AccuKnox

Secure Code to Cognition™

Zasilany sztuczną inteligencją

Zero zaufania CNAPP

Rated 4.5/5

Rated 4.3/5

Certified & Accredited by

As Featured In

Available On

Zarys

AccuKnox

Platformizacja

AccuKnox

ASPM (AppSec)

- Testowanie bezpieczeństwa aplikacji statycznych (SAST)
- Dynamiczne testowanie bezpieczeństwa aplikacji (DAST)
- Tajne skany
- Skanowanie IaC
- Wykaz materiałów oprogramowania (SBOM)
- Analiza składu oprogramowania (SCA)

CSPM (CloudSec)

- Widoczność zasobów i zapasów w chmurze
- Wykrywanie i usuwanie dryfu
- Egzekwowanie polityki Zero Trust
- Zgodność i audyt Wskaźniki odniesienia

CWPP (WorkloadSec)

- Ocena postawy najmniej pobłażliwej
- Menedżer zabezpieczeń tajemnic
- Wymuszanie kontenerów i maszyn wirtualnych
- Wykrywanie zagrożeń w czasie wykonywania

KSPM (KubernetesSec)

- Wykrywanie błędnej konfiguracji klastra
- Wyniki testów porównawczych CIS K8s
- Zarządzanie tożsamością i uprawnieniami K8s (KIEM)
- Monitorowanie bezpieczeństwa kontenerów i sieci

AI-SPM (AI Security)

- Wykrywanie i reagowanie na sztuczną inteligencję (AI-DR)
- Natychmiastowa zapora sieciowa
- Bezpieczeństwo aplikacji AI Runtime
- Bezpieczeństwo modeli i zbiorów danych
- LLM Red Teaming
- Zgodność ze sztuczną inteligencją

Wsparcie na całej platformie

Zgodność
Ponad 35 struktur: SOC2, PCI DSS itp.

CDR
Wykrywanie i reagowanie na chmury

Bezpieczeństwo API

Drugi pilot AI

SIEM
Informacje dotyczące bezpieczeństwa

Wyzwania... Rozwiązania...

AccuKnox

Wyzwania

❌ Wszystkie zaawansowane ataki są atakami w czasie wykonywania

❌ Różne narzędzia do AppSec, CloudSec i AISec

❌ Rozłączne narzędzia do zabezpieczeń lokalnych i chmurowych

Uderzenie

→ Narażenie na ataki typu Zero Day

→ Zwiększona powierzchnia ataku

→ ~ 100% wyższe koszty (narzędzi, ludzi)

Rozwiązanie AccuKnox – CNAPP z zerowym zaufaniem

✓ Wdrażaj we wszystkich chmurach publicznych i prywatnych

✓ Zabezpiecz wszystkie zasoby (K8, VM, API, Edge)

✓ Zintegrowane zabezpieczenia aplikacji, chmury i sztucznej inteligencji

✓ >50% oszczędności

Rozwiązanie AccuKnox Code to Cognition

AppSec ← → CloudSec CNAPP [Platforma ochrony aplikacji w chmurze] ← → API Sec ← → AISec

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

CHMURA PUBLICZNA: aws

PRYWATNA CHMURA

EDGE / IoT: ARM

SIEM – Kompleksowa analiza zagrożeń

Ask AI – Interfejs konwersacyjny – DevSecOps spotyka ChatGPT

Compliance – Obsługa ponad 35 standardów

CTEM – Ciągłe zarządzanie narażeniem na zagrożenia

Sukcesy klientów | Studia przypadków

ACCUKNOX

PRUDENT
THE FUTURE OF INSURANCE

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

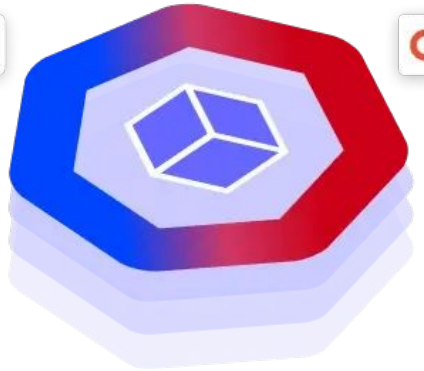
PRUDENT
THE FUTURE OF INSURANCE

SONESTA
INTERNATIONAL HOTELS

SupportLogic

G Rated 4.5/5

G2 Rated 4.3/5



Wspominać - accuknox.com/case-studies

AccuKnox
Secure Code to Cognition

Jeden skonsolidowany CNAPP

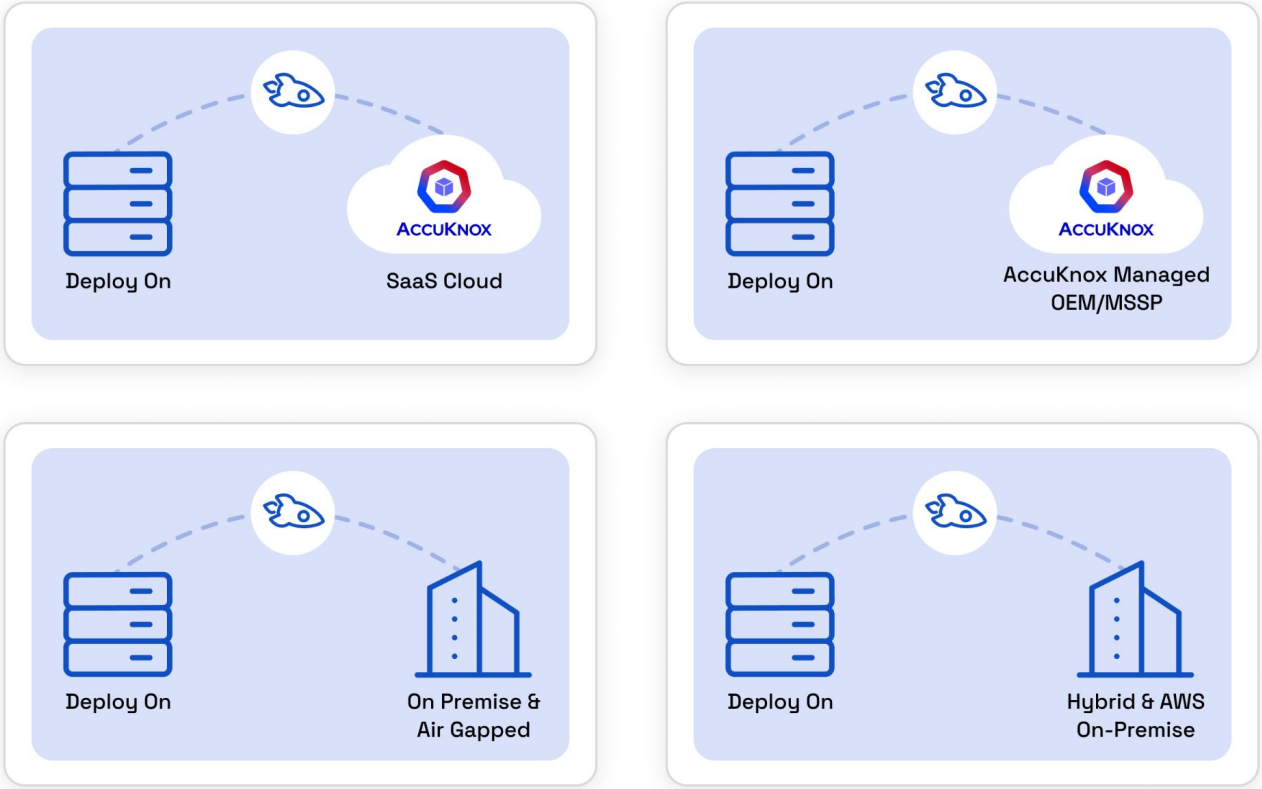
DevSecOps, drugi pilot AI

ASPM | CSPM | AI-SPM | KSPM | CWPP | GRC | Bezpieczeństwo środowiska wykonawczego

INTEGRACJE z SIEM, SOAR, EDR, platformami biletowymi

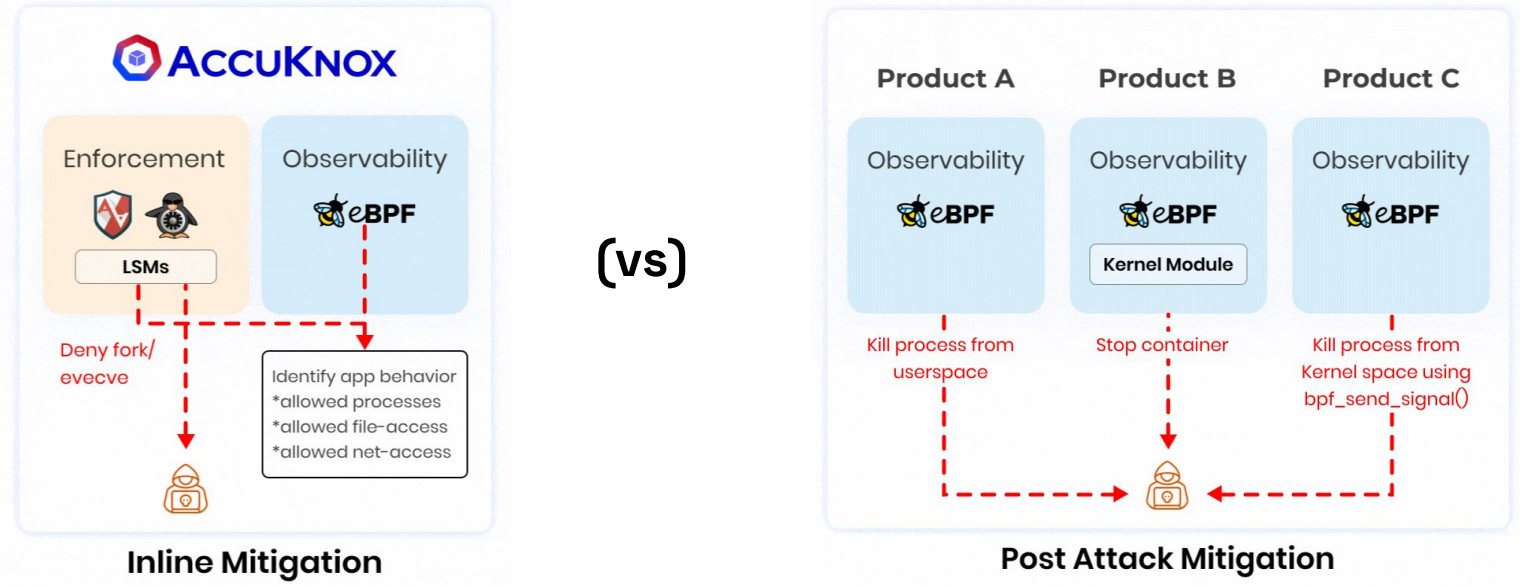
SIEM

Elastyczne modele wdrażania



Unikalne zróżnicowanie

AccuKnox może „obserwować” >>
„wymuszać” podczas ataku >> automatycznie generować „zasady” >



*** Bronimy się przed atakami typu Zero Day w czasie rzeczywistym!**

Matryca wsparcia

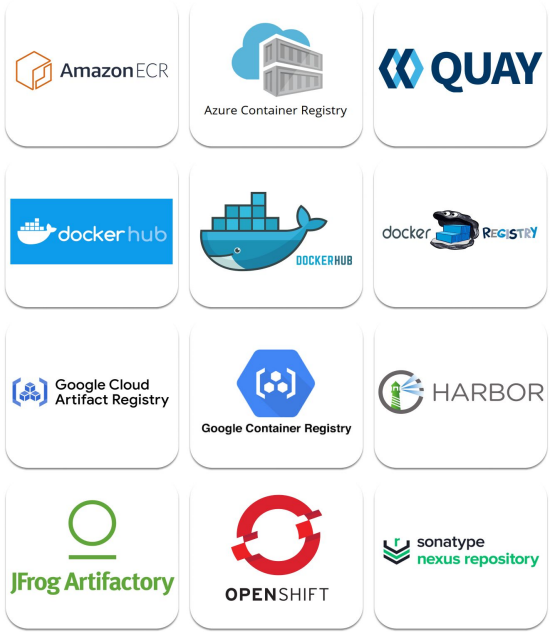
ACCUKNOX

1) Chmury

2) Klastry (lokalne, maszyny wirtualne)

**Systemy operacyjne oparte na Linuksie*

3) Rejestry kontenerów



Unikalne zróżnicowanie

AccuKnox

- → Jedna platforma - kompleksowe pokrycie od Code → Cloud
- → Automatyczne zasady Zero Trust - do naprawy w trybie inline
- → Elastyczne wdrażanie - Chmura publiczna i prywatna
- → Platforma SOAR - z ponad 50 integracjami od razu po wyjęciu z pudełka

Chmura

- Panel wykonawczy CSPM
- Wykrywanie błędnej konfiguracji
- Ocena zapasów
- Ciągła zgodność
- Linia bazowa do wykrywania dryfu

Kod

- Analiza kodu statycznego
- Analiza składu oprogramowania
- Tajne skanowanie
- Integracja CI/CD z cyklem kompilacji
- Zarządzanie podatnościami

Obraz

- Ocena ryzyka wizerunkowego
- Skanowanie podatności
- Priorytetyzacja oparta na ryzyku
- Zgodność i raportowanie
- Integracja CI/CD
- Zarządzanie podatnościami

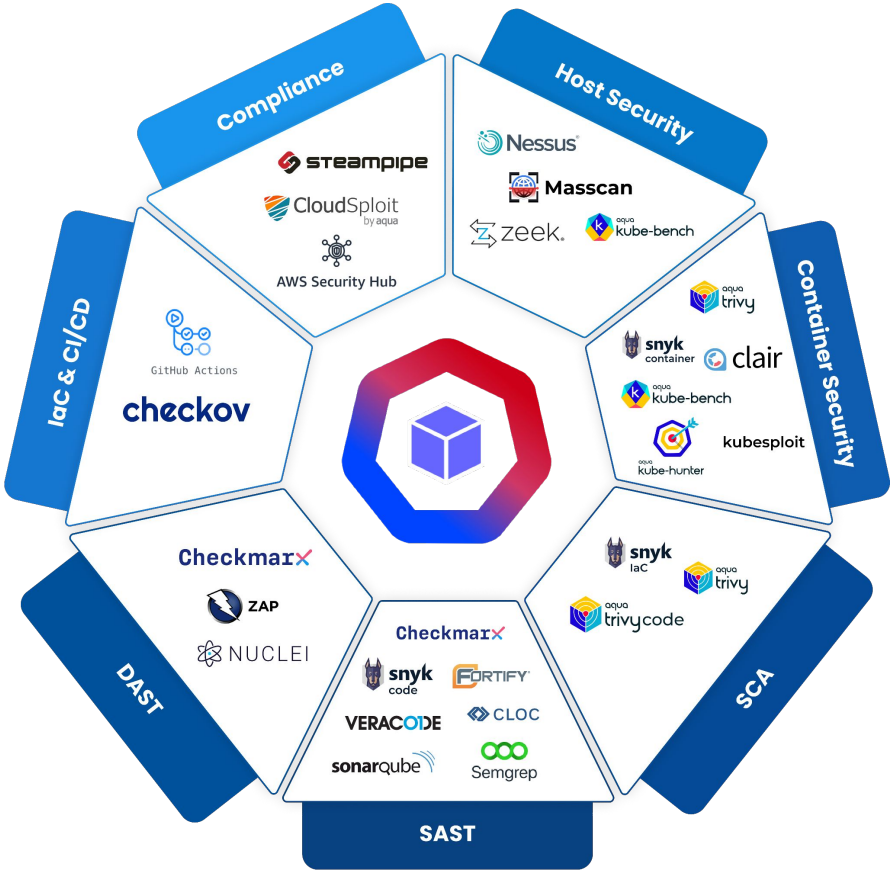
Obszar bezpieczeństwa	Funkcja
Obserwowalność	Obserwowalność obciążenia pracą
Zgodność	Zasady wzmacniania obciążenia pracą
Monitorowanie	Rejestry i alerty
Zero zaufania	Automatycznie odkryto politykę Zero Trust Niestandardowa polityka zerowego zaufania Naprawa w trybie inline Mikrosegmentacja sieci
Nowe funkcje	Wsparcie kontrolera przyjęć KIEM (Zarządzanie tożsamościami i uprawnieniami K8s) Wsparcie ECS/EKS Fargate

Narzędzia obsługiwane od razu po wyjęciu z pudełka!

AccuKnox

Przesuń w lewo i zabezpiecz w prawo

1. Bezpieczeństwo gospodarza
2. Bezpieczeństwo kontenera
3. Zgodność
4. Skanowanie IaC i CI/CD
5. SAST
6. DAST
7. SCA



DevSecOps z AccuKnox

AccuKnox

Luki w zabezpieczeniach kontenerów

SAST

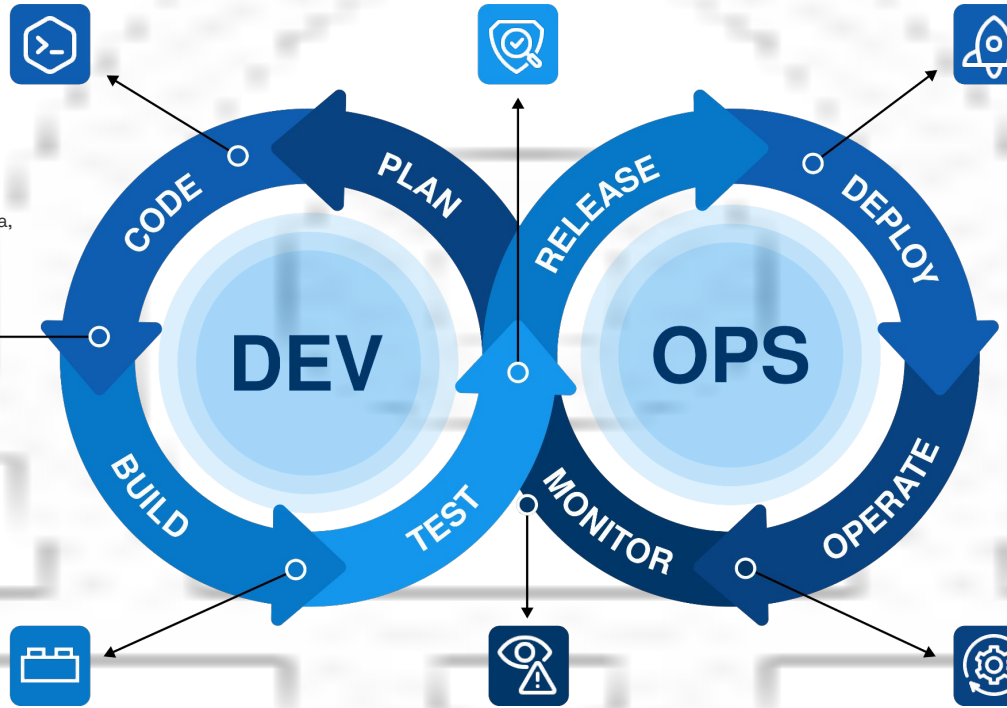
- Sprawdź kod źródłowy aplikacji lub kod bajtowy pod kątem niebezpiecznych konstrukcji.
- Proaktywne skanowanie, gdy aplikacja nie jest uruchomiona, dostęp wewnętrzny.

SCA

- Sprawdź kod źródłowy aplikacji lub kod bajtowy pod kątem niebezpiecznych konstrukcji.
- Proaktywne skanowanie, gdy aplikacja nie jest uruchomiona, dostęp wewnętrzny.

IaC

- Dostarczanie infrastruktury (tworzenie, modyfikowanie i usuwanie infrastruktury IaC)
- Zarządzanie konfiguracją (wyraźny stan infrastruktury za pomocą kodu/API) [KICS, Tfsec, Checkov]



Aplikacja MONITORUJ, ALARMUJ, KONTROLUJ, BLOKUJ, REJESTRUJ

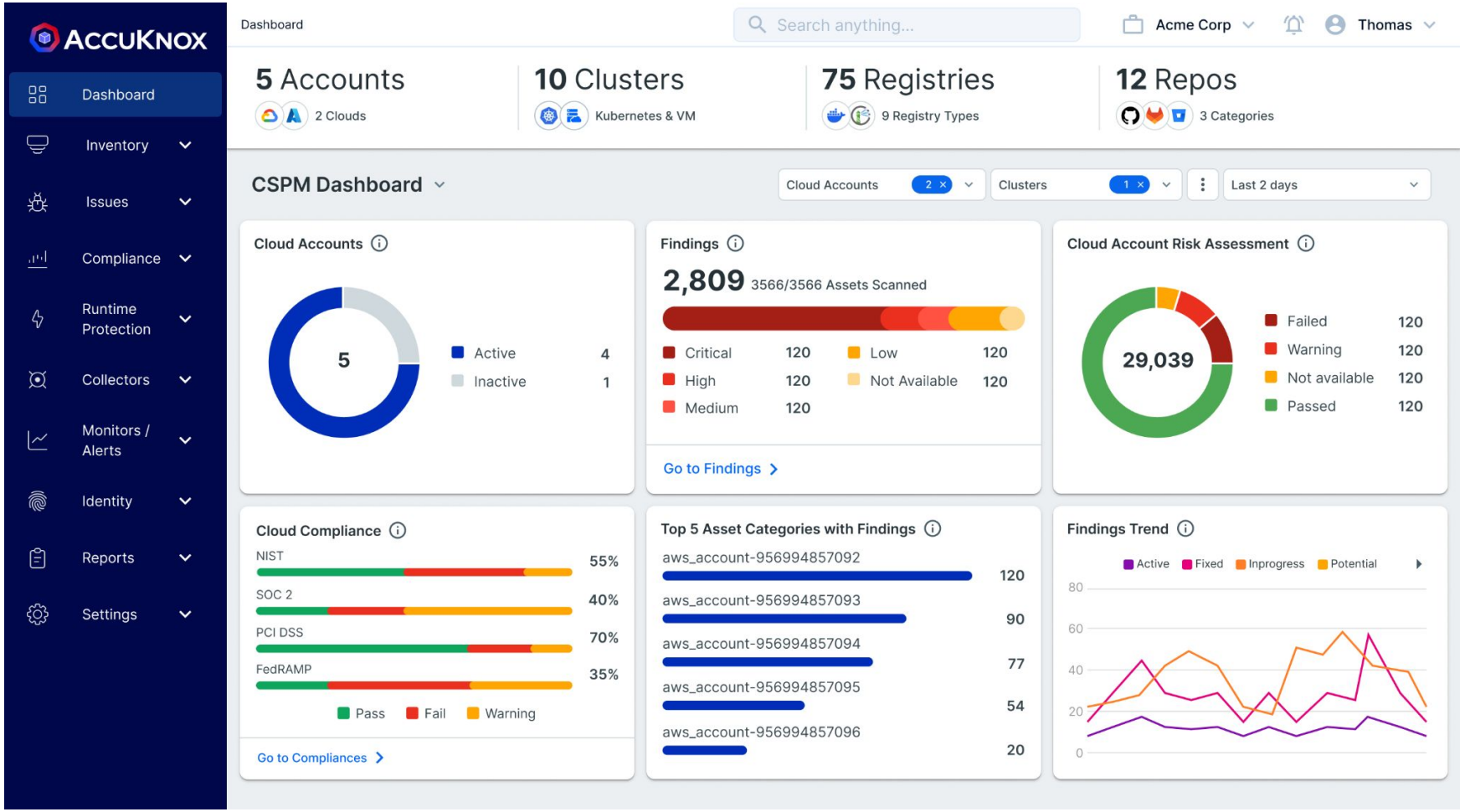
DAST

- Automatyczne i ciągłe skanowanie, które wywołuje złośliwe żądania http do interfejsu użytkownika i interfejsu API, obejmuje szeroki zakres ataków.
- Proaktywne skanowanie podczas działania aplikacji, wykrywanie dostępu z zewnątrz.

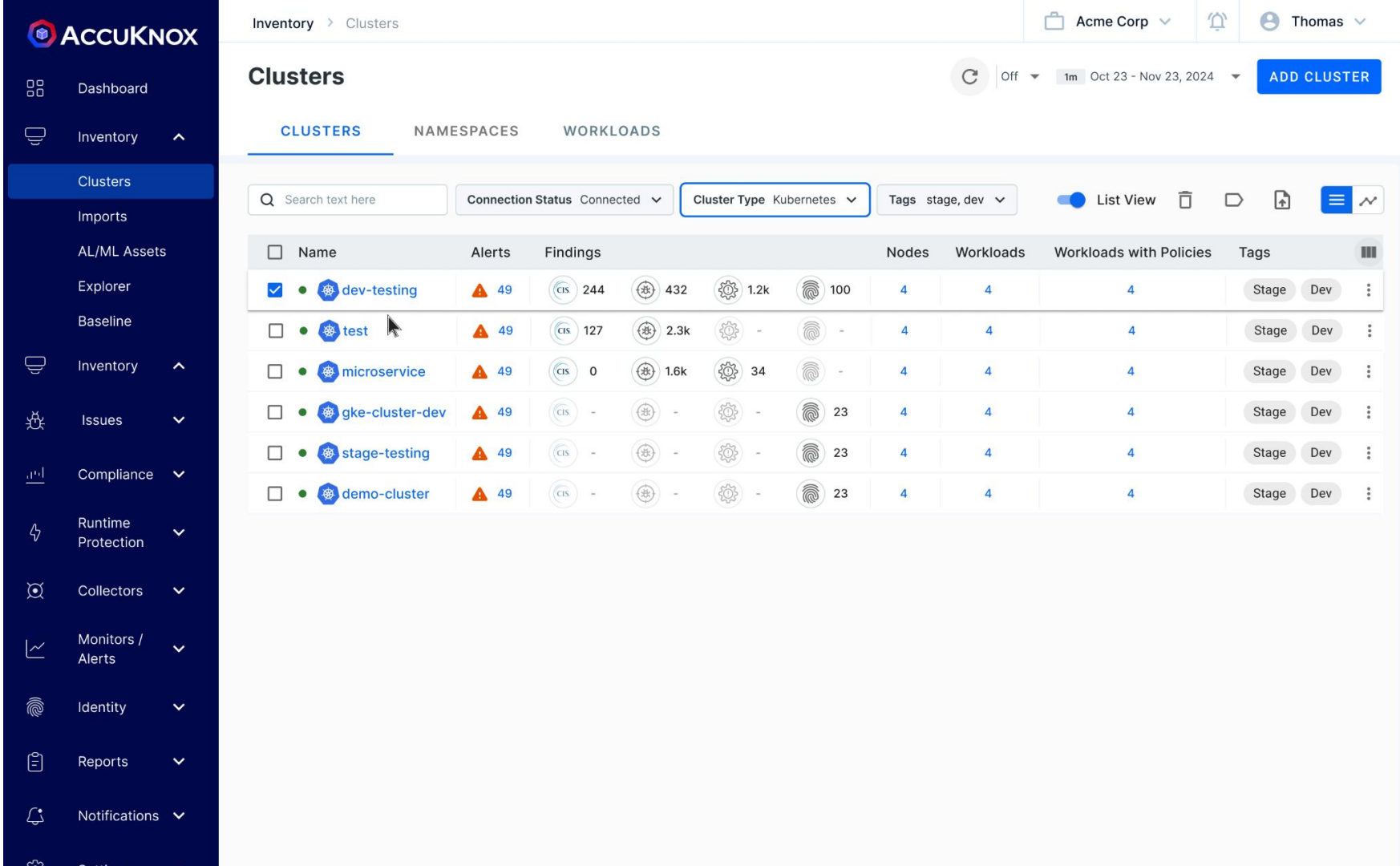
IAST

- Podłączają się pasywnie do działającej aplikacji i uruchamiają się po wykryciu bodźca.
- Skanowanie reaktywne, gdy aplikacja jest uruchomiona, dostęp wewnętrzny.

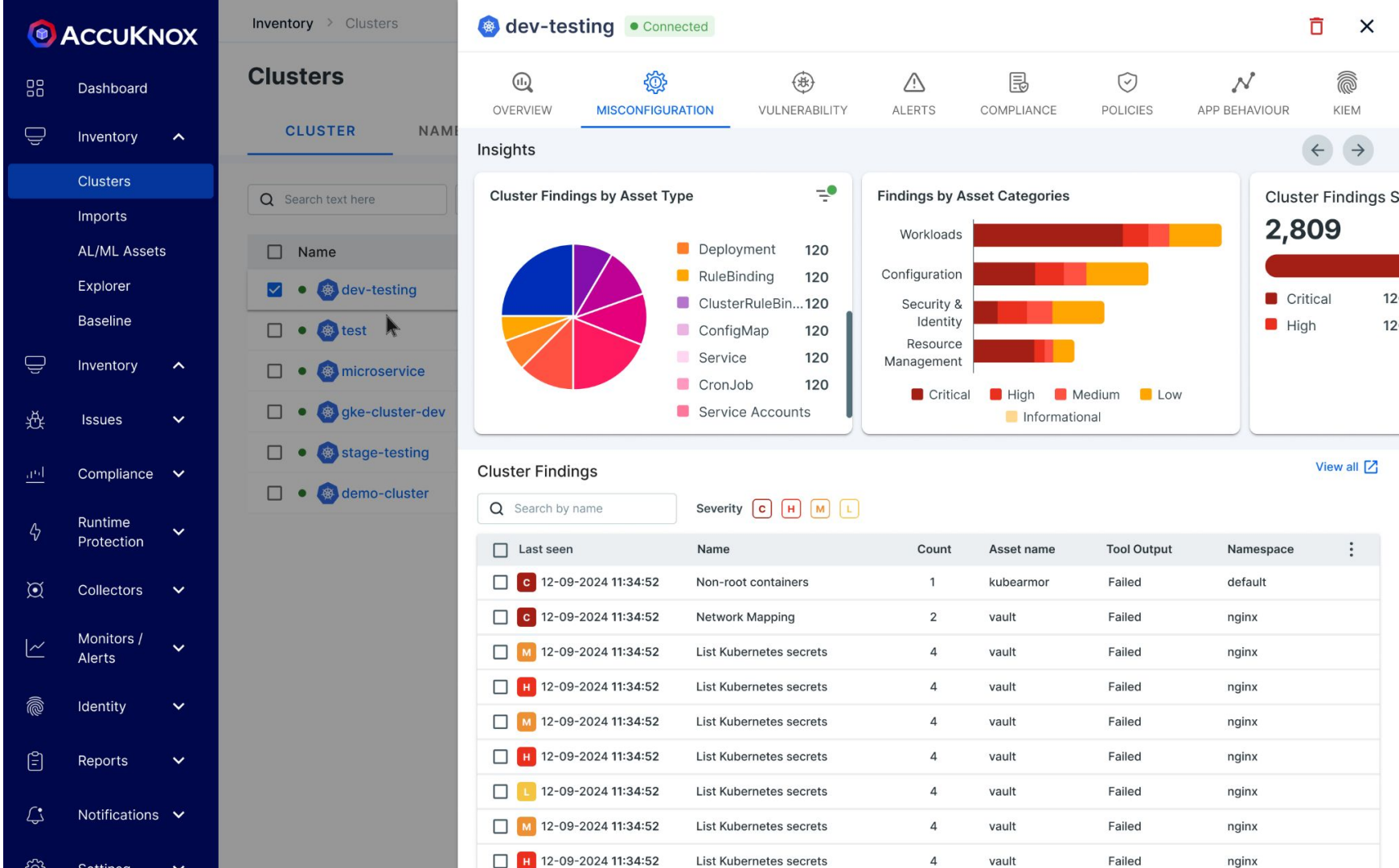
01 Panel


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
High 120
Medium 120
Low 120
Not Available 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

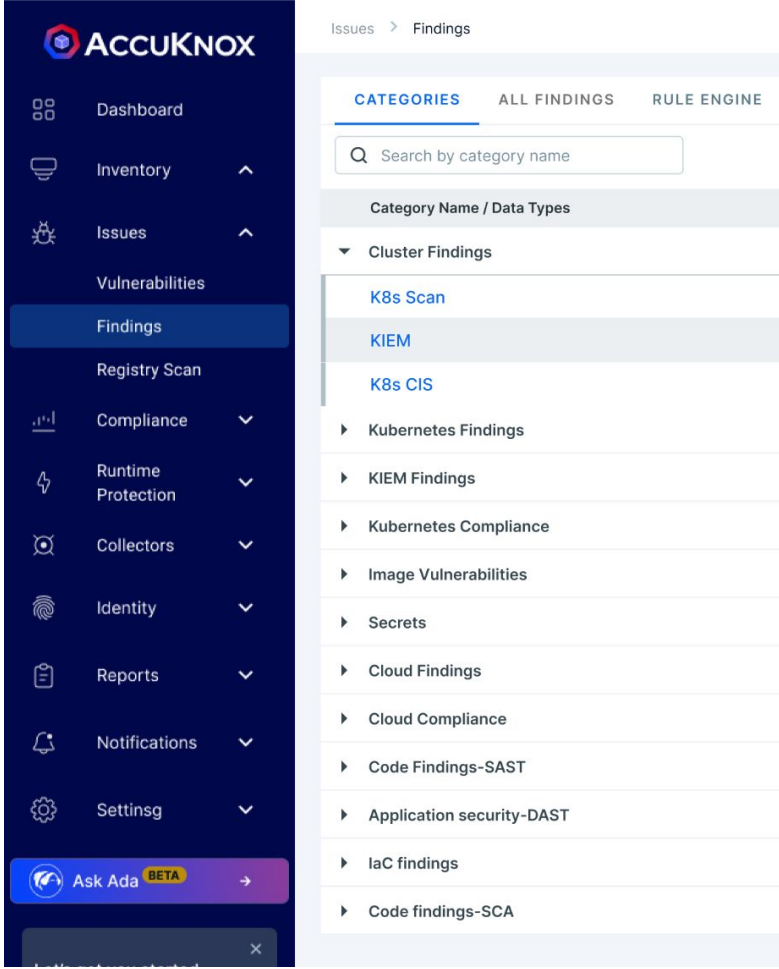
02 Klastry


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 Klastry

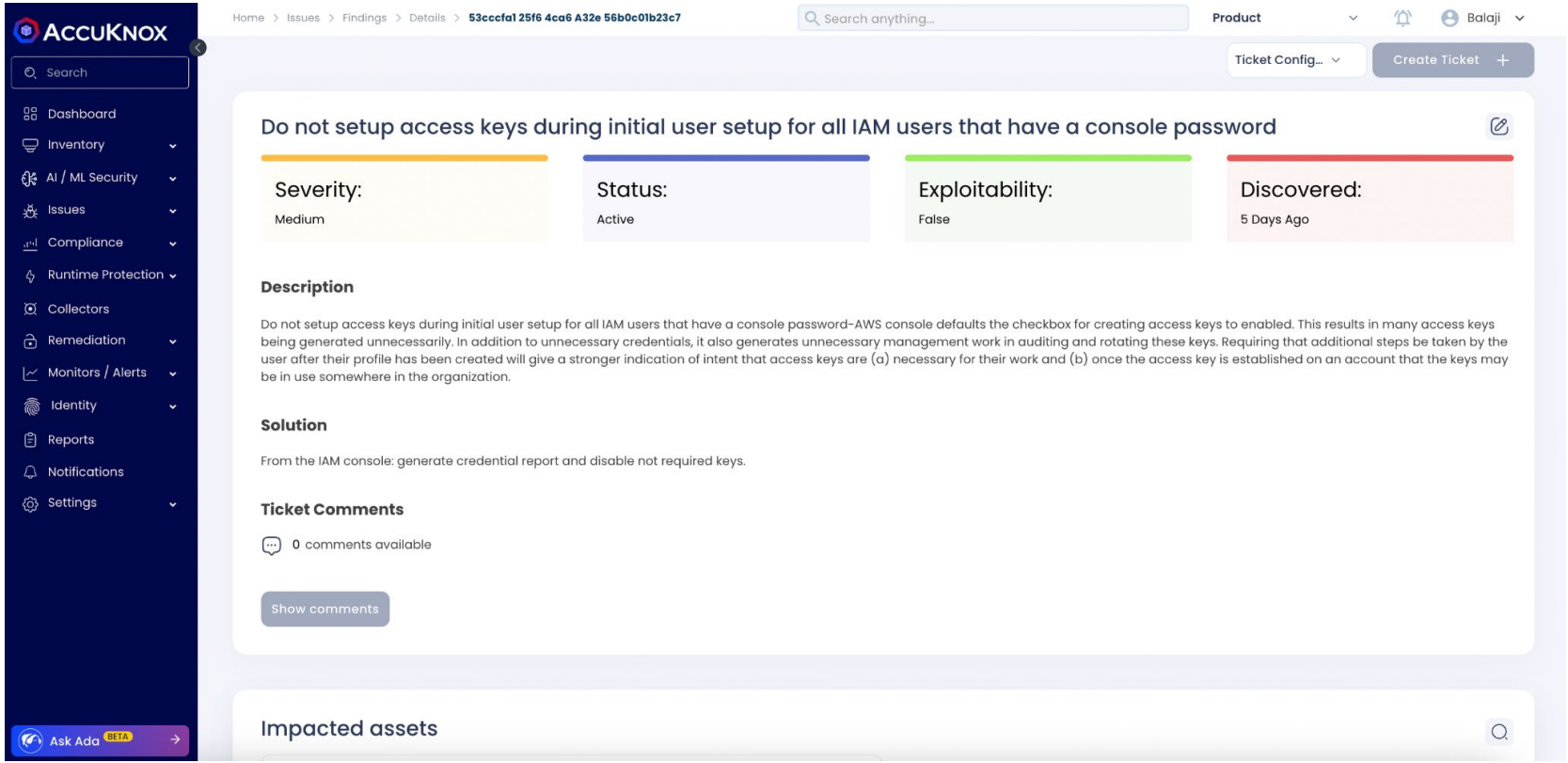

ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Notifications
Inventory > Clusters
Clusters
CLUSTER
Search text here
Name
dev-testing
test
microservice
gke-cluster-dev
stage-testing
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 Ustalenia

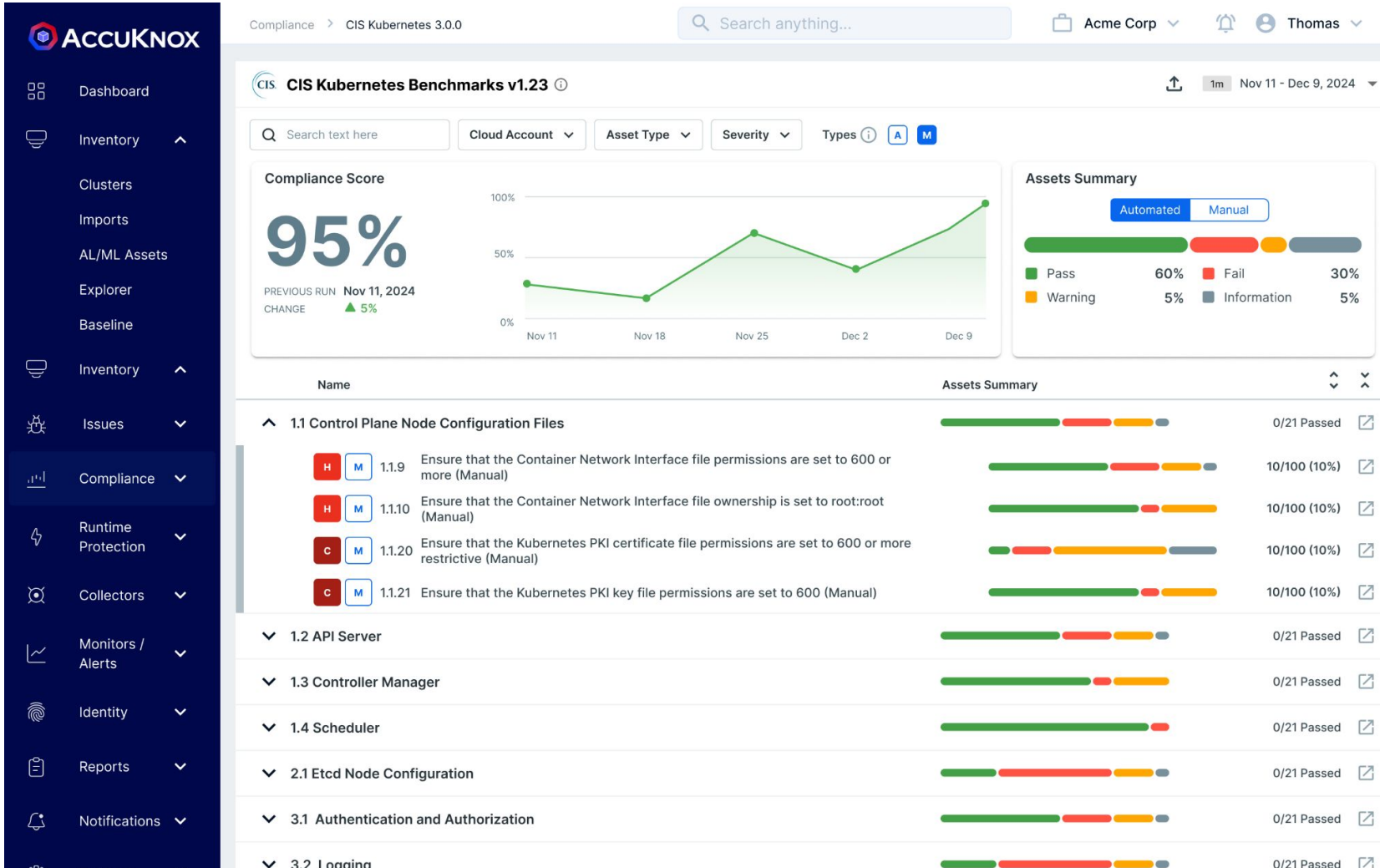


Category Name / Data Types	Findings	Affected Assets	Critical	High	Medium	Low
Cluster Findings	10k	5.5k	1,500	1,200	300	2,500
K8s Scan	100	500	200	100	100	100
KIEM	100	250	200	25	20	5
K8s CIS	100	250	200	25	20	5
Kubernetes Findings	12.5k	150	7,200	5,000	100	100
KIEM Findings	14.5k	150	75	75	75	75
Kubernetes 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

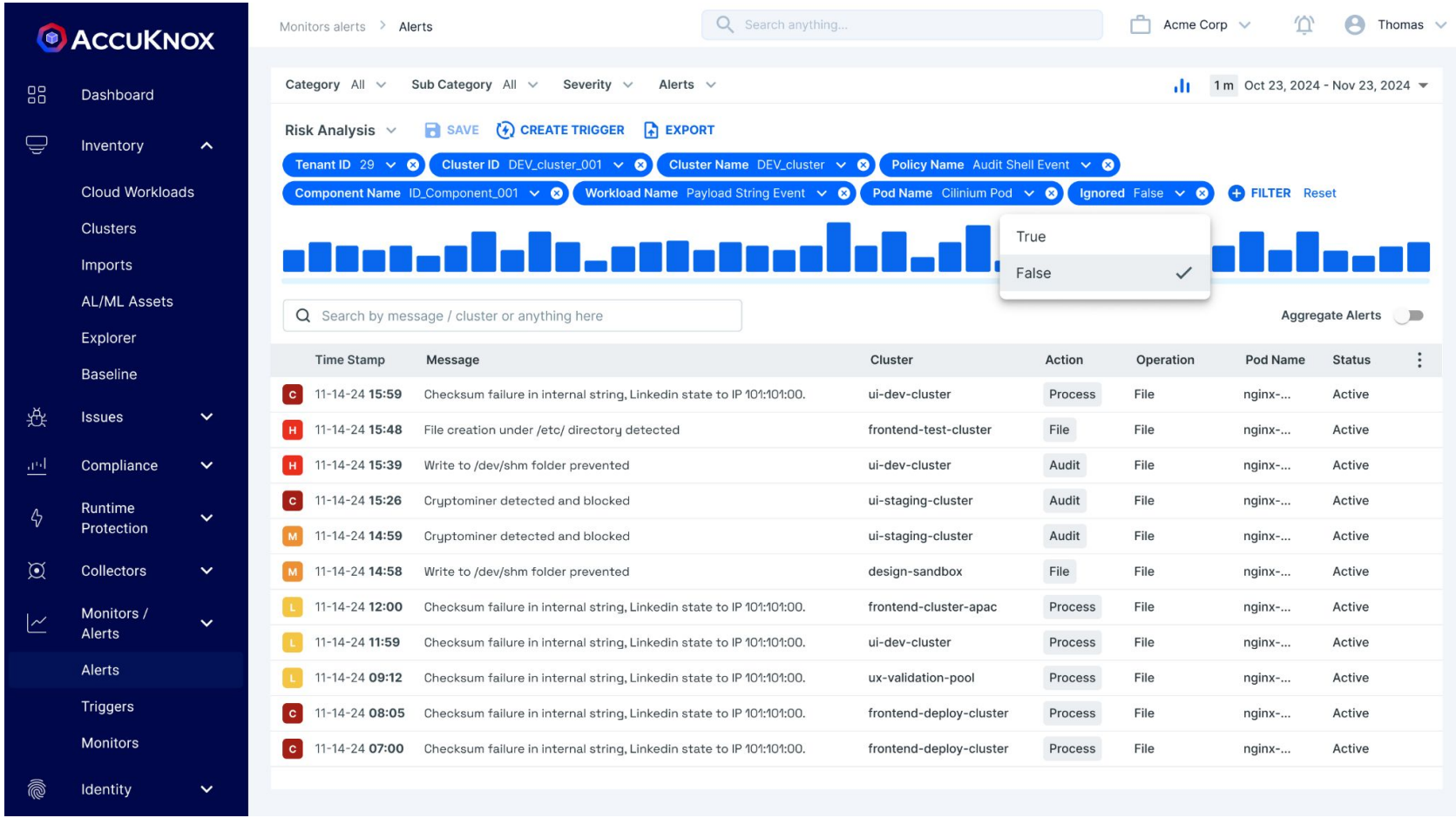
03 Ustalenia



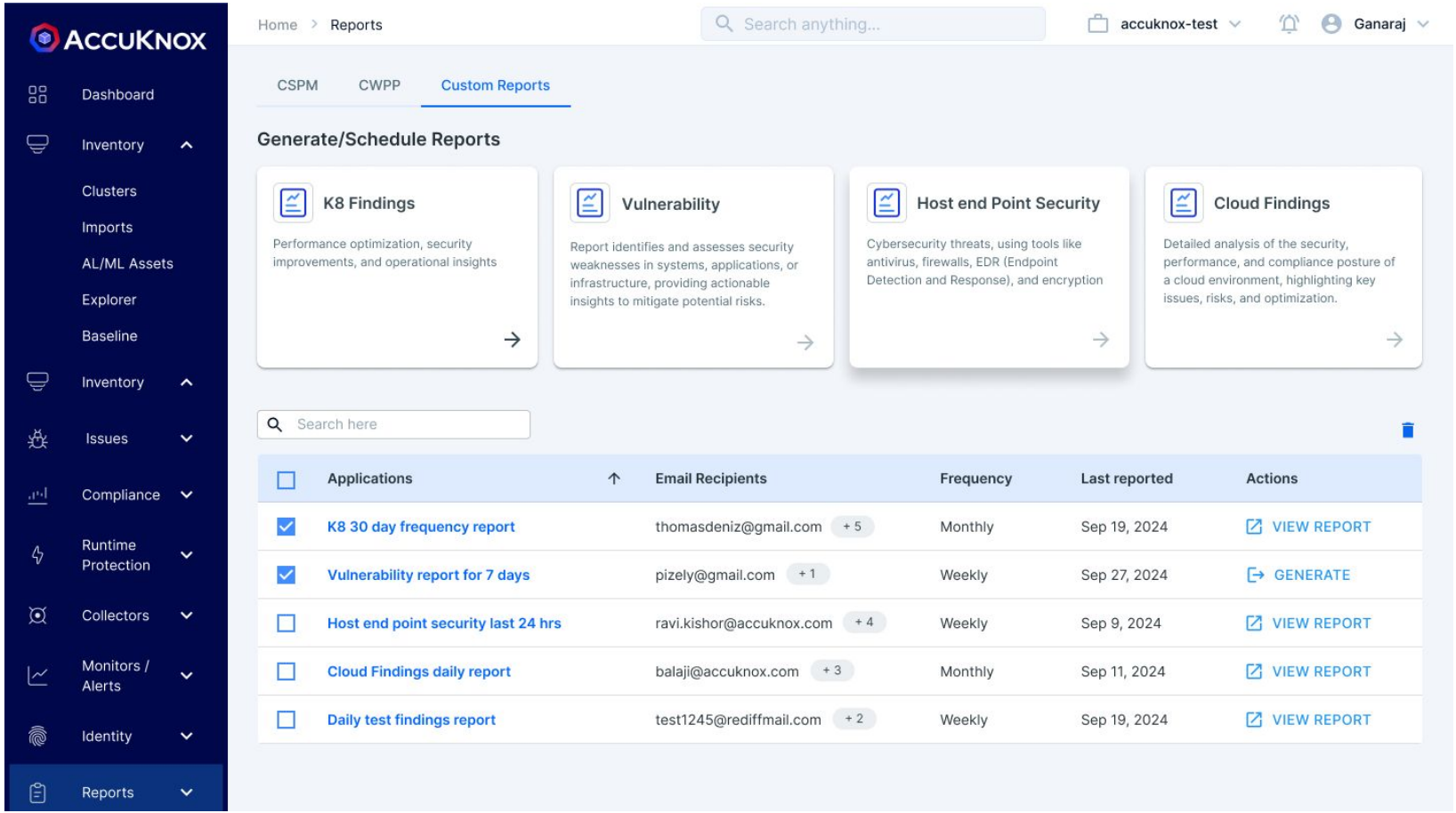
04 Zgodność


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

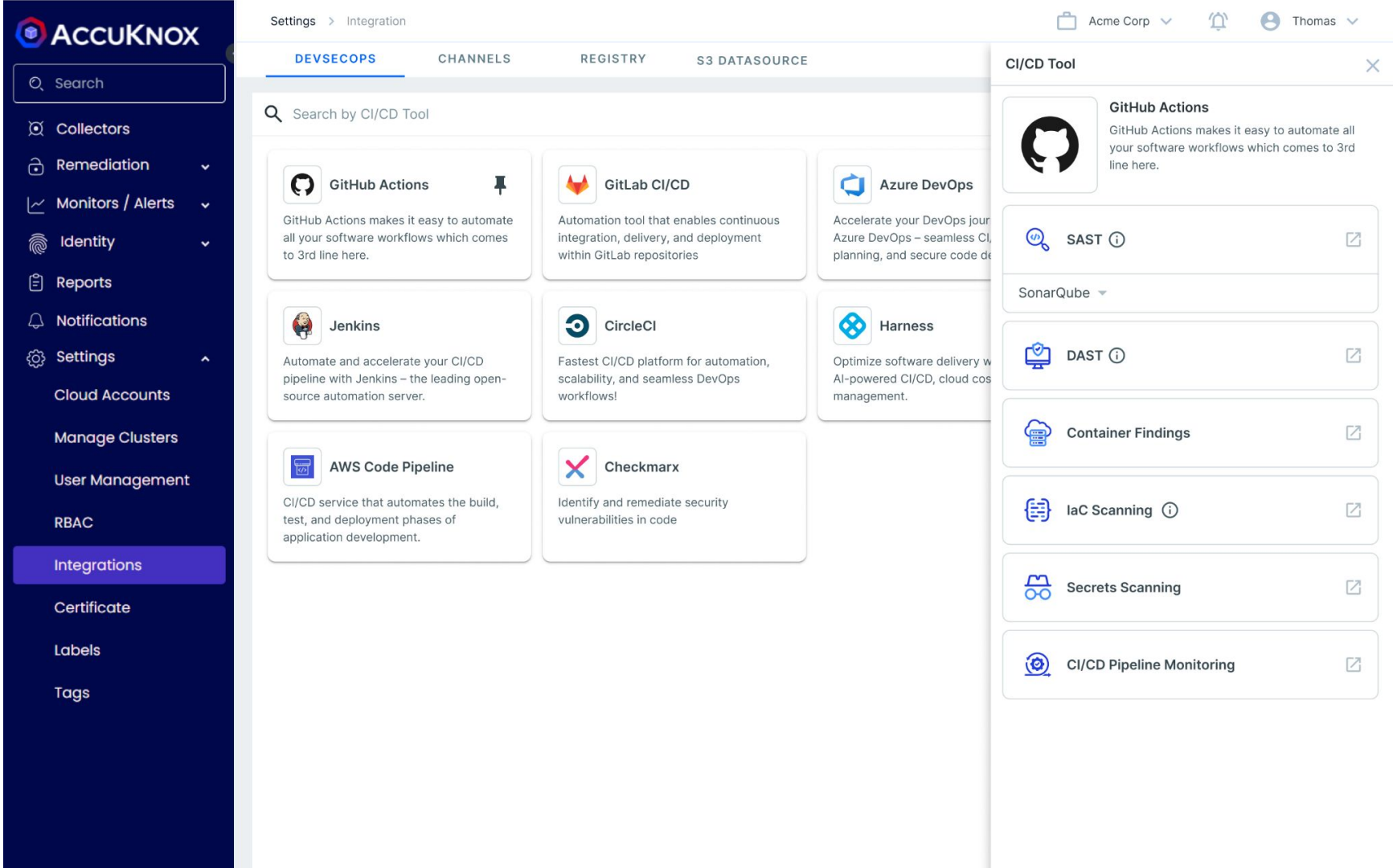
05 Alerty


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

06 Raporty

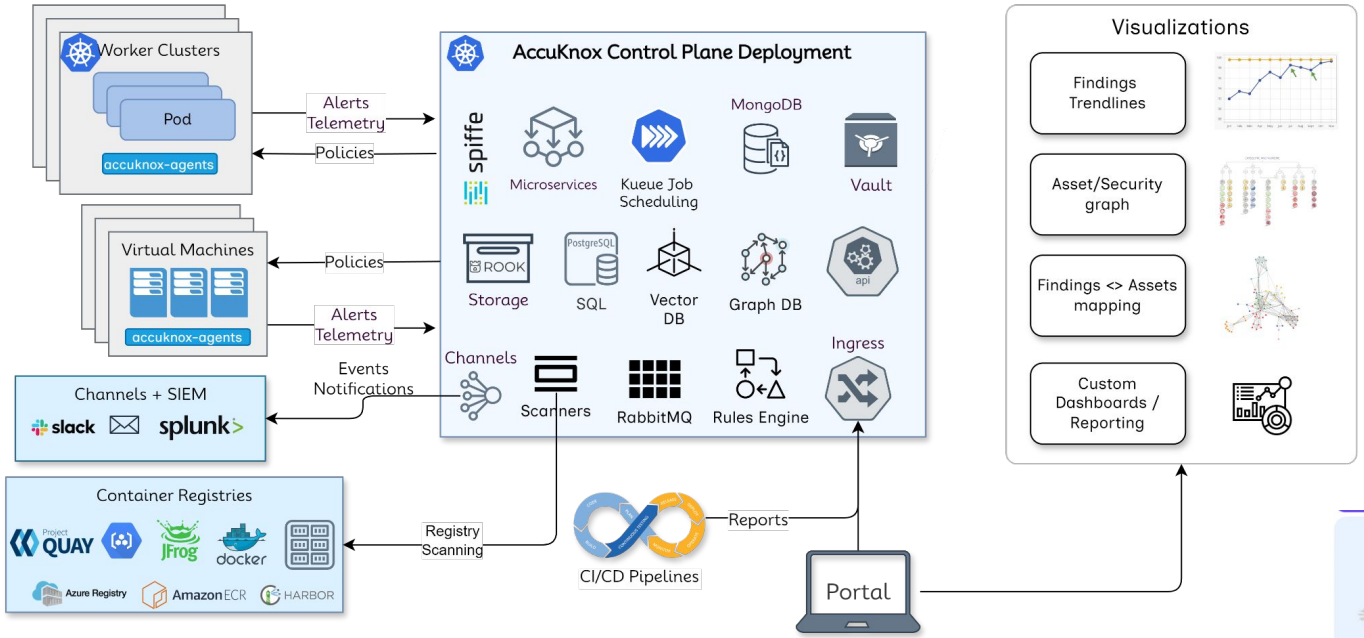

ACCUKNOX
Dashboard
Inventory
Clusters
Imports
AL/ML Assets
Explorer
Baseline
Inventory
Issues
Compliance
Runtime Protection
Collectors
Monitors / Alerts
Identity
Reports
Home > Reports
Search anything...
accuknox-test
Ganaraj
CSPM
CWPP
Custom Reports
Generate/Schedule Reports
K8 Findings
Performance 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 Integracja DevSecOps



Architektura i modele wdrażania

ACCUKNOX



4 typy modeli wdrażania:

1. Lokalnie u klienta (maszyny wirtualne, serwery)
2. Infrastruktura klienta z izolacją powietrzną
3. Publiczna i prywatna chmura hostowana przez klienta
4. Hostowana usługa SaaS firmy AccuKnox

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

Macierz integracji

50+

Integracje

accuknox.com/integrations

Wyróżnienia branżowe

AccuKnox

nationalgrid partners

Najważniejsze powody, dla których zainwestowaliśmy w AccuKnox →

CLOUD SECURITY LIST

AccuKnox pomaga inżynierom bezpieczeństwa w chmurze, którzy są znani z przepracowania i niedoboru zasobów →

THENEWSTACK

Weterani branży podkreślali wyjątkową różnicę w zabezpieczeniach środowiska wykonawczego AccuKnox →

Intellyx

Krótki opis Intellyx Brain Candy: AccuKnox wyróżnia się w branży zabezpieczeń kontenerów →

Medium

Nieuniknione było, że gdy Nat i Phil spotkali się i podzielili swoimi wizjami, wydarzy się coś magicznego – mówi Raghuram, inwestor w AccuKnox →

NUTANIX

Ogłasza, że AccuKnox jest jego programem partnerskim AI na rok 2024 →

aws

AWS ogłasza partnerstwo z programem Zero Trust CNAPP firmy AccuKnox →

LF EDGE

AccuKnox dołącza do mimik Technologies i IBM jako partner projektu Open Horizon →

aiTechPark
Connecting Insights with Individuals

Platforma bezpieczeństwa Kubernetes AccuKnox zabezpiecza 4,6 mln dolarów →

Red Hat

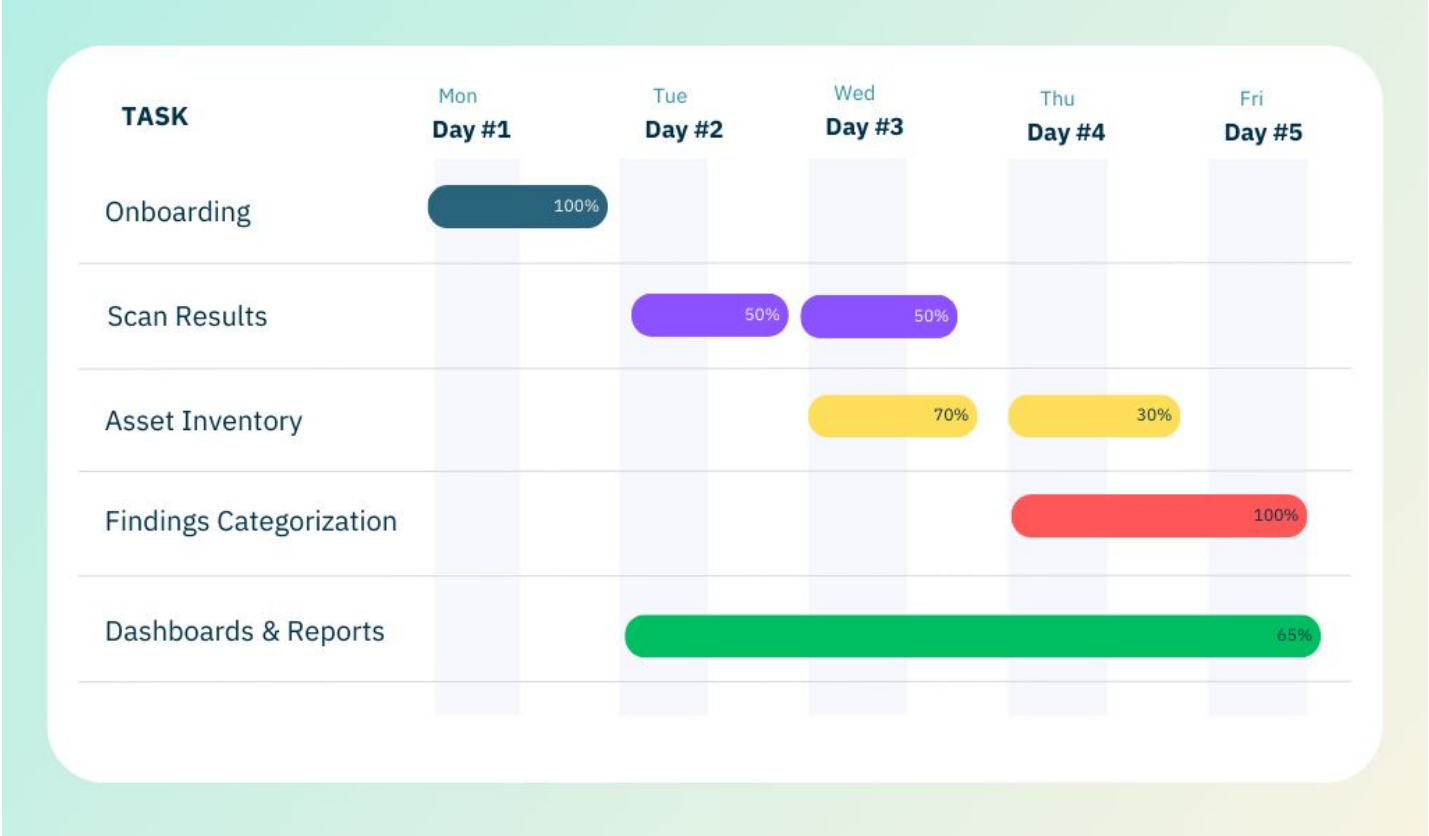
AccuKnox został zweryfikowany i zatwierdzony przez system bezpieczeństwa RHEL →

sjultra

SJULTRA i AccuKnox współpracują w celu dostarczenia CNAPP przedsiębiorstwom →

Terminy POC

AccuKnox



Streszczenie

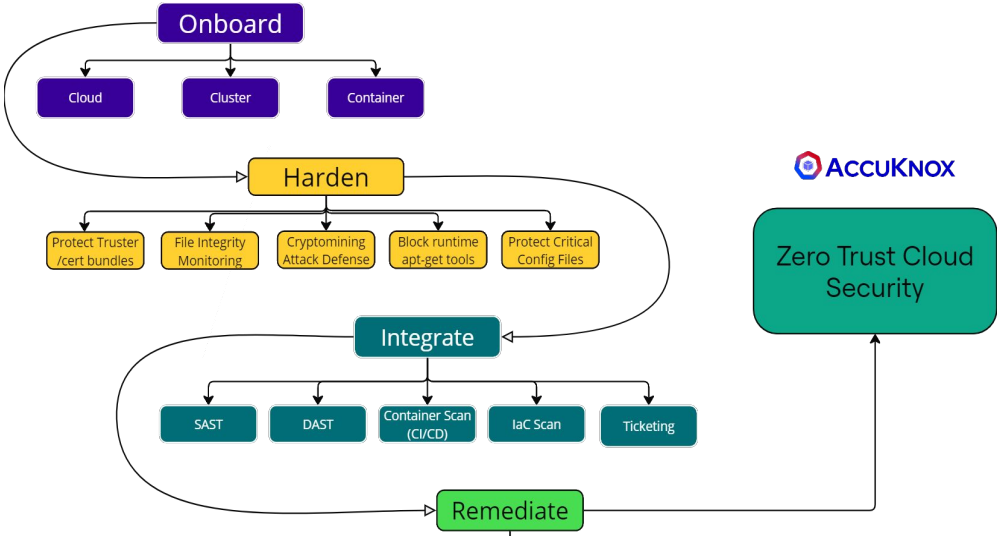
Wykonanie POC:

Etap 1: Inwentaryzacja aktywów (wdrażanie)

Etap 2: Odkryj ocenę ryzyka

Etap 3: Wykonaj priorytetyzację opartą na ryzyku

Etap 4: Naprawa (zasady, zgłoszenia)



Available in AWS Marketplace

Red Hat Marketplace Operated by IBM

Now available on Microsoft Azure MARKETPLACE

ORACLE Cloud Marketplace

accuknox.com/marketplace

Get AccuKnox CNAPP Demo

AccuKnox

ZOBACZ NAS W AKCJI

support@accuknox.com

Certyfikowany przez

kubernetes CERTIFIED SERVICE PROVIDER

AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

CLOUD NATIVE COMPUTING FOUNDATION SILVER MEMBER

NEPHIO

aws PARTNER Amazon EKS Ready

NUTANIX READY AHV