Proposed Updates to Release Templates (Dublin) - Security Questions

M1 Release Planning Milestone

Practice Area	Checkpoint	Yes/No	Evidence - Comment	How to?
Security	Has the Release Security/Vulnerability table been filled out in the protected Security Vulnerabilities wiki space?		Table in in the protected Security Vulnerabilities wiki space corresponds to the latest NexusIQ scan	PTL reviews the NexusIQ scans for their project repos and fills out the vulnerability review table
	Have known vulnerabilities (critical and severe) to address/remove in the release been identified with jira tickets?		Jira tickets exist for vulnerabilities or the project indicates that there will be no vulnerable library replacement	Create Jira tickets
	Has the project committed to the release CII badging level		Project plans that include	See https://www.coreinfrastructure.org/programs/badge-program/ and https://wiki.onap.org/display/DW/CII+Badging+Program
	Has the project created their project CII questionnaire and completed the ONAP-level CII requirements?		URL of the questionnaire and all ONAP level CII requirements are answered	See https://wiki.onap.org/display/DW/CII+Badging+Program
	If the project uses java, has the project integrated with the oparent.pom?		Oparent.pom included in project	

M2 Release Planning Milestone

Practice Area	Checkpoint	Yes/No	Evidence - Comment	How to?
Security	Has the Release Security/Vulnerability table been updated in the protected Security Vulnerabilities wiki space?		Table in in the protected Security Vulnerabilities wiki space corresponding to the latest NexusIQ scan	PTL reviews the NexusIQ scans for their project repos and fills out the vulnerability review table
	Have all project containers been designed to run as a non-root user?			https://wiki.onap.org/display/DW/Best+Practices • The Docker and Kubernetes engines may run as root until such time as the products support non-root execution. • Applications may run as root within a container. • The process ID of a container must not run as the root ID with the exception of containers supporting ONAP features that require the container to run as the root ID. • Containers may run with root privileges. • Project containers that run as the root ID must document this in the release notes along with the functionality that requires the container to run as the root ID.

M3 Release Planning Milestone

Practice Area	Checkpoint	Yes/No	Evidence - Comment	How to?
Security	Has the Release Security/Vulnerability table been updated in the protected Security Vulnerabilities wiki space?		Table in in the protected Security Vulnerabilities wiki space corresponds to the latest NexusIQ scan	PTL reviews the NexusIQ scans for their project repos and fills out the vulnerability review table

	Has the project committed to enabling transport level encryption on all interfaces and the option to turn it off?		Requirements and test cases for transport layer encryption have been created for all interfaces not currently supporting encryption.	
	Has the project documented all open port information?		Provide all port information to the Integration team	PTL collects from the project team all ports used to support the protocols required by the project.
	Has the project provided the communication policy to OOM and Integration?			Recommended Protocols
	Do you have a plan to address by M4 the Critical and High vulnerabilities in the third party libraries used within your project?		Update all Jira tickets with the plans.	• Replace vulnerable packages • Document false positives in the release notes if it is not possible to replace the vulnerable packages • Document vulnerabilities inherited in dependencies: include the name of the dependency and any mitigations that can be implemented by an ONAP user

M4 Release Planning Milestone

Practice Area	Checkpoint	Yes/No	Evidence - Comment	How to?
Security	Has the Release Security/Vulnerability table been filled out in the protected Security Vulnerabilities wiki space?		Table in in the protected Security Vulnerabilities wiki space corresponds to the latest NexusIQ scan; all NexusIQ finding are marked as false positive or exploitable with the supporting analysis.	PTL reviews the NexusIQ scans for their project repos and fills out the vulnerability review table
	Are all Defects of priority Highest and High in status "Closed" in Jira? (this includes the Jira for Critical and Severe NexusIQ findings)		All Jira tickets for vulnerability elimination are complete.	Complete Jira tickets
	Did the project achieve the enablement of transport level encryption on all interfaces and the option of disabling transport level encryption?		All interfaces are exposed over TLS and the secure protocol can optionally be turned off	
	Do all containers run as a non-root user and is documentation available for those containers that must run as root in order to enable ONAP features?		• ONAP project containers do not run as the root ID with the exception of containers supporting ONAP features that require the container to run as the root ID. • Project containers that run as the root ID have documented this in the release notes along with the functionality that requires the container to run as the root ID.	https://wiki.onap.org/display/DW/Best+Practices
	Provide the "% Achieved" on the CII Best Practices program. Moved from Development section		Provide link to your project CII Best Practices page.	As documented in CII Badging Program, teams have to fill out CII Best Practices
REMOVE FROM DEVELOPMENT	Is there any Critical and Severe level security vulnerabilities older than 60 days old in the third party libraries used within your project unaddressed? Nexus-IQ classifies level as the following: • Critical is level 7 to 10 • Severe is level 4 to 6 • Moderate is level 1 to 3 which is complaint with CVSS V2.0 rating.			