Building a Culture of Security

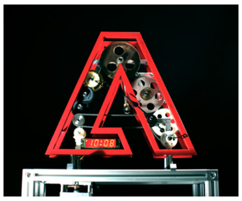

Table of Contents

Overview

Adobe believes that every action taken on or interaction with data and systems should be conducted with a lens of security to help ensure the security, privacy and availability of our customers' data. To achieve this goal, Adobe has created a culture of security that touches virtually every corner of the company, beginning with regular security awareness training and activities for all employees. Engineering and operations employees receive additional job- and/or function-specific security training and certification, helping them to be highly informed, adaptable, and responsive to whatever risks may arise. These employees can take advantage of many opportunities to demonstrate their ability to lead and create security projects that affect the entire company. In addition, each product organization includes a security champion - an Adobe employee who is specifically tasked with and responsible for ensuring the application includes the latest security mechanisms.

With this company-wide focus on security, Adobe can proactively help prevent potential security issues from affecting both the company and our customers and also more swiftly react to threats and remediate vulnerabilities when they appear.

Adobe also looks for opportunities to collaborate with other companies on best practices and strategies for defining and achieving a strong security culture. One example of this collaboration and sharing can be seen in our peer companies that have implemented a version of our security certification program.

Basic Security and Privacy Awareness Training for All Employees

All full-time, regular Adobe employees complete security and privacy awareness training. These trainings include information about appropriate handling of sensitive data, safeguarding assets, reporting security issues, secure vendor engagement, secure password use, avoiding dangers of phishing, social engineering, physical security, and insider threat.

In addition to this content, Adobe provides short training videos and various training presentations on key privacy, trust, and safety topics relevant to Adobe employees. Training topics range from high-level awareness and training on specific privacy, trust, and safety policies and standards that each Adobe employee must follow in his or her daily job responsibilities to more detailed and focused training for specific job functions or regulations.

Adobe regularly holds seminars featuring speakers who share the latest research in the field. Employees gain exposure to top security professionals, researchers, and academics through these seminars and periodical security summits, improving their overall security knowledge. In addition, the company's internal biennial event held in San Jose, California, called Tech Summit, includes a specific track for security, enabling Adobe developers and quality control engineers to share information with each other.

Security Specialists

A dedicated, centralized team of industry-leading experts in building, deploying and monitoring secure applications and services, the Adobe Secure Software Engineering Team (ASSET) works with individual Adobe product security and operations teams to help achieve the highest level of security for all Adobe products and services.

ASSET experts act as consultants to development teams to advise on security best practices for clear, repeatable, and cross-functional processes for development, deployment, operations and incident response. The team uses industry-standard benchmarks and reporting dashboards to constantly measure and convey progress in a variety of key areas. ASSET experts also maintain ties with the security community, exchanging information by collaborating with other organizations.

The Adobe Secure Product Lifecycle Process

Adobe product and service organizations employ the Adobe Secure Product Lifecycle (SPLC) process. A rigorous set of several hundred specific security activities spanning software development practices, processes and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing and deployment. Security training plays a significant role in the SPLC and is a requirement for the product teams.

ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe SPLC controls include, depending on the specific Adobe product or service, some or all of the following recommended best 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 teams 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
- Full readiness reviews, response plans, and release of developer education materials

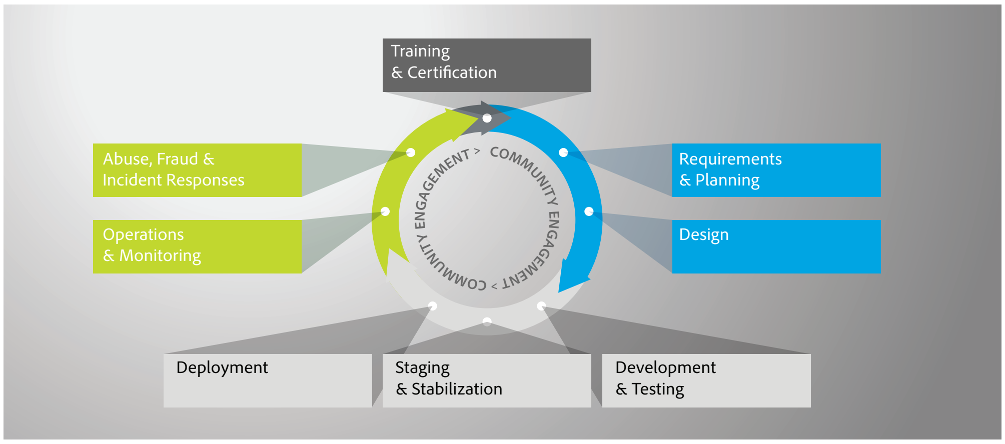

Figure 1: Adobe uses the Secure Product Lifecycle and the Common Controls Framework to provide a complete view of compliance with industry standards and regulations.

Adobe Security Training and Advancement Program

Adobe provides security training, and opportunities to be recognized for security contributions, through the Adobe Security Training & Advancement Program. The program is geared towards

Adobe product and operations engineers and are based on progressive certification advancements. The program is intended to help ensure security expertise in deploying Adobe products and services.

Certification

The advancements are based loosely on the model of martial arts belt color advancements, and are achieved in the following order: Green, Brown, and Black.

Security Green Belt

This belt is achieved by completing a role-based e-learning course. Engineers select a course that is most applicable to their role at Adobe and upon completion they are awarded the Security Green Belt certification. Some role-course examples are, but not limited to: Java Developer, PHP Developer, iOS Developer, Android Developer, Program Manager, and Software Architect.

These courses help teams meet applicable compliance requirements and build on their security skills and knowledge, ultimately improving the implementation of security at Adobe. Upon completion, Adobe engineers not only receive the Adobe Security Green Belt but they are provided and prepared for the option to obtain the (ISC)^2 Secure Software Practitioner Certification.

Enrollment in the Security Green Belt is self-enrollment or auto-enrolled depending on their job family at Adobe (e.g. Software Developer) or based on their managers discretion. Upon enrollment, they are given 90 days to complete. The role-based courses take on average 8-12 hours to complete. Recertification is required every three years; upon which time the trainings have been refreshed with new information where needed.

The curriculum includes approximately 40 subject offerings, and Adobe continually adds new and updates current material to the curriculum in a rolling-release format. Updates are made based on emerging security concepts, new products or technologies, and employee feedback and recommendations, thereby keeping program content fresh and current.

Some sample security-focused courses available include, but not limited to

- Application Security Fundamentals
- Secure Software Testing
- Software Acceptance
- Secure Software Requirements
- General Data Protection Regulation (GDPR)
- OWASP Top 10
- Defending Java
- Defending .NET
- Defending iOS
- Defending Mobile
- Defending Python
- Operational Security

Security Brown and Black Belt

The two higher belts, Brown and Black Belt are experiential based and therefore require completion of security project(s) that directly benefit Adobe and our customers. These belts are an opportunity for engineers to demonstrate and make a security difference at Adobe. As engineers achieve these belts, they are publicly recognized for their achievements and forever recorded as an individual who made a positive impact on security at Adobe.

Some projects that employees can undertake in order to gain Brown Belt or Black Belt certification include:

- Researching and presenting a topic at a security conference
- Implementing new testing strategies
- Researching and developing new content for the ASSET Software Security Certification Programs
- Architecting or re-architecting products or components to enhance security
- Creating new vulnerability detection and response strategies

Upon completion of a security project, the candidate submits a report to a security training & advancement committee, which then determines the appropriate points for the project. When an employee accumulates enough points to reach Brown Belt or Black Belt status.

Those who achieve these higher ranks are rewarded with as stickers, t-shirts, hats, etc,. Additionally, global announcements and awards ceremonies are conducted for those who achieve these higher ranks. The purpose in providing these rewards is to show pride in their achievements and to promote and encourage others to follow suit in becoming knowledgeable about and acting on implementation of security at Adobe.

Often, employees combine or undertake several projects to fulfill the Brown Belt and Black Belt certification requirements. For each project he or she completes, the participant earns points toward the 1,000-point requirement for Brown Belt status or the 3,000-point requirement for Black Belt status. Points are determined by multiplying the number of hours a candidate worked on a project against the "security expertise modifier," a number that reflects

1. The difficulty of the task and...
2. The impact of the project on security at Adobe. This number ranges from .03 to 3.0.

Overall, approximately 200 Adobe employees have completed more than 70,000 hours of security-focused engineering work that otherwise would not have been performed and has had a positive impact on the company as a whole.

Tracking Certification Progress and Rewards

Belt status is tracked on a dashboard available to all Adobe employees. This is beneficial as it creates a sense of pride for those who have achieved a higher belt status but also fosters friendly competition among peers. Additionally, the dashboards allow teams to accurately and reliably report on training completion for compliance or team goal purposes.

Security Champion Support

The embedded security champions within each of Adobe's product organizations are a critical part of the implementation of the Adobe SPLC process throughout the company. Security champions do not need to attain Brown or Black Belt status, but they are encouraged to do so. Champions assist the centralized ASSET team in scaling security efforts across the company, disseminating critical security information to and ensuring the completion of security tasks within their product or service teams. These security champions also participate in periodic security boot camps and industry events and conferences to further enhance their security knowledge.

In addition, ASSET employees in the office of the Chief Security Officer help provide high-level security training for the security champions in each of Adobe's product lines when requested by the security champion him- or herself. These training programs run from one day to a full week. Security champions may request or initiate training at any time.

Capture the Flag Program

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" children's game. This type of exercise is often used for security champion training, helping these employees to think like the adversary and try to stay one step ahead of malicious individuals.

In addition, engineers can also participate in Capture the Flag exercises at Adobe's regular engineering education conference, called TechSummit. Held at the Hacker Village erected specifically for the conference, employees can access a dummy server that is open to a specific class of vulnerability, such as SQL Injection or Cross-Site Scripting (XSS). Employees attempt to hack the server and leave their name in a file on the server as proof of the hack. The first person to hack the server gets a specific number of points, the second person to hack it receives a lesser number of points, and so on. The employee who accumulates the most points wins. Each employee who successfully hacks the server is eligible for a prize drawing. Typically, between 400 and 500 employees successfully hack the dummy server during TechSummit. This activity encourages engineers to "think like an attacker" in order to make them more aware of the types of issues that could compromise a system.

In 2016, Adobe also introduced a month-long Capture the Flag competition for engineers across the company during National Cybersecurity Awareness Month.

Internal Communications

Adobe maintains several active mailing lists specifically focused on security issues. These lists are used to announce new internal security material and training classes as well as to issue notifications about security threats and incidents in the industry. Maintained as opt-in lists, more than 750 employees subscribe to these security-focused mailing lists. The largest list has become a vibrant community where subscribers discuss security issues in the news, debate security practices, and recruit volunteers for special projects.

Adobe and the Security Community

Adobe is deeply involved in the security community, working closely with recognized industry groups including SAFECode (the Software Assurance Forum for Excellence in Code), the Cloud Security Alliance, OWASP (Open Web Application Security Project), MAPP (Microsoft Active Protections Program), Girls Who Code, r00tz, and Women in Cybersecurity.

Adobe employees are also encouraged to take full advantage of the wealth of security resources available outside the company. Adobe employees attend local and regional security meet-ups and conferences and take courses in cyber-security at nearby universities. Many product teams also send team members to industry conferences, such as BlackHat, Hack in the Box, and OWASP AppSec. Many Adobe employees also regularly speak at security conferences around the world.

In addition to the month-long Capture the Flag competition, Adobe will also hold several events around the world during National Cybersecurity Awareness Month to help reinforce positive security behaviors among our employees and their families at home and in social media. Throughout the month, we will publish the best practices we discover both internally and via social media. Our goal is that once employees apply these best practices at home, they will also improve their security savvy in the office.

Compliance Impact of Adobe's Security Culture

Security at Adobe is evangelized from the CEO on down, helping make security an important aspect of everything we do at Adobe. Besides evangelizing security, Adobe's security training and awareness program also aligns with the training controls defined in various industry standards and compliance frameworks. The Adobe Common Controls Framework (CCF) helps keep our training programs updated and focused on meeting the requirements of the standards and compliance initiatives that are most important to Adobe and our customers.

The Adobe CCF states that our training programs must meet the following four requirements:

- Implement a security awareness program for all employees
- Train all newly hired employees as soon as possible
- Offer annual, role-dependent training for existing employees
- Demonstrate levels of competence by testing attendees after each course and recording their performance

Adobe tailors our training programs based on the content as well as the level and depth requirements of the employees receiving the training. For example, engineers writing code may need a different level of training on a specific topic than a manager or system administrator. All employee training includes directions on how to report observed security issues.

By developing training programs that meet the specific requirements for the frameworks, Adobe had great success meeting the requirements for those compliance Frameworks, and enhancing the security profile at Adobe. You can find more information about our compliance programs in the Adobe Cloud Services Compliance Overview white paper.

Conclusion

Adobe is an established global leader in security culture, training, and awareness. Our developers, quality engineers, and program managers have access to a world-class technical training experience in the ASSET Secure Software Certification Program, which is quickly becoming the basis for industry standards. The Brown and Black Belt levels of this program alone have resulted in an estimated 70,000 hours of security work that benefits the company. Adobe also provides a range of hands-on support, practical training, and community building opportunities for the security champions in each product organization. We are constantly look for opportunities to create positive and fun ways to illustrate real-world security challenges and how to solve them, helping our employees stay engaged and improve their security savvy.

Please visit the Adobe Trust Center at https://trust.adobe.com for more information about security efforts across our products and services.

Adobe
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