

권한 접근관리 솔루션

IDIRA Privileged Access Management

June, 2026



업계 최고의 통합 아이덴티티 보안
플랫폼을 제공합니다

7회 연속, 리더

2025 Gartner® Magic Quadrant™ for Privileged Access Management

IDIRA(CyberArk)는 현대적 인프라 환경의 요구에 부합하는 보안 전략을 고도화하며, 특권(Privilege) 보안의 미래를 만들어가고 있습니다.

*GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

1 - Gartner® Magic Quadrant® for Privileged Access Management, by Abhyuday Data, Paul Mezzera, Shubham Gera, Tarun Rohilla, Michael Kelley, 13 October 2025

Figure 1: Magic Quadrant for Privileged Access Management



Gartner.

IDIRA 플랫폼은 보안을 선도하고 있습니다.

2003: 권한 계정 증명 관리 및
주기적인 변경

2009: 권한 세션 보호 및 모니터링

2012: 보호되지 않은
권한 계정 식별

2015: 권한 공격
연구소 설립

2016: 엔드포인트
자격증명 보호

2017: AWS와 연동한
자격증명 온보딩 자동화

2019: 제로트러스트 원격
접근 SaaS제공

2022: Just-In-Time 접근

2025: IGA온보딩

2024: CORA AI,
Venafi, MIS확장

2023: ZSP온보딩

2020: 적응형 SSO 및
MFA를 위한 IDaaS플랫폼

2018: 관리자 및 권한을 가진
비즈니스 사용자 보호

2017: DevOps Secret 보호

2015: Kerberos 공격 탐지 및 차단

2013: 권한 위협 탐지 및 차단

2011: 클라우드 및 가상 인프라보호

IDIRA 아이덴티티 보안 플랫폼

Powered by CORA AI



새롭게 정의된 워크포스 접근제어 솔루션



임직원



엔드포인트



브라우저



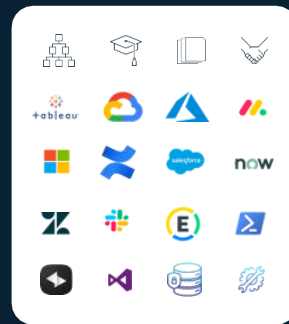
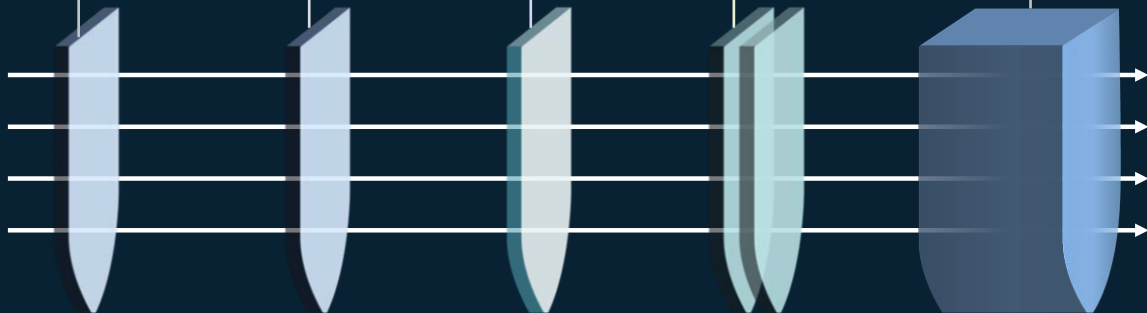
패스워드



접속

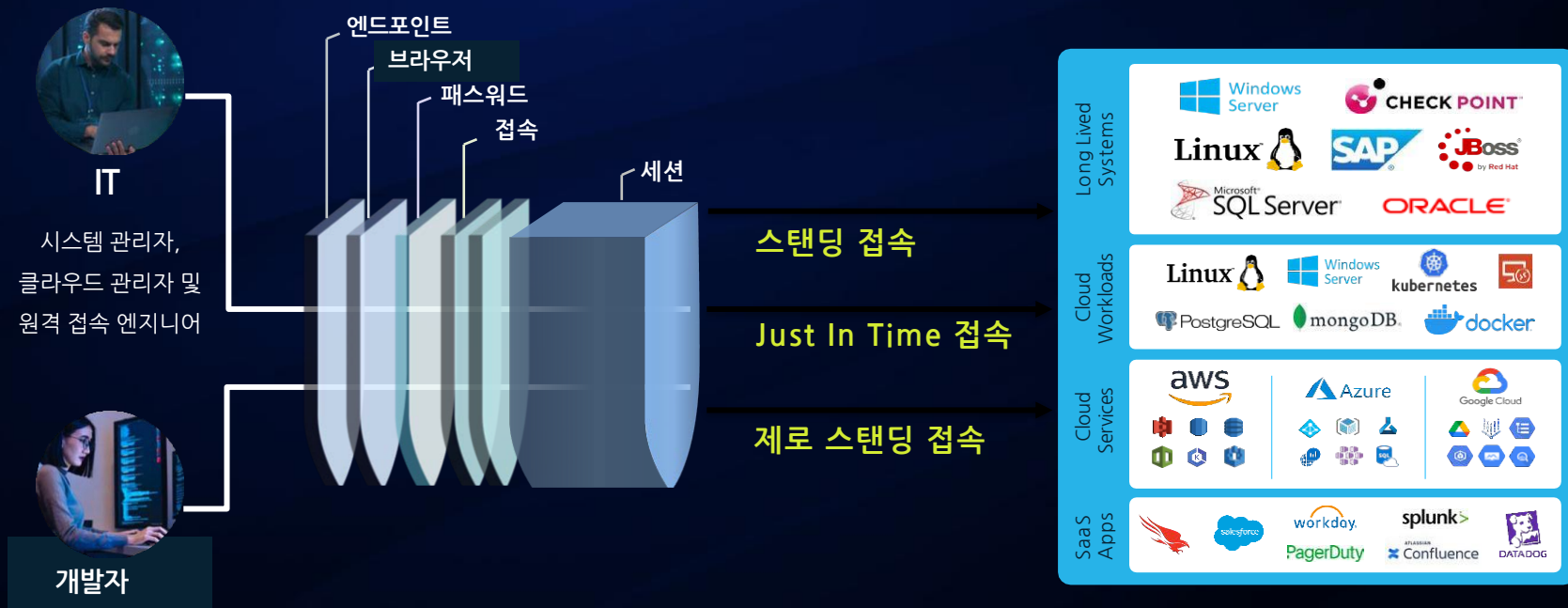


세션



인증 전후 단계별 보안을 위한 계층적 권한 제어

현대적 환경에서 IT 및 개발자 접근 보호



- 클라우드 콘솔/CLI 접근
- 아이덴티티가 보호되고 모니터링되는 세션

- Vault 없는 접속
- 세션 중계 및 모니터링

- 시스템 접근 및 비상 접근
- 다단계 보안 제어 기반의 자격 증명 저장

제로 트러스트 핵심 블루 프린트 제공



WHITEPAPER

Addressing the Department of Defense's Zero Trust Framework with the CyberArk Identity Security Platform

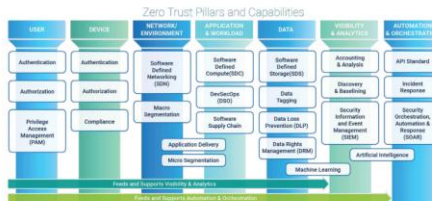
A Technical Review of how Federal Agencies can Leverage CyberArk Identity Security Solutions to Align to the DoD's Zero Trust Reference Architecture.

Introduction

In the spring of 2021, the White House issued an executive order putting into place guidelines on how to improve the nation's cybersecurity stance. This requires federal agencies to modernize their approach to cybersecurity by becoming more transparent about cyber threats for protection. Government agencies are required to move toward a Zero Trust architecture, which calls for an "assume breach" mindset and secures all cloud services. Federal agency heads must develop a plan for implementing the ZT Architecture and incorporate guidelines from the National Institute of Standards and Technology (NIST) as appropriate.

With the cybersecurity executive order in place, the U.S. Department of Defense recently published its Zero Trust Reference Architecture. What's important to note is that the newly revised DISA Zero Trust Architecture now includes the addition of privileged access management (PAM).

This technical whitepaper will outline the importance of PAM controls that are necessary to align with the DISA Zero Trust reference architecture and why federal agencies need to follow the government's recommendations for implementing a Zero Trust framework.



WHITEPAPER

www.cyberark.com

WHITEPAPER

Zero Trust Privileged User Credential Boundaries

CyberArk helps provide secure privileged user session isolation and create credential boundaries, giving only the right people access to the privileged resources. Monitoring and recording capabilities enable security teams to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions and maintain a comprehensive, searchable audit trail of privileged user activity. Native and transparent access to multiple cloud platforms and web applications provides a unified security approach with increased operational efficiency.

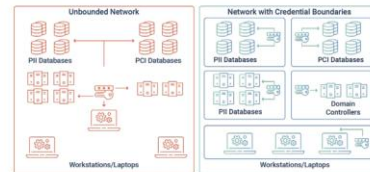
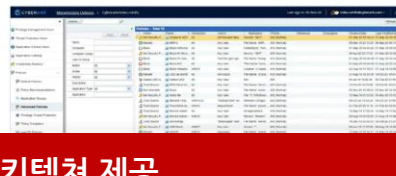


Figure 20: Mitigating privileged risk through established credential boundaries.

Zero Trust for Applications

CyberArk Endpoint Privilege Manager provides "allow" and "deny" list capabilities that quickly identify and block malicious applications. Leveraging CyberArk's Application Risk Analysis to quickly determine risk associated with any application streamlines policy definitions and aids in preventing malicious applications from running in the environment.



www.cyberark.com

www.cyberark.com

NIST 800-207 제로 트러스트 핵심 7가지 원칙 준수를 위한 아키텍처 제공

CYBERARK

CYBERARK

인증현황 & 고객사례

인증현황



DoDIN APL (미 국방부 공식 승인)

- 미 국방부(DoD) 육·해·공군 및 펜타곤 전산망 공식 신뢰 솔루션 등재
- 글로벌 항공방산 공급망 보안 규격(CMMC)을 충족하는 군사 표준 보안성



FedRAMP High (미 연방 클라우드 최고 등급)

- 국가 안보와 직결된 초민감 군사·정부 데이터를 다룰 수 있는 최상위 클라우드 인증
- 스마트 팩토리 및 원격 야드 환경에 안전한 제로 트러스트(SaaS) 보안 제공



Common Criteria (국제 CC 인증 - NIAP)

- 미국 국가안보국(NSA) 주도 NIAP 스키마를 통해 핵심 모듈 전체 인증 획득
- 솔루션 자체의 백도어 리스크 유무와 OT 망 우회 침투 차단 성능 공인

업무 생산성을 저해하지 않는 특권 권한 관리

로크웰 오토메이션, 선제적인 특권권한 관리 (PAM) 프로비저닝 통제를 위해 IDIRA(CyberArk) 도입

북 아메리카

목표 관리되지 않는 특권 계정과 관련된 식별된 리스크를 감소 및 완화하고, COBIT의 DS5.4(사용자 계정 관리)에 정의된 감사 요구사항을 충족함.

솔루션 특권 계정 및 자격 증명(Credentials)을 관리하고 보호하며, 세션을 격리 모니터링 하고, 위협을 탐지 하여 이에 대응함

결과 비밀번호 관리 자동화를 통한 리스크 감소
운영 비용 절감
온보딩(신규 등록 및 적응)프로세스 개선
특권 권한 접속(접근)프로세스 효율화

“ IDIRA(CyberArk)는 조직 전체로 확장하기에 매우 효율적이고 훌륭한 제품 기능을 제공해 주었습니다. 또한, 사이버아크의 솔루션은 다른 보안 툴에 비해 배포 속도가 훨씬 빠르다는 것이 입증되었으며, 덕분에 짧은 시간 내에 고품질의 인사이트를 얻을 수 있었습니다 ”

제인 리틀(Jayne Little)

로크웰 오토메이션 정보보안 엔지니어 (특권 권한 관리 담당)

<https://www.cyberark.com/resources/customer-stories>

국내외 주요 고객사



권한 접근관리 솔루션 소개

Privilege Access Management

모든 세션 제어 및 모니터링

대상 시스템 접근 세션에 대한 모니터링 및 감사



ISOLATE

사용자로부터 대상 시스템으로의
직접적인 접근 차단



MONITOR

이상 행위 탐지 및 실시간 이벤트
생성을 통한 모니터링 및 추적 제공



RECORD

모든 행위 상세 감사 및 포렌시 분석 제공
(동영상 재생 및 입력 명령어의 텍스트
기반 기록)

모든 세션 제어 및 모니터링

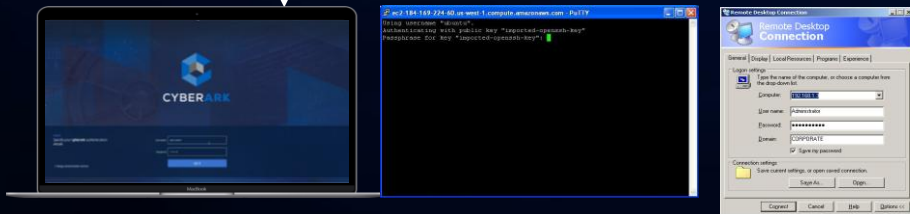
원격접속 사용자의 모든 세션은 타겟 업무시스템과 이원화 시키고, 모든 내역을 모니터링



접속 계정 탈취 차단 및 모든 세션 감사



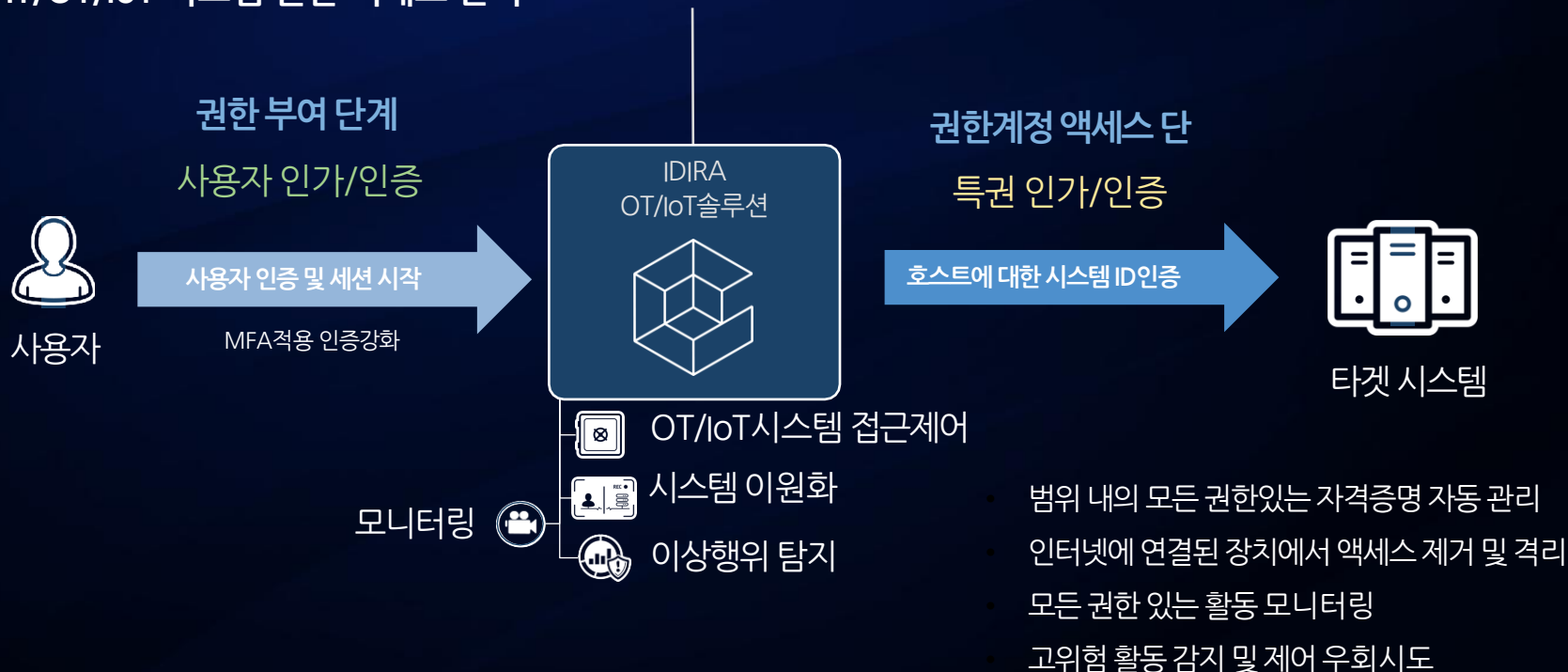
- Isolates 기업내 중요 서버 접속에 대한 세션 분리 제공
- Secure 효율적인 접속 관리 및 보안을 위한 단일 포인트 제공
- Audit 대상 시스템 접속 세션 활동에 대한 감사 제공



CYBERARK 웹 포탈 - OR - 선호 방식의 어플리케이션

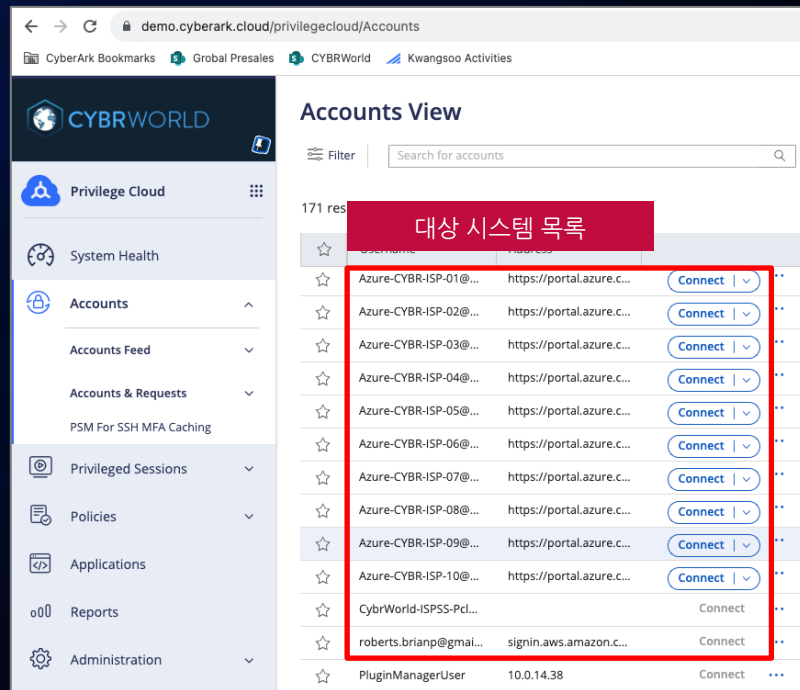
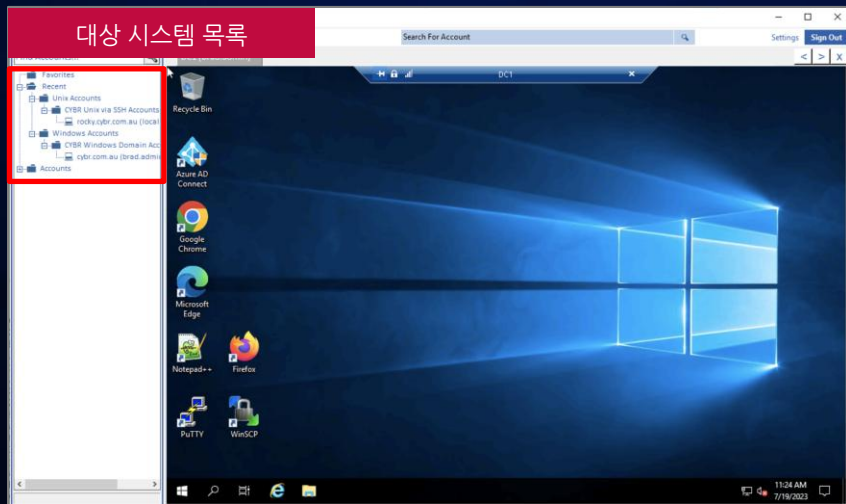
IT보안 강화를 통한 OT보안

IT/OT/IoT 시스템 권한 액세스 관리



대상 시스템 접속 프로그램

단일화된 Client 프로그램 또는 웹 포탈을 통해 대상 시스템에 권한 접속 지원



데이터베이스 권한관리

SQL패스워드 관리 및 접근제어, NoSQL 권한관리 지원

The screenshot displays the CyberArk Privilege Cloud Monitoring interface. The sidebar on the left contains navigation links for System Health, Accounts, Accounts Feed, Accounts & Requests, PSM For SSH MFA Caching, Privileged Sessions, Monitoring, Monitoring (Classic UI), Policies, Applications, Reports, and Help. The main content area is titled 'Monitoring' and shows 'Recordings' and 'Active sessions'. A session for 'tamir.benari@cyberarklab.com' is selected, displaying a timeline of activities. A red box highlights the '세션 레코딩 플레이' (Session Recording Play) button and the 'Activities' section, which lists SQL commands executed during the session.

세션 레코딩 플레이

Activities

6 Activities in the session

Aug 01 Tuesday

3:42:35 PM SQLCommand | SELECT DECODE(USER, 'XS\$NULL', XS_SYS_CONTEXT('XS\$SESSION', 'USERNAME'), USER) FROM SYS.DUAL

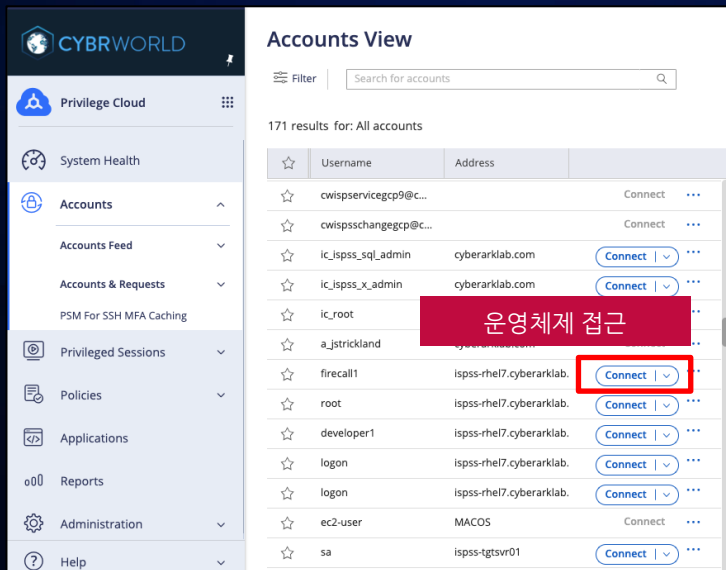
3:42:35 PM SQLCommand | BEGIN DBMS_APPLICATION_INFO.SET_MODULE(1, NULL); END;

3:42:54 PM SQLCommand | select * from dual

3:43:02 PM SQLCommand | select sysdate from dual

운영체제

단일화된 Client 프로그램 또는 웹 포탈을 통해 대상 시스템에 권한 접속 지원



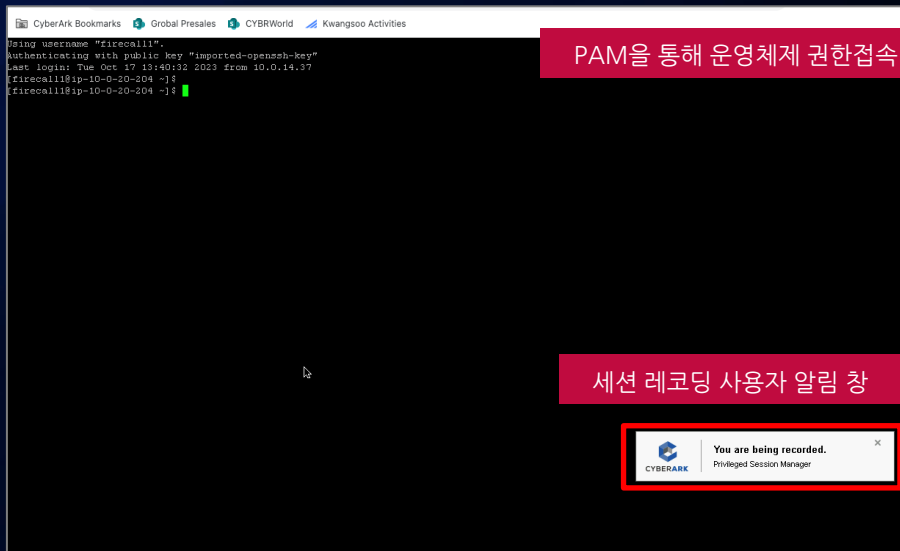
Accounts View

Filter | Search for accounts

171 results for: All accounts

☆	Username	Address	
☆	cwispervicecp9@...		Connect ...
☆	cwispsschange9@...		Connect ...
☆	ic_isspss_sql_admin	cyberarklab.com	Connect v ...
☆	ic_isspss_x_admin	cyberarklab.com	Connect v ...
☆	ic_root		...
☆	a_jstrickland		...
☆	firecall1	ispss-rhel7.cyberarklab.	Connect v ...
☆	root	ispss-rhel7.cyberarklab.	Connect v ...
☆	developer1	ispss-rhel7.cyberarklab.	Connect v ...
☆	logon	ispss-rhel7.cyberarklab.	Connect v ...
☆	logon	ispss-rhel7.cyberarklab.	Connect v ...
☆	ec2-user	MACOS	Connect ...
☆	sa	ispss-tgtsvr01	Connect v ...

운영체제 접근



CyberArk Bookmarks Global Presales CYBRWorld Kwangsoo Activities

```
Using username "firecall1".
Authenticated with public key "imported-openssh-key"
Last login: Tue Oct 17 13:40:32 2023 from 10.0.14.37
firecall1@p-10-0-20-204 ~$
firecall1@p-10-0-20-204 ~$
```

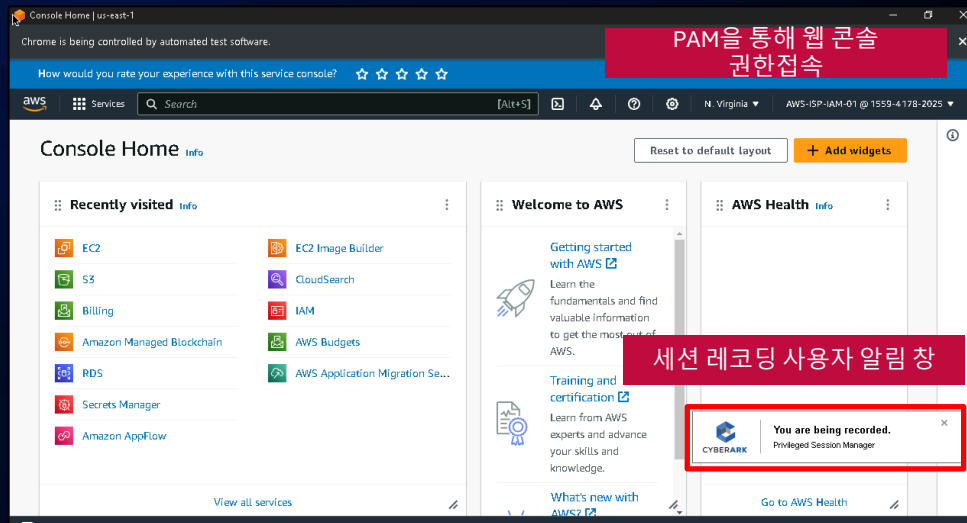
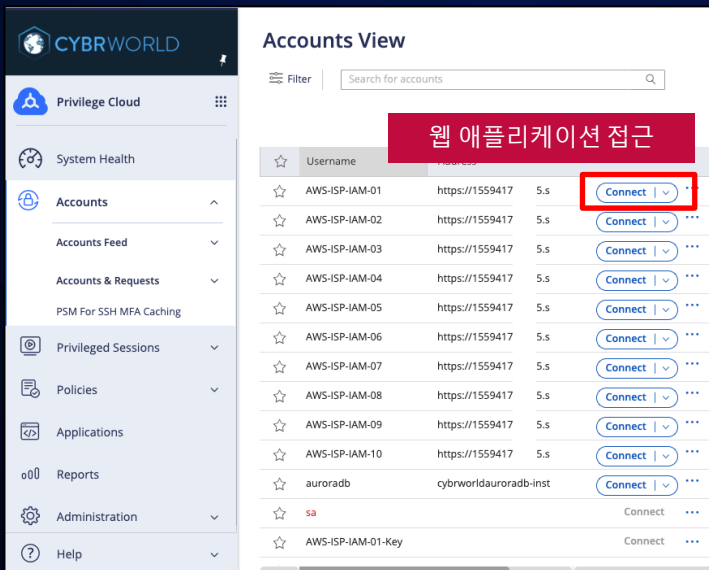
PAM을 통해 운영체제 권한접속

세션 레코딩 사용자 알림 창

You are being recorded.
Privileged Session Manager

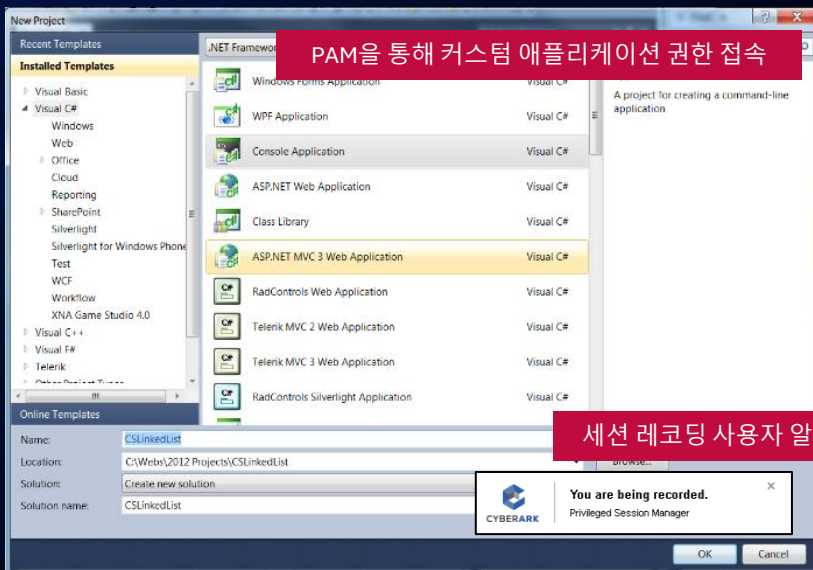
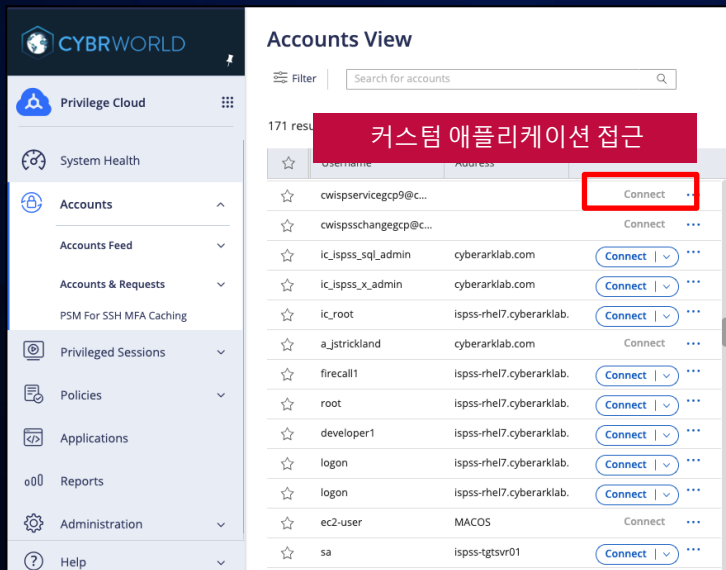
웹 애플리케이션 권한관리

그룹웨어, CSP콘솔, 보안솔루션 등 모든 웹 애플리케이션 권한관리 지원



커스텀 애플리케이션 권한 관리

직접 개발한 커스텀 애플리케이션 권한관리 지원



네트워크 장치 권한관리

SSH프로토콜을 통해 접근하는 모든 네트워크 장치 권한 관리 및 비밀번호 관리

CYBERWORLD

Privilege Cloud

System Health

Accounts

Accounts Feed

Accounts & Requests

PSM For SSH MFA Caching

Privileged Sessions

Policies

Applications

Reports

Administration

Help

Accounts View

Filter

171 results for: All accounts

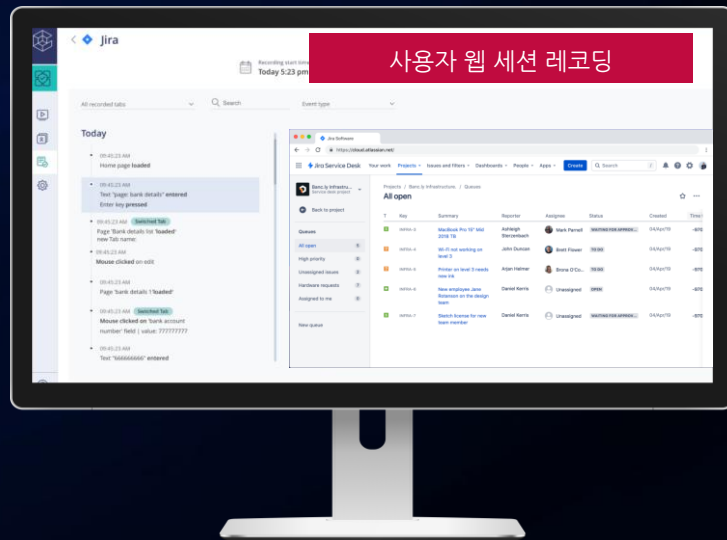
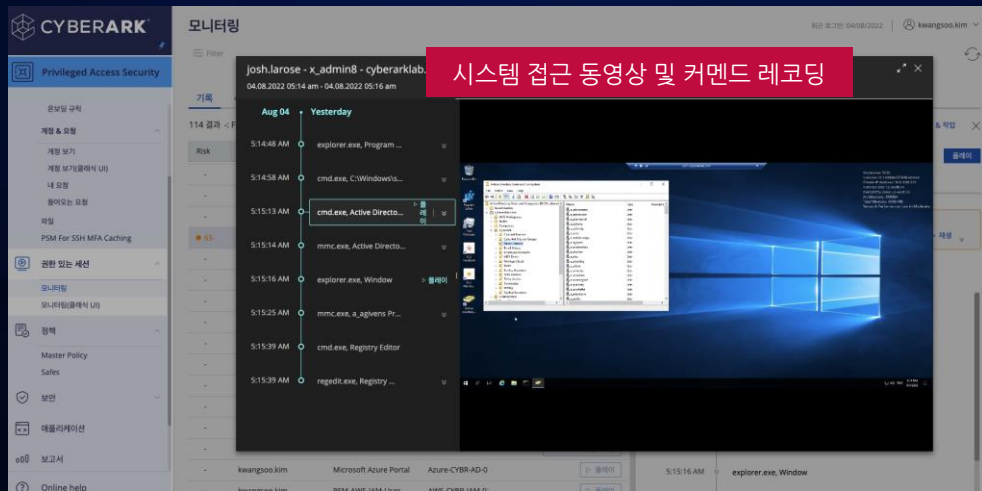
네트워크 디바이스 접근

Star	Account Name	Domain	Action
☆	l_admin	CYBERARKLAB.COM	Connect
☆	adminy-admin	cybr.com	Connect
☆	xsa	cybr.com	Connect
☆	isp_t_admin	CYBERARKLAB.COM	Connect
☆	isp_t_admin1	CYBERARKLAB.COM	Connect
☆	isp_t_admin10	CYBERARKLAB.COM	Connect
☆	isp_t_admin2	CYBERARKLAB.COM	Connect
☆	isp_t_admin3	CYBERARKLAB.COM	Connect
☆	isp_t_admin4	CYBERARKLAB.COM	Connect
☆	isp_t_admin5	CYBERARKLAB.COM	Connect
☆	isp_t_admin6	CYBERARKLAB.COM	Connect
☆	isp_t_admin7	CYBERARKLAB.COM	Connect
☆	isp_t_admin8	CYBERARKLAB.COM	Connect

```
COM3 - PuTTY
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>enable
LABSWITCH#write e
LABSWITCH#write erase
Erasing the nvram filesystem will remove all configurat
firmly[OK]
Erase of nvram: complete
LABSWITCH#
*Mar 1 00:05:57.405: %SYS-7-NV_BLOCK_INIT: Init
LABSWITCH#reload
Proceed with reload? [confirm]
```

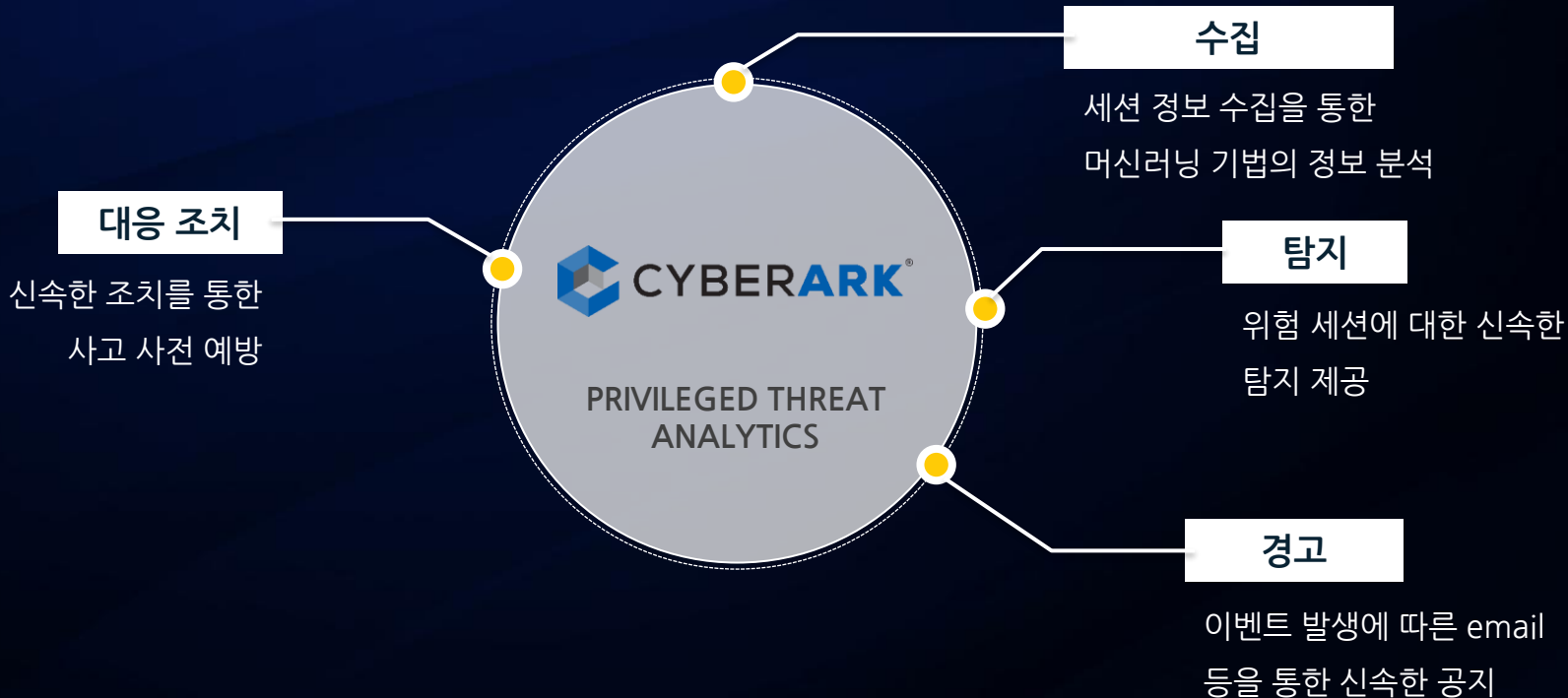
세션 레코딩

시스템 작업 내역 및 사용자 웹 세션 모든 행위 레코딩



위험 세션 탐지 및 대응

모든 접속 세션의 행위 분석을 통한 위협 탐지 및 대응 (세션 중지, 종료 및 모니터링)



위험 세션 탐지 및 대응 (1/2)

위험 탐지에 따른 위험점수 기반의 이벤트 제공

Privileged Access Security

온보딩 규칙

계정 & 요청

계정 보기

계정 보기(클래식 UI)

내 요청

들어오는 요청

파일

PSM For SSH MFA Caching

권한 있는 세션

모니터링

모니터링(클래식 UI)

정책

Master Policy

Safes

보안 사건

최근 로그인: 04/08/2022 | kwangsoo.kim

Filter

5

의심스러운 세션 활동 탐지

Aug 04 Yesterday

9:41:33 PM 100 HIGH

권한 있는 세션에서 의심스러운 활동이 감지됨 수정 시작됨
권한 있는 세션에서 <https://portal.azure.com>의 의심스러운 세션 활동이 감지되었습니다.
이 세션은 Azure-CYBR-AD-01@cyberark365globalabs.onmicrosoft.com@<https://portal.azure.com> 계정을 가진 Vault 사용자 amit.bendavid(가) Task Manager - Google Chrome 활동을 실행하여 시작되었습니다.

ID 62ebbe7fe4b0c59a465aa63b Close

세션 ID 0fca164e-f49a-4750-b8f4-f52a003e9b95

Vault 사용자 amit.bendavid

Cyberark PAS

대상 서비스 <https://portal.azure.com>

권장
세션 종료 요청이 시작되었습니다. 세션 및 해당 활동과 관련된 각 보안 이벤트를 검토하고 추가 대응이 필요한지 평가하십시오.

8:42:51 PM MEDIUM

비관리 권한 계정 수정 시작됨
계정 stefen.jwZwRFwn4fxk8@tgtsvr01.cyberarklab.com(가) tgtsvr01.cyberarklab.com에서 로컬 권한 그룹 Administrators에 추가되었지만 이 계정은 CyberArk PAS에서 관리되지 않습니다.

ID 62ebb0d2e4b0c59a465a26ce Close

위험 세션 탐지 및 대응 (2/2)

특정 명령어 수행에 따라 위험 점수 및 행위 발생에 따른 대응(차단, 중지, 모니터링) 설정

위험요소별 점수 및 대응 설정					
카테고리	패턴	점수	설명	용답	상태
SSH	(.*)id_rsa.pub(.*)	50	Indication of access to Linux key stores might be indica...	없음	활성 상태
SSH	(.*)identity.pub(.*)	50	Indication of access to Linux key stores might be indica...	없음	활성 상태
SSH	(.*)useradd(.*)	60	Indication of adding a user,which could indicate the cre...	일시 중지	활성 상태
SSH	(.*)history(.*)	70	represents a set of commands that may indicate a use...	일시 중지	활성 상태
SSH	(.*)authorized_keys(.*)	60	Manipulation of SSH keys on the machine. Could indica...	없음	활성 상태

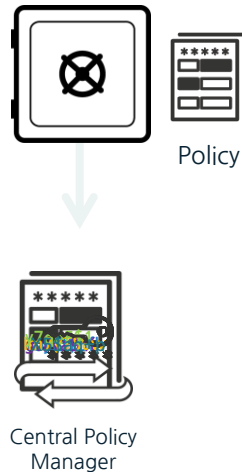
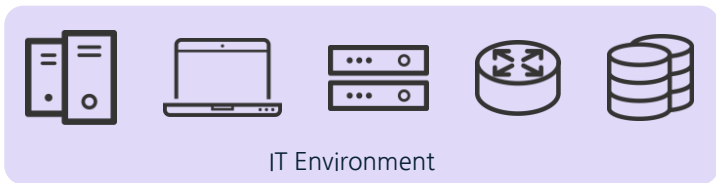
- 관리되지 않는 계정 등록
- 패스워드 강제 변경
- 세션 강제 종료 또는 중지

The image is a composite of two screenshots. The top screenshot shows a '규칙 편집' (Rule Edit) window. It has a '카테고리' (Category) dropdown set to 'SSH'. The '패턴' (Pattern) field contains '(.*)passwd(.*)', which is highlighted with a red rectangle. Below this is a '설명(선택 사항)' (Description (optional)) field. On the left, under '세션 용량' (Session Capacity), the '일시 중지' (Suspend) radio button is selected. On the right, under '점수' (Score), '점수 설정(1 - 100)' (Score Setting (1 - 100)) is set to 100, and '상태' (Status) is '활성 상태' (Active), indicated by a blue toggle switch. The bottom screenshot shows a terminal window with the prompt 'root01@unw1:~'. The command '[root01@unw1 ~]\$ passwd' is entered, and the password field is redacted with a green box. At the bottom right, a white box with a blue 'CYBERARK' logo contains the text: 'Your session has been suspended. Please contact your system administrator'.

패스워드 및 SSH Key관리

특정 명령어 수행에 따라 위험 점수 및 행위 발생에 따른 대응(차단, 중지, 모니터링) 설정

사이버아크의 솔루션에서는 일반적인
패스워드는 물론 SSH key에 대한
변경관리까지 제공함



System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t

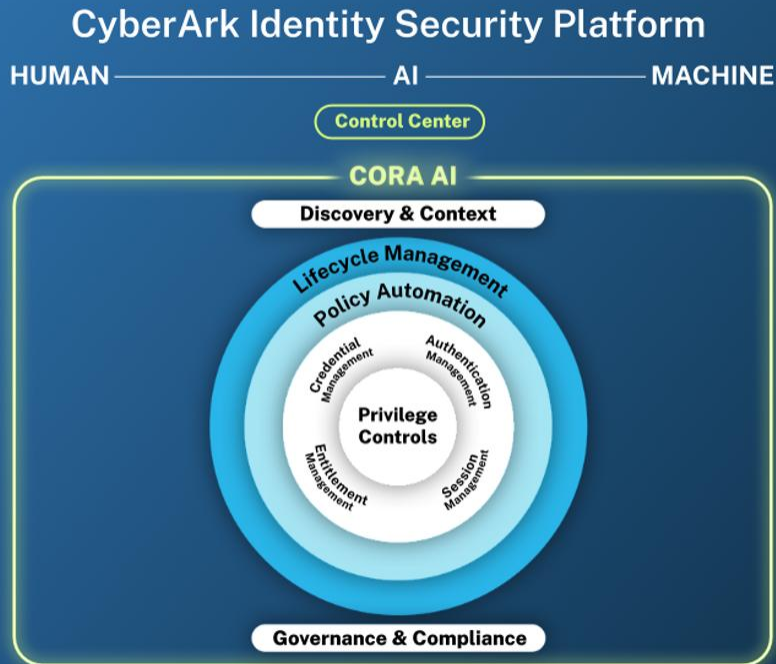


아이덴티티 플랫폼 확장

사이버아크 아이덴티티 보안 플랫폼

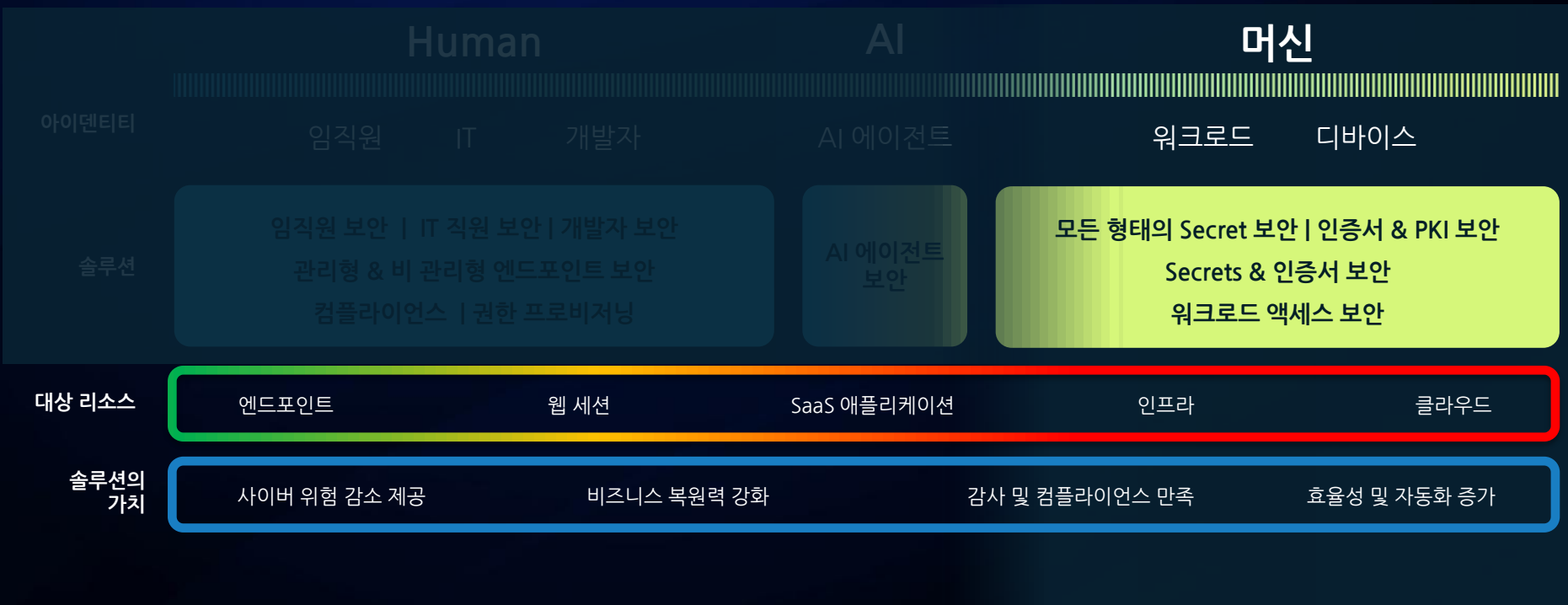
현대적인 아이덴티티 보안

- PAM, SSO, MFA 등 통합 아이덴티티 운영 자동화로 운영 감소, TCO 절감, 운영 효율 향상
- 사이버아크 핵심 클라우드 이전
 - 업그레이드 및 서버 운영 부담 제거
 - 운영 범위 축소 및 확장성, 성능 향상
- 커넨터 기반 구성요소 업그레이드 단순화
- No Code 기반 아이덴티티 워크 플로우 자동화 (3rd Party 연동 단순화)
- AI, ML 기반 전 영역 자동화 (탐지, 분석, 정책, 조치 등)



IDIRA 아이덴티티 보안 플랫폼

Powered by CORA AI



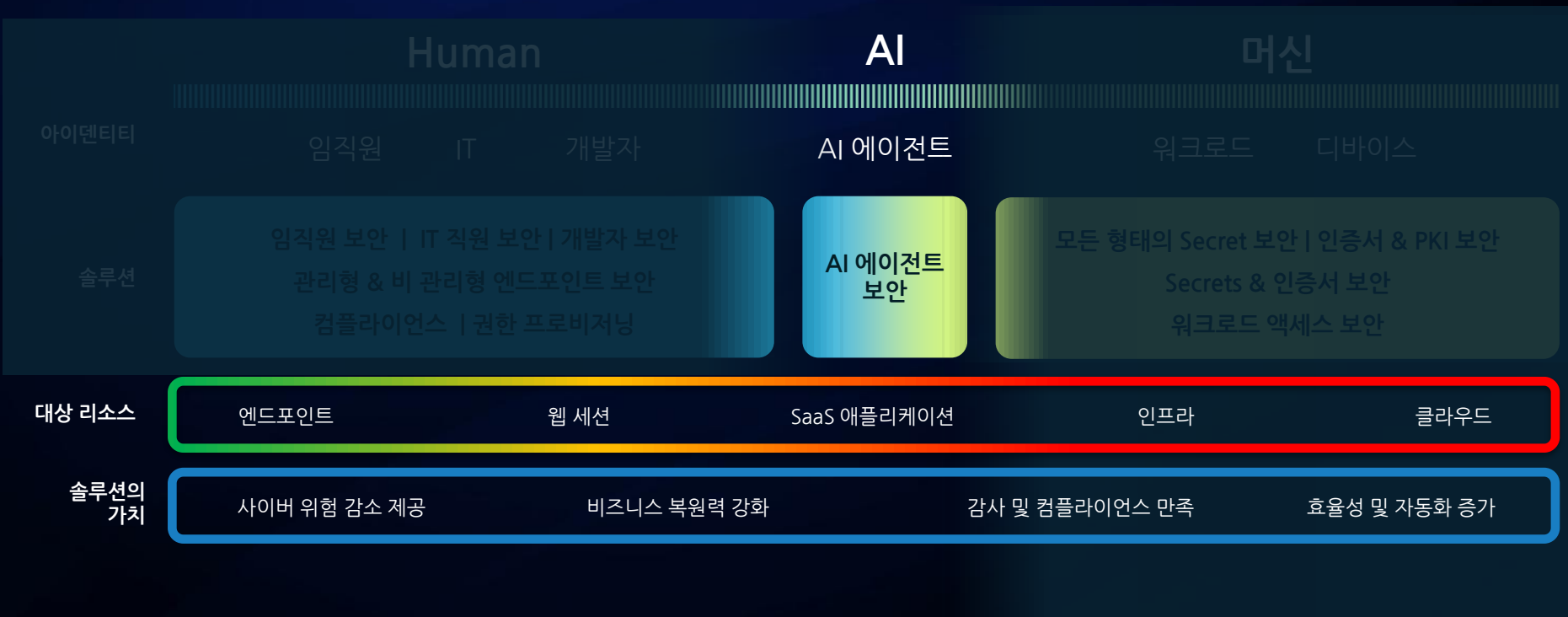
하이브리드 환경의 머신 아이덴티티 보안

 IOT / OT 프린터, 모바일폰, 카메라 등	 3rd Party Apps 위협 스캐너, RPAs, 탐지		 Homegrown Apps			 Cloud Native Apps 동적 CI/CD 파이프라인		
	RPA	보안솔루션	IT Ops	Custom Apps	App Servers	DevOps Tools	컨테이너 플랫폼	퍼블릭 클라우드
  	   	    	    	  	   	   	  	  
Gateway Connectors	Credential Providers CP, Central CP, Application Server CP					Conjur Enterprise	Conjur Cloud	Secrets Hub

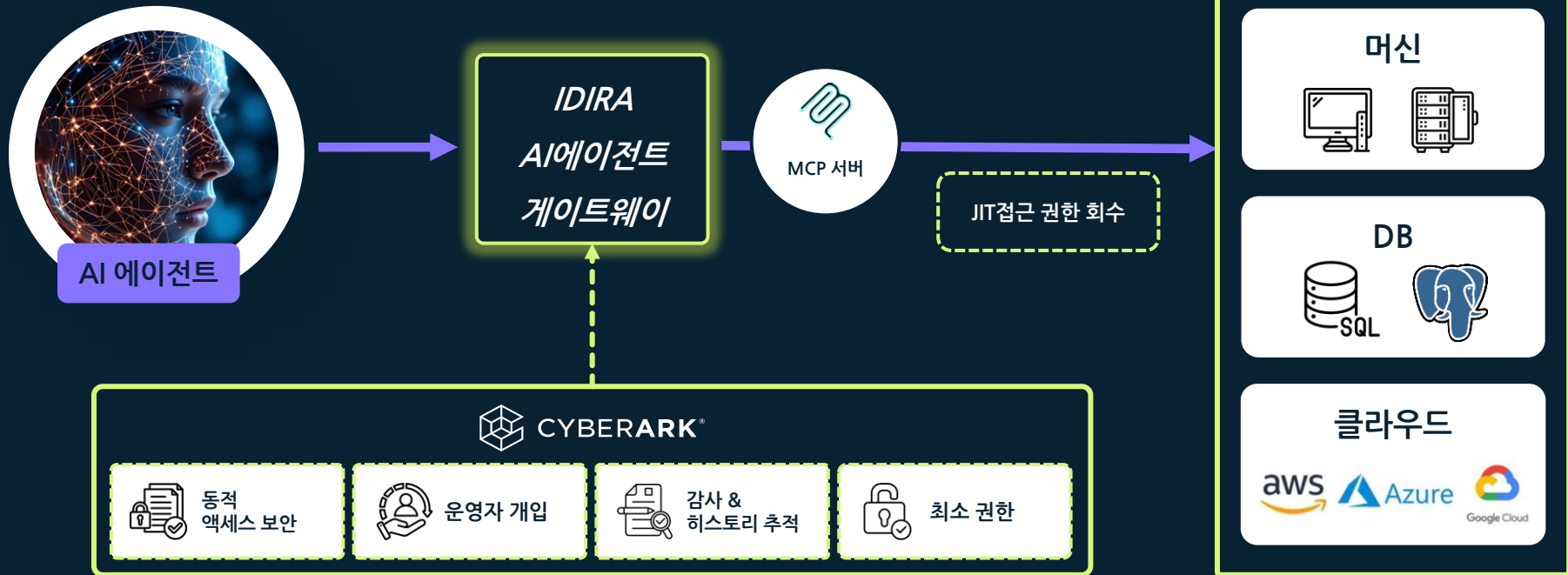
SaaS

IDIRA 아이덴티티 보안 플랫폼

Powered by CORA AI



AI 에이전트 접근 제어 보안



IDIRA 기술 파트너십

230+ Certified Partners



360+ Certified Joint Solutions

Analytics ICS Identity & Access Management Authentication ITSM Detection Orchestration & Response DevOps Robotic Process Automation Discovery SIEM Governance HSM Vulnerability Management

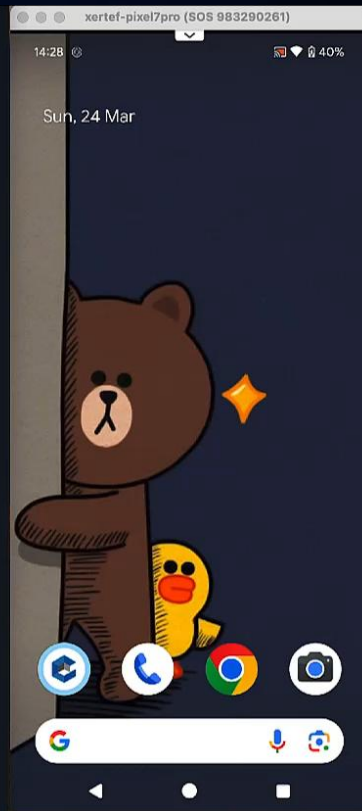
200+ Plug-ins

CPM Plug-ins PSM Plug-ins

데모

2:28

Sunday, March 24



Summary



아이덴티티 보안 리더

- 제로 트러스트 아키텍처 기반의 멀티 클라우드&하이브리드 환경의 차세대 아이덴티티 신원 보안 제공
- Fortune 500대 기업 55% 이상이 사이버아크 솔루션을 통해 보안강화



편리하고 유연한 구성

- 구축형, SaaS형 구축 옵션 제공
- Agentless 구성으로 대성 서버 및 사용자 PC에 Agent 설치 불필요
- 다양한 3rd Party 플러그인 제공



아이덴티티 보안 확장 전략

- SSO, MFA, Directory 서비스를 통해 계정 보안 및 편리성 강화
- 머신 아이덴티티 플랫폼 확장을 통해 애플리케이션, 클라우드 워크로드, CI/CD, SSL/TLS, SSH Key 보안 강화
- AI 엔진을 통해 보안정책, 라이프사이클 관리 등 자동화



감사 대응, 상시 통제 체계

- 세션 추적, 접근이력, 권한 변경 이력의 완전한 가시성
- 사후 증빙이 아닌 실시간 통제 기반 컴플라이언스

Thank You

paloaltonetworks.com

솔루션 엔지니어 김광수

kwkim@paloaltonetworks.com

권한 접근관리 솔루션 상세

Privilege Access Management

외부 네트워크(인터넷)

Level: External
Cloud Services



Level: External
Remote Access



사내 네트워크



Level 5 Network
Internet



웹 서버



이메일 서버

Level 4 Network
IT



도메인 컨트롤러



애플리케이션 서버



업무용 단말



Level 3.5 IDMZ 관리 네트워크

OT 네트워크

Level 3 Network
Operations



도메인 컨트롤러



데이터베이스



업무용 단말

Level 2 Network
Process



Local HMI



IP기반 컨트롤러

Level 1 Network
Control



PLCs



Remote I/O Devices

Level 0 Network
Field



센서

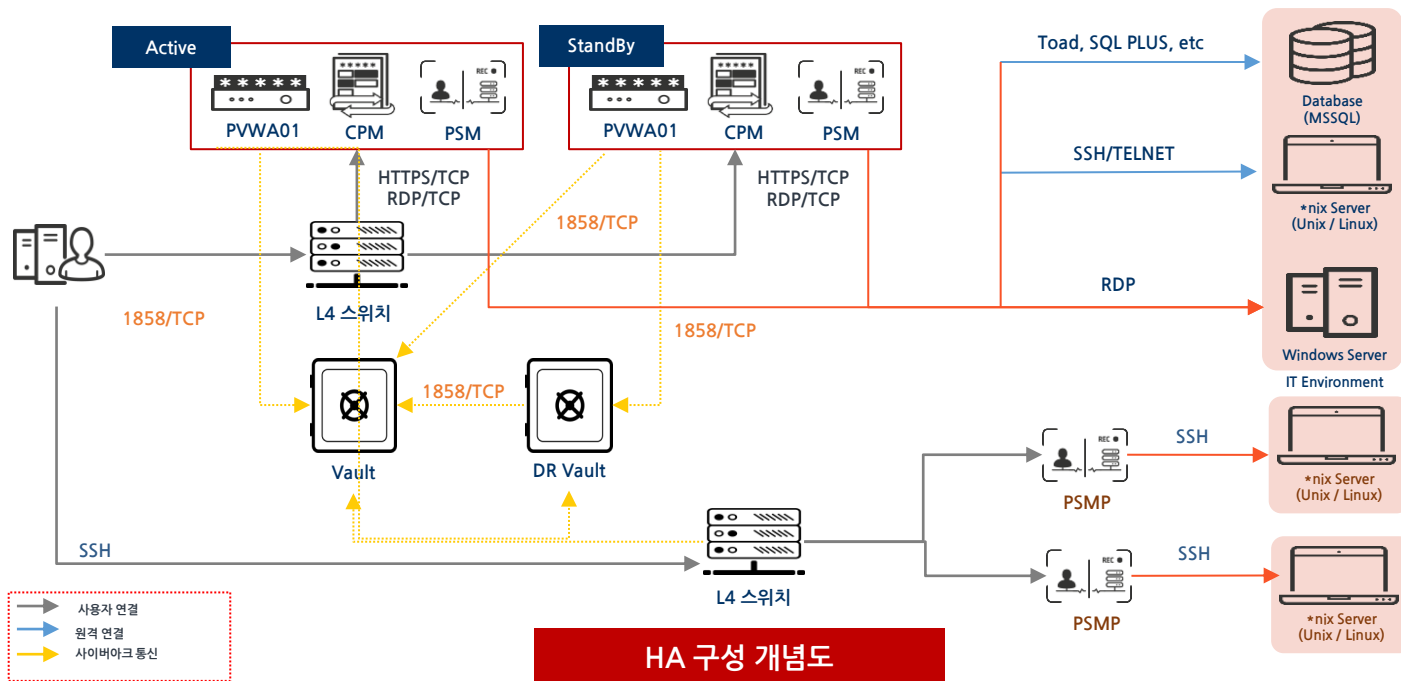


Actuators

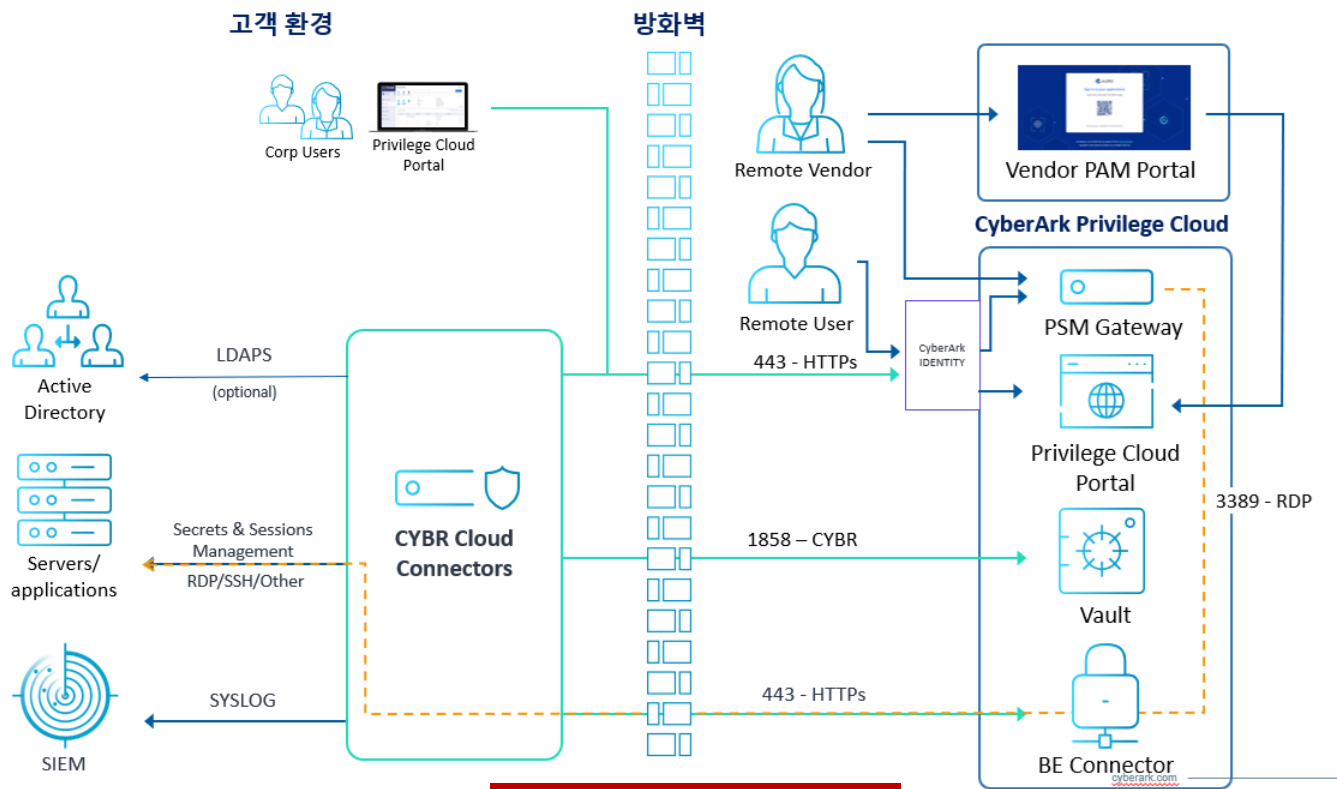
외부 네트워크 및 기타 네트워크에서 액세스 보호

- IT보안 강화를 통한 OT보안
- 운영 네트워크 보안강화
- 안전한 원격 액세스
- OT단말 인증정보 보안 강화

이중화 구성과 같은 서비스 가용성 확보를 위한 기능 제공 - 구축형

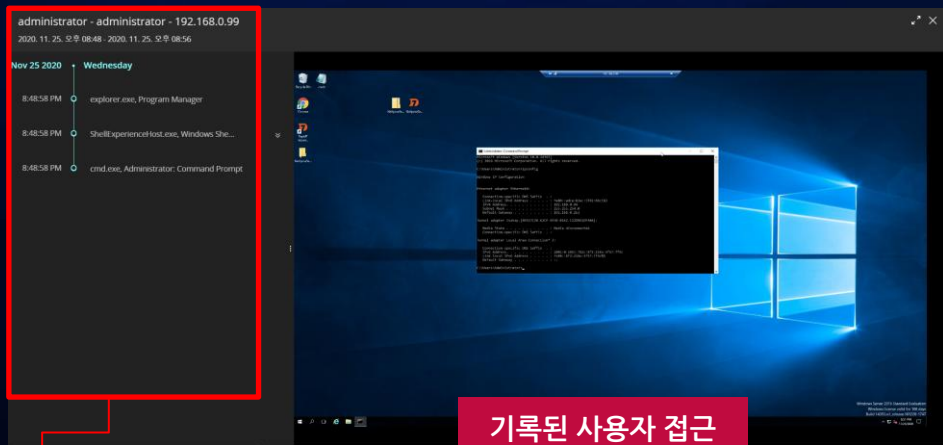


이중화 구성과 같은 서비스 가용성 확보를 위한 기능 제공 - SaaS 형



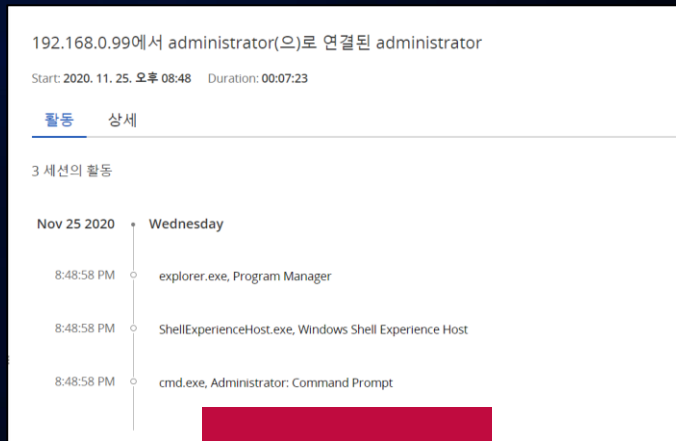
SaaS 구성 개념도

SSH, SFTP, RDP등 원격 접속 프로토콜을 제공하여 모든 접근 상세히 기록



세션 활동 확인 가능
(클릭 시 화면 이동)

기록된 사용자 접근
영상 상세 영상 화면



작업 내역 기록

키 기반 인증방식의 SSH 프로토콜 접근 지원

Add Account Last sign in: ...

✓ Select system type
*NIX

✓ Assign to platform
Unix via SSH Keys

✓ Store in Safe
Linux SSH Keys

4 Define properties

4. Define account properties

Primary properties

Address
psm01.cyberarklab.com

Username
firecall1

SSH Private key

Select file Paste content

Drop file or click to browse

☐ Customize account name

계정 등록 시 키 기반 인증방식
설정

☆	Status	Username ↓	Address	Platform ID	Safe	
☆	-	firecall1	rhel07.cyberarklab.co...	UnixSSH	Linux Root Accounts	Connect
☆	-	firecall1	rhel07.cyberarklab.co...	UnixSSHKeys	Linux Root Accounts	Connect
☆	-	dso-user1		MySQL	DSO-DevSecOps-Use...	Connect
☆	-	developer1	rhel07.cyberarklab.co...	UnixSSH	Linux User Accounts	Connect
☆	-	dev01	dso-devsecops-01.cy...	UnixSSH	DSO-DevSecOps-Use...	Connect
☆	-	CYBRWorldINT	cybrworld.service-no...	ServiceNow	ServiceNow Integration	Connect

키 인증 기반 인증 계정 등록
완료

```
Using username "firecall1".
Authenticating with public key "imported-openssh-key"
Last login: wed Dec 7 01:01:57 2022 from psm01.cyberarklab.com
[firecall1@ip-10-0-20-177 ~]$
[firecall1@ip-10-0-20-177 ~]$
[firecall1@ip-10-0-20-177 ~]$
[firecall1@ip-10-0-20-177 ~]$
```

키 인증 기반 계정 접속 성공

SecureCRT, Putty, mRemoteRG 등 외부 원격 접속 프로그램과 연동

```
Using username "firecall1".
Authenticating with public key "imported-openssh-key"
Last login: Fri Jun 16 10:43:16 2023 from 10.0.14.37
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$ pdw
-bash: pdw: command not found
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$ pwd
/home/firecall1
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$ ls
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$ cd ..
[firecall1@ip-10-0-20-204 home]$
[firecall1@ip-10-0-20-204 home]$ ls
david developer developer1 ec2-user firecall1 ic_root login logon monkeys tempadm test test123 test2
[firecall1@ip-10-0-20-204 home]$
[firecall1@ip-10-0-20-204 home]$
[firecall1@ip-10-0-20-204 home]$ cd test
-bash: cd: test: Permission denied
[firecall1@ip-10-0-20-204 home]$
[firecall1@ip-10-0-20-204 home]$ ls
david developer developer1 ec2-user firecall1 ic_root login logon monkeys tempadm test test123 test2
[firecall1@ip-10-0-20-204 home]$ cd ec2-user/
-bash: cd: ec2-user/: Permission denied
[firecall1@ip-10-0-20-204 home]$ ls
david developer developer1 ec2-user firecall1 ic_root login logon monkeys tempadm test test123 test2
[firecall1@ip-10-0-20-204 home]$
[firecall1@ip-10-0-20-204 home]$
```

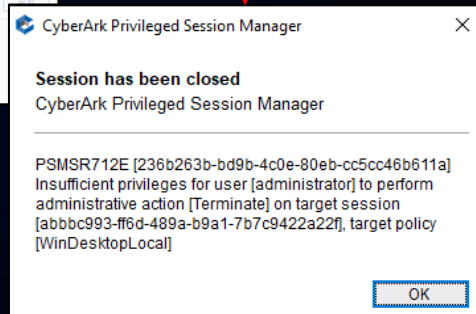
Putty를 통한 접속

실시간으로 사용자의 원격 접근 세션 차단

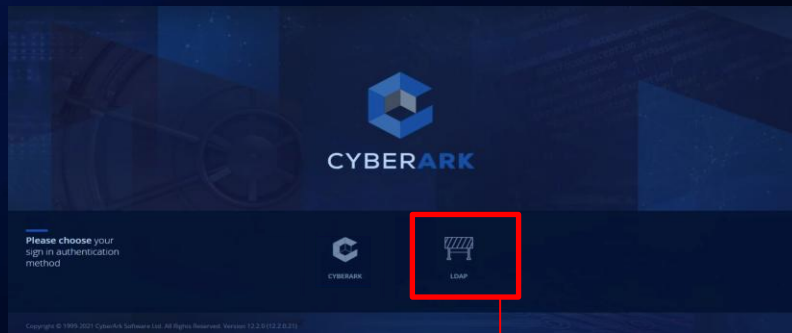
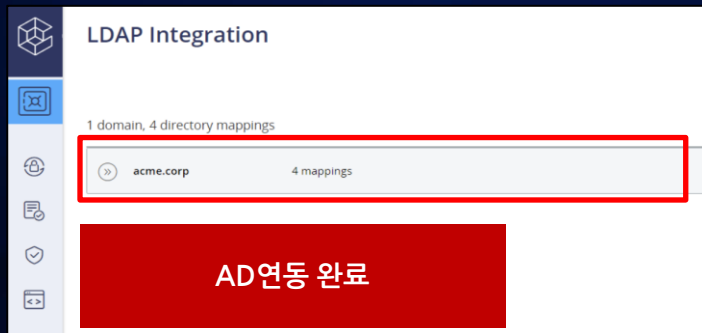
The screenshot shows the CyberArk Privileged Session Manager interface. On the left sidebar, the '모니터링' (Monitoring) icon is highlighted with a red box. A red arrow points from this icon to the '활성 세션' (Active Sessions) link in the top navigation bar, which is also highlighted with a red box. Another red arrow points from the '활성 세션' link to a table of active sessions. The table has columns for '사용자' (User), '시작 IP' (Start IP), '클라이언트' (Client), '계정 사용자 이름' (Account User Name), '계정 주소' (Account Address), '계정 정책 ID' (Account Policy ID), and '시작' (Start). The first row shows a session for user 'lsk' with start IP '192.168.0.55' and start time '2021. 1. 13. 오후 09:54'. A red box highlights the '종료' (End) button for this session, with a red arrow pointing to a dialog box.

사용자	시작 IP	클라이언트	계정 사용자 이름	계정 주소	계정 정책 ID	시작
lsk	192.168.0.55	SSH	sunguk	192.168.0.89	UnixSSH	2021. 1. 13. 오후 09:54
administrator	192.168.0.55	SSH	sunguk	192.168.0.89	UnixSSH	2021. 1. 13. 오후 09:50

악의적인 세션, 위험세션 실시간 강제 차단



Active Directory 도메인 환경에서 계정 연동 및 인증 통합 지원



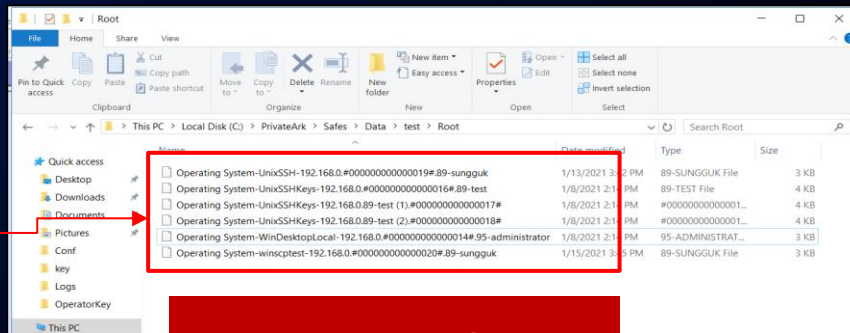
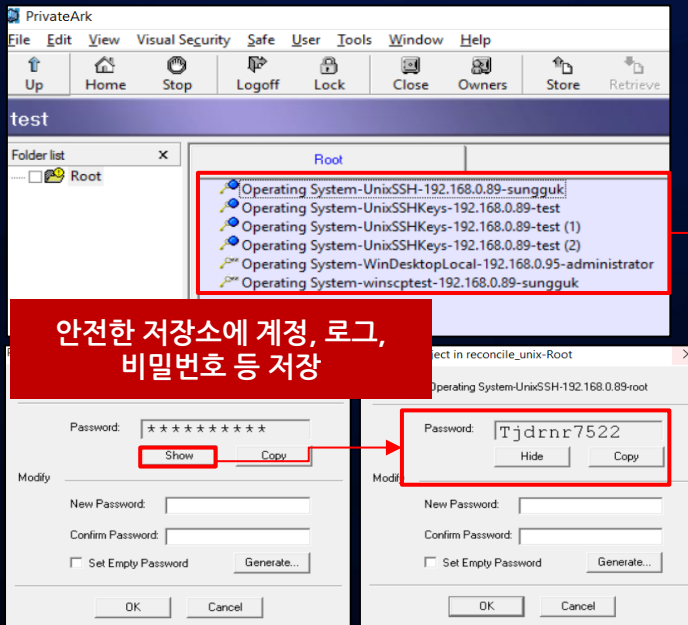
111 results for: All accounts

Status	Username	Address	Platform ID	Safe	
-	x_admin1	cyberarklab.com	WinDomain	Windows Domain Ad...	Connect
-	t_admin1	cyberarklab.com	WindowsDomainAcc...	Windows Domain Ad...	Connect
-	t_admin10	cyberarklab.com	WindowsDomainAcc...	Windows Domain Ad...	Connect
-	t_admin2	cyberarklab.com	WindowsDomainAcc...	Windows Domain Ad...	Connect
-	t_admin3	cyberarklab.com	WindowsDomainAcc...	Windows Domain Ad...	Connect
-	t_admin4				Connect
-	t_admin5				Connect
-	t_admin6				Connect

연동된 AD도메인을 통해 온보딩된 서버 계정 목록

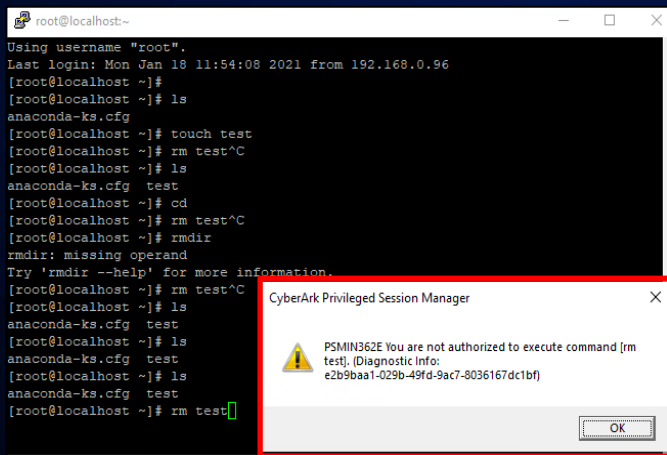
AD사용자 인증

모든 작업 내용 및 결과는 암호화되어 기록, 관리자가 쉽게 검색 할 수 있는 형태로 기록

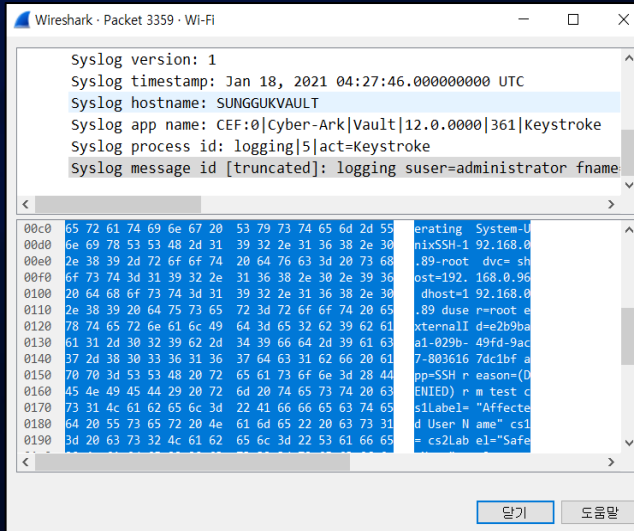


암호화되어 저장됨을 확인

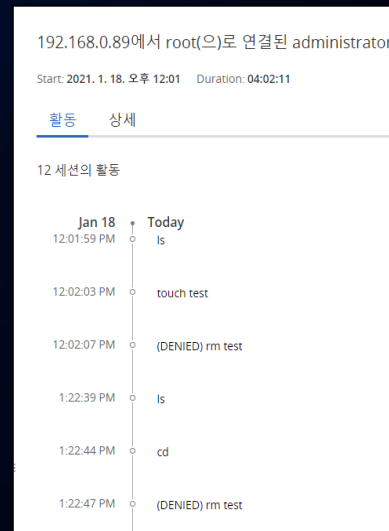
위험 명령어 별 차단 또는 알림 여부 설정 기능



위험 명령어 실행 시 발생하는
알림 캡처 화면

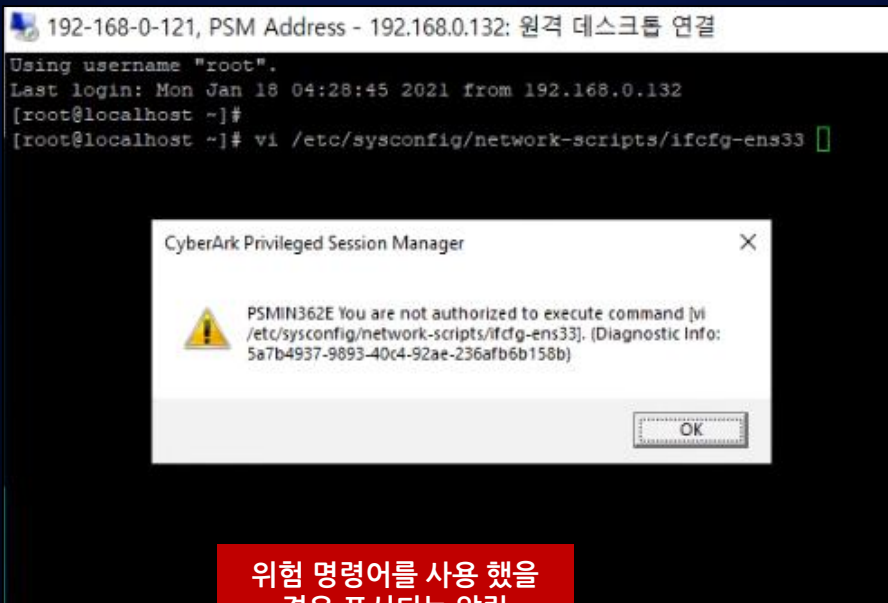


위험 명령어 사용시 syslog
화면

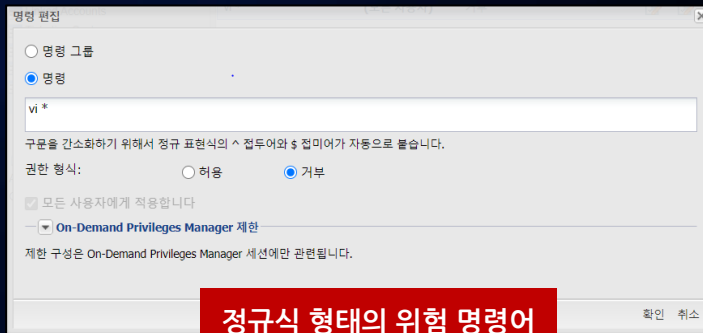


위험 명령어 사용 시 기록
화면

위험 명령어 설정시 정규 표현식을 사용하여 입력 문자열 패턴으로 통제



위험 명령어를 사용 했을
경우 표시되는 알림



정규식 형태의 위험 명령어
설정 화면

접근통제와 패스워드 관리가 단일화된 User Interface 지원

Accounts View Kwangsoo.Kim

Filter | Search for accounts | [Add hoc connection](#) | [Add account](#) | [Refresh](#)

Views | Recent | Saved

My accounts

	Status	Operational state
All accounts (default)	Disabled by CPM	Scheduled for Change
Recently used	Failed	Scheduled for Verification
Favorites	Newly added	Scheduled for Reconciliation
Checked-out	Deleted	Successfully Reconciled

[Show more](#)

18 results for: All accounts [Additional details & actions in classic interface](#)

☆	Status	Username	Address	Platform ID	Safe T	Accou
☆	-	administrator	172.31.8.201	WindowsServerLocal...	kkim team	Opera Connect ...
☆	-	AKIAW32AIVLFBY6B...			Notification Engine	ses-cr Connect ...
☆	-	administrator	172.16.3.174	WinServerLocal	pcloudcon	Opera Connect ...
☆	-	PluginManagerUser	172.16.3.128	PCLLOUDCON2_Accou...		Plugin Connect ...
☆	-	PSMAdminConnect	172.31.200.54	PSM		PSMAi Connect ...
☆	-	PSMAdminConnect	172.16.3.128	PSM		PSMAi Connect ...
☆	-	PSMConnect	172.31.200.54	PSM		PSMSi Connect ...
☆	-	PSMConnect	172.16.3.128	PSM		PSMSi Connect ...

시스템 접근통제

POLICIES Policies > Master Policy

Master Policy [Master Policy](#)

Policy by Platform

▼ Privileged Access Workflows

Policy Rule	Value
Require dual control password access approval	Inactive
Enforce check-in/check-out exclusive access	Inactive
Enforce one-time password access	Inactive
Allow EPV transparent connections ('Click to connect')	Active
Require users to specify reason for access	Inactive

▼ Password Management

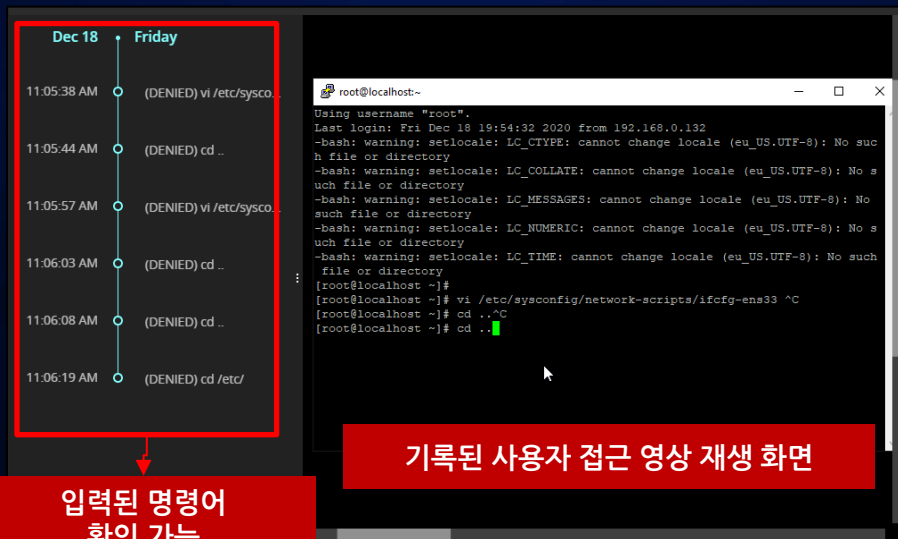
Policy Rule	Value
Require password change every X days	90
Require password verification every X days	7

► Session Management

► Audit

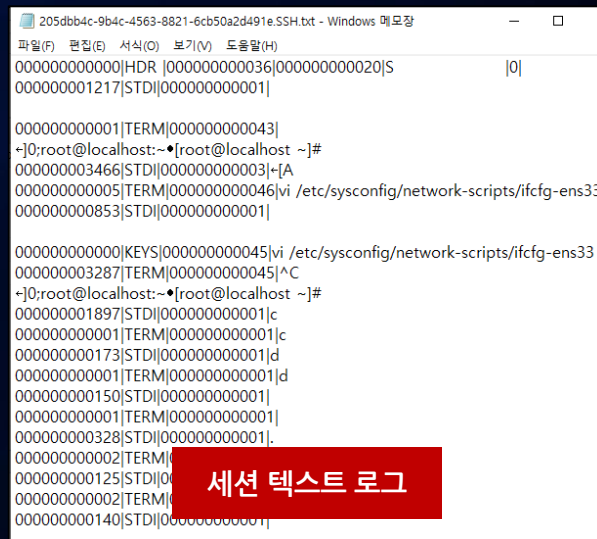
패스워드 관리

CLI 기반의 작업 내역에 대한 기록 및 동영상 재생 기능



입력된 명령어
확인 가능
(클릭 시 화면 이동)

기록된 사용자 접근 영상 재생 화면



세션 텍스트 로그

사용자 로그인 시 패스워드 OTP 추가 인증 연동 지원

Authentication Profile

Profile Name *

Multiple Authentication Mechanisms

Challenge 1

Challenge 2 (optional)

Something you have

☐ Mobile Authenticator
☐ Phone call
☐ OATH OTP Client
☐ Text message (SMS) confirmation code
☐ Email confirmation code
☐ QR Code
☐ FIDO2 Authenticator(s) (single-factor)

Something you are

☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

☐ Password
☐ Security Question(s)
1 Number of questions user must answer

Other

☐ 3rd Party RADIUS Authentication

Something you have

☐ Mobile Authenticator
☐ Phone call
☐ OATH OTP Client
☐ Text message (SMS) confirmation code
☐ Email confirmation code
☐ QR Code
☐ FIDO2 Authenticator(s) (single-factor)

Something you are

☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

☐ Password
☐ Security Question(s)

Other

☐ 3rd Party RADIUS Authentication

OK

Cancel

다양한 OTP 요소 항목

패스워드 정책 설정 기능 제공(문자/숫자/특수문자 혼합, 길이, 제한정책 등)

속성	
항목	값
PasswordLength	8
MinUpperCase	2
MinLowerCase	2
MinDigit	1
MinSpecial	1
PasswordForbiddenChars	#
PasswordEffectiveLength	
PreventSameCharPerPrevPassPosition	No
PreventRepeatingCharacters	No

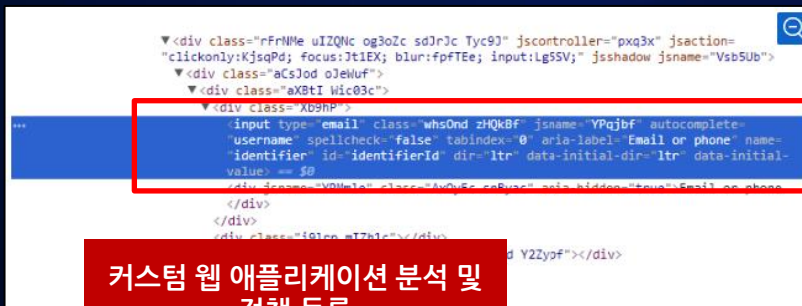
패스워드 복잡도 설정화면

▼ 암호 관리		
정책 규칙	값	예외
X일마다 암호 변경 요구	90	-
X일마다 암호 검증 요구	7	-

자동 패스워드 변경 주기 설정

자동 패스워드 검증 주기 설정

웹 애플리케이션에 대한 연결 환경 제공



111 results for: All accounts

☆	Status	Username	Address	Platform ID ↓		
☆	-	sa	tgtsvr01.cyberarklab.com	MSSql	Connect	...
☆	-	Azure-CYBR-AD-01@cyb...	https://portal.azure.com	MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-	Azure-CYBR-AD-02@cyb...	https://portal.azure.com	MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-			MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-			MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-			MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-			MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-			MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-	Azure-CYBR-AD-07@cyb...	https://portal.azure.com	MicrosoftAzurePasswordManagement-Cybr	Connect	...
☆	-	Azure-CYBR-AD-08@cyb...	https://portal.azure.com	MicrosoftAzurePasswordManagement-Cybr	Connect	...

웹 애플리케이션 등록 완료

