cenareo

Cyber Security - Change and Release Management

This policy outlines the formal procedures for Change and Release Management within Cenareo.

It ensures secure and controlled development, testing, deployment, and management of changes to our software applications, systems, and infrastructure.

This policy is subject to periodic review and updates to reflect changes in technology, industry best practices, and regulatory requirements.

Software Development Lifecycle (SDLC) Standard

Cenareo maintains a documented Software Development Lifecycle (SDLC) standard. This standard defines a structured approach for developing, testing, deploying, and maintaining software applications. The SDLC incorporates security best practices throughout all phases of development.

Change Control Process

A formal Configuration Management (CM) process governs all changes to hardware, software, and firmware across physical and virtual platforms. This process includes:

- **Change Request**: All proposed changes must be submitted through a formal change request process. The request will detail the nature of the change, its purpose, and potential impact.
- **Impact Assessment**: The Information Security team will assess the security implications of the proposed change.
- **Approval Process**: Changes will be reviewed and approved by a designated Change Approval Board (CAB) based on a risk assessment and alignment with business objectives.
- **Implementation and Verification**: Approved changes will be implemented following the documented procedures and tested thoroughly to ensure functionality and security.
- **Documentation and Version Control**: All changes will be documented and tracked within a version control system.

Baseline Configuration Management

We maintain documented baseline configurations for all critical systems and applications. These baselines define the authorized and secure state of the system, incorporating security best practices and industry standards. Any deviation from the baseline configuration requires justification and approval through the change control process.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

cenareo

Secure Coding Practices

We are committed to secure coding practices.

This includes:

- **Static Application Security Testing (SAST)**: We utilize automated SAST tools to identify potential security vulnerabilities in source code during development.
- **Code Review**: In addition to automated tools, we also employ manual code reviews by qualified personnel to detect security defects and promote secure coding practices within development teams.

Release Management

Releases of new applications and updates are controlled through the following release management process.

This process ensures proper testing, packaging, deployment, and rollback procedures are followed to minimize disruption and maintain system stability.

Release Planning

- **Initiation**: The product or development team submits a formal release request outlining the features, functionalities, and target release date.
- **Requirements Review**: The Information Security team reviews the request to assess security implications and ensure alignment with security policies and standards.

Release Planning Meeting

A cross-functional team, including development, testing, operations, and security personnel, participates in a release planning meeting to define:

- Release scope and features.
- Development timeline and milestones.
- Testing strategy and criteria.
- Deployment plan and rollback procedures.
- Communication plan for stakeholders.

Release Prioritization

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

Critical security updates or features with high business impact may be fast-tracked through the process, while lower-risk releases follow a standard timeline.

We prioritize considering the following factors:

- Security severity of addressed vulnerabilities.
- Business impact of the new features or updates.
- Dependencies on other releases.

Development and Testing

- **Development**: Development teams create new features or updates based on the approved release plan.
- **Security Testing**:
  - Static Application Security Testing (SAST): Automated SAST tools are used throughout development to identify potential security vulnerabilities in the code.
  - Dynamic Application Security Testing (DAST): As development progresses, DAST tools are employed to simulate real-world attacks and identify vulnerabilities in the functionality.
- **Unit Testing**: Developers conduct unit testing to ensure individual code modules function as intended.
- Integration Testing: Integration testing verifies the functionality of different modules working together.
- **System Testing**: System testing evaluates the overall functionality and performance of the release in a simulated production environment.
- **User Acceptance Testing (UAT)**: If applicable, UAT involves end-users testing the release to ensure it meets their needs and expectations.
- **Security Review**: The Information Security team performs a final security review of the release candidate, addressing any identified vulnerabilities before deployment.

Release Preparation

- **Release Build**: A final release build is created, incorporating all approved features and bug fixes.
- **Documentation and Release Notes**: Comprehensive documentation and release notes are prepared, detailing new features, functionalities, known issues, and upgrade instructions.
- **Pre-Deployment Review**: A final review is conducted by the cross-functional release team to ensure all criteria are met for deployment.

Deployment

- **Deployment Window**: Releases are deployed during pre-defined deployment windows to minimize disruption to production systems.
- **Deployment Strategy**: A phased deployment approach may be used, rolling out the release to a limited environment for testing before full production deployment.
- **Rollback Plan**: A rollback plan is in place in case of unforeseen issues after deployment.

Post-Deployment

- **Monitoring and Support**: The released version is monitored for functionality and performance. Support channels are available for users encountering issues.
- **Post-Deployment Review**: A post-deployment review is conducted to assess the success of the release, identify lessons learned, and improve future release processes.

Communication and Training

The Information Security team provides ongoing communication and training to developers, system administrators, and other relevant personnel on secure coding practices, change control procedures, and the importance of secure software development.

Monitoring and Improvement

The Change and Release Management processes will be regularly monitored and reviewed for effectiveness. We continuously strive to improve these processes based on lessons learned and industry best practices.