AccuKnox

Secure Code to Cognition™

AI 기반

제로 트러스트 CNAPP

Rated 4.5/5

Rated 4.3/5

Certified & Accredited by

NVIDIA Inception Program

AWS Partner Containers Software

NetApp Excellerator

Open Horizon

NASSCOM Emerge 50 Awards

Nutanix

As Featured In

Gartner

IBM Cloud

Oracle

aws

LF Edge

Nephio

Available On

awsmarketplace

Microsoft Azure Marketplace

Red Hat Marketplace

Oracle Cloud Marketplace

개요

1 우리는 어떤 문제를 해결하나요?

2 고객 승리

3 제품 제공

4 플랫폼화 - 통합 보안

5 지원 매트릭스

6 독보적인 차별화

7 아키텍처 및 배포 모델

8 POC 타임라인

과제... 해결책...

ACCUKNOX

Challenges

- ❌ 모든 고급 공격은 런타임 공격입니다.
- ❌ AppSec, CloudSec, AISec을 위한 다양한 도구
- ❌ 온프레미스 보안과 클라우드 보안을 위한 분리된 도구

Impact

- 제로데이 공격에 노출
- 공격 표면 증가
- ~ 100% 더 높은 (도구, 인력) 비용

AccuKnox Solution - Zero Trust CNAPP

- ❑ 모든 퍼블릭 및 프라이빗 클라우드에 배포
- ❑ 모든 자산(K8, VM, API, Edge)을 보호하세요.
- ❑ 통합 AppSec, CloudSec 및 AI 보안
- ❑ 50% 이상 절약

AccuKnox Code to Cognition™ Solution

AppSec ← → CloudSec CNAPP [Cloud Native Application Protection Platform] ← → API Sec ← → AISec

ASPM | CSPM | CWPP | KIEM | KSPM | CDR | API SECURITY | AI SECURITY

PUBLIC CLOUD: aws

PRIVATE CLOUD

EDGE / IoT: ARM

SIEM – End-to-end Threat Intelligence

Ask AI – Conversational Interface – DevSecOps meets ChatGPT

Compliance – Support for 35+ standards

CTEM – Continuous Threat Exposure Management

플랫폼화

AccuKnox

ASPM
(앱 보안)

- 정적 애플리케이션 보안 테스트 (SAST)
- 동적 애플리케이션 보안 테스트 (DAST)
- 비밀 스캔
- IAC 스캔
- 소프트웨어 자재 목록 (SBOM)
- 소프트웨어 구성 분석(SCA)

CSPM
(클라우드 보안)

- 클라우드 자산 및 인벤토리 가시성
- 드리프트 감지 및 교정
- 제로 트러스트 정책 시행
- 규정 준수 및 감사 벤치마크

CWPP
(워크로드 보안)

- 최소 허용 자세 평가
- 보안 비밀 관리자
- 컨테이너 및 VM 적용
- 런타임 위협 탐지

KSPM
(쿠버네티스 보안)

- 클러스터 오류 구성 감지
- CIS K8s 벤치마크 결과
- K8s ID 및 권한 관리(KIEM)
- Pod 및 네트워크 보안 모니터링

AI-SPM
(AI 보안)

- AI 탐지 및 대응(AI-DR)
- 프롬프트 방화벽
- AI 런타임 앱 보안
- 모델 및 데이터 세트 보안
- LLM 레드팀
- AI 규정 준수

플랫폼 전반 지원

규정 준수
35개 이상의 프레임워크 : SOC2, PCI DSS 등

CDR
클라우드 감지 및 대응

API 보안

AI 조종사

시엠
보안 정보

고객 성공 사례 | 사례 연구

PRUDENT

Insurance firms leverage AccuKnox Zero Trust CNAPP for Real Time Cyber Defense

Achieves 2x Operational Efficiency with AccuKnox

$1.5M Awarded for Cutting-Edge Security

IDT CORPORATION

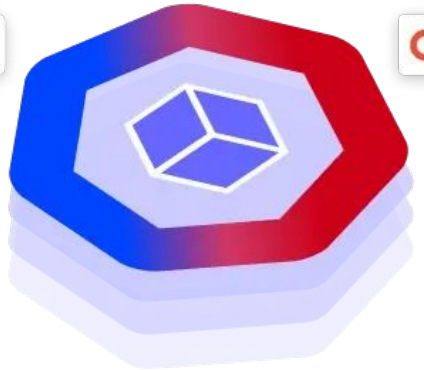
A Global Leader in Wholesale Telecommunications

Secures Point of Sale Devices, Reduced Service Interruptions by 80%

IDT CORPORATION PRUDENT SONESTA INTERNATIONAL HOTELS SupportLogic

G Rated 4.5/5

G2 Rated 4.3/5



Refer - accuknox.com/case-studies

ACCUKNOX

AI 기반 제로 트러스트

AccuKnox
인지에 대한 보안 코드

하나의 통합 CNAPP

DevSecOps, AI 공동 조종사

ASPM **CSPM** **AI-SPM** **KSPM** **CWPP** **GRC** **런타임 보안**

SIEM, SOAR, EDR, 티켓팅 플랫폼과의 통합

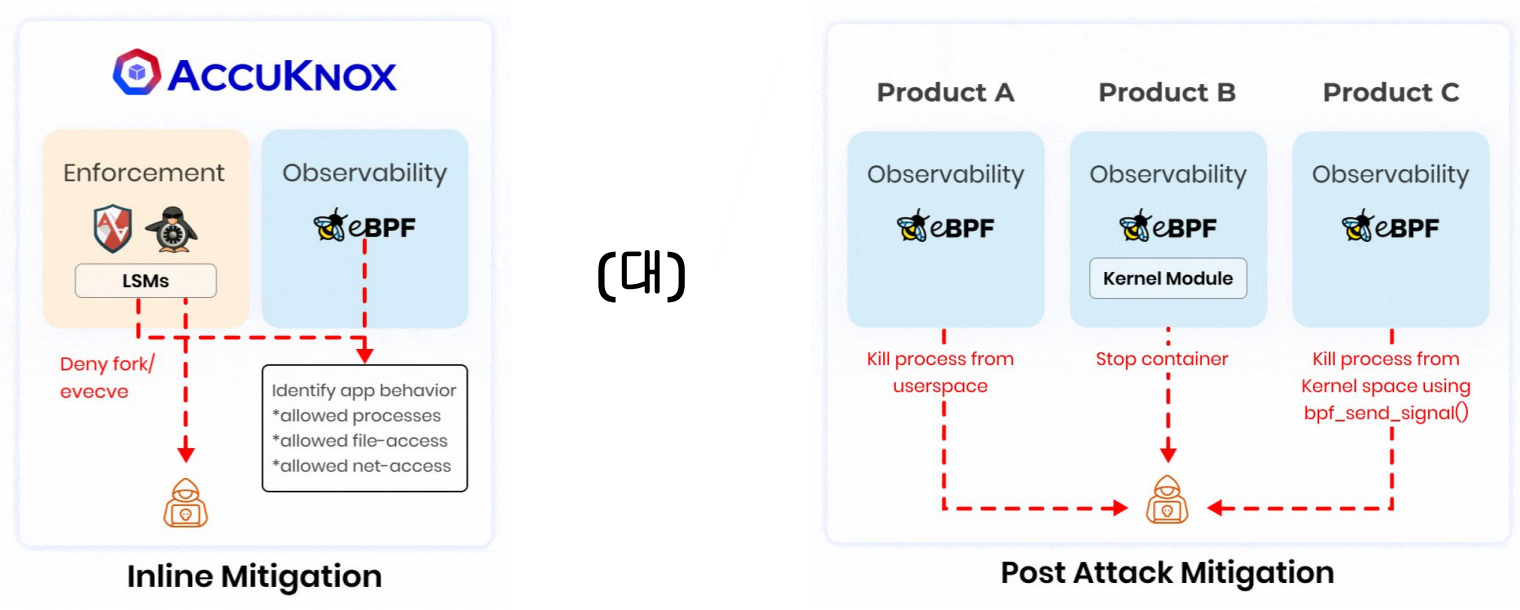
시엠

유연한 배포 모델

AccuKnox

독특한 차별화

AccuKnox는 "관찰하다" >> "억지로 시키다" 공격 시간 동안 >> 자동 생성" 정책">



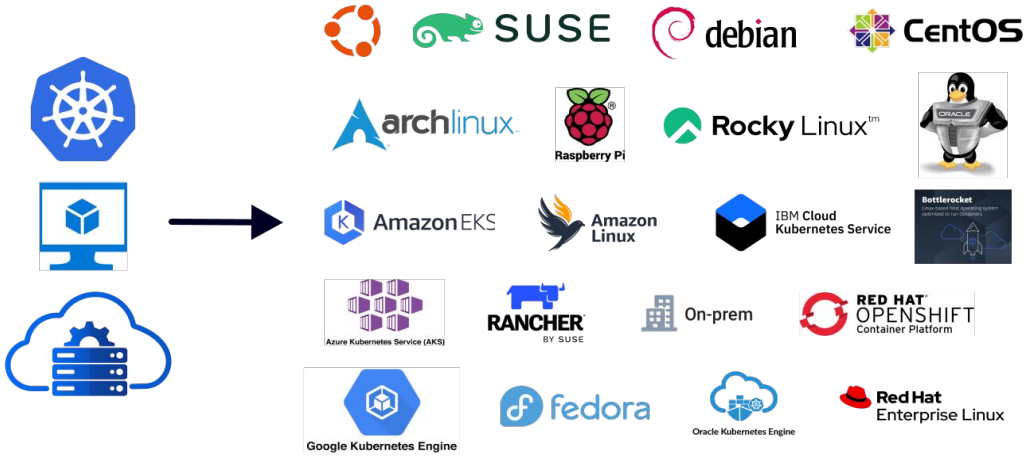
*We defend against real time
Zero Day Attacks!

ACCUKNOX

지원 매트릭스

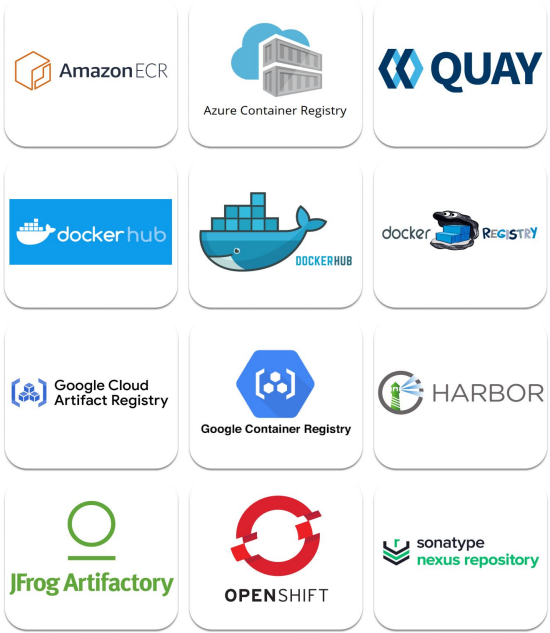
1) 구름

2) 클러스터(온프레미스, VM)



**Linux 기반 운영 체제*

3) 컨테이너 레지스트리



ACCUKNOX

독보적인 차별화

ACCUKNOX

- **하나의 플랫폼**
- - 포괄적인 범위
- ***코드 → 클라우드***
- **자동 제로 트러스트 정책**
- - 인라인 교정용
- **유연한 배포**
- - 퍼블릭 및 프라이빗 클라우드
- **SOAR 플랫폼**
- -
- 50개 이상의 통합 기능을 기본으로 제공합니다.

구름

- CSPM 임원 대시보드
- 잘못된 구성 감지
- 재고 평가
- 지속적인 규정 준수
- 드리프트 감지 기준

코드

- 정적 코드 분석
- 소프트웨어 구성 분석
- 비밀 스캐닝
- CI/CD 통합부터 빌드 사이클까지
- 취약점 관리

이미지

- 이미지 위험 평가
- 취약점 스캐닝
- 위험 기반 우선순위 지정
- 규정 준수 및 보고
- CI/CD 통합
- 취약점 관리

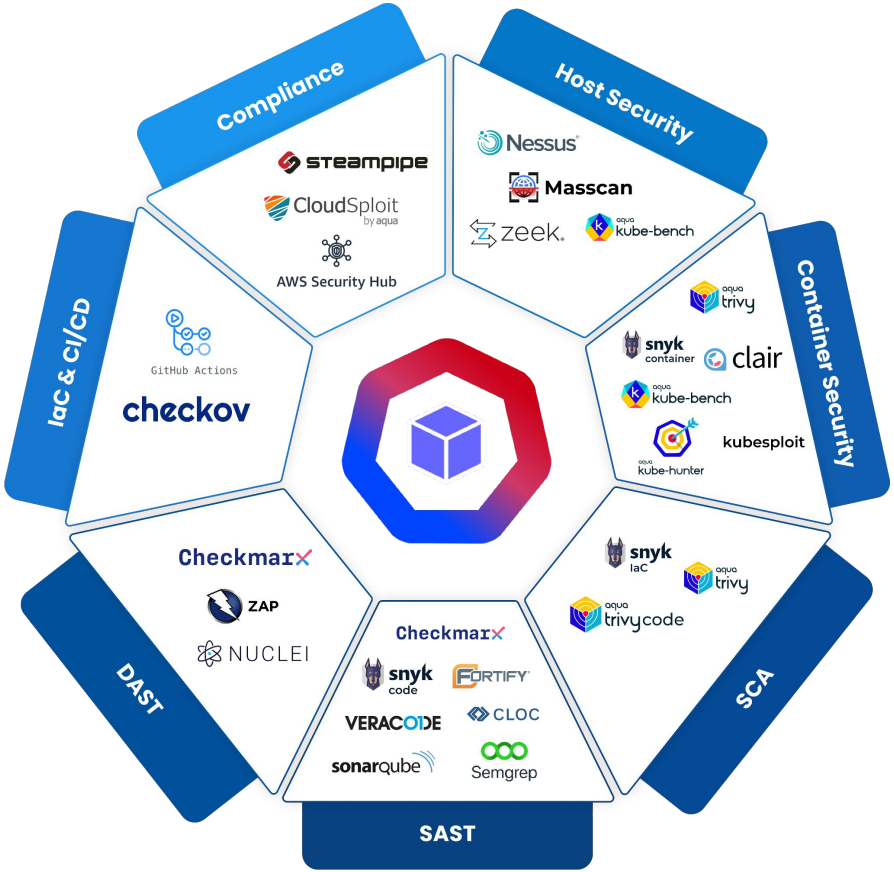
보안 구역	특징
관찰 가능성	워크로드 관측성
규정 준수	워크로드 강화 정책
모니터링	로그 및 알림
제로 트러스트	자동 검색된 제로 트러스트 정책 맞춤형 제로 트러스트 정책 인라인 교정 네트워크 마이크로세그먼테이션
새로운 기능	입학 관리자 지원 KIEM(K8s 신원 및 권한 관리) ECS/EKS Fargate 지원

바로 사용 가능한 도구!

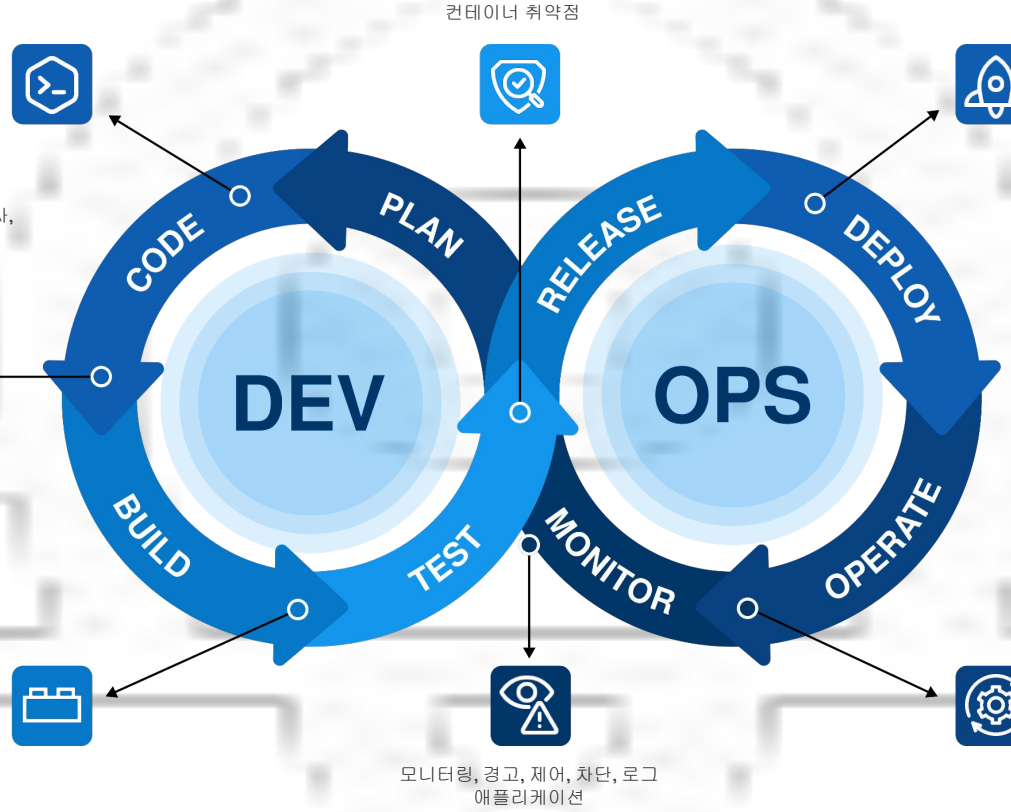
AccuKnox

왼쪽으로 이동하고 오른쪽으로 고정

- 호스트 보안
- 컨테이너 보안
- 규정 준수
- **IaC 및 CI/CD** 스캐닝
- 사스트
- 다스트
- SCA



AccuKnox를 활용한 DevSecOps



사스트

- 앱 소스 코드나 바이트코드에 안전하지 않은 구성 요소가 있는지 확인하세요.
- 앱이 실행 중이 아닐 때 사전 검사, 내부 접근.

SCA

- 앱 소스 코드나 바이트코드에 안전하지 않은 구성 요소가 있는지 확인하세요.
- 앱이 실행 중이 아닐 때 사전 검사, 내부 접근.

IaC

- 인프라 프로비저닝(IaC 생성, 수정 및 삭제)
- 구성 관리(코드/API를 사용하여 인프라 상태 표현) [KICS, Tfsec, Checkov]

다스트

- 웹 UI 및 API에 악성 HTTP 요청을 호출하는 자동화되고 지속적인 검사로 광범위한 공격을 포괄합니다.
- 앱이 실행 중일 때 사전 검사, 외부 접근.

IAST

- 이들은 실행 중인 앱에 수동으로 연결되어 트리거되면 실행됩니다.
- 반응형 스캔, 앱 실행 시 내부 접근.

ACCUKNOX

AccuKnox

- Dashboard
- Inventory
- Issues
- Compliance
- Runtime Protection
- Collectors
- Monitors / Alerts
- Identity
- Reports
- Settings

Dashboard

Search anything...

Acme Corp

Thomas

5 Accounts — 2 Clouds

10 Clusters — Kubernetes & VM

75 Registries — 9 Registry Types

12 Repos — 3 Categories

CSPM Dashboard

Cloud Accounts 2 | Clusters 1 | Last 2 days

Cloud Accounts

5

Active 4

Inactive 1

Findings

2,809 3566/3566 Assets Scanned

Critical 120 | Low 120

High 120 | Not Available 120

Medium 120

Go to Findings >

Cloud Account Risk Assessment

29,039

Failed 120

Warning 120

Not available 120

Passed 120

Cloud Compliance

NIST 55%

SOC 2 40%

PCI DSS 70%

FedRAMP 35%

Pass | Fail | Warning

Go to Compliances >

Top 5 Asset Categories with Findings

aws_account-956994857092 120

aws_account-956994857093 90

aws_account-956994857094 77

aws_account-956994857095 54

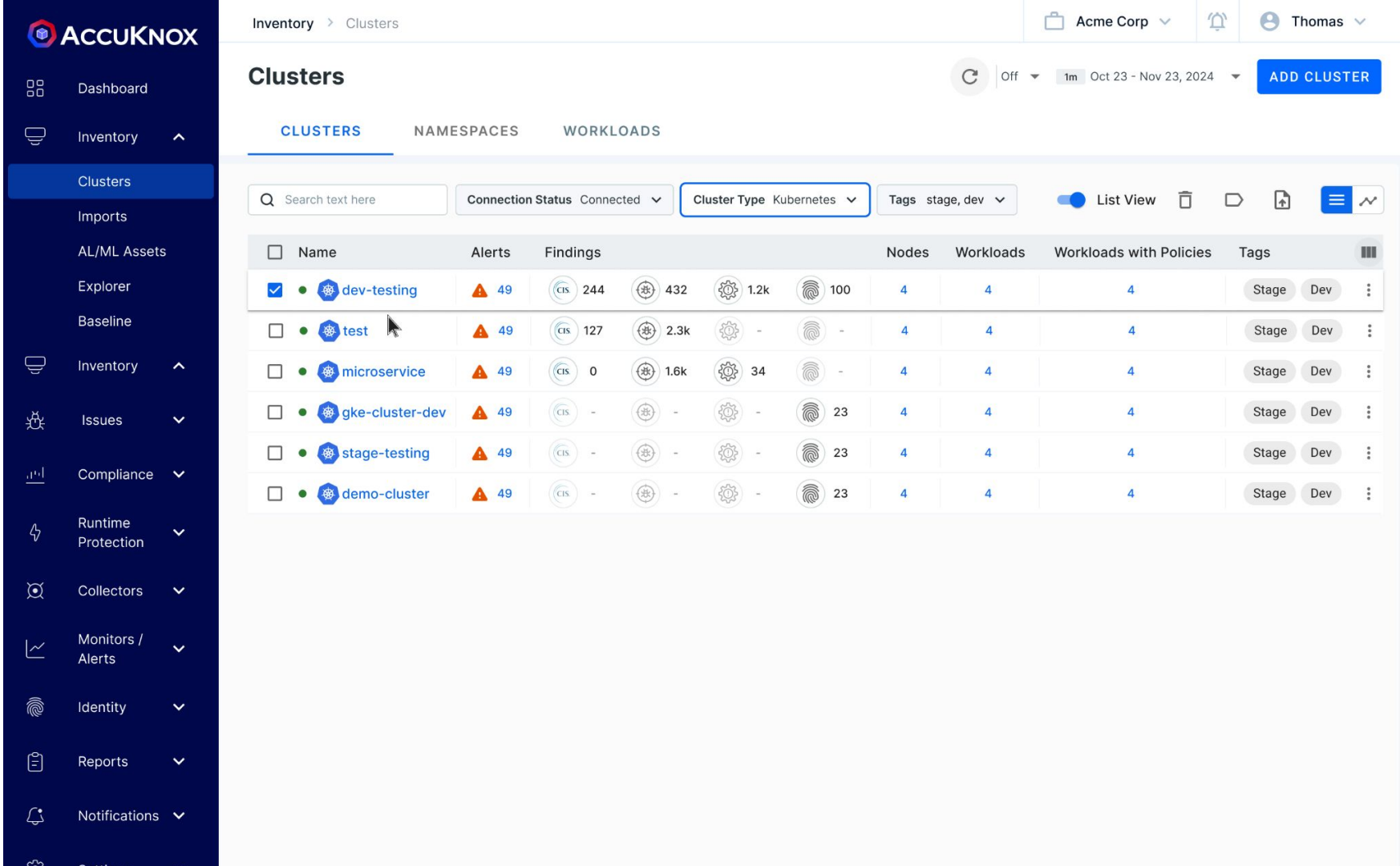
aws_account-956994857096 20

Findings Trend

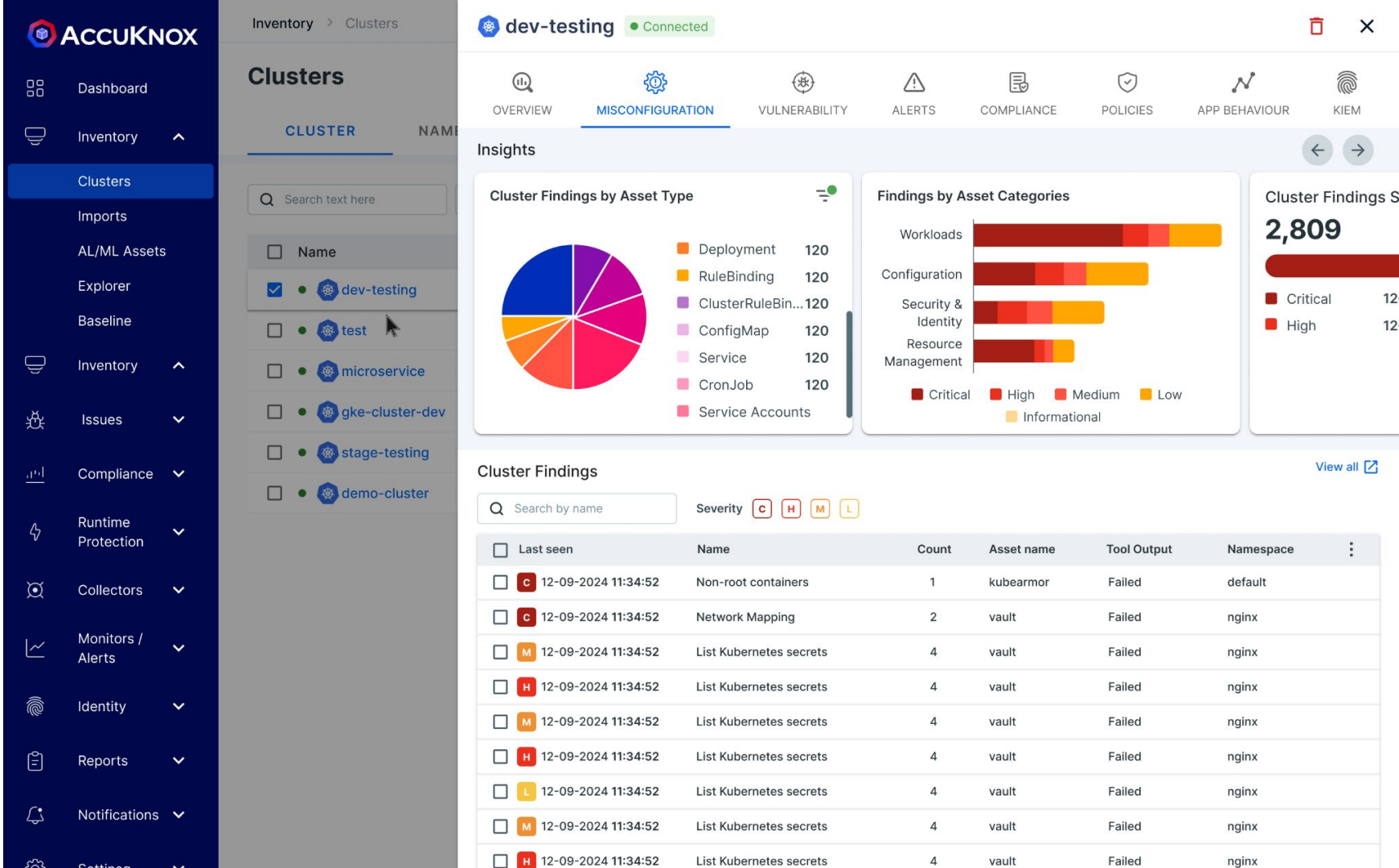
Active | Fixed | Inprogress | Potential

80 60 40 20 0

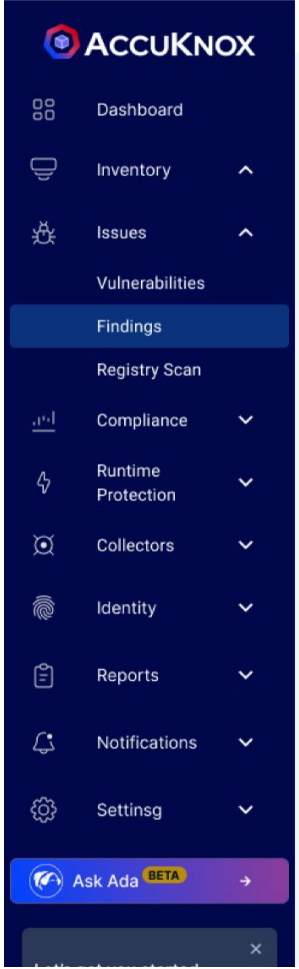
02 클러스터


ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Notifications
Inventory > Clusters
Acme Corp
Thomas
Clusters
Off
1m Oct 23 - Nov 23, 2024
ADD CLUSTER
CLUSTERS
NAMESPACES
WORKLOADS
Search text here
Connection Status Connected
Cluster Type Kubernetes
Tags stage, dev
List View
Name
Alerts
Findings
Nodes
Workloads
Workloads with Policies
Tags
dev-testing 49 244 432 1.2k 100 4 4 4 Stage Dev
test 49 127 2.3k - - 4 4 4 Stage Dev
microservice 49 0 1.6k 34 - 4 4 4 Stage Dev
gke-cluster-dev 49 - - - 23 4 4 4 Stage Dev
stage-testing 49 - - - 23 4 4 4 Stage Dev
demo-cluster 49 - - - 23 4 4 4 Stage Dev

02 클러스터


ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Notifications
Inventory > Clusters
Clusters
CLUSTER
Search text here
Name
dev-testing
test
microservice
gke-cluster-dev
stage-testing
demo-cluster
dev-testing
Connected
OVERVIEW
MISCONFIGURATION
VULNERABILITY
ALERTS
COMPLIANCE
POLICIES
APP BEHAVIOUR
KIEM
Insights
Cluster Findings by Asset Type
Deployment 120
RuleBinding 120
ClusterRuleBin... 120
ConfigMap 120
Service 120
CronJob 120
Service Accounts
Findings by Asset Categories
Workloads
Configuration
Security & Identity
Resource Management
Critical
High
Medium
Low
Informational
Cluster Findings S
2,809
Critical
High
Cluster Findings
View all
Search by name
Severity C H M L
Last seen
Name
Count
Asset name
Tool Output
Namespace
12-09-2024 11:34:52 Non-root containers 1 kubearmor Failed default
12-09-2024 11:34:52 Network Mapping 2 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx
12-09-2024 11:34:52 List Kubernetes secrets 4 vault Failed nginx

03 결과



Issues > Findings

Search anything...

Acme Corp

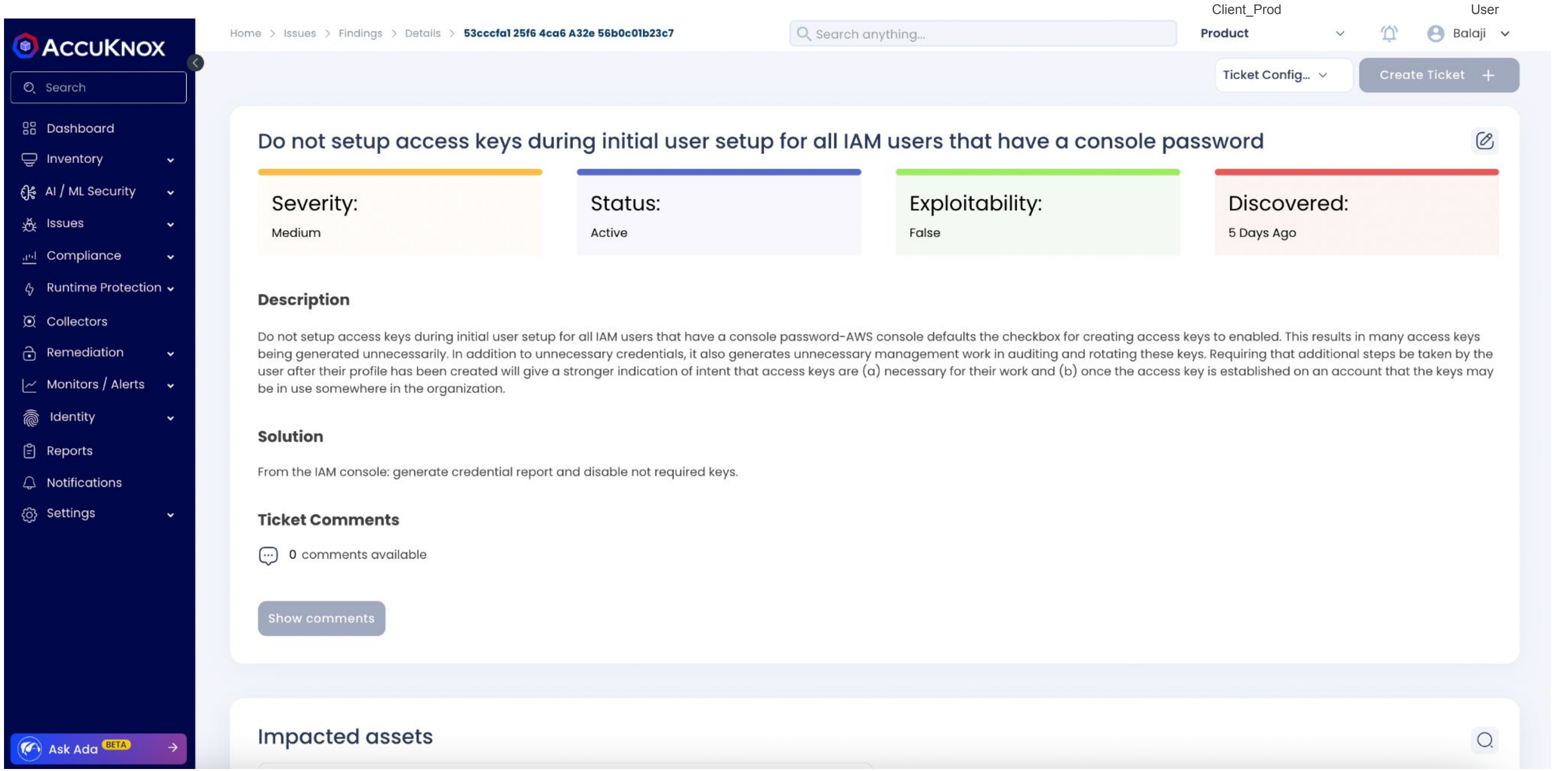
Thomas

CATEGORIES | ALL FINDINGS | RULE ENGINE

Search by category name

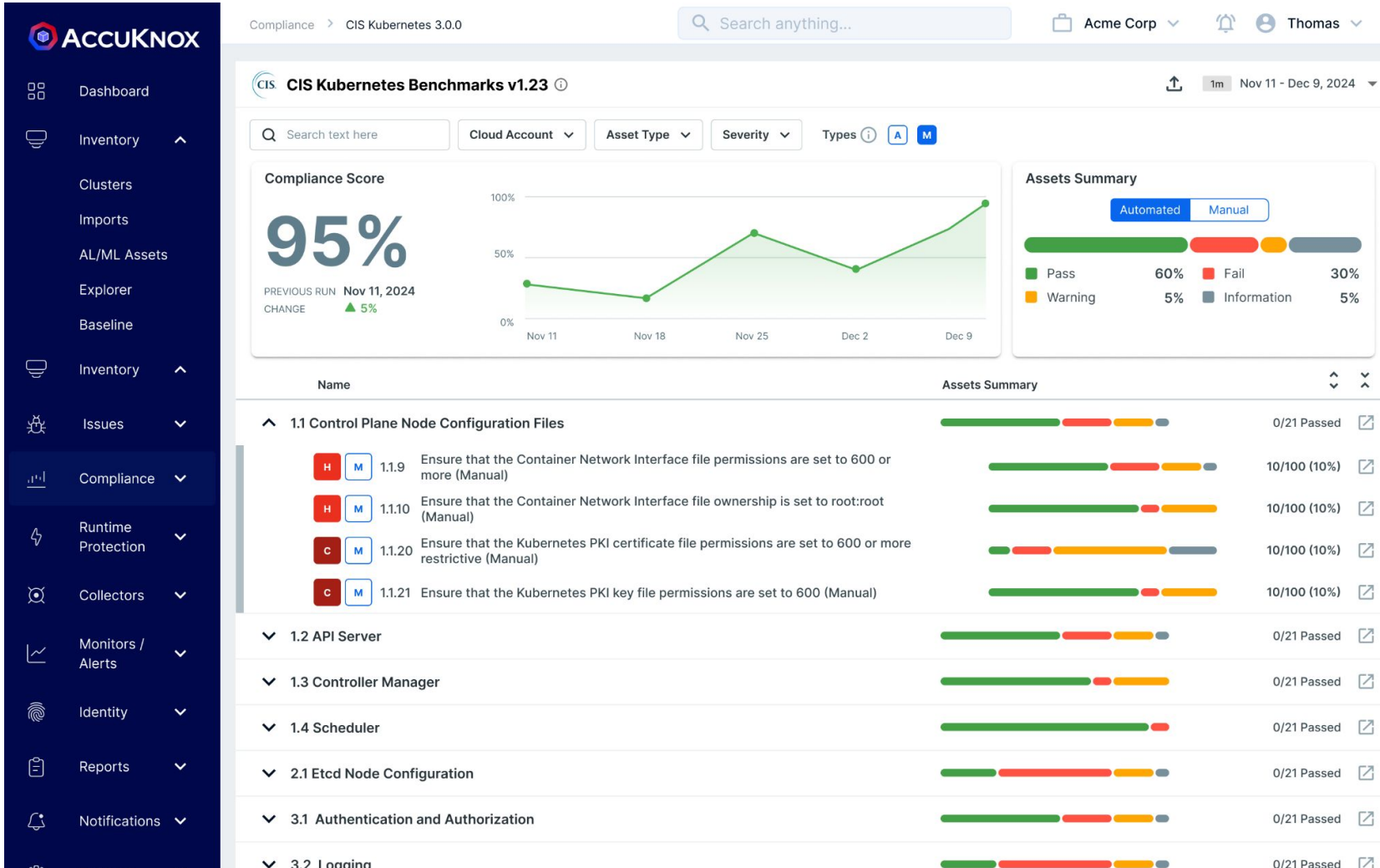
1 m Nov 23, 2024 - Dec 23, 2024

Category Name / Data Types	Findings	Affected Assets	Critical	High	Medium	Low
Cluster Findings	10k	5.5k	1,500	1,200	300	2,500
K8s Scan	100	500	200	100	100	100
KIEM	100	250	200	25	20	5
K8s CIS	100	250	200	25	20	5
Kubernetes Findings	12.5k	150	7,200	5,000	100	100
KIEM Findings	14.5k	150	75	75	75	75
Kubernetes Compliance	17.2k	150	75	75	75	75
Image Vulnerabilities	300	900	225	225	225	225
Secrets	20k	8.4k	7,400	500	250	250
Cloud Findings	30	675	75	300	200	100
Cloud Compliance	75	990	490	300	100	100
Code Findings-SAST	50	555	55	100	300	200
Application security-DAST	87.5k	650	300	300	25	25
IaC findings	80	2.2k	1,500	500	100	100
Code findings-SCA	30	150	100	30	10	10



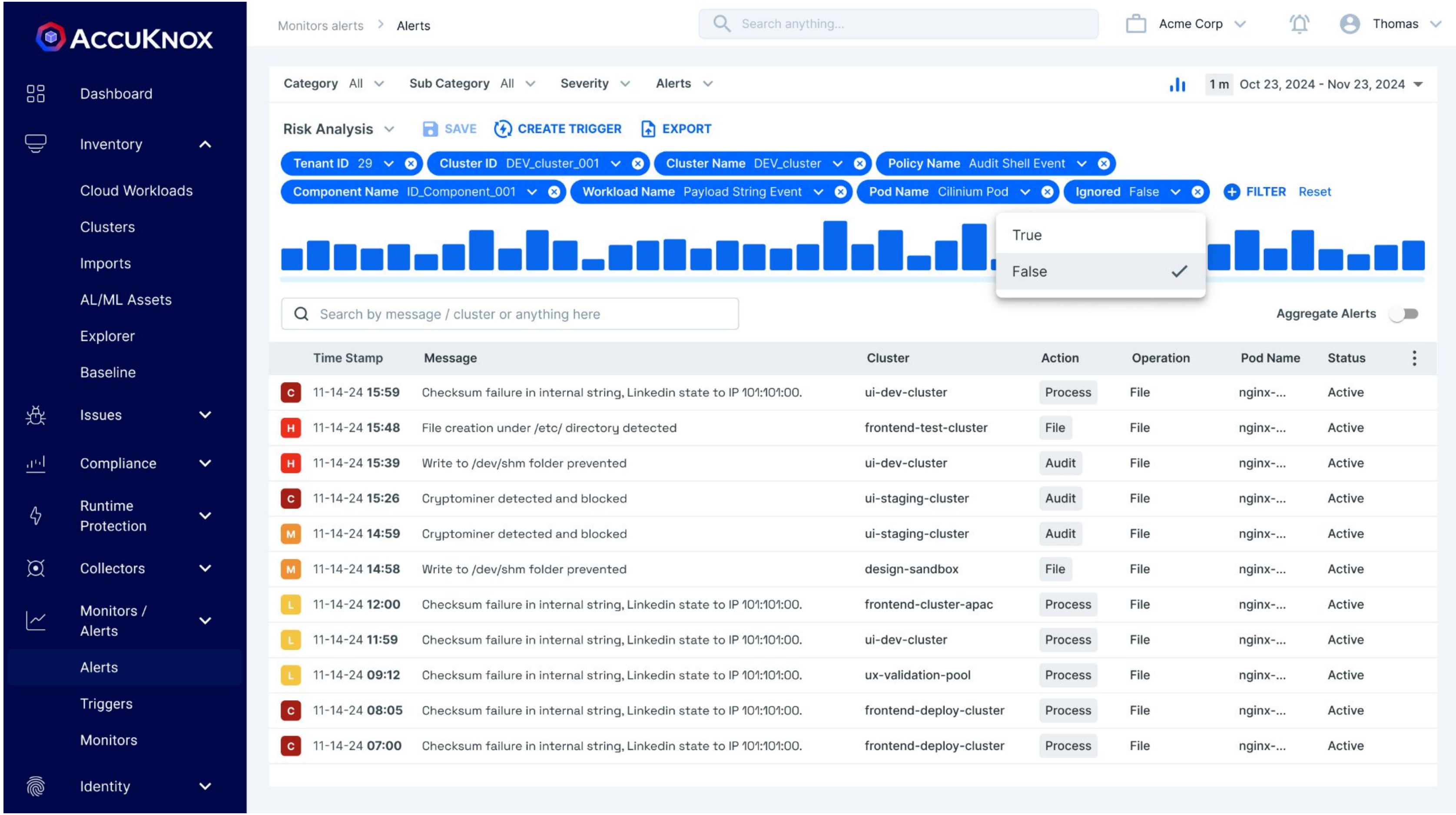
AccuKnox
Search
Dashboard
Inventory
AI / ML Security
Issues
Compliance
Runtime Protection
Collectors
Remediation
Monitors / Alerts
Identity
Reports
Notifications
Settings
Ask Ada BETA
Home > Issues > Findings > Details > 53cccfa1 25f6 4ca6 A32e 56b0c01b23c7
Search anything...
Client_Prod
Product
User
Balaji
Ticket Config...
Create Ticket
Do not setup access keys during initial user setup for all IAM users that have a console password
Severity:
Medium
Status:
Active
Exploitability:
False
Discovered:
5 Days Ago
Description
Do not setup access keys during initial user setup for all IAM users that have a console password-AWS console defaults the checkbox for creating access keys to enabled. This results in many access keys being generated unnecessarily. In addition to unnecessary credentials, it also generates unnecessary management work in auditing and rotating these keys. Requiring that additional steps be taken by the user after their profile has been created will give a stronger indication of intent that access keys are (a) necessary for their work and (b) once the access key is established on an account that the keys may be in use somewhere in the organization.
Solution
From the IAM console: generate credential report and disable not required keys.
Ticket Comments
0 comments available
Show comments
Impacted assets

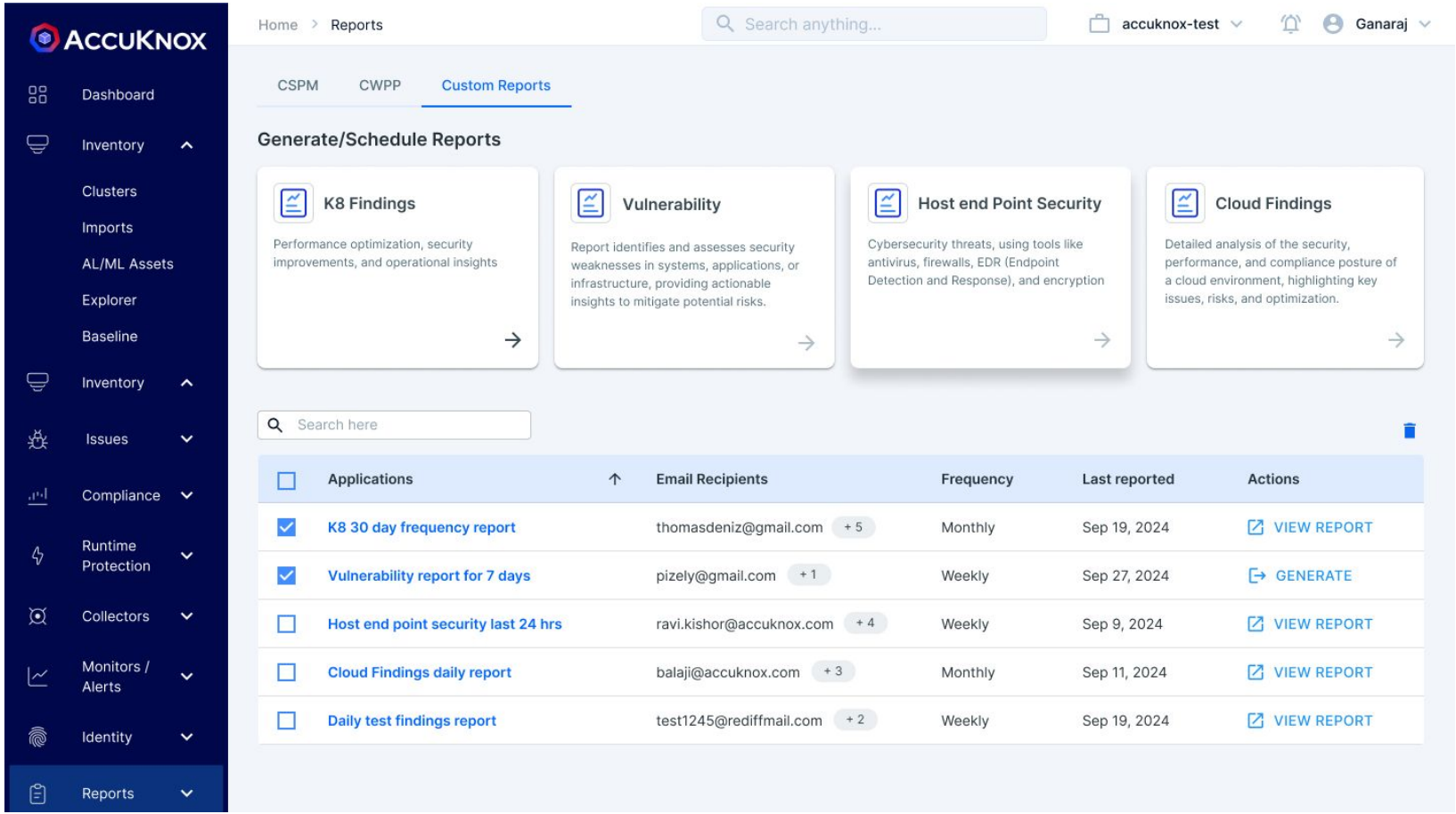
04 규정 준수


ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Notifications
Compliance > CIS Kubernetes 3.0.0
Search anything...
Acme Corp
Thomas
CIS Kubernetes Benchmarks v1.23
1m Nov 11 - Dec 9, 2024
Search text here
Cloud Account
Asset Type
Severity
Types A M
Compliance Score
95%
PREVIOUS RUN Nov 11, 2024
CHANGE ▲ 5%
100%
50%
0%
Nov 11
Nov 18
Nov 25
Dec 2
Dec 9
Assets Summary
Automated
Manual
Pass 60%
Fail 30%
Warning 5%
Information 5%
Name
Assets Summary
1.1 Control Plane Node Configuration Files 0/21 Passed
H M 1.1.9 Ensure that the Container Network Interface file permissions are set to 600 or more (Manual) 10/100 (10%)
H M 1.1.10 Ensure that the Container Network Interface file ownership is set to root:root (Manual) 10/100 (10%)
C M 1.1.20 Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive (Manual) 10/100 (10%)
C M 1.1.21 Ensure that the Kubernetes PKI key file permissions are set to 600 (Manual) 10/100 (10%)
1.2 API Server 0/21 Passed
1.3 Controller Manager 0/21 Passed
1.4 Scheduler 0/21 Passed
2.1 Etcd Node Configuration 0/21 Passed
3.1 Authentication and Authorization 0/21 Passed
3.2 Logging 0/21 Passed

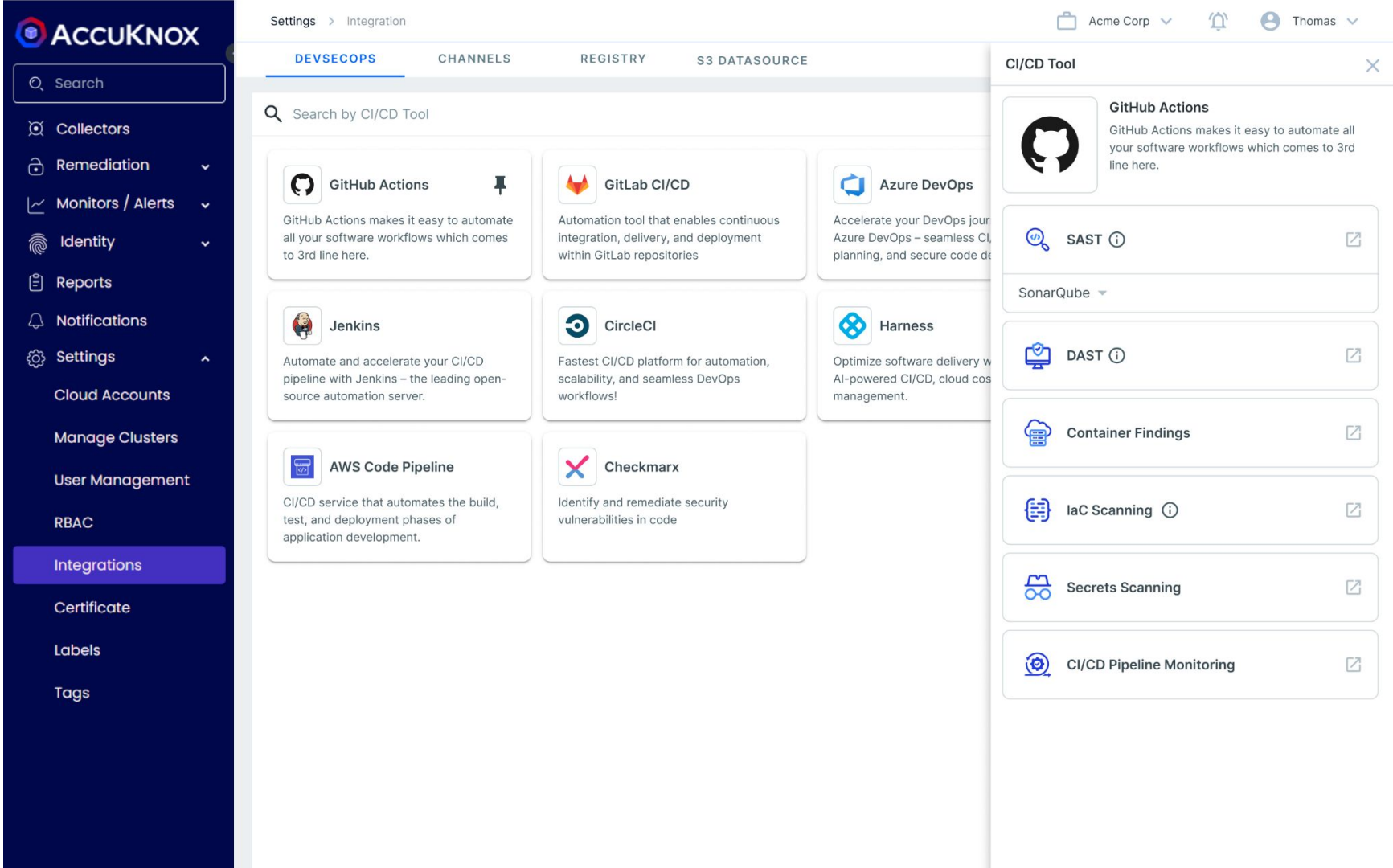
05

활용

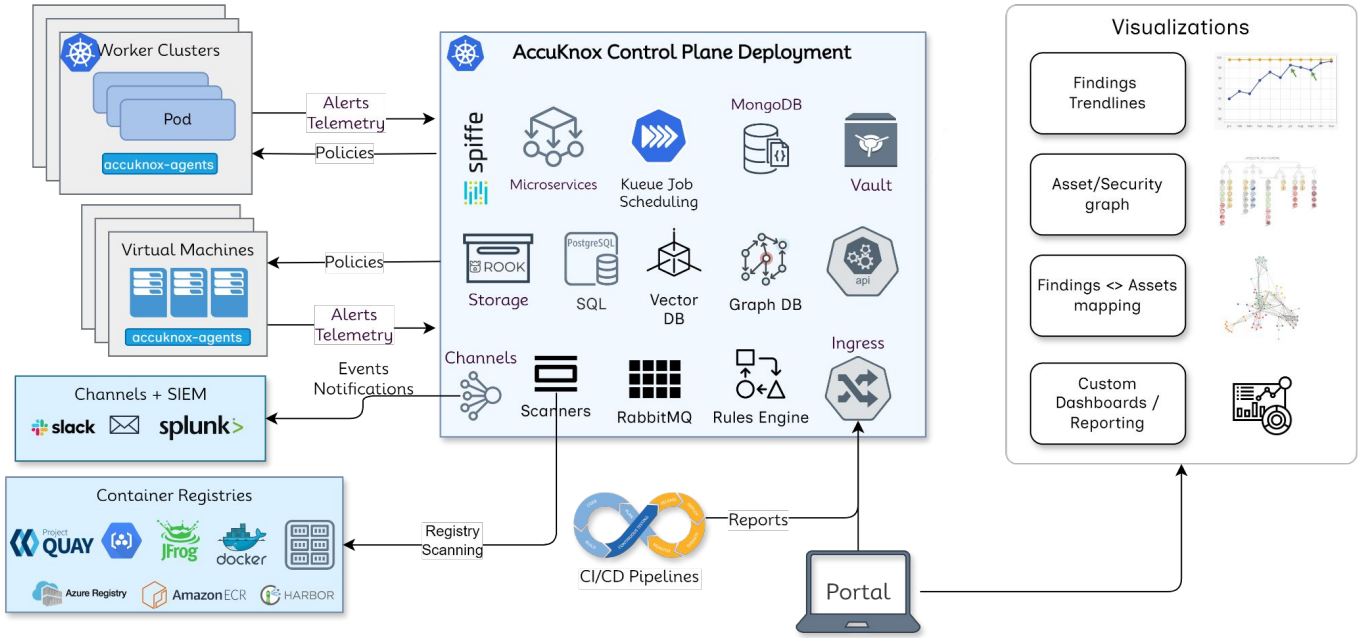

ACCUKNOX
Dashboard
Inventory
Cloud Workloads
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Alerts
Triggers
Monitors
Identity
Monitors alerts > Alerts
Search anything...
Acme Corp
Thomas
Category All
Sub Category All
Severity
Alerts
1 m
Oct 23, 2024 - Nov 23, 2024
Risk Analysis
SAVE
CREATE TRIGGER
EXPORT
Tenant ID 29
Cluster ID DEV_cluster_001
Cluster Name DEV_cluster
Policy Name Audit Shell Event
Component Name ID_Component_001
Workload Name Payload String Event
Pod Name Cilinium Pod
Ignored False
FILTER
Reset
True
False
Search by message / cluster or anything here
Aggregate Alerts
Time Stamp | Message | Cluster | Action | Operation | Pod Name | Status
C 11-14-24 15:59 Checksum failure in internal string, Linkedin state to IP 101:101:00. ui-dev-cluster Process File nginx-... Active
H 11-14-24 15:48 File creation under /etc/ directory detected frontend-test-cluster File File nginx-... Active
H 11-14-24 15:39 Write to /dev/shm folder prevented ui-dev-cluster Audit File nginx-... Active
C 11-14-24 15:26 Cryptominer detected and blocked ui-staging-cluster Audit File nginx-... Active
M 11-14-24 14:59 Cryptominer detected and blocked ui-staging-cluster Audit File nginx-... Active
M 11-14-24 14:58 Write to /dev/shm folder prevented design-sandbox File File nginx-... Active
L 11-14-24 12:00 Checksum failure in internal string, Linkedin state to IP 101:101:00. frontend-cluster-apac Process File nginx-... Active
L 11-14-24 11:59 Checksum failure in internal string, Linkedin state to IP 101:101:00. ui-dev-cluster Process File nginx-... Active
L 11-14-24 09:12 Checksum failure in internal string, Linkedin state to IP 101:101:00. ux-validation-pool Process File nginx-... Active
C 11-14-24 08:05 Checksum failure in internal string, Linkedin state to IP 101:101:00. frontend-deploy-cluster Process File nginx-... Active
C 11-14-24 07:00 Checksum failure in internal string, Linkedin state to IP 101:101:00. frontend-deploy-cluster Process File nginx-... Active


ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Home > Reports
Search anything...
accuknox-test
Ganaraj
CSPM
CWPP
Custom Reports
Generate/Schedule Reports
K8 Findings
Performance optimization, security improvements, and operational insights
Vulnerability
Report identifies and assesses security weaknesses in systems, applications, or infrastructure, providing actionable insights to mitigate potential risks.
Host end Point Security
Cybersecurity threats, using tools like antivirus, firewalls, EDR (Endpoint Detection and Response), and encryption
Cloud Findings
Detailed analysis of the security, performance, and compliance posture of a cloud environment, highlighting key issues, risks, and optimization.
Search here
Applications
Email Recipients
Frequency
Last reported
Actions
K8 30 day frequency report
thomasdeniz@gmail.com + 5
Monthly
Sep 19, 2024
VIEW REPORT
Vulnerability report for 7 days
pizely@gmail.com + 1
Weekly
Sep 27, 2024
GENERATE
Host end point security last 24 hrs
ravi.kishor@accuknox.com + 4
Weekly
Sep 9, 2024
VIEW REPORT
Cloud Findings daily report
balaji@accuknox.com + 3
Monthly
Sep 11, 2024
VIEW REPORT
Daily test findings report
test1245@rediffmail.com + 2
Weekly
Sep 19, 2024
VIEW REPORT

07 DevSecOps 통합



아키텍처 및 배포 모델



4가지 유형의 배포 모델:

1. 고객의 온프레미스(VM, 베어 메탈)
2. 고객의 에어갭 인프라
3. 고객 호스팅 퍼블릭 및 프라이빗 클라우드
4. AccuKnox의 호스팅 SaaS

https://help.accuknox.com/getting-started/deployment-models/

ACCUKNOX

통합 매트릭스

50세 이상

통합

accuknox.com/통합

ACCUKNOX

업계 인정

AccuKnox

nationalgrid partners

AccuKnox에 투자한 주요 이유 →

CLOUD SECURITY LIST

AccuKnox는 악명 높게 과로하고 자원이 부족한 클라우드 보안 엔지니어를 돕습니다. →

THENEWSTACK

AccuKnox의 독특한 런타임 보안 차별화는 업계 베테랑들에 의해 강조되었습니다. →

Intellyx

Intellyx Brain Candy 간략 소개: AccuKnox는 컨테이너 보안 분야에서 독보적인 위치를 차지하고 있습니다. →

Medium

AccuKnox의 투자자인 Raghuram은 Nat과 Phil이 만나 비전을 공유했을 때 마법이 일어나는 것은 불가피했다고 말했습니다. →

NUTANIX

AccuKnox를 2024년 AI 파트너 프로그램으로 발표 →

aws

AWS, AccuKnox의 Zero Trust CNAPP와의 파트너십 발표 →

LF EDGE

AccuKnox, Open Horizon 프로젝트 파트너로 mimik Technologies, IBM에 합류 →

aiTechPark

Connecting Insights with Individuals

쿠버네티스 보안 플랫폼 AccuKnox, 460만 달러 투자 유치 →

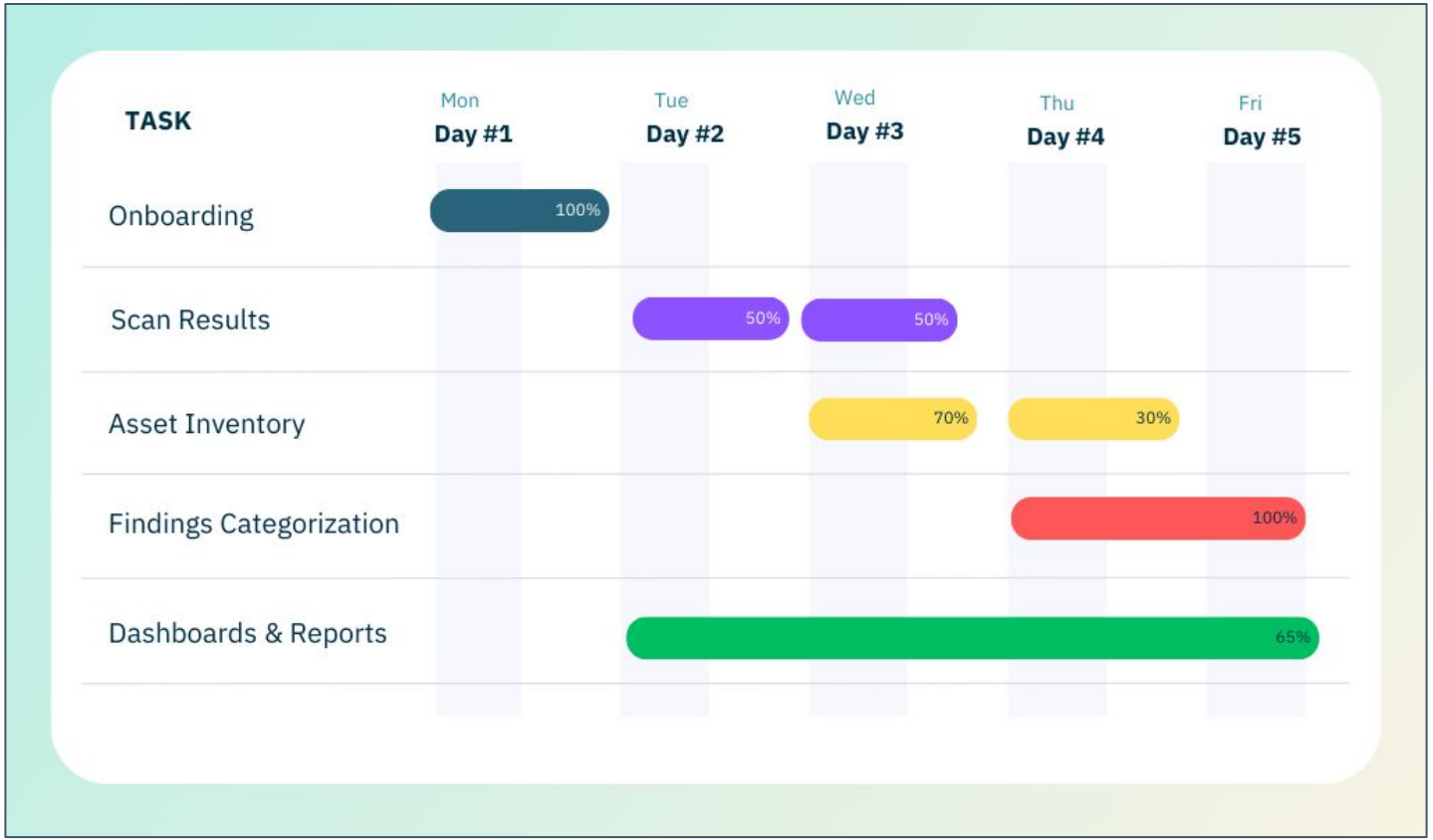
Red Hat

AccuKnox는 RHEL 운영 체제 보안에 의해 검증 및 검증되었습니다. →

sjultra

SJULTRA와 AccuKnox가 협력하여 기업에 CNAPP를 제공합니다. →

POC 타임라인


TASK
Mon
Day #1
Tue
Day #2
Wed
Day #3
Thu
Day #4
Fri
Day #5
Onboarding
100%
Scan Results
50%
50%
Asset Inventory
70%
30%
Findings Categorization
100%
Dashboards & Reports
65%

요약

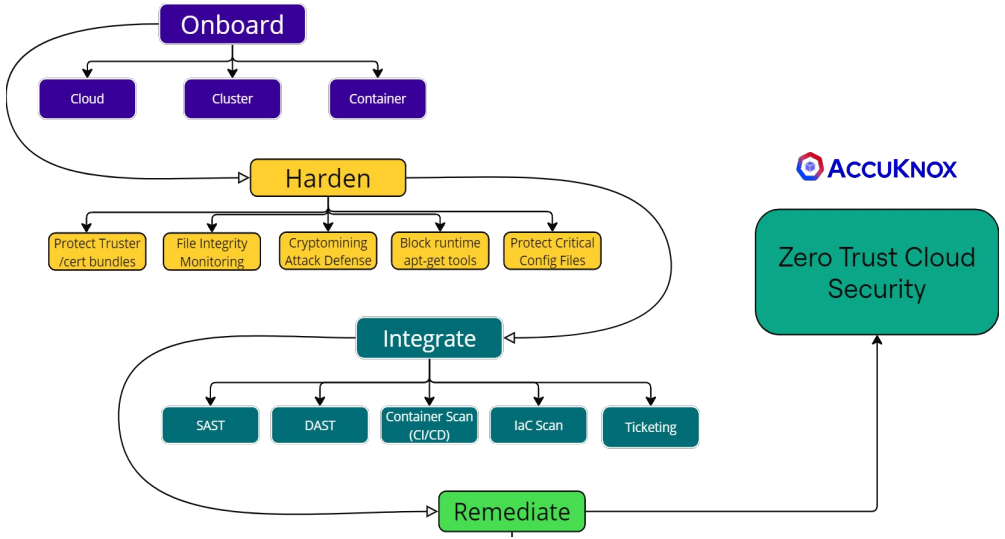
POC 실행: 1단계: 자산 재고(온보딩)

2단계: 위험 평가 발견

3단계: 수행

위험 기반 우선순위 지정

4단계: 개선(정책, 티켓팅)



aws Available in AWS Marketplace

Red Hat Marketplace Operated by IBM

Now available on Microsoft Azure MARKETPLACE

ORACLE Cloud Marketplace

accuknox.com/마켓플레이스

Get AccuKnox CNAPP Demo

ACCUKNOX

AccuKnox

우리의 활동을 직접 확인하세요

support@accuknox.com

인증됨