

제로 트러스트와 클라우드를 위한
인공지능, 위험 기반
차세대 계정 및
권한/접근 관리 전략



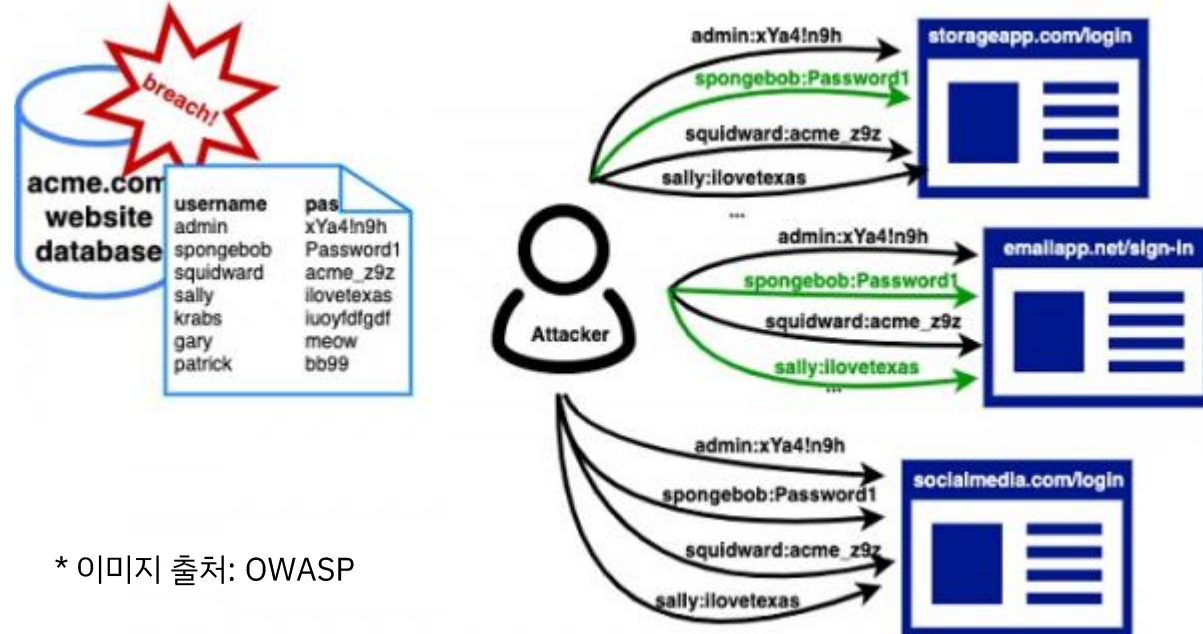
보안사업부 디지털 트러스트 부문
박형근 실장 (phk@kr.ibm.com)

다양한 아이덴티티 위협과 공격

- 최근 외부에서 도용된 아이디와 비밀번호를 통해 일부 고객이 구입한 전자 문화상품권 등을 사용하는 사례가 발생했다.
- 랩서스가 공개한 스크린샷 및 채팅 기록에는 유효한 가상 사설망(VPN), 원격 데스크톱 프로토콜(RDP), 아마존 웹 서비스(AWS) 및 MS 애저(Azure) 등 크리덴셜을 통해 접속하는 비중이 매우 높다. 외부에 공개된 취약한 서버와 유출된 크리덴셜을 주로 활용하는 것으로 예상된다.

91% E커머스 로그인 중 정상 로그인 대비 Credential Stuffing 공격 비율

(* 출처: SOCRadar E-Commerce Threat Landscape Report Nov.2022)



* 이미지 출처: OWASP



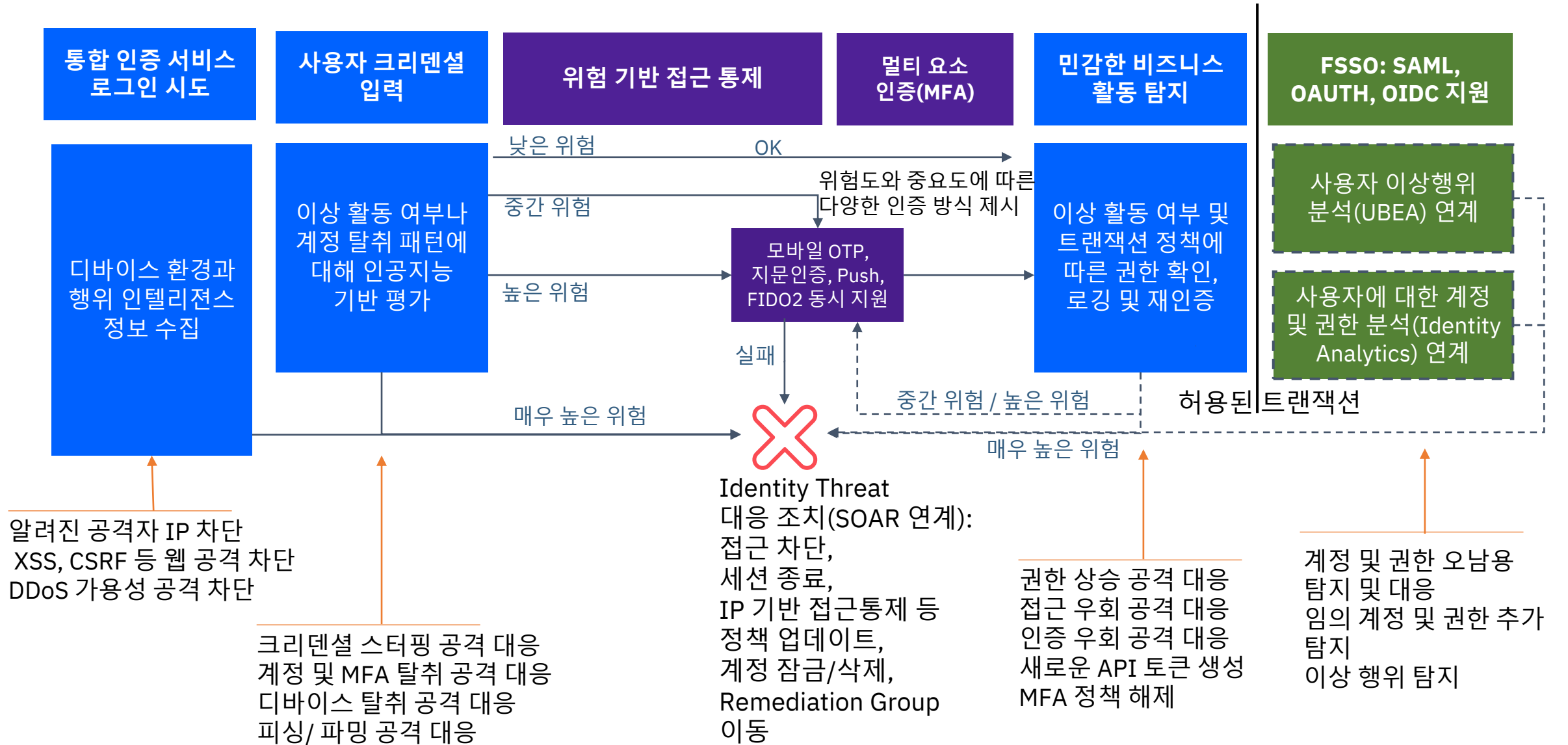
2 * 이미지 출처: Duo Security

Trend 3: Identity Threat Detection and Response

숙련된 기술을 가진 악의적인 공격자는 ID 및 접근 관리(IAM) 인프라에 대해 적극적으로 공격 대상으로 삼고 있으며, 이제 자격 증명 오용이 주요 공격 방법으로 대두되었습니다. 가트너는 ID 시스템을 방어하기 위한 방법을 설명하기 위해 **"Identity Threat Detection and Response(ITDR)"**이란 용어를 도입했습니다. 기업은 IAM 기능을 개선하는 데 상당한 노력을 기울였지만 그중 상당 부분은 사이버 보안 인프라 강화 측면이 아니라, 사용자 인증을 개선하는 기술에 집중되어 실제로는 공격 표면을 증가시켰습니다. ITDR은 인증 시스템을 보호하고, 공격받았을 때 이를 탐지하고 효과적으로 대응할 수 있습니다.

* 출처: Gartner Identifies Top Security and Risk Management Trends for 2022 (March 7, 2022)

ITDR(Identity Threat Detection and Response) 논리적 구성



인공지능 기반으로 사용자의 신뢰성 확보 및 앞선 보안 위협에 대한 대응 조치

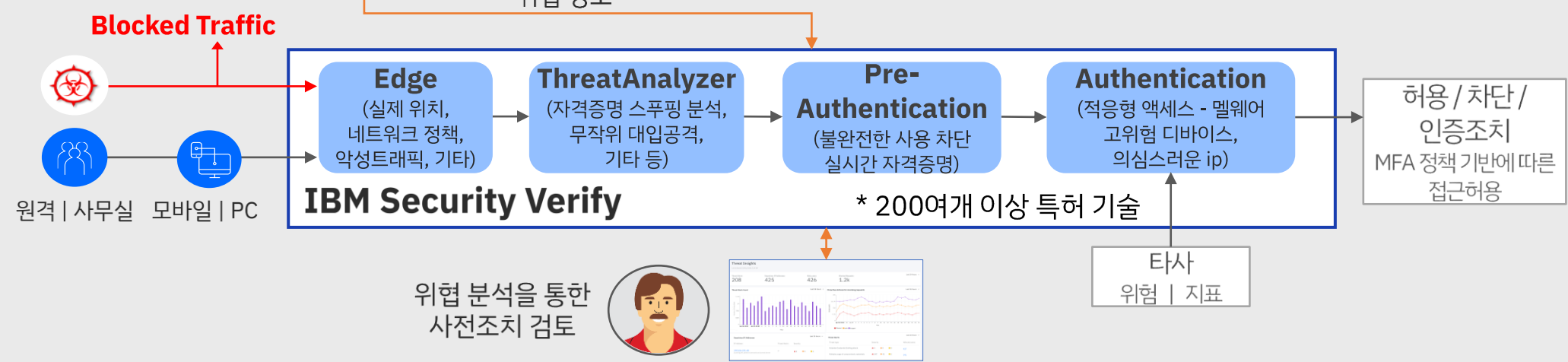
“
인공지능 기반
신뢰성 및
위험 분석



글로벌 위협정보
IBM X-Force Exchange

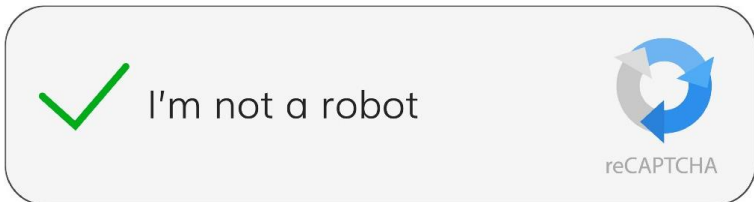
38B 분석된 웹 페이지와 이미지
8M 일일 스팸과 피싱 공격 모니터링
850K 악성 IP 주소
Millions 고유 악성 코드 샘플

위협 정보



- 복합적 디바이스 식별
- 인공지능 기반 신뢰성과 위험 분석
- 세션 및 트랜잭션 이상행위 식별
- 종합 위험 지표 및 스코어링 자동 관리
- 위협 인텔리전스 기반 분석 지원

1차 방어: Threat Intelligence의 활용과 Bot 방어



IBM Security Verify

Create an account

Already have an account? [Log in](#)

Email address

ppan@mailinator.com

Create account password

.....

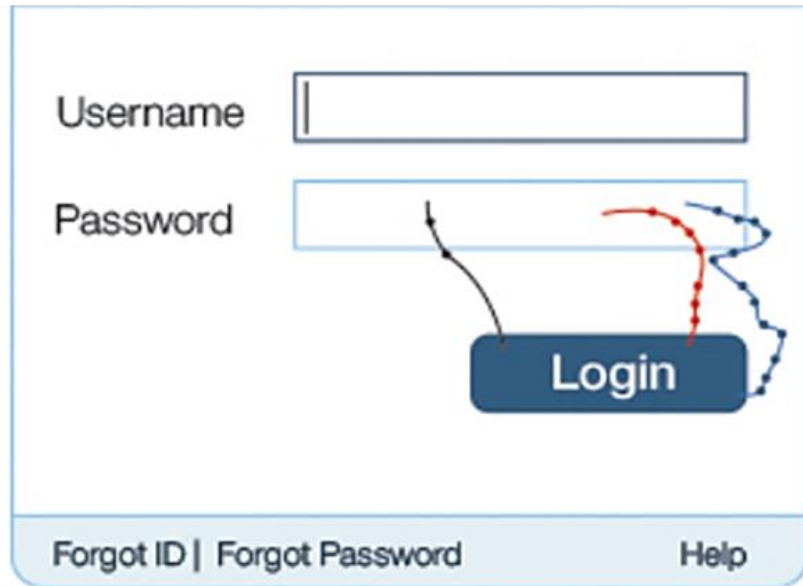
ⓘ Warn global.

```
"most_significant_data_grant_type": [],
"top5_affected_tenantid": "{\"1f5171cb-e98e-4b46-a14f-b6bc7d774e17\": 75}",
"top5_affected_tenantname": "{\"cia-us-prod.ice.ibmcloud.com\": 75}",
"most_significant_servicename": [
  "factors"
],
"anomalous_event_count": 50,
"most_significant_tenantname": [
  "cia-us-prod.ice.ibmcloud.com"
],
"summary": "Abnormal number of device enrollments: 50 anomalous events are observed,
10:00:00 UTC.",
"severity": "critical",
"top5_affected_data_origin": "{\"49.36.49.39\": 75}",
"rule_name": "Abnormal number of device enrollments",
"impacted_user count": 1,
"end_time": "2023-01-31 10:00:00",
"anomalous_suspicious_ips": [
  "49.36.49.39"
],
"index": "event-management-*",
"most_significant_tenantid": [
  "1f5171cb-e98e-4b46-a14f-b6bc7d774e17"
],
"rule_id": "ABNORMAL_DEVICE_ENROLLMENT",
"top5_affected_geoip_country_name": "{\"India\": 75}",
```

Last updated on Feb 15,
2023 8:17 PM SGT

! Warning Your password was updated. Consider changing your password because it was found on a list of commonly used and/or breached passwords.

2차 방어: 인공지능에 의한 신뢰도 분석 - 사용자 행위 기반 인증



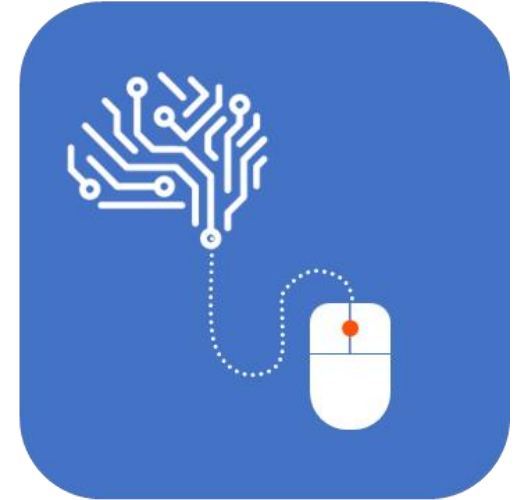
Normal User Behaviour



Abnormal User Behaviour



Known Fraudster Behaviour



Authentication factors

Enable the authentication factors that users can use to sign in to the target applications.

Behavioral biometrics

High confidence required

Off

2차 방어: 인공지능에 의한 신뢰도 분석



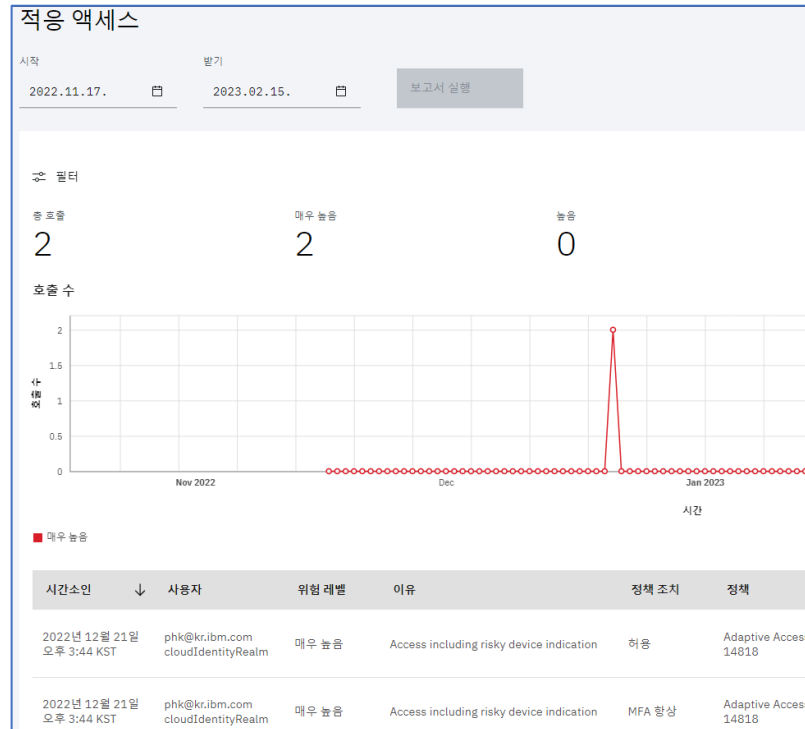
Authentication factors

Enable the authentication factors that users can use to sign in to the target applications.

Behavioral biometrics

High confidence required

Off

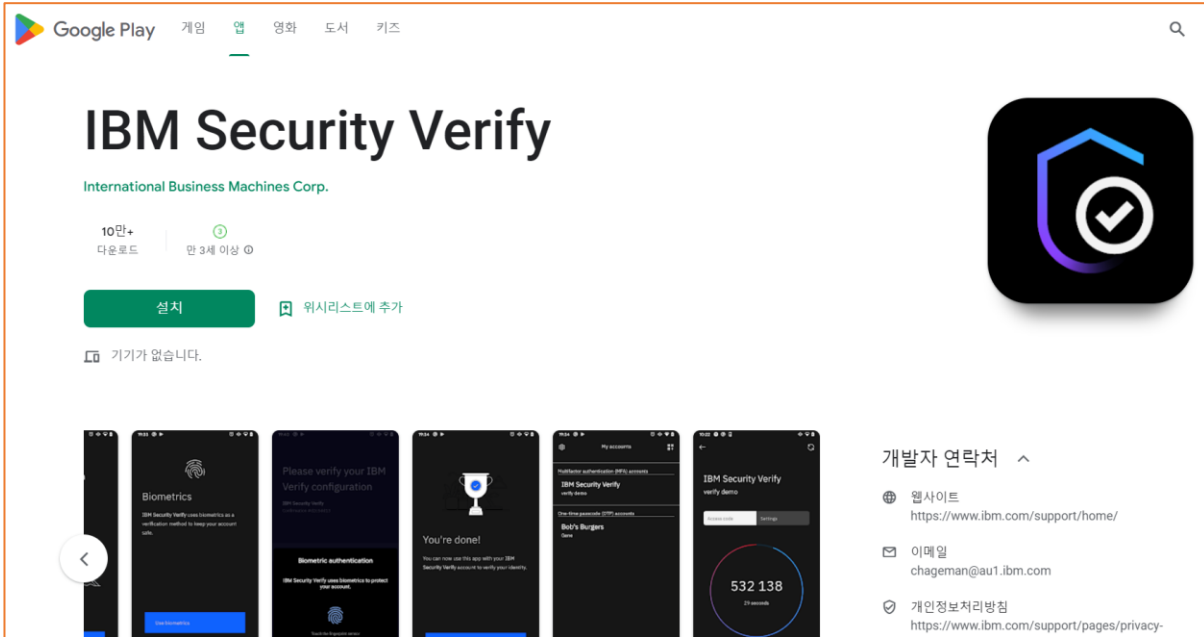


적용 액세스

사용으로 설정되면 각 인증 시도에 고유 위험 레벨이 지정됩니다.

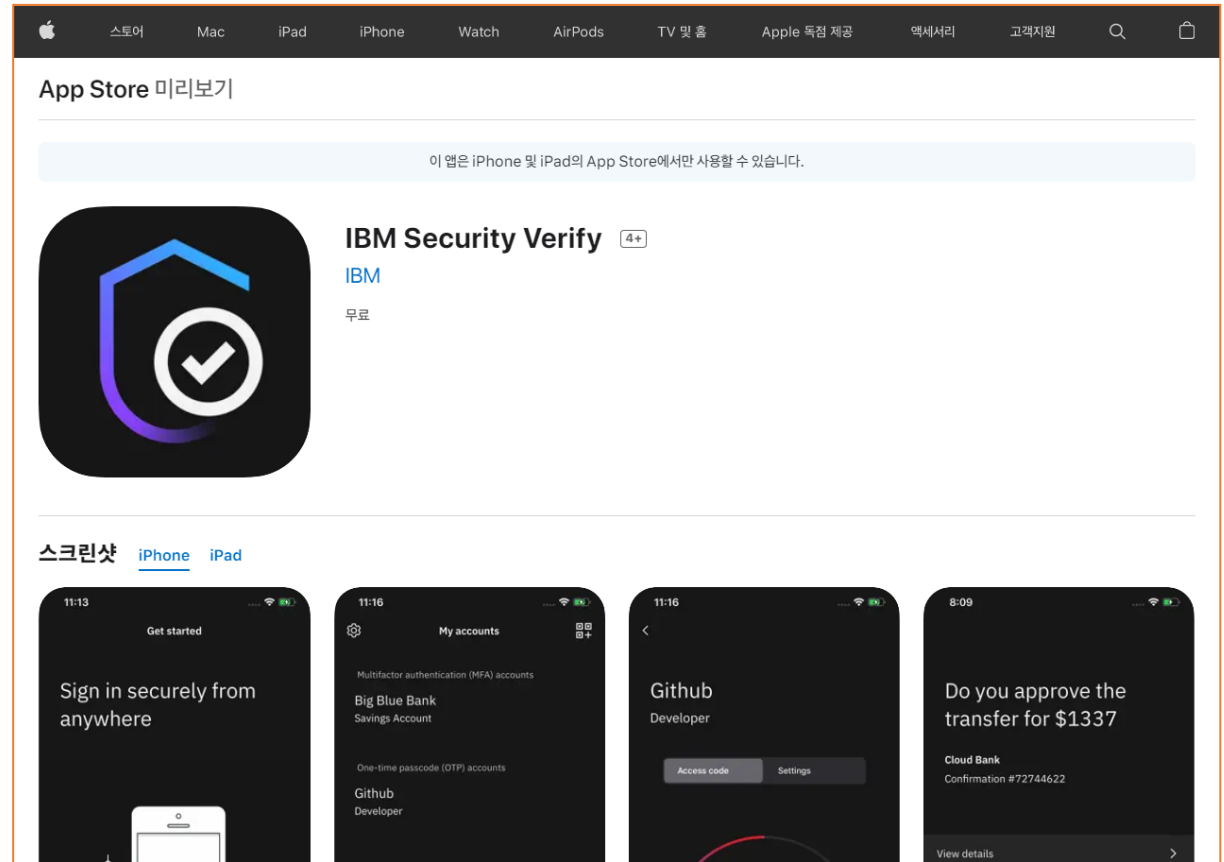
| | |
|--------|-----------------------------------|
| 적용 액세스 | 사용 |
| 매우 높음 | MFA 항상 사용 가능한 메소드(기본값) |
| 높음 | MFA 항상 사용 가능한 메소드(기본값) |
| 중간 | 세션당 MFA 사용 가능한 메소드(기본값) |
| 낮음 | 허용 |
| 알림 | 사용자 조치가 수행되기 어렵거나 차단되면 알림을 보내십시오. |

막간 광고: IBM Security Verify App 무료 배포!!!



스크린 캡처가 방지되는 보안 기능이 들어간,
가독성 좋은 무료 OTP를 지금 바로 사용해 보세요!

구글 OTP와 100% 호환되는,
IBM이 직접 개발 관리하는 무료 앱입니다.

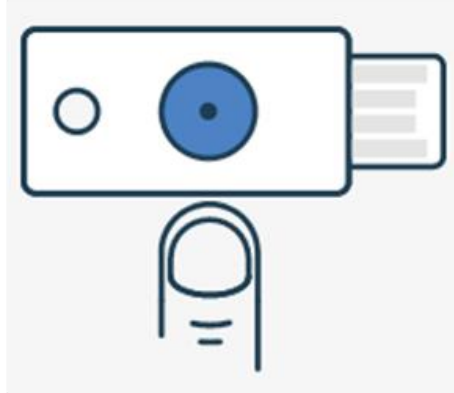


기본 지원: 다중 요소 인증(MFA)

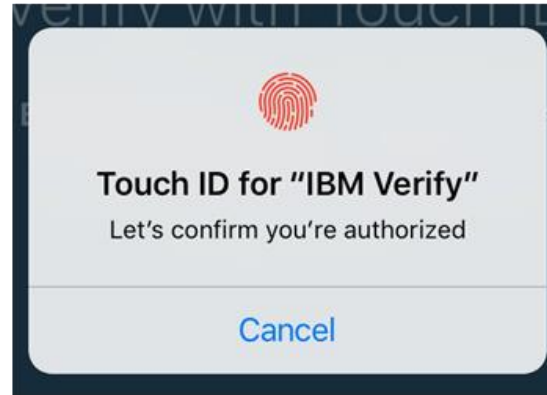
QR 코드 인증



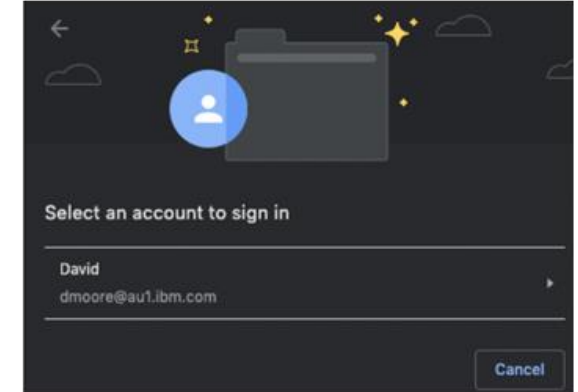
FIDO2 U2F 인증



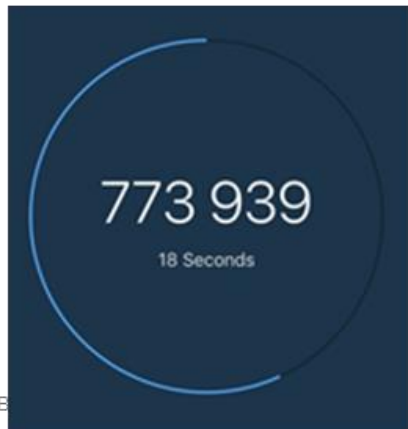
지문 인증



WebAuthn 인증



모바일 OTP 인증



SMS/EMAIL OTP 인증

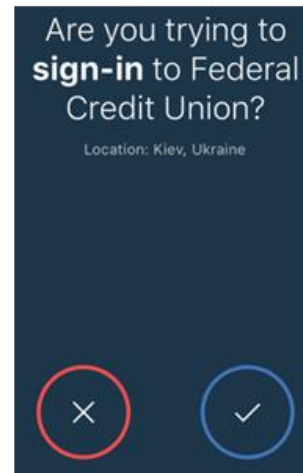
Enter your passcode

A passcode was sent as an SMS message to the phone number associated with your IBM w3 profile.

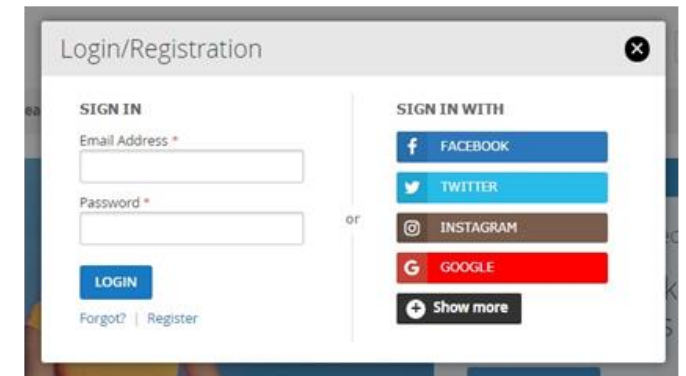
1895

Submit

User Presence



소셜 로그인



내 스마트폰으로 MFA 설정해 봤는데, 휴가는?

VPV_Control_Zone > AWS IBMTEST Root Account ☆



일반 보안 감사 원격 비밀번호 변경 종속 항목 공유 설정 메타데이터

지금 비밀번호 변경

기타

기본 정보

모두 편집

비밀 정보의 템플릿 유형, 도메인, 사용자 이름 및 비밀번호와 같은 일반 정보 및 기타 기본 정보를 포함합니다. 권한에 따라 이러한 필드를 보거나 편집하지 못할 수 있습니다.

| | | |
|------------|--------------------------|----|
| 비밀 정보 이름 * | AWS IBMTEST Root Account | 편집 |
| 비밀 정보 템플릿 | Amazon IAM 콘솔 비밀번호 | 편집 |
| 사용자 이름 * | securityplus@kakao.com | 편집 |
| 비밀번호 | ***** 표시 | 편집 |

One Time Password

 Generate One Time Password

다음 항목에 대한 일회성 비밀번호 AWS IBMTEST Root Account

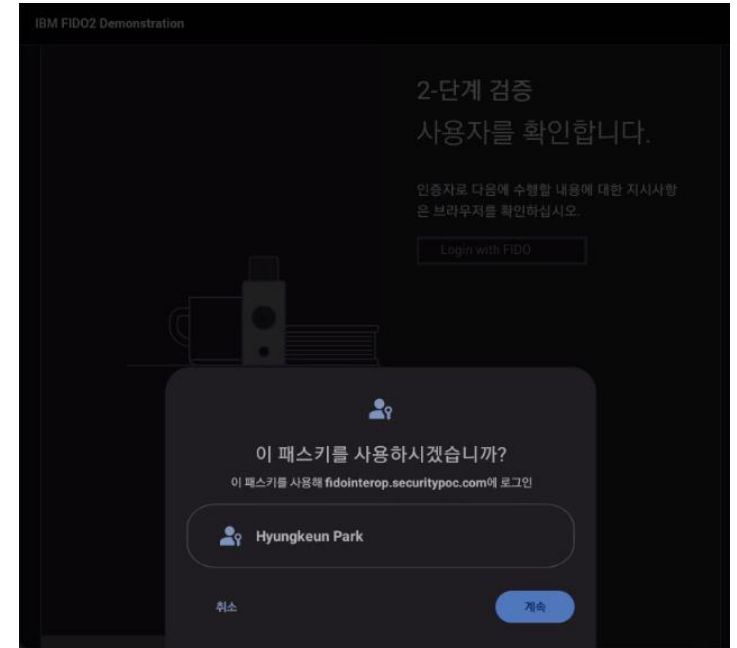
331 647 

클립보드에 복사할 일회성 비밀번호를 클릭

패스워드 대신 패스키로!!!!



- ✓ 계정 인증에 대한 업계 표준을 기반으로 하는 패스키는 암호보다 사용하기 쉽고 훨씬 더 안전합니다.
- ✓ 암호 없이 모든 플랫폼에서 앱과 웹 사이트에 간편하고 안전하게 로그인할 수 있는 패스키를 제공하는 SAMSUNG Pass와 디바이스 보안을 강화해 주는 SAMSUNG KNOX, 그리고, 위험 관리를 기반으로 한 IBM Security Verify의 접근 통제와 싱글사인온 기술이 결합하여 새로운 사용자 경험을 제공합니다.



SAMSUNG/애플/구글 Passkey

- 암호없이 간소화된 로그인
- 차세대 계정 보안으로 강력한 자격증명 제공
- 서버 유출이나 피싱으로부터 안전
- KNOX 등 디바이스 보안과 협업

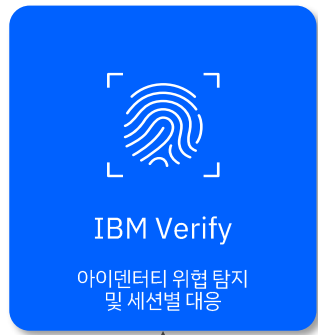


IBM Security Verify

- 인공지능 및 위험 기반 접근 통제
- IBM 보안 정보 활용한 선제적 위협 대응
- 표준(SAML, OIDC) 기반 싱글사인온



아이덴티티 위협 탐지에 대한 보다 고도화된 대응: SOAR와의 연계



이벤트
알람

IBM Security QRadar SOAR

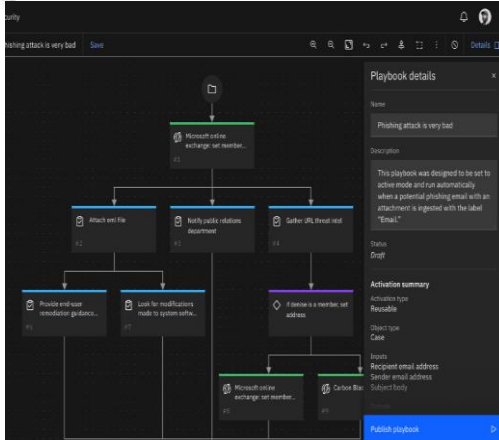
STEP 1.
Case Creation

automatically created when a target is found.

| Type | Value | Added By |
|------------|-----------------------------------|----------|
| Service | Tomcat | Randori |
| File Path | / | Randori |
| DNS Name | ferrari.demo.webernets. online | Randori |
| Port | 443 | Randori |
| IP Address | 35.201.103.45 | Randori |

STEP 2.
Playbooks

Execution begins and tasks are assigned for mitigation.



STEP 3.
Mitigation

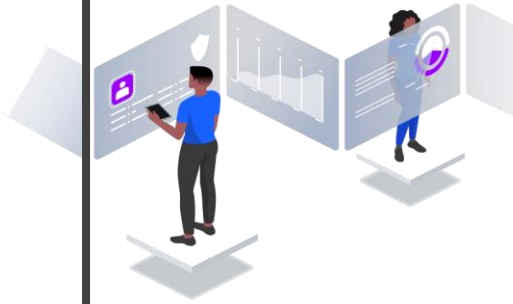
Automated target mitigations on policy, group, User inactive etc.

App: Verify for SOAR

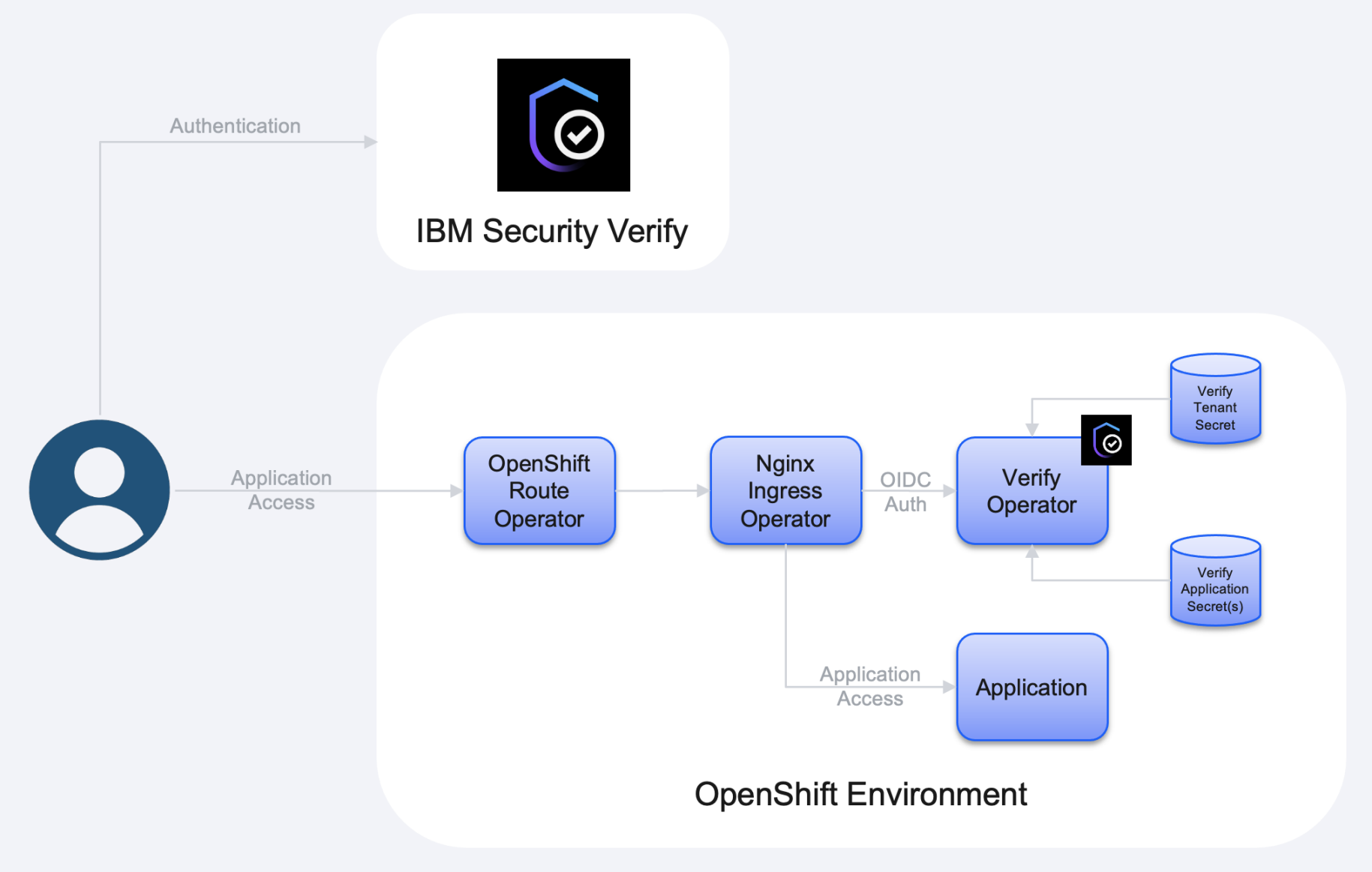
- Add User Entitlement
- Add User To Group
- Remove User Entitlement
- Remove User from Group
- Reset User Password
- Set User Inactive

App: Verify Priv for SOAR

- Create a secret policy
- Create a secret template
- Deactivate a secret
- Expire a session
- Get report audits
- Get reports
- Get secrets
- Search reports
- Search secrets
- Search security audit logs
- Update a secret policy
- Update a secret



DevSecOps: 어플리케이션 싱글사인은 및 접근 통제



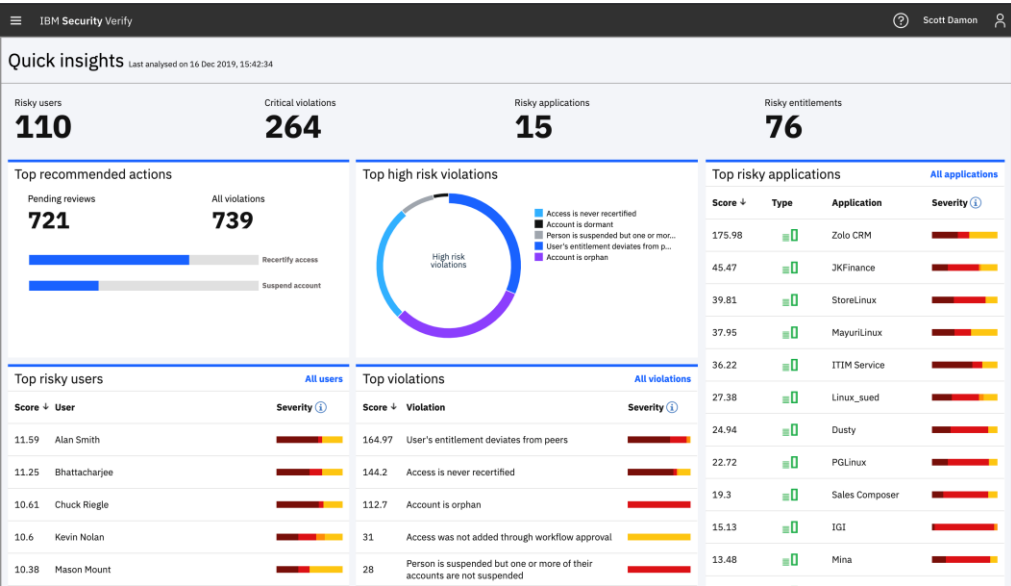
전사 통합 계정 관리: 레거시부터 클라우드까지

The screenshot displays the IBM Security Verify interface. On the left is a navigation sidebar with categories like Home, Applications, App role management, Directory, Authentication, Security, Data privacy & consent, User experience, Integrations, Analytics, Reports, and Global configuration. The main content area shows a list of permissions imported from target applications after account synchronization. A filter is applied for 'AWS IAM(Custom)'. The table below lists the permissions with their names, descriptions, applications, and categories.

| Permission name | Description | Application | Category |
|---------------------------------------|---|-----------------|-------------|
| Basic access | Provides access to the application with basic authorization | AWS IAM(Custom) | Default |
| aws-ec2-spot-fleet-tagging-role | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForConfig | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForElastiCache | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForElasticLoadBalancing | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForOrganizations | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForRDS | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForSSO | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForSupport | — | AWS IAM(Custom) | AWSIAMRoles |
| AWSServiceRoleForTrustedAdvisor | — | AWS IAM(Custom) | AWSIAMRoles |
| BaroniaVerifyRole | — | AWS IAM(Custom) | AWSIAMRoles |
| IAM_LAB_R1 | — | AWS IAM(Custom) | AWSIAMRoles |
| ISAM_IAM_LAB_R1 | — | AWS IAM(Custom) | AWSIAMRoles |

사용자에 대한 계정 및 권한 분석(Identity Analytics) 연계

단순한 계정 관리 솔루션이 아닌 제로 트러스트 대응을 위한 기반 핵심 인프라로 아이덴티티 분석이라는 ITDR 개념의 구현이 반드시 필요합니다.



승인 단계에서
조언

Overall Risk Details

Risk Info

| Risk Level | Risk Score | Reason | View Details |
|------------|------------|---|--------------|
| High | 305 | James Martin has recently gained an unusual number of entitlements. | View Details |
| High | 274 | James Martin's entitlements deviate from similar peers. | View Details |
| Medium | 104 | JamesM account had an alert for misuse of access in last 30 days. | View Details |
| Low | 19 | JamesM account has no activity since 7 days. | View Details |

Items per page: 50 | Results: 22 of 1

Recommendation: Revoke (80% confidence)

Similar certification requests:

- User: Maria Doss Entitlement: L1 Support Risk Match: 100% Action: Revoke
- User: Olive Diggs Entitlement: L1 Support Risk Match: 100% Action: Revoke
- User: Ronald Altentio Entitlement: AD_User Domain Resources Risk Match: 80% Action: Approve

Buttons: Accept, Revoke, Close

인공지능에 의해 각 사용자마다 현재 보유하고 있는 계정 및 권한 현황을 분석하여 아이덴티티 위험 정도를 분석 평가.

| Score ↓ | Policy | User | Application | Entitlement | Severity | Recommended Action | Source | |
|---------|-----------------------------------|------------------|--------------|---------------------------|----------|--------------------|--------|-------------------------------------|
| 1 | Access has never been recertified | Daniel Hoerr | G53 | MM:T_064_M | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Access has never been recertified | Francine Duvall | G53 | FI:T_065_V | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Access has never been recertified | Colleen Atherton | zSecure RACF | FACILITY/FILEM.TAPE/ALTER | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Account is currently dormant | Jack Reeves | IGI | N/A | High | Suspend account | IGI | <input type="checkbox"/> |
| 1 | Account is currently dormant | Erik Lutz | IGI | N/A | High | Suspend account | IGI | <input type="checkbox"/> |
| 1 | Account is currently dormant | Joan Johnson | IGI | N/A | High | Suspend account | IGI | <input checked="" type="checkbox"/> |
| 1 | Access has never been recertified | Cynthia Rothe | G53 | BC:T_046_M | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Access has never been recertified | Wanda Howell | G53 | BC:T_001_M | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Access has never been recertified | Colleen Atherton | zSecure RACF | FACILITY/VRAS.REFF/ALTER | High | Recertify access | IGI | <input type="checkbox"/> |
| 1 | Access has never been recertified | Randall Gonzalez | zSecure RACF | APPL/CNM19/READ | High | Recertify access | IGI | <input checked="" type="checkbox"/> |
| 1 | Account is currently dormant | Amy Bigelow | zSecure RACF | N/A | High | Suspend account | IGI | <input checked="" type="checkbox"/> |

3 of 30 Selected. Mark actioned

인공지능에 의해 분석된 정보를 기반으로 계정 및 권한에 대한 대응 조치 추천.

Next Steps

웹사이트 방문

대표적 유즈 케이스를 통한 인-앱 가이드와 함께
계정, 권한, 접근 관리와 CIAM 접근법 확인

<https://ibm.biz/KRverify>



전문가 상담 및 데모 브리핑 세션 신청

ibm.biz/askmeeting



IBM Security Verify 무료 평가판 사용하기



10분 이내로 시작하실 수 있습니다

- 원스톱 IAM 구성 및 관리를 제공하는 Verify 대시보드 사용
- 첫 애플리케이션을 추가하여 SSO(싱글 사인온) 경험
- 다중 인증 구성
- 기존 디렉터리 연결 또는 신규 사용자 추가

ibm.biz/VerifyFreeTrial



감사합니다.

