TECHNICAL WHITEPAPER

Security Review Guidelines for Predix Catalog Tile Services

October 2016

PREDIX

Security Review Guidelines for Predix Catalog Tile Services

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Contents

Security Review Guidelines for Predix Catalog Tile Services

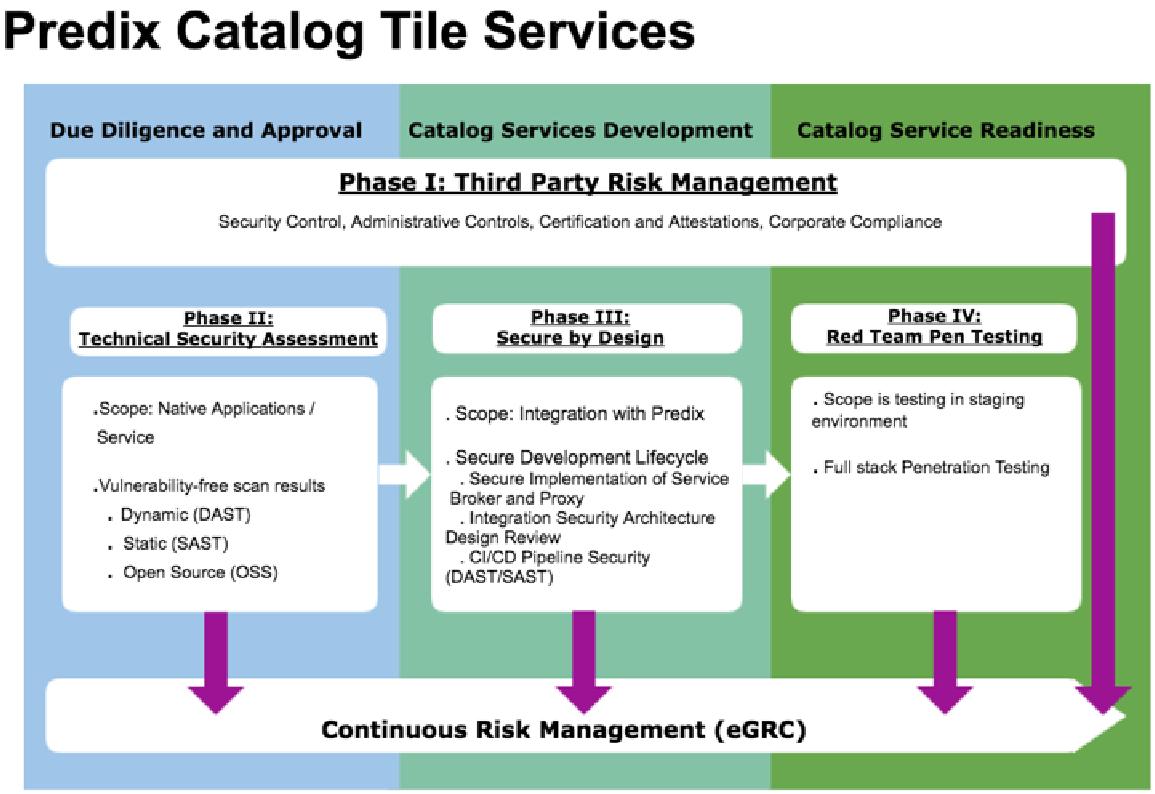
All services intending to become part of the Predix catalog offerings must go through a mandatory, periodic security review. The Security Review has been developed to assess the security posture of requesting service providers and development practices of software developers, to ensure that services published on the Predix catalog follow industry best practices for security, to meet the security demands of GE's standards for industrial internet, and to promote trust for GE's digital products and services.

Scope

The scope of the security review includes components that are intrinsic to the intending Predix Catalog Tile Service as well as its supporting peripherals. The components that are intrinsic to an intending tile service typically include but are not limited to its native code base, web services, APIs, integrations, authorizations/authentications and encryption mechanisms, etc. The supporting peripherals of an intending service typically include but are not limited to its detection/monitoring framework, code management approach, etc. All intrinsic and peripheral components will be reviewed by Predix Cyber Security without exception for any intending catalog tile service.

Predix Catalog Tile Service Security Review Overview

The Predix Catalog Tile Service Security Review process consists of 4 phases. Any intending catalog tile service must pass Predix technical security assessment (Phase II), a secure-by-design review (Phase III), and Predix penetration testing (Phase IV). Predix Catalog Tile Service Security Review will also determine which ISVs must undergo a Third Party Risk Management assessment (Phase I) in parallel.


Predix Catalog Tile Services
Due Diligence and Approval
Catalog Services Development
Catalog Service Readiness
Phase I: Third Party Risk Management
Security Control, Administrative Controls, Certification and Attestations, Corporate Compliance
Phase II: Technical Security Assessment
.Scope: Native Applications / Service
.Vulnerability-free scan results
. Dynamic (DAST)
. Static (SAST)
. Open Source (OSS)
Phase III: Secure by Design
. Scope: Integration with Predix
. Secure Development Lifecycle
. Secure Implementation of Service Broker and Proxy
. Integration Security Architecture Design Review
. CI/CD Pipeline Security (DAST/SAST)
Phase IV: Red Team Pen Testing
. Scope is testing in staging environment
. Full stack Penetration Testing
Continuous Risk Management (eGRC)

Predix will determine which ISVs must undergo TPRM assessment. This is based on several factors pertaining to the ISV.

Figure 1: Predix Catalog Tile Services

Security Review Guidelines

The guidelines below will help you understand what to expect and what to provide as you go through the Predix Catalog Tile Service Security Review process.

Table 1:

		Predix Cyber Security Review	**Artifacts Required**
Predix Catalog Tile Services Process	Technical Security Review	• Familiarize yourself with secure development practices by taking relevant free on-demand training courses from *SAFECode* • Review the free sources listed in our *Secure Development Lifecycle* guide (published separately) • Review the Predix Cyber Security Design & Architecture Guidance section in the *Secure Development Lifecycle* guide (published separately) • Review the *OWASP Top Ten Checklist* • Obtain scan reports from reputable providers. Required scan reports include: --DAST/SAST scan depending on your service --Open Source Vulnerability scan • Manually test your app 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 Predix Cyber Security team	• Information about your company/team • Business objective and technical objective of your Predix solution • Services to be provided by your intending Predix tile • Vulnerability Free Scan Reports for: • --DAST/SAST --Open Source Vulnerability scan
	Secure by Design	• Once your Predix service integration is created in the development environment, Predix Cyber Security team will review the implementation and assess the following aspects of your service: - Authentication/Authorization considerations - Web services and API security - Encryption - Detection / Monitoring - Threat modeling as needed • Predix Cyber Security team will review the provided DAST/SAST/OSS Scan Reports • Predix Cyber Security team will conduct cursory security assessment as needed	• Technical security contact(s) from your team • Documentations about your Predix solution: - Requirements Document(s) - Design Document(s) - Data Flow Diagram(s) • Working test environment of your Predix solution • Evidences of vulnerabilities remediated • Vulnerability Free Scan Reports for - DAST/SAST

		Predix Cyber Security Review	Artifacts Required
		• You shall implement the recommended remedial measures from Predix Cyber Security reviews • Predix Cyber Security team will validate the implementation of recommended remedial measures	- Open Source Vulnerability Scan
	Penetration Testing (Red Team Validation)	- You shall provide the latest test environment endpoints to Predix Cyber Security team - Predix Cyber Security team will conduct full-stack penetration testing of your service, and share vulnerability findings with you - You shall implement the recommended remedial measures from Predix Cyber Security reviews - Predix Cyber Security team will validate the implementation of recommended remedial measures	- Artifacts from previous phases - Deployed tile service in Predix staging environment
	Risk Management	- Vulnerabilities and risks found are shared with you by Predix Cyber Security Risk Management team during "Agreement on Facts (AoF)" meeting. - Recommended remediation actions and remediation dates are agreed upon and documented - Service/Predix Leadership teams are involved as needed - Go-Live decision for production rendered after remediation efforts are completed according to the section below.	

Predix Cyber Security Release Criteria

The matrix below demonstrates the security criteria for your service to become releasable on the Predix platform. It is IMPORTANT that you understand your timeline to Beta/GA is directly related with how fast you remediate the risks identified during the Predix Catalog Tile Services Security Review process, 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 right 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 Predix cyber security recommendation. Any risk that is not remediated to conform with Predix Cyber Security Risk Management principles must be reviewed by Predix Leadership teams for decision.

Predix Cyber Security look to our ISVs, Partners, Customers and Developer Community to proactively drive the action items to meet security demands and remediate risks for your service prior to any Predix production release. Predix Cyber Security 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 according to Predix Cyber Security may result in repercussions to your ability to meet your own prior customer commitment.

Security Risk Classification from AoF Readout	**Predix Cyber Security: Required Action Prior to Beta Release**	**Predix Cyber Security: Required Action Prior to GA Release**
Critical	Must Remediate	Must Remediate
High	Must Remediate	Must Remediate
Moderate	Notification to Partner and Predix Leadership Teams	Must Remediate unless Risk Accepted by Predix Leadership
Low	Notification to Partner and Predix Leadership Teams	Recommend Remediation