



# Cloud Security Maturity Framework: Best practices to operationalize cloud security

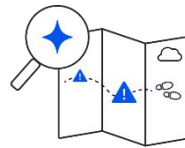


# Cloud is the biggest transformation security has experienced



New environment

How do I get visibility into my environment?



New risks

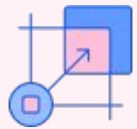
How do I prioritize the real risks and eliminate the noise?



New ownership model

How do I ingrain security into our teams?

# We've tried different approaches for **over a decade**



**Extend solutions  
from on-prem**



**Native tools  
per cloud**



**Build it yourself**



**Siloed, point  
solutions**

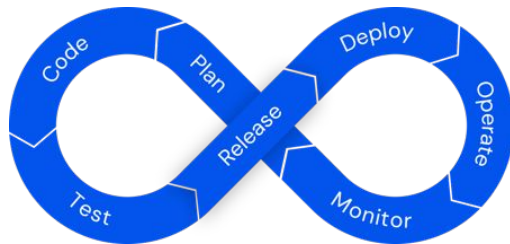


# Unified platform for the modern cloud security operating model



## Wiz Code Secure Cloud Development

Secure every stage of your SDLC to gain visibility & prevent risks in code, pipeline, registries and images



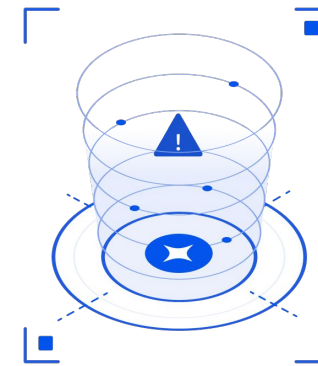
## Wiz Cloud Manage Security Posture

Agentless visibility & risk prioritization that proactively reduces the attack surface



## Wiz Runtime Respond to Cloud Threats

Cloud events and lightweight eBPF-based sensor to protect workloads from unfolding threats as a last line of defense



Remediate anywhere Cloud to Code

Build securely by design with Code to Cloud guardrails





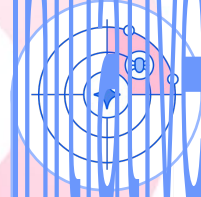
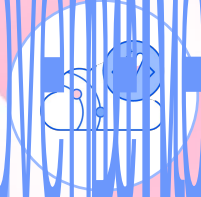
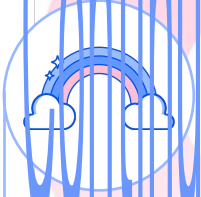
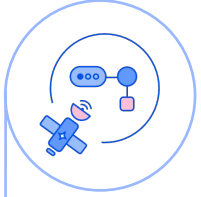
# Introducing the Cloud Security Maturity Framework

Best practices from customers

Taken from thousands of customers including 40% of the Fortune 100



# Cloud Security Maturity Framework



## Gain Visibility

- 5:** Complete multi-cloud visibility
- 3:** Agent-based visibility or single cloud/account visibility
- 1:** No visibility

## Reduce Critical Risk

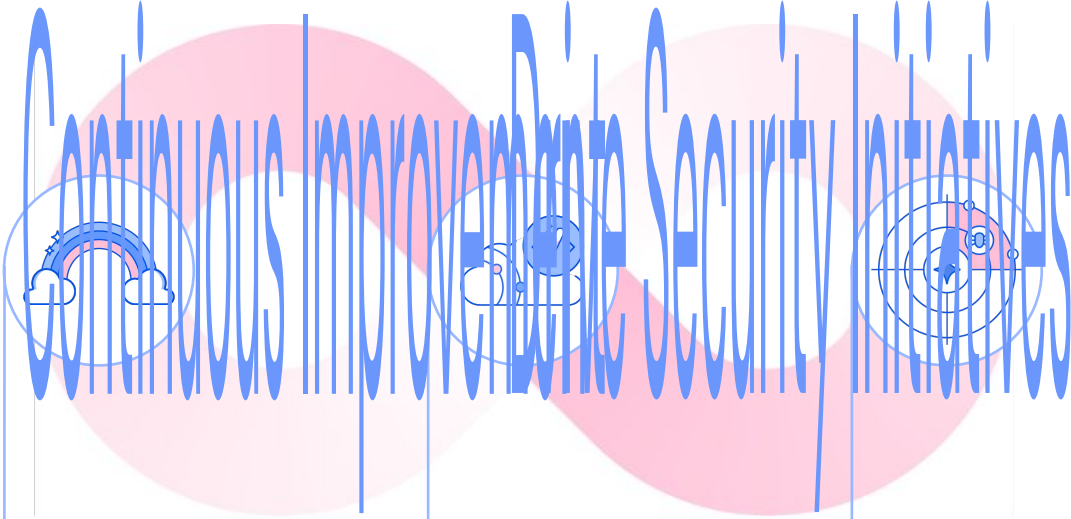
- 5:** Remove critical risks across clouds
- 3:** Remove critical risks from a single cloud/architecture
- 1:** Risk reduction programs in single domains

## Democratize Security

- 5:** Dev teams self-service remediate issues and maintain compliance
- 3:** Security sends issues to developers and developers remediate
- 1:** Security is fully owned by security teams

## Develop Securely

## Respond to Threats



# Complete multi-cloud visibility

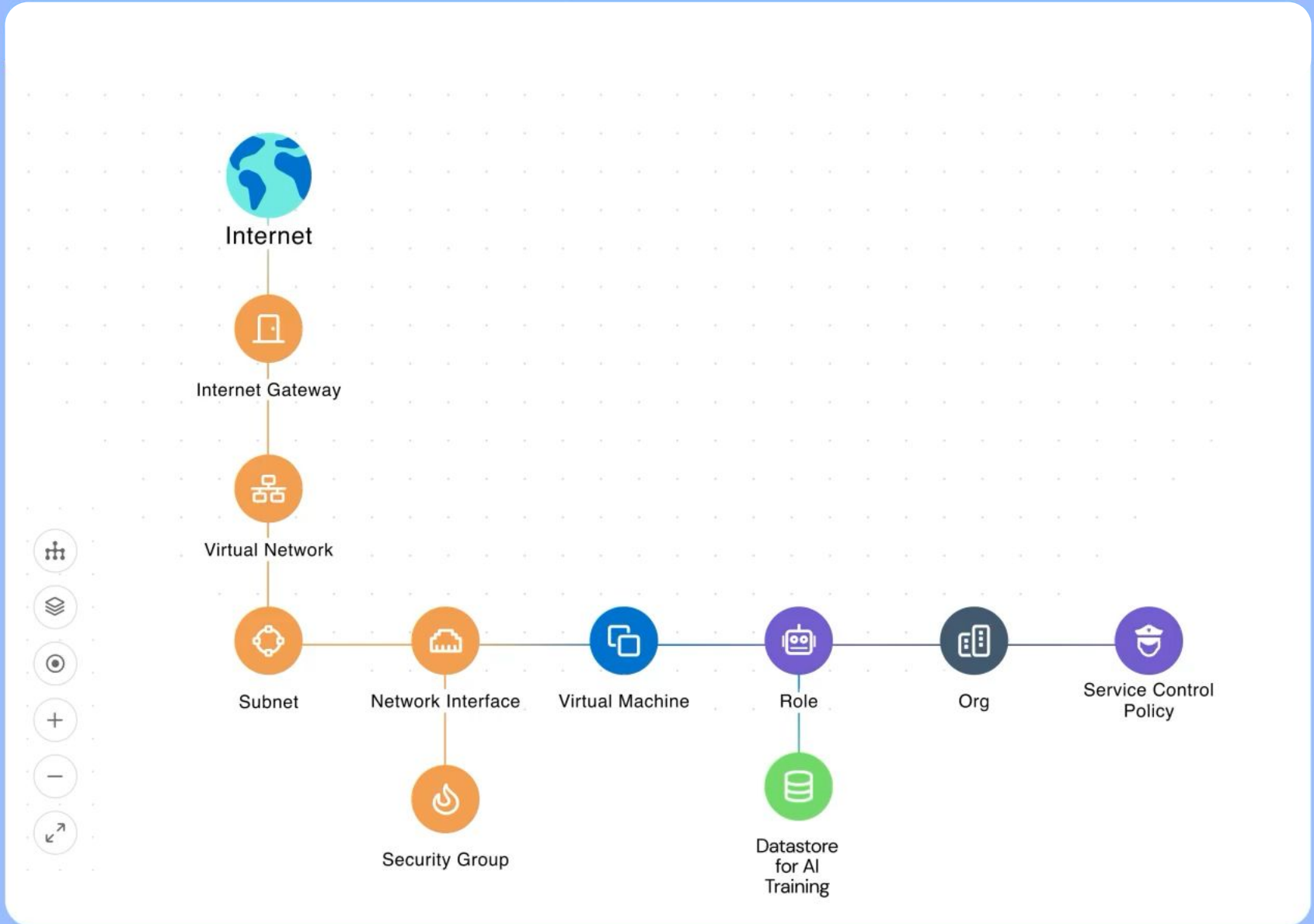
Best practice: Scan the cloud without agents for full visibility across:

- Cloud
- Orchestration
- Serverless
- Containers
- VMs
- PaaS



# Visibility into risks across cloud

- Misconfigurations
- Vulnerabilities
- Malware
- Sensitive data
- External exposure
- Excessive permissions
- Exposed secrets
- Lateral movement
- AI risks
- Novel vulnerabilities and attacks
- Business impact



# Visibility into critical attack paths that need to be prioritized



# Best practice: Focus on fixing toxic combinations

## 01 CSPM

Workload with a public IP (doesn't equal external exposure)

## 02 Vulnerabilities

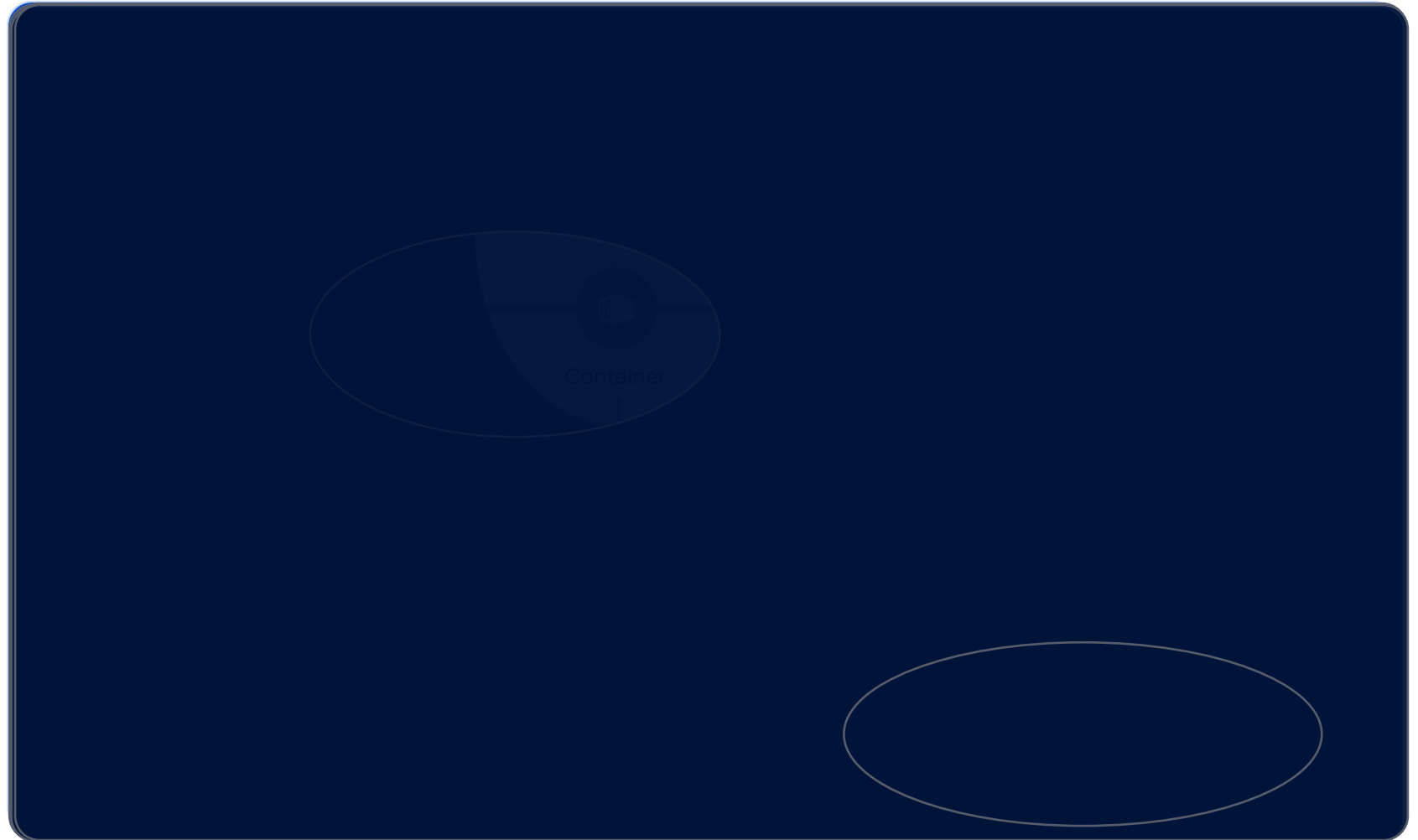
Critical CVE

## 03 CIEM

Admin permissions, which are excessive

## 04 DSPM

Sensitive PII data found in a database



# Best practice: Focus on fixing toxic combinations

## 01 CSPM

Workload with a public IP (doesn't equal external exposure)

## 02 Vulnerabilities

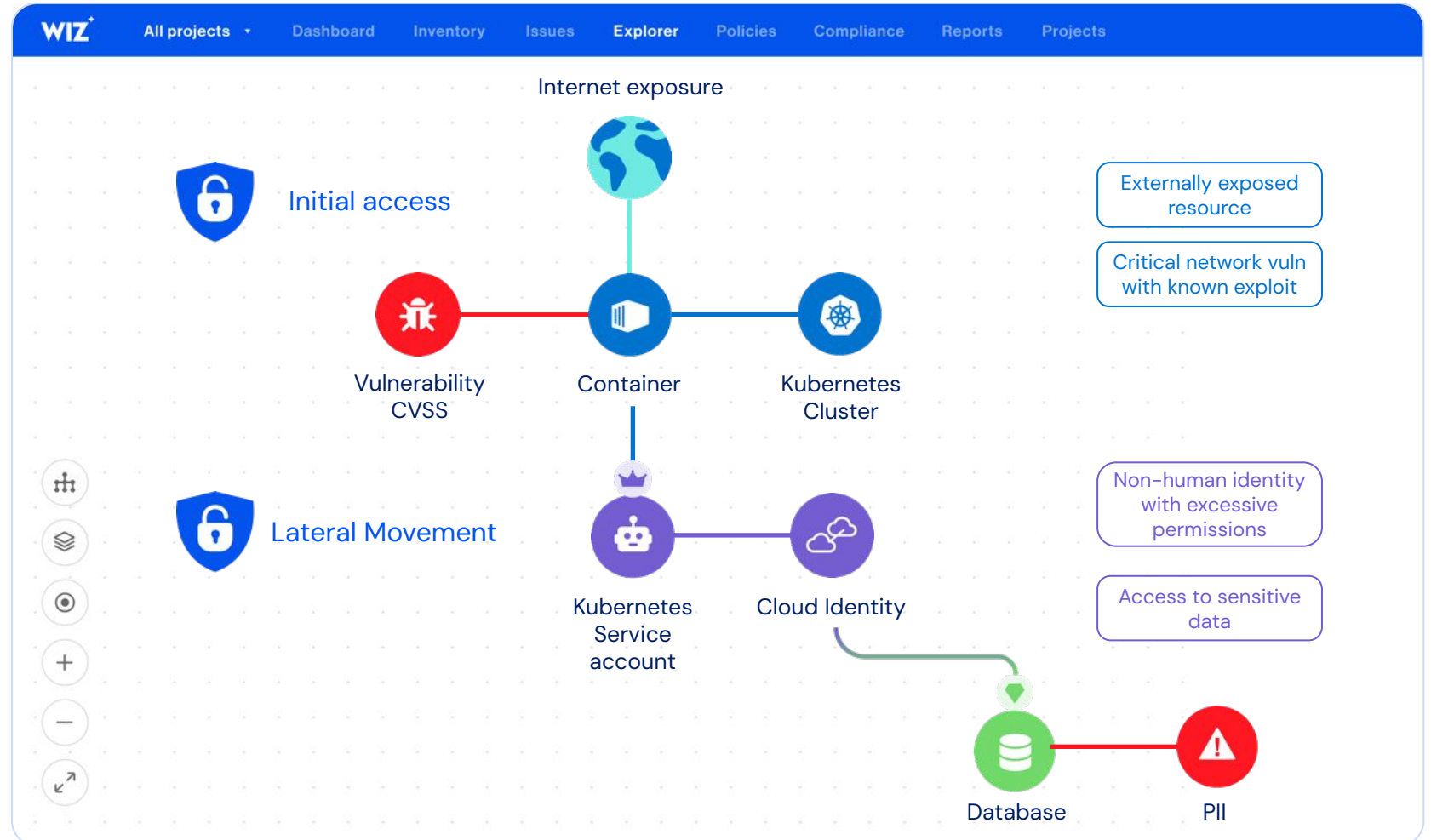
Critical CVE

## 03 CIEM

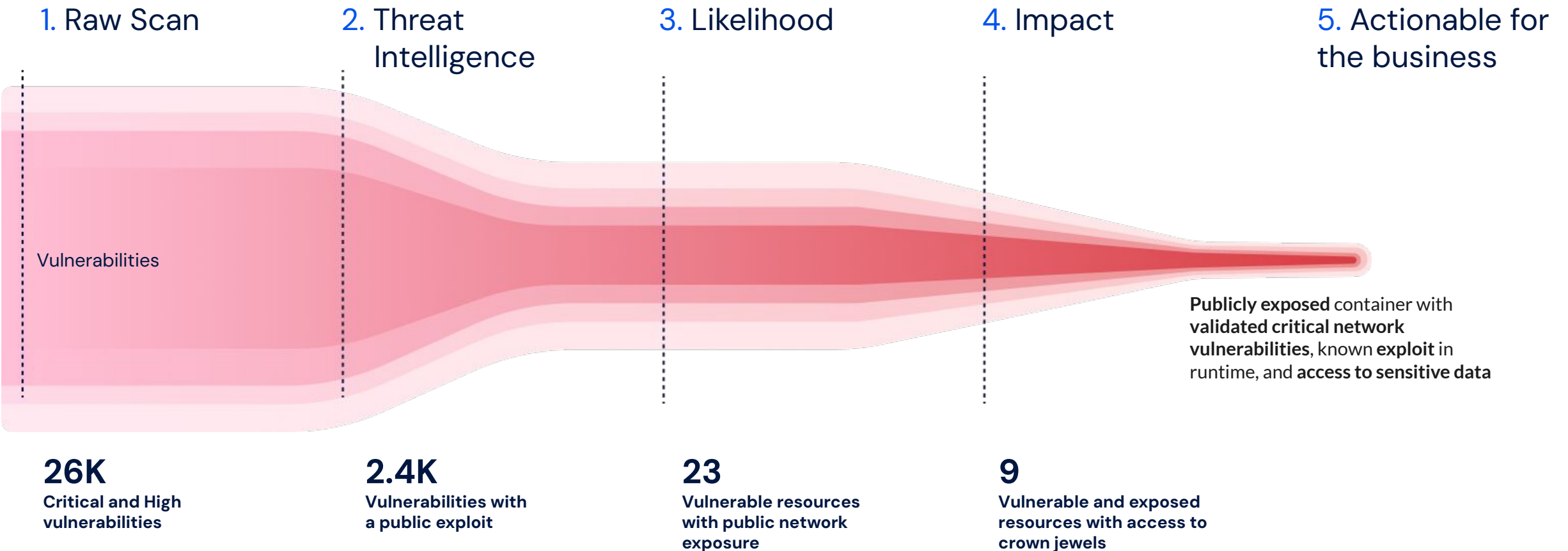
Admin permissions, which are excessive

## 04 DSPM

Sensitive PII data found in a database





# Risk-based approach to vulnerability management in the cloud







# Best practice: Zero-day response to high profile threats

Automated Threat Center to show the Zero-day indicators of the Emerging threats you need to pay attention to, including CISA, CERT-EU, and private research.

  **Critical Vulnerability in Argo CD**  
May 21, 2024, source: Wiz Threat Research

Researchers discovered a critical vulnerability (CVE-2024-31989) in Argo CD, a popular GitOps continuous delivery tool for Kubernetes, with a severity score of 9.1. This vulnerability leverages Argo CD's elevated permissions to allow attackers to escalate their privileges and potentially gain control over Kubernetes clusters. The vulnerability exploits the unsecured Redis caching server used by Argo CD, enabling attackers to manipulate application state manifests, deploy malicious pods, and access sensitive information.



0 Findings

  **Critical Vulnerability in Git**  
May 19, 2024, source: Wiz Threat Research

New versions of Git have been released, addressing five vulnerabilities, including the critical CVE-2024-32002, which allows remote code execution during a "clone" operation. This flaw lets malicious repositories trick Git into miswriting files, enabling unauthorized code execution without user inspection. It is recommended to upgrade Git to a patched version.

vulnerability critical rce

154 Findings

  **APT28 Targeting Print Spooler Vulnerability for GooseEgg Deployment**  
Apr 24, 2024, source: Wiz Threat Research

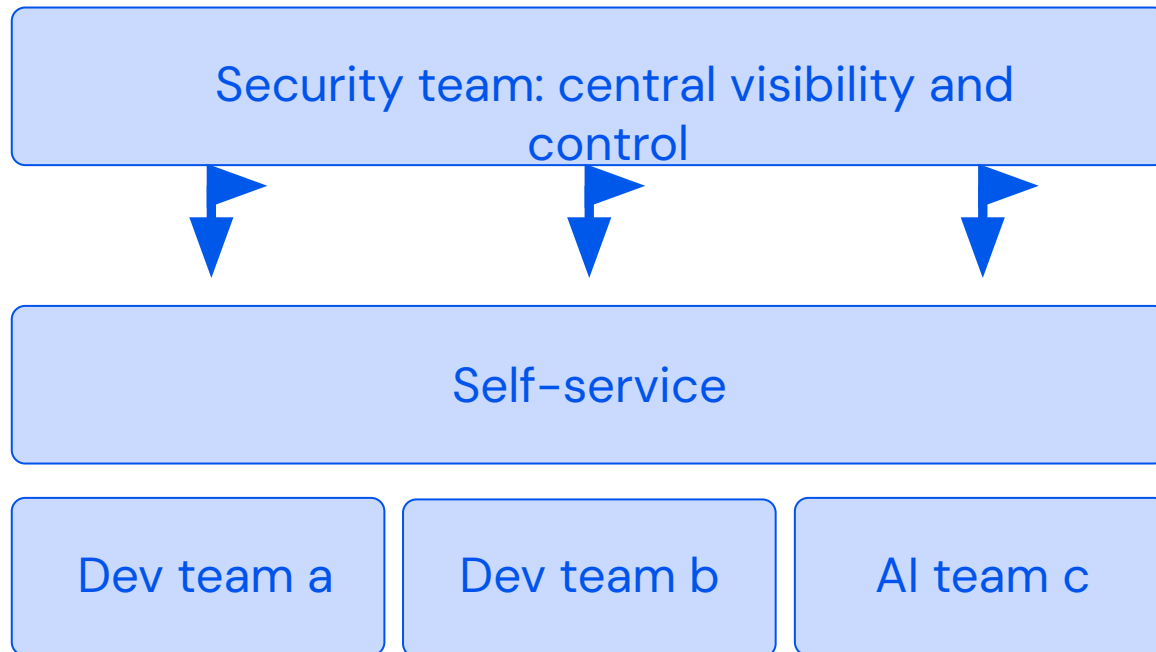
Microsoft Threat Intelligence has disclosed activities by the Russian-based threat actor Forest Blizzard, also known as APT28 or Fancy Bear, linked to GRU's Unit 26165. Forest Blizzard has been exploiting CVE-2022-38028, a vulnerability in the Windows Print Spooler service, since at least June 2020 to deploy a custom malware known as GooseEgg. These attacks have been targeting sectors such as government, non-governmental organizations, education, and transportation across Ukraine, Western Europe, and North America. In addition to CVE-2022-38028, the group has exploited other critical vulnerabilities, including CVE-2023-23397 in Microsoft Outlook and CVE-2023-38831 in WinRAR. It is recommended to look for indicators of compromise in your environment, and if any are identified, remove the files immediately and redeploy workloads from a known clean state.

malware APT28 in-the-wild Forest Blizzard Fancy Bear

[Read more](#)

0 Issues	0 Infected
9 Vulnerable	

## Best Practice: Make cloud security a team sport



## Democratization checklist:

- ✓ Answer the "so what" question
- ✓ Visualize for clarity
- ✓ Support by evidence
- ✓ Clear remediation description
- ✓ Provided remediation code
- ✓ Automation & workflow ready
- ✓ Code context for cloud-natives

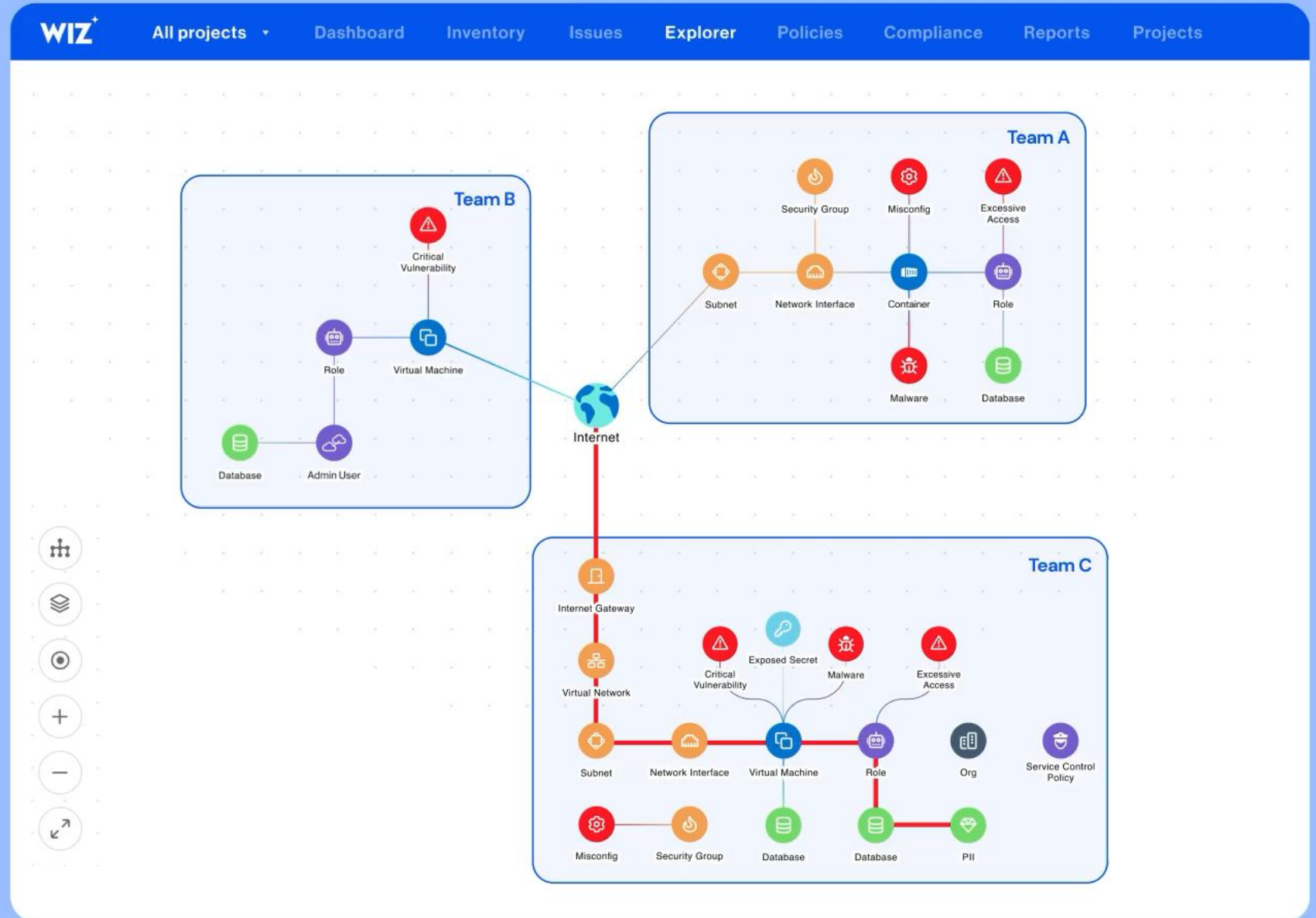
# Democratize security visibility

Determine cloud ownership by team

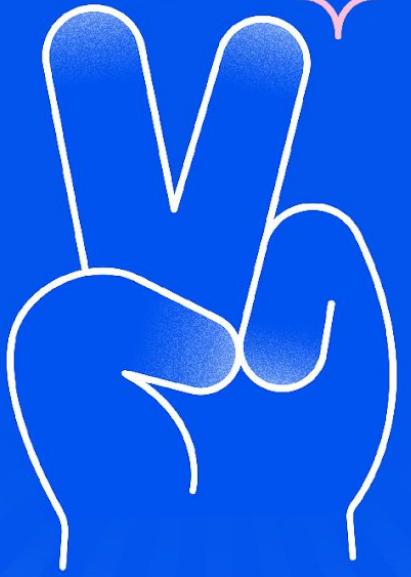


# Automate so dev teams can self-serve

Embed automation into existing dev workflows



CRITICAL CLUB \* ZERO CRITICAL CLUB \* ZERO



WIZ\*



# FOX

“Wiz allows us to achieve our philosophy of how to democratize security – scaling the cybersecurity team's reach through technology.”



Melody Hildebrandt

CIO,  
FOX Corp

# H E A R S T

“So I don't even need to ship these reports to people. I just give the team access to the tool and we're able to watch them burn [risks] it down to zero.”



Steven Craig

Senior Director, Cloud Center of Excellence,  
Hearst Enterprise Technology

# Securing data and AI development in cloud is a difficult and costly problem

**8 hrs**

for an unsecured and exposed DB to be breached

According to TechTarget research

**70%**

of cloud environments already use cloud AI services

According to Wiz's State of AI 2024 report

**50%**

of companies have at least one database or storage bucket exposed to the internet

According to Wiz's State of the Cloud 2023 report

**\$5M**

average cost of a data breach

According to IBM's Cost of a Data Breach Report 2022

# Best practice: Continuously discover sensitive data and reduce its risk

## Establish broad discovery

- **Discover** PII, PHI, PCI, and secrets across your cloud estate
- Leverage CNAPP to **scan any cloud, any architecture**

## Prioritize critical data exposure

- Remove **external exposure** via network or identity
- Ensure **access governance** to continuously reduce broad internal exposure

## Automate compliance assessments

- Continuously assess compliance to ensure standards are consistent across the cloud

The dashboard displays three main sections:

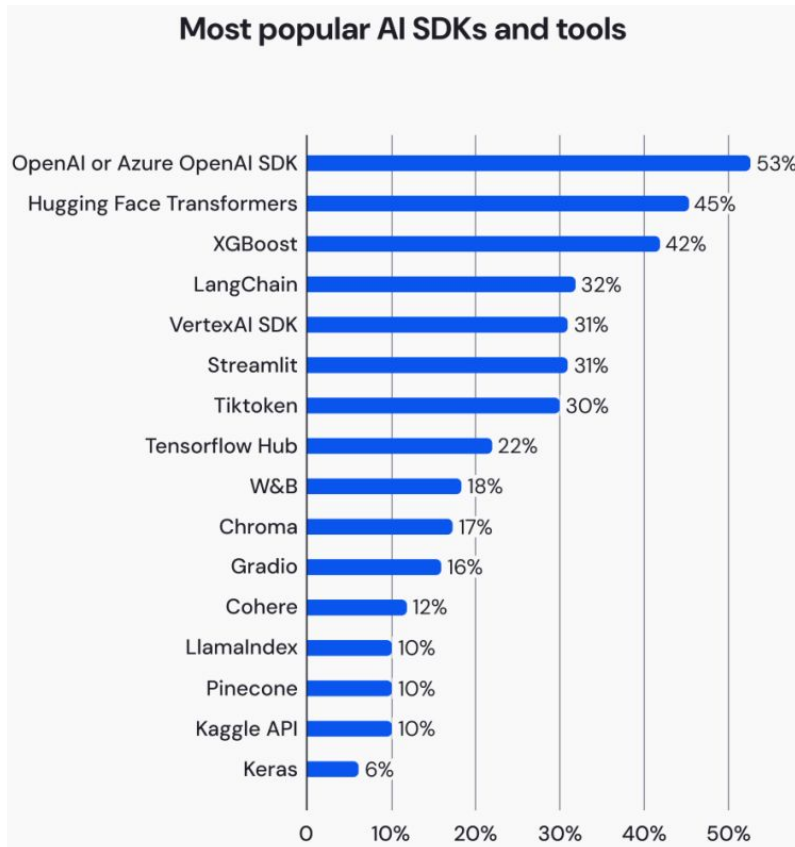
- Data Findings:** A table with columns for Classification Rule, Severity, Findings, Subscriptions, and Locations. It lists rules like 'Email PII' (High severity, 75 findings) and 'Name PII' (High severity, 31 findings).
- Cloud Entitlements:** A filterable table showing identities and their access to resources. Filters include 'Native Type is IAM Role' and 'Access Type is High Privilege'. Resources listed include 'lorax-aurora-db' (Amazon RDS Aurora MySQL Cluster).
- DSPM Compliance Scores:** A grid of progress bars for various standards: HITRUST CSF v9.5.0 (44%), SOC 2 (49%), GDPR (51%), PCI DSS v3.2.1 (51%), ISO/IEC 27001 (64%), NIST SP 800-53 R... (68%), HIPAA Security Ru... (79%), and NIST 800-171 Rev.2 (89%).



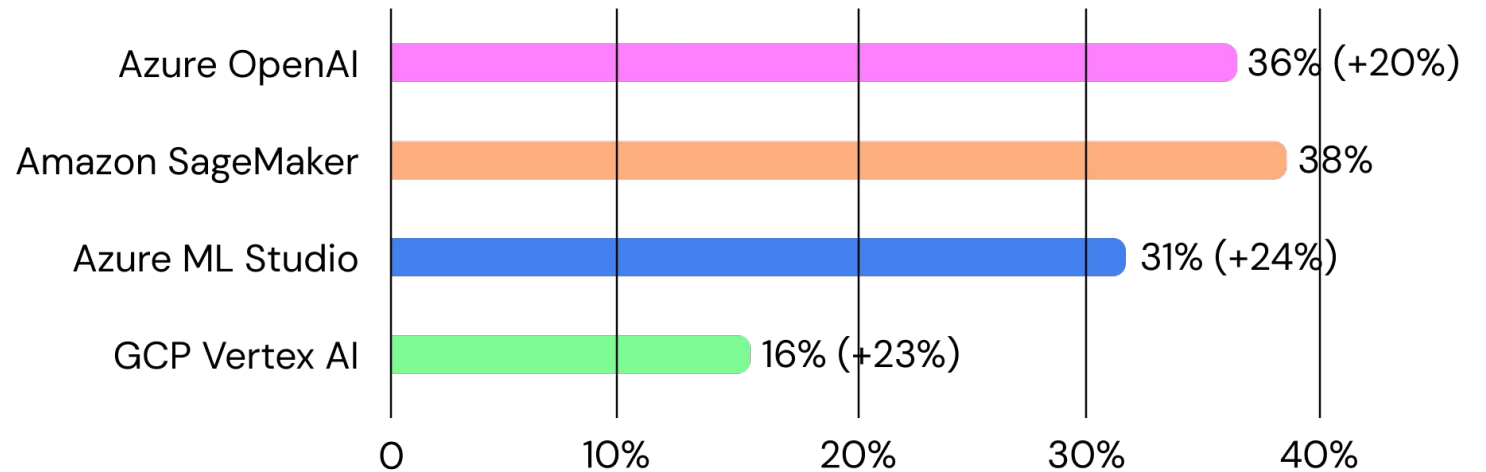


State of AI Report by Wiz Research<sup>(1)</sup>: AI is already here.

# 70% of cloud environments already use cloud AI services



### Percent of all cloud environments with instances of managed AI services (comparing Dec '23 vs. June '24)



(1) Wiz Research, January 2024, <https://www.wiz.io/blog/key-findings-from-the-state-of-ai-in-the-cloud-report-2024>

# Best Practice: Secure AI data by tracing the pipeline

## End-to-end AI pipeline visibility

- Detect every resource in AI pipelines, from machines hosting training jobs to data stores

## Deep risk analysis in AI pipelines

- Identify AI vulnerabilities, misconfigurations, permissions, data, secrets, and network exposure
- Scan AI Models like you would scan any container image

## Remove critical attack paths to AI models

- Prioritize and proactively fix the risks that create attack paths to sensitive data

VM hosting a suspicious AI model  
Issue

Comment Run an Action Create a Ticket 0 Past Activities Give Feedback

Overview Remediation Comments

### Evidence

Attack Path Visualization View on Security Graph

Hosted model 1  
Hosted AI Model (AI Model)

testing-models  
Amazon Web Services EC2 Ins...

Hosted model 2  
Hosted AI Model (AI Model)

CWE-502 Finding

CWE-502 Finding

**CWE-502**  
Finding

Description

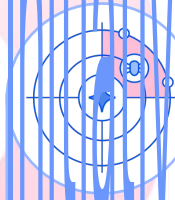
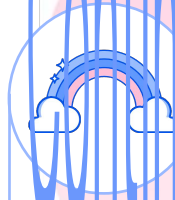
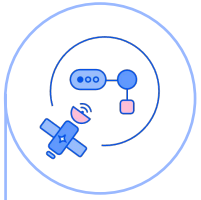
The model file `model.bin` which was detected in `/root/models/b'calc'` imports risky imports which may pose a security risk and allow arbitrary code execution or other unexpected security risks.

Verify the source of the model - if it was downloaded from an untrusted source, the model should not be executed in a sensitive environment.

If the model was downloaded from a trusted source or developed internally, ensure that the risky imports are necessary, as they could allow

[View Details >](#)

# Cloud Security Maturity Framework



## Gain Visibility

- 5:** Complete multi-cloud visibility
- 3:** Agent-based visibility or single cloud/account visibility
- 1:** No visibility

## Reduce Critical Risk

- 5:** Remove critical risks across clouds
- 3:** Remove critical risks from a single cloud/architecture
- 1:** Risk reduction programs in single domains

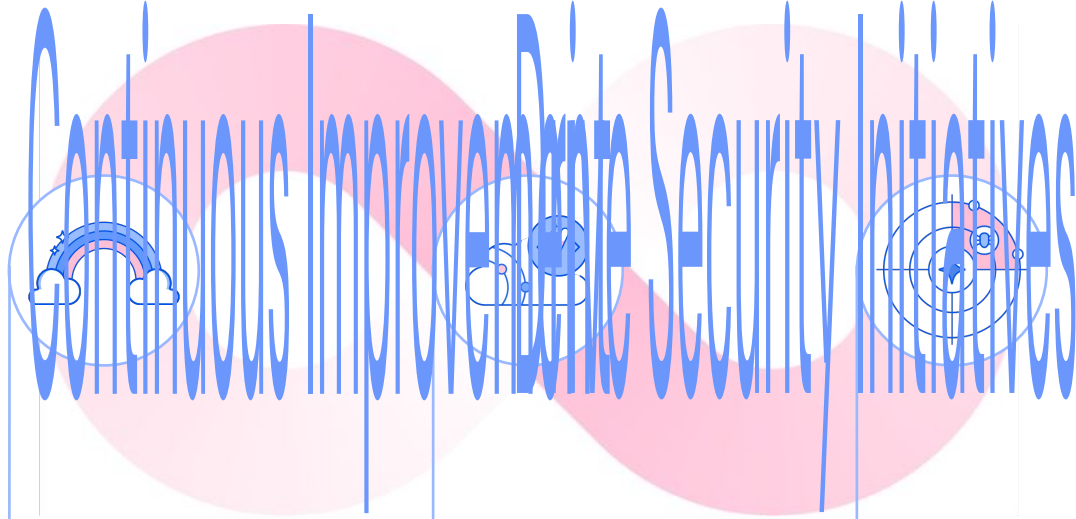
## Democratize Security

- 5:** Dev teams self-service remediate issues and maintain compliance
- 3:** Security sends issues to developers and developers remediate
- 1:** Security is fully owned by security teams

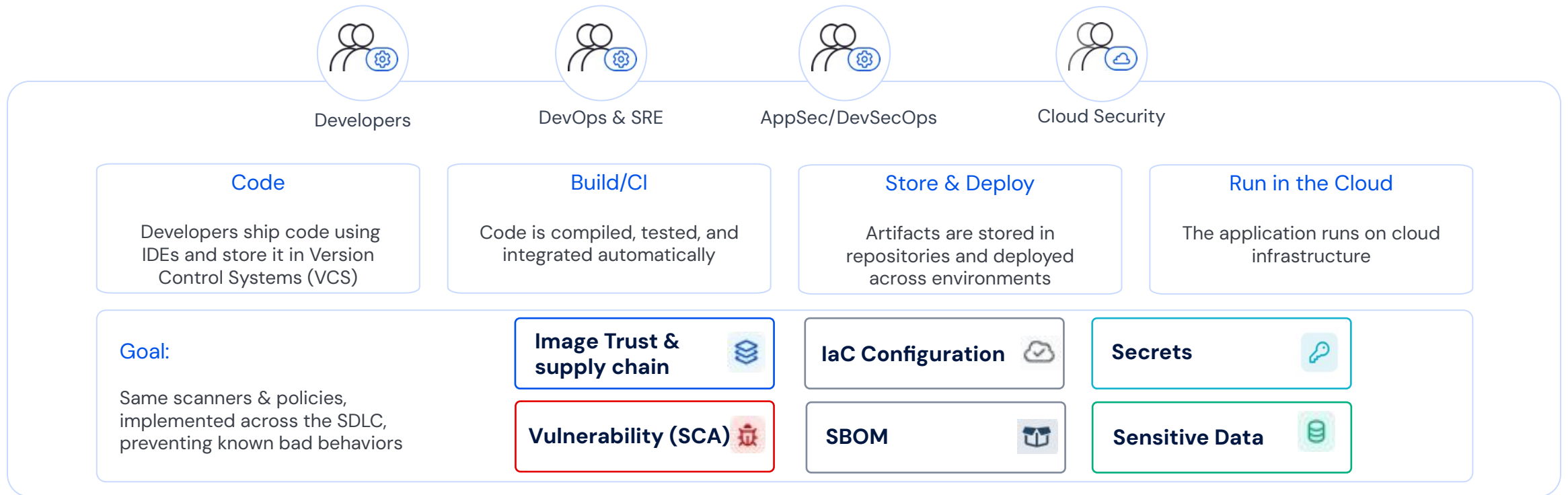
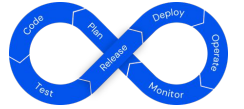
## Develop Securely

- 5:** Implement hardened golden pipelines to reduce drift
- 3:** Implement policies in a limited number of pipelines
- 1:** Developer ownership of apps and infrastructure known or partially known

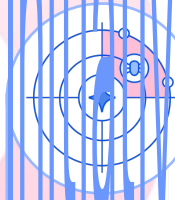
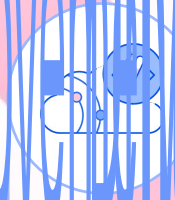
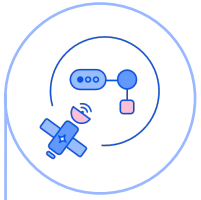
## Respond to Threats



# Gearing to the left: Build securely **by design**



# Cloud Security Maturity Framework



## Gain Visibility

- 5:** Complete multi-cloud visibility
- 3:** Agent-based visibility or single cloud/account visibility
- 1:** No visibility

## Reduce Critical Risk

- 5:** Remove critical risks across clouds
- 3:** Remove critical risks from a single cloud/architecture
- 1:** Risk reduction programs in single domains

## Democratize Security

- 5:** Dev teams self-service remediate issues and maintain compliance
- 3:** Security sends issues to developers and developers remediate
- 1:** Security is fully owned by security teams

## Develop Securely

- 5:** Implement hardened golden pipelines to reduce drift
- 3:** Implement policies in a limited number of pipelines
- 1:** Developer ownership of apps and infrastructure known or partially known

## Respond to Threats

- 5:** Automate cloud-native SOC workflows
- 3:** Implement incident response framework
- 1:** Ingest cloud events into SIEM/SOAR for SOC

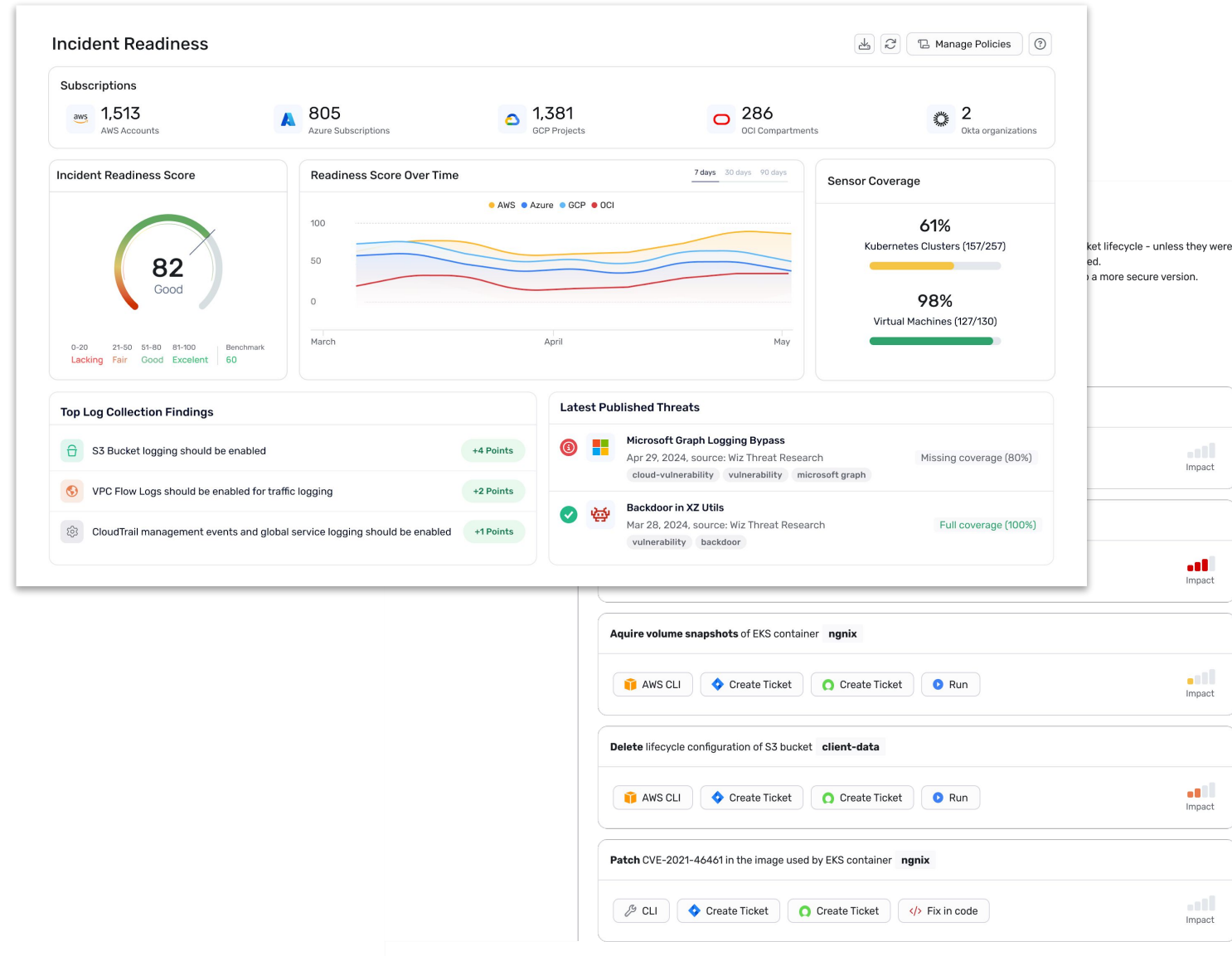
# Best practice: prepare your cloud for a breach

## Mature your Incident Response Readiness

- **Continuously evaluate** your visibility to ensure you eliminate all gaps
- **Prioritize and collect** the telemetry you need to analyze – both runtime and logs

## Be ready with Forensics and Response Playbooks

- Ensure you're ready to **capture forensic data quickly** – and don't chase to get access to images during a crisis
- **Create response playbooks** for each type of cloud threat



# Best practice: broaden your cloud-native visibility and detection coverage

## Align on a unified schema for all cloud data

- **Centralize telemetry** in a single data store for analytics, detection and investigation



07:12:29 PM  
April 30, 2024 Unusual SSH connection to a pod

07:19:43 PM  
April 30, 2024 Suspicious connection to IMDS

Runtime



02:35:47 AM  
May 1, 2024 Unusual exfiltration activity from an S3 bucket with sensitive data

Data Plane



03:28:09 AM  
May 1, 2024 Short Lifecycle Policy Applied to an S3 Bucket

03:31:42 AM  
May 1, 2024 Versioning Suspended for S3 Bucket

CSP Control Plane



05:26:17 PM  
April 30, 2024 Create Deployment

K8s Control Plane



03:41:03 AM  
May 1, 2024 Suspicious PR pushed and merged outside working hours

VCS & CI/CD



04:03:11 PM  
April 19, 2024 Admin Sign-In From Unusual Country

11:48:03 AM  
April 19, 2024 Country Switch Within Session

IdPs

## Implement cross-layer detection

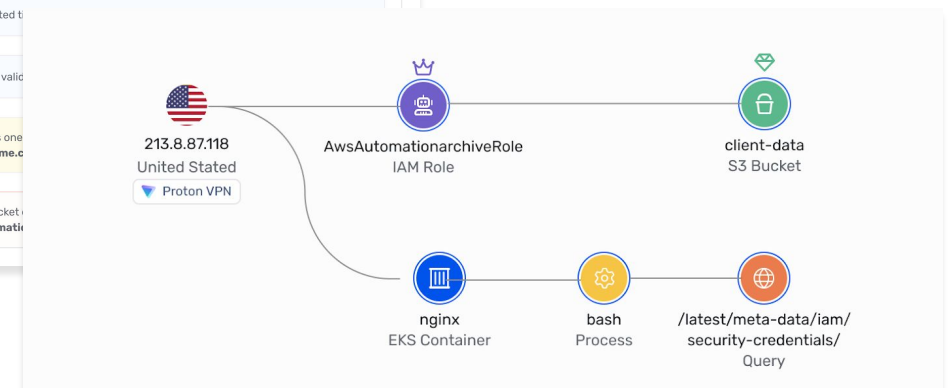
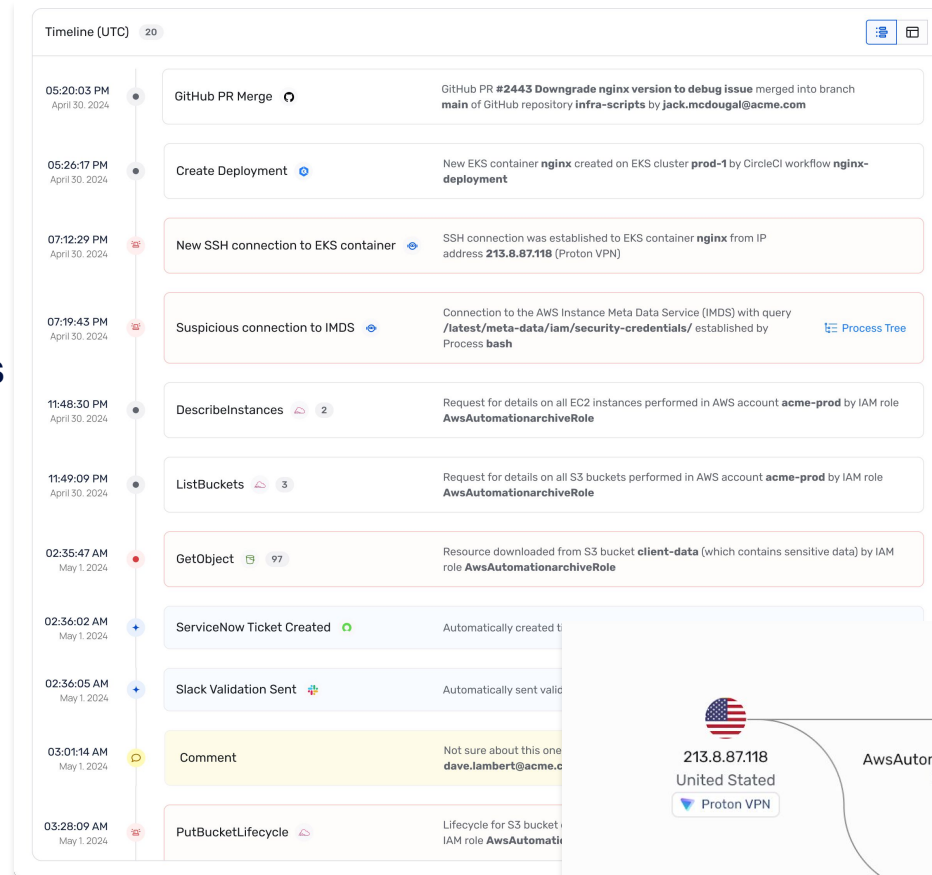
- **Correlate signals for detection** across the identity, data, network, compute, and control planes
- **Contextualize** to reduce noise



# Best practice: empower your SOC with cloud expertise and broad context

Level-up your cloud-native threat investigation and response skillset

- **Build the skills** on your team needed to triage and investigate cloud threats
- **Bring context** from across cloud, identity and dev





# Best practice: fix at the root and drive resilience

## Collaborate with dev to respond faster

- **Effectively collaborate with cloud security and developers** to remediate issues

## Drive resilience

- Every incident is an opportunity to become more resilient, fixing root cause issues

The screenshot displays a cloud security dashboard with several panels. The top panel, titled "Ask GitHub user jack.mcdougal@acme.com about related events from the alert's timeline", includes "Email" and "Slack" buttons. Below it, the "Isolate traffic of EKS container nginx" panel features "AWS CLI", "Create Ticket", "Create Ticket", and "Run" buttons. The "Acquire volume snapshots of EKS container nginx" panel also has "AWS CLI", "Create Ticket", "Create Ticket", and "Run" buttons. A "Delete lifecycle config" panel shows an "AWS CLI" button. A "Patch CVE-2021-464" panel includes "CLI" and "Create Ticket" buttons. A large overlay window shows a vulnerability alert: "The following vulnerability impacts github.com/docker/docker versions <24.0.9: CVE-2024-24557. It can be remediated by updating to version 24.0.9 or higher." Below the alert, a "Suggested change" box shows a diff: "- github.com/docker/docker v24.0.7+incompatible // indirect" and "+ github.com/docker/docker v24.0.9 // indirect". A "Commit suggestion" dropdown is at the bottom right of the diff box. At the bottom of the overlay is a "Reply..." input field.

# Cloud security as an organization-wide tool to democratize

Democratization

