ABSOLUTE™

Product Security Practices

December 2017

Absolute is fully committed to providing the most secure software products in the industry. The trust of our customers guides every decision to ensure that our products deliver the high level of security they need and expect for their environments and data. We view security as a key factor of quality, and quality as a factor of trust and reliability. In our mission to maintain this trust, we continually examine our internal development processes and adapt them to evolving industry standards, endorsing the most beneficial practices that balance improved productivity, increased reliability, and lead to a more robust, more secure product.

A more detailed version of this document is available with a signed non-disclosure agreement. For more information, contact securityQuestions@absolute.com.

A culture of collaboration

At Absolute, delivering advanced security begins with the careful building of highly skilled, cross-functional teams where leadership cultivates a culture of full team collaboration, involvement, and inclusiveness, and encourages questioning the status quo. Collaborative product development teams of this kind of culture today are most often associated with Agile development. Absolute has adopted Scrum as its Agile process.

The Agile process paired with the culture of collaboration and mutual respect significantly reduces the potential for security defects from lack of review or expressed dissension of work in progress.

Absolute's secure Agile software development lifecycle

Absolute's philosophy on developing truly secure products is to incorporate industry best practices of software security throughout the entire development lifecycle. Absolute employs a robust software development process. In our process, we have incorporated industry leading tools and best practices, which include:

- coding standards
- design and code reviews
- security standards
- threat modeling
- static code analysis
- dynamic runtime analysis
- continuous integration
- automated integration and unit testing
- test coverage analysis
- release management

Figure 1 shows a more detailed view of what occurs during each sprint. It illustrates how changes are hardened and become more secure over the course of sprints as a result of continuous integration of work completed, test automation, security reviews, changes incorporated from review feedback, and code analysis tool scanning. Often added to the project are optional hardening sprints, and penetration testing is typically initiated when high stability is achieved and release readiness approaches. Security-specific activities in the figure are shown in red text. Teams design and implement every sprint item with security in mind, and any changes in areas of data protection and cryptography, access control, communication (off-box and inter-process), and third-party library use receive special security review focus. All development is subject to this process, these reviews, and a high level of scrutiny and analysis—from the business layer down to the firmware.

A number of key process gates related to quality and completeness help assure project functionality is met before advancing further.

Absolute Product Security Group (APSG)

This working group is responsible for overseeing and refining security practices within Absolute, vulnerability management, and maintaining this document and approving it for publication and changes as required.

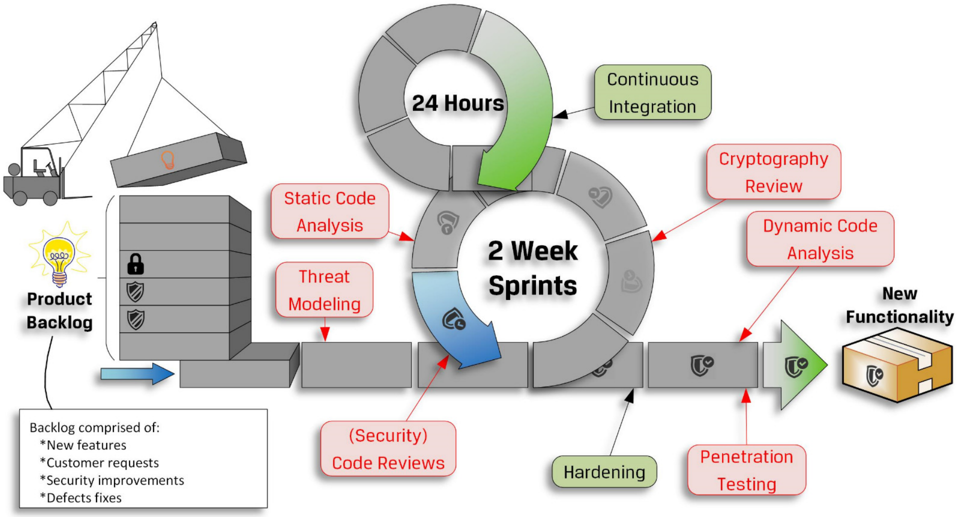

FIGURE 1. Absolute's Secure Agile Software Development Lifecycle incorporates security reviews throughout the process

Absolute Risk Management Committee (ARMC)

The ARMC's mandate is to provide risk management leadership for IT and Development, aligning program objectives and activities relevant to enterprise strategic objectives and processes. The committee prioritizes identified risk exposures and thresholds, and resource allocation issues based on risk prioritization to ensure optimal risk management through service target measurements. The ARMC ensures open communication between departments and other functional units to continually promote collaborative risk management.

Point of contact

For more information about Absolute's Product Security practices or if you have questions related to Product Security, contact Absolute's Product Security Group (APSG) at ProductSecurity@absolute.com.

Notice

No computer system is absolutely secure. Absolute makes no warranty with respect to any malfunctions or other errors in its hardware products or software products caused by viruses, infections, worms, or similar malicious code not developed or introduced by Absolute. Absolute makes no warranty that any hardware products or software products protect against all possible security threats, including intentional misconduct by third parties.

About Absolute

Absolute Software Corporation (TSX: ABT) is the industry standard in persistent endpoint security and data risk management solutions. Persistence® from Absolute provides organizations with visibility and control over all of their devices, regardless of user or location. For more information, visit www.absolute.com.

Copyright information