ACL Digital
an ALTEN group company

Continuous Integration, Continuous Delivery (CI/CD)

Industry best practices for securing continuous integration and continuous delivery (CI/CD) pipelines

Phase 03 of Software Lifecycle Management

Digital Product Engineering Services

Table of contents

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

Introduction

Gartner predicts that through 2024, 90% of organizations using iterative approaches to DevOps will optimize customer value relative to cost and risk.

DevOps is a customer value driven approach to delivery solutions using agile methods, collaboration, and automation. Without a clear focus and the right resources, DevOps initiatives will lose customer support, fail to scale, and deliver limited customer value.

The continuous integration, continuous delivery (CI/CD) pipeline forms an integral part of the DevOps cycle and the overall Software Lifecycle Management process. The compliance index for an application's security and privacy aspects must mature over time to matchup with the industry compliance levels. There could be a need to comply with additional cybersecurity and privacy regulations depending upon the type of software being produced. The following guidelines might help improve your application's cybersecurity and data privacy compliance index.

Apart from more organized team collaboration, quick turn-around-time (TAT) for issue repairs and requirement change management, DevOps has become a gamechanger for quicker delivery cycles of software applications and offers increased efficiency via automated workflows on the CI/CD pipelines.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

Securing Development and Operations

In the Gartner's Emerging Technology Roadmap for Large Enterprises report, few significant emerging technologies for cybersecurity are Dynamic Application Security Testing (DAST), Security Orchestration, Automation and Response (SOAR), Extended Detection and Response (XDR) and Cloud Access Security Broker (CASB) that completed deployment by 2021; network cybersecurity offering Zero Trust Network (ZTN), Endpoint Protection Platform (EPP), Cloud Workload Protection Platform(CWPP) and Secure Access Service Edge (SASE) will complete deployment in 2022.

1 Setup the desktop-based or browser-based integrated development environment (IDE) in a way that it facilitates secure continuous integration and continuous delivery cycles.

- **1.1** Setup interactive application security testing (IAST), Static application security testing (SAST), Dynamic application security testing (DAST) and Mobile application security testing (MAST) platforms and integrate with delivery pipelines.
- **1.2** Setup Open-Source Software (OSS) scanning tools and integrate with delivery pipelines
- **1.3** Utilize secure code versioning toolchains

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

1.4 Introduce multifactor authentication (MFA), privileged access management (PAM) for securing code management and protecting from unauthorized users.

1.5 Store API secrets and configuration parameters in key vaults and access using customer keys.

1.6 Introduce application and code signing before deployment.

1.7 Utilize mobile application management (MAM) or mobile device management (MDM) toolchains for secure mobile application release management. Use **develop once, deploy multiple** principles to reduce deployment related security risks.

1.8 Utilize pre-hardened containers for secure deployment of web applications.

1.9 Maintain a data dictionary of personally identifiable information (PII) and mask all occurrences of PII data across debug, information and audit logs.

1.10 Introduce pseudonymization and unique alpha-numeric Ids for referencing human entities containing PII data.

1.11 Introduce adequate documentation to code describing the intent, return types, parameters, and exception paths.

1.12 Introduce adequate unit testing for testing the privacy and security sensitive units of the application.

1.13 Measure code coverage using tools and improve it over multiple iterations of the software development lifecycle.

1.14 Fail builds if software bill of materials (SBOMs) is missing or cannot be verified.

1.15 Use SBOM data to surface security vulnerabilities, compliance policy violations and indicator of compromise during the build process.

1.16 Fail deployments if SBOM signature cannot be verified and if hashes of components don't match up.

1.17 Secure software supply chain from emerging threats and risks

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

2 If **Low-code/no-code application development platform (LCAP)** is used, it must be ensured that the LCAP provides security assurance against vulnerabilities.

- **2.1** It should provide evidence that development of its own platform follows secure application development practices.
- **2.2** Perform application security testing (AST) on the applications that are developed using the LCAP.
- **2.3** Implement secure access and governance for the development environment using multifactor authentication (MFA) or integration with privileged access management (PAM).
- **2.4** Assess the libraries for vulnerabilities, that the LCAP uses.
- **2.5** Use the LCAP to standardize secure components, reduce introduction of vulnerabilities during development and enhance security protection.
- **2.6** Follow the OWASP top 10 for low-code / no-code security risks.

3 **Digital Platform Conductor (DPC)** tools:

- **3.1** These tools are on the rise and coordinate infrastructure tools used for planning, implementing, operating, and monitoring underpinning technology and services for applications and digital products.
- **3.2** Setup a DPC tooling strategy by working with key stakeholders to identify infrastructure value, cost benefit objectives, and making selective investments in integration, resolving organization dependencies and continuous innovation capabilities.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

4 **Cloud security posture management tools (CSPM)** for securing the IaaS and PaaS workloads.

4.1 Organizations must invest in CSPM tools to protect serverless and container-based workloads from security threats and vulnerabilities.

4.2 Create protected environments and integrate intelligent security assessment tools along with delivery pipelines (e.g. infrastructure-as-code (IaC) scanning) to identify risks early in the development lifecycle and alert unsafe workload before being deployed.

4.3 Deploy lightweight CSPM technologies that offer read-only, least-privilege automation for generating workloads for agentless techniques such as API integration and log monitoring.

4.4 CSPM tools are driving the evolution of cloud workload protection platform (CWPP) towards cloud native application protection platform (CNAPP). Need to transition from securing infrastructure on the cloud to securing applications on the cloud.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

5 **Citizen automation and development platform (CADP):** The citizen automation and development platforms have emerged as a new class of solutions that specifically target the needs of citizen technologists.

5.1 They are represented by the convergence of rapid mobile app development (RMAD) platforms together with peripheral technologies such as low-code / no-code application platforms (LCAP), integration platform as a service (iPaaS), robotic process automation (RPA), intelligent business process management suites (iBPMS), Multiexperience development platform (MXDP), and collaborative work management (CWM). In most cases, there are overlaps between these categories.

5.2 The CADP enables business technologists, particularly the citizen developer, automator and integrator personas to contribute to application capabilities without any direct IT involvement.

5.3 The CADP greatly improves employee engagement as more business technologists come forward to construct their own solutions.

5.4 CADP encourages autonomy within business units and reduces dependency on IT so that they can focus on more strategic organization topics. It can also help fill out huge vacancies for business focused roles in IT.

5.5 CADP must have the ability to run or connect to on-premises systems and support regulatory compliance in the cloud.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

6 **Securing and shielding software supply chain** security risks

6.1 Protect the integrity of source code

6.1.1 Provide strong version control policies, trusted component registries, and third-party risk management

6.1.2 Enforce signed commits, multifactor authentication, zero-trust access based on user and device context, prevent forced pushes, mandate code-reviews, and scan for secrets and block sensitive data.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

6.2 Harden the delivery pipeline

6.2.1 Configure security controls in CI/CD tools and frameworks: Reproducible build practices ensure consistency and uniformity of build output, and signed pipelines create immutable, and verifiable artifacts.

6.2.2 Implement secrets management: Use a secrets management tool to create, rotate and revoke credentials, private keys, passwords, API tokens, etc.

6.2.3 Implement signing and hashing code and container images: Signing addresses the needs for provenance and authenticity, hashing ensures image integrity.

6.3 Secure operating environment

6.3.1 **Principles of least privilege access policies and methods:** Role-based authentication and authorization, adaptive access using zero-trust security model and privilege access management can help block unauthorized connections to critical systems.

6.3.2 **Zero-trust security model:** This provides controlled identity and context-aware access to development resources, reducing the surface area for supply chain attacks, and eliminates excessive implicit trust placed on machines and services simply because they share the same network, replacing it with explicit identity-based trust.

6.3.3 **Machine Identity Management:** The adoption of machine identities has increased due to distributed application architectures, cloud-native infrastructures, and API-as-products. Hosts, containers, virtual machines, database servers, sensor networks, services and API endpoints all use distinct machine identities. Machine identity management is a collection of practices and tools that enhances trust and integrity of machine-to-machine interactions, which is critical to securing development environments.

6.3.4 **Anomaly detection and automated response:** Anomaly detection and response tools must be setup to understand and define the expected behavior of their development platforms so that anomalies can be detected in real-time. This is especially critical in container-native, DevOps deployments that automate complete code-to-container workflows.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

Conclusion

In the wake of increasing adoption of cloud-native application deployments, containerization, and software supply chains, it is indispensable for organizations to take cognizance of the emerging threats and vulnerability attacks on the entire software development and delivery pipeline. It is not sufficient to only protect the delivery channels, but also take due measures to ensure complete protection of all sensitive and vulnerable resources together with granular implementation of security controls, access controls, secrets management and introduce onion-skin architecture for enforcing security mechanisms on the overall continuous integration, continuous delivery (CI/CD) cycle.

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.

Recommended Reading

Software Lifecycle Management Infographic

Phase-01: Requirement Lifecycle Management

Phase-02: Secure Architecture and Solution Design

References

- [1]Gartner report: 2021-2023 Emerging Technology Roadmap for Large Enterprises
- [2]OWASP Top 10 Low-code/no-code security risks

ACL Digital is a design-led Digital Experience, Product Innovation, Engineering and Enterprise IT offerings leader. From strategy, to design, implementation and management we help accelerate innovation and transform businesses. ACL Digital is a part of ALTEN group, a leader in technology consulting and engineering services.

business@acldigital.com | www.acldigital.com

USA | UK | France | India

Proprietary content. No content of this document can be reproduced without the prior written agreement of ACL Digital.
All other company and product names may be trademarks of the respective companies with which they are associated.