Oracle Cloud Guard Recommendations and Tips

July 2023, Version 1.2

Public

Cloud Guard Recommendations and Tips

- Set Cloud Guard target to the root compartment. To monitor IAM resources, the root compartment must be a target.
- There could be a need to have a different set of detectors in child compartments rather than root compartment. This can be achieved by declaring the respective child compartment as a target and apply the related user-managed recipes to this target. Rules at child compartment level will overwrite the rules at root compartment level.
- Prioritize problems by criticality and consider your critical asset, this is something that only you know.
- At activation of Cloud Guard a strategy can be to just detect for a few days, then start fixing problems, in this way you can benefit of trending metrics, it will help you to see changes over time.
- Configure user-managed detector recipes to your security posture. Clone the respective Oracle-managed recipe (Configuration Detector recipe, Activity Detector Recipe and Threat Detector Recipe) and configure as needed.
- Segregate duties for Cloud Guard operations, security administrators' group can manage cloud guard operations, especially when problems are sent to a SIEM. Auditors group can read. Do not use too many different groups for this, two groups are usually good enough.
- Examine the types of resources that are stored in different parts of the compartment hierarchy in your Oracle Cloud Infrastructure tenancy.
  - Are there groups of resources in different parts of that compartment hierarchy that need to be monitored for in different ways, to detect different types of threats?
  - Would the same problem, if detected in different compartments, represent different risk levels?
  - Tags are a good way to do specific handling in a detector.
- Once you have your security posture configured. Verify that your configurations trigger as expected. When done, enable automatic remediation using the respective policy statements. Automation saves time and labour.
- Adjust the Cloud Guard configuration, based on your experience with processing the problems that Cloud Guard detects. You can continually customize the Cloud Guard configuration to optimize performance toward a two-part goal:
  a. Not letting anything that represents a potential security risk go undetected.
  b. Not detecting "too many" false positives – problems that do not actually represent potential security risks.
- Integrate Cloud Guard with your notification system and SIEM, or similar.
- Make sure, services that report to Cloud Guard are activated, like Data Safe, Threat Intelligence, Vulnerability Scanning Service, etc.
- Use managed lists for large list of exclusions, use custom-list for short list exclusions.
- Use a managed list to exclude Emergency Users from Rogue Users or risk the deletion of these.

- Stop Cloud Guard from complaining to fix problems, update the baseline, by modifying the rules in the User-Managed detector recipes.
- To avoid interference, Security Zones should not be applied to the root compartment or other Cloud Guard targets. The Security Zone UI wizard shows already configured Cloud Guard targets when applicable.
- Use event notification, to be alerted of new problems and the automatic remediations of these problems by Cloud Guard responders.
- For Threat monitoring to work, enable Threat Intelligence and add threat detector recipe at the root target compartment. It will take few days for ML to start feeding users risk score trends.

Cloud Guard Resources

- Getting started Cloud Guard Documentation

  https://docs.oracle.com/en-us/iaas/cloud-guard/using/part-start.htm
- Oracle Cloud Security Posture Management

  https://www.oracle.com/uk/security/cloud-security/what-is-cspm/
- Cloud Guard public page

  https://www.oracle.com/uk/security/cloud-security/cloud-guard/
- Learn Cloud Guard YouTube videos

  https://www.youtube.com/watch?v=WrEBDKJxSjo&list=PLKCk3OyNwIzuzfWoqvCg4ucrkSK0J-vBD
- Oracle Cloud Infrastructure Blog

  https://blogs.oracle.com/cloud-infrastructure/search.html?contentType=Blog-Post&default=cloud%20guard*
- Cloud Infrastructure Community Forum

  https://community.oracle.com/tech/apps-infra/categories/18430-cloud-infrastructure
- Cloud Customer Connect

  https://community.oracle.com/customerconnect/
- Stack Overflow Oracle Infrastructure

  https://stackoverflow.com/questions/tagged/oracle-cloud-infrastructure
- My Oracle Support

  https://support.oracle.com/portal/