CMF Security and Scanning Tools

Group	Item	Gerrit	GitHub	Manual /Automatic	Notes
Utilities	GitSecrets	Yes	Not needed	Automatic	Looks for Amazon credentials and password strings via regexp. Limited value because we doesn't have "ignore me" functionality. GitHub has its own checks and contacts repo admins for questionable content.
	TruffleHog	Yes	Yes	Automatic	
	Binary File Detection	Yes	Yes	Automatic	Flags changes for attention. Aim: repo size management, external material esp. images
	Large File detection	No	No	N/A	Coming soon. Value: large files overwhelm the Blackduck tool so preventing code license checks
	Client Side Pre-Commit Web Hooks	No	No	N/A	(trufflehog related, not yet deployed)
Tools	Blackduck	Yes	Yes	Automatic	Checks for reused opensource code, copyrights, our own problem strings (e.g. Yocto license checks), our own problem filetypes (certificates, recipes) Doesn't check every language (rust).
	Copyright Scan	Yes	Yes	Automatic	Checks for unrecognised copyrights
	Audit	Yes	Yes	Manual	In-house tools run when opensourcing a repo. Check for file headers/correct license files/binaries/certificates/copyrights/empty files
	NVD	Yes	Yes	Manual	Monthly run for selected platforms (RDK-B/V/C) Produces a report per variant Uses opensource NVD database and Yocto plugin
	Coverity	Yes	Yes	Automatic	Being rolled out. Runs static checks on Java, javascript for CVE and code quality. Runs build checks on C/C++ for RDK-B platform, more to come Monthly build check on RDK-B/V/C with more important results in 3 reports. Hard to get notice.