Adobe Security Training

Table of Contents

1 Adobe Security
1 The Adobe Security Organization
2 Adobe Secure Product Development
3 ASSET Software Security Certification Program
5 Security Awareness Training
6 Conclusion

Adobe Security

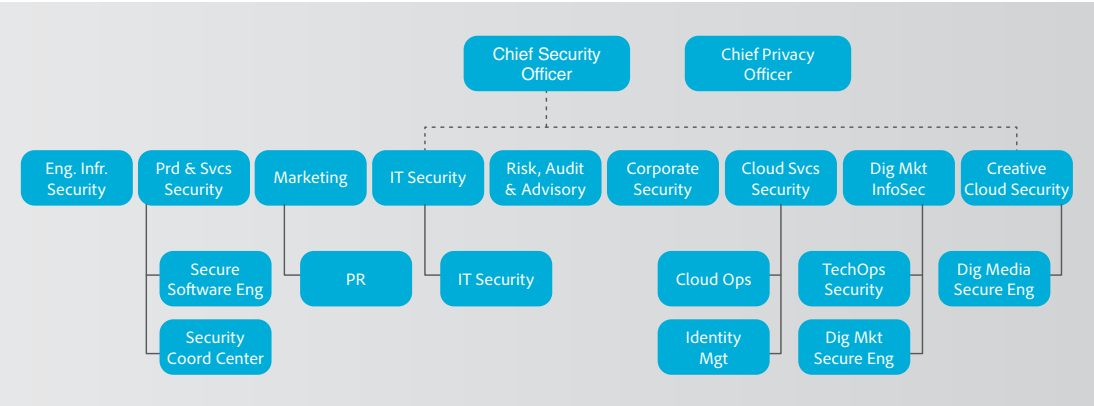
At Adobe, we take the security of your digital experience seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest security best practices as well as continually build security into the products and services we offer.

This white paper describes the Adobe security training and awareness activities that help increase the security IQ of Adobe employees and ultimately help improve the security of Adobe products and services.

The Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts, including security training, under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives as well as the implementation of the Adobe Secure Product Lifecycle (SPLC) process.

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security specialists who serve as consultants to key Adobe development and operations teams. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.



Adobe Security Organization

Adobe Secure Product Development

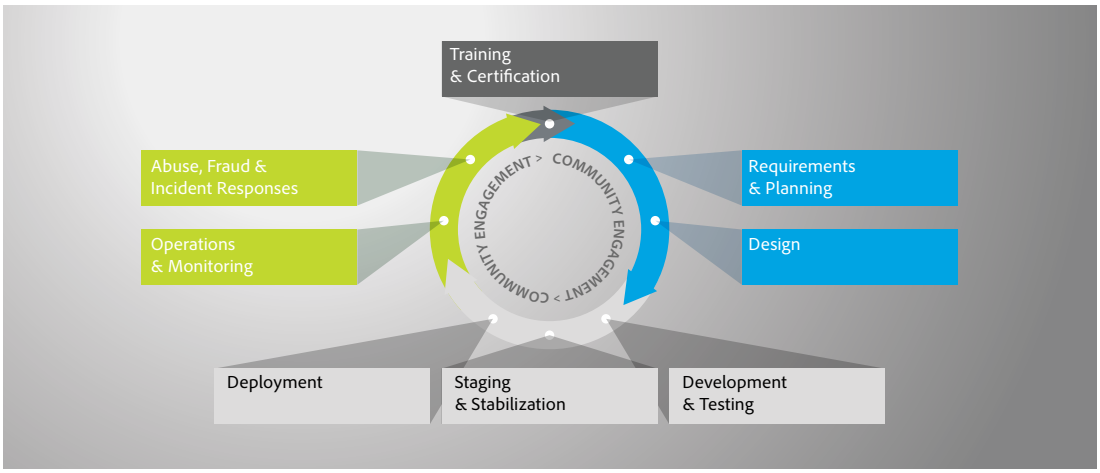
Adobe's ASSET team employs the Adobe SPLC process for product and services development. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment.

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 Secure Product Lifecycle

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 development teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Digital Publishing Suite 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
- Full readiness reviews, response plans, and release of developer education materials



Adobe Secure Product Lifecycle (SPLC)

ASSET Software Security Certification Program

A key part of the Adobe SPLC, the ASSET Software Security Certification Program includes ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. The program provides a foundation for participants to understand security fundamentals as well as a path for those individuals who want to become security leaders.

Since its inception in 2009, thousands of Adobe employees participate annually in the ASSET Software Security Certification Program, attaining one or more of the certification levels described in detail below. More recently, the program formed the basis for the newly released industry software security training program from SAFECode (the Software Assurance Forum for Excellence in Code), a global, non-profit organization focused on identifying and promoting best practices for developing and delivering more safe and reliable software, hardware, and services.

ASSET Certification Levels

White—Introduces basic security concepts (e.g., security in web-focused languages, such as Ruby on Rails and PhP)

Green—Builds on basic security topics covered in the white belt level

Brown—Measures, recognizes, and rewards the development of security components in Adobe product code (e.g., sandboxing)

Black—Recognizes the highest level of hands-on security expertise within Adobe development teams across the company

ASSET Certification Levels

Depending on their specific job function and role, Adobe employees may choose from one of four (4) levels of certification, also called 'belts'. Each level or belt requires a specific number of hours of training to achieve, again based on job function or role with Adobe. While the lower levels of certification only require online training sessions in basic security concepts, the higher certification levels include hands-on, experiential projects that may directly relate to or impact the employee's job responsibilities. Currently, White Belt certifications are required to be updated after eighteen months, unless an employee also earns a Green belt.

ASSET Course Content

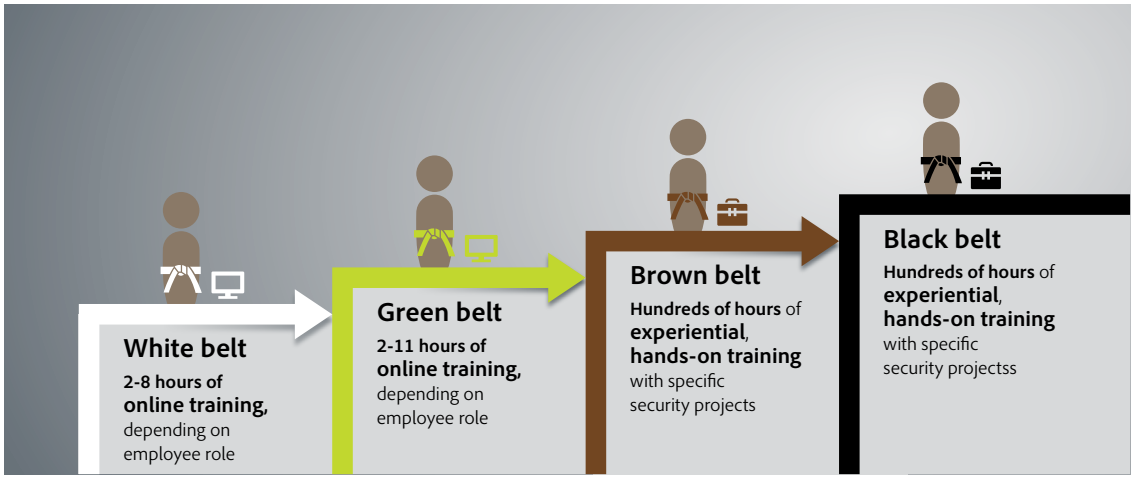
The current ASSET Software Security Certification Program curriculum includes more than 50 course offerings, and Adobe continually adds new material to the curriculum in a rolling-release format. Updates are made based on emerging security concepts, new products or technologies, and employee feedback and recommendations, thereby keeping program content fresh and current. Adobe notifies employees of new course content through online announcements, ensuring equal access and availability to important security concepts and achievement of training levels.

Adobe employees can choose different tracks within each level of the program based on their specific job function and requirements, with tracks designed for developers, quality engineers, and managers. Each track also includes sub-tracks that enable employees to focus on the particular products and technologies with which they work in their role at Adobe. At the end of each training module, program participants fill out a survey, asking them to rate the content and propose suggestions for improvement.

ASSET Certification Requirements

Through the four-tiered ASSET Software Security Certification Program, employees earn a colored 'belt' for each level they attain:

- **White**—Between two (2) and eight (8) hours of online training, depending on employee role
- **Green**—Between two (2) and eleven (11) hours of online training, depending on employee role
- **Brown**—Hundreds of hours of experiential, hands-on training with specific security projects
- **Black**—Hundreds of hours of experiential, hands-on training with specific security projects



Adobe Software Security Certification Program

White and Green Belts

Adobe designed the White Belt and Green Belt levels to provide basic security training for employees who need to understand security concepts for their job.

Employees attain one or both of these levels through computer-based trainings (CBTs), which include PowerPoint presentation decks with voice-overs and animated demos. While the CBTs vary in length, most of them are approximately 30 minutes long and include a quiz at the end of the training module to ensure that the participant has digested the content in the CBT.

In general, achieving a White Belt takes between two and eight hours of screen time, while training for a Green Belt can be completed in approximately two to 11 hours.

White Belt Curriculum

The White Belt curriculum is designed to ensure that the employee has a core competency in security concepts as well as possesses security knowledge that applies directly to his or her job responsibility at Adobe. To meet this goal, the White Belt curriculum includes a core syllabus of basic security concepts that affect every employee at Adobe, from policy training (e.g., SPLC: Adobe Secure Product Lifecycle) to more technical, yet platform- and language-agnostic security training (e.g., Authentication 101: A Passwords Backgrounder for Everyone).

From there, the participant can engage in specialized training in technologies directly related to his or her job responsibilities. For example, if a developer codes in C/C++ on a Windows platform, he or she can take White Belt-defined courses for developers for C/C++ on Windows. Similar courses exist for employees using Java, PHP, and Ruby on Rails in their day-to-day job responsibilities.

Green Belt Curriculum

Picking up where the White Belt curriculum ends, the Green Belt curriculum explores security concepts in greater depth and introduces more complex security topics and case studies. Examples of some Green Belt courses include: Anatomy of an Attack, XSS 201, Injections 201, and Web Architecture, Same Origin, and User-Generated Content.

Brown and Black Belts

The two higher certification levels, Brown Belt and Black Belt, require completion of hundreds of hours of hands-on experience with security projects over a period of several months or even a year.

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, (e.g. sandboxes)
- Creating new vulnerability detection and response strategies

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.

Upon completion of a security project, the candidate submits a report to the security training committee, which then determines the appropriate points for the project. When an employee accumulates enough points to reach Brown Belt or Black Belt status, the security training team sends a congratulatory email not only to the candidate, but also to the Adobe security community as well as the candidate's manager.

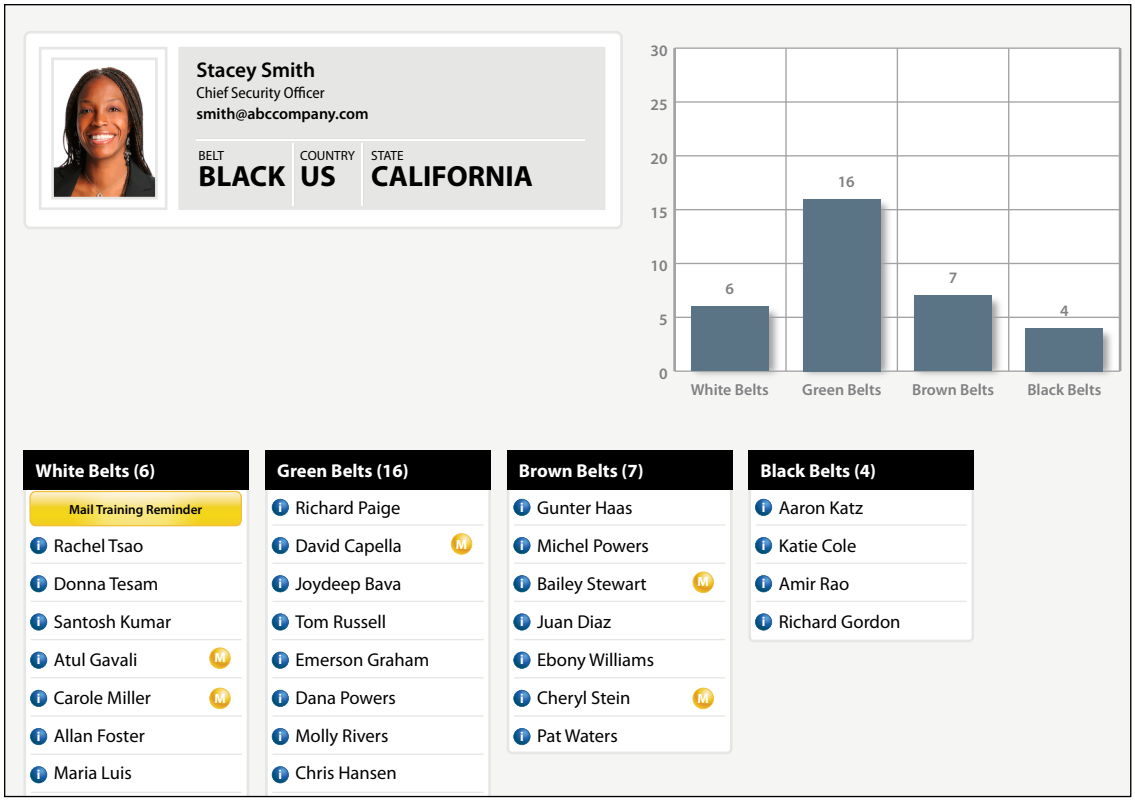
Employees attaining Brown and Black Belts become candidates for the embedded 'security champion' within their development teams and are a critical part of the implementation of the Adobe SPLC process throughout the company. Security champions assist the centralized ASSET team in scaling security efforts 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.

Tracking Certification Progress

Participants and their managers are encouraged to set goals for reaching a specific certification by a specific date. Motivated participants make achievement of the next level of certification a part of their annual performance objectives and can gain increased visibility and recognition when they achieve those levels.

Using an internal web tool that interfaces with Adobe Connect, employees can check their own progress through a particular certification level and managers can follow up with team members about their certification status.

Per-product certification status rolls up to an overall 'security health' dashboard, which is reviewed monthly at Adobe Senior Operations Staff meetings.



Adobe Security Certification Program Status Tool

The screen shot above shows current certification progress for an organization's security team. The yellow buttons allow the manager to automatically send a reminder email to anyone within the organization that has not completed his or her certification by the pre-defined date. Clicking on the yellow button opens the managers email client and populates a message with the appropriate content for the person he has selected to remind.

Security Awareness Training

In addition to the ASSET Software Security Certification Program, all full-time, regular Adobe employees are required to complete annual security awareness training, which includes information about safe handling of confidential information, safeguarding devices, using password protections effectively, and recognizing and avoiding social engineering. Security Awareness training is refreshed annually. Employees also regularly participate in internal security awareness seminars and other activities to increase awareness of how security affects their specific roles within the organization and the company as a whole.

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 bi-annual 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.

Adobe employees are also encouraged to take full advantage of the wealth of security resources available outside the company. Adobe employees attend local, regional and international security meet-ups and conferences and take courses in cyber-security at nearby universities. Many development teams also send team members to industry conferences, such as Black Hat, Hack in the Box, and OWASP (Open Web Application Security Project) AppSec.

In addition, Adobe holds global, hands-on cyber-awareness events for employees such as HackFests, which help participants gain a better understanding of how hackers exploit vulnerabilities as well as how these exploits are not as difficult as they may seem.

During Hackfests, employees gain access to a dummy server that is open to a specific class of vulnerability, such as SQL Injection or XSS. Employees attempt to hack the server and leave their name in a file on the server as proof of the hack. 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 a HackFest.

After participating in a HackFest, many participants comment that they have a greater appreciation for security in general and for the importance of security best practices in particular.

Conclusion

The proactive approach to security training described in this paper helps increase the security IQ of Adobe employees, which ultimately helps improve the security of your Adobe products and services, as well as your data. We recognize that the security landscape is not static, which is why we continually update and enhance our security training to meet the growing number of security challenges, helping to keep your Adobe digital experience safe and secure.

For more information, please visit: http://www/adobe.com/security.

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.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA

www.adobe.com

9/2014