Secure Software Development Framework

EPRI's SSDF Life Cycle Playbook for Developing Applications v1.0

April 2023

www.epri.com

Review this Playbook - Why and Who

Why?

The Secure Software Development Framework (SSDF) goal is to ‘shift security left’ at EPRI, enabling developers to deliver secure code utilizing leading DevSecOps practices. As a result of this effort, EPRI is on the path to utilize CI/CD pipelines and security tool integrations to streamline development life cycle processes.

Who?

This playbook provides guidance to:

- Software Project Managers
- Software Developers
- Sector Leadership
- EPRI IT Personnel

on the required processes and requirements to successfully deploy Desktop, Subscriber Website (SWS) and/or Cloud applications at EPRI. Use this playbook as a companion to SWDev.epri.com.

Review this Playbook - What is Changing and When

- Now
  - SQA checking compliance of complete source code package at SQA submittal (as documented in SOW)
  - Security Scanning Tools available (manual process):
    - Static Application Security Testing (SAST) utilizing Checkmarx
    - Dynamic Application Security Testing **(**DAST) utilizing Qualys
    - Container Image Scanning for SWS containers utilizing AquaSec
  - Code Signing for Windows desktop applications available when required
- Q3
  - On-Prem ADO (Azure DevOps) code repository to store source code for all applications
  - Manual SAST/SCA scanning for applications submitted to SQA
- Q4
  - Automated container image scanning for SWS containers (AquaSec)
- Q1 2024
  - Automated pipelines for all new applications
  - Automated SAST/SCA scanning for applications submitted to SQA

EPRI's SSDF Life Cycle

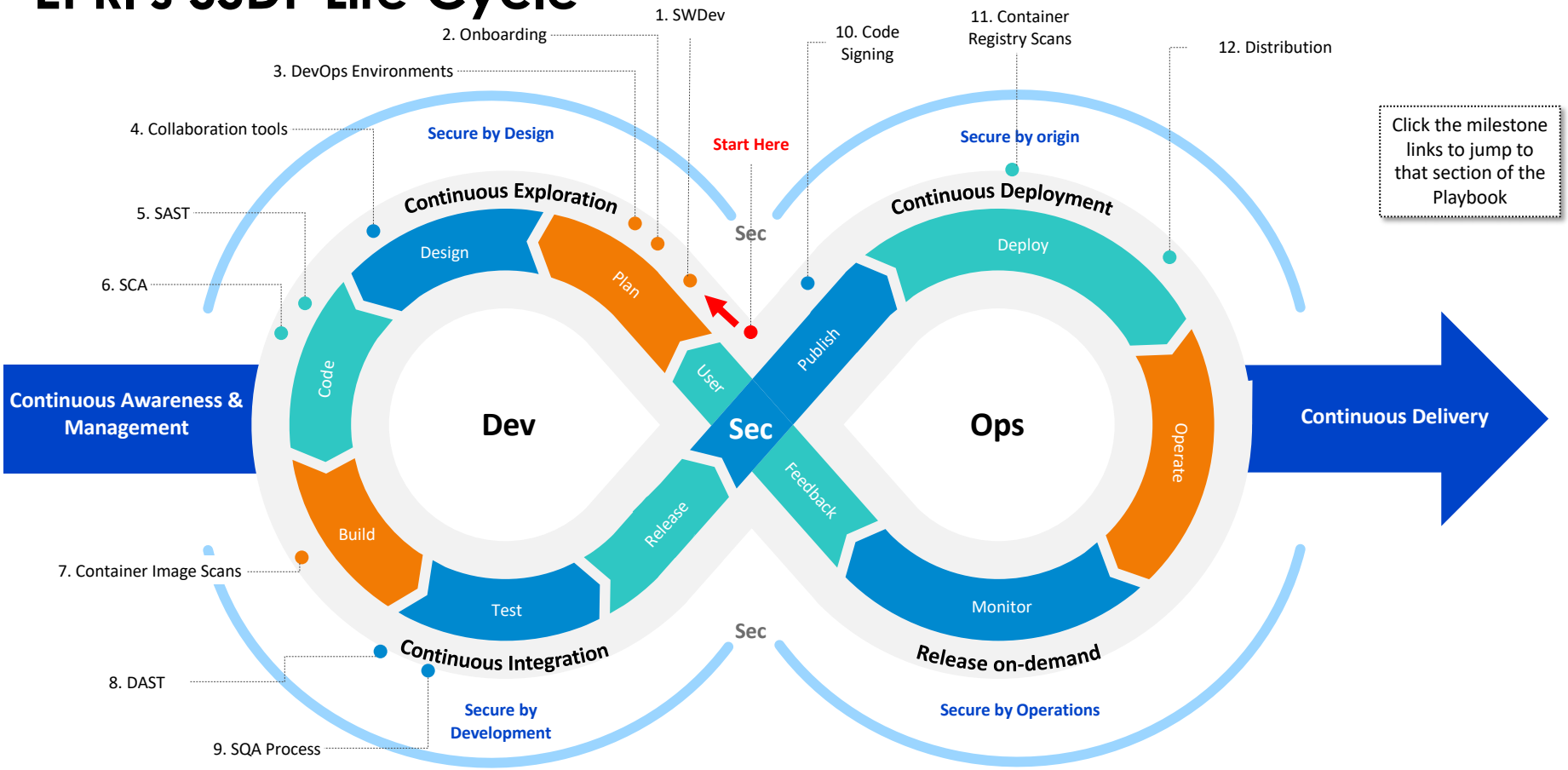
Life Cycle Process with Lead Responsibility

1. Software Development Website (SWDev)..... Project Manager
2. Contractor/Developer Onboarding..... Project Manager
3. DevOps Environments ..... IT/SQA
4. Collaboration Tools ..... IT/SQA
5. Static Application Security Testing (SAST) with Checkmarx ..... Developer
6. Software Composition Analysis (SCA) with Checkmarx ..... Developer
7. Container Image Scans..... IT/Infosec
8. Dynamic Application Security Testing (DAST) with Qualys..... IT/SQA
9. Software Quality Assurance (SQA) ..... IT/SQA
10. Code Signing ..... IT/SQA
11. Container Registry Scans..... IT/Infosec
12. Distribution ..... IT/SQA

- Definition of Terms

Playbook Life Cycle & Activities

EPRI's SSDF Life Cycle



1. Software Development Website

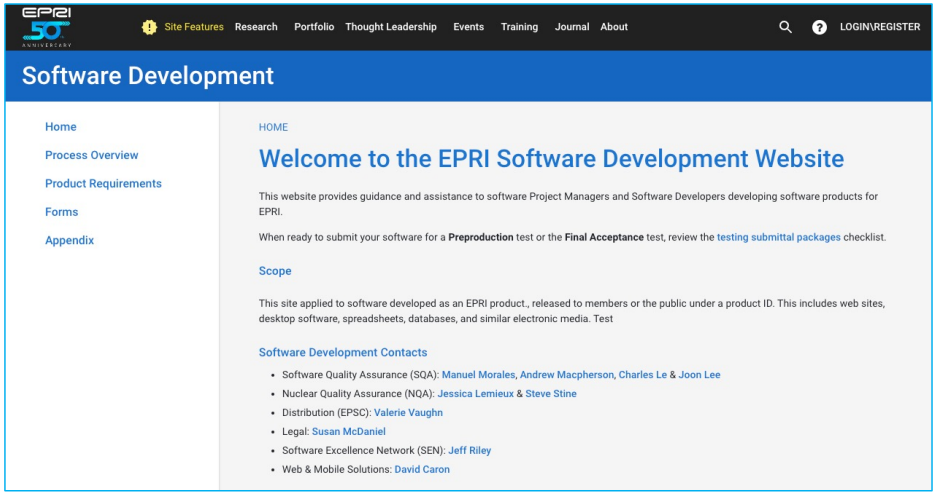
Lead Responsibility: **Project Manager (PM)**
Action Items: **PM and Developer** - Review & Understand SWDev.com requirements

All software development for EPRI starts with:

1. Review of the **EPRI Software Development Website**: swdev.epri.com for applicable guidance and requirements depending on the deliverable type (e.g., Desktop, Subscriber Website (SWS), Cloud, etc.).
2. Contact the SQA team (SQA@epri.com) to discuss the process and requirements.

Use this playbook as a companion to the development website.

As new practices from this playbook are implemented and integrated into the development process, they will be incorporated into swdev.epri.com.



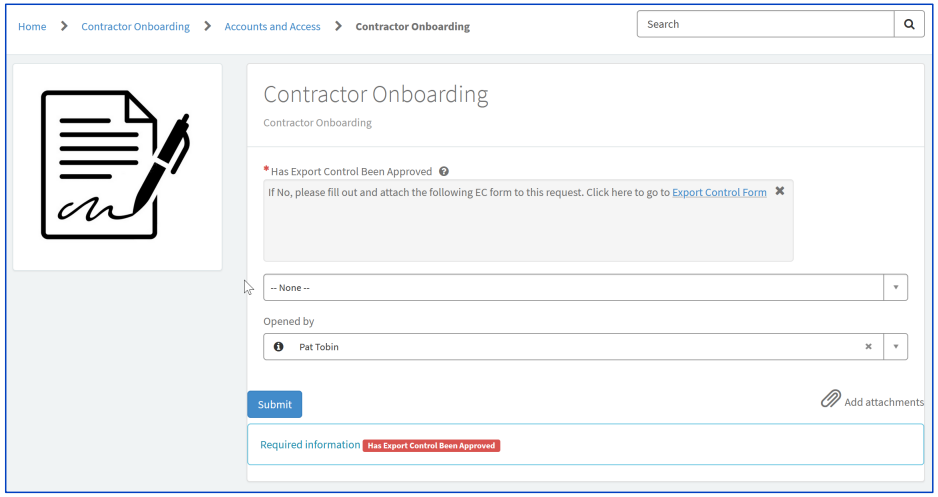
Life Cycle | **SW Dev** | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

2. Contractor/Developer Onboarding

Lead Responsibility: **Project Manager**
Action Item: **PM** performs onboarding

- EPRI Project Manager's using an external developer/contractor need to onboard the developer. The following form provides a job aid to guide you through the general steps/forms:
  - Contractor Onboarding Form & Job Aid
  - The ServiceNow forms will provide the developer with essential access to software development resources (e.g., Citrix, EPRIDT Environment, ADO, Checkmarx, Jira, Confluence, etc).

- For instructions on pushing code using Citrix and Box:
  - How to Push Code using Citrix and Box



Life Cycle | SW Dev | **Contractor/ Dev Onboarding** | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

3. DevOps Environments

Lead Responsibility: **IT/SQA**

Action Items: **IT/SQA** creates the environment following the Kickoff Meeting with PM, developer, and IT.
Developer utilizes DevOps environments

EPRI supports two Azure DevOps (ADO) Environments:

1. **On-prem ADO Server** (e.g., Subscriber Websites (SWS), Desktop).
2. **ADO Cloud** (e.g., EPRI.com, API Framework).

Environment usage requires Citrix access to ADO, Jira, other on-prem tools, including EPRIDT (required for testing)

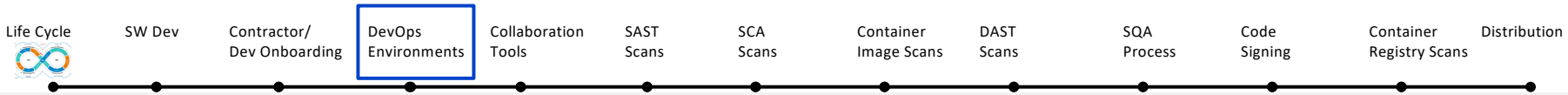
New Deliverables

- SQA provide On-Prem ADO project space
- SQA provide On-Prem ADO build pipeline
- SQA provide tools spaces (e.g., Jira, Confluence, etc.)
- Developers to provide source code
- Developers push code to repo and run SAST scans
- Project Managers ensure all documentation is in Jira or ECM

Existing Deliverables, New Updates

- SQA to migrate to On-Prem ADO
- SQA provide On-Prem ADO build pipeline
- SQA provide tools spaces (e.g., Jira, Confluence, etc.)
- Developers to provide source code
- Developers push code to repo and run SAST scans
  Note: If code cannot run through pipeline, must run SAST manually
- Project Managers ensure all documentation is in Jira or ECM

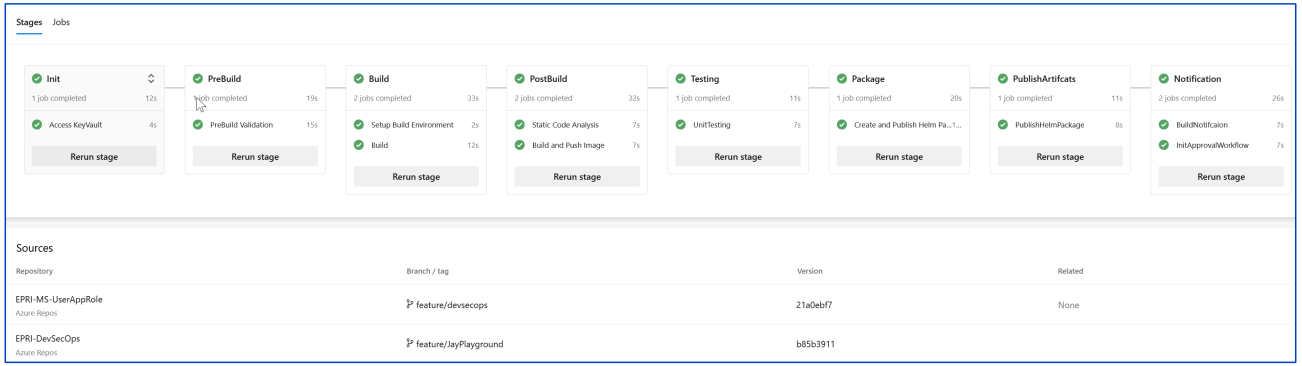
Contact the SQA team (SQA@epri.com) to discuss Environment options.



3. DevOps Environments: DevSecOps Guide & Demo

After the development environment is setup, use the DevSecOps Developer Guide EPRI, which includes:

- Predefined templates available to developers
- Prerequisites for the developer to work with build pipelines
- What pipelines are built and the purpose for each
- The parameters and variables in the pipelines a developer may need to edit
- What stages a build goes through (i.e., Build -> SAST -> DAST -> Package -> Deploy)

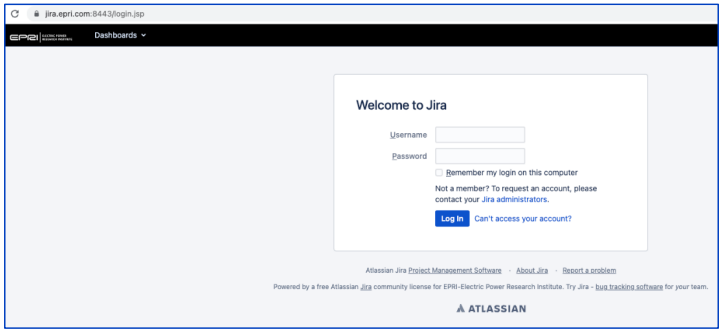


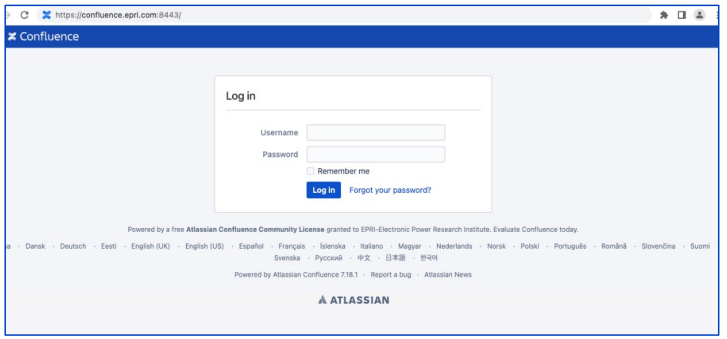
For demonstrations of the CI/CD build pipelines for: 'Nuclear API' and 'Power Quality Investigator (PQI)'

Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

4. Collaboration Tools

Lead Responsibility: **IT/SQA**
Action Items: **IT/SQA** creates Jira & Confluence spaces
PM & Developer utilize spaces





- **Jira** is a platform that combines issue/bug collection and agile software project management capabilities into a single application.
  - URL: https://jira.epri.com:8443/ (contact SQA team for access)
  - User guide: https://epri.box.com/s/iizw4v2ai6miuq3o7vu39qbdw8408mhs
- **Confluence** is a knowledge base platform for project documentation and organization that integrates with Jira.
  - URL: https://confluence.epri.com:8443/ (Contact SQA team for access)
  - User Guide: https://epri.box.com/s/2xiaydbgz62l7fvcmkwutrgtc2wdbbey

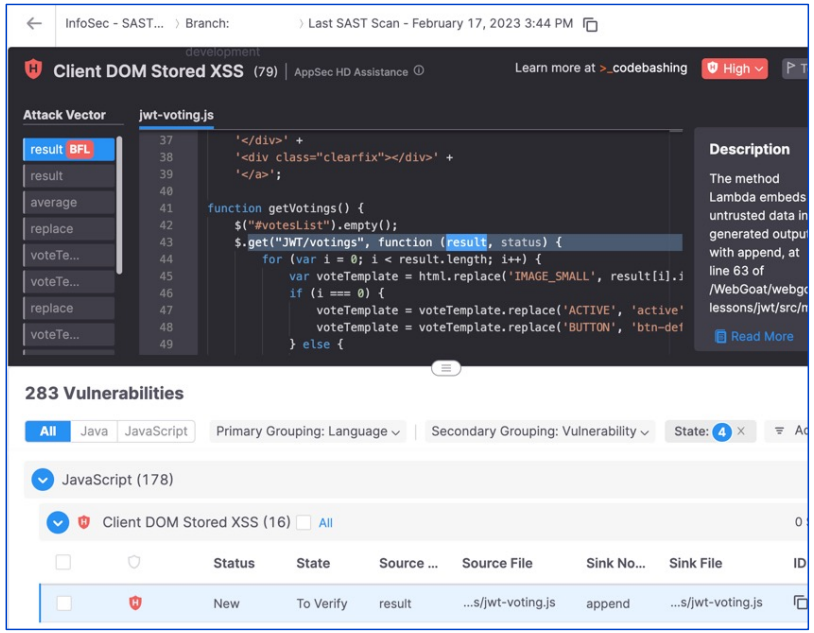
Additional Collaboration Tools:

- **Monday.com** is a platform for project management.
  For more information, contact the Project Management Office, also, visit Welcome to Monday!
- **Box.com** will continue to be available and is preferred storage for EPRI and Team documentation.

Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | **Collaboration Tools** | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

5. SAST (Checkmarx)

Lead Responsibility: **Developer**
Action Items: **Developer** runs scans and remediates
IT/Infosec reviews and advise/approve



Static Application Security Testing (SAST) with Checkmarx

- Before you submit your application for the SQA Pre-production (e.g., Alpha, Beta, Prototype, etc.) or SQA Production (e.g., Final Acceptance) test, the source code must be scanned by the Checkmarx source code scanner and the report must be approved by the Information Security (InfoSec) team.

- A SAST scan finds vulnerabilities in source code and can be a fully automated step of the CI pipeline or run manually as needed. Reach out to InfoSec@epri.com for Checkmarx access.

For more information on the process and responsibilities, review the documents defined below:

- SAST SOP
- SAST Process Flow

Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | **SAST Scans** | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

6. SCA (Checkmarx)

Lead Responsibility: **Developer**
Action Items: **Developer** runs scans and remediates
IT/Infosec reviews and advise/approve

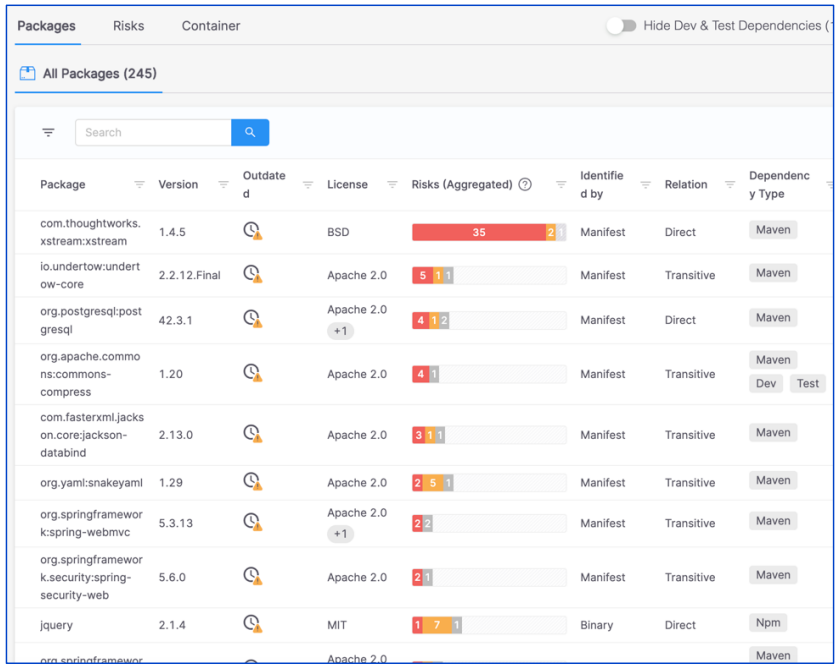
Software Composition Analysis (SCA) with Checkmarx

- A SCA scan documents the third-party and open-source packages in your code and identifies vulnerable components in these items.

- A Checkmarx scan will include a SCA scan along with SAST, which can be a fully automated step of the CI pipeline or run manually as needed.

For more information on the process and responsibilities, review the documents defined below:

- SAST SOP
- SAST Process Flow

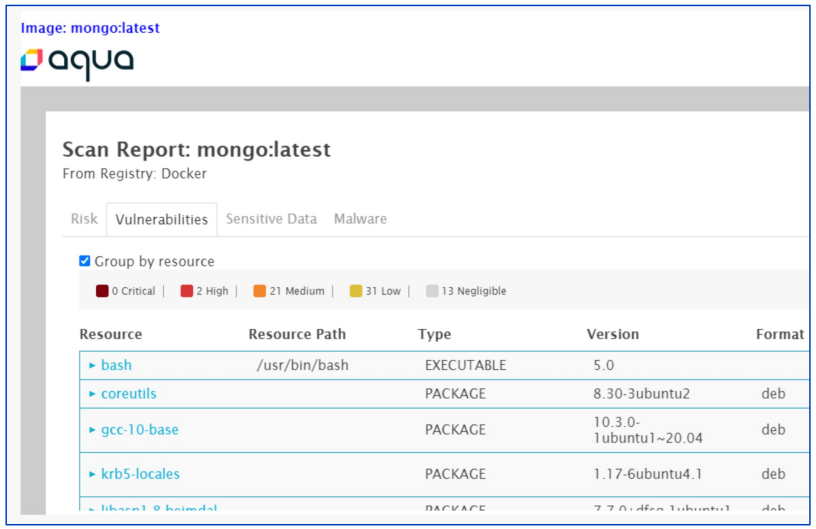


7. Container Image Scans

Lead Responsibility: **IT/InfoSec**
Action Items: **IT/InfoSec** performs scan
Developer remediates

Kubernetes/Container Security Scanning

- Kubernetes/container scanning: container images include system libraries, system tools, and other platform settings that your apps need to run—giving developers the benefits of portability and agility to quickly expand on or create new apps
- Scan container images to detect vulnerabilities in third-party code, sensitive data such as private keys, and malware
- Container image scanning can be integrated into the CI/CD pipeline, but will start as a manual process with InfoSec



Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | **Container Image Scans** | DAST Scans | SQA Process | Code Signing | Container Registry Scans | Distribution

8. DAST (Qualys)

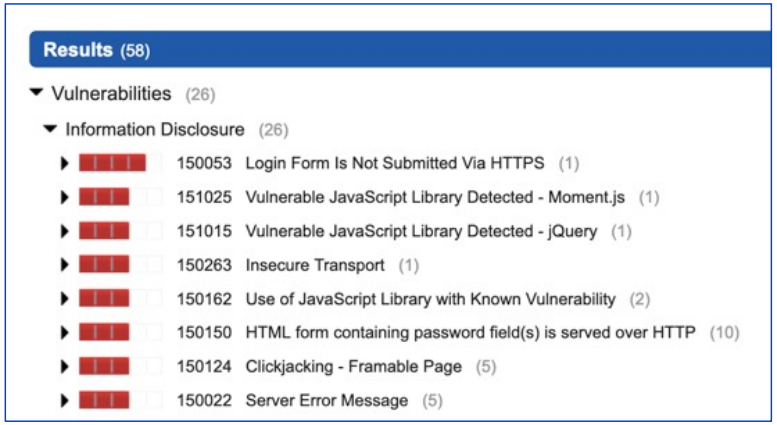
Lead Responsibility: **IT/SQA**
Action Items: **IT/SQA** Runs scan and generates report
Developer remediates
IT/Infosec reviews and advise/approve

Dynamic Application Security Testing with Qualys

- Before your web deliverable (e.g., Subscriber Website (SWS), Microsite, etc.) can be promoted to the EPRI Production Environment, it must be scanned by the Qualys web vulnerability security scanner and the report must be approved by the InfoSec team.

- The SQA team will run the vulnerability scan and send the project manager, developer, and InfoSec team the results. Infosec will review the report and the application and move it forward in the process with no Medium or higher identified vulnerabilities.

- For more information on the process and responsibilities, see the documents defined below:
  - DAST SOP
  - DAST Process Flow



9. Software Quality Assurance (SQA) Process

Lead Responsibility: **IT/SQA**
Action Items: **PM** initiates SQA submittal process
IT/SQA performs testing and scan

After the software has been developed, the next step is the SQA submittal (ECM for Nuclear, SecureShare for PDU & GEN), which initiates the SQA testing process:

https://swdev.epri.com/process-overview/acceptance

The submittal information page includes information on Pre-production (e.g., Alpha, Beta, Protype, etc.) and Production (e.g., Final Acceptance) testing options and requirements.

Process Update: SQA will check compliance of a complete source code package at the SQA submittal (as documented in SOW). Complete source code is required for the Checkmarx source code scan.

SQA Testing Submittal Package

Form	Required for Pre-production	Required for Production
1. Software Acceptance Form (SAF) Traveler (112 KB)	X	X
2. Developer Quality Plan	X	X
3. Requirements Specification	X	X
3. Software Executable/Installation package	X (with pre-production splash screen	X (remove pre-production splash screen)
4. User Documentation (e.g., Software Manual)	X	X
5. Software Source Code* (Checked into a GitLab project).	X	X
6. Source Code Build Instructions	X	X
7. Developer response to previous SQA Team report (i.e., Pre-production, "Not Pass" Final)	N/A	X
8. SWS Promotion Checklist (80 KB) **This checklist is only required for SWS submittals**	X	X
9. Nuclear QMP Database Agreement Splash Screen **This splash screen is only required for Nuclear sector SWS that utilize databases**	X	X
10. Mobile (Apple and Google Play) Distribution Checklist (102 KB) **This checklist is required for all mobile submittals**	X	X

* Source-code version must correspond to the submitted build version.

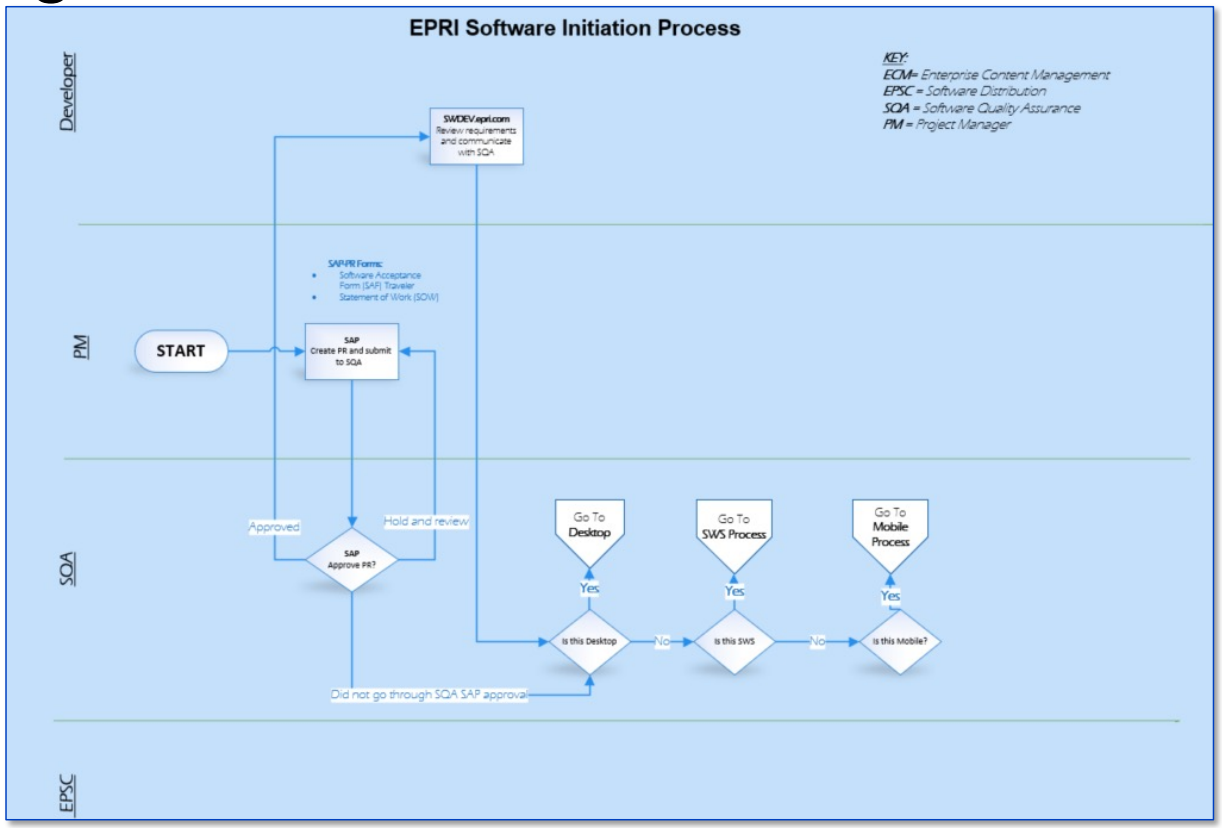
Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | **SQA Process** | Code Signing | Container Registry Scans | Distribution

SQA Process Diagrams

See the Workflow PDF to review the Software PR Initiation Process

From this Process Diagram you will be able to follow the SQA Development process for:

* Desktop
* Subscriber Website (SWS)
* Mobile Apps

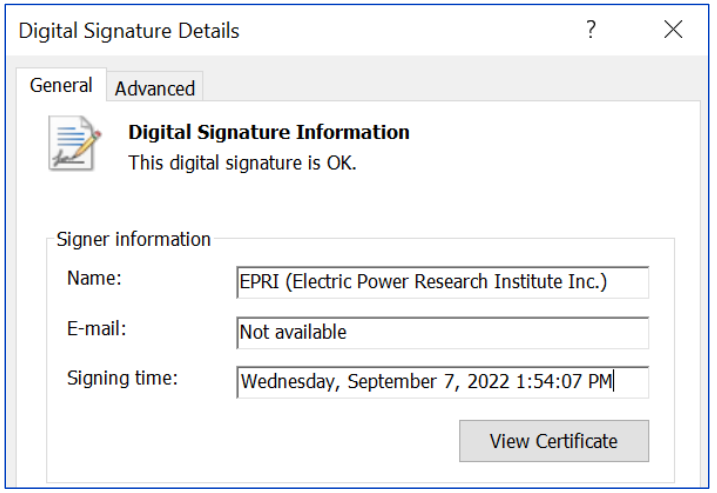


10. Code Signing

Lead Responsibility: **IT/SQA**
Action Items: **IT/SQA** to perform code signing process
IT/Infosec reviews and advise/approve

Desktop Applications: Upon successful SQA Usability Test completion, SQA will digitally sign the **installer .exe** and the **download .exe** if the EPRI Member business case has been approved by the Information Security (InfoSec) team.

- Only **Windows** desktop applications can be signed under the current manual process by SQA.
- **Mac desktop** applications cannot be signed at this time.
- Signing is not necessary for **web applications or APIs** which can be verified by SSL certificates.



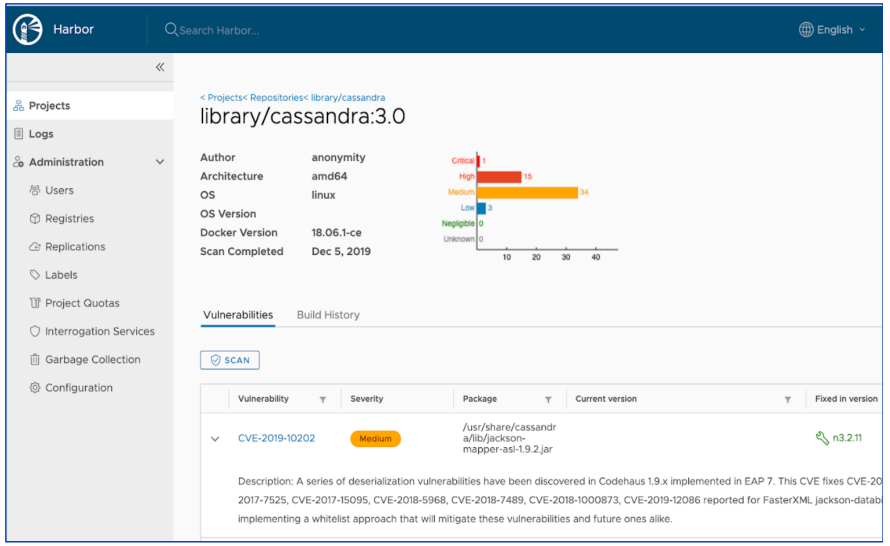
11. Container Registry Scans

Lead Responsibility: **IT/InfoSec**

Action Items: **IT/InfoSec** performs scan
Developer remediates

Container Registry Scans

- A container registry is a repository used to store and access container images. They can support container-based application development as part of DevOps processes, saving developers time in the creation and delivery of cloud-native applications, acting as the intermediary for sharing container images between systems.
- AquaSec will be used as our container registry scanner once the registries are built. Once image scanning is completed, the images are considered registered. Any containers that are to be used in EPRI, must be scanned and properly registered in an approved Container Registry.



Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | **Container Registry Scans** | Distribution

12. Distribution

Lead Responsibility: **IT/SQA**
Action Items: **IT/SQA** initiates distribution process

The Distribution Process is a Secure Transfer practice.

EPRI Approved Member Distribution Channels:

- EPRI.com for Subscriber Websites and web deliverables
- EPRI.com download for Desktop and Spreadsheet deliverables (Pre-Production or Production)
  - If the download file size is too big for download or the member has download issues, alternate solution is to order a physical CD/DVD from the Software Distribution Center (Charlotte office)
- GitHub for EPRI Open-Source deliverables
- Apple iTunes and Google Play for EPRI's mobile apps

Life Cycle | SW Dev | Contractor/ Dev Onboarding | DevOps Environments | Collaboration Tools | SAST Scans | SCA Scans | Container Image Scans | DAST Scans | SQA Process | Code Signing | Container Registry Scans | **Distribution**

Definition of Terms

Definition of Terms

- **Secure Software Development Framework (SSDF)**: EPRI wide approach to handing software development with best practices & tools to scan and verify software during development and after deployment
- **DevSecOps**: Development, Security, and Operations automating integration of security at every phase of the software development lifecycle, from design through integration, testing, deployment, and software delivery
- **Subscriber Website (SWS)**: EPRI web applications, typically developed by EPRI R&D as member deliverables
- **CI/CD**: Continuous Integration & Continuous Deployment
- **Pipeline (DevOps)**: automated processes and tools that allow developers and operations professionals to work cohesively to build and deploy code to a production environment
- **SWDev.epri.com**: EPRI website for software development processes and requirements to promote to production
- **SAST**: Static Application Security Testing - source code scanner providing direct access checking for common security vulnerabilities present in code before builds are completed
- **SCA: Source Composition Analysis**: The examination of a software product to identify the components being used, usually to identify available upgrades for vulnerable components.
- **DAST: Dynamic Application Security Testing**: Live application testing that runs security tests and records findings. Results include live application states to confirm if an application is vulnerable
- **SQA**: Software Quality Assurance team at EPRI, performs software acceptance testing, validation, and promotion to production
- **Container**: container images include system libraries, system tools, and other platform settings —giving developers the benefits of portability and agility to quickly expand or create new apps.
- **Kubernetes**: an open-source container orchestration system for automating software deployment, scaling, and management
- **Code Signing**: a method of putting a digital signature on a program, file, software update or executable, so that its authenticity and integrity can be verified upon installation and execution