Operationalize your cloud security with Wiz

Table of Contents

The importance of a cloud security operating model

Many organizations today still host their workloads solely on-prem, but cloud adoption has exploded in recent years and is still evolving. It's a trend that's only set to accelerate, as Gartner predicts that by 2028, 70% of all workloads will be executed in the cloud.

Robust cloud security is a requisite for success. However, not all enterprises are equally mature regarding the cloud and cloud security. Deficiencies like cybersecurity talent shortages, siloed security teams, suboptimal and fragmented tools, the inability to perform continuous real-time assessments of cloud environments, and high volumes of contextless security alerts can exacerbate existing vulnerabilities and put companies in the crosshairs of threat actors.

Fundamentally, cloud security comprises three critical components: technology, process, and people. Each component needs to be strengthened, unified, and synchronized to ensure bulletproof cloud security. Let's break them down.

- Technology: Siloed security technology can significantly weaken your enterprise's cloud security posture. Organizations must consolidate security tools into a single, unified platform that offers comprehensive visibility across complex cloud environments. More importantly, your cloud security technology should inform you which risks are critical to your organization and why.
- Process: It's no secret that software development lifecycles (SDLCs) have become increasingly decentralized and agile. That's why security and development in the cloud need to be unified. Enterprises need to embed cloud security practices early and deep into SDLCs by implementing new processes that reflect the realities of current cloud operations and security, as well as the surrounding threat landscape.
- People: If you steward a cloud asset, you're responsible for its security, plain and simple. Cloud security must be a shared responsibility. This means that all users — including DevOps and SecOps — must have a complete and contextualized understanding of their environments, clarity on ownership and responsibilities, end-to-end views of risks and vulnerabilities, and self-serving security capabilities.

Wiz's cloud security platform enables a modern cloud security operating model that helps organizations efficiently secure everything they build and run in the cloud. It does this by addressing technologies, processes, and people, in a five-step maturity model.

Note: Our proposed maturity model is not set in stone and can be adapted to suit your needs. Although the first three steps are essential, it is entirely possible to interchange steps 4 and 5, or to run them in parallel.

The cloud security maturity journey

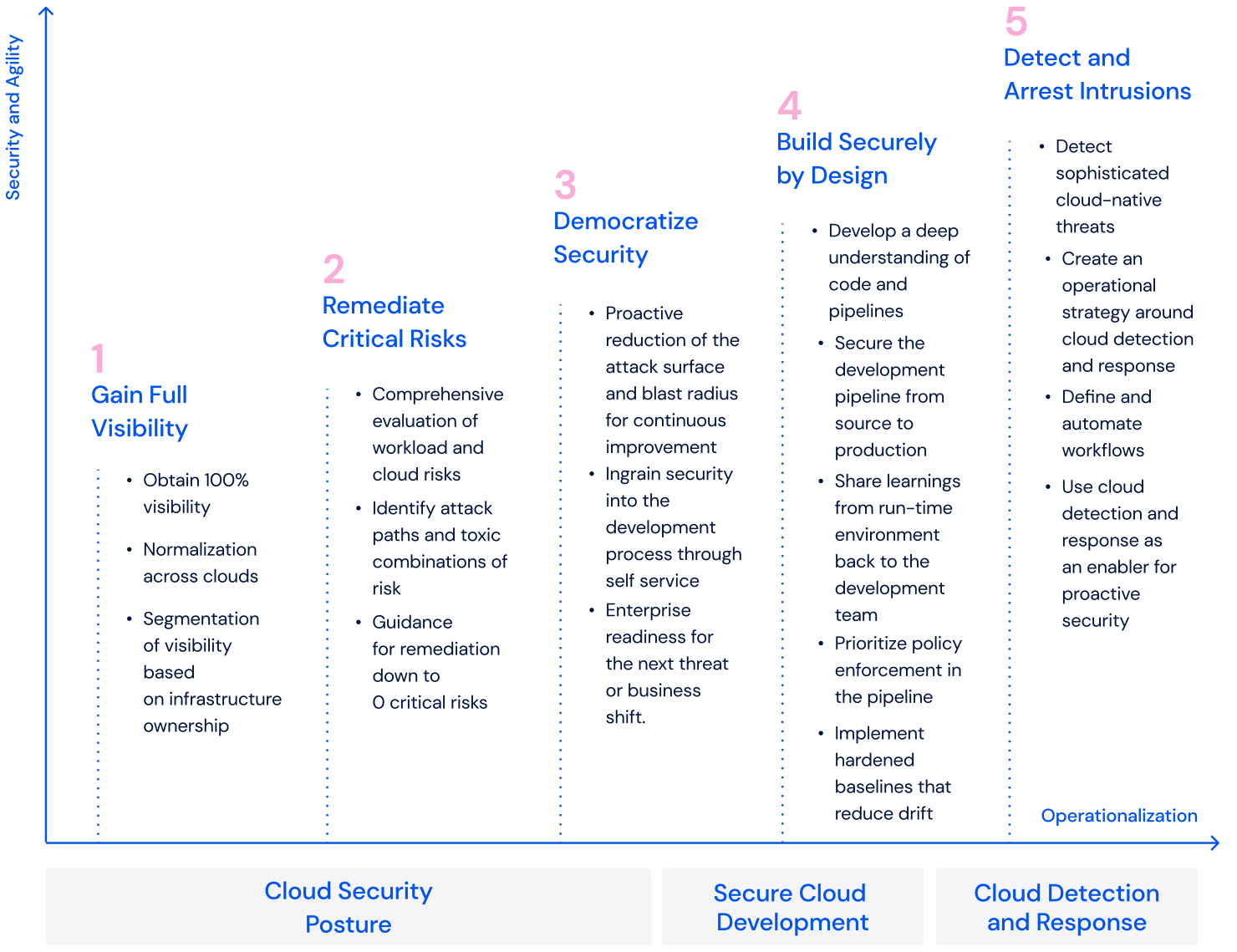

Fig 1 – Wiz maturity framework

This model can help you leverage Wiz for a variety of use cases that perfectly match the current and future trends in the cloud. Examples of these use cases include:

- **Cloud risk prioritization:** Prioritize your cloud risks based on several contexts and criteria to ensure that critical vulnerabilities are addressed first.
- Data security: Defend your organization against data breaches, the average cost of which reached $4.45 million in 2023.
- **Container and Kubernetes security:** Use the Wiz Security Graph to secure your containers and container images across their lifecycles, from code and build time to deployment and runtime.
- **Incident response:** Constantly and proactively assess your cloud environments to gain measurable insights about potential threats and how to respond to them.
- **DevSecOps:** Empower your DevOps engineers and security teams by seamlessly combining security and development at every stage in your SLDCs.

Operationalize your cloud security

Preparation phase: Build your foundation

Building a robust cloud security ecosystem is much like building a house. The first step is to lay a solid foundation upon which layers of security protocols and practices can be built. There are three main parts to this phase outlined below.

Part 1: Gather information

Cloud infrastructure demands real-time, highly integrable scanners that can conduct in-depth assessments across diverse resources. This is vital because cloud environments can expand with a few clicks, meaning an enterprise's protected surface is constantly in flux. In the past, agent-based scanners sufficed for IT security. Now, enterprises must shift to agentless scanners to tackle the speed and scale of the cloud. Agentless approaches can help secure companies across cloud, cluster, container, and code layers.

Wiz relies on connectors to canvas your cloud environments. These connectors need read-only access roles to be able to use cloud APIs. Before deploying and configuring them, make sure that you know critical details, like which providers your cloud services come from, where to connect to, and who oversees what. Furthermore, this is also a good time to identify cloud-related requirements, such as compliance constraints, data sovereignty, etc.

Cloud Provider	Name of the account	Regions	Owner (Contact info + Team)	Deployments constraints (TF, CFT, others)	Compliance constraints (Y/N)	Data Sovereignty (Y/N)

Fig 2 – Example of a table used to gather cloud account information.

Part 2: Plan ahead

Ask yourself a few pertinent questions while laying the foundation for your cloud security. It's essential to know which resources, and to which cloud service providers (CSPs) — like AWS, Google Cloud, and Azure — you need to connect. Similarly, it's important to anatomize how your cloud architecture is organized. Every cloud resource must be stewarded appropriately, and this is typically achieved with robust identity access management (IAM) controls. Every account within a cloud environment needs to be configured to limit access to a project level or allow users to enforce change at an organizational level.

When setting up your Wiz solution, be aware of which core features are enabled and what their functions are. Examples of core features include Infrastructure as code (IaC) scanning, contextualized detection and response, cloud security posture management, cloud infrastructure entitlement management, and cloud workload protection platforms. Don't forget to protect your most critical cloud data (PII, PHI, and PCI) with data security posture management (DSPM). Ensure that your DSPM capabilities include data lineage tracking and seamless third-party integrations. Also, remember to set up and configure compliance frameworks to measure adherence to data privacy regulations.

Part 3: Identify who is in charge

In a shared responsibility security model, it's vital to know who is responsible for what. Every enterprise needs to know who to refer to for cloud environments and IAM controls. Similarly, every connection between two cloud regions, providers, or privileged accounts must be accounted for. These connections must be bound to an organization's own logic, while considering the principle of least privileges.

Design a RACI matrix to designate accountability for every cloud resource. Pro tip: use our proposal as a starting point.

The following matrix summarizes who within your organization should be Responsible (R), Accountable (A), Consulted (C), and Informed (I) during different phases of implementing Wiz.

Task/Role	Project Manager	Wiz Champion	Cloud Admin	SAML-SSO/ Integrations Team	Specialized Global Security Teams
Cloud Deployment	I	I	R	I	I
Add Projects	I	R+A	C	-	C
SAML-SSO Integration	I	I	I	R	I
Configure Projects and Role-based and Access	I	I	I	R	I
Integrate ticketing service	I	I	I	R	I
Address critical Issues	I	A	I	-	R
Become a Wizard	I	R+A	I	-	R/I

Fig 3 – Example of RACI

Furthermore, when connecting various branches of your cloud environment, including containers registries and Kubernetes clusters, be sure to carefully choose your method to prevent over-entitlements and accidental exposures. Use connectors at an organizational level rather than at an account level to create more rigid access boundaries across resources.

A sure-fire way to build a robust foundation for your cloud security is to take inventory of all your cloud resources and services. Scour your cloud environments to identify every service being used. Next, implement approval policies so that sensitive activities and services are only used legitimately.

Step 1: Complete visibility

The first step in your cloud security operating model is ensuring comprehensive visibility across your cloud entities, e.g., VMs, users, accounts, and more. Let's explore how Wiz helps you to enhance visibility and mitigate potent risks that your organization faces.

Connect your environments

With the information retrieved during the preparation phase, it's now time to connect your various cloud providers. To do this, you'll need to deploy Connectors that enable Wiz to scan cloud environments through APIs (configuration, network, identity, and workload disks). This can be done at different levels, i.e., organization or account level. We recommend that you do this at the organization level, as this will automatically scan all existing and new accounts; this simplifies operations and always ensures complete visibility.

Full inventory

After connecting your environments, create a complete inventory of the technologies you use. You can use Wiz to do this by scanning the configuration, network, and identity layers of your cloud, as well as the workloads themselves (via a snapshotting mechanism).

This scan gives you complete visibility of all the technologies deployed in your cloud environments. This is important for understanding what is being used or not used in your environment.

Once you have this visibility, you have all the cards in hand to:

- Have a dynamically updated map of the technologies in use
- Define which are approved and which are not
- Create alerts on new technologies detected but not yet asserted
- Create report on unused resources to identify potential cost savings

Comprehensive Cloud context

All cloud service providers use different naming conventions for their services. For example, for virtual machines, AWS uses EC2, GCP uses Compute instance, and Azure uses Virtual machine. Wiz's ability to standardize service names within a simplified naming convention greatly helps security teams by making it possible to simply use the inventory to search for a particular technology, such as AWS EC2 or a MongoDB database.

In addition, the Security Graph can be queried. To do this, you no longer need to know the names of all the services; simply search for all virtual machines to display a list of all EC2, Azure VM, GCP Compute instance, or any other type supported by Wiz on all clouds. The same applies to technologies: simply query the graph to find all virtual machines with a deployed database, and you'll see a list of workloads with a MongoDB, MySQL or other database.

Expand to more domains

Now that you have the basics and complete visibility of all your assets in the cloud, you can think about connecting more environments. In the previous section, we discussed the importance of connecting at the highest level (Organisation), using the minimum required permission, to automatically onboard new accounts, but now it's time to think about what else could be connected. Depending on your priorities, you can connect your Kubernetes environments and/or your data.

To do so, you have to be well prepared and think about:

- **Kubernetes:**
  - Is my cluster private or public? If private, you have to add the deployment of the broker, a lightweight reverse-proxy service, that allows secure communication with the Wiz backend.
  - What should my deployment process be? We highly recommend using our unified helm chart.
- **Container registries:**
  - Does my container registry as full or partial internet access? If yes, the deployment allows to quickly create a new connector to your registry. If partial internet access, then you need to add Wiz cloud and registry scanner Ips to an allow list.
  - Does my container registry as no internet access? If yes, you have to deploy the broker to allow secure communication between the registry and the Wiz backend.
- **Data security**
  - What should I cover? Wiz can scan public and private buckets, managed and self-managed databases, and more. To do so, Wiz needs additional read-only permissions that can be deployed via the existing connector configuration.

Segment views by teams based on infrastructure ownership

Every team needs to have a dedicated view of which cloud resources and corresponding security vulnerabilities matter the most to them. The logic behind this is simple: everyone needs to be responsible for protecting the cloud resources they use. It isn't sustainable or effective to solely rely on external teams to identify, diagnose, and remediate security risks in an environment managed by other teams. Indeed, security teams rarely know the full context. It is therefore important that application or infrastructure teams themselves have visibility of their security posture. This greatly reduces the meantime to remediate (MTTR).

Wiz Projects are an ideal tool for segmenting an evolving cloud environment to ensure that various teams can identify and understand which cloud resources they are responsible for and what their ownership of those resources entails. This enhanced visibility will help teams know their security posture and focus on addressing prioritized security Issues that plague them.

The best way to optimize segmentation is by starting with one level of project. This involves creating a parent project under which child projects can be developed. The secret with Wiz Projects is to keep segmentation simple. If things are getting complicated, it's time to reassess your methods.

Wiz also lets you define policies by project. For example, you may not want the same level of severity between a development project and a critical production project. What's more, Wiz integrates with your ticketing or messaging ecosystem, including Jira, ServiceNow and Slack, to automate ticket generation by project. To do this, you'll need to define automation rules and scope them by project according to your own needs.

Wiz provides role-based access to cloud security features. Therefore, it's important to understand Wiz roles and map them to your existing IAM groups. SAML role mapping is the optimal path toward using role-based access controls (RBAC) in Wiz. Use a single sign-on (SSO) identity provider to help mediate the complexities of role-based access. This can help seamlessly designate Wiz roles for existing user groups within the organization. SSO is the ideal way to simplify access management and create a sturdy foundation for cloud security. Wiz supports all SAML 2.0 compliant Identity providers (IDP). While it's important to embed security into every sphere of your organization and empower every team with self-serve security capabilities, your security teams — including SOC (Security Operations Center) and IR (Incident Response) — need to have a global view of your cloud estate.

Outcomes

The completion of these tasks will enable you to:

- A complete overview of connected environments
- Know all the technologies used in your environment, and begin to identify which are approved and which are not
- Get the full context of your cloud, so you can easily search for workloads in any cloud
- Think about the next steps, including which services will be scanned by Wiz next
- Have a breakdown of roles by security team, so that each team can have a complete view of what matters to them.

Now it's time to reduce the risks, which we'll do in the next step.

Step 2: Reducing risks

Now that your cloud environment is visible to you, it's time to reduce the degrees of risk it poses. This step focuses on minimizing risks and overall time to remediation by focusing on what matters the most, using Wiz prioritization queue, integrating with your technology stacks (Jira, ServiceNow, Slack, SIEM, and more), and tightening your compliance posture.

Educate your team on Wiz Issues

Wiz's approach to risk is very different from what teams have used previously. Indeed, as each team had its own tools for vulnerabilities, misconfigurations and so on, it was difficult to understand which risks should be prioritized.

Wiz introduces the notion of outcome. It's no longer just a question of relying on a vulnerability's CVSS score to determine whether remediation of that risk is a priority, but also looking at whether the workload where that vulnerability is located is also publicly exposed to the Internet.

Therefore, it's important to educate teams so that they understand the importance of each Issue.

But first, let's explain what an Issue is. An Issue is the result of controls or critical/high threat detection rules, or cloud configuration rules (CCRs) that were selected to function as controls. A control is a graph-based query defining a combination of risks, called toxic combination, and its associated severity (for example, a publicly exposed VM instance with effective global admin privileges). On the other hand, critical/high threat detection rules generate Issues based on abnormal behavior detected in near-real time.

Fig 4 – Wiz's attack path visualization

To develop a better understanding of the severity of issues, there are of course classic training courses, such as videos, tutorials, instructor-led training, etc. However, we also recommend training your team about issue severity using a gamification approach with a hands-on work session in a dedicated environment. This will enable them to learn directly on the Wiz platform, and to experience real-life risk situations in a secure environment.We recommend holding a session every quarter to keep abreast of new capabilities and other use cases.

Improve security posture

Your company's cloud environment is susceptible to a multitude of risks including misconfigurations, insecure APIs, blind spots, and external threats like malware and supply chain attacks. Wiz prioritizes these risks by relentlessly contextualizing them with business, cloud, and workload-specific factors. By considering such a comprehensive range of contexts, you will be able to use your cloud security resources on the risks that matter most to your organization. But how do you navigate this?

You can quickly feel overwhelmed by the number of Issues you have in your environment. This is quite normal, as we're used to having thousands of alerts on vulnerabilities or misconfigurations in the cloud without knowing where to start.

Because Wiz identifies the most important real risks in your environment, we recommend that you start by remediating the most critical Issues. Once these have been resolved, you can continue with the high severity Issues.

Medium and low Issues can be dealt with in the background when teams are less busy.

Initially, we recommend remediating Issues manually, to understand how to do it and the different steps to follow. Once the remediation process is in place and proven, we recommend that you automate the remediation, starting with the simplest, lowest-risk tasks. How do you determine whether an Issue is a good candidate for automation? When it's a frequently recurring Issue that's easy to remedy, such as a bucket that doesn't use a customer-managed encryption key.

Reduce time to remediation

Remediation can involve various methods including patching outdated software, right-sizing privileges, and addressing misconfigurations. The best way to reduce time to remediation is to focus on key areas instead of dedicating time and resources to isolated incidents that may not have critical implications. Identify which risks may affect your company's primary activities and compromise your crown jewels. Focus on those first.

If you identify a cloud security risk that needs to be remediated by another team, it's essential to create a ticket to share security-related information. Wiz's integration platform allows you to generate tickets and messages to share with other existing services, including Slack, ServiceNow, PagerDuty, Google Chat, and Jira. These Wiz integration capabilities, coupled with a comprehensive list of renowned partners, can help you red-flag critical risks and optimally route them toward remediation.

Remember that your security teams will typically handle initial security remediation and triages. The secret to long-term success and democratization of security is to define robust automation rules. Automation rules will help route security risks to the right teams, enhancing the speed and quality of remediation efforts and eliminating manual interference.

SLAs are another key ingredient for reducing time to remediation and strengthening shared responsibility security models. Wiz can help define and optimize SLAs. Wiz analyzes diverse contexts to reveal the business impact of your IT resources. Therefore, it will ensure that your most critical applications have shorter SLA timeframes (like 24 hours), whereas medium and low-risk resources might have 7-day or longer SLAs.

Prepare the next steps

Risk reduction is essential because it eliminates major events like data leakage and unauthorized access to your cloud estate. Diving into more complex branches of cloud security without addressing gaping critical risks is a recipe for disaster. Most organizations have finite security bandwidths. Never spread yourself too thin. With security, start with the basics: address the obvious and most high-risk Issues first, and then methodically fine-tune and optimize.

Having improved visibility and reduced the degrees of risk your organization holds, you can now think about what's next. The order of priority is up to you. These include analyzing the current state of your cloud security posture and planning how to optimize IAM posture, container and Kubernetes security, cloud and threat detection and response, patch management and data security.

Outcomes

The completion of these tasks will enable you to:

- Have security teams trained on Wiz Issues and capable to understand why an Issue is critical
- Understand the security posture and where to start in terms of remediation
- Build a comprehensive workflow, enabling security teams to automatically triage Issues and send them to the right team
- Define clear Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) that can be tracked to ensure that the security program is running smoothly.
- Achieve zero critical Issues in your environment.

Step 3: Democratization

Your DevOps engineers and key IT personnel shouldn't waste valuable time and resources to remediate security threats and misconfigurations that are non-critical. Cloud security capabilities and information need to be available, accessible, and digestible for all users within your organization. This makes democratization a vital element in your cloud security operating model plan. Below are the best ways to make that happen.

Provide Self-Service access

As we saw in one of the previous sections, Wiz allows you to separate cloud and Kubernetes environments by setting up projects. This step takes us to the next level: integrating teams who are traditionally outside security. By combining SSO, RBAC, and projects, it's possible to open up the Wiz platform and authorize its use in self-service mode, and also to associate a level of criticality to each project.

Before fully opening up the platform, ask yourself the following questions:

- How should projects be organized? By team, by application, by business line?
- Do I need to define a project manager? If so, who?
- How do I define project criticality? What are the criteria?

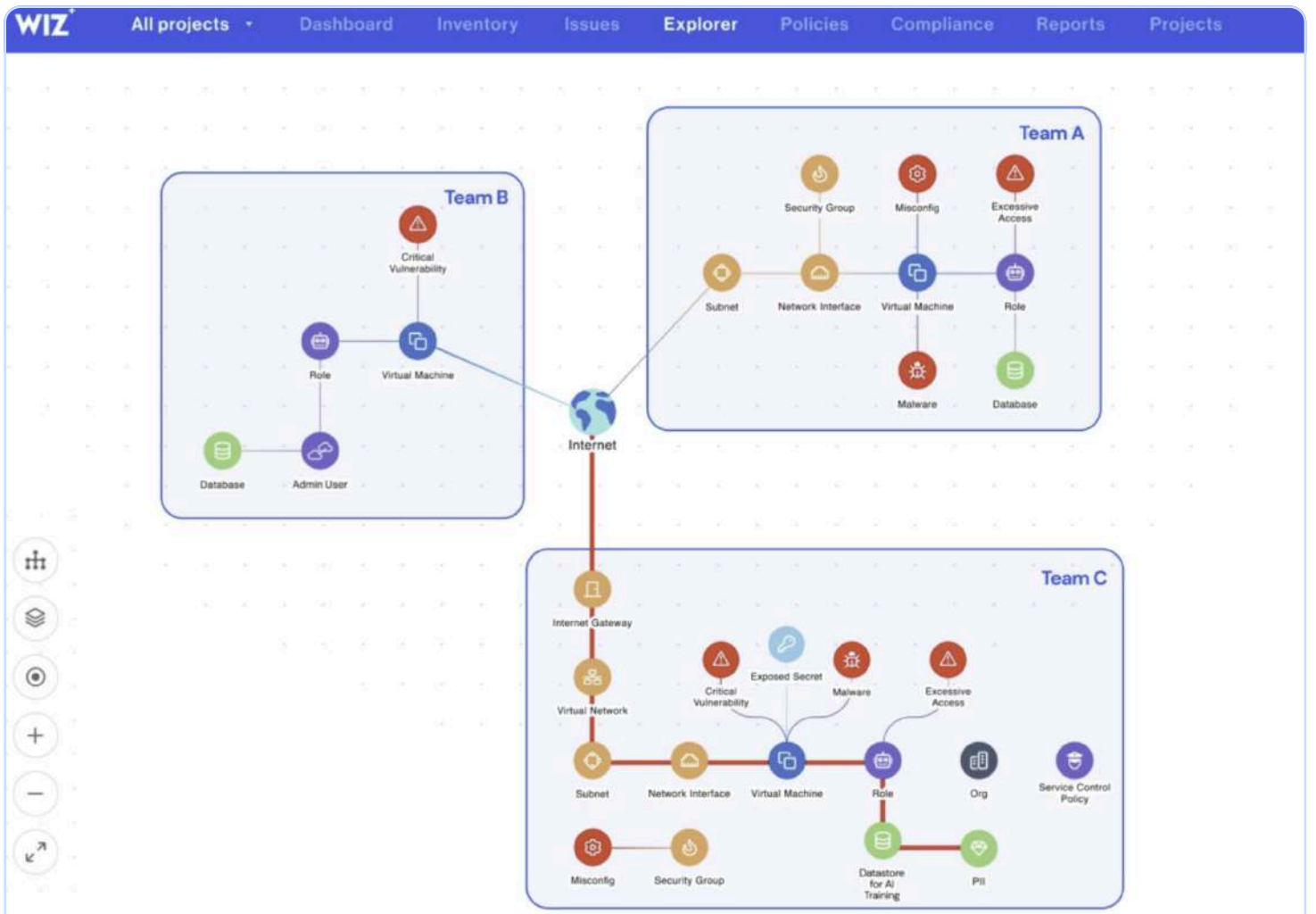

Fig 5 - Wiz's Projects

We recommend that you structure the definition of projects according to your organization's needs. However, we advise you to strike a balance between complexity and maintainability. You don't want to create technical debt, for example.

To automate the process of onboarding a new team, we recommend that you use the terraform provider and create a module so that this step can be controlled and repeated at will.

Define standards and best practices

Wiz offers more than 2000 cloud configuration rules for numerous frameworks including CIS, NIST, and PCI. At an OS and application level, Wiz boasts more than 10,000 host configuration rules as per CIS Benchmarks for Red Hat Enterprise Linux, Ubuntu Linux, Nginx, and Microsoft Windows Server. To fully democratize cloud security, Wiz enables an organization's users to customize policies (CCRs, HCRs, Data Classification Rules, etc.) and create ignore rules according to their needs and specificities.

This flexibility makes it possible, for example, to define severity levels by environment, or to ignore misconfigurations because they are known and the logic behind ignoring it is internally documented.

You can set up custom policies with a few simple clicks. As an example, let's describe the creation of a custom host configuration rules. Wiz allows you to select target platforms, which are applications and operating systems you might want to assess. For example, you may choose Nginx, Docker, or Ansible as a target platform. After choosing a target platform, Wiz leverages an OVAL schema called Direct OVAL language to help generate rule definitions. You can also include more detailed metadata in the form of rule descriptions. These custom rules can be paired with built-in and customized compliance frameworks.

For those well-versed in writing custom rules, it's easy to remove and ensure complete visibility. For those new to custom policies, Wiz provides comprehensive walkthroughs, ensuring that all users have fundamental cloud security capabilities.

Now it's time to identify the company's compliance constraints:

- What regulations is my company subject to?
- What standards do I want to implement?
- Does compliance have to be applied on a global level, or just to certain projects?
- Do the controls provided by Wiz meet my needs? If not, what controls would you like to add?

To further democratize cloud security, take advantage of Wiz's integration capabilities to connect it with the rest of your system. Ensure that Wiz reaches cloud services from all your providers, SIEM and SOAR platforms, and a range of other security and compliance tools. Bi-directional intelligence sharing should be a vital part of your cloud security operating model.

Improve compliance posture

Compliance has always been a challenge, but multi-tenant cloud environments present regulatory hurdles like never before. Wiz allows you to evaluate your compliance posture by leveling it against numerous federal and industry-specific regulations such as GDPR, CIS, HIPAA, and PCI DSS. Wiz provides more than a hundred built-in frameworks to choose from. If you're in an organization with specific or highly compliance requirements, Wiz provides custom frameworks for you to configure manually. Alternatively, you can duplicate built-in frameworks and reconfigure certain aspects as needed.

Wiz's compliance capabilities include easy-to-follow boards, visualized heatmaps, and granular and flexible reporting, all of which can help you evaluate your compliance posture at micro and macro levels. The reports can help various teams assess the compliance posture and periodically give senior management and other stakeholders a window into their organization's adherence to external regulations.

Build customized dashboards

It's impossible to effectively democratize security unless every team has direct access and visibility into the security issues and information that matter to them. Initially, Wiz's default dashboards will be the perfect solution to serve your teams. However, as your operating model matures, it's important to create customized dashboards that address the growing security needs and intricacies of different teams.

Security teams could also collaborate with other branches of your organization to create a comprehensive catalog of organization-specific dashboards and widgets that all users in the cloud estate can easily access and integrate.

Simplify audits

Audit processes can be long and tedious. Most of the time, it's about demonstrating that you meet the auditors' requirements. To do this, you use different tools or internal processes, which is time-consuming and often requires a lot of back-and-forth with the auditors.

Wiz allows you to visualize where you stand in terms of compliance posture, and to go into detail for each category if necessary. It is also possible to export data in the form of reports or raw data for transmission to auditors, thus speeding up the audit process.

Outcomes

The completion of these tasks will enable you to:

- Provide a self-service that can be consumed by all teams in the organization
- Have well defined standard and best practices associated with your needs
- Have a better understanding of your compliance posture in regards on your regulation needs
- Define a library of custom boards that could be reuse across the organization
- Respond quickly and easily to a compliance audit

Step 4: Shifting left

Once you have democratized cloud security, it's time to reassess and reconfigure fortifications across your SDLCs. Historically, businesses have often neglected security in the early stages of SDLCs, leading to the hidden mushrooming of security risks. This step guides you in avoiding the maturation of potential risks based on misconfigurations, vulnerabilities, hard-coded secrets or sensitive data and any corresponding long-term damage by remediating risks in the initial stages of SDLCs.

From a developer perspective (IDE and VCS)

The sooner you scan the code for risks, the better. That's why Wiz can be integrated as an extension/plugin into your developers' IDEs. The aim is to identify misconfigurations, vulnerabilities, secrets or sensitive data in application or infrastructure code as early as possible. We also recommend that you set up pre-commit policies to prevent a secret from ending up in a code repository.

But of course, this isn't enough. Developers and DevOps use version control systems to store the code they produce and be able to collaborate. That’s why, it's important to have an overview of the repositories and the associated code. It's essential to understand how they're architected and what developers are doing before you start anything.

The first step is to get visibility, which is why you need to use the Wiz connector for VCS (Github, Gitlab, Azure DevOps and Bitbucket). And rather than trying to make a big bang and implement rules across all repositories, it's best to do it step by step. To do this, we recommend that you identify one or two teams with whom you can work closely to define and validate the strategy to be implemented. You start off in audit mode to understand developers' habits and show them what needs to be changed in their methods. Once you have a good understanding, it's then possible to switch to block mode, with the teams' approval. After this phase, you can onboard other teams to achieve complete coverage.

Secure your CI/CD Pipeline

The second step is to protect CI/CD pipelines from build to application deployment. As in the previous step, Wiz will scan the IaC code and also the images once they have been built. This makes it possible to use Wiz in conjunction with the CI/CD pipeline to create golden images, whether for virtual machines or containers. In this way, you secure your images at build time, rather than once they're in production. Wiz integrates with all the majors CI/CD platform in the market, making it easy to add in your existing ecosystem.

Finally, to provide a last line of defense for containerized environments, it's important to think about setting up an admission controller. It is simply deployed through a helm and can therefore be part of the Kubernetes cluster deployment process. We recommend using a GitOps approach to ensure that the admission controller is automatically deployed at all times.

The admission controller will enable you to check images and application configuration before they are deployed on the cluster. If they don't meet your criteria, it can either audit them, giving you a complete overview of deployments on your clusters, or block non-compliant applications from being deployed.

Note: Although the pipeline scan and admission controller are totally independent, we recommend that you implement them together for complete protection from build to deployment.

Once this has been done, as we explain is the previous step, we recommend that you implement the policies in audit mode, so that developers can understand the changes to come and, above all, understand the potential impact this could have on their pipelines.

Once feedback has been collected, you can then activate pipeline blocking in the event of non-compliance with security standards and best practices. This will enable you to fine-tune your onboarding process and establish the training and communication plan needed to onboard other teams.

Indeed, for this to be adopted by the teams, it's important to educate them rather than monitor the smooth running of the pipelines. When development teams are ready, you can then activate blocking in the event of non-compliance with safety standards and best practices.

Automate and extend

The key to sustainable and effective long-term Wiz management across disparate cloud resources is to automate wherever possible. Wiz should also be integrated with your SOAR platforms like Cortex XSOAR, Torq, Blinkops, and Opus. The best SOAR platforms offer easy, limitless integrations and thousands of no-code automation options that can help build robust security workflows and optimize remediation playbooks.

Outcomes

The completion of these tasks will enable you to:

- Scan code early in the SDLC with IDE integration.
- Have a very good understanding of your repos and how developers manage code.
- Establish a well-defined workflow that you can replicate throughout your organization.
- Add guardrails in your CI/CD pipeline and learn from them to improve your security posture.
- Define and measure key performance indicators to ensure that your strategy is working as intended.

Step 5: Shifting Right – CloudThreat detection and response at runtime (CDR)

Remember that shifting left is not about transferring security emphasis from runtime to build. Instead, view it as a tactic to ensure security equity across your SDLCs and address vulnerabilities as early as possible. By doing this, only the most potent and concealed threats may seep into the runtime. This last step focuses on how to secure runtime and address those latter-stage risks.

Onboard your SOC and IR teams into the operationalization of threat detection that's linked to your cloud environments. The logic behind this is simple: Wiz generates and analyzes an abundance of highly relevant, business-specific contexts. In the hands of SOC and IR teams, this bounty of security information can help reduce remediation time and simplify forensic operations after security incidents.

Because Wiz provides a complete view on a single platform, onboarding the SOC and IR teams not only reduces response time in the event of a breach, but also automates a number of forensics-related processes.

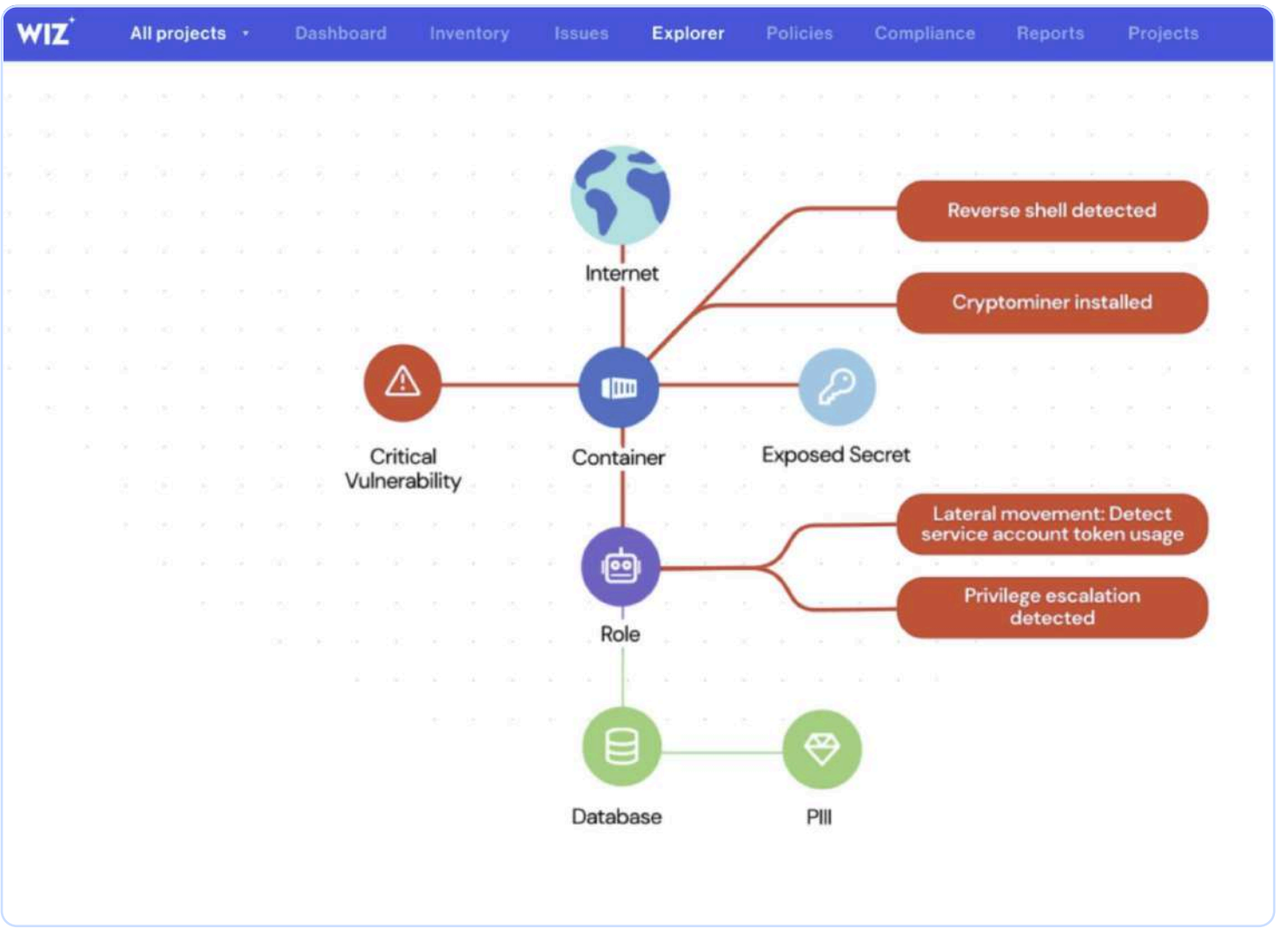

Fig 6 – Wiz's CDR with context

But first, it's important to define a workflow to clearly identify who's responsible for what. This means defining which team is responsible for each step. To help you do this, we propose the following workflow:

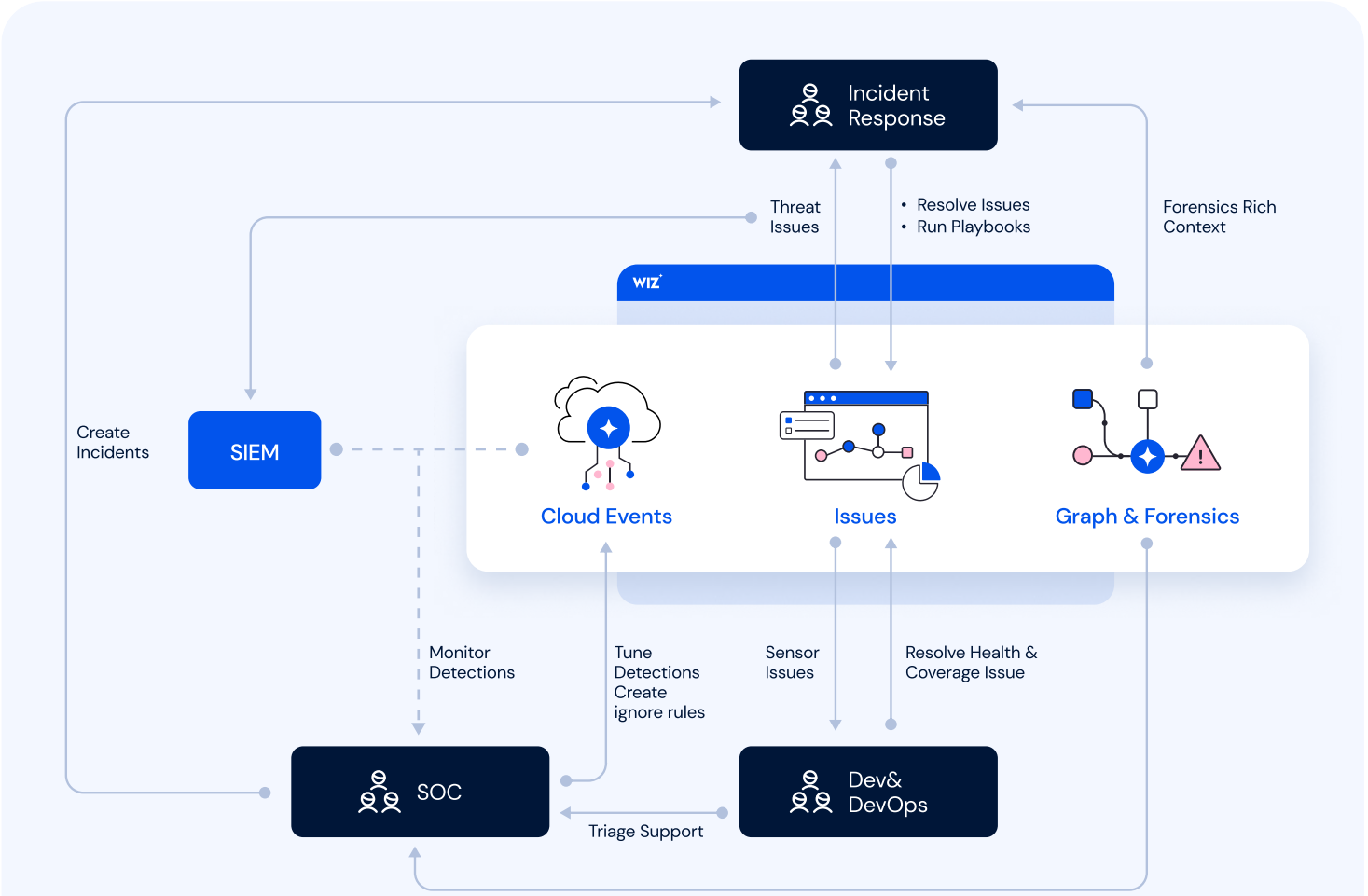

Fig 7 - Example of workflow

From a technical point of view, we recommend setting up a dedicated forensics account. This will enable the teams in charge of investigations to be autonomous in creating snapshots and retrieving logs from the suspected machine. This saves a considerable amount of time and, above all, removes the burden from cloud teams.

Finally, to help you understand where you stand in relation to your incident management, Wiz provides a framework, among others, called Incident Readiness. This framework will enable you to identify where necessary measures, such as log activation or sensor deployment, have not been put in place, reducing your preparedness in the event of a breach.

Outcomes

The completion of these tasks will enable you to:

- Onboard your SOC and IR teams to your global security program
- Reduce the mean time to detection and response
- Define a workflow and a clear RACI of who is responsible for what
- Have a clear understanding of your incident readiness

Continuous improvement

The best cloud security operating models are iterative. You should never be fully satisfied with your cloud security posture. Instead, you should continuously find ways to improve and optimize cloud security protocols and practices. The best way to do so is by evaluating the following points.

Platform usage and incident resolution

Your Wiz platform is an information goldmine. Constantly monitor platform usage and incident resolutions to form a high-level understanding of persistent cloud threats and corresponding remediation strategies. Assess why certain risks have been prioritized over others and how those risks have been mitigated. Even successful remediation efforts should be put under the scanner and analyzed critically to find areas for improvement.

In addition to deconstructing remediation efforts and incident resolutions, keep an eye on how various teams within your organization are using your platform. Ask yourself whether certain core features are being under-utilized and whether your Wiz solution is having a measurable effect on your organization's cloud security posture and digital acceleration. Frame and implement a specific set of KPIs to evaluate progress. Optimize where necessary.

Feedback from users

Successful democratization of your cloud security operating model will likely result in every member of your organization being responsible for the security of their respective cloud provinces. Feedback from them can be a game-changer. To get accurate and consistent feedback from your users, champion a culture of open communication, schedule periodic reviews, and strengthen the threat intelligence sharing ecosystem in your organization.

User feedback can provide a range of insights that can help security teams, developers, and the C-suite sharpen their cloud security posture and leverage the Wiz platform to its fullest potential. Your feedback ecosystem also needs to fold in and acknowledge certain exceptions. To do this, you must create feedback loops, which are channels for various teams to communicate.

One way of taking feedback into account is to implement Ignore Rules. These rules allow you to exclude findings on cloud configurations, vulnerabilities, sensor and cloud detections, and more. In this way, you can reduce noise to scale by ignoring known or expected security risks and events.

Training for security teams, users, and newcomers

Even the most effective cloud security solutions like Wiz are only as good as their implementation. Therefore, it's important to train in-house security experts, users, and newly onboarded employees to make sure that Wiz's platform is being leveraged consistently and appropriately. Remember that user feedback and platform usage analytics are critical to maintaining healthy cloud security hygiene. Therefore, suboptimal usage of your Wiz platform will directly result in inferior cloud security intelligence and reporting.

Training programs shouldn't be a one-time occurrence. Like every aspect of your cloud security operating model, training programs should be improved, updated, and broadened in scope regularly. If security training programs feel like a chore, it can have serious implications on your cloud security posture. Gamification is a simple and effective approach that can make security training a more accessible, inclusive, and fun experience for your employees.

As adoption increases, the cloud will continue to pose more complexities. Continuous improvement of your cloud security posture is the only way to ensure long-term digital success and resilience to defend against an ever-evolving list of dangers.

Conclusion

Implementing a new operating model for cloud security is a whole project. And as no two organizations are equally prepared to tackle cloud security, cloud security maturity levels can vary dramatically. That's why it's important to go step by step, and to define achievable objectives to ensure success. Wiz's cloud security platform, coupled with a robust cloud security operating model, can provide organizations at any level of cloud security maturity with a roadmap toward agile growth and complete fortification against cloud risks.

Wiz is at your side to accompany you on this journey. And following the recommendations and cheatsheet in this guide will help you achieve your goals.

Would you like more information or do you have any questions? Contact your sales team or customer success manager.