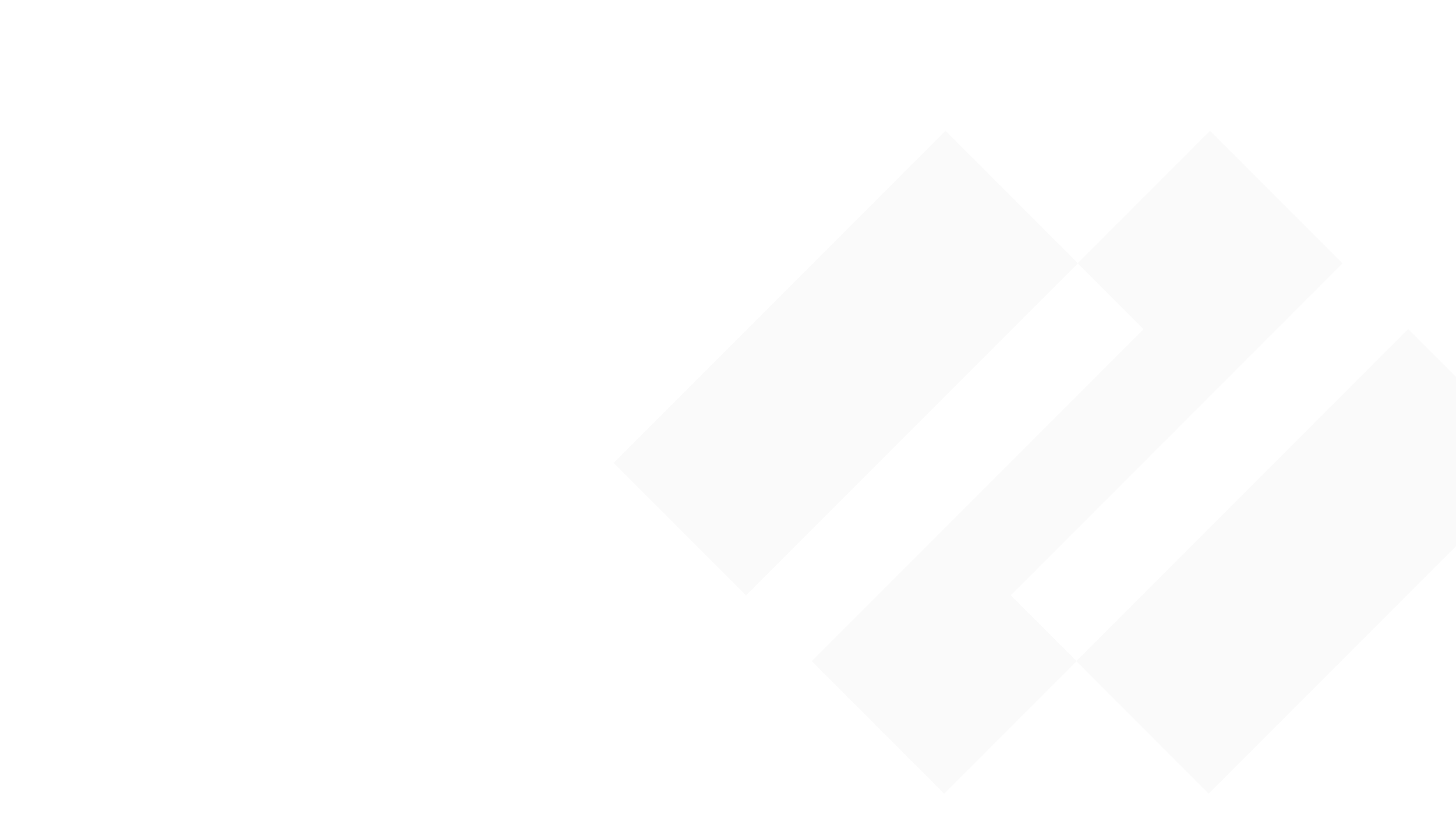
Prisma Cloud Professional Services Maturity Assessment Workshop - Advanced

Prepared for:[Customer Name]

*Workshop Date:* 

Prepared by:

<YOUR-NAME> - Prisma Cloud Consultant

Palo Alto Networks, Inc.

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

© 2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trade marks.html. All other marks mentioned herein may be trademarks of their respective companies.

Confidential and Proprietary Information: For authorized partners and customers under NDA with Palo Alto Networks only.

## **Document Properties**

This document is prepared for the customer [Customer Name].

### **Version History and Contributors**

| Version | Name(s) | Role(s) | Contact Information |
| --- | --- | --- | --- |
| 0.1 |  |  |  |
| 0.2 |  |  |  |

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trade marks.html. All other marks mentioned herein may be trademarks of their respective companies.

Confidential and Proprietary Information: For authorized partners and customers under NDA with Palo Alto Networks only.

## **Table of Contents**

[**Contact Information 1**](#_6tpvtiz3xkj8)

[**Document Properties 2**](#_s16sz3waiuaa)

[Version History and Contributors 2](#_2s8eyo1)

[**Table of Contents 3**](#_534m7ly8jii8)

[**Document Objectives 4**](#_gjdgxs)

[**Customer Information 4**](#_hlug7hvhnkqv)

[**Cloud Security General 5**](#_3z0ph7p6y7of)

[**Prisma Cloud - Cloud Security 9**](#_29g9yzejt3p1)

[**Prisma Cloud - Runtime Security 13**](#_hpfabetea2gj)

[**Prisma Cloud - Application Security 18**](#_ujts8pjmvy1y)

[**Prisma Cloud Automation & Extensibility 21**](#_x1b3ae84q9cu)

[**Recommendations 23**](#_94sibuxhmczw)

[Product Recommendations 23](#_lwu86uixisvn)

[**Roadmaps 25**](#_6y7g95npsi14)

[Cloud Security 25](#_rn7lfwsqvi5n)

[Runtime Security 26](#_1r6y58a47t8)

[Application Security 27](#_p60r46qcynl1)

[**Appendix A - Useful Documentation 28**](#_8mhuexfc2qst)

## 

## Document Objectives

* To create a custom Prisma Cloud Adoption Plan with recommendations tailored to the [Customer Name] Prisma Cloud environment and customer journey.
* Provide [Customer Name] with a plan deliverable on how they can achieve more with the Prisma Cloud platform

## **Customer Information**

| **Customer Name** | [Customer Name] |
| --- | --- |
| **Main Customer Point of Contact** |  |
| **Prisma Cloud License** |  |
| **Number of Credits Purchased** |  |

**NOTES FROM INTERNAL KICKOFF (To be Removed before Delivery):**

**Instruction for the Deployment Milestones (To be Removed before Delivery)**

During the assessment, emphasize and encourage the customer to enable or cover the deployment tasks related to the primary milestones of the good deployment status. These items must be implemented during the project to achieve the goal of customer values.

* **VPC Flow Logs are Enabled** on a Cloud Account to ensure visibility into network traffic
* **Create a Custom Policy** to meet customer security and compliance requirements
* **Enable IAM Policy** - Policy has been enabled to provide additional context to the attack path
* **Vulnerability has been fixed**: an Alert has been remediated
* **Setup 3rd Party Integration**

## 

## Cloud Security General

Recommendations to help the customer implement different approaches to increase credit utilization and gain additional benefits within the general Prisma Cloud environment.

| Question | Observation/Notes |
| --- | --- |
| 1. **What compliance standards are required to be monitored? (required)** 2. Are there any pre-defined measures for security scanning and posture?   How are compliance standard frameworks followed?  (Want to understand your current Info Sec practices)  How is threat detection carried out? |  |
| **Recommendation:**  Prisma Cloud assists with Cloud Security, providing a comprehensive multi-layer approach with Cloud Security Posture Management/Compliance that enhances visibility into misconfigurations of the AWS, Azure, GCP, and OCI environments. The CSPM module also has support for scanning cloud resources for violations against [Compliance frameworks](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/compliance-dashboard) such as CIS 1.5 (AWS & Azure) which are the frameworks [Customer Name] must be compliant against. Prisma Cloud CSPM can also ingest SCPs when the AWS Organization is onboarded into Prisma Cloud.  Cloud Workload Protection within Prisma Cloud also provides a multi-layer approach working with the full lifecycle from securing cloud infrastructure and applications early in development, container images, serverless, and many capabilities for the DevOps/Security team. With Prisma Cloud CWP, vulnerabilities can be identified and prevented across a customer's entire application lifecycle. The best practice is to utilize the CWP APIs to send the Prisma Cloud Vulnerability Data to [Customer Name]’s data lake to be able to then report the findings back to a BI tool such as PowerBI or Tableau to display various metrics like whether or not SLAs are being met for various types of vulnerabilities.  With Prisma Cloud CWP, vulnerabilities can be identified and prevented across a customer's entire application lifecycle. Integrating vulnerability management into [Customer Name]’s CI process will identify, monitor, and prevent risks to the cloud environment. Using a combination of vulnerability policies, CVE tagging, and configuring registry scans, it is possible to manage the vulnerabilities for applications themselves as well as the infrastructure as early in the development cycle as possible. Once the [Customer Name] team has vulnerability scan results published into Prisma Cloud, it is recommended to utilize [Alert Labels](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/annotate_audits) in order to automate the assignment of the alerts going into JIRA. To do this, [Customer Name] will need to have a proper labeling mechanism set up for Docker or Kubernetes labels. Once that is configured, Docker/Kubernetes labels can be defined in the Console as an Alert label and used for dynamically assigning JIRA tasks.  The best practice for sending CSPM alerts to third party tools for remediation is using a ticketing tool like Service Now to track the change as well as a tool like Cortex [XSOAR](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud/integrate-prisma-cloud-with-demisto) to perform the remediation once the ServiceNow ticket has been approved during [Customer Name]’s defined change management process.  It is also recommended to use the OOTB integration with [ServiceNow](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud/integrate-prisma-cloud-with-servicenow) to create tickets for CSPM alerts that can be tracked and remediated using the integration. If [Customer Name] does not want to use XSOAR for remediation, it is recommended to track the change in ServiceNow, once the change is approved then an assigned individual can remediate the alert directly from within Prisma Cloud for policies that have remediation baked in.  In regards to performing a scheduled remediation, it is recommended to utilize the integration with XSOAR to perform a [Time-Triggered Job](https://xsoar.pan.dev/docs/incidents/incident-jobs) event that allows you to schedule when you want the playbook remediation to take place after the Alert has been sent from Prisma Cloud to XSOAR. | |

| Question | Observation/Notes |
| --- | --- |
| 1. Identify any specific areas of concern related to cloud security. Any specific pain points to be addressed. 2. What are the most business critical applications that need to be protected? |  |
| **Recommendation:**  In order to have full coverage of all Cloud Accounts in CSPM, it is recommended first and foremost to onboard Cloud Accounts in AWS, Azure, and GCP at the Organizational level. To account for a bulk onboarding workflow, it is recommended (as mentioned during the workshop) to utilize the [Terraform Provider](https://registry.terraform.io/providers/PaloAltoNetworks/prismacloud/1.2.11/docs/resources/cloud_account) for automating the workflow for onboarding Cloud Accounts into Prisma Cloud.  To assist with feature parity between all Cloud Accounts that have been onboarded into Prisma Cloud, it is recommended to utilize the [Account Groups](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-account-groups) feature. The Account Groups feature in conjunction with Policy filters will assist with grouping certain Cloud Accounts together so that you can utilize Alert Rules to be notified when a group of Cloud Accounts are non-compliant with CIS 1.5 Azure for example. | |

| Question | Observation/Notes |
| --- | --- |
| 1. Is the customer planning on taking any Prisma Cloud training? |  |
| **Recommendation:**  For decommissioning defenders in an automated fashion, it is recommended to utilize this [documentation](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/decommission_defender) for decommissioning Host and Container defenders. For decommissioning of defenders deployed in Kubernetes or Openshift, it is recommended to follow this [documentation](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/uninstall-defenders). Another method for removing a daemonset defender is to run the following scripts in Kubernetes or Openshift:  For K8s clusters:  kubectl -n twistlock delete ds twistlock-defender-ds  kubectl -n twistlock delete sa twistlock-service  kubectl -n twistlock delete secret twistlock-secrets  For Openshift clusters:  oc -n twistlock delete ds twistlock-defender-ds  oc -n twistlock delete sa twistlock-service  oc -n twistlock delete secret twistlock-secrets  [Customer Name] teams can review Weekly webinars from Customer Success: [**LiveCommunity Webinars**](https://live.paloaltonetworks.com/t5/prisma-cloud-articles/prisma-cloud-monthly-product-overview-webinar-recordings/ta-p/306059). This site includes overview meetings where the Product Management Team goes over chosen topics and different aspects of Prisma Cloud and Prisma Cloud Compute every month. Product Managers will demo some of these exciting features and will be able to answer your questions live. Additionally, they will also share insights on respective modules to provide perspectives on the product trends. The [LiveCommunity](https://live.paloaltonetworks.com/t5/prisma-cloud/ct-p/PrismaCloud) page has also been updated with blogs, videos, articles, implementation plans and customer journeys for CSPM, CWP and CAS. There is also a Customer Discussion section that allows customers to collaborate on common issues they are running to in the field and also rally support for their existing RFEs.  PANW has also released a Prisma Cloud Field Guide that covers Best Practices. The Field Guide can be [found here](https://github.com/PaloAltoNetworks/prisma-cloud-best-practices). It covers both CSPM, CWP, and CAS.  The [Customer Name] team can also utilize the [Beacon Portal](https://beacon.paloaltonetworks.com/student/catalog) for specific training material. Here is a course that talks specifically about [Runtime Defense](https://beacon.paloaltonetworks.com/student/path/669636/activity/721018).  Palo Alto Networks is also working on creating an Instructor Led Training course for Prisma Cloud CSPM and CWP that will be available to our customers in April 2023.  Additionally, you can view the latest updates for CWP and Code Security at the following link [Prisma Cloud Limited PM Series Recordings Launch: CWP and CAS Release Updates](https://live.paloaltonetworks.com/t5/prisma-cloud-articles/prisma-cloud-limited-pm-series-recordings-launch-cwp-and-ccs/ta-p/505935)  You will need your support portal credentials to log into Live Community. | |

## Prisma Cloud - Cloud Security

Recommendations to help the customer implement different approaches to increase credit utilization and gain additional benefits specifically within Prisma Cloud Cloud Security Posture Management.

| Question | Observation/Notes |
| --- | --- |
| 1. Which Public Cloud Providers does the customer have? 2. How many cloud accounts will need to be monitored? 3. Are there organizational hierarchies in use? (i.e. AWS Org, Azure Tenant, GCP Org, etc.) 4. Is the network flow log enabled? |  |
| **Recommendation:**  If [Customer Name] has Cloud accounts that are unmonitored and not onboarded, review onboarding steps via documentation or Professional Services can help onboard as well as maintain the status of those accounts to allow proper ingestion. You should monitor all environments for their benefit from additional visibility with any other cloud providers also completely onboarded at the hierarchy (i.e. Organization, Tenant) level.  Review cloud account/hierarchy status (errors - flow logs, ingestion, etc.) regularly and remediate them. The [Alarms center](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alarms/set-up-email-notifications-for-alarms) (can be enabled from Settings if not done already) will also assist with being able to be notified whenever a cloud account is missing permissions. Once Adoption and further configuration processes are complete for the current environments, [Customer Name] will have the proper visibility into their security and compliance posture.  It is also recommended to segregate access for RBAC using the account groups that were created when the various Cloud Accounts were onboarded. This will help ensure that users who access the Prisma Cloud console will only see the alerts/data relevant to their Cloud Accounts/resources. Account groups can also be quite useful when setting up the Alert Rules for particular Cloud Accounts. This way, [Customer Name] can group together Cloud Accounts that should adhere to specific policies and Compliance standards and allow those alerts to be sent to the proper asset owners for remediation. | |

| Question | Observation/Notes |
| --- | --- |
| 1. What SSO provider do they use? |  |
| **Recommendation:**  The [Customer Name] team has done a great job by already configuring SSO integration with Okta and Prisma Cloud in both their Engineering and Ops tenants. The next step would be to set up the [Okta JIT integration](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/setup-sso-integration-on-prisma-cloud/set-up-jit-on-okta) for the Ops tenant just like the Engineering tenant has been configured.  Tip/Best Practice: As a best practice, enable a couple of administrative users with both local authentication credentials on Prisma Cloud and SSO access so that they can log in to the administrative console and modify the SSO configuration when needed, without risk of account lockout. | |

| Question | Observation/Notes |
| --- | --- |
| 1. What tools does the client use for ticket management, vuln management, and incident response? |  |
| **Recommendation:**  A suggestion is to integrate Prisma Cloud with [XSOAR](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud/integrate-prisma-cloud-with-demisto) once the alerts have been tuned and are actionable alerts by tuning the policies and alert rules. This will send a Prisma Cloud alert generated by a policy violation to XSOAR. This integration enables your Security operations team to be able to send policy violation alerts to XSOAR, which can then be routed through JIRA to appropriate application owners to remediate. Once the ticket has been approved, as long as remediation is enabled for the policy violation, the remediation can be triggered through Prisma Cloud or through XSOAR.  To be able to fine tune the alerts at the resource tag level, it is recommended to configure the [Alert Rule](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/create-an-alert-rule) for the asset (S3 buckets for example) and specify the tag on the S3 bucket that you would like to alert on. This way, you will only alert on S3 buckets that have the key-value pair defined in the alert rule.  Another suggestion is to burn down their Alerts inside Prisma Cloud by tuning their Alert Rules and Policies to ensure that the alerts within Prisma Cloud are actionable alerts and high priority alerts so that the alert data being sent to Splunk will only be actionable data and not contain noise that will pollute their Splunk environment. Start by prioritizing the Alerts based on Severity and Compliance Standards and tune the Alert Rules accordingly. Then, take a look at the alerts themselves and see if the underlying RQL for the policies need to be tuned to ensure the alerts that [Customer Name] want to prioritize are being alerted on and any excess noise is eliminated. Many mature alert remediation models have the established service level agreements (SLAs), notification, response, and remediation times based on the severity level of the alert. These SLAs ensure that organizations prioritize and respond to vulnerabilities efficiently and in accordance with predefined metrics.  It is also recommended to schedule at least one meeting per month to review all new Prisma policies. Typically Prisma CSPM has two updates per month, which may include new policies or updates to existing ones. This information is proactively published in [Prisma Cloud Release Notes](https://docs.prismacloud.io/en/enterprise-edition/rn/prisma-cloud-release-info/prisma-cloud-release-info). Recurring policy review calls ensures that new policies are considered for an addition to already defined policy baseline. | |

| Question | Observation/Notes |
| --- | --- |
| 1. Is the client planning on taking advantage of IAM security and Data Security modules? |  |
| **Recommendation:**  The CSPM module within Prisma Cloud has support for scanning cloud resources for violations against [Compliance frameworks](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/compliance-dashboard) such as HIPAA and HITRUST which are the frameworks [Customer Name] must be compliant against. Prisma Cloud CSPM can also ingest SCPs when the AWS Organization is onboarded into Prisma Cloud.  In order to migrate [Customer Name]’s own policies to Prisma Cloud, it is recommended to utilize [RQL](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/rql-examples) to create the policies within Prisma Cloud. In order to alert on the [Customer Name] Policies, it is recommended to create Alert rules that are scoped out to the new policies that were created with RQL.  The CIEM module helps to address the security challenges of managing IAM in cloud environments. Prisma Cloud CIEM capabilities automatically calculate effective permissions across cloud service providers, detect overly permissive access and suggest corrections to reach least privilege entitlements.  The IAM Security module works by running a proprietary algorithm that has two parts. It first combines services from various cloud entities such as AWS IAM roles, AWS IAM policies, AWS IAM groups, AWS service control policies (SCPs), Azure resource groups, Azure Active Directory (AD), GCP users, GCP service accounts, GCP groups, and GCP roles to compute the net effective permissions of cloud types. It then matches the actual usage ([last access](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security/investigate-iam-incidents-on-prisma-cloud)) to show when a permission was actually used. See [Net Effective Permissions Calculation](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security/context-used-to-calculate-effective-permissions#id9a49416f-ea8e-4374-b297-a2b029ac1640_id5104998a-a619-4b2d-b7bf-5980647df3cf) for more information.  The [Data Security](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/what-is-included-with-prisma-cloud-data-security) Module includes capabilities on Prisma Cloud that enable you to discover and classify data stored in AWS and Azure storage accounts and protect accidental exposure, misuse, or sharing of sensitive data. Additional information on the Data Security module is that our malware scanning capabilities are based on signature, content and behavior since we rely on Wildfire ([PANW Malware Analysis Engine](https://www.paloaltonetworks.com/products/secure-the-network/wildfire)).  This year Prisma Cloud Data Security is being enhanced with new scanning capabilities. This includes support for a wider variety of data stores including structured databases, unstructured stores, analytics across all three major cloud providers as well as DBaaS such as Snow flake. Most importantly all the scans are being done without leaving the customer environment.  **Recommendation:**  The recommended route to hunt down IP addresses that are accessing your applications is to utilize [Network RQL queries](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/investigate-incidents-on-prisma-cloud/investigate-network-incidents-on-prisma-cloud) to investigate whether specific IP addresses or IP address ranges have accessed your application. There are also some UI updates coming for the Network Investigate feature in Prisma Cloud in FY23Q4. It is recommended to work with [Customer Name]’s CS team to ensure [Customer Name] is included in the beta release.  In regards to being able to control login timeout for Users, it is recommended to tune the User Idle Timeout setting under Settings > Enterprise Settings. However, this setting will apply to all Users on the console. Controlling login timeout for each User is not a feature that is currently in the Roadmap for FY23. It is recommended to work with [Customer Name]’s CS team to log a [Feature Request](https://prismacloud.ideas.aha.io/) for this setting as well as the capability for saving a working session view as that is also not something on the Roadmap for FY23.  In regards to being able to see which EC2 instances are EKS nodes, it is recommended to utilize Cloud Discovery reporting to be able to understand the various workloads running in your environment such as EC2 instances and EKS clusters. By pulling the Cloud Discovery results via the [API](https://pan.dev/prisma-cloud/api/cwpp/get-cloud-discovery-download/), the [Customer Name] team can determine which EC2s are part of a node group and which EC2s are just standalone instances that are not part of an EKS node group. Another way to do this is utilizing the following RQL that will only display EC2 instances that are part of an EKS node group:  **config from cloud.resource where cloud.type = 'aws' AND cloud.service = 'Amazon EC2' AND api.name = 'aws-ec2-describe-instances' AND json.rule = tags[\*].key contains "aws:eks:cluster-name"**  NOTE: For queries that are looking for EC2 instances that are not part of an EKS cluster/node group, you can change the “contains” portion of the RQL to “does not contain”. | |

## 

## 

## Prisma Cloud - Runtime Security

Recommendations to help the customer implement different approaches to increase credit utilization and gain additional benefits specifically within Cloud Workload Protection.

| Question | Observation/Notes |
| --- | --- |
| 1. What are the client’s use cases for Prisma Cloud Workload Protection? 2. What do [Customer Name]’s general vulnerability processes look like? 3. What are the typical tools used for Vulnerability Management? |  |
| **Recommendation:**  The Prisma Cloud Enterprise Edition (SaaS) provides a holistic code to cloud approach utilizing the Code, Build, Deploy, and Run (CBDR) methodology. With access to the SaaS console, the [Customer Name] team is able to take advantage of securing their Cloud environments from all aspects of Cloud Application Security (CAS), Cloud Workload Protection (CWP), and Cloud Security Posture Management (CSPM). Another benefit of the SaaS console is being able to reuse existing integrations from the CSPM side, onboarded cloud accounts from CSPM, and the upcoming Command Center feature that will unify alerts for CSPM and CWP in one single pane of view. With the latest update to Prisma Cloud, there is now a unified onboarding experience for Cloud Accounts to not only ingest data for CSPM, but also to enable permissions on the IAM/Service Accounts for CWP features such as Agentless Scanning, Cloud Discovery, and several other features. | |

| Question | Observation/Notes |
| --- | --- |
| 1. What would be the preferred method for scanning workloads (Agentless vs Agent based)? |  |
| **Recommendation:**  The [Radar view](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology_overviews/radar) and Serverless Radar View are some of the most widely used features in Prisma Cloud Compute as they provide a comprehensive visual of the various deployed workloads as well as distinction between how vulnerable the resource is, and how compliant the resource is against [Customer Name]’s compliance policies. The Radar view also allows visibility into runtime alerts for workloads that have defenders deployed to them. Depending on the tools being used internally, there are various methods of automating the deployment of [defenders](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_kubernetes) on a K8s cluster (YAML file, Helm chart, twistCLI command) that can be implemented into [Customer Name]’s current deployment pipelines. Container Runtime Protection provides defense against various attacks such as Malware, Kubernetes attacks, Crypto Miners, Reverse Shell Attacks, Port Scanning, Suspicious queries to Cloud Provider APIs, and much more. More information about Runtime protection risk prevention can be found [here](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers). In addition to the Runtime Protection features Prisma Cloud provides, the deployment of a defender also enables the use of the WAAS protections. In regards to Cloud Discovery, the following [API](https://prisma.pan.dev/api/cloud/cwpp/cloud#operation/get-cloud-discovery-download) allows users to download a CSV file from Cloud Discovery that will provide the scan results of all the [Customer Name] workloads currently running in the cloud as well as providing information on whether or not those workloads have defenders deployed on them. In order to enable [Cloud Discovery](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/cloud-service-providers/cloud-accounts-discovery-pcee), the Cloud accounts will need to be onboarded via Compute > Manage> Cloud Accounts.  Prisma Cloud integrates security into your continuous integration workflows so you can find and fix problems before they enter production. By integrating defender deployment as a step in the CI/CD process, instances can start the CI process with a defender that is online and available to help with alerting and blocking. Automation and using the Prisma Cloud API calls can be used to deploy the defenders. Scopes (collections) can aid in targeting compliance and runtime rules for the proper environment.  In regards to automating the Fargate defender deployment, the recommendation is to utilize this [script](https://github.com/PaloAltoNetworks/prisma-cloud-compute-sample-code/blob/main/deployment/fargate/fargateProtect.sh) (from the Github we spoke about) to automate the generation of the protected Fargate task. From there, you would just have to deploy the new revision of the protected Fargate task that was generated as part of the previous script into your ECS cluster.  In regards to automating the Defender Upgrade process for Kubernetes or Openshift cluster, it is recommended to follow the following sequence: Add in the following lines in pipeline that will clear out old defender daemonsets and replace them completely with newest defender resources on the cluster to avoid any potential errors during upgrade process:  For K8s clusters:  kubectl -n twistlock delete ds twistlock-defender-ds  kubectl -n twistlock delete sa twistlock-service  kubectl -n twistlock delete secret twistlock-secrets  For Openshift clusters:  oc -n twistlock delete ds twistlock-defender-ds  oc -n twistlock delete sa twistlock-service  oc -n twistlock delete secret twistlock-secrets  Once the defender related resources are deleted, it is recommended to use twistCLI or the API to generate the newest defender deployment files and then use OC or Kubectl to deploy the latest defender deployment file for each cluster. [Customer Name] could use the results from Cloud Discovery to find out which Openshift clusters don't have defenders of the proper version deployed to them and then have the CI/CD pipeline run and upgrade the defenders for the clusters that have the outdated defender versions running.  Also, it is recommended to add validation steps in the CI/CD pipeline to validate the defender agents have deployed successfully. Some of the validation steps include verifying the defender service is running on the respective nodes as well as verifying communication between the console and defender agents.  The recommendation for using both Agentless scanning and Agent-based scanning is by following the methodology presented below:   * Start with enabling Agentless scanning for Cloud Accounts with critical workloads that are public facing in order to get the initial visibility of the vulnerabilities, failed compliance checks, and malware that exist on the running VMs and containers that are running on the VMs. * Now that the [Customer Name] team can see the vulnerability/compliance/malware scan results for their critical workloads, they can use the Attack Path policies to help identify the riskiest assets and start to prioritize them. * With the scan results from the Attack Path policies, the [Customer Name] team can now prioritize where they should deploy Defender agents in order to provide Runtime Protection and WAAS capabilities to help not only monitor the Runtime and Web Applications for threats, but also eventually go into Prevention mode. | |

| Question | Observation/Notes |
| --- | --- |
| 1. Are they looking to integrate with any third party tools to send CWP incidents and vulnerability scans? |  |
| **Recommendation:**  [Customer Name] should consider integrating their Gitlab CI/CD pipelines to allow Prisma Cloud to scan images before they are deployed into the environment, allowing full control over vulnerable images and being able to create rules to fail the pipelines depending on the vulnerability threshold. In order to integrate, it is recommended to utilize [TwistCLI](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images) to run scans against any images that are being deployed as part of the pipeline. This allows full control over vulnerable images and being able to create rules to fail the pipelines depending on the vulnerability threshold. It is recommended to configure and fine tune [CI rules](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins) in Prisma Cloud Compute in order to have a granular level of control over vulnerable images being deployed into [Customer Name]’s environments. [Admission control](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/access_control/open_policy_agent) policies can also be set up in Prisma Cloud using pre-existing policies or creating [Customer Name]’s own policies. These policies are enforced only when deployed to a workload that has a defender agent present. | |

| Question | Observation/Notes |
| --- | --- |
| 1. What requirements exist for scanning images/registries for vulnerabilities? |  |
| **Recommendation:**  [Customer Name] should ensure all of their [ECR](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/vulnerability_management/registry_scanning0/scan_ecr) and [Artifactory](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/vulnerability_management/registry_scanning0/scan_artifactory) container registries that are being used amongst the various development teams are on boarded into Prisma Cloud and are being scanned for vulnerabilities and compliance related issues.  This feature of Prisma Cloud is very helpful as it can catch vulnerable images earlier on in the development cycle. In order to further control image deployment, the [Customer Name] team should explore the benefits of using the “[Trusted Images](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/trusted_images)” feature of Compute. This feature will allow the [Customer Name] team to add their Trusted Repos in their Container Registries to a Trusted Group and create Trust Policies that allow control over untrusted images from being deployed into the environment.  In order to customize scan results of images, it is recommended to make use of custom vulnerability policies that can adjust vulnerability threshold for alerting and blocking on vulnerable images. Prisma Cloud also lets you filter out base image vulnerabilities from your scan reports. For more information, see the documentation for [Base Image Vulnerabilities](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/base_images).  For fine tuning policies in CWP, it is recommended that the [Customer Name]’ team creates Vulnerability/Compliance/Runtime policies that are scoped out using collections to control the various types of workloads deployed. Once the proper workloads have been identified in the collections, the relevant Vulnerabilities/Compliance/Runtime checks and protections need to be enabled to gain accurate alerting. The [Customer Name] team should fine tune their policies by catering the alerts to [Customer Name]’ specific Compliance Standards, Vulnerability thresholds, and Runtime protections.  [TwistCLI](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images) is a Prisma Cloud Compute command line utility tool that can be used to allow developers to scan images on their workstations as they develop the images. This allows image vulnerabilities to be found and addressed as early in the development cycle as possible. | |

| Question | Observation/Notes |
| --- | --- |
| 1. Are they planning on utilizing WAAS to protect their Web Applications and API endpoints? |  |
| **Recommendation:**  [WAAS](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas-intro) can help protect Web Applications from DDOS attacks, password hijacking, Cross site scripting attacks, code injection, shellshock, clickjacking as well as protection from various types of bots and crypto miners. [Customer Name] should look into implementing WAAS for their web applications as well as any exposed API endpoints. The idea is to create WAAS rules that start out with alerting, and then once the [Customer Name] team has a better understanding of their Web Application and how it’s being alerted, they can start implementing the prevent or ban controls. In order to prevent alert fatigue from WAAS related alerts, the best practice is to first fine tune the WAAS policies in order to ensure that [Customer Name] is getting legitimate alerts. Then, it is recommended to send these WAAS alerts to [Customer Name]’ SIEM tool of choice in order to aggregate the alerts to a single pane of glass. Another benefit to WAAS is that because of its design and the way it is implemented using defender agents, it will give more control over [Customer Name]’ network traffic flows.  The newest update of CWP involves new features, more specifically the [Out-of-Band](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy_waas/deployment_out_of_band) WAAS feature. The Out-of-Band feature takes the defender out of the application flow entirely, but still offers the same protections that the regular WAAS feature does. The limitation for Out-of-Band is that it can only alert on any of the protections that are enabled. This is due to the fact that when the Defender is in Out-of-Band mode for WAAS, it will only mirror the traffic from a read-only copy. The Out-of-Band WAAS is also more economical because of the reduction in licensing credits that are used. | |

| Question | Observation/Notes |
| --- | --- |
| 1. What type of serverless functions are deployed in the environment? |  |
| **Recommendation:**  Prisma Cloud Compute currently supports scan [capabilities](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions) of AWS, Azure, and Google Serverless functions. It is recommended to add the scan scope for [Customer Name]’s serverless functions so that Prisma Cloud can scan their functions for vulnerabilities. We support scanning the following Lambda Runtimes: Node.js, Python, Java, C#, Ruby, and Go packages. As far as runtime protection, we currently only support AWS Lambda functions and Azure functions.  Serverless Defender protects serverless functions at runtime. The defender monitors your functions to ensure they execute as designed. The defender monitors:  Process activity, which enables verification of launched subprocesses against policy.  Network connections which enables verification of inbound and outbound connections, and permits outbound connections to explicitly allowed domains.  File system activity which Controls which parts of the file system functions can access.  Prisma Cloud supports AWS Lambda functions (Linux) and Azure Functions (Windows only). It is also recommended to utilize the [Serverless Auto-Defend](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/auto_defend_serverless) feature for deploying serverless defenders onto Lambda functions.  TwistCLI can also be used to scan serverless functions as they are being developed. Please see this [documentation](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli) for more information on TwistCLI commands. | |

## 

## Prisma Cloud - Application Security

Recommendations to help the customer implement different approaches to increase credit utilization and gain additional benefits specifically within Prisma Cloud Code Security Module

| Question | Observation/Notes |
| --- | --- |
| 1. What kind of visibility do you have into your code security posture? 2. How much of the infrastructure in your cloud environment is codified in IaC? |  |
| **Recommendation:**  Collaborate with the organization’s cloud infrastructure team(s) to assist in identifying known repositories where IaC may exist. Onboarding more repositories to Application Security will increase visibility. All repositories containing IaC should be scanned by Prisma Cloud Application Security where appropriate. Work with the organization’s DevOps team to implement IaC scanning as a mandatory non-blocking stage in every pipeline that informs the code owners of the vulnerabilities. Once this is in place, beginning to force all new infrastructure to be deployed as IaC will ensure compliance with policies. Eventually these policies should lead to blocking the most critical vulnerabilities and misconfigurations and over time becoming more restrictive and having higher security standards for deployment.  It is recommended to use [tagging](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-code-security/scan-monitor/iac-tag-and-trace) from Yor to auto-tag your resource blocks. It uses a unique yor\_trace tag to detect drift in cloud resources compared to the code stored in repositories and locate the specific resource within a commit that identifies teams and resource owners to help triage a fix in the most time and cost-effective way.  Prisma Cloud Application Security can enable the customer to identify security misconfigurations, secrets in their IAC, Helm chart and Docker files while also detecting vulnerabilities in their software packages. The main recommendations will be to fully onboard all the repositories they have on Prisma Cloud and utilize the CAS capabilities at each stage of the lifecycle to ensure the security of their deployments.  These CAS capabilities are as follows:   * Using Prisma Cloud Checkov Integration to carry out scanning at the IDE level, during development and before Code is deployed to the Pipeline or Repository. * Integrate Prisma Cloud CAS with all CI/CD pipelines to scan at the Pipeline level * Onboard Repositories to Prisma Cloud to scan at the Repository level * Use the CI/CD Risks feature within Prisma Cloud to gain visibility into your attack surface and achieve full prioritization of risks to optimize your CI/CD security posture across your entire software delivery chain   Version Control System: [Customer Name] is using Gitlab and Bitbucket SAAS. Both are VCS platforms fully supported by Prisma Cloud. With the use of the Cloud Application Security Module, [Customer Name] can scan at all levels of the SDLC, from development, to code commit, to build and deploy.  **Reference:**  [CI/CD Risks](https://docs.prismacloud.io/en/classic/appsec-admin-guide/risk-prevention/ci-cd-risks) | |

| Question | Observation/Notes |
| --- | --- |
| 1. What kind of IaC templating tools are used within your organization? 2. What kind of version control systems (Github/Gitlab/Bitbucket) are used within your organization? |  |
| **Recommendation:**  Prisma Cloud Application Security can help to identify security misconfigurations in the customer’s Bicep, HELM, and Dockerfile templates to name a few. There are capabilities that allow you to use out of the box build policies as well as the option to create custom build policies that adhere to the customer’s internal IAC related policies.  Version Control System: [Customer Name] is using Azure Devops. The customer should onboard more repositories from their Azure DevOps repos that contain IaC. Prisma Cloud should be able to scan at all portions of the SDLC, from development, to code commit, to build and deploy.  Prisma Cloud Application Security can also help to identify security misconfigurations in the customer’s IaC in other frameworks including Terraform templates. Prisma Cloud fully supports Gitlab and Bitbucket as Version Control systems. Repositories for these 2 platforms can be onboarded and scanned every 12 hours. In addition, on demand scans can also be initiated.  **Reference:**  [Bitbucket Onboarding Documentation](https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/connect-your-repositories/code-repositories/add-bitbucket)  [Gitlab Onboarding Documentation](https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/connect-your-repositories/code-repositories/add-gitlab) | |

| Question | Observation/Notes |
| --- | --- |
| 1. What security or hardening requirements currently exist for your IaC code? |  |
| **Recommendation:**  Recommend reviewing customer’s static code analysis hardening requirement as a starting point. Once policy guardrails are documented, implement them as a CI/CD gate on repositories containing IaC to block merges with the main branch if the code contains vulnerabilities or misconfigurations that fail to meet the guardrails. These guardrails typically block merges when vulnerabilities are found with certain severities (Medium & High) present in the IaC. Some references to best practices for IaC can be found here:   * [Cheat Sheet Series](https://cheatsheetseries.owasp.org/cheatsheets/Infrastructure_as_Code_Security_Cheat_Sheet.html) * [Bridgecrew IAC](https://bridgecrew.io/blog/how-to-implement-an-infrastructure-as-code-security-program/)   Recommend reviewing [Customer Name]’s static analysis hardening requirement as a starting point. After Onboarding, Prisma Cloud’s Build policies should be reviewed and implemented as a guardrail at all 3 levels (IDE, Pipeline and Repository) to block merges with the main branch if the code contains issues that fail to meet compliance. Begin implementing Enforcement Rules within the Prisma Cloud Console and fine tune any Build policies you deem surplus to requirements.  **Reference:**  [Prisma Cloud Enforcement Rules](https://docs.prismacloud.io/en/classic/appsec-admin-guide/risk-prevention/code/enforcement) | |

| Question | Observation/Notes |
| --- | --- |
| 1. Are there any existing CI/CD guardrails in place for your IaC? 2. Have you implemented any custom policies or checks for your code? 3. What IDEs does the team use for IaC creation? |  |
| **Recommendation:**  Bicep templates should always only be deployed through some type of CI/CD process. This is for a few reasons:  -Only the service account has permission to deploy new templates  -This ensures that security checks are run and pass with the requirements set by the organization  -This also ensures that the source of truth for deploys is from the code repositories, so we can detect drift this way if a user makes a manual change in the cloud  In the long term no users should have access to any of the cloud consoles for making changes except in break-glass situations.  Implement the use of Prisma Cloud Checkov extension at the IDE level with VS Code. In addition, Implement additional custom checks and begin to enforce in the pipeline. “Fail open” functionality has been added to Checkov so if there is any failure from the backend then the pipeline will fail gracefully as opposed to crashing.  **Reference:**  [Prisma Cloud Checkov extension](https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/connect-your-repositories/integrate-ide/connect-vscode)  [Checkov CI/CD Runs](https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/connect-your-repositories/ci-cd-runs/add-checkov)  [Custom Build policies](https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/code-repositories-policy-management/custom-build-policy-examples) | |

## 

## 

## Prisma Cloud Automation & Extensibility

Recommendations to help the customer benefit from custom automation, integrations, and extend the capabilities of Prisma Cloud by implementing custom developed solutions.

| Question | Observation/Notes |
| --- | --- |
| 1. Are there any use cases for utilizing the public APIs in the current environment? |  |
| **Recommendation:**  Here is the API documentation for [CSPM](https://pan.dev/prisma-cloud/api/cspm/), [CWP](https://pan.dev/prisma-cloud/api/cwpp/), and [CAS](https://pan.dev/prisma-cloud/api/code/). It is recommended to utilize Python or Go scripting to automate the various tasks within Prisma Cloud utilizing the API endpoints that are documented. If there is a task that does not have a corresponding API endpoint in the documentation above, it is recommended to use the Developer Tools in your browser to look at the Network Endpoint that is being invoked in order to evaluate the API being used. However, it is important to note that any API endpoints found using this method that are not documented in our API reference documentation are subject to change.  Familiarity with the public APIs and tooling can assist in programmatically managing the Prisma Cloud console, report on specific items in the console, and help remediate issues faster. Documentation can be found [here](https://prisma.pan.dev/docs/cloud/).  The [Customer Name] team has some familiarity with the public APIs and have built some simple scripts for basic needs. Most of the automation around Prisma Cloud has temporarily halted due to an identified bug in the product that the product team is working through as the data needs to be correct before they pull the data out into other products for automation related use cases. So far there are a few use cases recommended for implementation, an automation for exception management, building an ETL automation to have the ability to downgrade/upgrade the severity of a finding and store somewhere for assignment, and an automation for compliance reporting on a given standard including building a library that others can leverage for pulling any listed standard’s stats. Automated exception management is key to a functional vulnerability management program. | |

| Question | Observation/Notes |
| --- | --- |
| 1. How does your team report on remediation (SLAs)? What would you like it to look like? 2. Any issues with manual tasks for updating or pulling data from other products to action in Prisma Cloud? |  |
| **Recommendation:**  The [Customer Name] team is already considering a few automation use cases for reporting on SLAs. Since the [Customer Name] team was unaware that the onboarding templates had a lack of permissions, it is recommended that the [Customer Name] team implement either Alarm Center notifications or even better, implement an automation to grab the latest onboarding template and commit to a repo. Since Prisma Cloud is constantly supporting new CSP APIs for ingestion, it is key to continue to update these templates otherwise [Customer Name] is not taking full advantage of all the capabilities that Prisma Cloud has to offer.  Further, a couple working sessions would be recommended since the [Customer Name] team had mentioned issues with authentication to the API as well as issues querying specific endpoints for the CIS reporting. Some limited documentation has been provided for these specific use cases but likely more time would be needed to go over any issues and confusion with API documentation.  Cloud Workload Protection within Prisma Cloud also provides a multi-layer approach working with the full lifecycle from securing cloud infrastructure and applications early in development, container images, serverless, and many capabilities for the DevOps/Security team. With Prisma Cloud CWP, vulnerabilities can be identified and prevented across a customer's entire application lifecycle. The best practice is to utilize the CWP APIs to send the Prisma Cloud Vulnerability Data to [Customer Name]’s data warehouse such as Big Query to centralize vulnerability data from Tenable and Prisma Cloud in order to display various metrics like whether or not SLAs are being met for various types of vulnerabilities as well as vulnerability trends. | |

## **Recommendations**

### **Product Recommendations**

**Prisma Cloud CSPM**

* Review Newest Release (Darwin) features relevant to CSPM
* Review and configure net effective permission policies from CIEM (High recommendation)
* Configure RBAC, Enterprise, and Anomaly settings per Best Practices
* Enable network flow log ingestion
* Configure SSO JIT Integration
* Configure custom alert rules to prioritize actionable alerts and improve remediation efforts
* Custom alert rules also will facilitate different team efforts (Security, DevOps, Compliance, etc.)
* Configure 3rd party integration to alert the responsible team
* Alert Burndown sessions to bring alerts to manageable state on a daily basis
* Configure custom Compliance & Alert Reports for both Compliance team and others for visibility
* Deep dive into RQL investigation and configure custom policies tied to security use cases

**Prisma Cloud CWP**

* Review Newest Release (Darwin) features relevant to CWP
* Automate Defender Deployments and Upgrades
* Identify Vulnerabilities, manage the risk associated with new found vulnerabilities by sending scan results through third party tools to application owners to remediate vulnerabilities
* Utilize Agentless scanning in cloud hosts and containers without having to deploy any defender agents
* Utilize Serverless function scanning for an agentless approach to scanning AWS, GCP, and Azure serverless functions for Vulnerabilities
* Identify risks in [Customer Name]’s web applications using WAAS module and manage risk through the Prevent/Ban protections
* Manage risky container images by addressing them early in the development cycle using Container Registry scans and twistCLI for developers to scan the images on their workstations as they are being developed
* Configure Trusted Image Groups to designate Trusted Images and create Trust Policies to generate alerts when images that are not Trusted are being deployed
* Integrate with CI/CD pipelines to scan images and provide gatekeeping measures to block vulnerable images from being deployed into the environment

**Prisma Cloud CAS**

* Configure Bitbucket and Gitlab Code Repositories to be scanned by Prisma Cloud CAS
* Create custom build policies and leverage out of the box build policies for alerting on vulnerable TF IAC templates
* Configure IAC scanning with CI/CD pipelines
* Utilize Checkov extension at the IDE level with VS Code to allow developers to scan their code as they are writing it.
* Use the CI/CD Risks feature within Prisma Cloud to gain visibility into your attack surface of your CI/CD Pipeline systems
* Implement Drift detection to detect drift between deployed cloud assets and the associated IAC
* Configure enforcement rules to tune alerting and prevention capabilities with IAC

### 

### 

### 

### 

### 

### 

### 

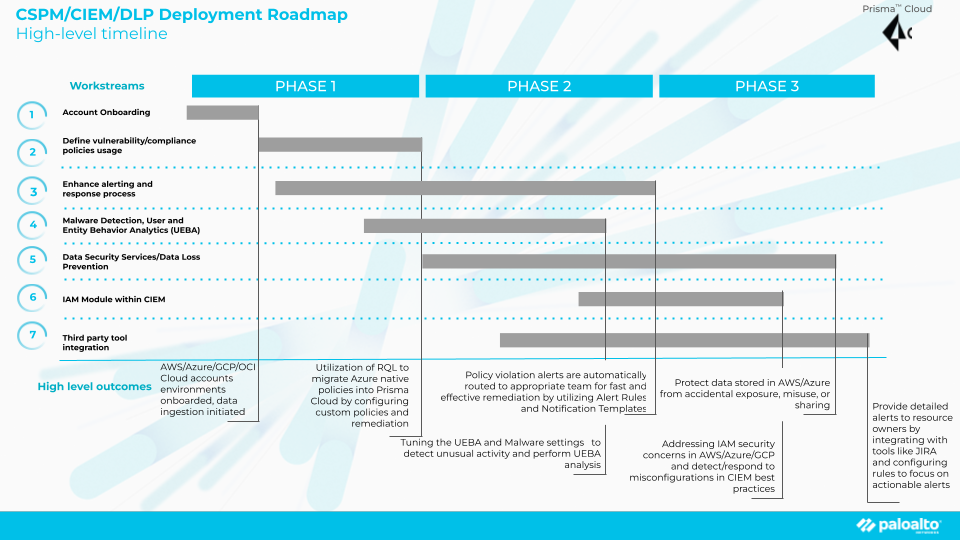
### 

### 

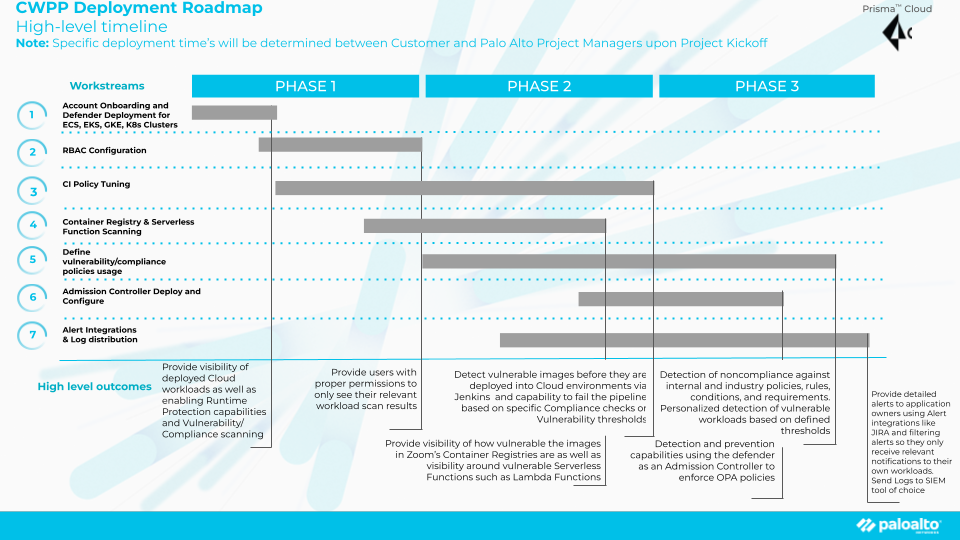
### 

## Roadmaps

### Cloud Security

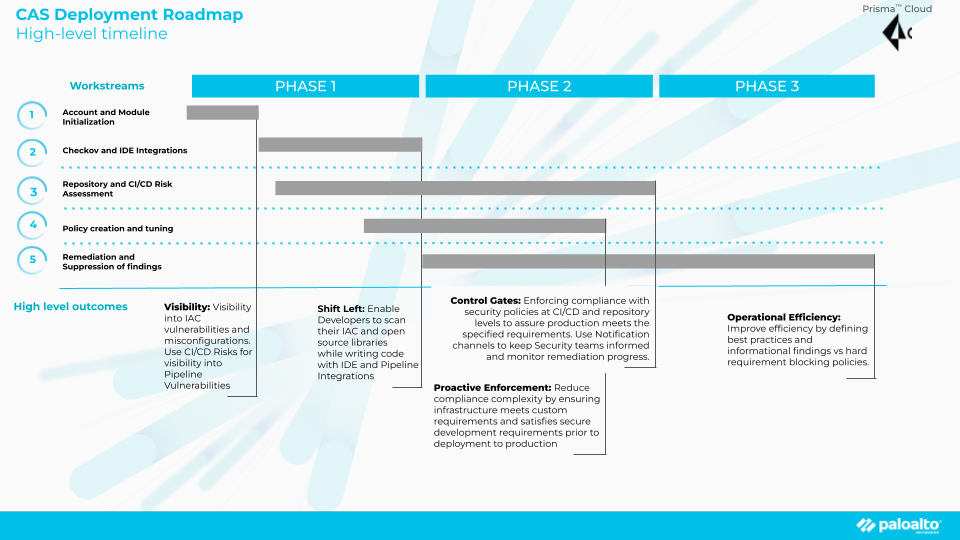


### Runtime Security



### 

### Application Security



### 

## 

## Appendix A - Useful Documentation

| **Reference Material** |
| --- |
| [Prisma Cloud Licensing Guide](https://www.paloaltonetworks.com/resources/guides/prisma-cloud-enterprise-edition-licensing-guide) |
| [Professional Services Service Descriptions](https://www.paloaltonetworks.com/services/consulting/servicedescriptions) |
| [IAM & DevOps Security](https://docs.paloaltonetworks.com/prisma/prisma-cloud.html#other-modules) |
| [Prisma Cloud Sample Code Github](https://github.com/PaloAltoNetworks/prisma-cloud-compute-sample-code) |
| [Prisma Cloud PANW Official Documentation](https://docs.prismacloud.io/en/enterprise-edition) |
| [Prisma Cloud API Documentation](https://pan.dev/prisma-cloud/api/) |