Adobe® Secure Engineering Overview

Introduction

Adobe has invested significant human and financial resources in creating security processes and practices that adhere to industry standards for product and service engineering. Because we take the security of your digital experience seriously, we have ingrained security practices into our internal software development and operations processes. We rely on a combination of training, guidance of experts, and automation of as many processes as possible to enhance security and help reduce human error. Adobe believes in a layered approach to security, using multiple tools and steps to help ensure products are hardened accordingly. Our cross-functional teams follow these steps to help prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities. We also regularly incorporate new security practices into the products and services we offer.

This white paper describes the evolution of Adobe's strategy and philosophy around security practices during product and service engineering.

Table of Contents

The Adobe Secure Product Lifecycle (SPLC)

A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC was designed from the ground up to help keep your information safe and secure when you use Adobe products and services and is integrated into multiple stages of the product lifecycle. Adobe's SPLC must meet the standard of due care that is reasonably expected by customers, shareholders, partners, Adobe workers, and the business itself within the product lifecycle. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape. One example of this evolution is how Adobe has adapted the SPLC to work in concert with agile development practices.

Adobe SPLC controls include, depending on the specific Adobe product or service, some or all of the following recommended practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture reviews and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Readiness reviews, response plans, and release of developer education materials

All security efforts, including product and service security initiatives, as well as the implementation of the Adobe SPLC, are coordinated by the office of the Chief Security Officer (CSO). The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams. ASSET researchers work with individual Adobe product and operations teams to achieve the right level of security for each product and service based on an assessment of potential security risk. ASSET team members also advise product development teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

History of the Adobe SPLC

In use now for more than a decade, the Adobe SPLC was modeled on Microsoft's Security Development Lifecycle, or SDL. Service roadmaps, security tools, and testing methods included in the Adobe SPLC help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors. Other frameworks, such as those from SAFECode (the Software Assurance Forum for Excellence in Code), a global, non-profit organization focused on identifying and promoting practices for developing and delivering more safe and reliable software, hardware, and services, the Cloud Security Alliance (CSA), and the Center for Internet Security (CIS) also greatly influence the Adobe SPLC.

Initially, the Adobe SPLC addressed the security controls needed for Adobe products on desktop systems, the primary method of software delivery when the SPLC was conceived. As mobile and cloud computing became ubiquitous, Adobe evolved the SPLC to include those platform requirements. By maintaining a baseline of SPLC controls and extending these with mobile-, cloud-, and desktop-specific controls, Adobe's modular approach to secure engineering enables the Adobe SPLC to keep up with the changing requirements of new and emerging environments.

Figure 1: The Modular Approach to the Adobe Secure Product Lifecycle

The Adobe SPLC Today

Today, the baseline Adobe SPLC includes eight distinct steps, to which Adobe products and services must adhere:

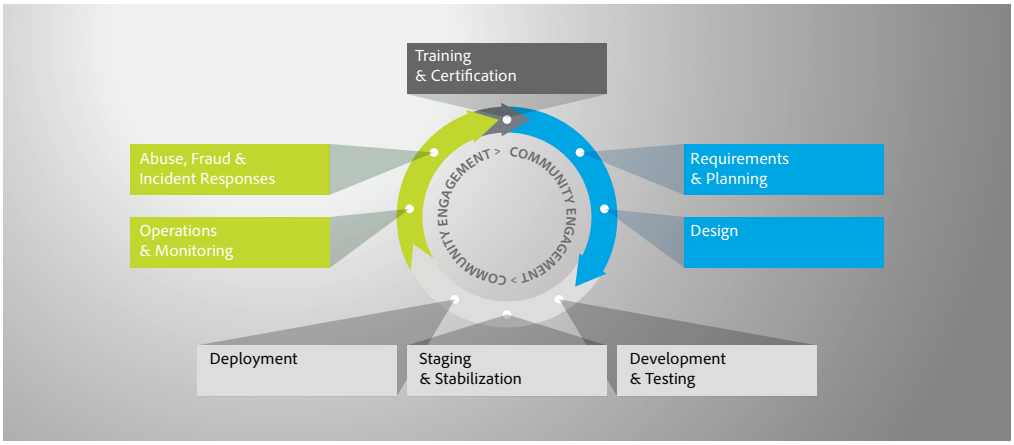

Figure 2: The Adobe Secure Product Lifecycle (SPLC) Process

Training and Certification—Focuses on training and certifying internal product teams on the SPLC process and keeps teams informed of the latest threats and approaches to software security. Also includes training for non-engineering roles in security best practices and general security hygiene.

Requirements and Planning—Provides an overall health and risk assessment of a product or service and facilitates any necessary adjustments based on the current threat landscape.

Design—Builds defenses against potential threats directly into the initial design of new products and services, as well as new features within existing products and services, and offers an opportunity to improve the security profile of existing features.

Development and Testing—Embeds security practices during the development of Adobe products and services to help avoid coding issues and subjects code to rigorous internal and third-party tests using industry standard testing frameworks and automated scanning tools.

Staging and Stabilization—Helps ensure that the Adobe product or service is customer-ready and verifies code robustness, scalability, and resistance to attack in a simulated production environment.

Deployment—Helps minimize risk of improper deployment through adherence to strict code-handling processes and restricted access.

Operations and Monitoring—Monitors and logs traffic to help ensure maximum server availability and server health.

Abuse, Fraud, and Incident Response—Helps ensure teams can respond quickly when incidents occur and guides interaction with proactive security experts in the Adobe Security Coordination Center (SCC) to more quickly and efficiently mitigate and resolve issues.

Implementing the Adobe SPLC in Product Development

As mentioned above, the office of the CSO drives the consistent implementation of the Adobe SPLC into each major product and service development team. Through the programs and models described in this section, the CSO helps ensure implementation accuracy, efficacy, efficiency, and consistency across the company.

Training, Certification, & Reporting

All full-time, regular Adobe employees complete security and privacy awareness training. This training includes information about safe handling of confidential information, safeguarding devices, using password protections effectively, and recognizing and avoiding social engineering. Employees also regularly participate in internal security and privacy awareness seminars and other activities to increase awareness of how security affects their specific roles within the organization and the company as a whole.

Each major Adobe product organization also includes embedded security champions who assist the centralized ASSET team in scaling security efforts across the company, disseminating critical security information to and driving the completion of security tasks within their product or service teams.

Depending on their specific job function and role, Adobe engineering employees choose from one of four (4) levels of certification, also called 'belts'. Employees earn a different colored 'belt' after completion of each level's specific number of required hours of training, which is based on the employee's job function or role with Adobe. While the two lower levels of certification only require online training sessions in basic security concepts, the two higher certification levels include hands-on, experiential projects that may directly relate to or impact the employee's job responsibilities. Employees must re-certify at their role-specific level on an annual basis. More information about all of our security training programs can be found on our website.

To further encourage engineering and technical personnel to sharpen their security awareness and vulnerability identification skills, Adobe holds regular security trainings in the form of a game that mimics the classic "Capture the Flag." This type of exercise is often used for security champion training, helping these employees to think like the adversary and stay one step ahead of malicious attacks. In addition, engineers can also participate in Capture the Flag exercises at Adobe's regular engineering education conference, called TechSummit.

Adobe also implements industry-standard benchmarks and reporting dashboards to constantly measure and convey progress in a variety of key areas. The security backlog has C-level and board-level visibility, helping keep executive staff and the board of directors updated on the security posture of Adobe's products and services on a regular basis. Among other things, the reporting dashboards help ensure that product teams make ongoing, measurable progress against security backlogs, complete training on an annual basis, update third-party libraries, and complete requested security testing and threat modeling.

Requirements and Planning

The office of the CSO kicks off product or service development engagement with many relevant security stakeholders, including compliance, privacy, and legal, in addition to application, operational security, and IT security. Adobe calls this the Unified Security Engagement (USE) model.

The USE model enables product teams to efficiently engage with multiple security and compliance teams and formally onboard the security process. Designed to help identify security-sensitive areas and practices, as well as streamline the engagement process, USE pulls in different security teams across Adobe based on the product or service's specific needs. Then, using an online onboarding tool to communicate review requests and various details about the product or service, the teams can decide on and schedule the appropriate security reviews.

The security review process includes a security risk assessment (SRA). The risk assessment is used to determine:

- Which portions of the project will require threat models before release?
- Which portions of the project will require security design reviews before release?
- Which portions of the project (if any) will require penetration testing by a mutually agreed upon group that is external to the project team?
- Are there any additional testing or analysis requirements the security advisor deems necessary to mitigate security risks?
- What is the specific scope of the fuzz testing requirements?

If the product or service development team plans on using third-party code in the service development, Adobe uses an internally developed assessment program to help ensure the security posture of the source. Adobe is also a member of the Vendor Security Alliance (VSA), an independent organization that helps ensure our third-party vendor assessment process meets industry standards.

Design

Because security is integrated into the planning and requirements phase of product development, by the time the product or service enters the design phase, product features should already conform to Adobe's initial security criteria. To help identify potential security flaws early in the development lifecycle and create a strong security foundation for the product or service, Adobe conducts extensive threat modeling in order to identify areas in which architectural changes may be required in order to avoid known threats. In this phase, the team also reviews security items including:

- Checking for the proper handling of passwords and authentication credentials
- Checking for effective use of content security policies (i.e., security headers)
- Checking for mistakes such as hard-coded secrets

This helps lessen the work required for correction after threat modeling. Adobe also makes use of container technology and tools that produce "clean images" to help meet as many security requirements as possible by default to keep developers focused on their code and lessen the chance of the introduction of security flaws.

Data classification efforts validate that teams adhere to Adobe data classification standards, which are designed to manage information handling risk across the company. Additionally, Adobe rigorously tests that the product or service design meets our cloud operational security baseline to help ensure secure service usage in the cloud. When appropriate, Adobe engages outside security consultants for architectural security reviews.

Development and Testing

One of our primary goals in ensuring more secure software development is to reduce possible attack surface as much as possible. Adobe uses automated tools for both static and dynamic code analysis, including an internally developed tool that helps automate security compliance and acts as a repository for storing the list of third-party libraries used in Adobe products. Adobe closely monitors the usage of third-party components in its products and services and regularly reviews the security posture of these components. The tool regularly synchronizes with vulnerability reporting systems to identify less secure libraries that require updating, helping to reduce the security risk from using third-party software. In addition to automated tools, Adobe also conducts manual source code reviews, as needed, to flag potential issues.

Tests against our software are carefully scoped in detail to ensure they are targeted and as complete as possible. The most common testing method we employ is penetration testing ("pen testing"). We leverage both an internal team as well as professional third party security reseachers to conduct design reviews and application, product, and network security testing. These tests evaluate Adobe products against industry standard practices. We perform these "gray box" tests using a combination of automated and manual techniques. Third party testers work closely with product teams to gain insight into product architecture and functionality.

We help ensure pen tests are effective by not only identifying individual risks, but by making strategic recommendations on changes which can reduce the attack surface and make the product more secure. Applications receive a form of peer review by being tested by different security teams on a regular basis. We also expect that our testers understand our applications intimately to help ensure the most actionable results. Findings from tests are ticketed and assigned and injected directly into our vulnerability management program for timely resolution. When an important risk is identified during a pen test, Adobe engineering teams must resolve the issue according to fixed timelines. Once the issue is resolved, we re-run the pen tests to ensure findings have been effectively remediated.

In addition to pen testing, we also maintain both external and internal bug bounty programs. Our external crowdsourced, time-bound pen testing activities leverage the creativity of many participants to test our security measures. These programs have included many participants actively testing Adobe services. Our internal bug bounties leverage the security talent within the company to help find issues. This program also helps us promote application security awareness throughout our engineering teams.

Staging and Stabilization

The staging environment is a test environment that resembles the production environment but has its own infrastructure and data. This allows for a stable, dedicated security testing environment that does not impact live customer data and helps ensure strong change management and finer access controls. The staging phase also allows engineering teams to test their security fixes before deploying them to the production environment, as well as flag any high-risk issues that must be resolved before deployment.

ASSET team members work closely with both Adobe product teams and cloud service providers to develop guidelines and standards for secure utilization of cloud hosting services. We also make use of automation tools that help better ensure that services are deployed into clean, secure images. This automated "image factory" is usable by all teams and helps streamline security processes by building security into the service images.

Adobe also uses automated tooling to help catch security issues and anomalies in services that are being prepared for deployment. These tools trigger notifications to the service developer(s) when security issues are uncovered in their scans. Developers must address those issues before they can move forward with deployment of their services.

Deployment

By default, code must be cryptographically signed. We require that all proprietary code be stored in an approved code repository. Code packages must be built using an approved build server including approved build applications. Build servers must interface with the code repositories in an automated and secure fashion in order to pull in trusted source code for packaging.

Adobe security teams validate configurations and ensure that the product or service logs the appropriate and relevant information. The product or service incident response teams conduct ongoing incident simulations (e.g., "tabletopping" or "red teaming") to stress-test the product group's process. All releases are automated within our defined change management processes. Releases must pass security tests on an ongoing basis to remain in deployment.

Operations and Monitoring

The Adobe Security Operations Center (SOC) closely monitors third-party vulnerability reports for potential security issues and anomalies. In addition, Adobe employs automated tools to help ensure and validate that the security configurations of each of the company's product and services remain in compliance with regulations, standards, and certifications. If any code is found to be out of compliance, these automated tools generate notifications to the developers about the issue(s) and request resolution. Code that fails our risk assessment policies is removed from deployment until it can be remediated. Our security engineers also continue their security backlog process identifying and pushing for resolution of any new security issues that are uncovered.

Abuse, Fraud, and Incident Response

A requirement of the Adobe SPLC, each product and service team must develop and implement a comprehensive incident response plan, including specific, designated individuals who closely coordinate reactive responses to incidents with the security experts in the Adobe Security Coordination Center (SCC), which is responsible for all proactive security monitoring and reactive incident response across the corporation.

The Adobe Security Operations Center (SOC) in the SCC uses off-the-shelf security information and event management (SIEM) solutions to consume and analyze data sources, including Adobe networking equipment, intrusion detection systems (IDS), and endpoint security agents. Local and remote analysis is conducted in a state-of-the-art forensics lab. The Adobe SCC uses all of the information gathered through SIEM to detect potential threats and make intelligent, informed decisions regarding an appropriate response for each threat, whether it is a low-risk, commodity threat or an advanced, high-risk security threat. Employees continually tune the SIEM tool to filter out noise, eliminate false positives, and ensure the most critical threats are properly prioritized.

While the Adobe SCC handles general threats to the Adobe network and proprietary corporate information, the Adobe Product Security Incident Response Team (PSIRT) manages the response to Adobe product vulnerabilities disclosed or discovered by third parties, specifically those that come from independent security researchers. PSIRT encourages coordinated disclosure in a manner that minimizes risk to customers, Adobe infrastructure, and the Adobe brand.

The Adobe SPLC and Compliance Efforts

Adobe product and service security teams work closely with the company's compliance team in an effort to substantively reduce Adobe's overall security risk. The Adobe SPLC leverages the compliance controls in the Adobe Common Controls Framework (CCF) – and vice-versa.

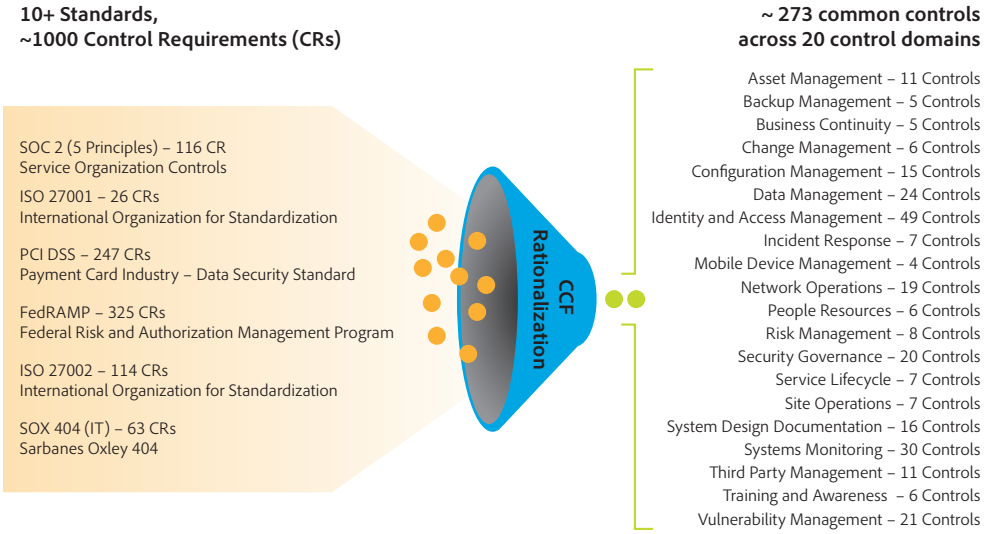

Figure 3: The Adobe Common Controls Framework

The Adobe CCF includes a set of security activities and compliance controls to help protect from the physical layer up. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards. The CCF helps protect the Adobe infrastructure, applications and services, as well as helps Adobe comply with a number of industry-accepted practices, standards, regulations and certifications.

Conclusion

Adobe has invested significant human and financial resources in the Adobe SPLC and secure engineering practices in general. These investments help Adobe to constantly evolve its secure product and service engineering processes in efforts to stay current as changes occur in technology, security practices, and the threat landscape. All of this is part of our committment to help keep your data and digital experiences secure.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 03/2018 Adobe Systems Incorporated. All rights reserved. Printed in the USA.