Security Review Guidelines

Contents

Security Review Guidelines

Security Review Guidelines for GE Digital or Predix Catalog/ Marketplace

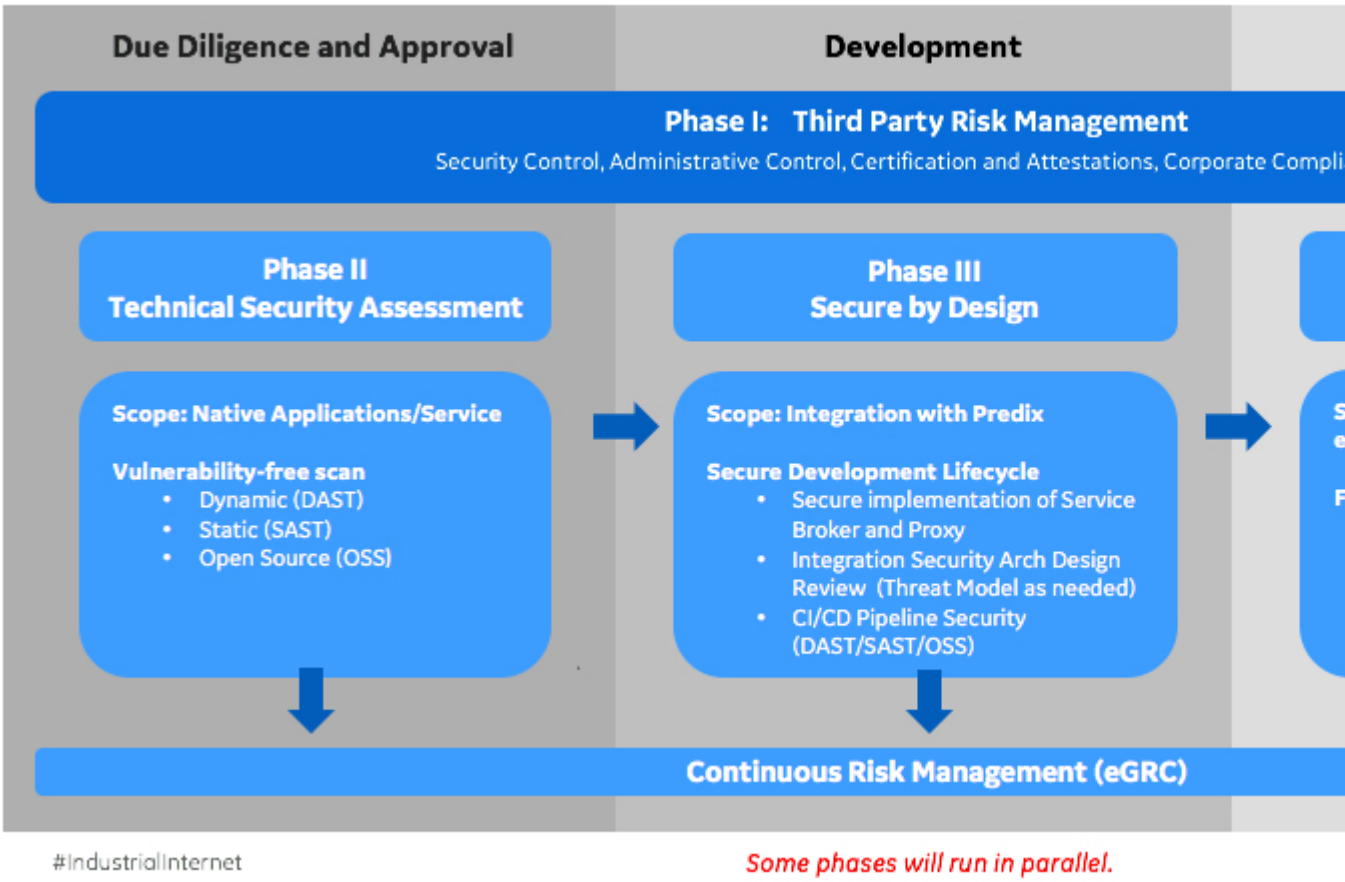
Any service, analytics or app wanting to be published as a GE Digital or Predix Catalog/Marketplace offering, must go through a mandatory, periodic security review. The GE Digital Platform & Product Cybersecurity (GED P&P Cybersecurity) team developed the following Security Review Guidelines to assess the security posture of the candidate service, analytics or app to ensure that each candidate follow the industry best practices for security, meet the security demands of GE's standards for the Industrial Internet, and promote trust for GE's digital platform, products and services.

Scope

The scope of the Security Review Guidelines includes analysis of the components that are intrinsic to the candidate as well as its supporting peripherals. The components that are intrinsic to a candidate service, analytics or app typically include, but are not limited to, its native code base, web services, APIs, integrations, authorizations/authentications, and encryption mechanisms. The supporting peripherals of a candidate service, analytics or app typically include, but are not limited to, its detection/monitoring framework or code management approach. All intrinsic and peripheral components for each candidate will be reviewed by the GED P&P Cybersecurity team without exception.

GE Digital or Predix Catalog/Marketplace Security Review Overview

The GE Digital or Predix Catalog/Marketplace Security Review process consists of four phases.



GE Digital will determine which partner or customer candidate must undergo Phase I, the Third Party Risk Management (TPRM) assessment.

The Phase II through Phase IV and Risk Management guidelines below give you details on what to expect and what to provide as you go through the Security Review process.

Phase II	Technical Security Review	Artifacts Required

	• Familiarize yourself with secure development practices by taking relevant free on-demand training courses from SAFECode
	• Review the free sources listed in the Secure Development Lifecycle document.
	• Review the Design & Architecture Guidance section in the Secure Development Lifecycle
	• Review the OWASP Top Ten Checklist
	• Obtain scan reports from reputable providers. The following scan reports are required:
	  ◦ DAST and/or SAST scan depending on your service
	  ◦ Open Source vulnerability scan
	• Manually test your application to ensure it meets review requirements not found by tools. For details, see: OWASP Testing Guide.
	• Remediate any issues found from all the scans.
	• Prepare to provide vulnerability-free set of scan results to the GED P&P Cybersecurity team.
		• Information about your company/ team
		• Business objective and technical objective of your solution
		• Services to be provided by your solution
		• Vulnerability-free scan reports for:
		  ◦ DAST and/or SAST
		  ◦ Open Source vulnerability scan

Phase III	Secure by Design	Artifacts Required

	• After you have integrated into the development environment, the GED P&P Cybersecurity team will review the implementation and assess the following aspects of your candidate:
	  ◦ Authentication/Authorization considerations
	  ◦ Web services and API security
	  ◦ Encryption
	  ◦ Detection/Monitoring/Logging
	  ◦ Threat modeling as needed
	• GED P&P Cybersecurity team will review the provided DAST/ SAST/OSS scan reports.
	• The GED P&P Cybersecurity team will conduct cursory security assessment as needed.
	• You shall implement the recommended remedial measures from the GED P&P Cybersecurity team.
	• The GED P&P Cybersecurity team will validate the implementation of recommended remedial measures.
		• Technical security contact(s) from your team
		• Documentations about your solution:
		  ◦ Requirements documents
		  ◦ Design documents
		  ◦ Data flow diagrams
		  ◦ Log Samples
		• Working test environment of your solution
		• Evidences of vulnerabilities remediated
		• Vulnerability-free scan reports for:
		  ◦ DAST and/or SAST
		  ◦ Open Source vulnerability scan

Phase IV	Penetration Testing	Artifacts Required
	• You shall provide the latest test environment endpoints to the GED P&P Cybersecurity team. • The GED P&P Cybersecurity team will conduct a full-stack penetration testing of your service and share vulnerability findings with you. • You shall implement the recommended remedial measures from the GED P&P Cybersecurity team. • The GED P&P Cybersecurity team will validate the implementation of recommended remedial measures.	• Artifacts from previous phases • Deployed solution in a non-production environment

Risk Management	Description
	• The GED P&P Cybersecurity Risk Management team will share the vulnerabilities and risks findings during the Agreement on Facts (AoF) Readout meeting. • Recommended remediation actions and remediation dates are agreed upon and documented. • GE Digital leadership teams are involved as needed.

GE Digital Platform & Product Cybersecurity Release Criteria

The matrix below shows, depending on the security risk level, the action you need to take before you can release your candidate service, analytic or app onto any GE Digital platform or product. It is **important** that you understand that your timeline to beta or GA is directly related to how fast you remediate the risks identified during the Security Review process and/or presented to you during the Agreement on Facts (AoF) readout meeting. All risks presented to you during the AoF meeting must be provided formal remediation dates that are mutually agreeable during or immediately after AoF readout. These risks will then be sufficiently remediated by your team/company to a point that the residue risk is **under** the threshold of the GED P&P Cybersecurity team recommendations. Any risk that is not remediated to conform with the GED P&P Cybersecurity Risk Management principles must be reviewed by GE Digital leadership teams for a decision.

The GED P&P Cybersecurity team looks to our partners, customers, and developer community to proactively drive the action items to meet security demands and remediate risks for your service prior to any production release. The GED P&P Cybersecurity team will validate the remediation to confirm that the risks have been adequately addressed. Failure to sufficiently remediate risks prior to your planned production release date may impact your ability to meet your commitment to the customer.

Security Risk Classification from AoF Readout	Required Action Prior to Beta Release	Required Action Prior to GA Re
Critical	Must remediate	Must remediate
High	Must remediate	Must remediate
Moderate	Notification to partner and GE Digital leadership teams	Must remediate unless risk accep leadership
Low	Notification to partner and GE Digital leadership teams	Recommend remediation

A candidate service, analytic or app that has met the Release Criteria above will be approved by the GE Digital Change Advisory Board.