Building a Culture of Security

Table of Contents

Overview

Adobe believes that every action taken on or interaction with data 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 seminars 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 highly responsive to whatever vulnerabilities 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 incudes 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 not only proactively help prevent potential security issues from affecting both the company and our customers but also more swiftly react to threats and remediate vulnerabilities when they do 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. Additionally, we work with a number of industry organizations, such as SAFECode (the Software Assurance Forum for Excellence in Code), and share our training material in an open source format.

Basic Security and Privacy Awareness Training for All Employees

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.

In addition to ongoing live trainings, 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.

In line with the company's culture of security, 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 semi-annual event held in San Jose, California, called TechSummit, includes a specific track for security, enabling Adobe developers and quality control engineers to share information with each other.

Security Training for Engineering and Operations

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

Adobe Engineering and Operations Certification Program

A key part of the Adobe SPLC, the ASSET Software Security Certification Program includes ongoing security training within engineering and operations teams to enhance security knowledge throughout the company and help improve the overall security of our products and services. The program provides a foundation for everyone within the Adobe organization 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, a global, non-profit organization focused on identifying and promoting best practices for developing and delivering more safe and reliable software, hardware, and services.

Certification Levels

Depending on their specific job function and role, Adobe engineering employees choose from one of four (4) levels of certification, also called 'belts'. Adobe operations employees currently choose from one of two (2) levels of certification, with an additional two (2) levels planned for the future.

Adobe Engineering and Operations Security 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 product teams across the company

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:

- **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

Employees who attain any level of certification in the program are known as 'Security Ninjas' and receive physical pins and paper certificates to display and digital badges to include in their online profiles and email signatures. Employees must re-certify at their role-specific level on an annual basis.

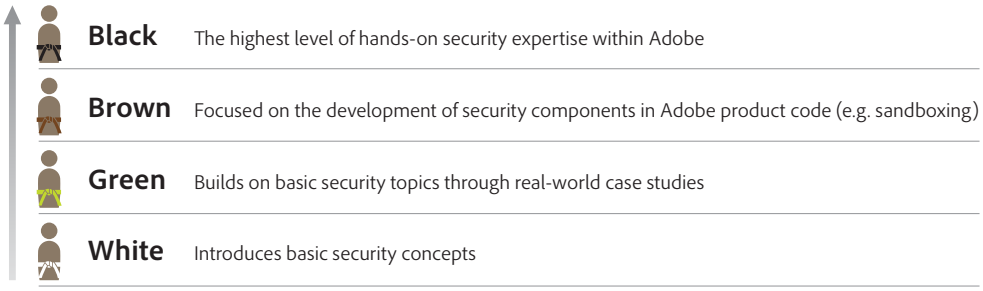

Figure 2: ASSET Software Security Certification Program

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, 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. Operations professionals can pursue a white belt track specifically focused on the security challenges in operations.

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. At this time, these two belts are only available to engineering and product development employees.

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

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.

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. Some examples of these important efforts include helping other engineering employees understand how to spot and then diffuse the Java deserialization bug, which gives attackers a way to remotely gain total control of an application server; updating and improving KLAM (K[C]LoudOps Access Manager), a tool for managing Adobe Web Services (AWS) logins, tokens, and keys; and making integration of LDAP and other authentication frameworks into Adobe products and services easier and faster to complete.

Engineering Security Course Curriculum

The current ASSET Software Security Certification Program curriculum includes 40 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.

Some sample security-focused courses available to Adobe engineering employees include:

- Authentication Basics
- Click-Jacking
- HTML 5 Security
- Injections 101
- Product Health, Risk and Threat Landscape Analysis

- Security Training and Certification for Product Teams
- Using JavaScript Frameworks Securely
- XSS 101 (a.k.a., Cross-Site Scripting for Developers)

Operations Security Course Curriculum

The current Adobe operations security course curriculum includes 10 course offerings for Adobe Cloud Operations and Technical Operations employees. At this time, Adobe only offers courses in the White and Green Belt levels, but we are actively researching and developing Brown and Black Belt courses to be added in the near future. Most operations employees who achieve White Belt status go on to attain a Green Belt as well.

Some of the security-focused courses available to Adobe operations employees include:

- Access Control
- Architecture
- Authentication
- Compliance
- Cryptography
- Disaster Recovery
- Monitoring
- Secure Operations

Tracking Certification Progress and Rewards

Product teams and managers set goals for each employee to reach a specific certification by a specific date. Motivated individuals make achievement of the next level of certification a part of their annual performance objectives and 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. Every employee's status is publicly visible to anyone within the company, helping encourage competition among teams and individuals.

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

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), OWASP (Open Web Application Security Project), MAPP (Microsoft Active Protections Program), Girls Who Code, r00tz, and Women in Cybersecurity. In fact, Adobe recently donated its security engineering training curriculum to SAFECode, with the global, non-profit organization adopting the curriculum as the basis for its newly released software security training program.

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 security information site at http://www.adobe.com/security for more information about security efforts across our products and services.

Adobe

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