

Oracle Cloud Success Protection Services – OCI Security Health Check

Customer Name:



Author: Charan Kumar Asthigiri – Lead Cloud Architect

Creation Date: Nov, 2024

Version 1.0

Copyright © 2024, Oracle and/or its affiliates

Confidential – Oracle Internal

Purpose Statement

The OCI Security Health Check service is designed to identify deviations from Oracle recommended Cloud Guard recipes and problems within a customer's OCI environment. Oracle ACS will conduct the health check on a target OCI tenancy and document the findings in this document.

Disclaimer

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

This report of findings is intended to provide you with general information, and you acknowledge that a number of facts and circumstances outside the scope of this service may affect the outcome of your project.

In addition, you acknowledge that the information contained herein may represent one of many ways to facilitate success of your project goals and that successful completion of your project is subject to factors outside of Oracle's control such as performance by your staff, partner staff, third party staff and other third-party products and services. For these reasons, it cannot be ensured that this document provides a complete assessment of the system or technology reviewed and you should take this into consideration if acting based on any findings or recommendations set out in this report.

Similarly, you should carefully consider all relevant assumptions, prerequisites and constraints noted in this report.

Table of contents

Purpose statement

Disclaimer

Customer Information

Cloud Guard Detector Recipes Compliance Report

Threat Detector Recipes

Instance Security Recipes

Configuration Detector Recipes

Activity Detector Recipes

Problem Details

Appendix – Additional Reading

Customer Information

Customer Name	
Tenancy Name	
Data Collected On	

Cloud Guard Detector Recipes Compliance Report

This section includes the list of health checks that have been conducted on the environment under analysis. This section includes the data that was captured and reviewed as part of the health checks. The findings are based on OCI Cloud Guard Recipes and Detected Problems:

Threat Detector Recipes

Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
IAAS_THREAT_DETECTOR	ROGUE_USER	None	Unknown	Compliant

Non-Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status

Instance Security Recipes

Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
IAAS_INSTANCE_SECURITY_DETECTOR	AIDE	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	WLP_AGENT_HEARTBEAT_MISSING	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	CHEF	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	CONTAINER_INVENTORY	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	SOFTWARE_INVENTORY	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	CLAM	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	CONTAINER_SCAN_VULN	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	CONTAINER_SCAN_30DAY	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	GRIFFIN	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	HOSTMETRICS	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	IMDS_DEPRECATED_VERSION	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	LOCAL_ACCOUNTS	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	NTP	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	ODO_READ_ONLY_FS	None	LOW	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	ODO_NON_PRIVILEGED_USER	None	LOW	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	RPM_PACKAGES	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	SELINUX	None	HIGH	Compliant
IAAS_INSTANCE_SECURITY_DETECTOR	SECSCAN	None	HIGH	Compliant

Non-Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status

Configuration Detector Recipes

Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
IAAS_CONFIGURATION_DETECTOR	ADMIN_GROUP_HAS_TOO_MANY_MEMBERS	IAM	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	JIT_DISABLED_BOAT_GROUP_HAS_PRIVILEGES	CIS_OCI_V1.1_IAM, CIS_OCI_V1.0_IAM, IAM	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	BLOCK_VOLUME_NOT_ATTACHED	Storage	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	BUCKET_IS_PUBLIC	CIS_OCI_V1.1_OBJECTSTORAGE, ObjectStorage, CIS_OCI_V_2.0.0	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	DATA_SAFE_NOT_ENABLED	Database Security	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	DATABASE_PUBLICLY_ACCESSIBLE	Database	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	DATABASE_SYSTEM_VERSION_NOT_SANCTIONED	Database	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	DATABASE_VERSION_NOT_SANCTIONED	Database	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	SECRET_KEY_TOO_OLD	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM, CIS_OCI_V_2.0	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	IAM_MFA_TOTP_DEVICE_TOO_OLD	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	OCI_IAM_GRP_TOO_MANY_MEMBERS_FOUND	IAM	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	INSTANCE_NOT_RUNNING_OPC	Compute	LOW	Compliant

5 Oracle Cloud Success Protection Services – OCI Security Health Check

Copyright © 2024, Oracle and/or its affiliates / Dropdown Options

IAAS_CONFIGURATION_DETECTOR	INSTANCE_RUNNING_OPC	Compute	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	INSTANCE_WITHOUT_REQUIRED_TAGS	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, TAGS	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_HAS_PUBLIC_IP	Network	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_CERTIFICATE_EXPIRING_SOON	Network	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_WEAK_SSL_COMMUNICATION	Network	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_WEAK_CIPHER_SUITE	Network	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_NO_BACK_END_SET	Network	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	LB_NO_INBOUND_RULES_OR_LISTENERS	Network	MINOR	Compliant
IAAS_CONFIGURATION_DETECTOR	VCN_NSG_EGRESS_RULE_PORTS_CHECK	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	VCN_NSG_INGRESS_RULE_PORTS_CHECK	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Network, CIS_OCI_V_2.0.0	HIGH	Compliant
IAAS_CONFIGURATION_DETECTOR	BUCKET_ENCRYPTED_WITH_ORACLE_MANAGED_KEY	CIS_OCI_V1.1_OBJECTSTORAGE, ObjectStorage, KMS, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_CONFIGURATION_DETECTOR	PASSWORD_POLICY_NOT_COMPLEX	CIS_OCI_V1.1_IAM, CIS_OCI_V1.0_IAM, IAM, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	BUCKET_READ_LOG_ACCESS_DISABLED	CIS_OCI_V1.1_OBJECTSTORAGE, ObjectStorage	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	RESOURCE_NOT_TAGGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, TAGS, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	SCANNED_CONTAINER_IMAGE_VULNERABILITY	VSS	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	SCANNED_HOST_OPEN_PORTS	VSS	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	SCANNED_HOST_VULNERABILITY	VSS	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	SECURITY_LISTS_OPEN_SOURCE	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Network, CIS_OCI_V_2.0.0	CRITICAL	Compliant
IAAS_CONFIGURATION_DETECTOR	VCN_HAS_LPG_ATTACHED	Network	LOW	Compliant
IAAS_CONFIGURATION_DETECTOR	VCN_NO_INBOUND_SECURITY_LIST	Network	MEDIUM	Compliant
IAAS_CONFIGURATION_DETECTOR	BUCKET_WRITE_LOG_ACCESS_DISABLED	CIS_OCI_V1.1_MONITORING, CIS_OCI_V1.1_OBJECTSTORAGE, ObjectStorage, CIS_OCI_V_2.0.0	LOW	Compliant

Non-Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
IAAS_CONFIGURATION_DETECT OR	INSTANCE_PUBLICLY_ACCESSIBLE	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Compute	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	NO_MFA_ENABLED_FOR_USER	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM, CIS_OCI_V_2.0.0	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_API_KEY_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_CONSOLE_PASSWORD_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	SECURITY_LIST_ALLOWS_TRAFFIC_FROM_ALL_SOURCES	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Network	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	SECURITY_LISTS_OPEN_PORTS	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, Network, CIS_OCI_V_2.0.0	CRITICAL	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	DATABASE_HAS_PUBLIC_IP	Database	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	DATABASE_HAS_NO_AUTO_BACKUP	Database	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	INSTANCE_WITH_PUBLIC_IP	CIS_OCI_V1.0_NETWORK, CIS_OCI_V1.1_NETWORK, COMPUTE	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_AUTH_TOKEN_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_CUSTOMER_SECRET_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_DB_CREDENTIAL_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	HIGH	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	API_KEY_TOO_OLD	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM, CIS_OCI_V_2.0.0	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	DATA_SAFE_DB_NOT_REGISTERED	Database Security	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	DATABASE_PATCH_NOT_APPLIED	Database	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	DATABASE_SYSTEM_PATCH_NOT_APPLIED	Database	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	AUTH_TOKEN_TOO_OLD	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM, CIS_OCI_V_2.0.0	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	KEY_NOT_ROTATED	CIS_OCI_V1.1_MONITORING, KMS, CIS_OCI_V_2.0.0	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	PASSWORD_TOO_OLD	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	MEDIUM	Non-Compliant

IAAS_CONFIGURATION_DETECT OR	POLICY_GIVES_MANY_PRIVILEGES	CIS_OCI_V_2.0.0, CIS_OCI_V1.1_IAM, CIS_OCI_V1.0_IAM, IAM, CIS_OCI_V_2.0.0	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	POLICYUSES_ANY_USER	CIS_OCI_V1.1_IAM, CIS_OCI_V1.0_IAM, IAM	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	POLICY_TENANCY_ADMIN_GROUP_PRIVILEGES	CIS_OCI_V1.1_IAM, CIS_OCI_V1.0_IAM, IAM, CIS_OCI_V_2.0.0	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_SMTP_CREDENTIAL_CAPABILITY	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM	MEDIUM	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	OCI_IAM_GRP_FEW_MEMBERS_FOUND	IAM	LOW	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	USER_HAS_API_KEYS	CIS_OCI_V1.0_IAM, CIS_OCI_V1.1_IAM, IAM, CIS_OCI_V_2.0.0	LOW	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	VCN_HAS_INTERNET_GATEWAY_ATTACHED	Network	LOW	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY	Storage, KMS, CIS_OCI_V_2.0.0	MINOR	Non-Compliant
IAAS_CONFIGURATION_DETECT OR	VNIC_WITHOUT_NETWORK_SECURITY_GROUP	COMPUTE, Network	MINOR	Non-Compliant

Activity Detector Recipes

Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
IAAS_ACTIVITY_DETECTOR	BASTION_CREATED	Bastion	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	BASTION_SESSION_CREATED	Bastion	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	CA_BUNDLE_UPDATED	Certificates	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	CERTIFICATE_AUTHORITY_DELETED	Certificates	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	DRG_ATTACHED_TO_VCN	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	DRG_CREATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	DRG_DELETED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	DRG_DETACHED_FROM_VCN	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	DATABASE_SYSTEM_TERMINATED	Database	HIGH	Compliant
IAAS_ACTIVITY_DETECTOR	EXPORT_IMAGE	Compute	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_API_KEY_CREATED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_API_KEY_DELETED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_AUTH_TOKEN_CREATED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_AUTH_TOKEN_DELETED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_CUSTOMER_KEY_CREATED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_CUSTOMER_KEY_DELETED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_GROUP_CREATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_GROUP_DELETED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_OAUTH_CREDENTIAL_CREATED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_OAUTH_CREDENTIAL_DELETED	IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	NON_IAM_USER_SMTP_CREDENTIAL	CIS_OCI_V1.0_IAM,	HIGH	Compliant

		CIS_OCI_V1.1_IAM, IAM		
IAAS_ACTIVITY_DETECTOR	IAM_USER_UI_PASSWORD_CREATED_OR_RESET	IAM, IAM_Credentials, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_USER_CAPABILITIES_MODIFIED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	IAM_USER_CREATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	IMPORT_IMAGE	Compute	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	INSTANCE_TERMINATED	Compute	HIGH	Compliant
IAAS_ACTIVITY_DETECTOR	INTERMEDIATE_CERTIFICATE_AUTHORITY_REVOKED	Certificates	HIGH	Compliant
IAAS_ACTIVITY_DETECTOR	NON_MFA_USER_LOGIN	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM	HIGH	Compliant
IAAS_ACTIVITY_DETECTOR	SECURITY_POLICY_MODIFIED	CIS_OCI_V1.1_MONITORING, IAM, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	SUBNET_CHANGED	Network	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	SUBNET_DELETED	Network	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	SUSPICIOUS_IP_ACTIVITY	Network	CRITICAL	Compliant
IAAS_ACTIVITY_DETECTOR	UPDATE_IMAGE	Compute	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	USER_ADDED_TO_GROUP	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, IAM, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	USER_REMOVED_FROM_GROUP	IAM, CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, CIS_OCI_V_2.0.0	MINOR	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_DHCP_OPTION_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	INTERNET_GATEWAY_CREATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	INTERNET_GATEWAY_TERMINATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_LOCAL_PEERING_GATEWAY_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	NSG_DELETE	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	HIGH	Compliant
IAAS_ACTIVITY_DETECTOR	NSG_EGRESS_RULE_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	NSG_INGRESS_RULE_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	ROUTE_TABLE_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_SECURITY_LIST_CREATED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_SECURITY_LIST_DELETED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_SECURITY_LIST_EGRESS_RULES_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_SECURITY_LIST_INGRESS_RULES_CHANGED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_CREATE	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	LOW	Compliant
IAAS_ACTIVITY_DETECTOR	VCN_DELETED	CIS_OCI_V1.0_MONITORING, CIS_OCI_V1.1_MONITORING, Network, CIS_OCI_V_2.0.0	MEDIUM	Compliant

Non-Compliant Recipes

Detector ID	Detector Rule ID	Labels	Risk-Level	Status
-------------	------------------	--------	------------	--------

Problem Details

1. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\":\"Public\",\"vnicPublicIp\":\"129.80.14.25\"}]", "vnicDetails": "[{"vnicAttachmentId":"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmaciucr13eenexv2tb3fifnixmlazpatxfayxqvdaigia","vnicAttachmentDisplayName":null,"vnicId":"ocid1.vnic.oc1.iad.abuwcljtmcorn6ndbo72qmid7ywq3xs45laocm46ljjtwq7246sf74qf3nha","vnicDisplayName":"security-health-checks-demo","vnicPublicIp":"129.80.14.25"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osflrqpnko4yobhh3bmnga4kt4saq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhsdczpxfhsgbjm6q7imrkfvo74vldfxvh2jkoxz55uaa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS OCI V1.0 NETWORK", "COMPUTE", "CIS OCI V1.1 NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacojdvcwska4gznsmkbozvpdfjsnunmd4xnqir6xnaa
resource-name	security-health-checks-demo
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaaqsoer7pl4mbnepmiqz4wqnjuxzgqef3sv5icn4i2xja
time-first-detected	2024-11-03T18:10:41.957000+00:00
time-last-detected	2024-11-04T01:20:02.503000+00:00

2. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[({\"subnetAccessType\":\"Public\"},\"vnicPublicIp\":\"158.101.96.99\")]\", \"vnicDetails\": \"({\"vnicAttachmentId\":\"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacrnfcfkapuzyfznr2w6is6rgf7te3nr75mg6gmb4aza\"},\"vnicAttachmentDisplay Name\":null,\"vnicId\":\"ocid1.vnic.oc1.iad.abuwcljtbh6nd4u3zd2lwuuugtr4msgzb2g2zobvfdfkcvqeqot7whavkonq\"},\"vnicDisplayName\":\"security-health-checks-demo2\"},\"vnicPublicIp\":\"158.101.96.99\")]\"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osflrqnko4yobhh3bmnga4kt4saq
description	Checks public IP only
detector-id	IaaS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4di25xf355shi66zio2czvflzahialzvg72icschk2qq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmackmb5ccpi6ysrf4gkl6ltktup3xiik2d4ctjydepnmtsq
resource-name	security-health-checks-demo2
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaaqsoer7pl4mbnepmiqz4wqnjuxzggef3sv5icn4i2xjya
time-first-detected	2024-11-03T18:10:41.247000+00:00
time-last-detected	2024-11-04T01:20:02.702000+00:00

3. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osfirqpnko4yobhh3bmnga4kt4saq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqir6pjgkq2mh6h4mnhdbl3gvhri2b4ayqongs2ygotpa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwclitmcorn6ndbo72qmid7ywq3xs45laocm46jttwq7246sf74qf3nha
resource-name	security-health-checks-demo
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaaqsoer7pl4mbnepmiqz4wqnjuxzgqef3sv5icn4i2xjya
time-first-detected	2024-11-03T18:10:41.513000+00:00
time-last-detected	2024-11-04T01:20:01.733000+00:00

4. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osflrqpnko4yobhh3bmnga4kt4saq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5j6ero6i5q2x3tygamy4shb4jh4muyluv7i5awxtd7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtbh6nd4u3zd2lwxxuugtr4msgzb2g2zobvfdgdkcvqeot7whavkong
resource-name	security-health-checks-demo2
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaaqsoer7pl4mbnepmiqz4wqnjuxzggef3sv5icn4i2xjya
time-first-detected	2024-11-03T18:10:42.668000+00:00
time-last-detected	2024-11-04T01:20:02.758000+00:00

5. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-10-28T21:08:25.665Z", "User Name": "kotireddy.kurakula@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdeh35ujmepkqsmp5h7aiaksyq7fmk7p757mqeatrpoq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-30T02:29:54.715000+00:00
time-last-detected	2024-11-04T02:44:49.428000+00:00

6. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-10-28T21:06:55.125Z", "User Name": "avinash.vajrala@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7df2lpvug2fj4nibjoisuxd3xbusn6kbw3g6lxbga
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasar6jrnb4qkcvlpv36kkhpdxihnuwc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-30T02:29:53.851000+00:00
time-last-detected	2024-11-04T02:44:49.172000+00:00

7. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqtlhjb7pekougslhkp32fxofuhvq4henzosg6dspz6ta
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.466000+00:00
time-last-detected	2024-11-04T02:44:49.424000+00:00

8. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqktlrnwzl3xlwcqskfdtvbeucfg5wm6f66vqr5a76ztmq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.904000+00:00
time-last-detected	2024-11-04T02:44:49.155000+00:00

9. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7pkmj777e7y5ycti3rmq465azkqkzpjo04hzj7an5hq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.928000+00:00
time-last-detected	2024-11-04T02:44:49.195000+00:00

10. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6jvh2yx47ds4ja7pv5q47pp65twdm7ndvjlmywymcca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.459000+00:00
time-last-detected	2024-11-04T02:44:49.417000+00:00

11. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzb5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3zvv6mwbfbjlbpeljucm2c6rpqcu732hvfnwqtdcuqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.462000+00:00
time-last-detected	2024-11-04T02:44:49.420000+00:00

12. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqfgl4ofj4m735vvhxaeo5wvsaa6rf2mtmuq2jtiyekk24a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.931000+00:00
time-last-detected	2024-11-04T02:44:49.199000+00:00

13. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqicxfuef3mua62la5agvzv3hbzemnlvl46gdmeplgtq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.482000+00:00
time-last-detected	2024-11-04T02:44:49.439000+00:00

14. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqndju5jzkzetc3ymi6ghs7al5fgx4iaefdag3innnq2zma
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.451000+00:00
time-last-detected	2024-11-04T02:44:49.410000+00:00

15. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqauxoi6eh6vz44riffunfcswj3yltyvy7ky2rfyfimqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.911000+00:00
time-last-detected	2024-11-04T02:44:49.167000+00:00

16. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnuc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqkbhe4ttdukndsrvoaa6xpbp3vp5j2utia5voxqh5noqa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnuc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.908000+00:00
time-last-detected	2024-11-04T02:44:49.163000+00:00

17. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqybe5ikovomgrcosig3ye4cdstvdou4aor2722cgli7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.475000+00:00
time-last-detected	2024-11-04T02:44:49.433000+00:00

18. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "kotireddy.kurakula@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5zm4pwsckrcotkbf6675l6idyzzevh2vat3oyfz7a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa75rucz5ndiv2cpb4leavkb73bq4ok273hx5edd4angpqugrqbapa
resource-name	kotireddy.kurakula@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:10.486000+00:00
time-last-detected	2024-11-04T02:44:49.442000+00:00

19. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqlp2vw3xyzx6vxe2y3jtmkjcnlnlobscwpczhgg6m6a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnwuc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.897000+00:00
time-last-detected	2024-11-04T02:44:49.146000+00:00

20. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "avinash.vajrala@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4jgqgob64drekbhfs7w3kdnzgfufvyyogtgu2lgx7ptq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaathasav6jrnba4qkcvlpv36kkhpdxihnluwc5y4a7u625fogphls3a
resource-name	avinash.vajrala@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-29T02:11:08.921000+00:00
time-last-detected	2024-11-04T02:44:49.188000+00:00

21. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "129.213.124.225"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmaecc5fqihjedxdqbdpl5fj2ynlqrtfz7ahigci5pv3a", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtrcq6bnsmqoiyhxsnrgfnv5dc5kkqancw74srnxwr7fmnepg6o3l2q", "vnicDisplayName": "CSSCOGSVM", "vnicPublicIp": "129.213.124.225"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqe7nfitmvr132zl2xb5g2ly5zgcirqap5vqfxgckdh7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmaclej3npnaqavtcg76vocyeu43bwtm60wwgsrbzonllnq
resource-name	CSSCOGSVM
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T20:13:22.640000+00:00
time-last-detected	2024-11-04T01:14:00.173000+00:00

22. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"129.158.53.160\\""}]", "vnicDetails": [{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmachjwqdymqoiafezlsqbn3qjsapwc7qdyys7h5w3blq\\", "vnicAttachmentDisplay Name": null, "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljt4k4g5aglccicysrdo5pbmxwfn6l6yfxfcer75wgm6qyebb45vko\\", "vnic DisplayName": "\\"css-gold-image-test-20240213\\", "vnicPublicIp": "\\"129.158.53.160\\""}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqn6ctwxh5hp5phf5djhmls2gpf457huulhh7uinvp3q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacikm2oenistmu6uc6gsjfnw7qggwj6nzqbu4jqq66pzea
resource-name	css-gold-image-test-20240213
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T20:06:00.733000+00:00
time-last-detected	2024-11-04T01:13:59.427000+00:00

23. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "141.148.12.20"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmaccfmersvn66ox6twta5kkewre3nxpihzv4h2wqwhma", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtj3hkvsid3ykszcx6zw47gjdmlcjpfilogv46plrdfrj7kcfwnmq", "vnicDisplayName": "UATVM_RUCHIR", "vnicPublicIp": "141.148.12.20"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awtlyla
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2wpnglukdojhjjei7vcfb6mow4l3vvzruvhn4otsq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ytmacs5oqbup4n6juyllu7y6s23b424emxshrmky4kxg6jq
resource-name	UATVM_RUCHIR
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T20:03:31.323000+00:00
time-last-detected	2024-11-04T01:13:38.382000+00:00

24. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"129.158.216.145\"}]", "vnicDetails": "[{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmaczcvlbcsudsukv36gdttydl7qoovzi2xd6iad2ua\", \"vnicAttachmentDisplayName\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwlkjtkwlhbagelxr22ly6m4au5yfwajkzvtypbktxsqkhfj6yp5lcywa\", \"vnicDisplayName\": \"VMMIHAL\", \"vnicPublicIp\": \"129.158.216.145\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqao5aqwrb6rlnkhpmpvhvstd6yj7qlfswdtvmxfirgl
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacyopvdvyq5qifr3nul57i6qhojd5hvta17ld47ebjxgxd
resource-name	VMMIHAL
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-24T19:32:30.212000+00:00
time-last-detected	2024-11-04T01:13:38.692000+00:00

25. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "150.136.247.110"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcltjw2ytmaccsgm4ccoyff7whktjqojjpwxnyct6f45pzd3yks6q"}, {"vnicAttachmentDisplayName": null}, {"vnicId": "ocid1.vnic.oc1.iad.abuwcltfmhkx4xadzrstayi7l57grs2eyhvkmatlvpdoj6jbozzo5nwmq"}, {"vnicDisplayName": "instance-20240602-1514"}, {"vnicPublicIp": "150.136.247.110"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxrj64iqumm47bdakmaqkpzjnjkuiawgk6khxsmcnua
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcltjw2ytmacddurhlttq6izficctxbcxzh3negwlyyq7zuhskyexqa
resource-name	instance-20240602-1514
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:56:32.948000+00:00
time-last-detected	2024-11-04T01:19:51.592000+00:00

26. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"129.80.14.25\\"}]", "vnicDetails": "[{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmaciucru3eenexv2tb3fiftnixmlazpatxfayxqvdaigia\\", "vnicAttachmentDisplayName": null, "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljtmcorn6ndbo72qmid7ywq3xs45laocm46ljjtwq7246sf74qf3nha\\", "vnicDisplayName": "\\"security-health-checks-demo\\", "vnicPublicIp": "\\"129.80.14.25\\"}]"}}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osflrqpnko4yobhh3bmnga4kt4saq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4nrndq5shivbgfli7kssyoekbrhqbmsy7jrofig5gq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacojdvcvwska4gznsmkbozpdffdjsnumd4xnqrir6xnaa
resource-name	security-health-checks-demo
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:48:40.223000+00:00
time-last-detected	2024-11-03T12:13:52.706000+00:00

27. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"150.136.128.57\"}]\", \"vnicDetails\": \"[{\\" vnicAttachmentId \": \"ocid1.vnicattachment.oc1.iad.anuwljtpwzvtmacvkk65amabcpwk2pehpaaowqjfilf6w3iusry2p7zgqa\\\", \"vnicAttachmentDisplay Name\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwljtp4etfm4ovt3auso5o2ghosetdv5cggeyyxp4nzm3j6m6wv4zwxyq\\\", \"vnicDisplayName\": \"ESS-Collection-VM01\\\", \"vnicPublicIp\": \"150.136.128.57\"}]\"}"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2qh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq666k3gfi33zsgiajwjeqpzlbvym44glarvdulqs3j4xa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtpwzvtmacrbiugzq6drphaha6nkuthkyxjm57jcvr47g35bqkdveq
resource-name	ESS-Collection-VM01
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:34:22.297000+00:00
time-last-detected	2024-11-04T01:14:00.074000+00:00

28. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "129.153.171.72"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacqcap4il5kuocap2p7tn4wua3ynxwgirvdno2dj5l6qq", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwljtibyo16svemuexpakvwnticrowvmdm3mayvrxgkf357vvk4ds5bq", "vnicDisplayName": "database23ai", "vnicPublicIp": "129.153.171.72"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3q2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmhg6y6d3uzb6osfqzqebrwj5aapxigumabmv6tzvtkq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacblndnjacgapkgkmoqrq3rwv4nf35necano5dcge2bxja
resource-name	database23ai
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-24T05:34:27.728000+00:00
time-last-detected	2024-11-04T01:19:51.692000+00:00

29. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"129.159.99.43\\"}]", "vnicDetails": "[{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacgjfrdqaj7jwvfdueuyaafsezh6ugyudusyw2grwro4ea\\", "vnicAttachmentDisplayName": "\":null\", \"vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljtvft73y5lhgczbuhu6dshxsvyj63w4n4xtkytywcuo2eqh5aq7yua\\", \"vnicDisplayName": "\\"cogs-image\\", \"vnicPublicIp": "\\"129.159.99.43\\"}]"}}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjiybhaoa
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqgvxd4slpewj5qm4bxodl6377wgqzqx533ymwgr2h47a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacb6bq4ud7oanqzano2mitsse2l73zfu4ivhobgspcjka
resource-name	cogs-image
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:33:31.118000+00:00
time-last-detected	2024-11-04T01:13:28.505000+00:00

30. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\"SubnetAccessType\\\": \"Public\", \"vnicPublicIp\\\": \"150.136.163.101\\\"}]\", \"vnicDetails\": \"[{\\"vnicAttachmentId\\\": \"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacbr5yot2kyn7r5qqaeydobjbps4npteagonnubqoy4yzq\\\", \"vnicAttachmentDisplayName\\\": null, \"vnicId\\\": \"ocid1.vnic.oc1.iad.abuwcljt5pslypogs5jsxpaxn4kpwa5riyeeaomdcec44yyxhiur3xuww43a\\\", \"vnicDisplayName\\\": \"UAT-VM-RICK.1.5.4\\\", \"vnicPublicIp\\\": \"150.136.163.101\\\"}]\"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfsu2fykejmbmad4e44heghqczlg7awt1pyla
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqf3mbdnptfxsgeokc2dwqokfmnmohkyq6ruibhijgphya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacqvlpzfl2jfkpvd3pcqjrhjh76zp2jria7yr4y6ggph37a
resource-name	UAT-VM-RICK_1.5.4
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:23:34.701000+00:00
time-last-detected	2024-11-04T01:13:39.390000+00:00

31. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwljtw2ytmackodsmky5bruuqg43seympjwqkepfny4rslot5ixuyw7a"}, {"vnicAttachmentDisplay Name": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtf6ew6ugpiupbjawai776iuqzfqcd7taqot5pxgshgwwad73gqdqq"}], \"vnic DisplayName\": \"ess-compliance-prod01\", \"vnicPublicIp\": \"129.153.9.7\"}"]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqp3pvub6l2zj7542kxwu37hy5bhoww77mzkmgao6uxbq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtw2ytmackbe6myuwcd5v6hvibzd6ocqptjxr5r3g57nerzqpyqa
resource-name	ess-compliance-prod01
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:22:00.600000+00:00
time-last-detected	2024-11-04T01:13:59.399000+00:00

32. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"129.80.210.83\"}]", "vnicDetails": "[{" vnicAttachmentId \": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacd42flxaxynpwq22y6mwjjhhmmu2xb6jb4sorndgk4kjq \", \"vnicAttachmentDisplayName \": null, \"vnicId \": \"ocid1.vnic.oc1.iad.abuwcljte4g6gilwtrlcdzdiuum3mlw27syb2ouw5ivr3hgxf4b3l7p4tfca \", \"vnicDisplayName \": \"sshtest\", \"vnicPublicIp \": \"129.80.210.83\"}]"}]
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaajw2ytmcqf6j5bdhxrxmljggpkgxq3i653fgpoasi7wvfq4fm cuija
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmac6vh67rowikzafelgrdetzurffbctalfjrxdnrvzaea
resource-name	sshtest
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckfdwkna
time-first-detected	2024-10-24T05:20:47.653000+00:00
time-last-detected	2024-11-04T01:19:51.625000+00:00

33. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"129.153.2.142\\"}]", "vnicDetails": [{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacs3ureumumfyqwftrhquv2isn22j5j3nswnm47qdikcqql\\", "vnicAttachmentDisplay Name": "null", "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljta5bgmia3yhxo2uqlupmrel5guwazgtl67wjyv4a3vrfkbf5woa\\", "vnic DisplayName": "\\"vm-ruchir-new\\", "vnicPublicIp": "\\"129.153.2.142\\"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfsu2fykejmbmad4e44heghqczlg7awtlyla
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqch5s6bwrv5zbi6tbpuhqa3lv6gabvpaf713fbukgg7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmac2nu4rjuxoobjnt3lf5fon3a7o6e2acrjdculztff6fq
resource-name	vm-ruchir-new
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:18:55.916000+00:00
time-last-detected	2024-11-04T01:13:38.677000+00:00

34. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\": \"Public\", \"vnicPublicIcp\": \"150.230.173.58\"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anucljtjw2ytmac56q3xygip6lr4trm24rbokjx3cia6jwtkhtyaxasuq", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtutisngfijmovlugjqhbymynk33zc5wpghx64rrjllusb5cy33q", "vnicDisplayName": "css-tools-vm-oracle", "vnicPublicIcp": "150.230.173.58"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq42xlgb5hgsmrgu2rovmwigbjwojtf72zaetff2eeh6pa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anucljtjw2ytmacixmrpundo4rtyz6ez3x4du45fkwnkbd2jxyiyccfx76a
resource-name	css-tools-vm-oracle
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7yy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:11:54.533000+00:00
time-last-detected	2024-11-04T01:13:58.772000+00:00

35. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"150.136.245.193\"}]\", \"vnicDetails\": \"[{\\" vnicAttachmentId \": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacifsgi5jd34mmnb5jqou6k3ujxoiyb3gtj3rjjim3usq\\\", \"vnicAttachmentDisplayName\": \"null\", \"vnicId \": \"ocid1.vnic.oc1.iad.abuwcljtjqjachz7nncbx57wqmq4vmochcd4anlqwtam2hqagrcz62d6taiq\\\", \"vnicDisplayName \": \"instance-20240326-0843\\\", \"vnicPublicIp \": \"150.136.245.193\"}]\"}"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kqutb2qh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyztestroylbqxrfi7n5lwpt2id6odpvu36hvqznruq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacelqdix4rzphadczsn4wgkihislgm4qn3vhmjymxmza
resource-name	instance-20240326-0843
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:07:29.277000+00:00
time-last-detected	2024-11-04T01:13:58.628000+00:00

36. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"150.136.50.193\\"}]", "vnicDetails": "[{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacletakh755k2wfuu6mwmw4hpowc44ds5wcrqkecb34zq\\", "vnicAttachmentDisplayName": "\\"null\\", "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljtu52iftylb67o4lkoi5l42dprqxirsnlkd4ejux6zj24s3nfdh6qa\\", "vnicDisplayName": "\\"css-tools-vm-prod-oracle\\", "vnicPublicIp": "\\"150.136.50.193\\"}]"}]
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqgomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqjnmemhh5f2mofox2zwwd36xvibbdheg7c7iztjdpuhya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmac4mvhmijqnujurqt3eobl5m27muwk2cqxhmgtnuzq3wha
resource-name	css-tools-vm-prod-oracle
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:06:38.705000+00:00
time-last-detected	2024-11-04T01:13:59.483000+00:00

37. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[\"subnetAccessType\\\"Public\\\", \"vnicPublicIp\\\"132.145.167.92\\\"]", "vnicDetails": "[{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacoge5bjp4lffqjz5kixz3cws3tckihso3etyztyrsq"}, {"vnicAttachmentDisplayName": "null", "vnicId": "ocid1.vnic.oc1.iad.abuwcljtwuc34uzfihmv323zfgokdkmtaq6bz2y3mdrqjk3o2sncoecdca"}, {"vnicDisplayName": "css-gold-test2"}, {"vnicPublicIp": "132.145.167.92"}]"}}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqguxet4bjxix4zzlqo6fvnj6sl3mxhkhrp56gp3qvc3qq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacpkggqe7cx27rfvxjrjgdibxgihf2qzg55bpqmr7qxka
resource-name	css-gold-test2
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:05:48.940000+00:00
time-last-detected	2024-11-04T01:13:58.624000+00:00

38. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"141.148.53.64\"}]", "vnicDetails": "[{\\ vnicAttachmentId \": \"ocid1.vnicattachment.oc1.iad.anuwcjtjw2ytmacy5kvz3cfgz6wr2sc5i7htm2tzgvkmcoimhyqetodita\\\", \\ vnicAttachmentDisplayName \": null, \\ vnicId \": \"ocid1.vnic.oc1.iad.abuwcljthrati4bby6rbh3sxx2u3g4qe2xprczbani7uwm2ugtirq7u3mfq\\\", \\ vnicDisplayName \": \\ instance-20240321-1427\\\", \\ vnicPublicIp \": \"141.148.53.64\\\"]}"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kqutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7qxlxdpnihl6hevnhyvujejaiovqfrldxvgjoyckbqxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcjtjw2ytmacplogvxrzgtztnrc6b4pwn3ebj6j4okmxmfjkowvivqq
resource-name	instance-20240321-1427
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:06:10.156000+00:00
time-last-detected	2024-11-04T01:13:59.683000+00:00

39. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\": \"Public\", \"vnicPublicIp\": \"150.136.254.131\"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljjw2ytmac6tgcg3m624ch3znks26wlnx2so3gsm3w2v2jmduj2ka", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtraww3nm5zrv7hsylvgqlpuwz7aoavupmvfnexjtec5q6epueohhq", "vnicDisplayName": "instance-20240513-1445", "vnicPublicIp": "150.136.254.131"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmnh6fvd7g4m736twrxvz24jkrkg3wmrwx7kstg7pcya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljjw2ytmackjf2iisqv3dt3w4betyo6xigew3hoqmdg7bab274x4a
resource-name	instance-20240513-1445
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:05:10.066000+00:00
time-last-detected	2024-11-04T01:19:51.590000+00:00

40. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\": \"Public\", \"vnicPublicIp\": \"129.158.57.120\"}]", "vnicDetails": [{"vnicAttachmentId": "\\\\"ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmacf6epgcafzbqvdfi7gzj43dokjkvc2ubsjaajufgvgod\\\"", "vnicAttachmentDisplayName": "\":null, \"vnicId": "\\\\"ocid1.vnic.oc1.iad.abuwljtsvwkmjkpanj3u3i6eg5gnqkpyk2jveq5j5fuuxpgvsnmjebfucta\\\"", "vnicDisplayName": "\\\\"CSSNavGW_Mihai_2.0.3\\\"", "vnicPublicIp": "\\\\"129.158.57.120\\\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfsu2fykejmbmad4e44heghqczlq7awtlyla
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqr76qqah3rdgkwdxukrfznnngfch3vj7lxouzkimebyva
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmackgofmjz3xbknvx4roscolvwdx4ryaivxtnqj2ez4oxha
resource-name	CSSNavGW_Mihai_2.0.3
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljkuy4vbsqckfdwkna
time-first-detected	2024-10-24T05:05:14.943000+00:00
time-last-detected	2024-11-04T01:13:39.364000+00:00

41. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "150.136.168.240"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacpis5yg65ghloocwibx6arks23pc5y7amzpjhqj4rtda", "vnicAttachmentDisplayName": "null", "vnicId": "ocid1.vnic.oc1.iad.abuwljtsdy4efguxumek7dks4lzeh32nw4m2ivly5hudcrehgjzw7g3ma", "vnicDisplayName": "instance-20240422-1435", "vnicPublicIp": "150.136.168.240"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3q2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxqksuzv6g5xuiderble pncwb23acxvztanywxubjdcq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacd4o5bcamqgmmmdokvvvgbbs2z2wfcqb74mrljyt5h3naq
resource-name	instance-20240422-1435
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T05:00:32.215000+00:00
time-last-detected	2024-11-04T01:19:51.640000+00:00

42. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\"SubnetAccessType\\\": \"Public\", \"vnicPublicIp\\\": \"150.136.155.48\"}]\", \"vnicDetails\": \"[{\\"vnicAttachmentId\\\": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacqvx7pwqctpcmmjzidpvo6qft7al4fzvnacbyzihondxa\\\", \"vnicAttachmentDisplay Name\\\": null, \"vnicId\\\": \"ocid1.vnic.oc1.iad.abuwcljtolaenygzbz343utew5nczskpqzv5iu7ckkp6hvryflcfa\\\", \"vnicDisplayName\\\": \"instance-20240328-1158\\\", \"vnicPublicIp\\\": \"150.136.155.48\"}]\"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcztaubb3q2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2vwiex7rjwr7lgdmcdpdjglia3tb52jaxmsj5zey5iaa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacvu527siuhkn2mkp6f7jamr3kkxg4b6ujpjtpkdb7dq
resource-name	instance-20240328-1158
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:59:10.670000+00:00
time-last-detected	2024-11-04T01:19:51.394000+00:00

43. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\" subnetAccessType \": \"Public\", \\" vnicPublicIp \": \"129.213.199.149\"}]\", \"vnicDetails\": \"[{\\" vnicAttachmentId \": \\"ocid1.vnicattachment.oc1.iad.anuwcljtv2ytmac7upuwqllwub4jp4mowqsjpeevlrozv46pbwv7cmq\\\", \"vnicAttachmentDisplayName\":null, \"vnicId \": \\"ocid1.vnic.oc1.iad.abuwcljtk2fzqttlwowawgtfgknnds6x52hvdd7et7mgumepccwxrouyv4bna\\\", \"vnicDisplayName \": \\\"oracle-ebs-12213\\\", \"vnicPublicIp \": \\\"129.213.199.149\\\"}]\"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjiybhaoa
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqtcuhbyegeyq7kepgl3fwdktvvuj5jdvuov3o6ae7eona
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacuqxt36nkd7nxcryudxn6y76p4gydicj4d4rsbkyj27q
resource-name	apps
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:59:14.373000+00:00
time-last-detected	2024-11-04T01:13:28.896000+00:00

44. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmacjsfn2jyaafq7uwnasai4q26p56gws2lh23yi6mxik3ya"}, {"vnicAttachmentDisplay Name": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljt3uyramxtbpkkjxeklmnpfrzepxecivhs3yud7pmthduvwxyzotvuqa"}, {"vnic DisplayName": "CSS-ESS-Gold-Image-Prod-test01", "vnicPublicIp": "129.213.185.235"}]"}, "vnicDetails": "[]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqktigocmsv42myjet2na6f62tddj7x4bdegexsfazcra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacoc2knox6fkxxq32nhqwfuj7i5rani6oipxjckqjaua
resource-name	CSS-ESS-Gold-Image-Prod-test01
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:56:36.335000+00:00
time-last-detected	2024-11-04T01:14:00.096000+00:00

45. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\"SubnetAccessType\\\": \"Public\", \"vnicPublicIp\\\": \"129.80.227.133\"}]\", \"vnicDetails\": \"[{\\"vnicAttachmentId\\\": \"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmactcp2m3qxsx7vi2vdexdk2qs52jwpnggzbzfgkh2ika\", \"vnicAttachmentDisplayName\\\": null, \"vnicId\\\": \"ocid1.vnic.oc1.iad.abuwljtexqo6qmigesbneybki3azhbmnoulkiu2l3cbzb4u276cltl2lq\", \"vnicDisplayName\\\": \"instance-20240311-1652\", \"vnicPublicIp\\\": \"129.80.227.133\"}]\"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfieeihgog6cx2z6yvan774jxcpahyda7t7u3vv5nwt7sa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacsjcq6zpinv7s5wdujrrze5gae6chppryhxzmzbtko2m4q
resource-name	instance-20240311-1652
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:49:41.044000+00:00
time-last-detected	2024-11-04T01:14:00.082000+00:00

46. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"150.230.174.29\\"}]", "vnicDetails": [{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcjtjw2ytmackl5sqferpclbozsskipempwatnmdnfsia456bs7a\\", "vnicAttachmentDisplayName": "\\"null\\", "vnicId": "\\"ocid1.vnic.oc1.iad.abuwljtj2dh6oyqi5ruexnre42jd35xs64scsl6qclihobotwuxgxu2lwa\\", "vnicDisplayName": "\\"instance-20240930-0737\\", "vnicPublicIp": "\\"150.230.174.29\\"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxczaubb3g2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqgcmk2uxyyw74qimru64nxgyxu3mo5zupkwxj7zwrmlmsa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcjtjw2ytmac732vxdypz72daygtue227ynxyjd7bpuvp3ef7gl57tcq
resource-name	instance-20240930-0737
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:49:34.664000+00:00
time-last-detected	2024-11-04T01:19:51.625000+00:00

47. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\": \"Public\", \"vnicPublicIp\": \"129.80.197.193\"}]", "vnicDetails": "[{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacehhbhanf2wwkvhfdkowtity7k4l636lc04weojpjugyq\", \"vnicAttachmentDisplayName\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwcljtz2am5sfh55qxn72nvhr3ux6igqi2be537qw2nqrtrwcahmghd4q\", \"vnicDisplayName\": \"instance-202\", \"vnicPublicIp\": \"129.80.197.193\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yxomhmpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqom4tuef27z74aoymbad4bxrp7voaugyvqhw4jy2yzawa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacnj3apfmx6junmaaaqj6zdqtw6wbjptcxriy5f2yk7a
resource-name	instance-202
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:46:57.027000+00:00
time-last-detected	2024-11-04T01:14:01.724000+00:00

48. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"150.136.157.43\"}]\", \"vnicDetails\": [{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcjtjw2ymaccny2nkjvryeqrmszfg2hrbebsanu7sf66dmeybuphowq\"}, \"vnicAttachmentDisplayName\": \"null\", \"vnicId\": \"ocid1.vnic.oc1.iad.abuwcjtqz257653enwtqhg44hbxcjvdgo6ltk4lsxcpadeoqzkrqkulddla\", \"vnicDisplayName\": \"essuat-discovery-vm02\", \"vnicPublicIp\": \"150.136.157.43\"]}"]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrehu4ojxch4y6gthkxcqzaubb3q2ctobrpwq
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5aujguubqmgg3cdpdiomdsz4waezqkus4iviaplbyoha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcjtjw2ytmac2hhhvltzncup4nmbtpukjqz4asirowkqu5dmrjt7x7a
resource-name	essuat-discovery-vm02
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:46:19.384000+00:00
time-last-detected	2024-11-04T01:19:51.714000+00:00

49. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "141.148.53.41"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacvftui07wi5cviaepgshwmur2bj3c4j2sok3f4bofwa"}, {"vnicAttachmentDisplay Name": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtw6jlc6e72jxnjwku2lvzn43o5gy4uqq337mty2g2gwellix3uq"}, {"vnic DisplayName": "css-tools-vm-prod", "vnicPublicIp": "141.148.53.41"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqztfkw2g5qgfid6gt2u2bnjksr6jvdeaanux2tdgezq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacqj7kowxouriludzsn7qm34j5kyhgejulmtugidzvn53a
resource-name	css-tools-vm-prod
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:44:20.254000+00:00
time-last-detected	2024-11-04T01:14:00.024000+00:00

50. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"129.80.18.187\\"}]", "vnicDetails": [{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ymaczwfrhrkf2xdn6lbh2fyf4ibsgg3bujfz3f55keiluq\\", "vnicAttachmentDisplayName": "\\"null\\", "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljt33o4tlmmstyxt5fnx7srrhkzoqymv6fmviwddd274ukjy2gchxq\\", "vnicDisplayName": "\\"instance-20240313-0904\\", "vnicPublicIp": "\\"129.80.18.187\\"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpkd2rpefohdyapk2jm6lktqiiqlxarfcuryk2zmde4a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacuuqjzx6gklsfef3d43ajvs cuq6luands7oaabwbomp a
resource-name	instance-20240313-0904
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:38:14.823000+00:00
time-last-detected	2024-11-04T01:13:58.597000+00:00

51. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\"subnetAccessType\": \"Public\", \"vnicPublicIp\": \"141.148.60.234\"}]", "vnicDetails": "[{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcltjw2ytmac5shqfyw6dswm3jq7zugognuezhd4nk6s6coucs6ma\", \"vnicAttachmentDisplayName\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwljtatioap3ldms45jf2jegp6ynj5ej6ymj24prxqy3akan2lrqmxnq\", \"vnicDisplayName\": \"ess-discovery-vm02\", \"vnicPublicIp\": \"141.148.60.234\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcd6bjddj2hswqd63oni2zy733zkiucbyiv57x54fqxda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcltjw2ytmacrbyflrdkts4b7ock5ya4wxlvj6rdywd4phw6h6g37zpa
resource-name	ess-discovery-vm02
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:37:18.981000+00:00
time-last-detected	2024-11-04T01:13:59.714000+00:00

52. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[\"subnetAccessType\":\"Public\",\"vnicPublicIp\":\"150.136.139.28\"]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmacyunbhhrab5ff2yhk7wwfe7zokgp7egb53consf7a"}, {"vnicAttachmentDisplay Name": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtsiuafzyhaeilspvfjpjznbo5rhrcq2kyfulfavxjzllibshuq"}, {"vnicDisplayName": "essgenai", "vnicPublicIp": "150.136.139.28"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1.aaaaaaaaoff7w4qhroknuayke3ddflc3pup6f6o52foknpscik62g7o3qbe7a
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmwfbq6o3lzmghpeh5w7bh6onntiivkknadnigkt5ma
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ytmacpucn6hi3cnobr2ien6wtsbpt5e4rgqysdvzjnrudqjiq
resource-name	essgenai
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:32:38.218000+00:00
time-last-detected	2024-11-04T01:13:42.808000+00:00

53. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[\"Public\"]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmaco2cgso7zdweenyfn5iecegbwvktcdvdkbredzpxn3a"}, {"vnicAttachmentDisplayName": null}, {"vnicId": "ocid1.vnic.oc1.iad.abuwlcj45soiookq6cwlcwca33jgj5dqnylmpdf2d2zle3cijleobsrrcua"}, {"vnicDisplayName": "\ess-collection-vm02"}, {"vnicPublicIp": "141.148.76.92"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvibcjh2elcgwkfht4gfkh2poyz25wyruqh7cqqw2asq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacpcibn6wt7zzvphjxjgbjf4qfw6gzchjeo6etp6hgb7ta
resource-name	ess-cd3-vm01
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:31:44.877000+00:00
time-last-detected	2024-11-04T01:14:00.473000+00:00

54. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "\\"Public\\", "vnicPublicIp": "\\"143.47.119.70\\"}]", "vnicDetails": [{"vnicAttachmentId": "\\"ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmacxhxh6vn63hirqtsjh6wifjc2ieapdexvi54u5czkfwjq\\", "vnicAttachmentDisplayName": "\\"null\\", "vnicId": "\\"ocid1.vnic.oc1.iad.abuwcljtnluf2rlsxjeayo7ftddz6hx7hpbgwjlmpnwnoq7zzxb23db52cla\\", "vnicDisplayName": "\\"instance-20240829-1122\\", "vnicPublicIp": "\\"143.47.119.70\\"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxei4orw47r2vciisyonrvfamcedhaqo6s4a6wex7y5sq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ytmac4la2poqgguzjdgrnarrrqdf6dpowj56sdjtpjp5ssvcnq
resource-name	instance-20240829-1122
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:31:24.411000+00:00
time-last-detected	2024-11-04T01:14:00.095000+00:00

55. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"141.148.38.78\"}]", "vnicDetails": "[{\\ vnicAttachmentId \\: \"ocid1.vnicattachment.oc1.iad.anuwcjtjw2ytmacahn7jjv7a7swhllduwghum5mpimlsropgro7a2q64yuq\", \\ vnicAttachmentDisplayName \\: null, \\ vnicId \\: \"ocid1.vnic.oc1.iad.abuwcljt5j2qjnbdhloar5zveiqcintvn6ab7robphq75x3umbxdwmh3mga\", \\ vnicDisplayName \\: \"esb-prod-12213\", \\ vnicPublicIp \\: \"141.148.38.78\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpjjpph4dr76uf47rnjiybhaoa
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5z7ojityphw52ueqteaukjvfi45ztjqktmjpbgx65ya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcjtjw2ytmaczqnxbg2d6gwzvs7lk7ivieikr2mqewfmxjblvynsa
resource-name	esb-prod-12213
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-24T04:24:15.254000+00:00
time-last-detected	2024-11-04T01:13:28.971000+00:00

56. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmacculok4a2hkemlcmyngmtlw46nelnnmj2ebfrns4ca", "Public IPs": "[129.80.17.26]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d26uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngyza]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyeekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcflijemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfcetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4rkwgqaqyun7xpxar7r4wlqli4q4nnqlouabeamziekpq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacculok4a2hkemlcmyngmtlw46nelnnmj2ebfrns4ca
resource-name	ESS_Base
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T11:00:50.739000+00:00
time-last-detected	2024-11-04T01:19:54.727000+00:00

57. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"129.80.17.26\"}]", "vnicDetails": "[{\\" vnicAttachmentId \": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmac7qyja3ao7btb62ckc2sam7m7jf3flhg4yeos766yqa\", \"vnicAttachmentDisplayName \": \"null\", \"vnicId \": \"ocid1.vnic.oc1.iad.abuwcljtzzdwqi4mezd7tere63zltbz62hbsjn2cquhdretpporrc2xa7xta\", \"vnicDisplayName \": \"ESS_Base\", \"vnicPublicIp \": \"129.80.17.26\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuiuehdriil7egerkk4g7jwcfucetakuyoikfjwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaajw2ytmcqu3hg2gx65vrypuuehcjeqmpuxqqkpgfvb46qqywumpq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmacculok4a2hkemlcmyngmtlw46nelnnmmj2ebfrns4ca
resource-name	ESS_Base
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljkuy4vbsqckfdwkna
time-first-detected	2024-10-23T11:00:50.739000+00:00
time-last-detected	2024-11-04T01:19:54.733000+00:00

58. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"\"Subnet Access Type and Public IPs\": \"[{\\"subnetAccessType\": \"Public\", \"vnicPublicIp\": \"129.153.141.229\"}]\", \"vnicDetails\": \"[{\\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcljtjw2ytmaci6337ark4rtrusaskzzwdxh4355phmkxbkblech4biqa\", \"vnicAttachmentDisplayName\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwcljt3bcdg245sp4vaso4yhrbadtixftxgurnnho2wmojllujmjzzahdq\", \"vnicDisplayName\": \"instance-20231012-1531\", \"vnicPublicIp\": \"129.153.141.229\"}]\"}"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqolf64ffmnufzdtsq6beug6y2pxb33yiedeawxou3kiva
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtjw2ytmaccw5fiesycfhpuayklb3c3wyhfqy57yz2cxr4p5cmqca
resource-name	instance-20231012-1531
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:52:46.846000+00:00
time-last-detected	2024-11-04T01:19:54.525000+00:00

59. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmaccw5fiesycfhpuaykylb3c3wyhfqy57yz2cxr4p5cmqca", "Public IPs": "[129.153.141.229]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d6uswktbascbld6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngya]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyqekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfilgemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfcetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwb252lf3ofy5aflj37h7evsrkpwwu3xuxzywgu5b3ma
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmaccw5fiesycfhpuaykylb3c3wyhfqy57yz2cxr4p5cmqca
resource-name	instance-20231012-1531
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T10:52:46.846000+00:00
time-last-detected	2024-11-04T01:19:54.520000+00:00

60. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmacowxxow37yrnmycnjquwi367gfjkwheaxclvzerxu3va", "Public IPs": "[129.213.54.117]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d26uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngya]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapygeekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfilgemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7wcfucetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcsg43yr5tust3q62l6kvqibrws5sud2rt4agjcca6p3q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacowxxow37yrnmycnjquwi367gfjkwheaxclvzerxu3va
resource-name	ess_test
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:49:50.584000+00:00
time-last-detected	2024-11-04T01:19:54.720000+00:00

61. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[\"Public\"]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmacj6n745priuc4j7jicvdtbzlw2oylmvoluri4q5aq"}, {"vnicAttachmentDisplayName": null}, {"vnicId": "ocid1.vnic.oc1.iad.abuwcljtlm27lgp4fjsb5taxf3wady7tsjuharq77z3rmzmwlgy4c4j7nwbn"}, {"vnicDisplayName": "ess_test"}, {"vnicPublicIp": "129.213.54.117"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaaa37l7tpuieuhdriil7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq4y4sgaoueoahetw3nci6z34x5jvg3cmv6gtqadfct7sq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ytmacowxxow37yrnmycnjquwi367gfjkxheaxclvzerxu3va
resource-name	ess_test
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:49:50.584000+00:00
time-last-detected	2024-11-04T01:19:54.724000+00:00

62. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{"subnetAccessType": "Public", "vnicPublicIp": "129.159.87.24"}]", "vnicDetails": [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacmtrzionp6izcwo7fz7v52qulggy5kw7qpznjrkqw2jq", "vnicAttachmentDisplayName": "ESS_GOLD_IMAGE_ENCRYPTION_TEST", "vnicPublicIp": "129.159.87.24"}]}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq46o5my2nhtmaihsxg6l5tzpya5wbutnj7c5e5its2pa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmackruzh4jkspi45oeqaeie5ykmkwhraql7bfjsy6xnga
resource-name	ESS_GOLD_IMAGE_ENCRYPT_TEST
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:43:55.889000+00:00
time-last-detected	2024-11-04T01:19:54.332000+00:00

63. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmackruzh4jkspi45oeqaeie5ykmkwhraqs17bfsjy6xnga", "Public IPs": "[129.159.87.24]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d26uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngyza]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyqekhbdht5s3vkbkan2jd3oqhgwql]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfllqemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7wcfcetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqonzfj4upm4jnsxg43obmeyeauwlbpwk2yeq4mxnm46a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmackruzh4jkspi45oeqaeie5ykmkwhraqs17bfsjy6xnga
resource-name	ESS_GOLD_IMAGE_ENCRYPT_TEST
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T10:43:55.889000+00:00
time-last-detected	2024-11-04T01:19:54.325000+00:00

64. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnqz77hv4wrc6ntj2j4xhk7hikjo2m5dq7tcochv5buba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcltexqo6qmigeesbneybki3azhbtdmnoulkuu2l3cbzb4u276cltl2lq
resource-name	instance-20240311-1652
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:42:16.540000+00:00
time-last-detected	2024-11-04T01:14:00.488000+00:00

65. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyjq2ov6jtsjqqrny7lpstk6ieuvn5gynscge6y3esia
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwclite4g6gjlwitrlcdzdiium3mlw27syb2ouw5ivr3hgxf4b3l7p4tfca
resource-name	sshtest
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:40:24.567000+00:00
time-last-detected	2024-11-04T01:19:51.688000+00:00

66. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqar2fmchopebccluauhgfujinke5p6zhazntoemlhbstq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtzwdwqi4mezd7tere63zltpz62hbsjn2cquhdretpporrc2xa7xta
resource-name	ESS_Base
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:39:36.376000+00:00
time-last-detected	2024-11-04T01:19:54.418000+00:00

67. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqs3jgig7wsklvoftqfw2u2sny2iw6aj4c5mw2mv5buczq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtibyo16svemuexpakvnticrowvmdm3mayvrqkf357vvk4ds5bq
resource-name	database23ai
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:38:33.874000+00:00
time-last-detected	2024-11-04T01:19:51.333000+00:00

68. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqn5mtswizkjh2vwz5fcv4uxr3vvlbqtqxqedo5vus6oq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtp4etfm4ovt3auso5o2ghosetdv5cggeyyxp4nzm3j6m6wv4zwxyq
resource-name	ESS-Collection-VM01
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:35:25.790000+00:00
time-last-detected	2024-11-04T01:13:58.588000+00:00

69. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwxqt4or3yajxrsotdhlgl47bjhuv5hzf5qm3zmmcbkbg
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtdioap3ldms45juf2jeqp6ynj5ej6yjmj24prxqy3akan2lrqmxng
resource-name	ess-discovery-vm02
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:35:58.742000+00:00
time-last-detected	2024-11-04T01:13:59.527000+00:00

70. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjybhaoa
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqflawuhbcwzxyxm73ogv22efdhuvkxratddby527inug
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtvft73y5lhgczbuhu6dshxsvyj63w4n4xtkytywcuo2eqh5aq7yua
resource-name	cogs-image
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:34:22.640000+00:00
time-last-detected	2024-11-04T01:13:28.606000+00:00

71. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjybhaoa
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqqg5nlsis3fw3ly62uc7axajnoo2wajsevslzpl7ih2zrq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtk2fzqttlwowawgtfgknds6x52hvdd7et7mgumepccwxrouuyv4bna
resource-name	apps
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:34:21.439000+00:00
time-last-detected	2024-11-04T01:13:28.879000+00:00

72. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwowxsizhxmlpm3ham5b7ufuz6aezvn6io4bbpq44lc7hmq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtsvvwmjkpanj3u3i6eg5gngkpyk2jveq5j5fuuxpgvsnmjebfucta
resource-name	CSSNavGW_Mihai_2.0.3
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:34:31.653000+00:00
time-last-detected	2024-11-04T01:13:38.696000+00:00

73. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqu772mribuamnkqycvdwygxr7ws7ox4eqpu6dmvu5ata
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt4k4g5aglccicysrdo5pbmxwfn6l6yfxfcer75wgm6qyebb45vko
resource-name	css-gold-image-test-20240213
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:33:15.065000+00:00
time-last-detected	2024-11-04T01:13:58.773000+00:00

74. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaotf7w4qhroknuayke3ddflc3pup6f6o52foknpscik62g7o3qbe7a
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2di2nc2envml5hpeqmhbbybxna5ofoyyqh5cvizuqndkq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtsua2fzyhaeijspvfpjiznzbo5rhrcq2kyfulfavxjzllibshug
resource-name	essgenai
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:33:29.344000+00:00
time-last-detected	2024-11-04T01:13:42.858000+00:00

75. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnsib4pfxqz4zk6iq7wxojkvxafed6sfwpl6rhhp3elq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt6jls6e72jxnjkfu2lvzn43o5gy4uqq337mty2g2gwellix3uq
resource-name	css-tools-vm-prod
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:33:37.522000+00:00
time-last-detected	2024-11-04T01:13:59.579000+00:00

76. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmackjwpywyqigcqzbg7v7niqmwjxclnglsdvm6xyxx5a", "Public IPs": "[150.136.166.214]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d26uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngyza]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyqekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfilmemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7wcfucetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqeiai5dgdwbsiglislcxbemljp23f4nslbx2eklkdu3a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmackjwpywyqigcqzbg7v7niqmwjxclnglsdvm6xyxx5a
resource-name	ESS_test_prod_customer_side
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:30:35.003000+00:00
time-last-detected	2024-11-04T01:19:54.758000+00:00

77. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyqptssf2z4nlvx7o4jeqxyxmpk6lt5ik3nqenblecea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtti444tdhler6le2u57tnt6plahpjep3upte6oe3y6ghmeja2mqa
resource-name	ESS_GOLD_IMAGE_ENCRYPT_TEST
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:30:35.038000+00:00
time-last-detected	2024-11-04T01:19:54.519000+00:00

78. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIp\": \"150.136.166.214\"}]", "vnicDetails": "[{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwcljtw2ytmacponggrcrqio6vglmml6ob2x524etxpcaz3322pk6isvq\", \"vnicAttachmentDisplayName\": \"ESS_test_customer_side\", \"vnicPublicIp\": \"150.136.166.214\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnhuskin5mabjqjgwp4htt5jjm6kdeu36f3na4xasggshq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmackjwpywyqigcqzbgt7v7niqmwjxclnglsdvmmm6xyxx5a
resource-name	ESS_test_prod_customer_side
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:30:35.003000+00:00
time-last-detected	2024-11-04T01:19:54.762000+00:00

79. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqsy55e5phho4fvx7qhmhhonb7pmlvfb6zgykh7pueu4a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtz2am5sfh55gxn72nvr3ux6igqi2be537qw2ngrtwcahmhghd4q
resource-name	instance-202
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:29:48.391000+00:00
time-last-detected	2024-11-04T01:14:00.377000+00:00

80. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaaruvh4k52jh77u4jbv7vhin3osfirqpnko4yobhh3bmnga4kt4saq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcquequqko7iv5xppjdzijcjcfqxpkfqaqtp3gw24z3ybiq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwclitmcorn6ndbo72qmid7ywq3xs45laocm46jittwq7246sf74qf3nha
resource-name	security-health-checks-demo
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:28:49.574000+00:00
time-last-detected	2024-11-03T12:13:48.400000+00:00

81. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6jizmmj4mq4aeyz45wejraqqal7a6kk2cp224rg7d4oq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtnlf2rlsxjeayo7ftddz6hx7hpbgwjlmrnwnoq7zzxb23db52cla
resource-name	instance-20240829-1122
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:28:25.738000+00:00
time-last-detected	2024-11-04T01:14:00.169000+00:00

82. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqrj2l7uixc52dqtnlj24773h7xrugi6rdgl2o53vqatta
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljutxtisngjffijmovaugjqlhbymynk33zc5wpghx64rrjllusb5cy33q
resource-name	css-tools-vm-oracle
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:28:53.257000+00:00
time-last-detected	2024-11-04T01:14:00.470000+00:00

83. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkhr4hxymb5zjnbsoclno2wsq2rjyjgol5gzbakptaya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt6ew6ugpiupbjiwai776iuqzfqcd7taqot5pxgshgwwad73gadgq
resource-name	ess-compliance-prod01
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:25:05.620000+00:00
time-last-detected	2024-11-04T01:13:59.671000+00:00

84. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq326mncvizkwjnebt32iuouc4ubqb66j7dy4xcexvtwna
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtrcq6bnsmqoiyhxsncgfnv5dc5kkqancw74srxwr7fmnegp6o3l2q
resource-name	CSSCOGSVM
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:24:02.820000+00:00
time-last-detected	2024-11-04T01:13:59.571000+00:00

85. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyfb2ys7fbioxzhqc74x4erlygbrievmtkxcjksimv5a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtkwlhbagelxn22ly6m4au5yfwajkzvtypbktxsgkhfj6yp5lcywa
resource-name	VMMIHA1
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:24:04.868000+00:00
time-last-detected	2024-11-04T01:13:42.862000+00:00

86. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqr4zi6p6txlpcq67xbqyvls4bkfxqv3x6bhbhfik6b2q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcltsdyo4efguxumek7dks4lzeh32nw4m2ivlyl5hudcrehgjzw7g3ma
resource-name	instance-20240422-1435
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:23:33.940000+00:00
time-last-detected	2024-11-04T01:19:55.318000+00:00

87. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcquqssvjna4gjpaelmdykq6ckckkk5dmdrvp5ll4f6vqdq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtmlpapsnmieryh27qmsoilkojzezrueoioufvvcvf77i32fwumpq
resource-name	sshdb
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:22:28.184000+00:00
time-last-detected	2024-11-04T01:19:55.391000+00:00

88. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmacvwelzz6kltneqq3wrnusu4iae7ywt6bfek3wwr2tb6a", "Public IPs": "[150.136.247.96]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d26uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngyza]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw2sijnfq2tgbapygeekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfilmemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7wcfucetakuyoikfljwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvdpox4lrzr2jqkqeaspuf23ag5x5sjw3nayt36efxqa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacvwelzz6kltneqq3wrnusu4iae7ywt6bfek3wwr2tb6a
resource-name	ESS_test_prod_oracle_side
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:22:08.305000+00:00
time-last-detected	2024-11-04T01:19:54.619000+00:00

89. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[\"subnetAccessType\":\"Public\",\"vnicPublicIcp\":\"150.136.247.96\"]", "vnicDetails": "[{"vnicAttachmentId": "ocid1.vnicattachment.oc1.iad.anuwljtjw2ytmacadanza2dyuzo6svst5c7nqwel5dbaijq3f1cg3urrj2q"}, {"vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.iad.abuwcljtc7ewcnacdgcwmnsmcqk5v4rv7zejoetbd2goce7illyakt3ldzpmq"}, {"vnicDisplayName": "ESS_test_prod_oracle_side", "vnicPublicIcp": "150.136.247.96"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuiuehdriil7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqr4dy5rl4hctoq37yho2rn4ikcarjvcy5uiikyn5wrbma
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ytmacvvelzz6kltnegq3wrnusu4iae7ywt6bfek3wwr2tb6a
resource-name	ESS_test_prod_oracle_side
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:22:08.305000+00:00
time-last-detected	2024-11-04T01:19:54.623000+00:00

90. Problem details for INSTANCE_WITH_PUBLIC_IP

Key	Value
additional-details	{"Subnet Access Type and Public IPs": "[{\\" subnetAccessType \": \"Public\", \"vnicPublicIclp \": \"129.158.211.112\"}]", "vnicDetails": "[{\"vnicAttachmentId\": \"ocid1.vnicattachment.oc1.iad.anuwljtjw2ymacszgxuyjceunipsfmm7x7yhwtodaahglxxbfwk5gca\", \"vnicAttachmentDisplayName\": null, \"vnicId\": \"ocid1.vnic.oc1.iad.abuwcltg6st4wiputtc76wflgdke3vwomy7us6musrpibilwnapphdye7ua\", \"vnicDisplayName\": \"ESS_GOLD_IMAGE_TEST\", \"vnicPublicIclp \": \"129.158.211.112\"}]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuiuehdriil7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Checks public IP only
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_WITH_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqy5q2xqu3az2cumuac7h3ighcfxivavyfhvdnn5vwcug
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "COMPUTE", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For example, you do not want to accidentally allow internet access to sensitive database instances.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwljtjw2ymacb66oh24yeasdgef7shlyixgksg4pqmxvt2jk26od24a
resource-name	ESS_GOLD_IMAGE_TEST
resource-type	Instance
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:20:46.235000+00:00
time-last-detected	2024-11-04T01:19:54.537000+00:00

91. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqewujx2iroqlpey7pvvxjmngsjoisb77qbauuf25l6ra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtj2dhd6oyqj5ruexnre42jd35xs64scsl6qclihibotwuxgxu2lwa
resource-name	instance-20240930-0737
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:20:42.293000+00:00
time-last-detected	2024-11-04T01:19:51.414000+00:00

92. Problem details for INSTANCE_PUBLICLY_ACCESSIBLE

Key	Value
additional-details	{"Instance OCID": "ocid1.instance.oc1.iad.anuwcljtw2ytmacb66oh24yeasdgef7lshlyixgksg4pqmxvt2jk26od24a", "Public IPs": "[129.158.211.112]", "Route Table OCIDs": "[ocid1.routetable.oc1.iad.aaaaaaaaam2d2uswktbasclbd6jx3k3m4nx2n5ntcdptjkjeaeavnlnqngyza]", "Security List OCIDs": "[ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyceekhbdht5s3vkbjkan2jd3oqhgwq]", "Subnets": "[ocid1.subnet.oc1.iad.aaaaaaaaeak5b63rcjd764l2j4vhxqecpns3d3mpm75plcfliigemtiyjbaa]"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfcetakuyoikfjwfsrdtya
description	This detector rule identifies all instances that have a public IP assigned and reside on a public subnet reachable via an Internet Gateway, has a route table entry to the Internet Gateway and allows traffic from any protocol.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	INSTANCE_PUBLICLY_ACCESSIBLE
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhhj73whasa7fz6scraluvaofsdmb2vwewciemf2c5awa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Compute", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Carefully consider allowing internet access to any instances. For an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet or in VCN NSG ingress security rule, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.instance.oc1.iad.anuwcljtw2ytmacb66oh24yeasdgef7lshlyixgksg4pqmxvt2jk26od24a
resource-name	ESS_GOLD_IMAGE_TEST
resource-type	INSTANCE
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T10:20:46.235000+00:00
time-last-detected	2024-11-04T01:19:54.533000+00:00

93. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqtbu6x3kwz2kmhjhps6lf3vwnzaymjeb3dwijvxamyka
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcltoliaenygzxdbzu343utwew5nczsdpqzvu5iu7ckkp6hvryflcfa
resource-name	instance-20240328-1158
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:53.062000+00:00
time-last-detected	2024-11-04T01:19:51.487000+00:00

94. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqlgvcciw2ymewxbqwpuiony4uukfd3mbk3zjvcyiq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtu52iftylb67o4lkoi5l42dprqxirsnlkd4ejux6zj24s3nfdh6qa
resource-name	css-tools-vm-prod-oracle
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:41.686000+00:00
time-last-detected	2024-11-04T01:13:59.478000+00:00

95. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjybhaoa
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqrdfjy4giuitfow6kjn744wzbr47r5267zrfqr6wbwuja
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt5j2qjnbdhloar5ezveiqcintvn6ab7robphq75x3umbxdwmh3mga
resource-name	esb-prod-12213
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:33.768000+00:00
time-last-detected	2024-11-04T01:13:28.495000+00:00

96. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbw6t7wa7panz3ejpq3nbys7cuteymgnhstupo7w24jq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtlm27lgp4fjsb5taxf3wady7tsjuharq77z3rmzmwlgy4j7nwbna
resource-name	ess_test
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:56.760000+00:00
time-last-detected	2024-11-04T01:19:54.610000+00:00

97. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqox445ud6b5ktgjujuam3k6vp5hbdqyztcv3b2ts4euxq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljta5bgmia3yhxo12uqlupmrel5guwazgtl67wjyv4a3vwwfkvfj5woa
resource-name	vm-ruchir-new
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:38.117000+00:00
time-last-detected	2024-11-04T01:13:39.374000+00:00

98. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdfq5jawnbrxkuoo7ated7rq6uxzxfufzayd7evntjqa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt5pslypogs5jsxpaxn4kpwa5riyeeaomdcec44yyxhiur3xuww43a
resource-name	UAT-VM-RICK_1.5.4
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:23.002000+00:00
time-last-detected	2024-11-04T01:13:38.656000+00:00

99. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqumzhtnztbxvkqr4f4vbzhcxtjsuh7gt2v3v377ljra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtwuc34uzfihmv323zfgoxdkmtauq6bz2y3mdrqjk3o2sncoecdca
resource-name	css-gold-test2
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:19:15.137000+00:00
time-last-detected	2024-11-04T01:13:59.689000+00:00

100. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3n7u7wig5meezjaqy6uugc3tt66rkhfm4xyer5pe27a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt3uyramxtbpkkjxeklmnpfrzepxecivhs3yud7pmthduvgxotvuqa
resource-name	CSS-ESS-Gold-Image-Prod-test01
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:18:49.073000+00:00
time-last-detected	2024-11-04T01:14:00.171000+00:00

101. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqedzegbll6n7r4ibmoayprfytv7y254acqq6kfs2foa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt45soiookq6cwlwca33igj5dqnylmpdf2d2zle3cijleobsrrcu
resource-name	ess-cd3-vm01
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:18:57.086000+00:00
time-last-detected	2024-11-04T01:14:00.012000+00:00

102. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqepga5jd4p5e3seuse3fdbumlq5wp7bgbt744cry6osca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtqz257653enwtqhg44hbcxjvdgo6ltk4lsxcpadeoqzkrqkulddla
resource-name	essuat-discovery-vm02
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:17:08.193000+00:00
time-last-detected	2024-11-04T01:19:51.409000+00:00

103. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnxzu3brns4cyuvnqy4q6su5azvcfpj3yaxk4hkovme2lq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcltc7ewcnacdgcgwmsmcqk5v4rv7zejoetbd2goce7lyakt3ldzpmq
resource-name	ESS_test_prod_oracle_side
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:17:52.583000+00:00
time-last-detected	2024-11-04T01:19:54.395000+00:00

104. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqoxfaia46fulxd52k4ovxkcdp6basakisl4dgbrl4iq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt33o4tlmmstyxt5fnx7srrhkzogymv6fmviwddd274ukjv2gchxq
resource-name	instance-20240313-0904
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:17:10.548000+00:00
time-last-detected	2024-11-04T01:13:59.477000+00:00

105. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqs3do74rlv44isnyu6rpbkq6ut7fr2pnad3xy3eautkua
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljfmnhkx4xadzrstayj7l57grs2eyhvkmatlvpdoj6jbozzo5nwmq
resource-name	instance-20240602-1514
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:01.744000+00:00
time-last-detected	2024-11-04T01:19:51.533000+00:00

106. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqrsbalbiyy5v4ma5dl2rx2xk7qn2xpparilm7kl265a6q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtiqjachz7nnncbx57wqm4vmochcd4anlgwtam2hqagrz62d6taiq
resource-name	instance-20240326-0843
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:33.980000+00:00
time-last-detected	2024-11-04T01:14:00.398000+00:00

107. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqilx2vdpd5dcqjlyb7d7qbrr4lwfwpq4w3gcmljp253tq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljthratzi4bbby6rbh3sxx2u3g4qe2xprczbani7uwm2ugtirq7u3mfq
resource-name	instance-20240321-1427
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:06.978000+00:00
time-last-detected	2024-11-04T01:13:59.519000+00:00

108. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqifbbpdbymiwtrunx2bav2d4pfrmzdj4kdfhd5hrrsoa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt3bcdg245sp4vaso4yhrbadtixftxgurnnho2wmojjljmjzzahdq
resource-name	instance-20231012-1531
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:37.953000+00:00
time-last-detected	2024-11-04T01:19:54.661000+00:00

109. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7cyhniasvqxueuhwx4gbmanbnjmjhabsc3doi25ycneuq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljt4n7uaollmannph7q2ugflfp4myhoslwvdvsne4skhh6sj66d2nma
resource-name	ess-uat-db01
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:07.452000+00:00
time-last-detected	2024-11-04T01:19:51.531000+00:00

110. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyp7tmcylb5nanta54spqezeblysaov5sasroiqcivrq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljth3sgb5wnh3u3eb2b7qmk5wiru6kbi3jgr4izvkd6iosvk4agwrua
resource-name	ESS_test_prod_customer_side
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:32.328000+00:00
time-last-detected	2024-11-04T01:19:54.615000+00:00

111. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkrr7hp4h4p357j5ysnxj4u5kx23542hiax3w3ehhpswa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtj3hkvsid3ykjszcx6zw47gjdmlcjpfilogv46plrdrfj7kcfwnmq
resource-name	UATVM_RUCHIR
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:16:52.145000+00:00
time-last-detected	2024-11-04T01:13:42.800000+00:00

112. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfj6z5errquq4doxquj6uhyh2aqi6zvxeqjicaneq2cbq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcljtraww3nm5zrv7hsylgqlpuwz7aovupmvfnexijtec5q6epueohhq
resource-name	instance-20240513-1445
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:15:57.005000+00:00
time-last-detected	2024-11-04T01:19:51.633000+00:00

113. Problem details for VNIC_WITHOUT_NETWORK_SECURITY_GROUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	A virtual network interface card (VNIC) is a networking component that enables a resource such as a compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN. An VNIC with an NSG may trigger a connectivity issue.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VNIC_WITHOUT_NETWORK_SECURITY_GROUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjzmp4ui4llyr5eb5yrwmx2b2omqtsiaju5y6e4noka
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["COMPUTE", "Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the missing NSG association from this VNIC is expected.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vnic.oc1.iad.abuwcltg6st4wiputtc76wflqdke3vwomy7us6mxrpibilwnapphdy7ua
resource-name	ESS_GOLD_IMAGE_TEST
resource-type	Instance
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T10:15:44.429000+00:00
time-last-detected	2024-11-04T01:19:54.710000+00:00

114. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jfifiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo3d3jjzvx6ofhqxgmfbakcik7k7dnlb7m5dnpyfsqky
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jfifiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.169000+00:00
time-last-detected	2024-11-04T02:44:49.466000+00:00

115. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "ravi.srinivasan@oracle.com", "Password Time Created": "2023-12-19T22:07:12.253Z", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusksaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfttrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqz6ogjggd56curhg7xqqukmfsrj7nscvny35g6y3wj4a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusksaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.183000+00:00
time-last-detected	2024-11-04T02:44:49.479000+00:00

116. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2yemg2dgxkwkhrs6oeg3tpewezo6bxpapk2raapphnyta
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.108000+00:00
time-last-detected	2024-11-04T02:44:49.365000+00:00

117. Problem details for VCN_HAS_INTERNET_GATEWAY_ATTACHED

Key	Value
additional-details	{"internetGatewayId": "ocid1.internetgateway.oc1.iad.aaaaaaaaakhkjpyso62nf3crl7glbjp3dd5vtg4tkt3drmvlstvcqjpaefshq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7wcfucetakuyoikfljwfsrdtya
description	Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VCN_HAS_INTERNET_GATEWAY_ATTACHED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq75irlekhm67mvxkcwot4wwe24np33td5f3op7urzzqdq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vcn.oc1.iad.amaaaaaajw2ytmaai2drkcn6ansvlyax5j4qeehkd4i7dsiuufwdtvb5xva
resource-name	ESSVCN
resource-type	VCN
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.067000+00:00
time-last-detected	2024-11-04T01:37:47.330000+00:00

118. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qreo7bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq3rpvb5rqiapuezmdu7kkys5qvgsntadwqgdy2i5heja
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qreo7bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.261000+00:00
time-last-detected	2024-11-04T02:44:50.172000+00:00

119. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "ea:99:63:00:dc:29:e5:ca:58:55:ba:47:7f:db:8b:0d", "IAM API key too old for user": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaqqdczpzzp6ymhppfymqi7hnd3h4mxlmer2bnlyznhcjzidoqzng"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3cyu5fwlt3u2caxnwhhhz562y6ikcrtz3q7hhu7yflq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaqqdczpzzp6ymhppfymqi7hnd3h4mxlmer2bnlyznhcjzidoqzng/ea:99:63:00:dc:29:e5:ca:58:55:ba:47:7f:db:8b:0d
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaqqdczpzzp6ymhppfymqi7hnd3h4mxlmer2bnlyznhcjzidoqzng/ea:99:63:00:dc:29:e5:ca:58:55:ba:47:7f:db:8b:0d
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.066000+00:00
time-last-detected	2024-11-04T02:44:50.404000+00:00

120. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{"ICMP": "3", "TCP": "22", "vcnDisplayName": "ESSVCN", "vcnId": "ocid1.vcn.oc1.iad.aaaaaaaaajw2ytmaai2drkcn6ansvlyax5j4qeehrd4i7dsiuufwdtvb5xva"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaa37l7tpuieuhdril7egerkk4g7jwcfucetakuyoikfljwfsrdtya
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq7zps6w53n2phacrrirj4cnrl6turkclfrhdz75oxlita
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaavw2pcflw62sijnfq2tgbapyqekhbdht5s3vkbjkan2jd3oqhgwq
resource-name	Default Security List for ESSVCN
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.906000+00:00
time-last-detected	2024-11-04T01:37:46.978000+00:00

121. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T18:32:33.796Z", "User Name": "manish.kakade@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqzi4q7mfs/wsqrbcy7ycdctvfitygs7flyouz5wievwa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuiq5poiwsmbtu2a6epswdfwcrxbsm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.185000+00:00
time-last-detected	2024-11-04T02:44:50.537000+00:00

122. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "Autonomous Transaction Processing"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqsu2fykejmbmad4e44heghqczlq7awt1pyla
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpksr5mjt37yp55gftoraxkvplskwm5qr xlk4pvh3dta
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.autonomousdatabase.oc1.iad.anuwcljsjw2ytmaahxl7wrssoxhurpzy5ffo4wph2hzis4z7dru45ej3l7ja
resource-name	UAT_DB_MIHAI
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:50.643000+00:00
time-last-detected	2024-11-04T01:37:06.875000+00:00

123. Problem details for VCN_HAS_INTERNET_GATEWAY_ATTACHED

Key	Value
additional-details	{"internetGatewayId": "ocid1.internetgateway.oc1.iad.aaaaaaaaak3u4ekmhvvhmeinz656oerbezumlipaexoyzqsowy3ugwb3fra"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zxh633c7amzi5zaozoygg
description	Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VCN_HAS_INTERNET_GATEWAY_ATTACHED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyqmt36zudmjf43tew4fhx2vfdtr6q2hs3iv5zql6xpsa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vcn.oc1.iad.amaaaaaajw2ytmaaxlvfb27g5b2vb3r7zfid2vhxknete2j22rixel2g2l3a
resource-name	ACS-VCN01
resource-type	VCN
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.978000+00:00
time-last-detected	2024-11-04T01:37:41.532000+00:00

124. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "DB System"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfle6ecnfa52ffdsp45sezhlgwvxeyqir3r6ytkjlm3ha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dsbsystem.oc1.iad.anuwcljtjw2ytmaa2s5hn6otglpbegxovntiojyrnojiccmaomsuxenbhxa
resource-name	DBSystem-202401031146
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.073000+00:00
time-last-detected	2024-11-04T01:37:51.576000+00:00

125. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "harinath.subramaniam@oracle.com", "Password Time Created": "2023-09-12T23:38:25.501Z", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyvj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhsdmwx4am764y6nznxcicmj6u4yh6r3irr7rfix3rpa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyvj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.686000+00:00
time-last-detected	2024-11-04T02:44:50.473000+00:00

126. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "allow group ACS_ESS_Data_Safe_Admin to manage data-safe-family in tenancy where request.region=iad,allow group ACS_ESS_Data_Safe_Admin to manage data-safe-family in compartment ESSDEV,allow group ACS_ESS_Data_Safe_Admin to manage database-family in compartment ESSDEV,allow group ACS_ESS_Data_Safe_Admin to manage target-databases in compartment ESSDEV,allow group ACS_ESS_Data_Safe_Admin to manage data-safe-private-endpoints in compartment Networks,allow group ACS_ESS_Data_Safe_Admin to manage target-databases in compartment ESSDEV,allow group ACS_ESS_Data_Safe_Admin to manage data-safe-assessment-family in compartment ESSDEV,Allow group ACS_ESS_Data_Safe_Admin to manage object-family in tenancy,Allow service objectstorage-us-ashburn-1 to manage object-family in tenancy,Allow service objectstorage-us-ashburn-1 to manage object-family in compartment ESSDEV")}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user/group> to manage <some-resource> all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqt2acf6t764bsmwqtvjkxbmdr3nmuzgucjq5uwjtm32q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaa3c4x6vtw2cbu6qh63b6gcfsmhikdjrrbuol5qminpxf373yo5va
resource-name	ACS_ESS_Data_Safe_Policies
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.179000+00:00
time-last-detected	2024-11-04T02:44:50.475000+00:00

127. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Created": "2023-05-19T19:00:57.254Z", "User Name": "mihai.alistar@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqybmd5nghoe3pshi4on2yllk2xz7yag6cxdzypud5whq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.370000+00:00
time-last-detected	2024-11-04T02:44:49.386000+00:00

128. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxujfixv4ggr3goyuh7nzqvhgmywjtyv2gremkonekoq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.165000+00:00
time-last-detected	2024-11-04T02:44:49.463000+00:00

129. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4cjyeakunrnuzrlt6nickkrc4rcvwccmwidb5glds2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefyzdwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.265000+00:00
time-last-detected	2024-11-04T02:44:50.175000+00:00

130. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq244tls3gq3l4c5e4mj6wu2h7mdgdq2eqxzcaf6ewuf2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.187000+00:00
time-last-detected	2024-11-04T02:44:49.482000+00:00

131. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1.aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq63mywqademqaigjagk4qmr6ql73k36w7scbcoanwkocq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1.aaaaaaaaadax27hchavycud6us5jzfiriscygbaydusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.157000+00:00
time-last-detected	2024-11-04T02:44:49.456000+00:00

132. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqulzkzw6f5riuwe3ffqwfqjktsftcwuundhhisutyzq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.596000+00:00
time-last-detected	2024-11-04T02:44:49.280000+00:00

133. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqascrsxp7upc5lir2uogh6ht2ze33ivmpnusljce6ja
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.202000+00:00
time-last-detected	2024-11-04T02:44:50.554000+00:00

134. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqafpt5yh27wrb2kmpz4ucdh7a73a7t3wxxyqmidosuxlq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.169000+00:00
time-last-detected	2024-11-04T02:44:50.532000+00:00

135. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-09-24T17:18:09.043Z", "User Name": "yevhen.udod@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqstny73f733ddgxo2jos7jdcl26fhwpeyzzz63l6mda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xbq55w6s3tgcxpdnpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.519000+00:00
time-last-detected	2024-11-04T02:44:49.388000+00:00

136. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "Allow service objectstorage-us-ashburn-1 to manage object-family in tenancy"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user group> to manage <some-resource all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpk3pnfefemgo62gqqay2cfubf7qasvpnrhbztnl7pkxma
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaa4u3kccby26ixgjpnbmxzvndlodegvw4hgkwpce7b75ro274cce4
resource-name	FunctionsServiceObjectStorageManageAccessPolicy-c7f3
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.275000+00:00
time-last-detected	2024-11-04T02:44:49.751000+00:00

137. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7r4i7pibepa5ajjfd5c42tftqy66pzisecire22gt75a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.233000+00:00
time-last-detected	2024-11-04T02:44:50.188000+00:00

138. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvtta2xuc7x53wotbmds5a5vt2z4ddc5lxbk55absz7vba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.516000+00:00
time-last-detected	2024-11-04T02:44:49.384000+00:00

139. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqlex4tqh2pakijxyzscv44xiwwuidj6quuy6xdq7hmmsa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjvj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.662000+00:00
time-last-detected	2024-11-04T02:44:50.452000+00:00

140. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfjohqrhtjmxfhlid5ddct6l45qpuch45wgcwks2spva
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.249000+00:00
time-last-detected	2024-11-04T02:44:50.204000+00:00

141. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq25gxzhpbmbxrd43etqr3rewu7npkv4i5ghnvs52zba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.566000+00:00
time-last-detected	2024-11-04T02:44:50.186000+00:00

142. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcquae4v4ynig5pcjtmf2bew7nipxb5ek25v5mtcbd5mwhq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.533000+00:00
time-last-detected	2024-11-04T02:44:49.769000+00:00

143. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq5uz3cgnb7yhl5q7xxtvgijqm5n6hm7pubk5gybv5or6la
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.553000+00:00
time-last-detected	2024-11-04T02:44:50.172000+00:00

144. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "da:09:98:f8:de:59:33:99:72:0:c:8:f6:a:6:a:8:c:4:2f", "IAM API key too old for user": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvdy3zbddxw43sdofyb7mx3yapvk4v4z7ckbdklci7ua
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwylo/a:da:09:98:f8:de:59:33:99:72:0:c:8:f6:a:6:a:8:c:4:2f
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwylo/a:da:09:98:f8:de:59:33:99:72:0:c:8:f6:a:6:a:8:c:4:2f
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.555000+00:00
time-last-detected	2024-11-04T02:44:50.160000+00:00

145. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2mxhesfgj7oz5wq4mywmyzycs5gxinksccrvlwazda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.505000+00:00
time-last-detected	2024-11-04T02:44:49.434000+00:00

146. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "ricardo.e.acosta@oracle.com", "Password Time Created": "2024-02-08T18:34:37.295Z", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4aqjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqv2kzo3i3ohouelj4ceizfiipyknr3b4rbshroshjca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4aqjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.591000+00:00
time-last-detected	2024-11-04T02:44:49.274000+00:00

147. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwr43zumec2zjcavr6uoaihz4l74ne6qdkscjr3cb52q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.163000+00:00
time-last-detected	2024-11-04T02:44:49.443000+00:00

148. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcxu4zvg2ebih4ryx3eiat6gmwnm4ntxmlucmsbkux6qq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.510000+00:00
time-last-detected	2024-11-04T02:44:49.378000+00:00

149. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq55s6ubdas6n47feecxm3or6pcdeuqer642ago6aauvkq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.047000+00:00
time-last-detected	2024-11-04T02:44:50.439000+00:00

150. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5phuhh6xu2hsn5til623iswepgkp3tjswyb7xfbatla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.665000+00:00
time-last-detected	2024-11-04T02:44:50.455000+00:00

151. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphic232o4qhdblhdwp5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkjaikh2sjhvhk7fe4vk5jznafvsjbyk2axkin4spsq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.100000+00:00
time-last-detected	2024-11-04T02:44:49.359000+00:00

152. Problem details for DATABASE_SYSTEM_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-29T08:14:14.421Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Database system patches often include updates that eliminate known security vulnerabilities. Raise a problem when a database system is discovered which has one or more patches, available for 90 days or more, that have not been applied.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_SYSTEM_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqv5ueshvvt3sco62dcthiydym2zq76f4aemj4p53mqla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the DB system as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaak3llbp3gmaefyaqd7ugowvnfbynfdhhwpxjigx72q6a
resource-name	DBSystem-202403280916
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.023000+00:00
time-last-detected	2024-11-04T01:37:08.652000+00:00

153. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7dihy6gnqhrl2x6ulgpgrvcdzxji724uo5dwipcbta
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.582000+00:00
time-last-detected	2024-11-04T02:44:49.251000+00:00

154. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqugfn5h47bd4oahbhvrlrtdi3rlapqtkfijztnhauza
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xbq55w6s3tgcxpdnpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.507000+00:00
time-last-detected	2024-11-04T02:44:49.374000+00:00

155. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "allow dynamic-group FunctionsServiceDynamicGroup-c7f3 to manage all-resources in compartment id ocid1.compartment.oc1..aaaaaaaaotf7w4qhroknuayke3ddfc3pup6f6o52foknpscik62g7o3qbe7a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaotf7w4qhroknuayke3ddfc3pup6f6o52foknpscik62g7o3qbe7a
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user/group> to manage <some-resource> all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq752r2cqrlrmhruummpgtz7skpjgbaqigakvqlmf2vomq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaiovj72fix3ak7gshdpqydzfqyh3kj2dhjzhdmv3ldu5garc4zmq
resource-name	FunctionsServiceDynamicGroupPolicy-c7f3
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.352000+00:00
time-last-detected	2024-11-04T02:44:50.455000+00:00

156. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqynequermbtm4v5n2x7bthstv2grivy3thg6j6z2baooq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.504000+00:00
time-last-detected	2024-11-04T02:44:49.841000+00:00

157. Problem details for DATABASE_SYSTEM_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-29T08:14:14.421Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Database system patches often include updates that eliminate known security vulnerabilities. Raise a problem when a database system is discovered which has one or more patches, available for 90 days or more, that have not been applied.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_SYSTEM_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcquddzqclj6ozhnua543ajsqkzxatmc2pl5nn775j4mnra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the DB system as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaa2s5hn6otglpbegxovntiojyrnojiccmaomsuxenbhxa
resource-name	DBSystem-202401031146
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.064000+00:00
time-last-detected	2024-11-04T01:37:50.831000+00:00

158. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqi5jogu46xwcsxa5cw7sje7nqsclejntgapbsnimsxgtq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.191000+00:00
time-last-detected	2024-11-04T02:44:49.486000+00:00

159. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T19:00:36.925Z", "User Name": "anand.poovakkat@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo6fqirfdbtibxrsq75g2kwwdxgt4m3bmvhgxnlgnqca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqt4xjog2wlqqcek3j7mj3avtdsbpha3tiy5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.492000+00:00
time-last-detected	2024-11-04T02:44:49.827000+00:00

160. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6kqpqb3cov43npldyv75z2b4fxifpr2zk4bye5byxq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.187000+00:00
time-last-detected	2024-11-04T02:44:49.465000+00:00

161. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzb5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqghkcrgszcoc5cu5imt5ikxswytlsjmbh15gfvtylea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.524000+00:00
time-last-detected	2024-11-04T02:44:49.393000+00:00

162. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqsulgcd2iutlnl6qcaxpfz3mrjjoxkvjwqso2krseqya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.181000+00:00
time-last-detected	2024-11-04T02:44:49.459000+00:00

163. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7kymb4burqyfm4jktdixq2gpzrx7l4pxn4n4lfkiuq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.558000+00:00
time-last-detected	2024-11-04T02:44:49.419000+00:00

164. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqddjknifoifyxjsyu3fkedisf2zxsg5ogy666tc2cw2tq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.539000+00:00
time-last-detected	2024-11-04T02:44:49.775000+00:00

165. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "ruchir.khanna@oracle.com", "Password Time Created": "2024-02-05T14:46:22.390Z", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqeghx26qwzz4ivvugr35o3bjtabt45k3gond3n7qhhd4q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.246000+00:00
time-last-detected	2024-11-04T02:44:49.186000+00:00

166. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{"ICMP": "3", "vcnDisplayName": "ACS-VCN01", "vcnId": "ocid1.vcn.oc1.iad.amaaaaajw2ytmaaxlvfb27g5b2vb3r7zfid2vhxknete2j22rixel2g2l3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zrh633c7amzi5zaozoygg
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaajw2ytmcpq2o7w57lpbpqjbzfb3ctwilvk7j37742laut3ezy3xq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaag7jgvrsooktpsisjecpx2ivrbvjg5zhtlmem2jymstyagshi435ra
resource-name	security list for private subnet-ACS-VCN01
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpillxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.088000+00:00
time-last-detected	2024-11-04T01:37:42.671000+00:00

167. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqeo3uwqud6rahuaytwlfjbmhomithkd7ks4wxcfryffa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.352000+00:00
time-last-detected	2024-11-04T02:44:49.366000+00:00

168. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdydlf6oigo3yqidgtudzvdvizoplsk6pkzvmbhsxiao
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.693000+00:00
time-last-detected	2024-11-04T02:44:50.479000+00:00

169. Problem details for KEY_NOT_ROTATED

Key	Value
additional-details	{"Key's Time Created": "2023-09-27T02:11:16.406Z", "managementEndpoint": "https://ejsrhdwuacvs-management.kms.us-ashburn-1.oraclecloud.com", "vaultId": "ocid1.vault.oc1.iad.ejrhwdwuacv.abuwcljrutufjt37op2dntu4uiwa2663y5e3tg3cy2uyq4zl7cylmogugq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqgomhmpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	For information security, you should periodically change or rotate, passwords, keys, and cryptographic materials. Rotating your keys in vault reduces the impact and probability of key compromise.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	KEY_NOT_ROTATED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqoywgwayv3yzket3sf3llwfjuznuaoj5cai3yigoroa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["KMS", "CIS_OCI_V1.1_MONITORING", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that you rotate the vault keys regularly.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.key.oc1.iad.ejrhwdwuacv.abuwcljrazeb56i5pqxwe76gqh6j3ps3yfp2kork2onwdz7fizrlhdifmxvq
resource-name	DMS_KEY
resource-type	VaultKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:46.167000+00:00
time-last-detected	2024-11-04T01:37:13.919000+00:00

170. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmqnvdbeprvzwgd53nqqlmq775vviyoiohi5nfmunqda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.481000+00:00
time-last-detected	2024-11-04T02:44:49.818000+00:00

171. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "Autonomous Data Warehouse"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdql5uhy2faat3kovstche4zmq4kfst22a5ecawfh2ica
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.autonomousdatabase.oc1.iad.anuwcljsjw2ytmaa763ra4hi52fj6qqnwb4odq7vmopyr2u2qvaa35fzepnq
resource-name	CSSDB
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.022000+00:00
time-last-detected	2024-11-04T01:37:45.573000+00:00

172. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphic232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq22wfasm6f4h3tmfb2z4zk5szlphrlpmobhdp3sq7bdba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.179000+00:00
time-last-detected	2024-11-04T02:44:49.476000+00:00

173. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfpj5mgfhzedxmrkun3b56itnixepa2cnip3miko4frxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.055000+00:00
time-last-detected	2024-11-04T02:44:50.444000+00:00

174. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq")}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqf5ps3lpsswpezs2k24pb7t1cambj7lxgw25regmeqa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:55.076000+00:00
time-last-detected	2024-11-04T02:44:50.460000+00:00

175. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6pqsfxmlqwqzahz37f3qty5s2kicwgadq5wjkhkomda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.589000+00:00
time-last-detected	2024-11-04T02:44:49.454000+00:00

176. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "ana.delafuente@oracle.com", "Password Time Created": "2024-02-05T14:43:41.355Z", "User OCID": "ocid1.user.oc1..aaaaaaaaagcqielr5qlrljs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5jik4i26ypdljjrh2ltydzmb74ipl3uk25y5ehlhqq2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagcqielr5qlrljs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.487000+00:00
time-last-detected	2024-11-04T02:44:49.866000+00:00

177. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyedjqcinscxdr3jebskqqvbtlvzfm745q7d5qiu2x6iq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.485000+00:00
time-last-detected	2024-11-04T02:44:49.821000+00:00

178. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqcbhalbj4mlnka6ix6gcw4tnbdaoixgdn2ax3uu6uwha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.546000+00:00
time-last-detected	2024-11-04T02:44:49.227000+00:00

179. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagcjielr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqz7sxp3btzo7n2qccpdv6tlewacqjumzbtvn66louoa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagcjielr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.474000+00:00
time-last-detected	2024-11-04T02:44:49.853000+00:00

180. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharjya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7cw3sgrow3mizdlhcjsyqgennjsalpljzxewpoea24aq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.273000+00:00
time-last-detected	2024-11-04T02:44:50.145000+00:00

181. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqdczpp6ybhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5wwpu3jq6r7lyhjgu5nnrevuv6y7aa3olpms5gg5odnq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqdczpp6ybhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.111000+00:00
time-last-detected	2024-11-04T02:44:49.368000+00:00

182. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "DB System"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqsu2fykejmbmad4e44heghqczlq7awt1pyla
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7eznymaxtm6vlht4its5muujy4isvvw5hskxwysbjtb3a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaaxv2jnla6l4c3se53f7xufh4q34lv5upud6fvdiwknfq
resource-name	UATDBMIHAI
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.870000+00:00
time-last-detected	2024-11-04T01:36:43.707000+00:00

183. Problem details for VCN_HAS_INTERNET_GATEWAY_ATTACHED

Key	Value
additional-details	{"internetGatewayId": "ocid1.internetgateway.oc1.iad.aaaaaaaaatsrvkw2bsyofogvk66yxqkyrf2w7epltel355disbi4eq7zlv cq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaotf7w4qhroknuayke3ddfc3pup6f6o52foknpscik62g7o3qbe7a
description	Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VCN_HAS_INTERNET_GATEWAY_ATTACHED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjzmz3bqvjr7zz55d5kq5mtzqydzo3szb2jfz6raxdla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vcn.oc1.iad.amaaaaaajw2ytmaavpc52fyhsc6skkolbrd2w4panma2gwp6woz44r6iow6a
resource-name	vcn
resource-type	VCN
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.044000+00:00
time-last-detected	2024-11-04T01:38:08.493000+00:00

184. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyrmtd7bz2rotgqr5eo2nw7c4e2cpwokxwsozrr4wu7a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.390000+00:00
time-last-detected	2024-11-04T02:44:49.405000+00:00

185. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "allow group DYN_GRP_ESS_INSTANCE_PRIN to manage all-resources in tenancy,allow group DYN_GRP_ESS_INSTANCE_PRIN to manage database-family in compartment ESSDEV"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user group> to manage <some-resource all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnpypyzpmpcqryb6hrn7ymyr2rrob5e6m6lqdkydyci6q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaaj6w3qtoehm67shglonn5ayuj44ycvscdunbjxleak4neimriia
resource-name	CSS_ESS_Discovery_VM_INST_PRIN_Policies
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.075000+00:00
time-last-detected	2024-11-04T02:44:50.398000+00:00

186. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "20:19:79:a6:ae:9d:d2:0a:35:41:97:f:e:00:95:f8:1f", "IAM API key too old for user": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frpp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmqr3t7qo6q63owtsshg734oj4kd77c2wcmzjq2bq2b5mna
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frpp6t6xtjansd4agjrmh7gmpriiocqvoobhta/20:19:79:a6:ae:9d:d2:0a:35:41:97:f:e:00:95:f8:1f
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frpp6t6xtjansd4agjrmh7gmpriiocqvoobhta/20:19:79:a6:ae:9d:d2:0a:35:41:97:f:e:00:95:f8:1f
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.676000+00:00
time-last-detected	2024-11-04T02:44:49.343000+00:00

187. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "71:80:26:d1:06:1d:1b:d7:c8:f3:60:a6:86:90:62:c8", "IAM API key too old for user": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqq2jxknpa6sdte15uyzckpavrcia6l4mb27tq4rgb5oda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frrp6t6xtjansd4agjrmh7gmpriiocqvoobhta/71:80:26:d1:06:1d:1b:d7:c8:f3:60:a6:86:90:62:c8
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frrp6t6xtjansd4agjrmh7gmpriiocqvoobhta/71:80:26:d1:06:1d:1b:d7:c8:f3:60:a6:86:90:62:c8
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.068000+00:00
time-last-detected	2024-11-04T02:44:50.182000+00:00

188. Problem details for DATABASE_HAS_NO_AUTO_BACKUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Enabling automatic backup ensures that you will be able to restore the database with minimal data loss, if there is a catastrophic hardware failure.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_HAS_NO_AUTO_BACKUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcql2zxkrsary4zxlprqmyin3676rigclz2f3udratq2jqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that automatic backup is enabled.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaaz3h2zngouadipdwhugwwt4qb75uoayssp3po54gerja
resource-name	DB0103
resource-type	DB System
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:46.860000+00:00
time-last-detected	2024-11-04T01:37:51.379000+00:00

189. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq4wadx6a3jjschalfqy5xdewbxlmtlqviqq4uq7zkm6a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.089000+00:00
time-last-detected	2024-11-04T02:44:49.349000+00:00

190. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqz74owxe67vncatodmtl3tqhezuqocutxqyjshgexdyoa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.220000+00:00
time-last-detected	2024-11-04T02:44:50.175000+00:00

191. Problem details for DATABASE_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-26T13:07:30.358Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6id7i36t22nmc7kgutb2gh6scha
description	Database patches address functionality, security, and performance issues. The vast majority of security breaches can be prevented by applying available patches.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqcp5cjar2rs26vvr7i4ddrplz2b4od5pmldkjheoexhva
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the database as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaaz3h2zngouadipdwhugwwt4qb75uoayssp3po54gerja
resource-name	DB0103
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.857000+00:00
time-last-detected	2024-11-04T01:37:51.087000+00:00

192. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "UserName": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyh2iox5vkmhxq4ennbvhz4mghn6t23k6hceu4qivsiq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.219000+00:00
time-last-detected	2024-11-04T02:44:49.144000+00:00

193. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7acj6xkmo47kntvq3sa46lgutg5llm5b4ckqzi7kbbzq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.293000+00:00
time-last-detected	2024-11-04T02:44:50.201000+00:00

194. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlukjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwezczy2gb7ywq5eabvluwqgjyjjn2o5iad36uvg3kfq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlukjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.559000+00:00
time-last-detected	2024-11-04T02:44:50.178000+00:00

195. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharjya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbar46opmlfewt3hlthyplvuhupv5l37pwijzgnrq77q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.269000+00:00
time-last-detected	2024-11-04T02:44:50.142000+00:00

196. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq35v7ln7o2wsmwwzy53xz3qa5pu7amwg4ipejjipwgwcpq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.469000+00:00
time-last-detected	2024-11-04T02:44:49.397000+00:00

197. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqj777k3jgtbwtsga4jezh6mqaby7qhbqedfluv4ra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.532000+00:00
time-last-detected	2024-11-04T02:44:49.403000+00:00

198. Problem details for DATABASE_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-26T13:07:30.358Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Database patches address functionality, security, and performance issues. The vast majority of security breaches can be prevented by applying available patches.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvvtgrs474prrf3hptguqax3j65i3l2dradl4afzfqmla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the database as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaaqww3lzyi5z34jcas3dy3my7wf4m6ksbln6jt4tkmzrea
resource-name	DB0328
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.165000+00:00
time-last-detected	2024-11-04T01:37:08.641000+00:00

199. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmprofjdgr7s3z7w4hqnybeh2xlnsk5uxush7xa25ja
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.462000+00:00
time-last-detected	2024-11-04T02:44:49.841000+00:00

200. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjaxnngfnukkdg62x474iafgkfgyfgcv6kyioktfasv7a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.576000+00:00
time-last-detected	2024-11-04T02:44:50.196000+00:00

201. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6mzc4lezagv4q6fdkfapjuslix5kfaw3zyozmz7ihz5a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.199000+00:00
time-last-detected	2024-11-04T02:44:50.551000+00:00

202. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "Allow group CSS_DATA_MANAGE_ADMIN to manage opensearch-family in compartment opensearch,Allow service opensearch to manage vcn in compartment Networks,Allow service opensearch to manage vnics in compartment Networks"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfttrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user group> to manage <some-resource all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo6hzb6e65mfiedjs6ctjthxe5syr6h3vnqxyosiko2q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaapmw6cr6s6222kefk6ij5yluaibwdfkjrz5kgqdwk6fkf5vdbqa
resource-name	opensearch_pol
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.653000+00:00
time-last-detected	2024-11-04T02:44:49.342000+00:00

203. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnig4mzoffchyyppjmiahmqzjj2ywiy23swrhnbxbia
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.290000+00:00
time-last-detected	2024-11-04T02:44:50.198000+00:00

204. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqcdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqybou7xf5jzp2ydia5czlfncdqifsnlvfkcowdinekda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqcdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.085000+00:00
time-last-detected	2024-11-04T02:44:49.346000+00:00

205. Problem details for DATABASE_HAS_NO_AUTO_BACKUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Enabling automatic backup ensures that you will be able to restore the database with minimal data loss, if there is a catastrophic hardware failure.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_HAS_NO_AUTO_BACKUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqps7dz3wz2zj2bwemlin5ugaxkqiup3slz5gs5rbvfzea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that automatic backup is enabled.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaaqww3lzyi5z34jcas3dy3my7wf4m6ksbln6jt4tkmzrea
resource-name	DB0328
resource-type	DB System
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.557000+00:00
time-last-detected	2024-11-04T01:37:08.362000+00:00

206. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqey76p3vxzmcfcqroanywnby7hu7jjrssoholypvgbeq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.542000+00:00
time-last-detected	2024-11-04T02:44:49.778000+00:00

207. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqocwjvqdry3ielvg5tisepoug7lzugw4u2kqo3fnvcea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.275000+00:00
time-last-detected	2024-11-04T02:44:50.184000+00:00

208. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "gary.cook@oracle.com", "Password Time Created": "2023-12-19T22:07:24.638Z", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7klxhqmalc4irg3ignm5rr7jkac46u2kypfrtvftkzq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.582000+00:00
time-last-detected	2024-11-04T02:44:49.445000+00:00

209. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "DB System"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo42pzdwaoiyddorydc5fcf2e3ejvxotoknxtjwwgz6q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dsbsystem.oc1.iad.anuwcljtjw2ytmaaevlhpamyjcsv4v5u5y7bcs7loap637mg3wftl6mecqoq
resource-name	DBSystem-202402071242
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.040000+00:00
time-last-detected	2024-11-04T01:37:51.077000+00:00

210. Problem details for BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Encryption of volumes provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify Block Volumes encrypted Oracle-managed keys in order to apply their own key lifecycle management to the volume.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqts6347dcg7cktp37x4exz22tuiwuxhsnbmrrt5hq6q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["KMS", "Storage", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Assign a vault key to this volume
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.volume.oc1.iad.abuwcljtos6suqn6l6qca4mhq7alqutmkm65nlf4yoaxjvgmyvhqjowcra
resource-name	Oracle GoldenGate 21.11.0.0.0 Microservices Edition for Oracle (Trails)
resource-type	BlockVolume
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.076000+00:00
time-last-detected	2024-11-04T01:36:52.380000+00:00

211. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Created": "2023-09-08T18:02:26.042Z", "User Name": "karthik.muthu@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmnazundlk67ogazv2fsqnauknmjkfleez7bzngyeg4ba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaausu3qd3acuf7ocmefumxjnsw77azpbzgwyipiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.487000+00:00
time-last-detected	2024-11-04T02:44:49.416000+00:00

212. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqk4gtcvzo7m25o7qfnzijwpiw74dbkfpdgq5qnawjotla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuig5poiwsmbtu2a6epswdfwcrbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.188000+00:00
time-last-detected	2024-11-04T02:44:50.541000+00:00

213. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqh7nk357wpdc7ag5xh6tmg3z2lpnvs7hgbaagedmvggq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.669000+00:00
time-last-detected	2024-11-04T02:44:50.457000+00:00

214. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqcdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqlpvtl5bzml6yjd4adajz47rt2curx3en326veg2sbl4a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqcdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyznhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.074000+00:00
time-last-detected	2024-11-04T02:44:49.337000+00:00

215. Problem details for DATABASE_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-26T13:07:30.358Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Database patches address functionality, security, and performance issues. The vast majority of security breaches can be prevented by applying available patches.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpeamwdpiuocdb43silh2jyhmu6hdu2i6g627rqtv7xq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the database as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaa4wc2bitqd7nkb6ccafv6u4wodxxohd5ghqfp63a7oza
resource-name	DB0207
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.727000+00:00
time-last-detected	2024-11-04T01:37:50.888000+00:00

216. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzb5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3h6onnmkrxebjeqjxqdrhsd3kaqc6zl7zb7zcoe6nba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.587000+00:00
time-last-detected	2024-11-04T02:44:49.270000+00:00

217. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T18:59:46.498Z", "User Name": "chuck.hellier@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqchkkqakzri3u32haw3bg5uc3f2yuxnfvmdst7hpn5ba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.174000+00:00
time-last-detected	2024-11-04T02:44:49.454000+00:00

218. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "carlos.v@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7xbja7bjadtkax2saisraqe4qyf5cfamowcavz3jljnq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaqdczpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.082000+00:00
time-last-detected	2024-11-04T02:44:49.343000+00:00

219. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-10-21T13:48:20.571Z", "User Name": "charan.asthigiri@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxniciavxbhccmz7r5te7inb6tvbtb3nj4i5xrj7k6b2scq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.548000+00:00
time-last-detected	2024-11-04T02:44:49.785000+00:00

220. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjal77ye6ejctjlcrfv2rxuurqumzm4hveus2hmhyja
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.672000+00:00
time-last-detected	2024-11-04T02:44:50.460000+00:00

221. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxbpbyg4g36xyckbv4wernxvhwhgpdl5445ugaztuka
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.508000+00:00
time-last-detected	2024-11-04T02:44:49.844000+00:00

222. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2iazxnemlao7wyxwu4io3w65zgnl4qrcbgrjgqlj44a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jzfiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.161000+00:00
time-last-detected	2024-11-04T02:44:49.460000+00:00

223. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "ajay.manda@oracle.com", "Password Time Created": "2023-09-28T03:52:20.924Z", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7v7yq5cs6v6okt75kid2j2on7xl6xaedaqqayebkdwxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.579000+00:00
time-last-detected	2024-11-04T02:44:50.199000+00:00

224. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "f6:3b:9e:ed:88:7f:0a:e7:a2:11:cb:4d:7d:85:93:eb", "IAM API key too old for user": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqzkuwkkuywb3u7qgh53ant63zt7ddoeyak4p7wjdcqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlq qcek3j7mj3avtdsbpha3tiyj5jqkq/f6:3b:9e:ed:88:7f:0a:e7:a2:11:cb:4d:7d:85:93:eb
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlq qcek3j7mj3avtdsbpha3tiyj5jqkq/f6:3b:9e:ed:88:7f:0a:e7:a2:11:cb:4d:7d:85:93:eb
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.556000+00:00
time-last-detected	2024-11-04T02:44:49.747000+00:00

225. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "Autonomous Data Warehouse"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaaotf7w4qhroknuayke3ddflc3pup6f6o52foknpscik62g7o3qbe7a
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqu3evn5kbsgww54rjzkastupise5p4oibba3pjvfxkca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.autonomousdatabase.oc1.iad.anuwcljsjw2ytmaaz53r4kzmubtevxdl4uwmwsvbvi5u5uidqmtkidsyg5rq
resource-name	ADWDB1
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.567000+00:00
time-last-detected	2024-11-04T01:37:27.701000+00:00

226. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharjya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkeopscukfjg7pk7f4h7k5lyhyvlzf6ysh4z6aetru2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.292000+00:00
time-last-detected	2024-11-04T02:44:50.162000+00:00

227. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqavdxwrqq3zgolkzxbgqtqucmjfee74722aa3h5zm2tda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.471000+00:00
time-last-detected	2024-11-04T02:44:49.850000+00:00

228. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Created": "2024-02-05T14:44:57.441Z", "User Name": "ruchir.khanna@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6yvecvdjnjhslmv2222btqn7zfx63zepyuclwv7tohq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.235000+00:00
time-last-detected	2024-11-04T02:44:49.167000+00:00

229. Problem details for SECURITY_LISTS_OPEN_PORTS

Key	Value
additional-details	{"TCP": "11, 17 - 19, 21, 23 - 25, 43, 49, 53, 70 - 74, 79 - 81, 88, 111, 123, 389, 445, 500, 636, 3306, 3389, 5901, 5985 - 5986, 7001, 8000, 8080, 8443, 8888", "vcnDisplayName": "ACS-VCN01", "vcnlId": "ocid1.vcn.oc1.iad.amaaaaaajw2ytmaaxlvfb27g5b2vb3r7zfid2vhxknete2j22rixel2g2l3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkwtayzf33t6ynmrh57n7qcklg67e7zjh633c7amzi5zaozoygg
description	This detector rule triggers a problem when traffic is allowed to certain restricted ports (see Input Settings, Restricted Protocol:Ports List) as part of the Security list ingress rule. If "Restricted Protocol:Ports List" includes port values that are identified or allowed for your workloads, then modify the list of ports in Input Settings accordingly.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LISTS_OPEN_PORTS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwslwmuoozm5y7rqwa7haxw6uamhclvbnlxnrxdltpha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Additional details section of the problem provides a list of open Restricted ports that triggered this problem. Ensure that your OCI VCNs use security lists with ingress or inbound rules to only allow traffic access to identified ports. Review if detected ports should be open on this security list Ingress rule and close them if they are not required to be open. It is also recommended to check the "Restricted Protocol:Ports List" in the Input setting of this detector rule and modify it to allow certain required ports and thus notifying Cloud Guard to not detect a problem for those ports.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaag7jgvrsooktpsisjecpx2ivrbvjg5zhtlmem2jymstyagshi435ra
resource-name	security list for private subnet-ACS-VCN01
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:44.079000+00:00
time-last-detected	2024-11-04T01:37:42.661000+00:00

230. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqzeh6v6ua3sez53tiuhpau6fnomhh2xmczhibsaxwo2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.226000+00:00
time-last-detected	2024-11-04T02:44:50.182000+00:00

231. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcg3smw3polwrzg5ot5kjmgmktt633vcpbky72xbt4na
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.488000+00:00
time-last-detected	2024-11-04T02:44:49.824000+00:00

232. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq67lsnom6zvqwslicpwcdqjdyoai2vacduwd7v2pnxxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.553000+00:00
time-last-detected	2024-11-04T02:44:49.790000+00:00

233. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "DB System"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaanozdmhew3byktzrrehu4ojxch4y6gthkxcqzaubb3g2ctobrpwq
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3s7sdv3x4w3ixhw173bujdxltjd266tl6hlyek2yiza
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dsbsystem.oc1.iad.anuwcljtjw2ytmaak3llbp3gmaefyaqd7ugowvnfbynfdhhwpxjigx72q6a
resource-name	DBSystem-202403280916
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.525000+00:00
time-last-detected	2024-11-04T01:37:07.563000+00:00

234. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxb253ielcgxg3xvgemzosgcnblcepfoafbg6rosvkq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.242000+00:00
time-last-detected	2024-11-04T02:44:50.196000+00:00

235. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbffsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3ygsuf4hsozxbuhzvfbwusimws5r77ekpeulj37kvyia
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.363000+00:00
time-last-detected	2024-11-04T02:44:49.378000+00:00

236. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvooxtkujf5unstafidwmjd2wwcnpy3xrul7lyf2rga
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.155000+00:00
time-last-detected	2024-11-04T02:44:49.437000+00:00

237. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{""ICMP": "3", "TCP": "22", "vcnDisplayName": "vcn", "vcnId": "ocid1.vcn.oc1.iad.amaaaaaajw2ytmaavpc52fyhsc6skkolbrd2w4panma2gwp6woz44r6iow6a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaotf7w4qhroknuayke3ddflc3pup6f6o52foknpcik62g7o3qbe7a
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnnfsqopuygsuhj5zyf3g7vecjfyzqrpvzjroqnei4gwq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaajhcoybn5hbrvds53r25pphic4434zuau74atmg7h3uyf72ttbca
resource-name	Default Security List for vcn
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.154000+00:00
time-last-detected	2024-11-04T01:38:08.517000+00:00

238. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7de7xlb4yy7hzeytcmwicplv7co2oxhlr6spqizaefq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.561000+00:00
time-last-detected	2024-11-04T02:44:49.423000+00:00

239. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-09-28T03:52:20.929Z", "User Name": "ajay.manda@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5tgovqn56rwqapgh6svfg5shcjpijsbi75emuay32cq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnakbwliukjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.570000+00:00
time-last-detected	2024-11-04T02:44:50.189000+00:00

240. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-02-07T09:53:36.643Z", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphic232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq2y5abhn44olshiiduztmbnyunemwga5xhhb2dimhxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.236000+00:00
time-last-detected	2024-11-04T02:44:50.191000+00:00

241. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmulkhqkynqzis775a2wv5ur7mjxlo4o6efppnvrcqa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.253000+00:00
time-last-detected	2024-11-04T02:44:49.196000+00:00

242. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{""ICMP": "3", "TCP": "443, 8080", "vcn DisplayName": "ACS-VCN01", "vcnId": "ocid1.vcn.oc1.iad.amaaaaaajw2ytmaaxlvfb27g5b2vb3r7zfid2vhxknete2j22rixel2g2l3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zrh633c7amzi5zaozoygg
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqg23sw4j2idmvtqf4ei7ezqkidcojzyusrrprlk6glnq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaq5s3fle57lpkynki57irfyri3ixiz3qb63g5ybs5pzgk6i4goy46a
resource-name	Default Security List for ACS-VCN01
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpillxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.159000+00:00
time-last-detected	2024-11-04T01:37:41.809000+00:00

243. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "dhanasekara.pandian@oracle.com", "Password Time Created": "2023-11-20T09:54:09.673Z", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwqdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjskew3u4xlohwtnxsobq3txsme4ht7bkazkvj4qlbuzq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwqdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:55.080000+00:00
time-last-detected	2024-11-04T02:44:50.463000+00:00

244. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T19:01:24.920Z", "User Name": "sudhanshu.x.sharma@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq576kpuv35coyo6skamqanyrtcyuwr7v56ckd2g3ibd3a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjya4wnxu5qre07bveco2xpiqr3r4uu5vvcpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.278000+00:00
time-last-detected	2024-11-04T02:44:50.187000+00:00

245. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfttrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqswoz4ij5grb2nrkqebkssug2a7nokpbkmwmj6e4h355a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.386000+00:00
time-last-detected	2024-11-04T02:44:49.402000+00:00

246. Problem details for BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Encryption of volumes provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify Block Volumes encrypted Oracle-managed keys in order to apply their own key lifecycle management to the volume.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6xq6ppfeibtpix5kaccy3w5e7bawhhvgaon3dzxumwla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["KMS", "Storage", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Assign a vault key to this volume
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.volume.oc1.iad.abuwcljt4wy7jpuquo47mgaimn3gj6toydqyrvn3v3winzx3lvku72fegzq
resource-name	Oracle GoldenGate 21.11.0.0.0 Microservices Edition for Oracle (Cache Manager)
resource-type	BlockVolume
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.356000+00:00
time-last-detected	2024-11-04T01:36:52.306000+00:00

247. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagcjielr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbpv67tlndisjoro3njmw5qmouioysp72yk2vnu57y5bq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagcjielr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.484000+00:00
time-last-detected	2024-11-04T02:44:49.862000+00:00

248. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T19:00:10.480Z", "User Name": "ana.delafuente@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcp3ucnbbnholjmppk5kquaecervcwuapdahft7ed3354a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagcier5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinnhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.478000+00:00
time-last-detected	2024-11-04T02:44:49.857000+00:00

249. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-09-24T17:19:04.277Z", "User Name": "prabhanjan.acharjya@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmqr26vpebisypwx34rh2ylyklxs4szvnexqju6baixq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.280000+00:00
time-last-detected	2024-11-04T02:44:50.151000+00:00

250. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqa2fmddyhyhzrcj6tuzj3ssahpqyuriqp5i5q7sqa2wa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.228000+00:00
time-last-detected	2024-11-04T02:44:49.160000+00:00

251. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7oilp3j7wqogqiyipmhnc46vr7tjwrd4uirhaejt6ga
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5frrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.556000+00:00
time-last-detected	2024-11-04T02:44:49.237000+00:00

252. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwgq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmpbbhjoy5tf7qjz4tgbpkjc7e6pqbmdgcqky6yz5p4a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwgq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.088000+00:00
time-last-detected	2024-11-04T02:44:50.470000+00:00

253. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq33lsor2uktm3mtvc7vujqqa06yuolp4nh6cw6bfwyrjq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.529000+00:00
time-last-detected	2024-11-04T02:44:49.400000+00:00

254. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqqlbjl5m3k3mptgoi6v7jf67kewfwfpvcpyfc1vpvselca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.553000+00:00
time-last-detected	2024-11-04T02:44:49.234000+00:00

255. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3qwt7sxesj7ldmgzxa35bm5vqx6mik2h4rrhicugcqla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiy5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.495000+00:00
time-last-detected	2024-11-04T02:44:49.830000+00:00

256. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqzbv6srpsqjr6hqhn4y7ltp4okz7274l4z7ayr6lzuqmq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.250000+00:00
time-last-detected	2024-11-04T02:44:49.191000+00:00

257. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"User Name": "ravi.srinivasan@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jfifiriscygbiadusklsaix7ayj5biqqjq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7xnnoyrf6mbc33na4bcloliry4hcjsy7jfebc7iocda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaadax27hchavycud6us5jfifiriscygbiadusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.152000+00:00
time-last-detected	2024-11-04T02:44:49.453000+00:00

258. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqi257dk67un2b4ocbpvvk7hzaf3zp6yb335fcnjpopa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.690000+00:00
time-last-detected	2024-11-04T02:44:50.476000+00:00

259. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7j7p7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqao2zbq3pr7ai6i2yjvoezpuzn7cekg7kp3trucddzq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.359000+00:00
time-last-detected	2024-11-04T02:44:49.374000+00:00

260. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7oxstb6wheeywxbgns7byhlcrlhmqiqa34n3it3s33ona
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.504000+00:00
time-last-detected	2024-11-04T02:44:49.370000+00:00

261. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqc74knoex2smdipzdcxqjha7zapy5oznucrys2pcmthq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.225000+00:00
time-last-detected	2024-11-04T02:44:49.150000+00:00

262. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwqdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3m2klvhqdm3mkuvom5eti4awu5kpfg6ovme52l7exva
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwqdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.059000+00:00
time-last-detected	2024-11-04T02:44:50.447000+00:00

263. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhum4j2p2b456m7yaacwhlvkc4d2sacvy7fakggtt7qaq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.502000+00:00
time-last-detected	2024-11-04T02:44:49.431000+00:00

264. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharjya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqu6rrba44mjzyhbc63wjb27rhf2ddqknv72toervxn2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.295000+00:00
time-last-detected	2024-11-04T02:44:50.164000+00:00

265. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvdnbzqcdru6slhaoh3iauakv3k73355lprwwb7h3f5qa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxg dsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.491000+00:00
time-last-detected	2024-11-04T02:44:49.420000+00:00

266. Problem details for DATABASE_SYSTEM_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-29T08:14:42Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqfqsu2fykejmbmad4e44heghqczlq7awt1pyla
description	Database system patches often include updates that eliminate known security vulnerabilities. Raise a problem when a database system is discovered which has one or more patches, available for 90 days or more, that have not been applied.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_SYSTEM_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqkf5xcbhlq2u3aan6yqu6qnrrmmay6islbc6ze4or5vjq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the DB system as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaaxvv2jnla6l4c3se53f7xufh4q34lv5upud6fvdiwknfq
resource-name	UATDBMIHAI
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:48.236000+00:00
time-last-detected	2024-11-04T01:36:43.470000+00:00

267. Problem details for SECURITY_LISTS_OPEN_PORTS

Key	Value
additional-details	{"TCP": "11, 17 - 19, 21, 23 - 25, 43, 49, 53, 70 - 74, 79 - 81, 88, 111, 123, 389, 445, 500, 636, 3306, 3389, 5901, 5985 - 5986, 7001, 8000, 8080, 8443, 8888", "vcnDisplayName": "ACS-VCN01", "vcnId": "ocid1.vcn.oc1.iad.amaaaaaajw2ytmaaxlvfb27g5b2vb3r7zfid2vhxknete2j22rixel2g2l3a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaafkwtayzf33t6ynmrh57n7qcklg67e7zjh633c7amzi5zaozoygg
description	This detector rule triggers a problem when traffic is allowed to certain restricted ports (see Input Settings, Restricted Protocol:Ports List) as part of the Security list ingress rule. If "Restricted Protocol:Ports List" includes port values that are identified or allowed for your workloads, then modify the list of ports in Input Settings accordingly.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LISTS_OPEN_PORTS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqgtjrcpv6f6klo6aag4dkcw6b3zbv22hdvstis7wlisfa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Additional details section of the problem provides a list of open Restricted ports that triggered this problem. Ensure that your OCI VCNs use security lists with ingress or inbound rules to only allow traffic access to identified ports. Review if detected ports should be open on this security list Ingress rule and close them if they are not required to be open. It is also recommended to check the "Restricted Protocol:Ports List" in the Input setting of this detector rule and modify it to allow certain required ports and thus notifying Cloud Guard to not detect a problem for those ports.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaq5s3fle57lpkynki57irfy3ixiz3qb63g5ybs5pzgk6i4goy46a
resource-name	Default Security List for ACS-VCN01
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:44.152000+00:00
time-last-detected	2024-11-04T01:37:41.798000+00:00

268. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "Allow service objectstorage-us-ashburn-1 to manage object-family in compartment ESSDEV"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzb5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user group> to manage <some-resource all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmdxozz6jfp7d5v23labf2y4wx5b3nayv7rjsnr556oda
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaa3jeyjm5kv3kxmpmkoleakmsvehhzfhszlmav7wtztk5fgoc5efq
resource-name	ACS_Data_Manage_Pol
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtppljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.506000+00:00
time-last-detected	2024-11-04T02:44:49.372000+00:00

269. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdy4v7n2rf4mdsg4wlwve4yx3iwt2tobwjqupu23nb6woa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.559000+00:00
time-last-detected	2024-11-04T02:44:49.796000+00:00

270. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo53wwzx7rva76v3sqqxbjqzoa5txdnx7alwb3ceyugla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaqqdczpzzp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.096000+00:00
time-last-detected	2024-11-04T02:44:49.355000+00:00

271. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcaww4rljhuiwg2enwc6ook3xbjry32mpjdimboyuobq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7jx6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.491000+00:00
time-last-detected	2024-11-04T02:44:49.869000+00:00

272. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqv33uzppmmanj4gwwyx56fwzqeebh72bdvxi67tyxcla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.243000+00:00
time-last-detected	2024-11-04T02:44:49.182000+00:00

273. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqavu4cobeuftnkxjply2hhxz3idv7dfuc2o6dk7lciq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.170000+00:00
time-last-detected	2024-11-04T02:44:49.450000+00:00

274. Problem details for BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Encryption of volumes provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify Block Volumes encrypted Oracle-managed keys in order to apply their own key lifecycle management to the volume.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcp62ek6faubix7rvkkb4hwenkkj5pr37vo26ozit4kaq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["KMS", "Storage", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Assign a vault key to this volume
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.volume.oc1.iad.abuwcljtz4tmo7xjh7gxipxv77xqdar7xsjcsbz3ll2nesqvfoopu74odcq
resource-name	Oracle GoldenGate 21.11.0.0.0 Microservices Edition for Oracle (Deployments)
resource-type	BlockVolume
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:44.127000+00:00
time-last-detected	2024-11-04T01:36:53.288000+00:00

275. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqz2tyivwr33m3ltt7av5y3ubkyeeojayek7wthwa3baq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.560000+00:00
time-last-detected	2024-11-04T02:44:49.241000+00:00

276. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqjqsxy4uxs726f7dkiv6mzhtnnfu4pxtqbrvon5mmxtq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.474000+00:00
time-last-detected	2024-11-04T02:44:49.811000+00:00

277. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7jp7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbsawusxpfe3cxuz7iohsmu6ff76za2eqyvedyolkjqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.477000+00:00
time-last-detected	2024-11-04T02:44:49.405000+00:00

278. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqckeuj2pd736pgjyofzv23exvbffnlvh63nq5pio6hdq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.284000+00:00
time-last-detected	2024-11-04T02:44:50.192000+00:00

279. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-09-12T23:29:44.512Z", "User Name": "harinath.subramaniam@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkyjf322qynt4azwhipwrlbjx4jv53qgbxnip5farca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarakwtmcpzjyyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.676000+00:00
time-last-detected	2024-11-04T02:44:50.464000+00:00

280. Problem details for BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Encryption of volumes provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify Block Volumes encrypted Oracle-managed keys in order to apply their own key lifecycle management to the volume.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	BLOCK_VOLUME_ENCRYPTED_WITH_ORACLE_MANAGED_KEY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqesjj3jexchjuavtzqzado6v4stsmnfbievi3ummm4weq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["KMS", "Storage", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Assign a vault key to this volume
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.volume.oc1.iad.abuwcljta5wgwzkhfvbbtrq7oh2aptvdc4vqwacr3mw3ofvn5yqq5y2c2dfq
resource-name	Oracle GoldenGate 21.11.0.0.0 Microservices Edition for Oracle (Swap)
resource-type	BlockVolume
risk-level	MINOR
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:44.135000+00:00
time-last-detected	2024-11-04T01:36:52.080000+00:00

281. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3unyfk7rsgkka62ewd6ee5e2joyyxije3vrrg7ncszq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.569000+00:00
time-last-detected	2024-11-04T02:44:49.431000+00:00

282. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "a0:61:17:e5:d1:e9:d0:52:3c:78:d3:5b:ce:75:b7:f3", "IAM API key too old for user": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwyipiqtzcxgdsp4raf5a")}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhmb5iqff47wbmvskeuzhobzrzax7fdwbowcvnfn7a3q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwyipiqtzcxgdsp4raf5a/a0:61:17:e5:d1:e9:d0:52:3c:78:d3:5b:ce:75:b7:f3
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwyipiqtzcxgdsp4raf5a/a0:61:17:e5:d1:e9:d0:52:3c:78:d3:5b:ce:75:b7:f3
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.601000+00:00
time-last-detected	2024-11-04T02:44:50.148000+00:00

283. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2024-02-08T11:56:37.932Z", "User Name": "ricardo.e.acosta@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcycti3y2vpewe4extqc3effclnyqillsvu5gysx4ha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.564000+00:00
time-last-detected	2024-11-04T02:44:49.246000+00:00

284. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "yevhen.udod@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7j7p7f47wzb5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkzaiaz27rrtgu7a644obgbnweyhdye7ccgedwpjpqlq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaxymnnmi3csfnquerukt4dvkefobd6xhbq55w6s3tqednpvexwgwa
resource-name	yevhen.udod@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.513000+00:00
time-last-detected	2024-11-04T02:44:49.381000+00:00

285. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmkrthuod3ffdjdsqasmd2o3dftflqjc5ufxc7uytila
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.232000+00:00
time-last-detected	2024-11-04T02:44:49.163000+00:00

286. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcq5wtbn5efz55skcd2c6qffz5ufbjp45wmco54sr6kfaa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpackbwlujkjj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.587000+00:00
time-last-detected	2024-11-04T02:44:50.207000+00:00

287. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq53b4ntesyjpcq4fzfqos3thuqfjemxnpoq2zyhyqx5gq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.481000+00:00
time-last-detected	2024-11-04T02:44:49.409000+00:00

288. Problem details for DATA_SAFE_DB_NOT_REGISTERED

Key	Value
additional-details	{"Database Type": "Autonomous Data Warehouse"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaamjskiq3tlgm7olkrqankwmsetnpijpph4dr76uf47rznjiybhaoa
description	Data Safe helps ensure your databases are securely configured. An Oracle cloud database has been discovered that is not yet registered with Data Safe.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATA_SAFE_DB_NOT_REGISTERED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqek7jybt7agpqeqfhuy3ikclhh25ythpaw6ptoij5xq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database Security"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Register this database instance with Data Safe and configure assessments to evaluate and monitor configuration, check user activities, and mitigate risks.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.autonomousdatabase.oc1.iad.anuwcljrjw2ytmaag3mdgd6bcnv72kxc3oshhu7vfbzkrwy2dzbimjbqsra
resource-name	cogs-adw
resource-type	Database
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:45.898000+00:00
time-last-detected	2024-11-04T01:37:20.728000+00:00

289. Problem details for DATABASE_SYSTEM_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-29T08:14:14.421Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpldb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Database system patches often include updates that eliminate known security vulnerabilities. Raise a problem when a database system is discovered which has one or more patches, available for 90 days or more, that have not been applied.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_SYSTEM_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqurpcn567vtcnafs72pqxiypr2lshpais4wnni6zhbq7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the DB system as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaaevlhpamyjcsv4v5u5y7bcs7loap637mg3wftl6mecqoq
resource-name	DBSystem-202402071242
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.923000+00:00
time-last-detected	2024-11-04T01:37:50.877000+00:00

290. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "65:d9:d8:20:f6:71:f3:55:5d:d4:f0:02:0e:11:39:92", "IAM API key too old for user": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwui5poiwsmbtu2a6epsdfwcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmqr3qjv3rgfbzp2y7funwicr2dkqcas32tdqjd4dscw4xq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaffwui5poiwsmbtu2a6epsdfwcrxbsfm7yahd4n3b3pnabpaduq/65:d9:d8:20:f6:71:f3:55:5d:d4:f0:02:0e:11:39:92
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaffwui5poiwsmbtu2a6epsdfwcrxbsfm7yahd4n3b3pnabpaduq/65:d9:d8:20:f6:71:f3:55:5d:d4:f0:02:0e:11:39:92
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.151000+00:00
time-last-detected	2024-11-04T02:44:50.485000+00:00

291. Problem details for DATABASE_HAS_NO_AUTO_BACKUP

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.compartment.oc1..aaaaaaaaabv6yqxomhmhpdb6d3y532wqe6jd7i36t22nmc7kgutb2gh6scha
description	Enabling automatic backup ensures that you will be able to restore the database with minimal data loss, if there is a catastrophic hardware failure.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_HAS_NO_AUTO_BACKUP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqlh5ahhnynla7xhyfmdht2qbldepdkvu6gj5njcpk3hq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that automatic backup is enabled.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaa4wc2bitqd7nkb6ccafv6u4wodxxohd5ghqfp63a7oza
resource-name	DB0207
resource-type	DB System
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.846000+00:00
time-last-detected	2024-11-04T01:37:51.431000+00:00

292. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "mihai.alistar@oracle.com", "Password Time Created": "2024-07-24T08:53:01.318Z", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbffsphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyfkgmozlmldys2knye6msabobioubhn3ajilertyoida
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.382000+00:00
time-last-detected	2024-11-04T02:44:49.398000+00:00

293. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"User Created": "2023-12-19T22:07:12.259Z", "User Name": "ravi.srinivasan@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1.aaaaaaaadmjyftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqavr2ebxhsfu5yk3w52hh2x7vm26ms3id35hbrrtxkgq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1.aaaaaaaadx27hchavycud6us5jzfirsccygbiydusklsaix7ayj5biqqjq
resource-name	ravi.srinivasan@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.173000+00:00
time-last-detected	2024-11-04T02:44:49.470000+00:00

294. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharjya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjnw5fqkkpkw4pzajt3akrujrcmhwf7zcouyjakys4qsa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharjya@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.276000+00:00
time-last-detected	2024-11-04T02:44:50.148000+00:00

295. Problem details for AUTH_TOKEN_TOO_OLD

Key	Value
additional-details	{"Auth Token Time Created": "2024-04-26T22:15:57.938Z", "IAM auth token too old for user": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwyiptzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfr7jp7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Auth Tokens at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	AUTH_TOKEN_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqxi7js33e7sey4hrjq6cbreopejdijlamucsc5dv7naq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Auth token regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.credential.oc1..aaaaaaaa6ftkn2luvzccj6onxuankl7w4x7sf46uvl2p2bunpvjx65s6vuq
resource-name	my-token
resource-type	IAM auth token key
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.545000+00:00
time-last-detected	2024-11-04T02:44:50.145000+00:00

296. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "24:37:3ca5:c9:c9:ad:fa:8c:c7:8a:14:c3:bc:af:2c", "IAM API key too old for user": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuig5poismbtu2a6epswdfwcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5222o7jcqepp3o7n2ei5ugs4vv4bkmu5hbfdwv2mfqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaffwuig5poismbtu2a6epswdfwcrxbsfm7yahd4n3b3pnabpaduq/24:37:3:c:a5:c9:c9:ad:fa:8:c:c7:8:a:14:c3:bc:af:2c
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaffwuig5poismbtu2a6epswdfwcrxbsfm7yahd4n3b3pnabpaduq/24:37:3:c:a5:c9:c9:ad:fa:8:c:c7:8:a:14:c3:bc:af:2c
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.062000+00:00
time-last-detected	2024-11-04T02:44:50.487000+00:00

297. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-11-14T16:30:45.081Z", "User Name": "dhanasekara.pandian@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqgbmk57rn4kodoh7nji62yz4tmqskun5ravevfdnepq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.068000+00:00
time-last-detected	2024-11-04T02:44:50.454000+00:00

298. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "88:40:02:e5:fe:a0:e9:9d:66:52:49:6b:2d:b6:b2:ab", "IAM API key too old for user": "ruchir.khanna@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdwp5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjdjxooqjnkrpu32rql6rad4am2i6rspr3nyk3xhc7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdwp5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa/88:40:02:e5:fe:a0:e9:9d:66:52:49:6b:2d:b6:b2:ab
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdwp5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa/88:40:02:e5:fe:a0:e9:9d:66:52:49:6b:2d:b6:b2:ab
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.660000+00:00
time-last-detected	2024-11-04T02:44:50.120000+00:00

299. Problem details for DATABASE_HAS_PUBLIC_IP

Key	Value
additional-details	{"Public IP": "[150.136.252.156]", "Subnet Access Type": "Public", "Subnet OCID": "ocid1.subnet.oc1.iad.aaaaaaaaaffjpato2jlwfsqaexogak56bku4l3bz3ndfacflnbwk47seop6ha"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqszu2fykejmbmad4e44heghqczlg7awt1pyla
description	Use of a public IP address to access a database increases your exposure to potential security and business continuity risks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_HAS_PUBLIC_IP
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq7luiphftfwfdukx546ni5a45l3hiqbq6q23ktyxj2rq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the database system does not have a public IP address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.dbsystem.oc1.iad.anuwcljtjw2ytmaaxv2jnla6l4c3se53f7xufh4q34lv5upud6fvdiwknfq
resource-name	UATDBMIHAI
resource-type	ExadataBareMetalVM
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.541000+00:00
time-last-detected	2024-11-04T01:36:43.773000+00:00

300. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqe6bvqopxw4to5sgmqsm5t5cap3bjdgip5clwiy5fawtq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.374000+00:00
time-last-detected	2024-11-04T02:44:49.389000+00:00

301. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuiq5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzb5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqczjasbmoetyk2tkqdndzxzn3sa5o2apzfqs42fbvbk4q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuiq5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.179000+00:00
time-last-detected	2024-11-04T02:44:50.530000+00:00

302. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmihflx lou3bndye7szkpu7egmr2xc5mulpsdl6uuveq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.579000+00:00
time-last-detected	2024-11-04T02:44:49.440000+00:00

303. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "manish.kakade@oracle.com", "Password Time Created": "2023-05-19T18:57:51.882Z", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuiq5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqqkrdropumzyiit5y4e34mem5d26sv5fc42x3yordz5q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuiq5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.195000+00:00
time-last-detected	2024-11-04T02:44:50.548000+00:00

304. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{"ICMP": "3", "TCP": "22", "vcn DisplayName": "vcn-20240321-1516", "vcnId": "ocid1.vcn.oc1.iad.aaaaaaaaajw2ytmaad2rgjzwfjg3hbwykqz6fzzihj6nzoio77fa3hqufua"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlfsu2fykejmbmad4e44heghqczlg7awt1pyla
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqrkjz2776b5wcdhqwg6ukyhmcpmxnsl44odiqxpgsa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.securitylist.oc1.iad.aaaaaaaaag3soktwk3eixsphcc7w6ffd5zsckpz4hw2dy7qoedprnjid6sq
resource-name	Default Security List for vcn-20240321-1516
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:48.608000+00:00
time-last-detected	2024-11-04T01:37:18.540000+00:00

305. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq24o3qfh157miyv66bid4qp3tcjppji7zv63brgen2q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.063000+00:00
time-last-detected	2024-11-04T02:44:50.450000+00:00

306. Problem details for POLICY_USES_ANY_USER

Key	Value
additional-details	{"policyStatements": "admit any-user of tenancy CopyDestinationaucasmp01 to manage object-family in compartment ESSDEV"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Because any-user means any-principal, it is difficult to control what entities might be encompassed by an any-user policy. "any-user" includes user principals, instance principals, and any number of resource principals that exist now or will exist in the future.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_USES_ANY_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbkat7hbn6a72crmgu56luoeo5gn4xle4r55hpobvmb7a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Use a narrower set of entities in the policy. If the intention is to include any human user, consider using "any-group" which will only include user principals.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaa3c4x6vtw2cbu6qh63b6gcfsmhikdjrrbuol5qmnpwx373yo5va
resource-name	ACS_ESS_Data_Safe_Policies
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.173000+00:00
time-last-detected	2024-11-04T02:44:50.467000+00:00

307. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1.aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5lkiu6u6ancvka7rsduhezk5fvnagfhswski3t3wzvqm
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1.aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.159000+00:00
time-last-detected	2024-11-04T02:44:49.440000+00:00

308. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "anand.poovakkat@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqclukrvrpdkofy7j5wtzqlq55zaldkgb5vj2jlvwsq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.498000+00:00
time-last-detected	2024-11-04T02:44:49.834000+00:00

309. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqg6til355htzy5ckffp7wjmfburovx2gu42s2m7nfpxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.586000+00:00
time-last-detected	2024-11-04T02:44:49.450000+00:00

310. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "allow DYNAMIC-GROUP logging_analytics_agent to manage management-agents IN COMPARTMENT Management-Agents"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user group> to manage <some-resource all-resources> [in tenancy in compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbmez2eues7zhopisklzkajheohknid3ncb2rrybw
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaapeq7qnncbs7lkyohskkaqfizomezn7t737x4yx5ni4mezgynbung
resource-name	logging_analytics_automatic_ingestion_policies
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtplijxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.168000+00:00
time-last-detected	2024-11-04T02:44:50.153000+00:00

311. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6fyd2mzsjjb4uhyyuu7d5uj6h4qrllucgxogbhpswcca
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.566000+00:00
time-last-detected	2024-11-04T02:44:49.427000+00:00

312. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdblhdwp5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqbd06iyvfp5worwl2xkjnrrp76xrfdt2zgqv3a7vrq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.229000+00:00
time-last-detected	2024-11-04T02:44:50.185000+00:00

313. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqgt6a4fcgjctf75gxa5tluqeqlfzghmd4l2vycs55ufa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrbvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.562000+00:00
time-last-detected	2024-11-04T02:44:49.799000+00:00

314. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqhfirmsbfdtb6zrvgi42g4i4rfsbkowtedrxud2tnea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.467000+00:00
time-last-detected	2024-11-04T02:44:49.847000+00:00

315. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"User Created": "2023-12-19T22:05:38.419Z", "User Name": "gary.cook@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1.aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5ktwwvtqv3elous2hn2yocxcwpjacstlyjyti4ujpa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAMS", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1.aaaaaaaaap06juhunvleixs2sy7u7gmj65ooe3fumnvbkbqhvboyazmadfq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.573000+00:00
time-last-detected	2024-11-04T02:44:49.434000+00:00

316. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqqaj6ku3k6yandywmif7owfvjdctk3azkrx4lfo4esaa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.484000+00:00
time-last-detected	2024-11-04T02:44:49.413000+00:00

317. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ana.delafuente@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjstssylvemkjoobs2ejdyynyvd2 cwdhut2xhhqfy5hd2a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagccjelr5qlrjs7s3oexquddzqkjlfqgn4nlmghkvinlhh7x6aka
resource-name	ana.delafuente@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.495000+00:00
time-last-detected	2024-11-04T02:44:49.872000+00:00

318. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcpnsnbezeexflyueqfomnrlt7764tzjhvkioxnic5fvq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.175000+00:00
time-last-detected	2024-11-04T02:44:50.527000+00:00

319. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "netzahualcoyotl.xuluc.martin@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqduz2mu6ixq24etnd7bvlwh7ksyruh7pfofnkk3mkgd
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.252000+00:00
time-last-detected	2024-11-04T02:44:50.207000+00:00

320. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "netzahualcoyotl.xuluc.martin@oracle.com", "Password Time Created": "2024-02-07T18:23:32.881Z", "User OCID": "ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbff5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqijxcvltqv4qbqxsaocls5lw2xchnnpf3ikdl5svps2ya
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaazs2pwftoxir3ws7gqjrnjax5p4ysc25jtz4dx7aoug7uanp2xria
resource-name	netzahualcoyotl.xuluc.martin@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.245000+00:00
time-last-detected	2024-11-04T02:44:50.200000+00:00

321. Problem details for DATABASE_PATCH_NOT_APPLIED

Key	Value
additional-details	{"Patch Time Released": "2024-07-26T13:07:30.358Z", "databaseSystemPatchNotAppliedConfig": "10"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqfqsu2fykejmbmad4e44heghqczlq7awt1pyla
description	Database patches address functionality, security, and performance issues. The vast majority of security breaches can be prevented by applying available patches.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	DATABASE_PATCH_NOT_APPLIED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqjn6b55sybc3hsgsbbijavy5y7u6ghni2mbni5ofaqhaq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Database"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Oracle recommends that released patches be applied to the database as soon as possible.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.database.oc1.iad.anuwcljtjw2ytmaahpily2nufpa7z6upog5c4gdyjki4x3mlqugg4b5wlida
resource-name	DBMIHAI
resource-type	DB System
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:47.565000+00:00
time-last-detected	2024-11-04T01:36:42.915000+00:00

322. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzb5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcxoa4jqmptjwbu7xu66ouyef5iggt3lbuoiqddr6ira
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.192000+00:00
time-last-detected	2024-11-04T02:44:50.544000+00:00

323. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "charan.asthigiri@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpit4apf5zyk5kp74vbguciieb7txqboj4wgbrckuuq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaas654t5s37u4xrdvglb5od76zpqbyp42ap5fv33wmjxb7xoemaa
resource-name	charan.asthigiri@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.545000+00:00
time-last-detected	2024-11-04T02:44:49.781000+00:00

324. Problem details for POLICY_TENANCY_ADMIN_GROUP_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "allow group DYN_GRP_ESS_INSTANCE_PRIN to manage all-resources in tenancy"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Default tenancy administrator group members can perform any action on all resources in that tenancy. This high-privilege entitlement must be controlled and restricted to only those users who need it to perform their job functions.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_TENANCY_ADMIN_GROUP_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqm74wkcan3fr2zxtvtc4juev7t2fo4qhpy7kbtkoizqea
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Verify with the OCI administrator that this entitlement grant was sanctioned and that the membership of the group remains valid after the grant of the administrator privilege.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaaj6w3qtoehm67shqlionn5ayui44ycvsdunbjxleak4neimria
resource-name	CSS_ESS_Discovery_VM_INST_PRIN_Policies
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.071000+00:00
time-last-detected	2024-11-04T02:44:50.395000+00:00

325. Problem details for USER_HAS_API_KEYS

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM API keys are credentials used to grant programmatic access to resources.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEYS
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwgqua6qqwvxatim7l7rzzezhwzdympp462ognnx44ama
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaciwdev7bsc5imrm5id5h7ulzaa4le26w6ss6xd7yokl4gkhwyloa
resource-name	ruchir.khanna@oracle.com
resource-type	User
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.238000+00:00
time-last-detected	2024-11-04T02:44:49.171000+00:00

326. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "sudhanshu.x.sharma@oracle.com", "Password Time Created": "2023-06-23T15:15:53.398Z", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefyzdwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftjr7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqtowt4qauxw7cfhkqk6eowgabs7ryl5eyca724u54putq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefyzdwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.287000+00:00
time-last-detected	2024-11-04T02:44:50.195000+00:00

327. Problem details for USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Created": "2023-05-19T19:02:41.092Z", "User Name": "carlos.v@oracle.com"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	A local user exists within the tenancy who does not have the username set to 'break_glass_account' and is not part of the Administrators group.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_EXISTS_WITHIN_TENANCY_WITH_NON_STANDARD_NAMING_CONVENTION
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqvtxspmv465mesqxdctmipcyux547eq6mt4x4g35nvzeq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Delete all users apart from break_glass_account.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaqqdczpzzpp6ymhhppfymqi7hnd3h4mxlmer2bnlyzhcjzjdoqznq
resource-name	carlos.v@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.092000+00:00
time-last-detected	2024-11-04T02:44:49.352000+00:00

328. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"User Name": "gary.cook@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqugbrwtt6uqppg37wxuizmwlaa6rgagvxf44z5g25fbqrq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaapo6juhunvleixs2sy7u7gmj65ooe3fumnvbkvbqhvboyazmadfqq
resource-name	gary.cook@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.553000+00:00
time-last-detected	2024-11-04T02:44:49.415000+00:00

329. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqdrmvhigbtbf6kmnxqhyryus7fsg5icxtc6lgjj2qa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharya@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.262000+00:00
time-last-detected	2024-11-04T02:44:50.136000+00:00

330. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqyxhulvcgscbt6zkzpc5trcjdhz3xgkz6ljd77edpyha
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.191000+00:00
time-last-detected	2024-11-04T02:44:49.468000+00:00

331. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbffsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqo4tsqj4ljgbvo5yd3h5d5baj2cmqji3iqto4fiwfvoq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.378000+00:00
time-last-detected	2024-11-04T02:44:49.394000+00:00

332. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "prabhanjan.acharya@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqd5tyleygrt4djiqlibxseh5xrzwhlaysmkf27lj6bq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaigoundh3m2m4b7siyambjdhcwjbrhjq7oclqag3s2jv2k4rsq6ca
resource-name	prabhanjan.acharya@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.286000+00:00
time-last-detected	2024-11-04T02:44:50.157000+00:00

333. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, ACS_DATA_MANAGE_ADMIN, Administrators, ACS_ESS_Data_Safe_Admin]", "User Name": "karthik.muthu@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbivapzeax4lyxsr7leb5nzh3zdrjyp6h5ir3l6gycoq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.494000+00:00
time-last-detected	2024-11-04T02:44:49.423000+00:00

334. Problem details for USER_HAS_API_KEY_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Api Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_API_KEY_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.aaaaaaaaajw2ytmcqfdecmyk3rkqq6ekqzbsuhhtij3ck35b63yqg7fb3qa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing API Keys associated with user and disable the API Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmcpzjyj46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.aaaaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.658000+00:00
time-last-detected	2024-11-04T02:44:50.448000+00:00

335. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "chuck.hellier@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqd2ghmhi4i6lya7jjl2yaodawx7c6yinws4bl3syairnq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.167000+00:00
time-last-detected	2024-11-04T02:44:49.447000+00:00

336. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "manish.kakade@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq6f6vzeptcdbpq4vhnnviovtvnhecardplzknlw7jm7q
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaaffwuij5poiwsmbtu2a6epswdfcrxbsfm7yahd4n3b3pnabpaduq
resource-name	manish.kakade@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.182000+00:00
time-last-detected	2024-11-04T02:44:50.534000+00:00

337. Problem details for USER_HAS_DB_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has DB Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_DB_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwuufgcwcr7liyktl3yfn2qa25dlim4ofd3jsthqfhnq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing DB credentials associated with user and disable the DB credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrp6t6xtjansd4agjrmh7gmpriiocqvoobhta
resource-name	ricardo.e.acosta@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.599000+00:00
time-last-detected	2024-11-04T02:44:49.283000+00:00

338. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "68:2a:81:aa:d3:dd:d1:a3:c3:d1:d9:e6:92:c4:ee:d0", "IAM API key too old for user": "ricardo.e.acosta@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrrp6t6xtjansd4agjrmh7gmpriiocqvoobhta"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqloxiuwja6dofztdftzsn4uaxabuqroyeln5tslnkiq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrrp6t6xtjansd4agjrmh7gmpriiocqvoobhta/68:2a:81:aa:d3:dd:d1:a3:c3:d1:d9:e6:92:c4:ee:d0
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaa3gps4x4epvy5fhrrp6t6xtjansd4agjrmh7gmpriiocqvoobhta/68:2a:81:aa:d3:dd:d1:a3:c3:d1:d9:e6:92:c4:ee:d0
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.461000+00:00
time-last-detected	2024-11-04T02:44:49.140000+00:00

339. Problem details for USER_HAS_AUTH_TOKEN_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[CSS_DATA_MANAGE_ADMIN, Administrators]", "User Name": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbffsphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Auth Token capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_AUTH_TOKEN_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq5z6t62btdec2n6tzonabqsk45z4x43s64ykphwsadlqq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Auth Tokens associated with user and disable the Auth Token capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfqeilsmbd6x3pl3va7nm6ma
resource-name	mihai.alistar@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.367000+00:00
time-last-detected	2024-11-04T02:44:49.381000+00:00

340. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3obgcgvqfnnd7zbyds5bshw2uduknwpfmiux54sepifa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.583000+00:00
time-last-detected	2024-11-04T02:44:50.203000+00:00

341. Problem details for API_KEY_TOO_OLD

Key	Value
additional-details	{"Fingerprint": "10:1e:c8:31:59:61:6a:60:da:9e:23:44:44:89:61:1b", "IAM API key too old for user": "mihai.alistar@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfgeilsmbd6x3pl3va7nm6ma"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	API_KEY_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqfuelzerqnbyd3b55wnqgsmx33txxacbunhaehjc3a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate API keys regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfgeilsmbd6x3pl3va7nm6ma/10:1e:c8:31:59:61:6a:60:da:9e:23:44:44:89:61:1b
resource-name	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq/ocid1.user.oc1..aaaaaaaaagwcnhr73647dywzpxj4tnjurfwuotfgeilsmbd6x3pl3va7nm6ma/10:1e:c8:31:59:61:6a:60:da:9e:23:44:44:89:61:1b
resource-type	IAMKey
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtplijxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.456000+00:00
time-last-detected	2024-11-04T02:44:50.211000+00:00

342. Problem details for POLICY_GIVES_MANY_PRIVILEGES

Key	Value
additional-details	{"policyStatements": "Allow service objectstorage-us-ashburn-1 to manage object-family in compartment ESSDEV,allow group CSS_DATA_MANAGE_ADMIN to manage object-family in compartment ESSDEV,Allow service objectstorage-us-ashburn-1 to manage object-family in compartment ESSCTL,allow group CSS_DATA_MANAGE_ADMIN to manage object-family in compartment ESSCTL,Allow service objectstorage-us-ashburn-1 to manage object-family in tenancy")}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	IAM policies give access and control of resources. If an IAM policy entry grants management (full control) of a family of resources or all resources to either the tenancy OR a compartment (e.g., allow <user/group> to manage <some-resource>[all-resources] [in tenancy/compartment]) and that group's OCID or the policy OCID is NOT exempted from this check, a problem is created.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	POLICY_GIVES_MANY_PRIVILEGES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqpi3hz367r4hnpwiyqrk5hu2l5k56lrvlg2wsh76bba
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.policy.oc1..aaaaaaaaagvvvsusmjldtgaxz6k7id66ikkxtqyd5mer2g57w5hs4kbq4c4ba
resource-name	CSS Data Manage_Pol
resource-type	Policy
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.510000+00:00
time-last-detected	2024-11-04T02:44:49.351000+00:00

343. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "chuck.hellier@oracle.com", "Password Time Created": "2023-05-19T18:59:46.496Z", "User OCID": "ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqlknhbijo5cpeyit5xxqq2uyqwu3rnmnfd5xd5b6oqwq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaah3scp2wtqp2xtfy47qhzn4v323az43n5ywhjsdjlwn3bdnyshmq
resource-name	chuck.hellier@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.184000+00:00
time-last-detected	2024-11-04T02:44:49.462000+00:00

344. Problem details for VCN_HAS_INTERNET_GATEWAY_ATTACHED

Key	Value
additional-details	{"internetGatewayId": "ocid1.internetgateway.oc1.iad.aaaaaaaa46kd5on36ge32m3uzzhk26e4mbjv74fst7g6gr77pficmqkz25g"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaazasktsmr3pz52xlqfqsu2fykejmbmad4e44heghqczlg7awt1pyla
description	Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VCN_HAS_INTERNET_GATEWAY_ATTACHED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqseml2u3xij63qibtauzzmnvkkbnmlawobjttsjaglq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.vcn.oc1.iad.amaaaaaajw2ytmaad2rgizwfjg3hbxyykkqz6fzzihj6nzoio77fa3hqufua
resource-name	vcn-20240321-1516
resource-type	VCN
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:46.747000+00:00
time-last-detected	2024-11-04T01:37:17.997000+00:00

345. Problem details for USER_HAS_CUSTOMER_SECRET_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qreo7bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Customer Secret Key capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CUSTOMER_SECRET_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqaa2sfpuqgu372ypskvw5astzyfv7gdww7zrn3dwmjlu7aa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing Customer Secret Keys associated with user and disable the Secret Key capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qreo7bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	HIGH
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.269000+00:00
time-last-detected	2024-11-04T02:44:50.178000+00:00

346. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "ajay.manda@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukj77i7rghq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdblhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqnhxcygxx3ajnfpawtj4o6krq4rbvvpnsbk2wqhrh6pfa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaalni7fnt2ebgxydb5jiv6d4ueq4swdebxnpakbwliukj77i7rghq
resource-name	ajay.manda@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.563000+00:00
time-last-detected	2024-11-04T02:44:50.182000+00:00

347. Problem details for USER_HAS_CONSOLE_PASSWORD_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "sudhanshu.x.sharma@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjftrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has Console Password capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_CONSOLE_PASSWORD_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqwd2faztivb5pqaxijqpr2hmjstqvblse5m77ofapnxa
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Disable the Console Password capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa3vkd3v2hjyja4wnxu5qre07bveco2xpiqr3r4uu5vvcrpefydwa
resource-name	sudhanshu.x.sharma@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpilljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.272000+00:00
time-last-detected	2024-11-04T02:44:50.181000+00:00

348. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "anand.poovakkat@oracle.com", "Password Time Created": "2023-05-22T02:43:33.386Z", "User OCID": "ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqcjjplmcpmvgr7r5x72jpwgudih45ckk5h7stthshrmga
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiyj5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.501000+00:00
time-last-detected	2024-11-04T02:44:49.837000+00:00

349. Problem details for USER_HAS_OAUTH_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "harinath.subramaniam@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyv46odmoafeypzega5rw6x6etknm3wa"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has OAuth2 Credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_OAUTH_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqmeihgsp67q33zdg3pczr4einw7w5wccmgv7smvx5cy5a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing OAuth2 credentials associated with user and disable the OAuth2 credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaaatomjahsesarikwtmpzjyv46odmoafeypzega5rw6x6etknm3wa
resource-name	harinath.subramaniam@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334qkbtpllxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:54.682000+00:00
time-last-detected	2024-11-04T02:44:50.470000+00:00

350. Problem details for PASSWORD_TOO_OLD

Key	Value
additional-details	{"IAM console password too old for user": "karthik.muthu@oracle.com", "Password Time Created": "2024-05-30T21:38:57.207Z", "User OCID": "ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdpw5i34den7qhu7oq
description	Changing IAM Console password at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	PASSWORD_TOO_OLD
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqkg45r53kssmt54gotsyfhzmdfpysc7l4wgb5q42yfxla
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Rotate IAM Console password regularly, at least every 90 days.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaauwsu3qd3acuf7ocmefumxjnsw77azpbzgwypiqtzcxgdsp4raf5a
resource-name	karthik.muthu@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpiljxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.497000+00:00
time-last-detected	2024-11-04T02:44:49.427000+00:00

351. Problem details for USER_HAS_SMTP_CREDENTIAL_CAPABILITY

Key	Value
additional-details	{"Group Membership": "[Administrators]", "User Name": "dhanasekara.pandian@oracle.com", "User OCID": "ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbfsph232o4qhdublhdpw5i34den7qhu7oq
description	User in tenancy has SMTP credential capability enabled.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	USER_HAS_SMTP_CREDENTIAL_CAPABILITY
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqbi3n4elhvnrh53mgjoiw2c6v27lcjmdtxbgr7zmk4rra
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Users in tenancy should not have capabilities enabled. Delete any existing SMTP credentials associated with user and disable the SMTP credential capability.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1..aaaaaaaa4mwh3zkayhrpoou2i5k7zpkdw5woo56okot7n54brovpswkdwdq
resource-name	dhanasekara.pandian@oracle.com
resource-type	User
risk-level	MEDIUM
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwknna
time-first-detected	2024-10-23T09:10:55.084000+00:00
time-last-detected	2024-11-04T02:44:50.467000+00:00

352. Problem details for OCI_IAM_GRP_FEW_MEMBERS_FOUND

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1..aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	IAM group membership frequently grants access to resources and features. Group memberships that have too few members may represent excess privileges being "orphaned".
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	OCI_IAM_GRP_FEW_MEMBERS_FOUND
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqq6cikhxnp24hquoy2tvply5t74uvbevpfly2knuemka
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["IAM"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Review the group membership related privileges to ensure that excessive or orphaned privileges are not present.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.group.oc1..aaaaaaaaauzl33jok3ihinotob4tqzgq2y2nfsrvhajmgtmkcrqynmmpq3ua
resource-name	All Domain Users
resource-type	Group
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpiljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:10:55.178000+00:00
time-last-detected	2024-11-04T02:44:49.118000+00:00

353. Problem details for NO_MFA_ENABLED_FOR_USER

Key	Value
additional-details	{}
auto-resolve-date	None
comment	
compartment-id	ocid1.tenancy.oc1.aaaaaaaaadmyjfrj7p7f47wzbf5sphi232o4qhdublhdw5i34den7qhu7oq
description	Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	NO_MFA_ENABLED_FOR_USER
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcq3xied37kihcwpmxya7mxbk5x76ygmlxwm2vppnurk7a
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_IAM", "IAM", "CIS_OCI_V1.1_IAM", "CIS_OCI_V_2.0.0"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.
region	us-ashburn-1
regions	["us-ashburn-1"]
resource-id	ocid1.user.oc1.aaaaaaaaatpseyaxaihsqit4xjog2wlqqcek3j7mj3avtdsbpha3tiy5jqkq
resource-name	anand.poovakkat@oracle.com
resource-type	User
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpijxkuy4vbsqckfdwkna
time-first-detected	2024-10-23T09:10:54.478000+00:00
time-last-detected	2024-11-04T02:44:49.814000+00:00

354. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{""ICMP": "3", "vcnDisplayName": "ACS-VCN02", "vcnId": "ocid1.vcn.oc1.us-chicago-1.amaaaaajw2ytmaa45isdoz2e6exayxxnlz5lt65vv7ctnhptvz5kfkarga"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zrh633c7amzi5zaozoygg
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaajw2ytmcqmubzqozz6fbcfejgzop3stt3a4ronqok6d5qzt5zdaq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-chicago-1
regions	["us-chicago-1"]
resource-id	ocid1.securitylist.oc1.us-chicago-1.aaaaaaaaabih5ineraia2y4axy32ysmqqsrwf6t7e3qiucnpkoxnkiyxqlq
resource-name	security list for private subnet-ACS-VCN02
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtplljkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:05:07.668000+00:00
time-last-detected	2024-11-03T22:10:31.378000+00:00

355. Problem details for VCN_HAS_INTERNET_GATEWAY_ATTACHED

Key	Value
additional-details	{"internetGatewayId": "ocid1.internetgateway.oc1.us-chicago-1.aaaaaaaaaddukaqt2rxqni2hoahc6gxtnhn6cle372jdxddsyzbz4jscvoeq"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zrh633c7amzi5zaozoygg
description	Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity.
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	VCN_HAS_INTERNET_GATEWAY_ATTACHED
id	ocid1.cloudguardproblem.oc1.iad.amaaaaaajw2ytmcqp7syi3nr3uxyo6pjbn6qjwz63ueqn2msjafyng
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["Network"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0.
region	us-chicago-1
regions	["us-chicago-1"]
resource-id	ocid1.vcn.oc1.us-chicago-1.amaaaaaajw2ytmaa45isdoz2e6exayxxnlz5lt65vv7ctnhptvz5kfarga
resource-name	ACS-VCN02
resource-type	VCN
risk-level	LOW
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpljxkuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:05:07.215000+00:00
time-last-detected	2024-11-03T22:10:31.365000+00:00

356. Problem details for SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES

Key	Value
additional-details	{"ICMP": "3", "TCP": "22", "vcnDisplayName": "ACS-VCN02", "vcnId": "ocid1.vcn.oc1.us-chicago-1.amaaaaajw2ytmaa45isdoz2e6exayxxnlz5lt65vv7ctnhptvz5kfkarga"}
auto-resolve-date	None
comment	None
compartment-id	ocid1.compartment.oc1..aaaaaaaaafkcwtayzf33t6ynmrh57n7qcklq67e7zrh633c7amzi5zaozoygg
description	Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0)
detector-id	IAAS_CONFIGURATION_DETECTOR
detector-rule-id	SECURITY_LIST_ALLows_TRAFFIC_FROM_ALL_SOURCES
id	ocid1.cloudguardproblem.oc1.iad.amaaaaajw2ytmcqqlac22u6dbets46uwfdkgycbotjvgv44jxtkehwq
impacted-resource-id	None
impacted-resource-name	None
impacted-resource-type	None
labels	["CIS_OCI_V1.0_NETWORK", "Network", "CIS_OCI_V1.1_NETWORK"]
lifecycle-detail	OPEN
lifecycle-state	ACTIVE
locks	None
peak-risk-score	None
peak-risk-score-date	None
peak-risk-score-lookup-period-in-days	14
recommendation	To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized CIDR blocks, rather than leaving them open to the internet (0.0.0.0/0).
region	us-chicago-1
regions	["us-chicago-1"]
resource-id	ocid1.securitylist.oc1.us-chicago-1.aaaaaaaaalz5fno5klribnest7ccsdbymyhsynbnykn5ejoz667aojv3q2q
resource-name	Default Security List for ACS-VCN02
resource-type	VCN
risk-level	CRITICAL
risk-score	None
target-id	ocid1.cloudguardtarget.oc1.iad.amaaaaajw2ytmaajpwn2kdoue6b7vy334gkbtpillxuy4vbsqckqfdwkna
time-first-detected	2024-10-23T09:05:08.066000+00:00
time-last-detected	2024-11-03T22:10:31.271000+00:00

Appendix – Additional Reading

Connect with us

Call **+1.800.ORACLE1** or visit oracle.com. Outside North America, find your local office at: oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.