IBM

Security Summary

External Report
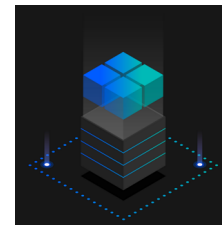
Product name:	Cloud Pak for Watson AIOps
Product version:	3.3.2-rc2-202205110601
Report date:	Wed May 25 2022
Description:	This is an external security transparency document.
Instructions:	For more information about the document please refer to the following information page
	Information Page https://ibm.biz/Bdfs2e

Image Vulnerability Management   Compliance

Product images are scanned for vulnerabilities and all known vulnerabilities are within their remediation timelines ✓

Principle of Least Privilege   Compliance

All Pods run with the Red Hat restricted security context constraint

All product containers specify an alphanumeric USER (non-root) in their Dockerfile or equivalent OCI build file for container images ✓

No product containers use sudo ✓

No product containers run as root ✓

Host and Container Isolation   Compliance

Product containers do not target a host IP ✓

Host and Container Isolation   Compliance

Product containers do not specify a host port   ✓

Product containers do not specify a host path to mount file or directory from host node's filesystem   ✓

Product containers do not enable host network access   ✓

Product containers do not share the host process ID namespace   ✓

Product containers do not share the host Inter Process Communication namespace   ✓

SSH/remote access to containers is disabled   ✓

Network Security and Protection   Compliance

Product does not allow anonymous access   ✓

Install default Network Policies that limit network traffic

Data Security   Compliance

Data encryption in transit is enabled by default using at least TLS 1.2

Audit Capability   Compliance

Pods are able to be identified as belonging to a product

Key and Certificate Management   Compliance

Support key rotation and replacement   ✓

Certificate rotation and replacement is supported by the product   ✓