



Tenable Cloud Security CNAPP을 활용한 기업의 클라우드 보안 강화 방안

Member of the Global **IFSEC** Group

전자정부 정보보호 솔루션 페어

SECON | eGISEC 2024

목차

1

클라우드 보안
어려운 점

2

CNAPP 환경
정의

3

인증 중요성

4

테너블 클라우드
시큐리티

클라우드 보안의 어려움

퍼블릭
클라우드

복잡성

1000개 이상의 인증과
권한 설정

가시성

사용자와 서비스 계정,
정책, 멀티클라우드

위험

실제 접속 위험 분석 및
우선순위 선정

소유권

Dev | DevOps | IAM |
클라우드 보안

90%

의 클라우드
계정은 서비스이고
10% 만이 사용자
계정

85%

이상의 기업이
지나치게 많은
권한을 가진
관리자 계정 보유

5%

이하의 권한만
실제 사용*

* Microsoft Security, 2023 State of
Cloud Permission Risks Report

클라우드 보안의 기초 전략

CIS CIS AKS 1.2.0 - Prescriptive guidance for running Azure Kubernetes Service following recommended security controls

Requirement

4.2 Pod Security Policies

Requirement

4.2.1 Minimize the admission of privileged containers

Privileged containers have access to all Linux Kernel capabilities and devices. A container running with full privileges can do almost everything that the host can do. This flag manipulating the network stack and accessing devices.

4.2.5 Minimize the admission of containers with allowPrivilegeEscalation

A container running with the allowPrivilegeEscalation flag set to true may have processes that can gain more privileges than their parent.

4.2.7 Minimize the admission of containers with added capabilities

Containers run with a default set of capabilities as assigned by the Container Runtime. Capabilities outside this set can be added to containers which could expose them to r not generally permit containers with capabilities assigned beyond the default set.

5.4 Cluster Networking

Compliance

AWS Well Architected

CIS AKS 1.2.0

CIS AWS 1.4.0

CIS Azure 1.5.0

CIS EKS 1.2.0

CIS GCP 1.3.0

CIS GKE 1.3.0

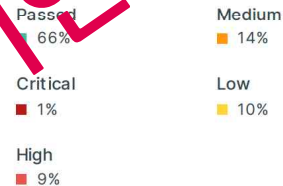
Last 30 days

컴플라이언스

tenable Cloud Security | SOC2 Type II

SOC2 Type II summary

Represents the overall status score while categorizing the findings by their severity.



Cloud	Policy	Severity	Standards	Status	Result	Actions	Exclusions
AWS	EC2 instance metadata service supports insecure version	Low	ISO 27001, NIST 800-53, CIS 1.4.0	Enabled on all accounts	78 of 80 resources failed 2 Findings >	resources > resource patterns	
AWS	ECR critical repository vulnerabilities	Low	ISO 27001, NIST 800-53, CIS 1.4.0	Enabled on 2 accounts	2 of 5 resources failed 1 Findings >	resources > resource patterns	
AWS	Public Lambda function	Low	ISO 27001, NIST 800-53, CIS 1.4.0	Enabled on all accounts	28 of 28 resources passed	resources > resource patterns	
AWS	Virtual machine is using unmanaged disk	Low	ISO 27001, NIST 800-53, CIS 1.4.0	Enabled on all accounts	3 of 34 resources failed 3 Findings >	resources > resource patterns	

tenable

지속되고 있는 클라우드 보안 사고



과도한 권한을 가진 내부자가 대량의 데이터를 유출



직원이 기가 단위의 내부 기밀 데이터를 유출



3rd पार्ट 인증 정보 유출로 인해, 4만7천거의 B2B 고객 정보 유출



저장소에서 사용자 접근 키 유출



사회공학적 방법을 통해 사용자 계정 획득, 고객 개인정보 획득



유출된 계정 정보와 잘못 구성된 스토리지 버킷으로 유출



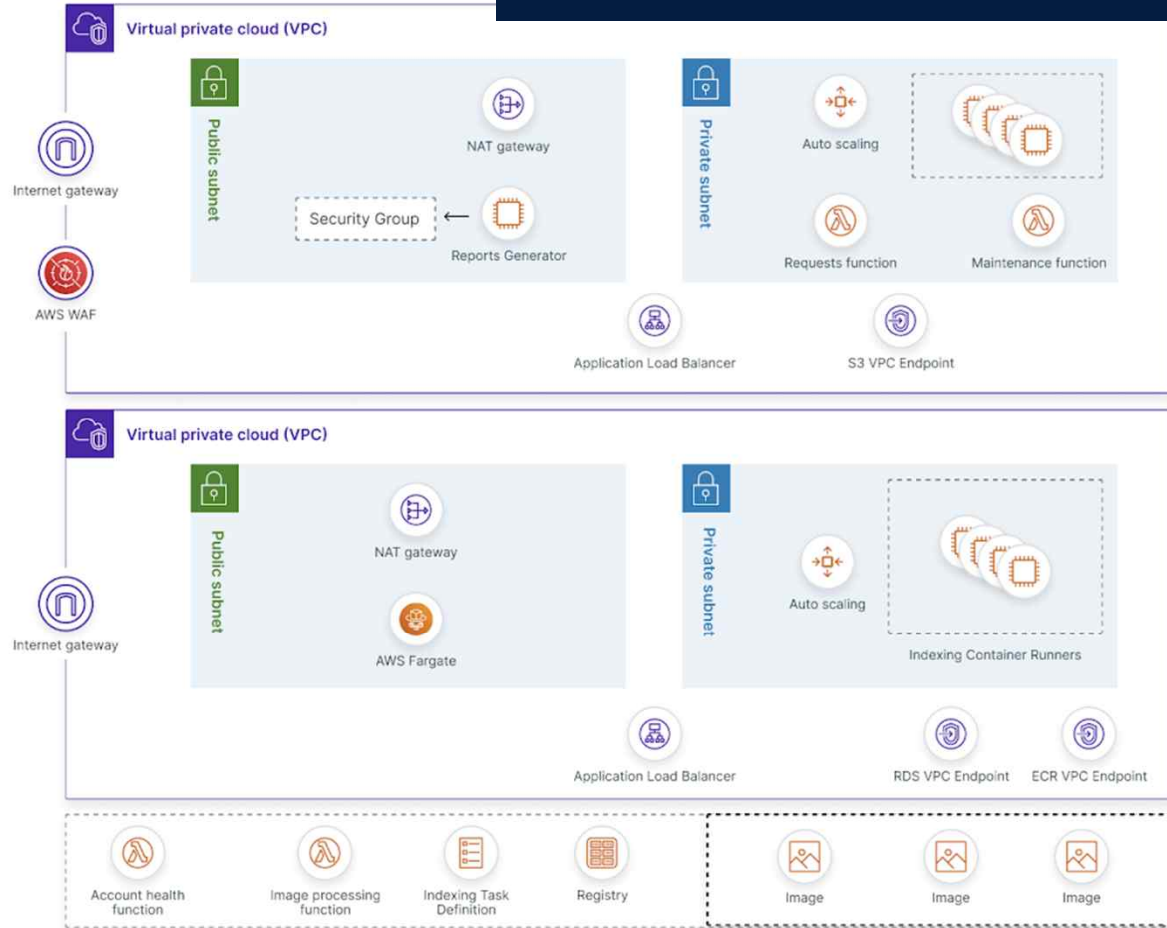
6.5테라 데이터 유출



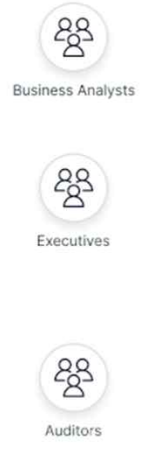
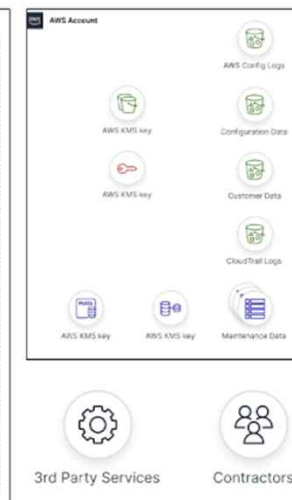
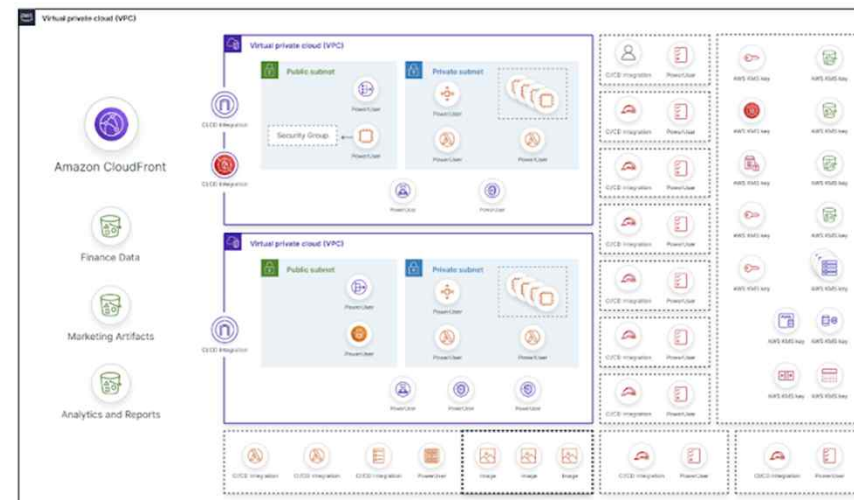
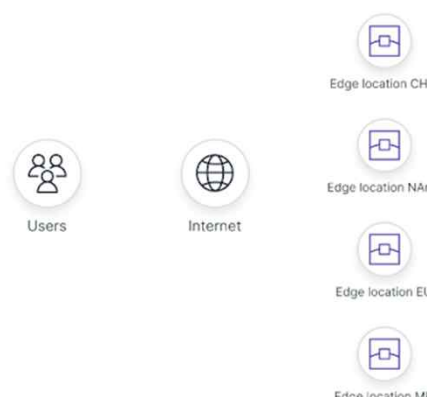
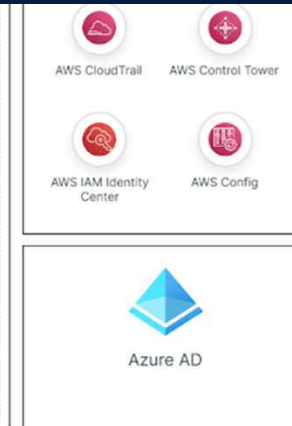
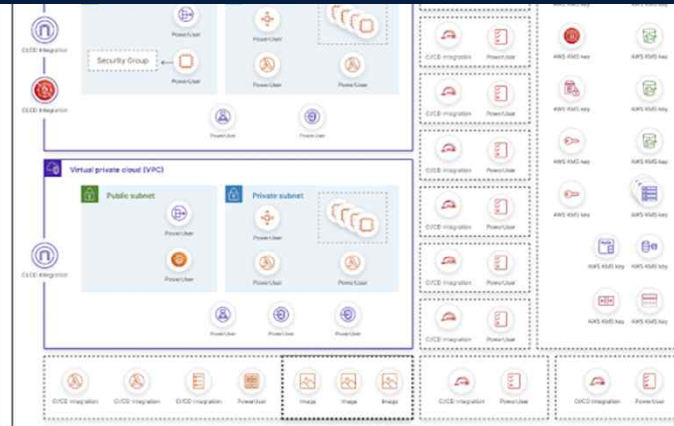
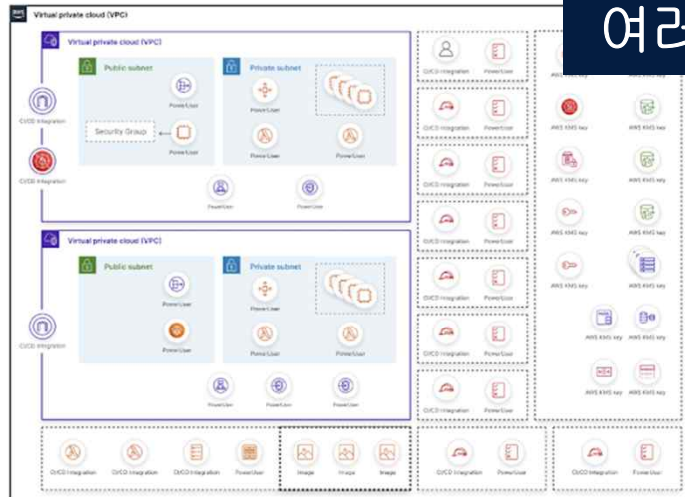
여러분의 클라우드는 어떤 모습인가요?



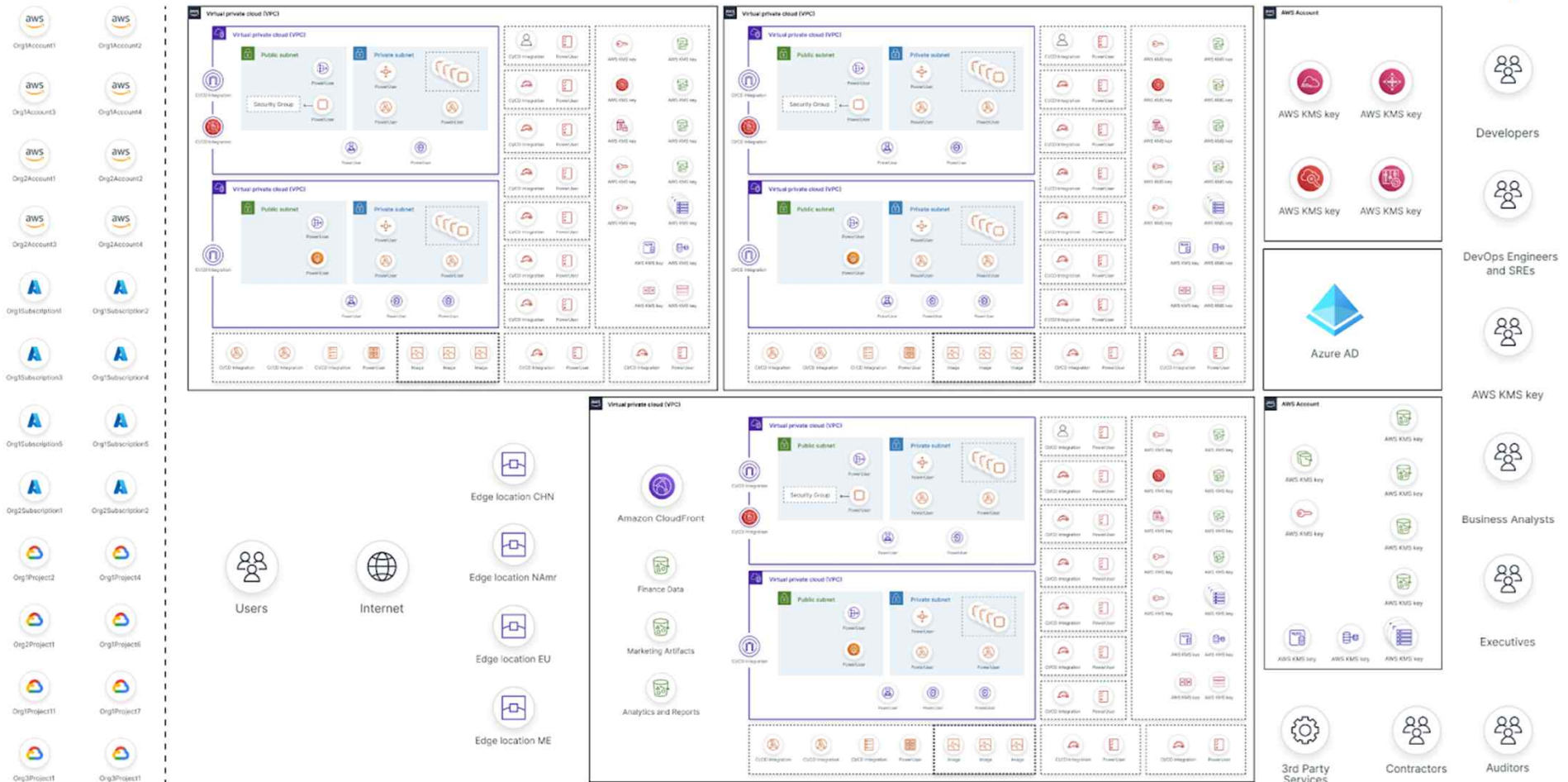
Virtual private cloud (VPC)

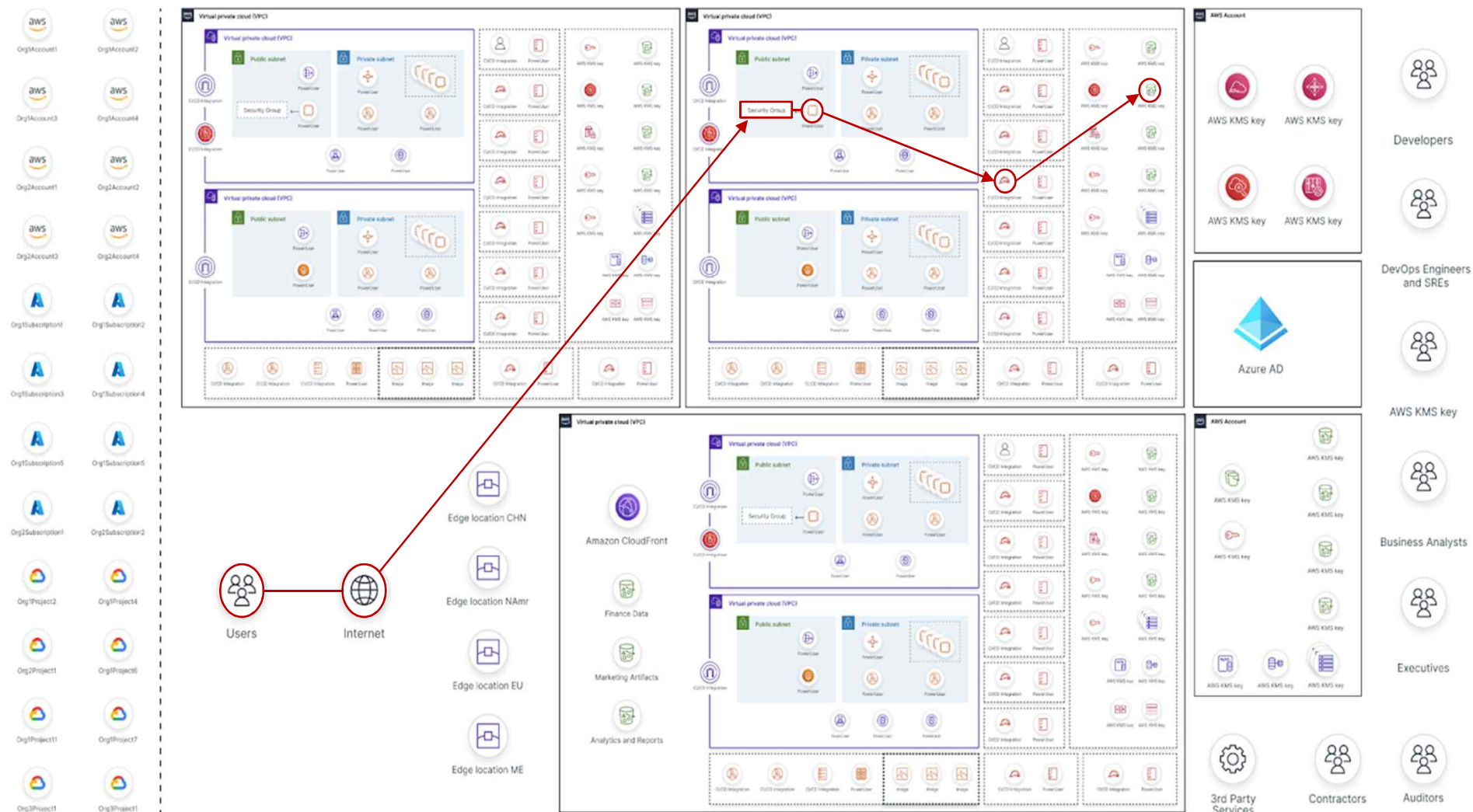


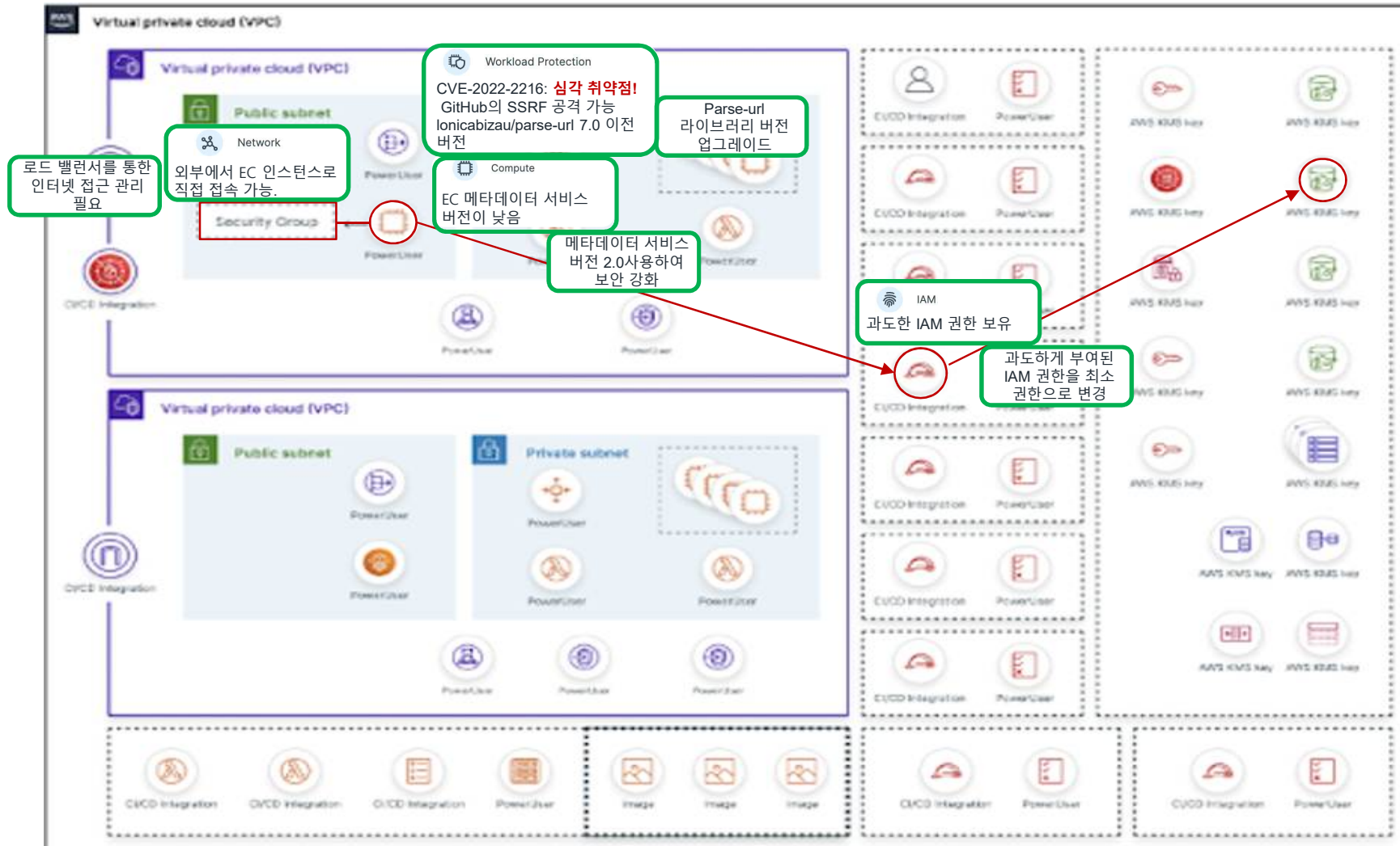
여러분의 클라우드는 어떤 모습인가요?



여러분의 클라우드는 어떤 모습인가요?







클라우드 보안을 위한 **CNAPP** 플랫폼

클라우드
보안 환경
CNAPP

CIEM

계정 접속 및 권한 관리 |
최소권한 설정 | Just-in-Time

CSPM

멀티클라우드 환경 구성 오류 |
위험 평가 및 보고서 |
컴플라이언스

CWP

워크로드 보호 | 취약점 관리 | 악성
파일 탐지 | 비밀번호

IaC

CI-CD 단계에서 잘못된 설정
확인 | 코드 수정

CDR

로그 쿼리 | 이상 행위 탐지 및 조사 |
빠른 조사 | 포렌식

KSPM

쿠버네틱스 잘못된 설정 가시성
확보 | 취약점 분석 | 컴플라이언스

CNAPP에는 SASE (CASB, ZTNA, SWG), IGA, PAM, SSPM 등은 포함되지 않음

“75%의 클라우드 보안의 문제는 잘못된 권한 관리의 결과”
- Gartner

“80%의 기업은 지난 12개월내에 계정 연관된 사고를 경험”
- IDSA Survey 2022

출처: [Managing Privileged Access in Cloud Infrastructure](#), Gartner
[Why Cloud Security Risks Have Shifted to Identities and Entitlements](#)

클라우드 보안 강화를 위해 개별 솔루션의의의 사용

“**30% 미만**

기업만이 **CSPM**, **CWP**
및 **CIEM** 같은 통합 보안
도구를 멀티클라우드
환경에서 사용중입니다.”

-CSA

CSPM

CWPP

IAC

KSPM

CDR

CIEM

“**80%**의 조직이

지난 12개월간
인증 관련 보안 침해를
경험했습니다.”

- IDSA 설문 조사

...클라우드 보안 관리에서 가장 취약한 부분은 **인증보안(CIEM)**

*출처: Cloud Security Alliance: 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP) 설문 조사 보고서, 2023년 8월
Identity Defined Security Alliance: [2022년 디지털 ID 보안 트렌드](#)

인증 보안이 **CNAPP**으로 가는 유일한 진입로

CSPM, CWPP



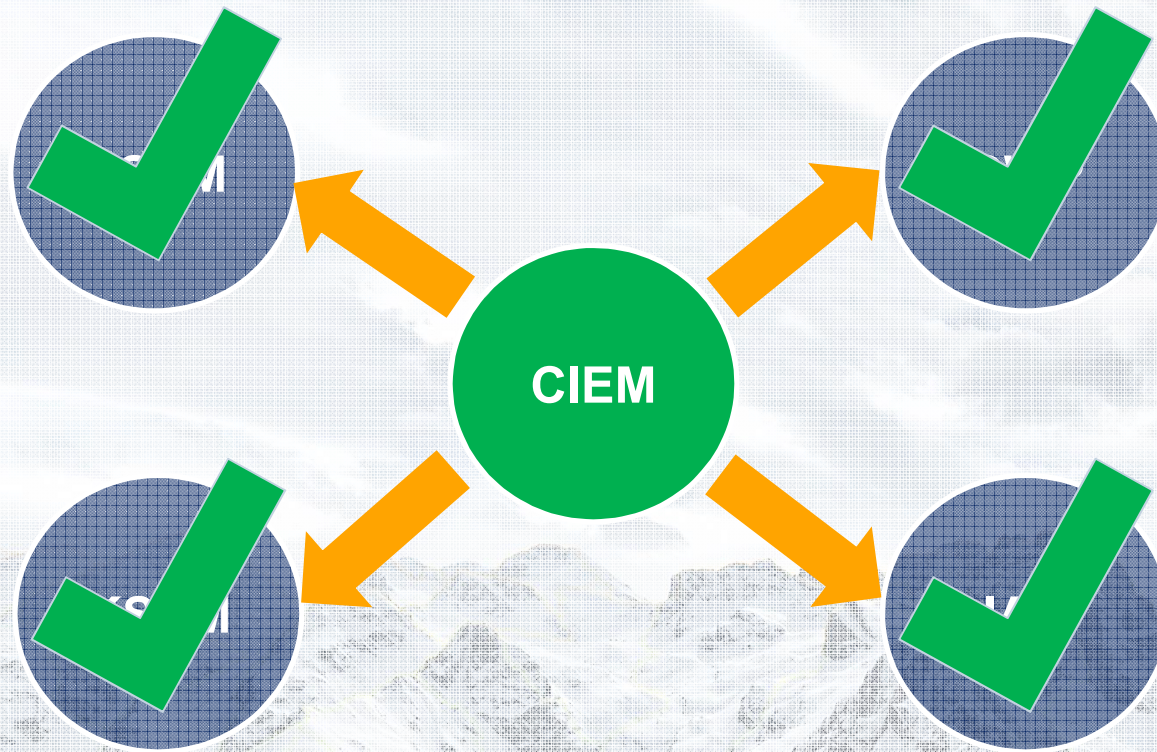
CIEM



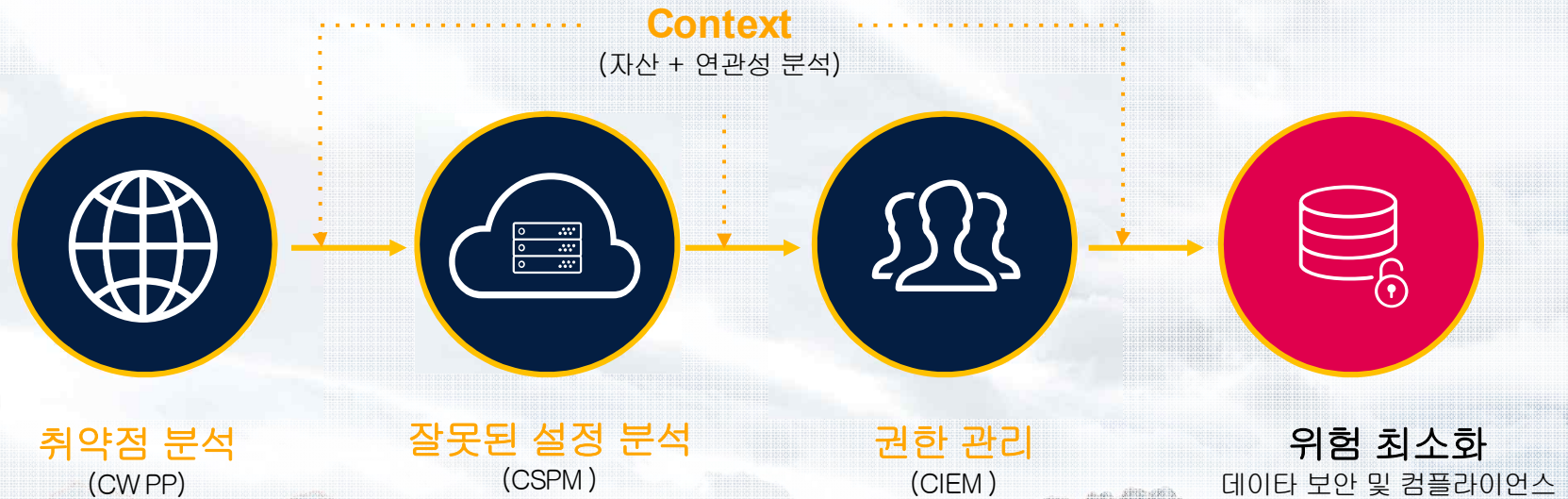
CNAPP를 위한 간단한 점검

- 1 멀티 클라우드 환경의 모든 사용자와 자원에 부여된 권한 점검 수행
- 2 외부에 노출된 자원의 잘못 설정된 보안 그룹 또는 네트워크 접근 통제와 공격가능한 취약점 확인
- 3 자원 단위에서 외부 연결 계정 권한과 접속 가능 경로 확인
- 4 어떤 특권사용자 계정이 사용중인지 또는 휴면/유효하지 않은지 확인
(비상상황 접근, 권한 이탈등.)
- 5 규정이 준수되지 않고 있는 정책을 확인하고 최소 권한 설정으로 변경

CNAPP 보안 강화 방안

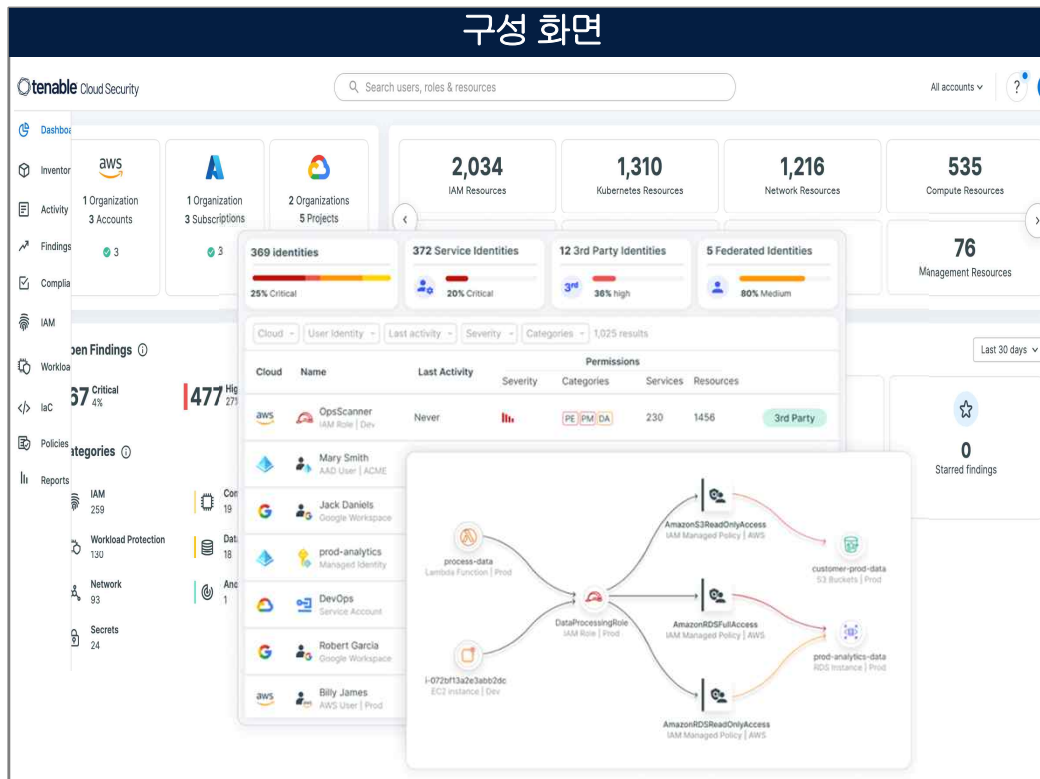


CNAPP에서 가장 중요한 것



단일 플랫폼을 통한 모든 위험을 분석

모든 클라우드 자산 통합 관리 및 통제

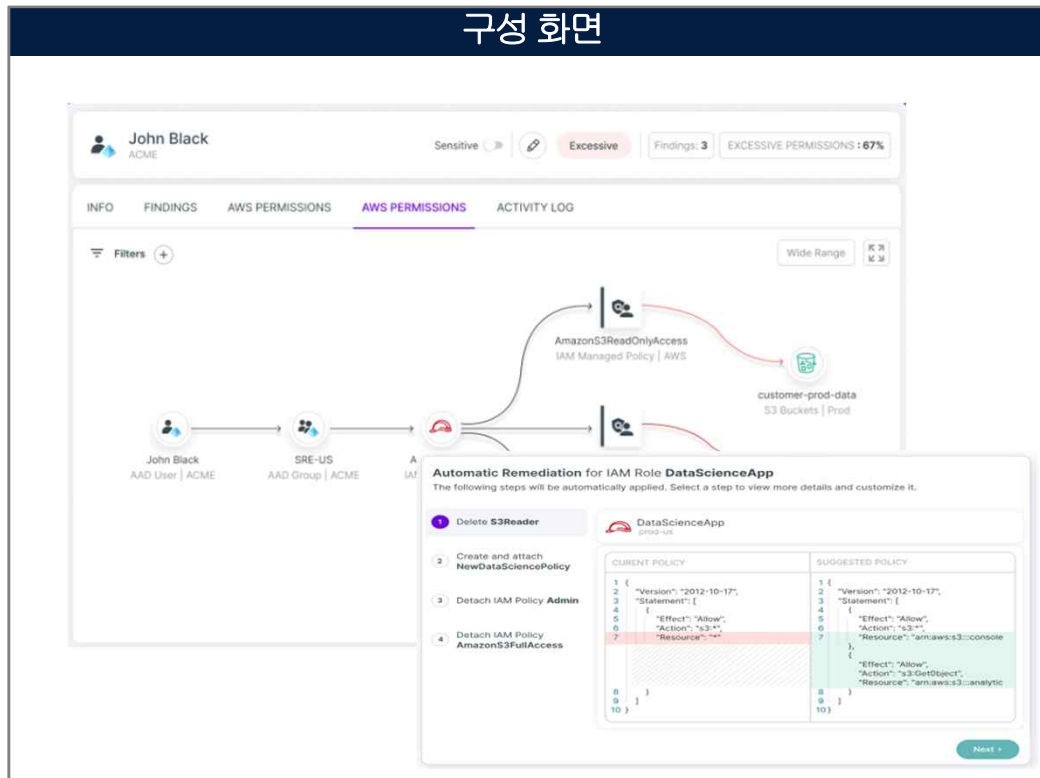


내용

- 지역, 계정, 비즈니스 단위로 AWS/Azure/GCP 전반에 대한 전체 자산 목록을 관리
- 모든 자원, 구성, 권한 및 활동에 대한 세분화된 상황별 가시성 제공
- 서비스 종류, 자원 및 설정별로 스마트 검색과 쿼리를 통해 분석 기능 제공

사용자의 모든 권한을 시각화 제공 하고 최소 권한 방안 제공

구성 화면



내용

- 사용자 친화적 방식으로 복잡한 구성 내역을 시각화하여 제공
- 누구나 위험 발생 가능성을 쉽게 찾을 수 있고 원인을 확인할 수 있어 신속한 위험 분류 및 조치가 가능하게 제공
- 복잡한 권한 문제를 쉽게 해결 할 수 있도록 문제 해결 방안 제공, “문제점을 직접 눈으로 확인”
- 최소 권한을 적용할 수 있는 방안을 제공

Just-in-Time (JIT)을 통한 접속 관리

구성 화면

Access Requests




+ Request Permission

▼

...

Pending

2

Cloud	Requestor	Group	Permission	Duration	
aws	 Theo Wiggins	IT	Power user	3 Hours	<div><div>✖ Deny</div><div>✔ Approve</div></div>
	 Mary Smith	IT	BigQuery Reader	2 Days	<div><div>✖ Deny</div><div>✔ Approve</div></div>

>

✔

Active




0

▼

🕒

History

2

Created	Requestor	Permission	Duration	Status
aws	 Robert Garcia	Read-only	4 Weeks	<div><div>🕒</div>Cancelled by me 10:34 am Nov 7, 2022</div>
	 Ahmud Haddad	Contributor	1 Week	<div><div>✖</div>Denied by admin 09:25 am Nov 21, 2022</div>

내용

- 관리자 설정 가능 자격: 누가 접속 가능한 사용자 인지, 어떤 계정인지, 어떤 권한을 가질 수 있는지, 최대 권한 사용 시간, 누구의 승인을 받아야 하는지
- 사용자 권한 요청 - 포탈을 통해서 기능 제공
- 사전 승인 및 수동 및 최소 2인 승인 프로세스 (4 eye approval)
- 이메일과 슬랙을 통한 접속 요청 공유
- 자격, 접속 요청 및 접속 검토에 대한 전체 감사 제공

위험 우선순위 평가

구성 화면

Toxic Combinations ⓘ

- 9 public workloads with critical vulnerabilities and high privileges
- 54 public workloads with an unpatched operating system
- 28 public virtual machines with critical vulnerabilities
- 2 ECS services with critical vulnerabilities
- 1 public App service with high privileges

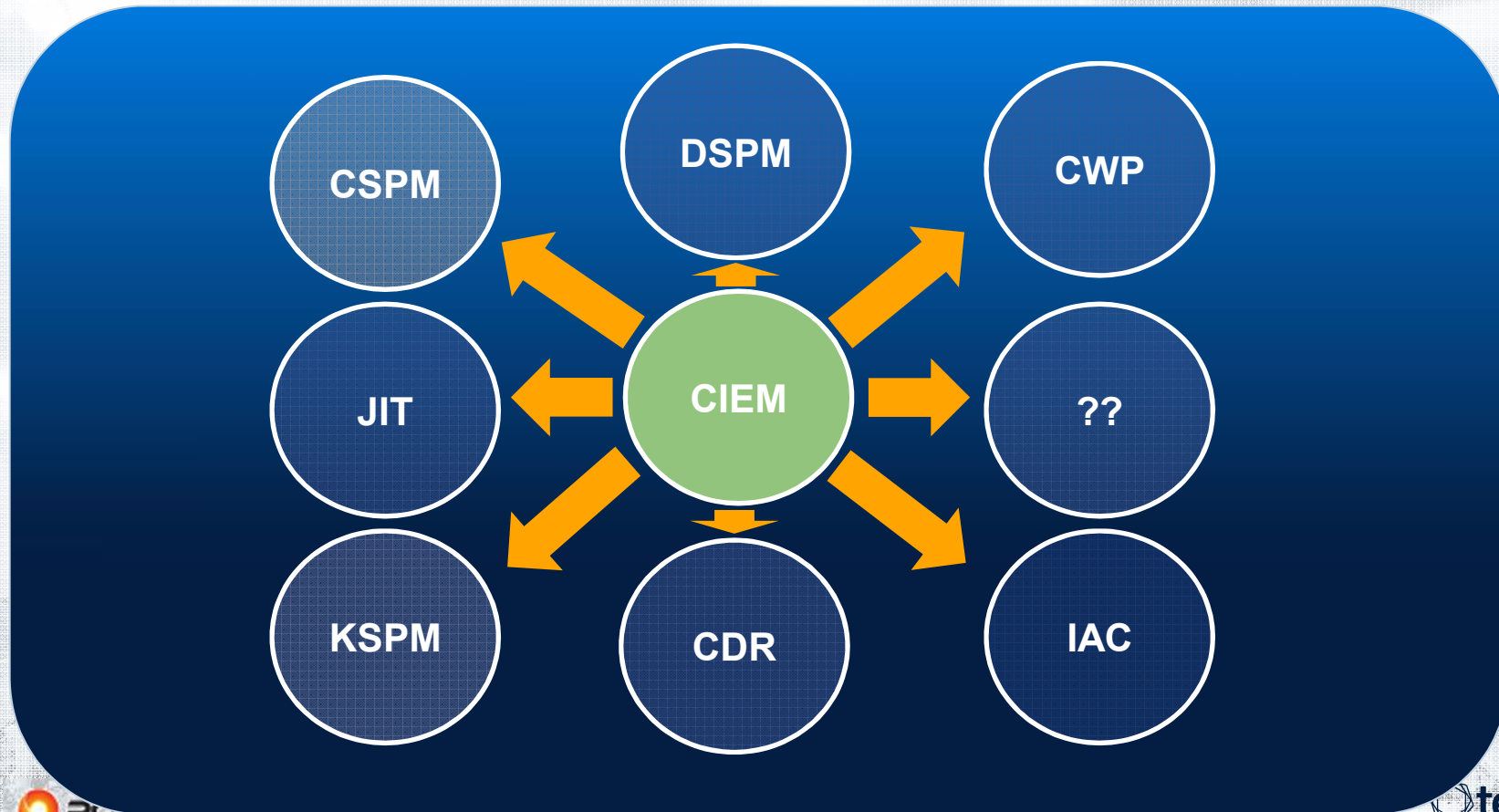
If you only have 5 minutes... ⓘ

- Public IAM role**
sePublicIAMRole_AlexaBusiness | aws Dev (463107564615)
- Public EC2 instance**
EC2ContainerService-eagle-cluster-EcsIn... | aws Dev (463107564615)
- EC2 instance has an unpatched operating system**
i-068e969ffacea00a1 (Service1) | aws Dev (463107564615)
- Public KMS key**
service1 | aws Prod (226366691213)
- Cloud Run service is exposing secrets**
hello | Prd-Env (prd-env-341521)

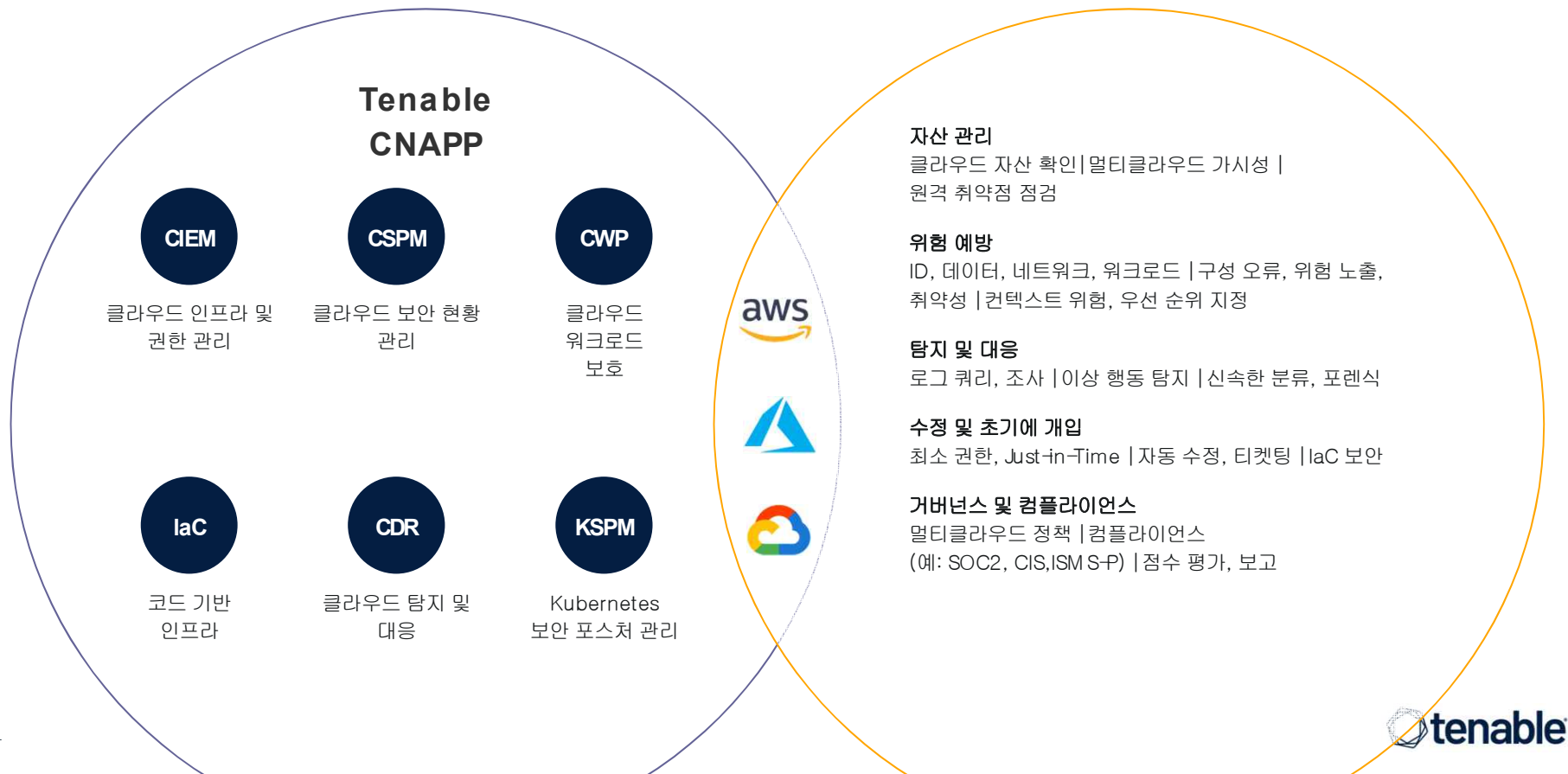
내용

- 클라우드 보안 위협을 결합하여 연계 위험을 확인
- 연계된 위험을 함께 분석하여 쉽게 위험을 평가할 수 있도록 지원
- 최단 시간 위험 분석 방안을 제공하여 높은 위험도에 대한 조치를 유도

CNAPP 환경의 지속적 변화



클라우드 보안 위험 탐지 및 대응



클라우드 보안 성숙도 향상

- 클라우드 보안을 위한 성숙도 향상 방안
- 조직 구성 - 인력 및 프로세스
- 보안 강화를 위한 기술: 가시성, 예방 및 탐지
- 성숙도를 평가하여 기업의 보안 구성 목표를 설명
- 모든 분야를 평가한 후 조직에 한 개의 전체적 성숙도 레벨을 할당

	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
PEOPLE				
Roles and responsibilities	No dedicated personnel for cloud infrastructure security	Some knowledge and responsibility within the security team Executive sponsor for cloud security program, early form of CCOE	Dedicated person / team with relevant training and expertise Established CCOE	Additional expert delegates within R&D team
Training	No dedicated training / expertise in cloud security	Some members of security team undergo cloud security training	Cloud security team undergoes formal cloud security training and certification	Cloud security awareness training program for R&D
PROCESSES				
Remediation process	Best effort with no structured process	Security team owns and prioritizes security findings	Prioritized findings automatically shared with stakeholders	Full ownership of R&D teams for resolution of issues
Integration to CI/CD pipeline	Infrastructure is not managed as part of CI/CD pipeline	Proper process for governing change management	Managing infrastructure as Code	Embedding infrastructure security in the CI/CD pipeline
Compliance	Meeting no defined standard	Mandatory compliance standards are met	External best practice(s) implemented and audited Governance principles documented and tracked Screen reader support enabled	Custom compliance rules enforced
Access governance	Rudimentary access review is done based on best effort, if it all	Groups / labels / organizational-structure based level access review Consistent access and	Risk-based access review for sensitive resources and privileged identities	Risk-based access review for all resources and identities

	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
VISIBILITY				
Inventory management	Manually or with cloud console	Using a script or in-house solution	Automatically, centralizing from all cloud platforms	Inventory is filterable and searchable
Contextualization	Basic information only	Mapping relationships between resources	Classifying inventory manually	Automatic classification of inventory
PREVENTION				
Identities	Best effort identity governance	Implementing basic best practices	Retire the use of static credentials	Governing unused identities and credentials
Entitlements	Best effort governance of human / service entitlements	Visibility into what identity can access what resource	Classifying privileged identities	High resolution least privilege
Data	Data security best practices	Public data exposure governance	Governing segregation to critical environments	Governing sensitive data segregation on the resource level
Computing	No governance and visibility of compute security posture	Conducting Host (OS / Containers) patch management	Implementing Host (OS / Containers) configuration best practices	Vulnerability management for software packages
Network access	Ungoverned network access	Public access is governed and remediated	Network access to sensitive resources is restricted	Microsegmentation of network resources
DETECTION				
Log collection	Distributed /cloud vendor default	Centralized logs	Indexed and queryable logs	Normalized and enriched information
Log analysis	None / Manual review of logs	Detection of specific suspicious events	Detection of IoCs from native monitoring tools	Comprehensive detection of anomalous behaviour



고맙습니다.

자세한 사항은 S065에서 설명 드리겠습니다.

Member of the Global **IFSEC** Group

전자정부 정보보호 솔루션 페어

SECON | **eGISEC 2024**