Cloud Software Group Secure Development Lifecycle

Content

1. Introduction

Cloud Software Group Product Security team is responsible for the security of all the Cloud Software Group products and services. This team works with the Product Engineering teams to implement the Secure Development Lifecycle (SDL) process that incorporates security throughout the lifecycle of all Cloud Software Group products and services. Secure Development Lifecycle (SDL) extends its scope to govern and manage the specific security and ethical risks associated with the design, development, and deployment of Artificial Intelligence (AI) systems and components.This document shall also serve as the Cloud Software Group Artificial Intelligence Management System (AIMS) documentation, with the AIMS scope covering all products and services that incorporate, utilize, or distribute AI systems.

This document provides an overview of the security processes for Cloud Software Group products and services. *This information is provided "AS-IS" without warranties of any kind (express or implied) and is subject to change at Cloud Software Group's discretion.*

2. Security Training

Underpinning the SDL process is Secure Development training. We have instituted a continual, level-based security training program for all engineers. This training covers various security elements including threat modeling, secure design principles, secure coding practices, and new modules on AI ethics and bias mitigation. Training includes mandatory AIMS awareness for all personnel and specialized training to ensure competence in AI-related security controls. As part of the training program, engineers are required to annually revalidate their security awareness knowledge.

3. Planning and Requirements Gathering

Cloud Software Group has adopted Scaled Agile Framework for Enterprise (SAFe) to drive product development. For each development iteration, the Product Security team engages with engineering teams during the planning stage to evaluate the security risks and ensure the documentation of :

- System Definition: Intended use, target users, and known technical/operational limitations.
- AI Impact Assessment (AIIA): A formal identification and treatment of AI-related risks and opportunities in line with AIMS objectives.

This documentation ensures the system is not deployed in contexts where its accuracy or bias profiles could lead to unacceptable risks.

4. Threat Modeling

Threat modeling activities are designed to address security design concerns at the initial stage of the development lifecycle. New features, services, and interactions between existing services undergo a threat modeling activity where the product security and engineering teams work together to identify the relevant assets, attack surface, potential threats and corresponding threat vectors, including AI-specific threats like adversarial attacks and data poisoning, prompt injection, and model inversion/extraction.

5. Code Review

A. Manual Code Review

New features go through a code review for any security-sensitive changes, including but not limited to: multi-tenancy flow, memory management, Role-based access control (RBAC), cryptographic code, and authentication/authorization.While performing manual code reviews, the Product Security team focuses on identifying vulnerabilities that might otherwise be missed by Static Application Security Testing (SAST) tools, with a dedicated focus on auditing the security and ethical compliance of AI model logic and data handling components. These activities serve as a key operational control of the AIMS to verify the secure implementation of AI components.

B. Assisted Code Review

Beyond the manual code review, Cloud Software Group uses various industry standard SAST tools that are integrated into the pipeline to scan the source code, identify and mitigate any potential vulnerabilities

6. Supply Chain Security

A. Third Party Dependency Tracking

Cloud Software Group uses industry standard tools to perform Software Composition Analysis (SCA). These tools are integrated into build pipelines to track third-party components, vulnerabilities, and licensing policies. For AI-enabled products, this scope is extended to include the maintenance of an AI Software Bill of Materials (AI-SBOM), which mandates the tracking and verification of all third-party AI models, pre-trained weights, and external training datasets. Supply chain verification includes validating the provenance, licensing, and security integrity (e.g., cryptographic hash verification) of pre-trained models and third-party datasets to ensure legal compliance and mitigate risks associated with 'black-box' dependencies.

B. Data Quality and Lineage

For all AI systems, the Product Security and Engineering teams must ensure the integrity and quality of training, validation, and testing datasets. This includes:

- Data Lineage: Maintaining records of where data originated and how it was processed.
- Privacy: Implementing data minimization and de-identification techniques (e.g., PII masking) before data enters the training pipeline.
- Bias Review: Evaluating datasets for historical biases that could be codified by the model.

7. Security Testing

The Product Security team performs manual and automated security testing in line with industry best practices for security validation, including dedicated testing for AI model robustness, fairness, and performance monitoring to detect model drift. The results of this testing are used to measure AIMS performance and effectiveness.

Product teams are encouraged to maintain 'Model Cards' or equivalent documentation that describes the AI model's performance metrics, training data characteristics, and intended use-cases to provide transparency for internal and external stakeholders.

8. Third Party Penetration Testing

A. External penetration testing

Along with above internal activities, we commission yearly external security assessments and penetration testing engagements by reputable external firms across our product and service portfolio.

B. Bug Bounty Program

Cloud Software Group has a public bug bounty program on HackerOne that provides a pathway for researchers to submit findings in a number of Citrix and NetScaler managed services. We believe the researcher community to be an extension of the security functions performed within the organization and look to engage with the community through regular outreach.

9. Product Security Vulnerability and Incident Response Program

The Product Security function follows industry wide standards for the vulnerability and incident response process to investigate and respond to vulnerabilities that are discovered by external parties

10. Product Security Incident Response (PSIRT)

A. Vulnerability Response

Cloud Software Group takes a comprehensive approach to investigating, addressing and informing customers of known product vulnerabilities. Cloud Software Group also offers multiple avenues to report product vulnerabilities including a continuously monitored, dedicated inbox, and through our active Bug Bounty program.

A customer or security researcher may report a vulnerability through the Trust Center and Report a Security vulnerability. The Vulnerability Response section of the Trust Center includes additional details on the program.

Cloud Software Group publishes security advisories to provide remediation information about security vulnerabilities in customer-managed Cloud Software Group products which have been reported to us through the vulnerability response program.

Further details related to our response process and our approach to vulnerability disclosures can be found on our Trust Center Response Process page.

Cloud Software Group looks to the issues reported or identified through these avenues as feedback to further improve upon the features and components within Cloud Software Group products and services. With this added insight, we can prioritize these components and features for retrospective SDL reviews with a view to use this as an opportunity to identify and implement fixes for the security vulnerabilities.

11. Performance Evaluation & AI System Monitoring

- Monitoring and Measurement: Performance of all AI systems and their associated controls are continuously monitored for robustness, fairness, and detect model drift as defined in Section 7. This process includes defined Human-in-the-Loop (HITL) triggers, where automated decisions with low confidence scores or high-impact outcomes are routed for human review before final execution.
- Internal Audit: The AIMS shall be subject to periodic internal audits to determine its conformance to the planned arrangements and the requirements of the standard.

12. Revision History

The Cloud Software Group Security Program management team is responsible for maintaining and updating this policy document as needed to ensure the guidance and standards presented reflect the current control environment to support and align with management's overall objectives.

Revision History

Version	Revision Date	Author	Comments/Notes
1.0	1 March 2023	Andy Nallappan, CISO Mohan Sekar, Sr. Director Product Security	New SDLC Product Security
2.0	Feb 2025	Mohan Sekar, Sr. Director Product Security	FY2025 Policy Refresh
3.0	24 June, 2026	Mohan Sekar, Sr. Director Product Security	Annual Review

Approval History

Version	Revision Date	Author	Comments/Notes
1.0	1 March 2023	Andy Nallappan, CISO Mohan Sekar, Sr. Director Product Security	New SDLC Product Security
2.0	Feb 2025	Kumar Palaniappan - CISO Mohan Sekar, Sr. Director Product Security	FY2025 Policy Refresh
3.0	25 June, 2026	Kumar Palaniappan - CISO	Reviewed the proposed changes and approved