Apexon

WHITE PAPER

SOFTWARE SUPPLY CHAIN GOVERNANCE

AN OVERVIEW & CASE STUDY

apexon.com

THE IMPORTANCE OF SOFTWARE SUPPLY CHAIN PIPELINES

Effective software supply chain pipelines are integral to businesses and organizations that depend on new digital products and services.

Whether they are looking to engage with customers in different ways, open new revenue channels, or streamline operations, companies need to be able to deliver these new services quickly and predictably with high levels of user satisfaction.

It's much easier said than done though. Modern software supply chain pipelines have continued to increase in complexity and sophistication as a result of fragmented toolsets, open-source software adoption and zero day vulnerabilities, microservices architectures, hybrid and multi-cloud deployments.

Managing those pipelines involves the thoughtful planning and implementation of a combination of processes, including Continuous Integration, Continuous Delivery, Continuous Deployment, and Continuous Testing. In some cases, this may also require specialized expertise and tools.

But for those organizations that can master these processes, the benefits are significant and include:

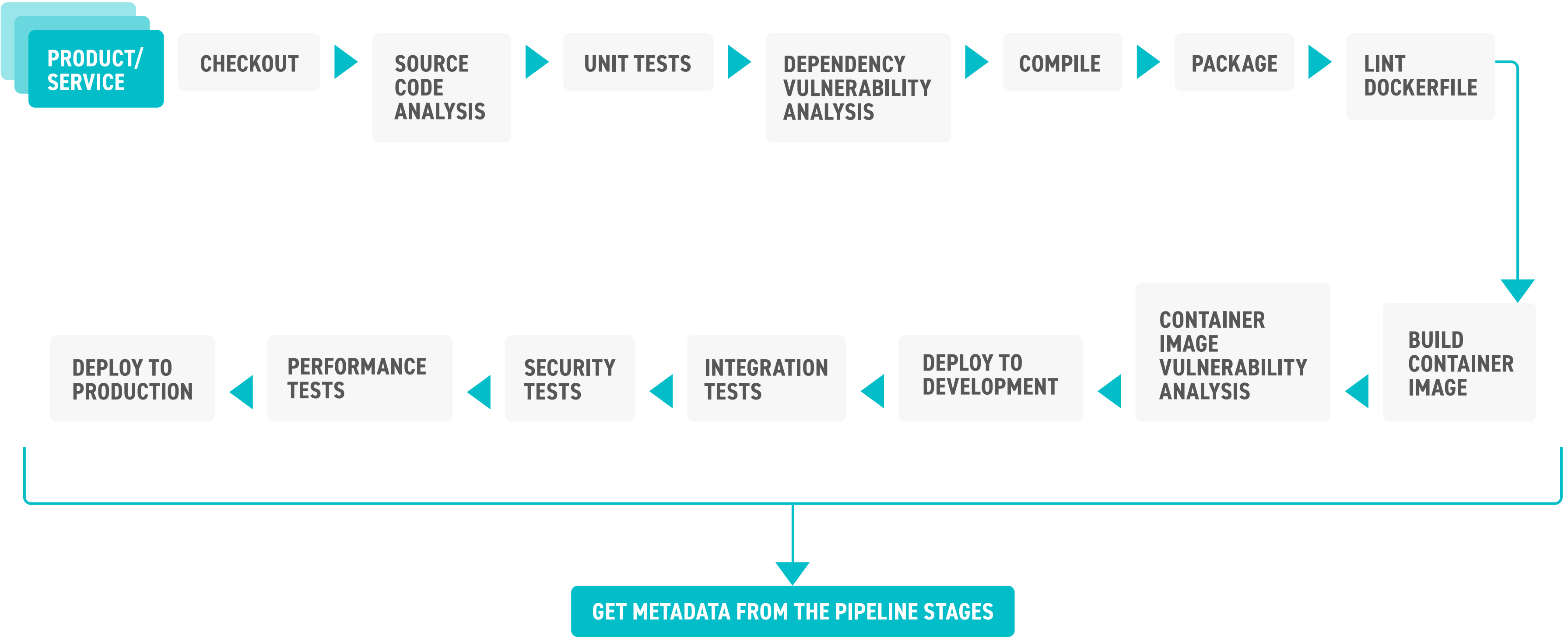
- ACCELERATED INNOVATION
- INCREASED DEPLOYMENT FEATURE FREQUENCY
- FASTER RELEASE CYCLES
- REDUCED CHANGE FAILURE RATES
- BETTER USER QUALITY AND SERVICE
- MORE EFFECTIVE AND EFFICIENT MANAGEMENT
- REDUCED OPERATIONAL COSTS

LEVERAGING THE METADATA IN YOUR SOFTWARE SUPPLY CHAIN

The sophistication of modern software supply chains create a number of opportunities in the form of valuable data that can be gathered from multiple tools such as:

- Source code repository
- Source code analysis
- Unit testing frameworks
- Deployment frameworks
- Integration testing frameworks
- Dependency vulnerability analysis tools
- Performance testing tools

The gathered metadata can be stored in both raw and processed format to further automate, govern, analyze, and audit the produced software package and its deployment. It can transform an organization's software supply chain pipeline from process-driven to data-driven.



(Standard Modern Software Supply Chain Pipeline Flow)

AUTOMATING SOFTWARE SUPPLY CHAIN AUDIT & GOVERNANCE

Different organizations have different compliance, security, and acceptance criteria depending on their business domain and practices.

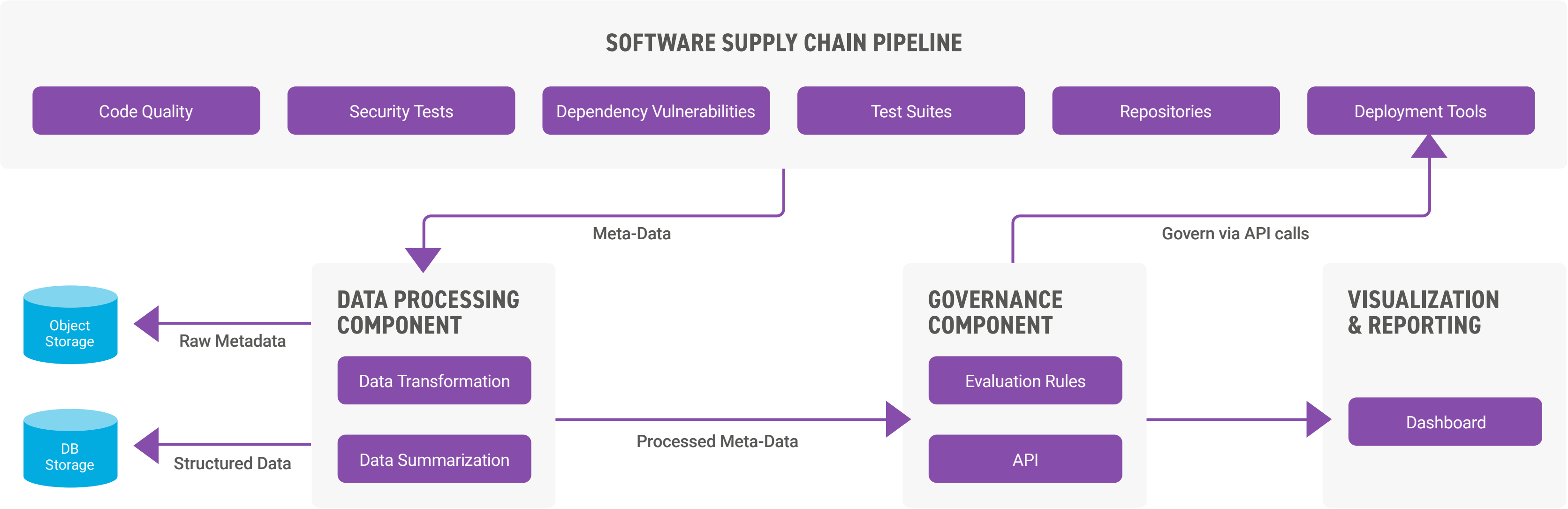
These criteria must be met before promoting new features to production. Performing these tasks manually can be time-consuming and error-prone and impact the overall quality and timeliness of the software features. In many cases, these criteria are based on rigid pass/fail mechanisms which do not accurately portray the quality of a prospective software service.

Instead, leading delivery organizations today can create custom policies which audit the metadata in the software supply chain pipeline and use it to automatically govern, analyze, and deploy new software packages to the production environment. See the case study later in this paper for an example of this more automated approach.

The Impact of Automated Software Supply Chain Governance

The benefits realized by leading delivery organizations able to automate their supply chain governance are substantial including:

- Improved visibility and reporting across fragmented toolsets in the supply chain
- Auditability of open source dependencies and libraries for zero-day vulnerabilities, security, and compliance
- The ability to gather information uniformly across multiple or hybrid clouds for deployments
- Architecture independence and freedom from the Polyglot programming paradigm
- The ability to create and enforce custom policies
- Automated decision making
- Faster cycle time



(Automated Software Supply Chain Governance Data Flow)

A CASE STUDY IN SOFTWARE SUPPLY CHAIN GOVERNANCE

IMPLEMENTING SOFTWARE SUPPLY CHAIN GOVERNANCE

FOR TIER 1 HEALTHCARE COMPANY

THE CHALLENGE

This healthcare organization has built its reputation on patient care and is well known for providing its patients with exceptional experiences and quality outcomes.

This commitment extended to all the ways its patients interacted with the organization, including an increasing number of digital patient services.

Each digital product or service had to meet a strict and long list of acceptance criteria before it could be promoted to a higher level environment. The checklist included more than 50 items which had to be executed and analyzed manually before a software release could be considered ready for production – or meet the definition of done (DoD). This significantly impacted the organization's ability to deliver new features and versions of its software services.

THE APPROACH/SOLUTION

To better understand how to optimize this process, the company's digital team reviewed every single recent release from concept to production.

That analysis revealed a very manual, time-consuming and error-prone DoD adherence process. From there, the decision was made to automate it — with the help of Apexon.

The Apexon team started by helping the company understand how the data from the existing tools could be leveraged to quickly assess whether a software service element met the acceptance criteria.

Working together, we then proceeded to build a solution to push metadata and automate the analysis on that data to check whether it met both pre and post-commit acceptance criteria and govern the deployments accordingly.

For pre-commit quality checks, the client installed a set of tools and hookups that triggered checks every time a developer tried to check in code into the local code repository. The system permitted a commit only if all the quality checks and gates were cleared.

For post-commit quality checks, the CI engine of the client executed a set of scripts and tests that checked after the code has been pushed to the remote repository and updated the status if the artifact cleared all the quality checks and gates.

THE AUTOMATION SOLUTION FOCUSED ON FOUR KEY AREAS:

Pluggability, Extendibility, Flexibility, and Ease of Use

The solution is entirely modular, where each DoD is an independent module that can be plugged and played. This makes it flexible enough to allow additional quality gates to be added quickly.

A Pre-Commit Framework allowing Code Commits Only if all Quality Checks/ Gates are Cleared

Apexon provided a framework with Git hooks that acts as a quality gate where the code is flagged and held if it does not meet the DoD. The DOD items are verified at the time of commit to make sure there is no hard coding of API Keys and to validate the Schema of the OpenAPI specification stored in the code.

A Post-Commit Framework that Executes a Set of Scripts and Tests that Check and Update Status if the Software Package Has Cleared All of the Quality Checks and Gates

Apexon provided a Framework within its Jenkins pipeline which provided an automated way to:

Simulate error paths and automatically validate the corresponding exception/error codes and generated application logs.

Run APIs and inspect the headers to match the swagger file.

Inspect if there are unauthenticated POST calls upon commit.OpenAPI specification stored in the code.

A Pluggable User-Friendly UI to Check DoD/Quality Status

A DoD dashboard to view the evaluation status of all the DoD’s and quality gates analyzed.

The dashboard enables a simple click on the DOD item to display Passed/Failed and other relevant information.

THE OUTCOME

Overall, the supply chain governance solution helped the organization increase the feature deployment frequency, decrease cycle time, and decrease resource utilization for manual tasks.

The initial POC implementation proved that the automated framework helps reduce the cost and time required for the DOD adherence while improving quality.

It also advanced the client's cause of delivering an exceptional patient care experience.

Approximate savings of:

~ $800,000 a year in cost

48 hours in manual effort

Apexon

APEXON IS A PURE-PLAY DIGITAL ENGINEERING SERVICES FIRM FOCUSED ON HELPING COMPANIES ACCELERATE THEIR DIGITAL INITIATIVES FROM STRATEGY AND PLANNING THROUGH EXECUTION.

We leverage deep technical expertise, Agile methodologies and data-driven intelligence to modernize systems of engagement and simplify human/tech interaction.

We deliver custom solutions that meet customers’ technology needs wherever they are in their digital lifecycle. Backed by Goldman Sachs and Everstone Capital, Apexon works with both large enterprises and emerging innovators — putting digital to work to enable new products and business models, engage with customers in new ways, and create sustainable competitive differentiation.

✉ info@apexon.com 🌐 www.apexon.com

FEELING SOCIAL?