

기업보안의 핵심! 계정 및 권한 관리의 현재와 미래

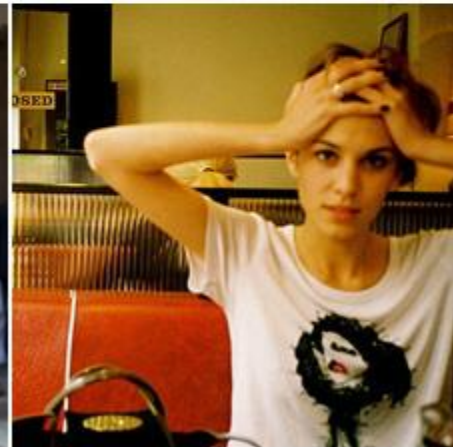

박형근 실장, Information Risk Protection 부문
(securityplus@securityplus.or.kr)

계정 권한 관리?

싱글사인온?

IAM(Identity and Access Management)?

완전 식상한데!!!!!!!!!!!!!!!!!!!!!!





RETRO

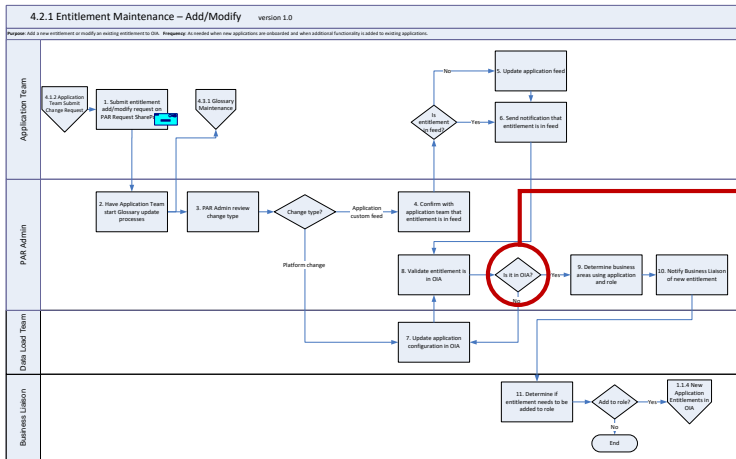
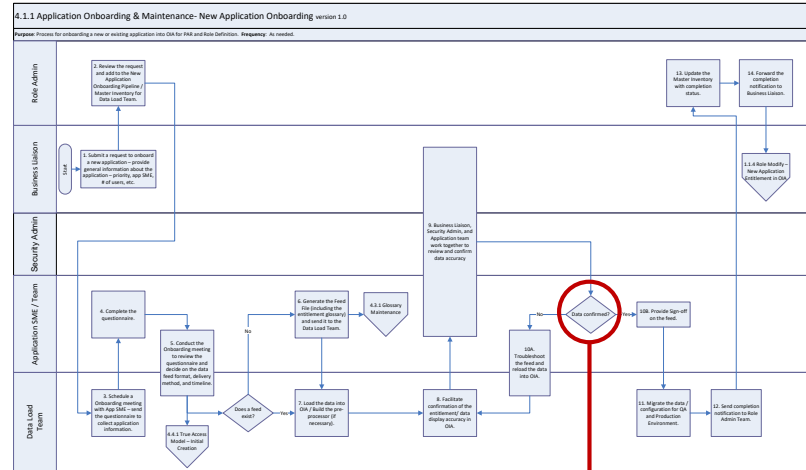
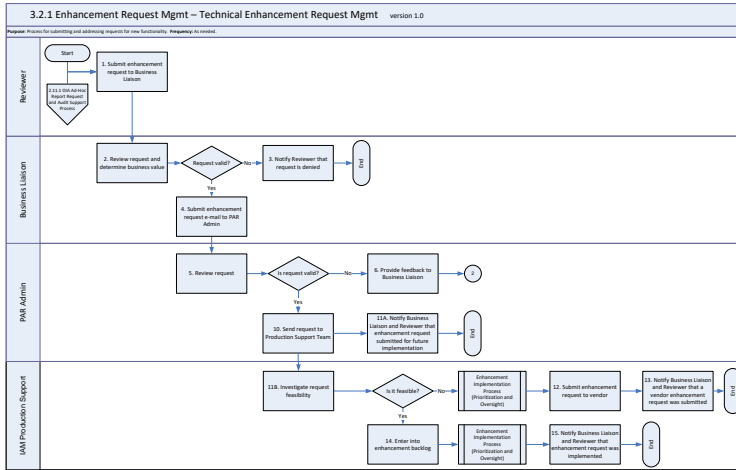
계정 권한 관리의 수준 진단

항목	표준	현재 수준 진단
User Account Management	Cobit DS5.4 ISO27002-11.2.1	<ul style="list-style-type: none"> 생성과 변경은 잘 됨. 변경 시 불필요 권한 유지 퇴사 시 적시에 삭제되지 않거나 누락 예외 관리 안 됨. 승인에 대한 책임 미인지 및 판단 근거 부재로 반려가 거의 없음. Role에 대한 라이프사이클 관리 미흡
Management Review of User Account	Cobit DS5.4 ISO27002-11.2.4	<ul style="list-style-type: none"> 대부분 부분적으로 주로 보안팀에서 검토하는 적절치 않는 프로세스 운영
SoD	ISO27002-10.1.3	<ul style="list-style-type: none"> 직무분리 예외 승인에 대한 관리 미흡
Client Control of Accounts	Cobit DS5.5 ISO27002-10.10	<ul style="list-style-type: none"> 비정상 행위에 대한 분석 및 탐지를 수작업에 의존하고 있어 한계 존재
Central Identification and Access Rights Management	Cobit DS5.3	<ul style="list-style-type: none"> 많은 수작업 존재와 증적 누락 부분적 중앙 집중적 통제 인사 관리의 이슈 전체적인 계정, 권한, Role에 대한 파악 어려움



고도화를 어떻게 할까?

그 첫 걸음, 계정 및 권한 관리 프로세스부터 정리하자!



불필요한 프로세스가 존재하는지?

근거와 증거가 존재하는지?

IT 중심에서 비즈니스 중심으로, 소통의 방식 필요

CFO, CEO, CISO



사용자 접근권한을 적절히 관리하고 있습니까? 다음 감사에서 보안 통제 상에 문제는 없습니까?

1

감사팀



박형근 씨가 본인의 업무에 대해 "적절한" 접근 권한을 가지고 있는지 증명할 수 있습니까?

2

보안팀



4

어플리케이션 관리자



박형근씨가 적절한 접근권한을 갖고 있는지 확인할 수 있습니까?

3

나는 박형근씨가 접근하고 있는 것이 무엇인지 말할 수 있습니다. 그러나 그것이 적절한지는 말할 수 없습니다.

5

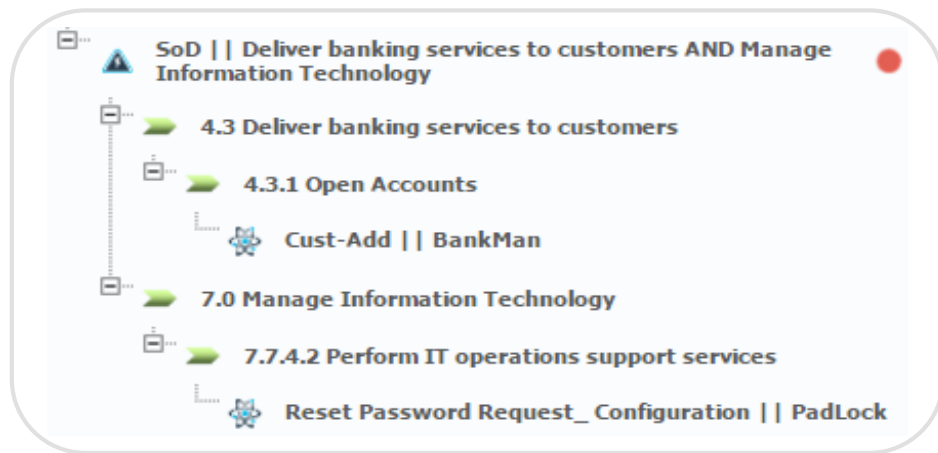
비즈니스 관리자



박형근씨가 적절한 어플리케이션 권한을 갖고 있는지 확인할 수 있습니까?

6

모든 IT의 상세한 내용을 충분히 이해할 만큼 기술적이려면 아마도 할 수 있겠지만.... 할 수 없습니다.



RA, Role, SoD



Business Analyst

Access Recertification 1/2



bluemine (Market Development & Insights web site) Revalidation Notice for HyungKeun Park/Korea/IBM
bluemine to: HyungKeun Park

2017-04-13 오전 09:06

[Show Details](#)



Validate business need for continued access to IBM confidential information on "bluemine" web site

Audience	Worldwide employees who have access to IBM confidential information on bluemine , provided by IBM Market Development & Insights (MD&I). bluemine is MD&I's digital channel for delivering insights on clients, competitors and the market to all IBMers. Some of bluemine's content contains IBM confidential information and data on IBM, our position in the market and how we compare to competitors. Therefore, we must revalidate that users have a business need for access to confidential information.
Purpose:	IBM IT Security standards require annual revalidation of continued business need for people with access to applications that are within the scope of the standards.
Action required:	Please consider your current confidential access for bluemine and determine if there is still a continued business need for accessing IBM confidential information on the site. If you still need confidential access, no further action is required. If you no longer require confidential access, please submit a request to bluemine@us.ibm.com by clicking on this link .

Access Recertification 2/2

Actions	Application	Entitlement /	Description	W
<input type="checkbox"/> Approved <input type="button" value="Revoke"/>	Hyperion-GRS	Hyperion-GRS_MM-SC_AREA_GEO_R		
<input type="checkbox"/> Approve <input type="button" value="Revoked"/>	Network Services	ALIT MARE_MARE_DUMMY		
<input type="checkbox"/> Approved <input type="button" value="Revoke"/>	Network Services	ALIT MARE_RDM_COMP		
<input type="checkbox"/> Approve <input type="button" value="Revoke"/>	Network Services	ALIT MARE_PARAM_VISUAL		
<input type="checkbox"/> Approve <input type="button" value="Revoke"/>	Network Services	Net_ADM_TO_USR_pers_tools		
<input type="checkbox"/> Approve <input type="button" value="Revoke"/>	Hyperion-GRS	Hyperion-GRS_MM-PRAGMA_SERV_R		

Entties: 22 25

Campaign Management IDEAS / A810223 [Help](#) [Logout](#)

Summary | **Details**

Campaign: Company Wide Access Recertification Campaign type: Supervision User Assignment

Start date: 05/12/2014 End Date: 05/02/2015

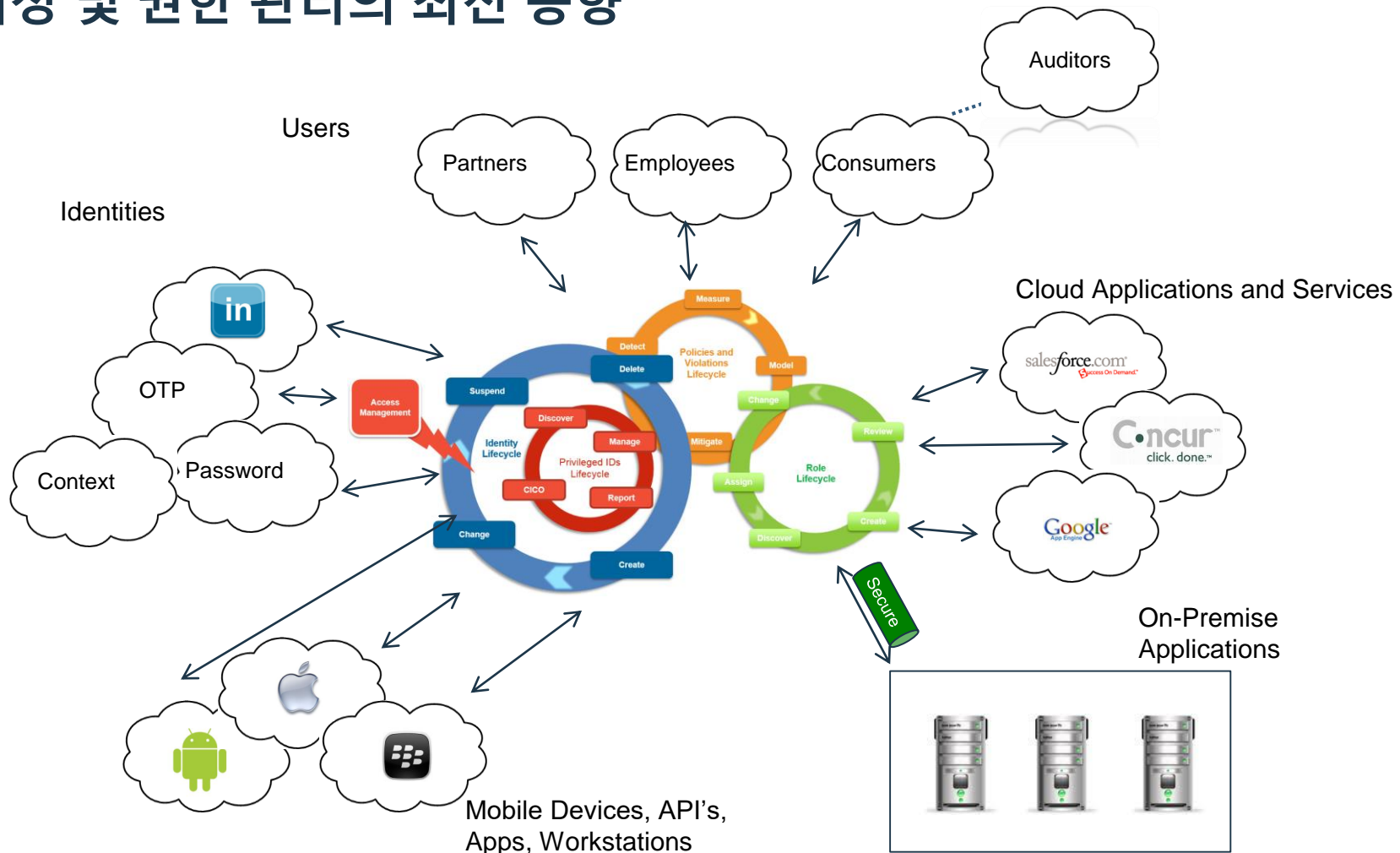
Sign Off: By User

% Completion: 2 / 24 Users

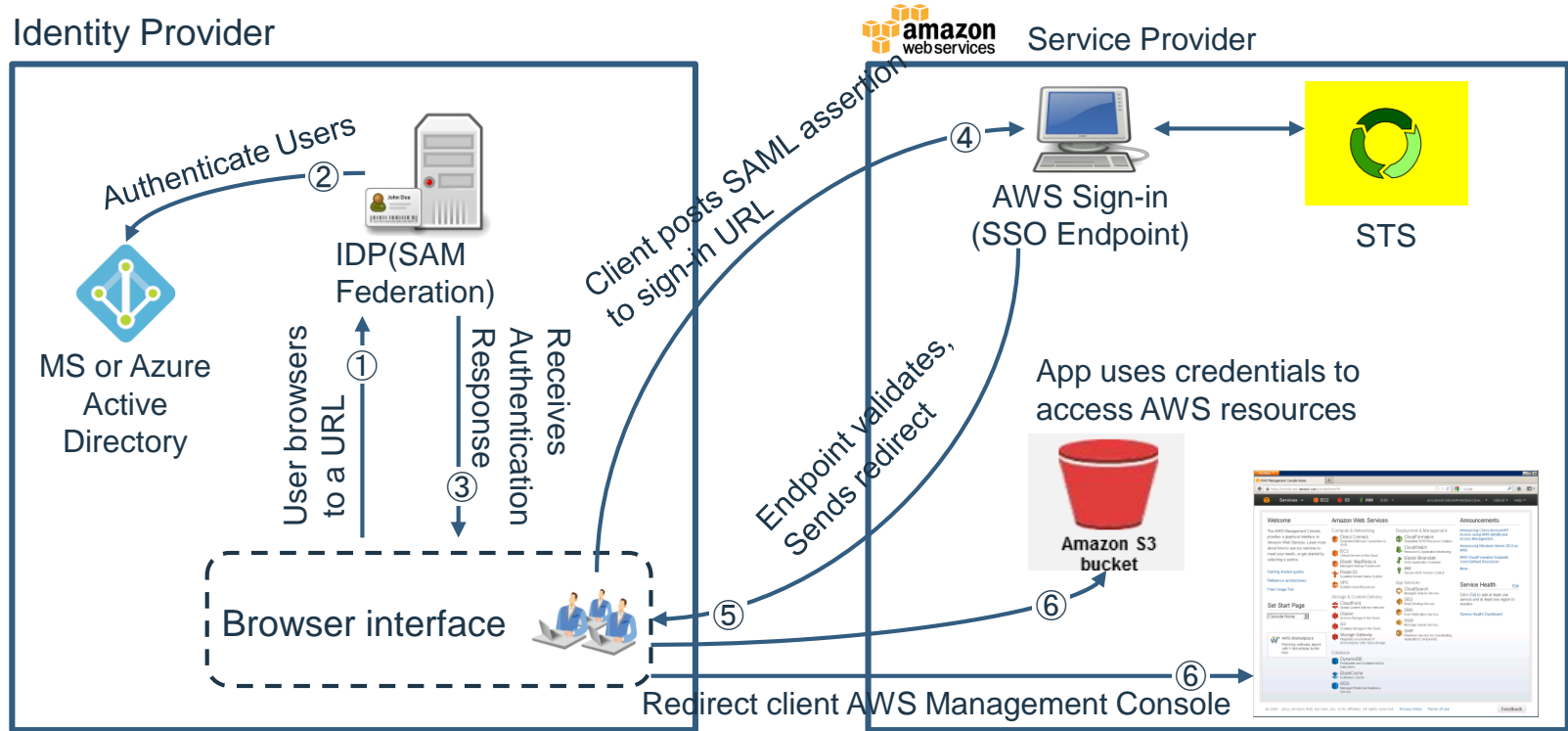
Actions	Master UID	Name	Last Name	Ou Name [Code]	% User Completion
	AAYN003	Jean	Hidis	CORPORATE / Administration, Finance and Control [CORPORATE / Administration, Finance and Control]	<input type="text" value="7.9 %"/> 39 / 492
	A232583	Shirley	Chang	CORPORATE / LEGAL [CORPORATE / LEGAL]	<input type="text" value="100 %"/> 20 / 20
	A809787	Mary	Nunez	CORPORATE / PROCUREMENT [CORPORATE / PROCUREMENT]	<input type="text" value="0 %"/> 0 / 14
	A259952	Elizabeth	Kimble	PRODUCT DIVISION / CENTER [PRODUCT DIVISION / CENTER]	<input type="text" value="100 %"/> 15 / 15
	ATSY088	Mark	Powers	SALES / MARKETING [SALES / MARKETING]	<input type="text" value="0 %"/> 0 / 15
	A254896	Chad	Little	CORPORATE / HUMAN RESOURCES [CORPORATE / HUMAN RESOURCES]	<input type="text" value="0 %"/> 0 / 23
	A254884	Jessica	Hills	PRODUCT DIVISION / CENTER [PRODUCT DIVISION / CENTER]	<input type="text" value="0 %"/> 0 / 24

Entties: 24 25

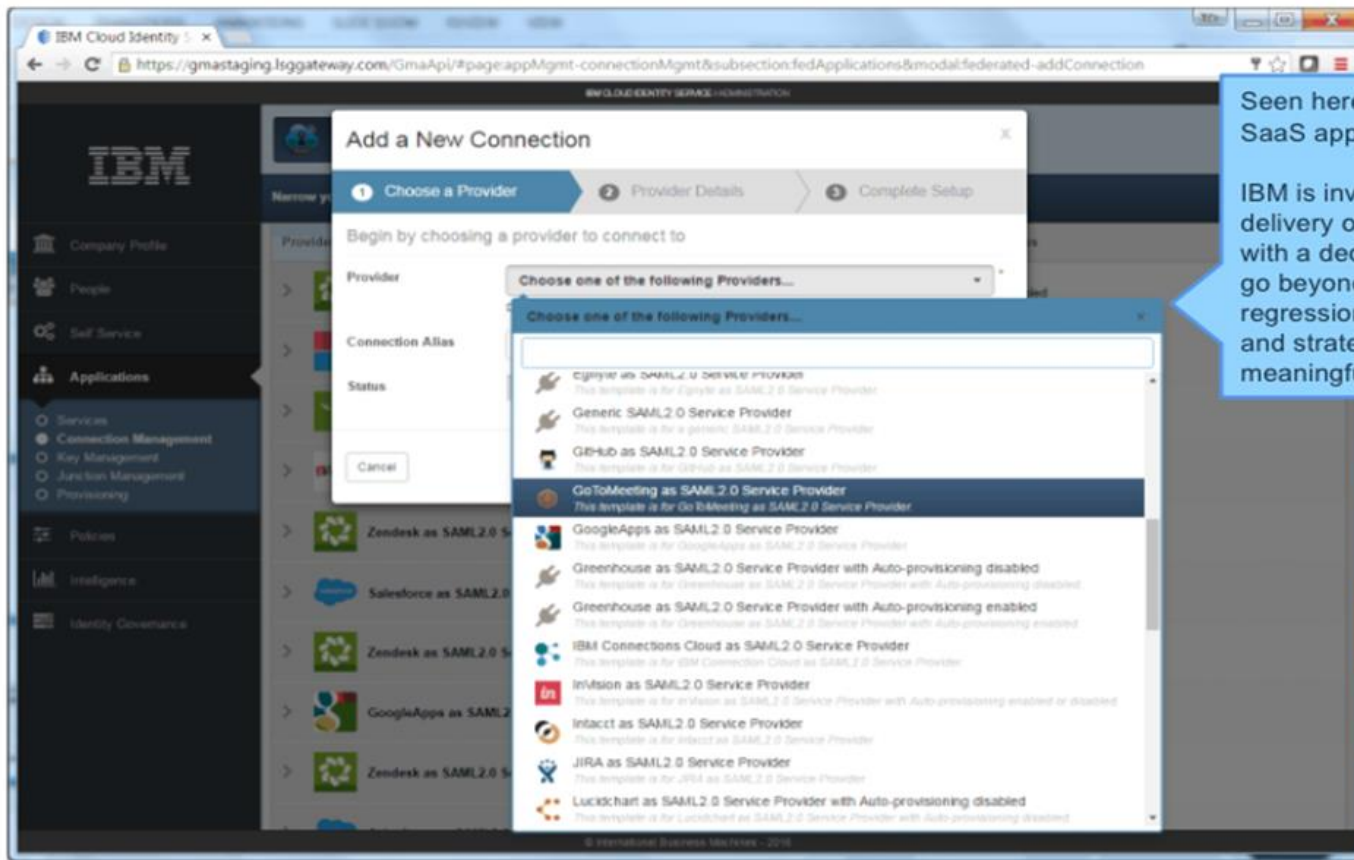
계정 및 권한 관리의 최신 동향



첫번째 단계, IDP(Identity Provider) 구축부터



IDaS(Identity as a Service)

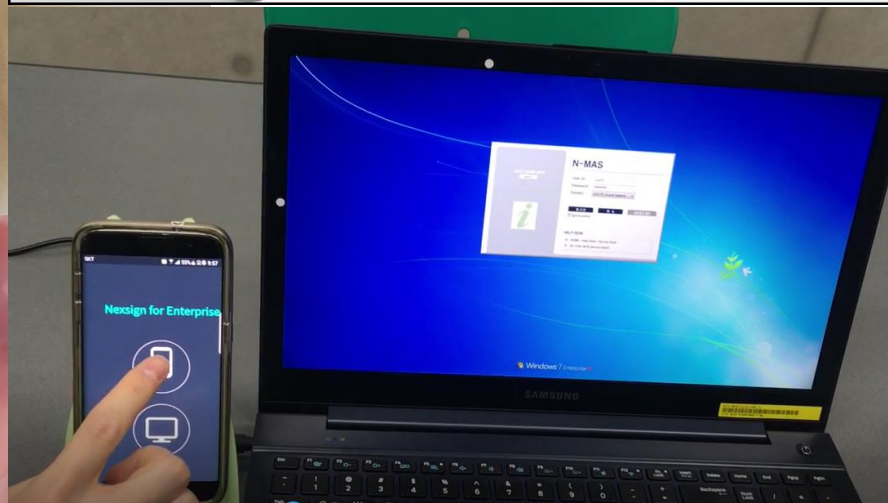
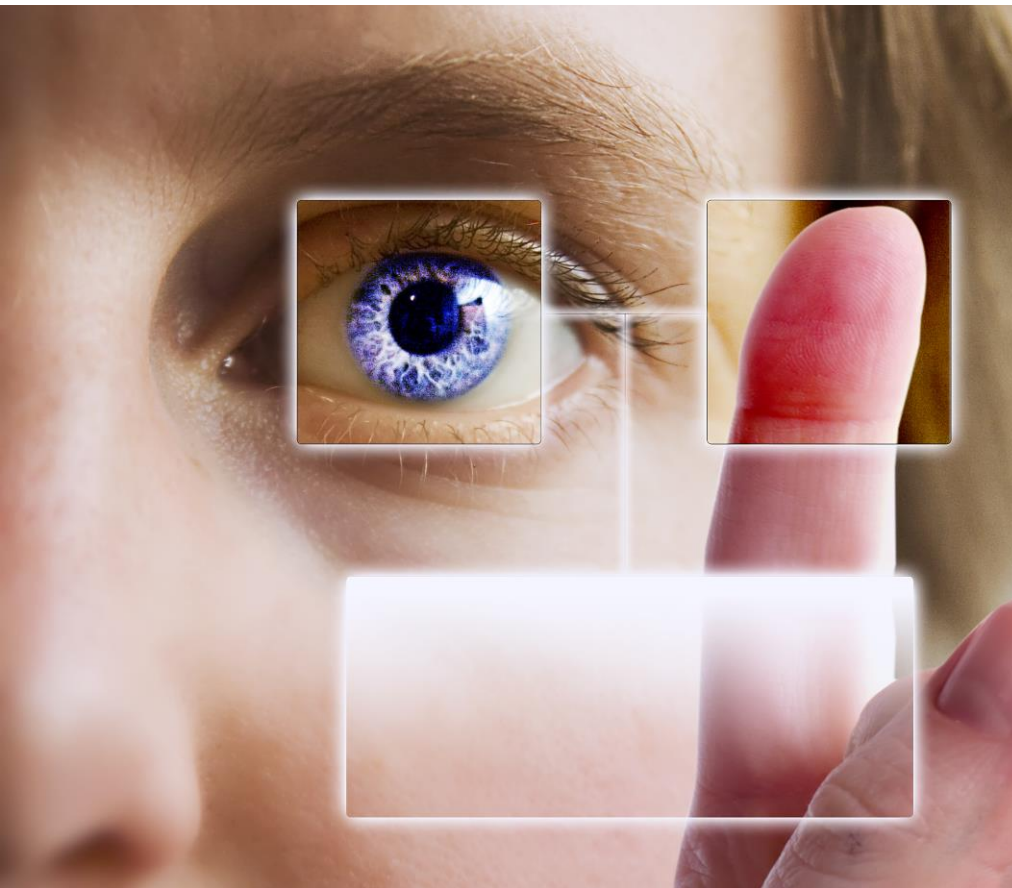


Seen here, an administrator configures a new SaaS app for SSO using pre-profiled providers.

IBM is investing in continuous development and delivery of profiles for SaaS partner applications with a dedicated integration factory. Partnerships go beyond simple integration but include 24-hour regression testing, formal partnership programs, and strategic relationships that will help build meaningful value beyond SSO.



생체 인식 기반의 인증 강화



사용자 이상행위 분석(1/2)

UBA 시나리오

클라우드 서버 연결

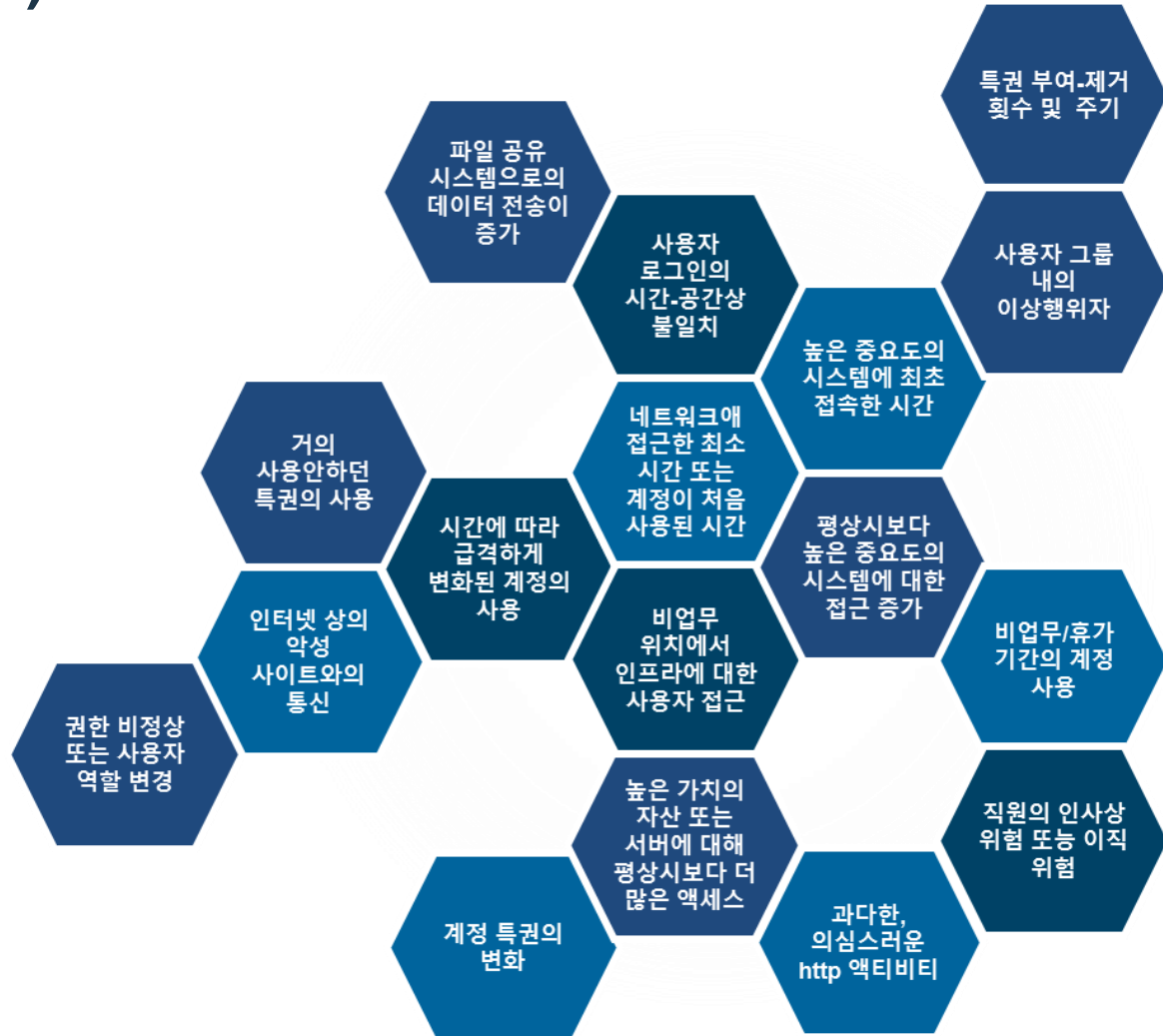
- 사용자가 클라우드 서버 혹은 Box 개인 계정에 접속하여 민감한 데이터를 업로드 함

높은 중요도의 자산에 액세스

- 사용자가 높은 중요도의 자산에 접근하여 다운로드하는 행위의 빈도가 점차적으로 증가함

시간에 따른 사용행위의 변화

- 사용자 행위가 비교적 짧은 시간에 평상시와 차이가 많거나 시간이 지남에 따라 점차적으로 달라짐



사용자 이상행위 분석(2/2)

UBA 시나리오

자산에 대한 접근 횟수 변경

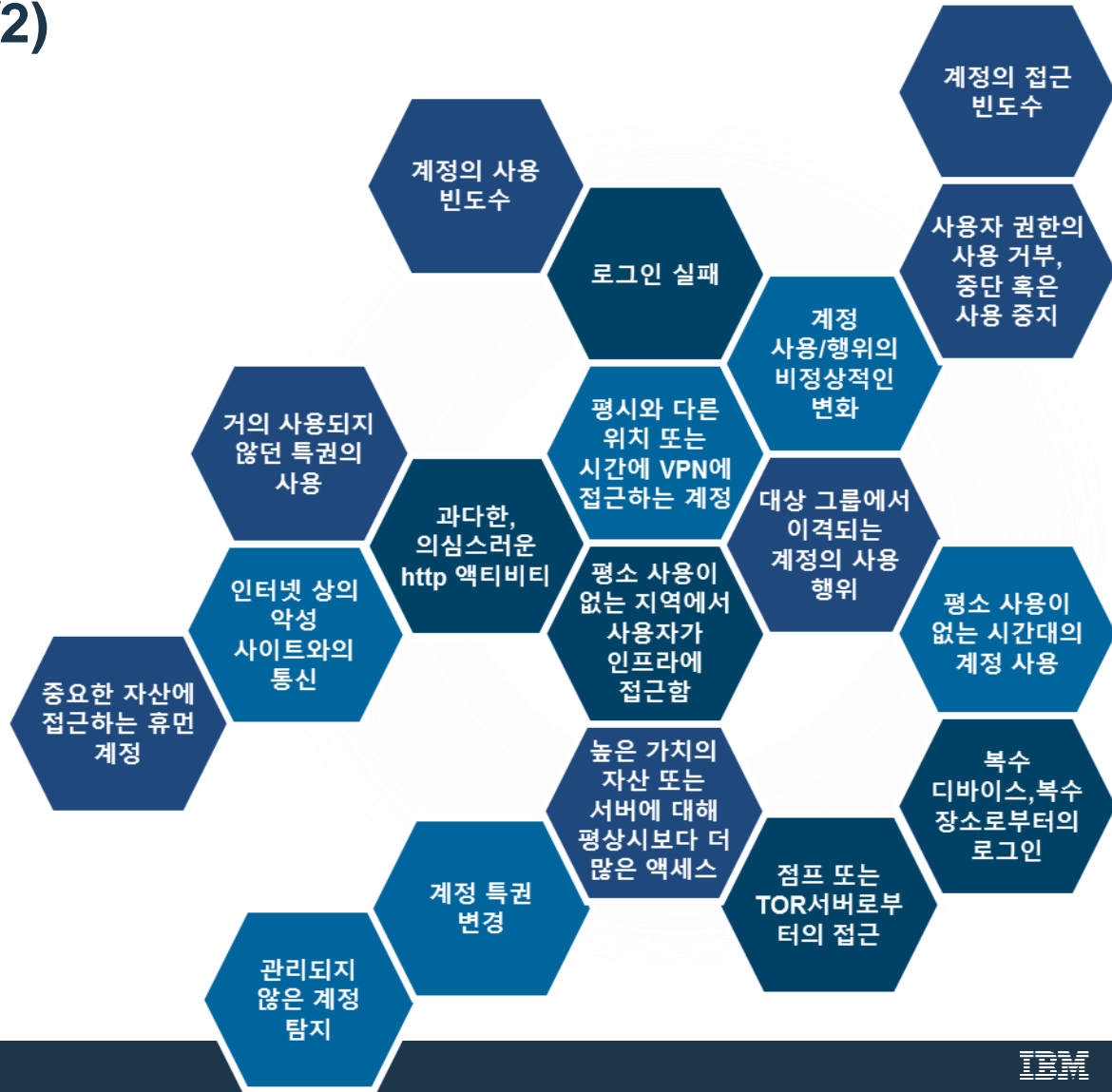
- 사용자 행위의 양이 갑자기 증가하거나, 접근하는 자산의 수가 급격히 늘어남

대상 그룹에서 이격되는 움직임

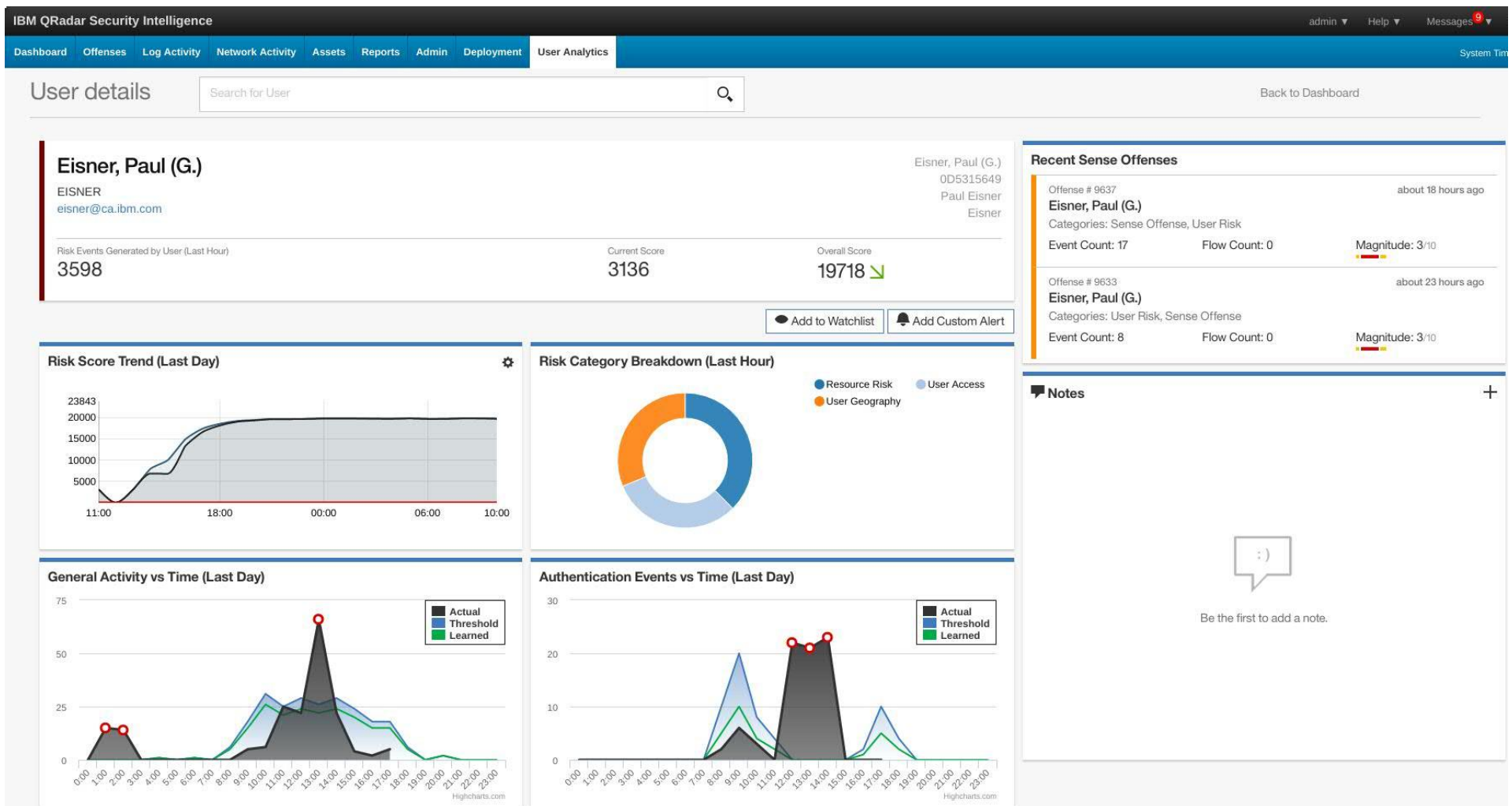
- 사용자 패턴이나 행위가 대상 그룹에서 이격되기 시작함

계정 권한의 변경

- 사용자가 존재하는 계정에 대해 권한을 변경 시도하거나 다른 시스템에 새로운 계정을 생성






User Behavior Analysis with Machine Learning





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.