
# *Operationalizing Prisma Cloud for SOC / IR*

Palo Alto Networks, Inc.
www.paloaltonetworks.com

# Table of Contents

## Introduction

This guide provides direction, advice, and recommendations for putting Prisma Cloud into operation in your environment. The guide is based on the extensive experience of our Customer Success Team, which onboards all customers, advises them how to best secure their environment, and helps them to configure and deploy Prisma Cloud to meet those objectives.

The guide is presented as a timeline-based journey that starts at day zero, when you've purchased the product. We offer the timeline to help you plan for the work ahead and measure your progress.

Our Customer Success Team is always available to assist you, and we encourage you to contact us. We can give you advice about how to deploy and operate Prisma Cloud in your environment.

## Roles

Prisma Cloud is a collaborative tool. You will get the most value when representatives from DevOps, SecOps, SOC/IR, and Compliance actively participate in planning and operations. When teams work in silos, the CI/CD pipeline will be disjointed and exasperating. When the teams are aligned, your CI/CD pipeline will be fluid and frictionless, with security controls transparently governing the flow

The personas are defined as:

- DevOps: Understands the infrastructure. Understands the environment's topology. Develops, remediates, and deploys assets in cloud accounts. Technical owner of cloud assets.
- SecOps: Has the expertise and authority to sign off on policy decisions. Understands policy structure. Analyzes and interprets audit data.
- Security Operations Center/Incident Response (SOC/IR): Understands relationships between components. Investigates activities and recommends remediation or policy modifications. Helps Security tune the models that protect running software.
- Compliance: Has the expertise and authority to sign off on compliance decisions. Understands compliance requirements. Acknowledges and recommends policy modifications based on mitigating controls or risk acceptance. Analyzes and interprets compliance reporting data.

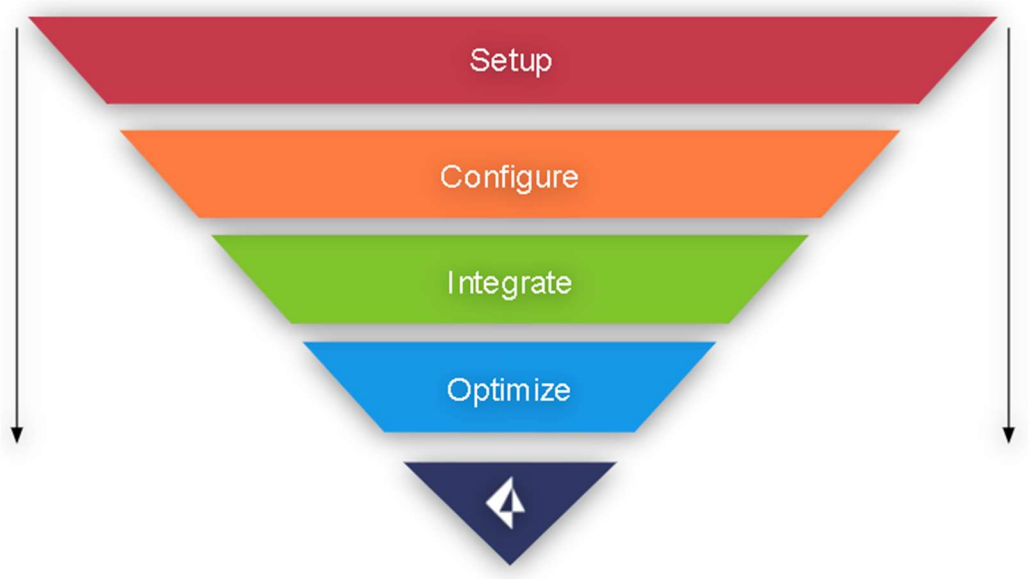
Typically, one group "owns" the Prisma Cloud tool, and it tends to be SecOps.

DevOps, Compliance, and SOC/IR are not generally granted elevated access to Prisma Cloud Console. Rather, they should be granted read-only access to areas of the product for which they will be responsible. Prisma Cloud provides several roles that provide different levels of access to the product, as along with the ability to limit the scope of visibility to a group(s) of Cloud Accounts.

Because DevOps and SecOps start working with the tool from day zero, they're the first to grasp concepts and workflows. The closer those two groups work, the better your results will be, with faster time to mitigation and shorter service interruptions. Schedule regular meetings with DevOps to discuss expectations, demonstrate how Prisma Cloud works, and decide how it fits into their workflow.

## Methodology

Palo Alto Networks utilizes a four-phase methodology for operationalization. The following dedicated sections discuss the considerations, trade-offs, and strategies for working through each step. Links to detailed articles on our Documentation Portal are provided throughout.




### Setup

Familiarize yourself with the application. Inventory cloud accounts need to be secured, and users need access to the platform and their functions. Onboard them to the Prisma Cloud platform.

### Configure

Configure, enable, and customize Prisma Cloud policies. Familiarize yourself with and customize compliance requirements.

### Integrate

Configure integrations with 3rd party security tools and SOC workflow tools. Configure alert workflows for notifications and remediation.

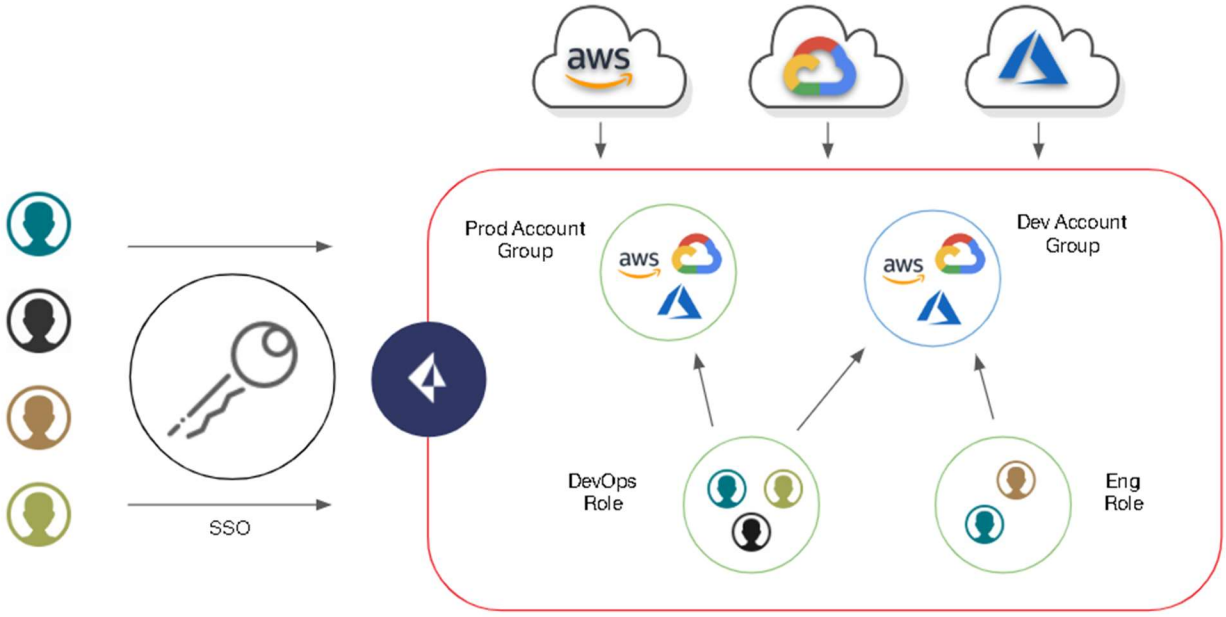
### Optimize

Ensure end-to-end adoption of the product and full utilization of Custom RQL, Automated Remediation, UEBA, and Compliance Reporting.

## Setup

Understanding of the application and the platform is integral to full utilization of all its capabilities. To aid in educating yourself and your team, please review our digital training course: EDU-150: Prisma Cloud Digital Learning. Register for access here.

Review the Administration Guide, which contains all our documentation for managing, configuring, and implementing all features in Prisma Cloud.



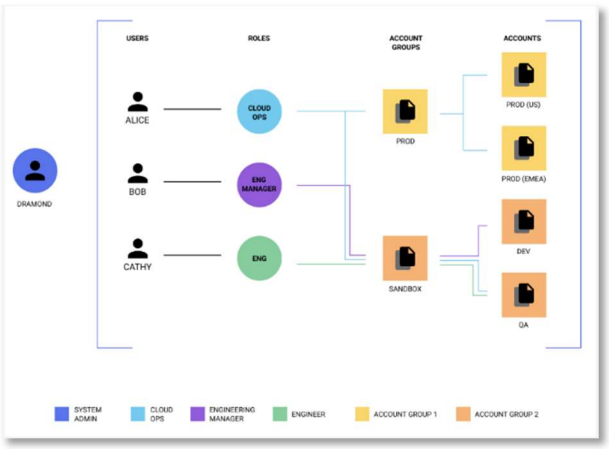

### User Access

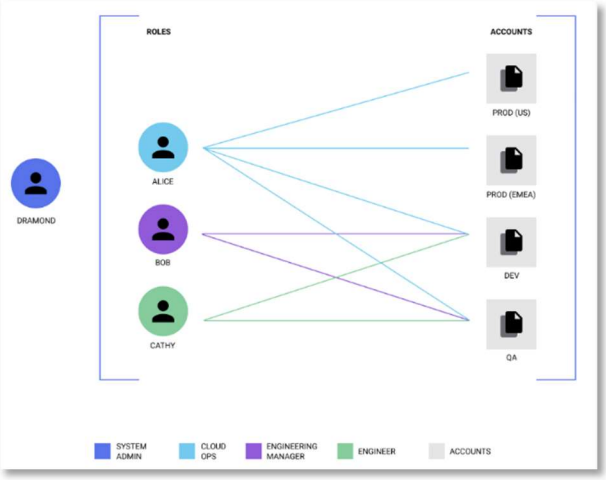
Prisma Cloud supports integration with enterprise directory services and identity providers so that you can simplify and secure access to Platform. Users will receive access details from their SecOps/Security team once they have been granted access to the system.

SOC/IR users will have access to review alerts and query against assets within the accounts they have been granted access to. Cloud Account visibility can be customized and defined by the SecOps or Security Team.

Confirm you can access the platform, and have access to the Cloud Accounts you are responsible for. Ensure you are familiarized with the Compliance Section of the Platform.

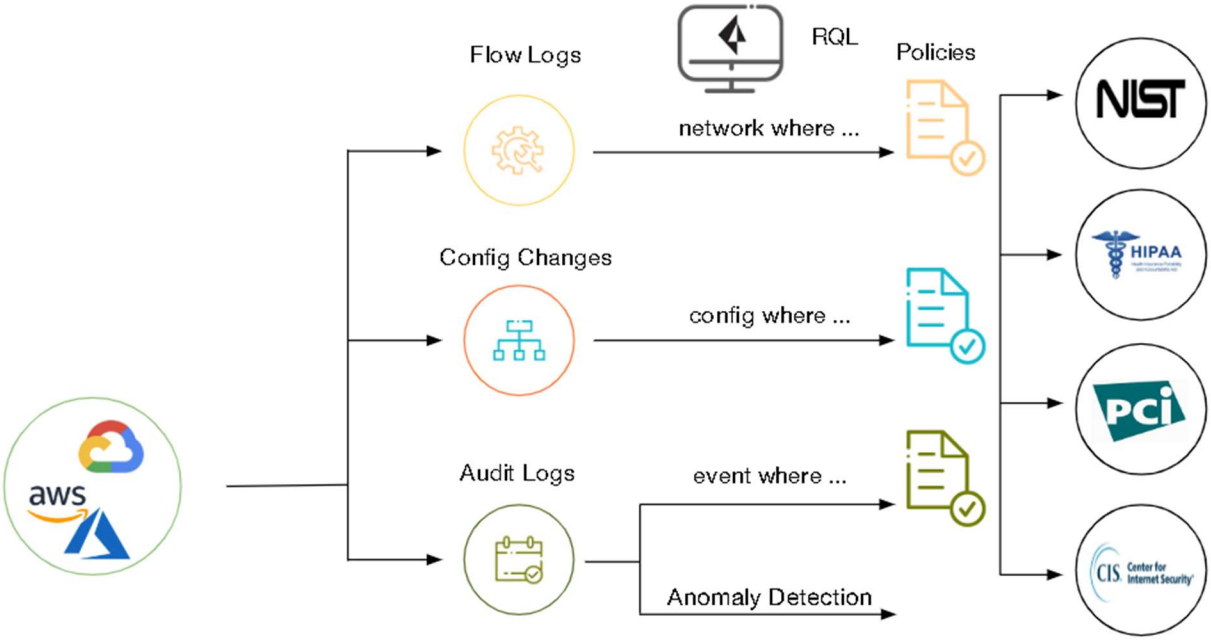
Below can be used to conceptualize RBAC in the application.




## Configure

After you complete your planning and onboard your cloud accounts, you may begin to see alerts within minutes. More than 200 alerts per cloud account often are seen. In this phase of the process, you will begin curating what you want to see or mitigating the controls that are in place. Ensure that proper compliance reporting is in place, and that alerts are going where you want them to go.



## Baseline

After you review the alerts that are generated, you should first identify which policies align most closely to your current security posture. Do you have a set baseline for security measures? Do you have a compliance mandate?

You must know which policies and/or security guardrails need to be in place. This knowledge requires preparation and clear guidance. Are there key areas that you need to implement immediately?

You will want to disable policies that are not currently required and to enable policies that need to be implemented to meet your immediate needs. There are a few items to note during this time:

- Audit alerts may be extremely noisy. They alert based on activity, and are broad by default to include activities such as all IAM modifications. You should disable these alerts until you tune them.
- One Audit policy should be kept enabled, "Root user activities." This policy provides alerting whenever activities are done as the root user.
- Anomaly detection requires a training model period in which the system consumes the user activity to "learn" the "normal" behavior of a user. During the training model creation, no anomaly alerts will be generated.

## Customization and RQL

During the baselining of the policies you may identify some alerts/policies that don't provide exactly what you are looking for, don't take into account other mitigating controls, or include accepted risks.

You can use the RQL reference as a guideline to clone and customize existing policies to suit your needs, or to develop internal policies to provide capabilities beyond standard security requirements. Some common use cases for customization can be found in our RQL Example Library.

## Workflows

The platform's goal is to get the alerts that are generated to the correct team to mitigate or take action. These goals are accomplished using a matrixed alert rule system to map the accounts and alerts that you want to generate, and then to determine where they need to go. Alert rules allow for extremely customized workflows to ensure that all necessary resources are engaged accordingly and in the manner that best suits their normal operations.

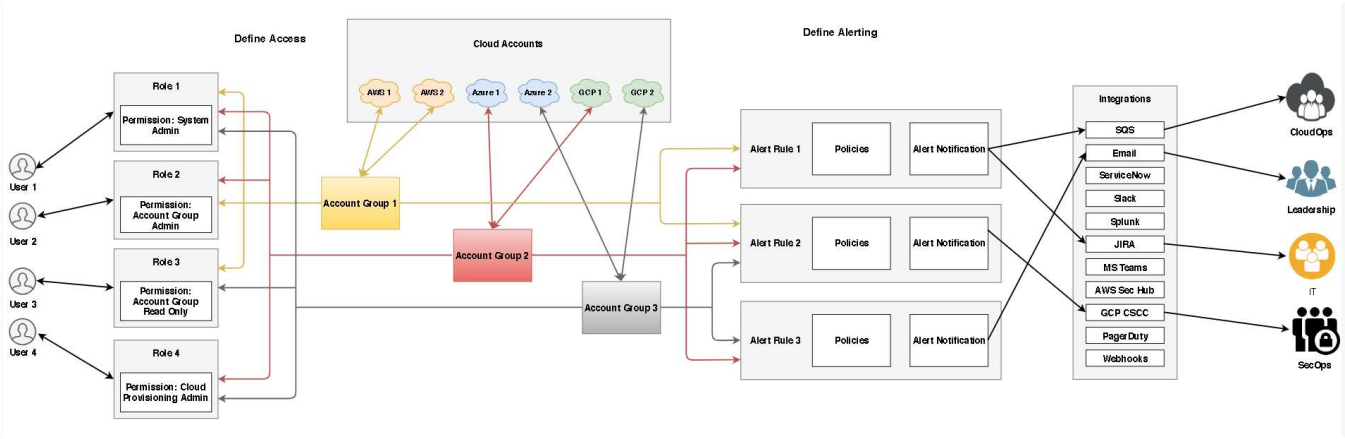
Here is an example of a common implementation workflow:

1. All alerts from accounts A, B, C are sent to the SecOps team for visibility via email in a daily digest.
2. Config alerts from accounts A and B are sent to Jira and assigned to John Smith, who is the account owner, immediately upon detection, so he can assign team members to remediate.
3. Audit/network/anomaly alerts from accounts A, B, and C are sent to Splunk, where the SOC automation determines the proper resource to engage for investigation, and validation of the incident.
4. High-severity alerts are sent to the executive management team via email in a weekly digest for review.
5. All alerts from account C pertain to a sensitive environment, and thus are sent to a tiger team via PagerDuty to ensure immediate action on any asset/activity in this account.

Alert rules are extremely powerful, but you should remember the following points when you create a workflow and plan how alerts will be disseminated:

- Alert rules are the method in which you can scope the account and region boundary for an alert. If an account or region boundary is set in the RQL for a policy, it is ignored when processing alerts.
- Alerts will trigger only if at least one alert rule applies to the account/policy combination.
- Alert rules for use with ITSM tools (Jira, ServiceNow) require an additional notification template to be configured.
- Multiple alert rules may apply to a single alert.
- Alert rule modification will not affect prior alerts. Only newly generated alerts will follow the updated workflow.
- If automated remediation is used, you will not receive a notification through any matching workflow for an alert that successfully is remediated.

The following workflow diagram depicts the relationship from users through alert rules:




## Alert Mitigation

Key items to consider when reviewing alerts are as follows:

- You can't immediately begin to look at all of your tech debt for immediate remediation.
- Focus on the "now." Don't feel inundated by the number of alerts. Focus on the new alerts generated in the last one to three days.
- Begin modifying your CI/CD pipeline and internal processes to ensure that deficiencies are caught before being released into the cloud.
- Work your way back to all open alerts.
- An additional strategy is to look at several types of alerts for activity and address them holistically/systemically. Examples are high-severity/low-impact alerts, low-effort/low-impact alerts, etc.

Additional resources are as follows:

- How to Create an Alert Rule
- How to Create an Alert Rule with Automated Remediation
- How to Create an Alert Rule with Third-Party Integration

## Integrate

After you have tuned your alerts, you should utilize Prisma Cloud to tie into existing security processes to reduce the time of adoption of the product and increase the value of your investment.

Prisma Cloud has two fundamental types of integrations, which are described in the following sections.

### Inbound

This is used for additional data ingestion, and correlation of third-party intelligence streams. (Qualys, Tenable.io, AWS GuardDuty, and AWS Inspector).

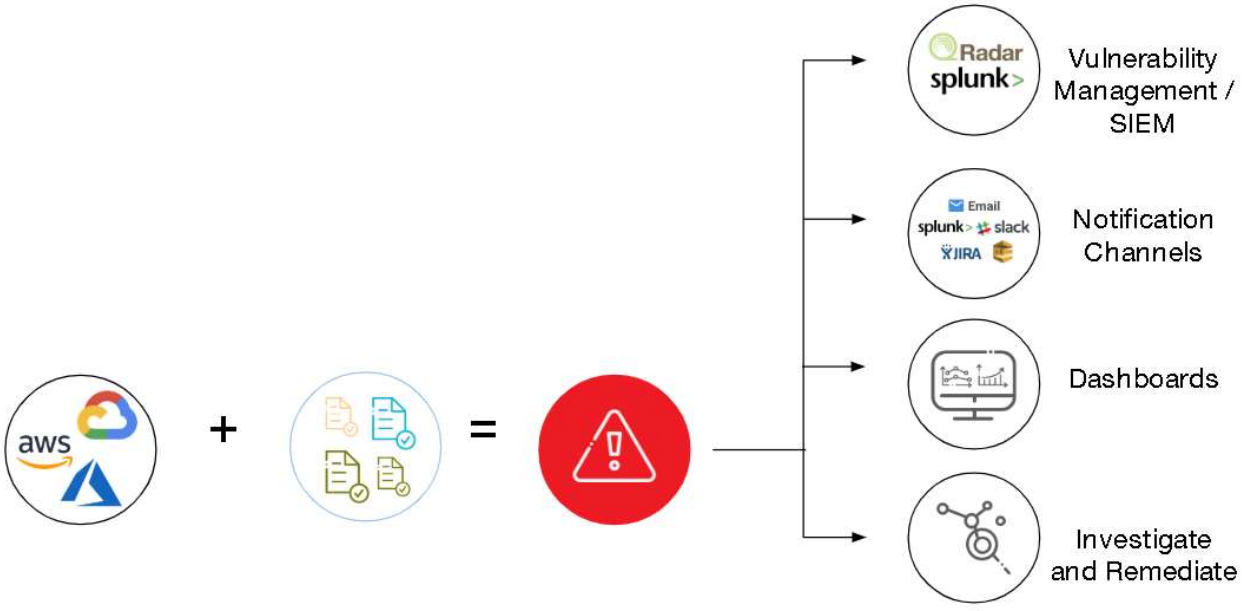
If inbound ingestions are allowed, you can utilize that 3rd third-party data to further refine your policies. These refinements can allow you to see current activity and to identify whether there are additional risk factors that should elevate the visibility of the alert to your teams.

For example, the presence of a network alert that identifies accepted inbound traffic from the internet or suspicious IPs is a concern. But if that traffic was on port 22, and that system is currently flagged as being vulnerable to CVE-2019-6111, concern is even greater. The issue should be mitigated immediately and you should confirm whether there was any compromise.

### Outbound

This is used for dissemination of alert data to third-party systems. These outbound integrations can be grouped in several ways:

- Cloud Native Security Applications - AWS SecurityHub, Google Cloud SCC
- ITSM Applications - Jira, ServiceNow
- SIEM Applications - AWS SQS, Splunk, QRadar
- Collaboration Applications - Slack, Microsoft Teams
- Trigger-Based Applications - Email, PagerDuty, Webhooks



Outbound integrations are the most common way to increase the value of the Prisma Cloud product. They allow you to do the following:

1. Utilize existing technologies and workflows for your standard security practices.
2. Reduce the need to learn a new product/platform while getting the benefit of Prisma Cloud.
3. Immediately ensure user adoption by not changing the day to day workflow.
4. Reduce time-to-action by ensuring that actionable alerts are directed to the necessary parties instantaneously.

For well-established organizations, these third-party tools already are in place. The ability to direct alerts to the necessary parties is a significant attribute in maturing your cloud security posture. This maturity benefits all organizations, and reduces the need to have a gatekeeper of alerts, which thus reduces overall security management effort and increases efficiency.

Here are the benefits and uses for each type of outbound integration:

- Cloud Native Security Applications: Allows your DevOps team to handle and address issues in a single location, which is the Cloud they are responsible for. This approach means that they can keep their focus in the cloud and not have to learn a new security application.
- ITSM Applications: Allows you to create tickets for tracking automatically. This ability allows Prisma Cloud to integrate with existing ticketing workflows and to utilize existing escalation channels as necessary. The ITSM Applications integration will allow for the tracking and reassignment of activities and give greater visibility for responsibility and time-to-resolution metrics.
- SIEM Applications: Centralized incident/log management is the most common tool in use by security teams globally. This typically is the first step in automation as a security team matures. The inclusion of alert data into your SIEM allows you to create customized workflows and automation tasks that already may have been developed by your teams.
- Collaboration Applications: This integration allows you to easily give visibility to activities in the cloud without necessarily having to give all users access to Prisma Cloud or managing too many roles in the product. Posting to a Slack channel or teams group allows you to quickly disseminate alert information to a diverse and dynamic group in near real-time.
- Trigger-Based Applications: This is the most rudimentary integration. Email notification and PagerDuty have been used since the beginning of security in technology. Crafting of critical page groups and incorporation of incident response into this process allows for minimal lag during time-sensitive activity investigation and remediation.

SOC/IR users typically do not have the necessary access to configure and implement integrations. Coordination with your SecOps or Security Team is necessary for the implementation and utilization of the above integrations.

## Optimize

The purpose of this phase is to continuously cycle through the process of increasing efficiency in incident handling, reducing "noise," and ensuring that you are getting alerts that provide as much context as necessary to enabled you to take immediate action and strengthen your security processes.

After you reach Optimize, you are seeing the full usage and overall value of Prisma Cloud. To ensure that you are getting the full value of the Prisma Cloud platform, you should ensure that you continuously look at completing the following activities at regular intervals throughout the life of your subscription.

### Policy Review

Prisma Cloud releases new policies and RQL regularly. You should review policies at least once per quarter, and perhaps even once per month. This review should include new policies that have been released and existing policies that are not yet enabled. Security is an ever-changing landscape, and as your cloud presence matures, so too, should your security posture.

Key activities related to the policy review are:

- Review new policies for enablement
- Review existing policies and alerts for RQL refinement
- Review disabled policies for enablement
- Review user activities for auditing requirements

### Activity Review

Prisma Cloud is not just a tool that alerts you for misconfigurations or issues. It can easily and automatically take action. It can get the alert to the responsible parties almost immediately for remediation, thus you should identify whether there is value in refining the processes attached to the application to ensure the most efficient handling, and that alerts are being addressed. This activity is best done weekly or biweekly to ensure that processes can be adjusted quickly, as necessary.

Key activities related to the activity review are:

- Review alert trends and determine if autoremediation is applicable
- Review alert trends and determine if a DevOps process needs to be modified/updated to prevent alerts. "Moving Security Left"
- Review time-to-resolution, and the reasons for it. Can it be reduced?
- Review workflows to ensure that responsible parties are getting the appropriate alerts

## Operationalize

In addition to the constant refinement of the policies and customization of the platform, these are common day-to-day tasks expected for the SOC/IR teams that are engaged with the Prisma Cloud platform.

### Enforcement

Once visibility is achieved, you should begin the enforcement of security in the environment. The first and most basic step is to identify what security controls are REQUIRED in the organization. Each organization can vary significantly with its security posture, and security mandates, from moderate to very strict.

To ensure adoption and security adherence while minimizing business impact, you should start with a small subset of policies that are deemed "MUST HAVES." These non-negotiable rules should include the guardrails that are most important to the SecOps team and organization as a whole.

After this list is defined and implemented, hold the responsible parties accountable. This process will ensure that good procedural hygiene is in place and that associated teams will become familiar with the function of the application, and thus gain confidence in its utility and results.

Coordination with teams during this activity is very important. If there is a requirement to be CIS-compliant, your starting point may be just the policies necessary for CIS. If the SOC/IR looks for key activities, you also may want those activities to be included. The general guidance would be to enable no more than 25 to 50 policies initially, unless the requirement includes more.

Management engagement is critical. Highly Successful deployments of Prisma Cloud all have regular management engagement, and in some circumstances Executive sponsors internally to drive a adoption.

### Analytics

Analysis of the activities in the organization is helpful to staying ahead of any threats. Prisma Cloud has several methods in which we aid in bringing that ability to analyze the activity to your attention. We allow you to see the forest for the trees when it comes to activity.

User and Entity Behavior Analytics (UEBA) elevates raw audit data to actionable security intelligence by automatically correlating individual events generated to the learned normal behavior of the user, and raising the alarm when there is deviation. These analytics include but are not limited to unusual activity within the cloud, unusual location activity, and unusual login activity.

Prisma Cloud utilizes machine-learning AI to map a user's normal behaviors and can easily raise to the surface any deviation from that behavior. For example, a user that only manages IAM and then begins to interact with RDS will trigger an alert to investigate. A user that logs in typically from IPs isolated to the southeastern United States but is now seen to be logging in from Asia will generate an alert.

In addition, to the AI capabilities of Prisma Cloud, you can create custom policies to alert when certain high profile/high risk activities occur. This allows swift visibility and ensures immediate analysis and action by the SOC/IR team to determine if activity is malicious or benign.

## Need Assistance?

While this document is meant to give you a solid workflow to onboard, optimize, and operationalize the Prisma Cloud platform. We couldn't fit in everything you need. For that we recommend access some of our self-help repositories.

Within the platform, we have a quick access help center with the ability to get to our status page, LIVEcommunity, technical docs, and our release notes. The help center also contains our protected documentation for our APIs and CLI capabilities. As discussed earlier in the document, they can only be accessed after logging into your Prisma Cloud tenant.

Just look for this icon in the bottom right of your Prisma Cloud Web GUI . 

The With some of references in this document, you are already familiar with our technical documentation, which can be found with all other Palo Alto Networks documentation at https://docs.paloaltonetworks.com/prisma/prisma-cloud.html

Our LIVEcommunity allows easy access the community forum to interact with other Prisma Cloud customers, and technicians. Quickly find the latest release notes, featured articles, and media content all in one place! Need to submit a service request…? That is also available through the LIVEcommunity landing page.