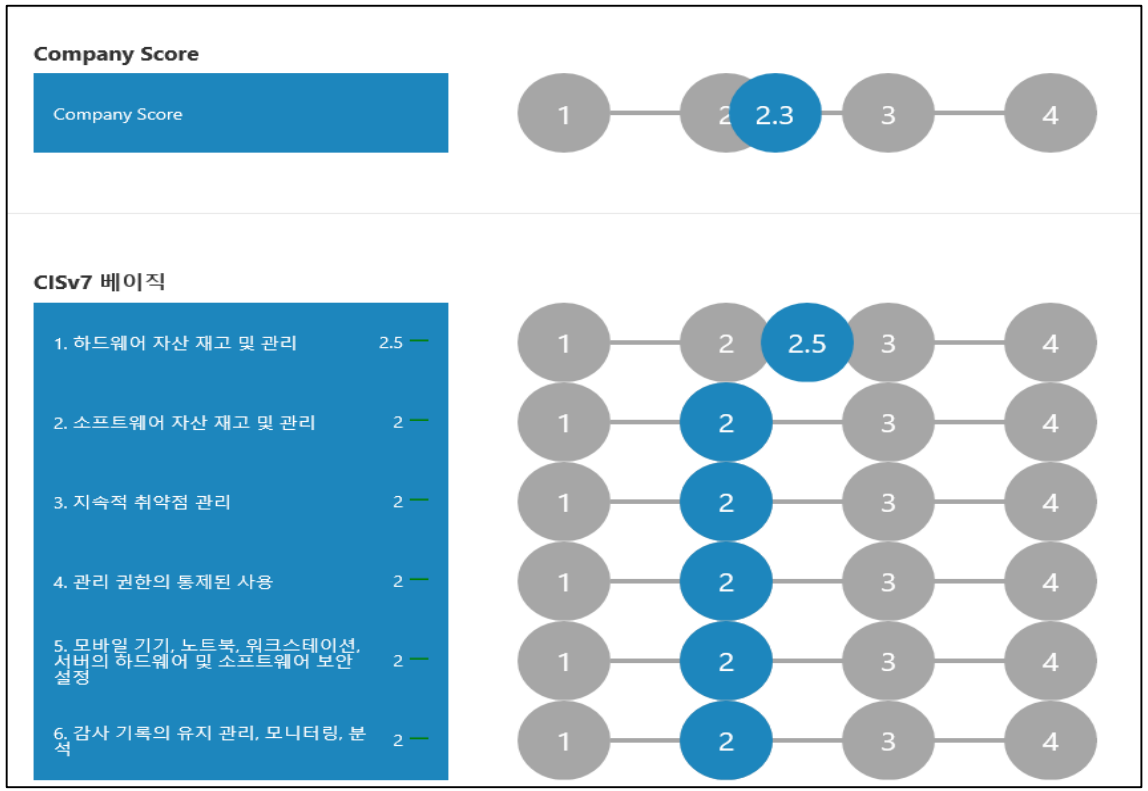
CSAT보고서

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인



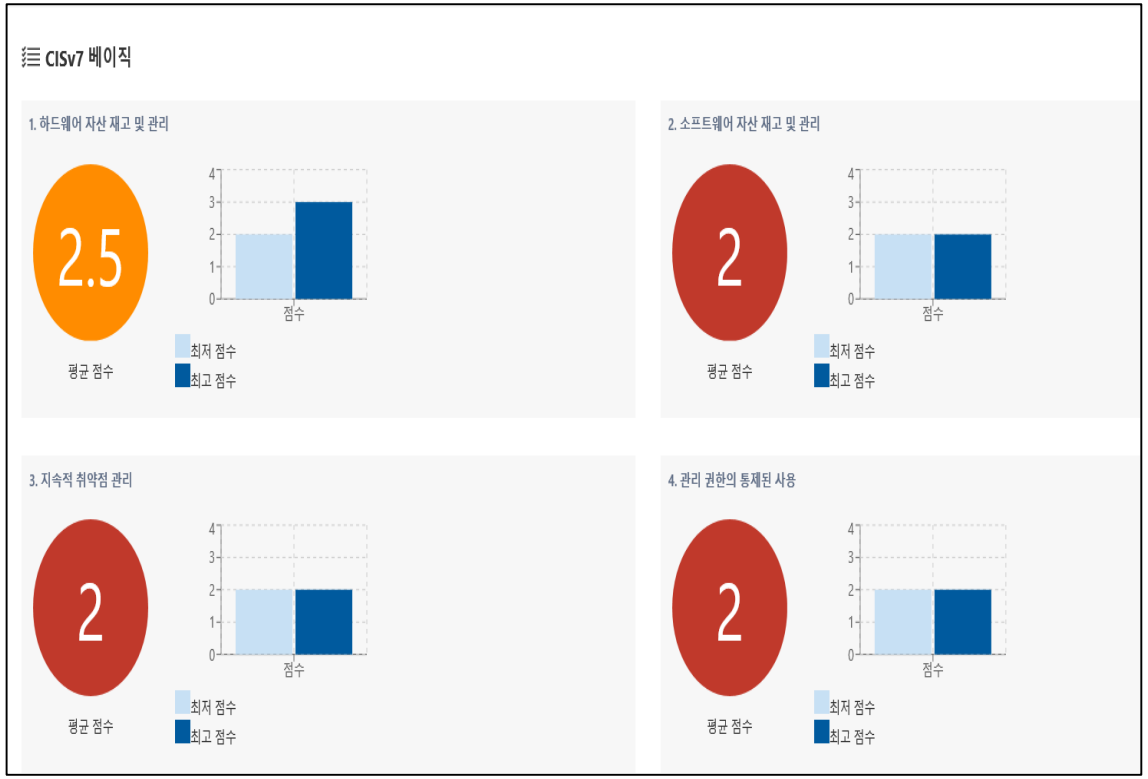
CSAT 보고서 메뉴 화면



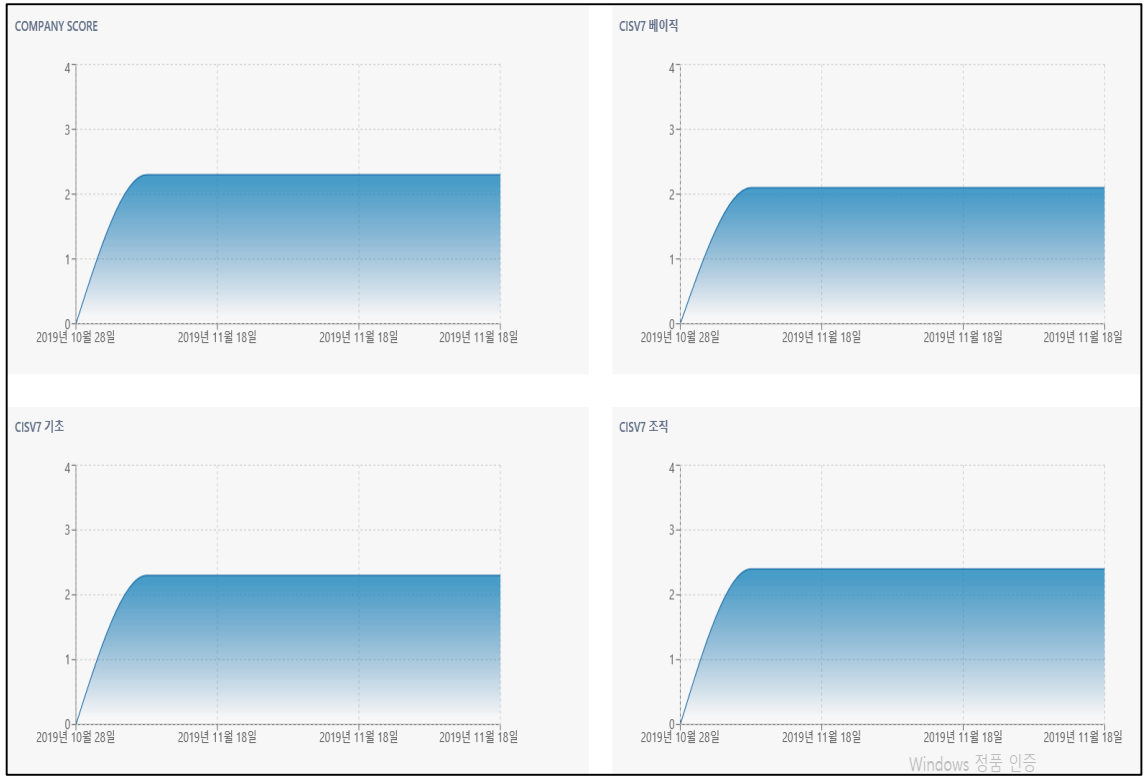
CSAT 보고서 점수 화면

CSAT 화면 및 기능 소개

CSAT 분석 결과 확인



CSAT 보고서 성숙도 세부정보 화면



CSAT 성숙도 진행률 화면

Microsoft

THANK YOU