INFOBRIEF

Secure software development lifecycle validation

Placing a significant importance on the validation phase of Ciena's secure software development lifecycle (SSDLC) process is crucial. In this digital age, security is not just a responsibility but a critical necessity. At Ciena, we ensure that our SSDLC process undergoes rigorous validation to provide customers with reliable, efficient, and—most importantly—secure systems, services, and software. We know our customers' success is dependent on the confidence, integrity, and safety of the products they use. The SSDLC process demonstrates Ciena's commitment to developing secure products and services with a range of security requirements, which are implemented on a product-by-product basis to address customer security needs.

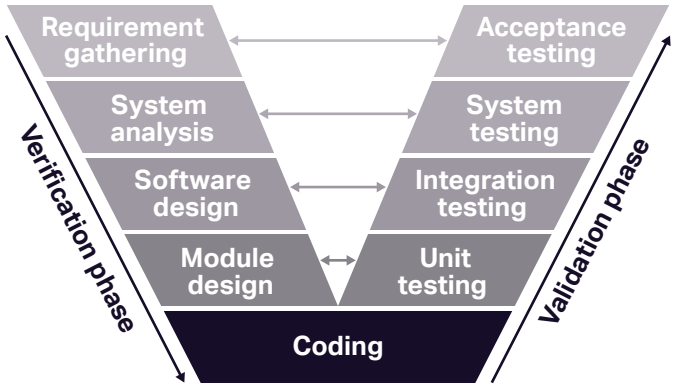

Figure 1. V-model comprising verification phases on one side and validation phases on the other, joined by the coding phase at the base of the V

The SSDLC process covers all phases of software development, from planning and design to testing and deployment, and incorporates security and privacy requirements, code analysis, vulnerability testing, and incident response. As the fourth phase of the SSDLC process, validation is often done in a V-model (Figure 1)—an extension of the waterfall model that is based on the association of a testing phase for each corresponding development stage. Validation helps identify vulnerabilities and necessary changes early in the process, saving time and money.

The validation phase in the SSDLC process includes checking whether the software product meets customer expectations and requirements. Also known as dynamic testing, it involves executing the software and comparing the expected and actual outcomes. Validation helps ensure that the software product is fit for its intended purpose and satisfies the user's needs. Some of the activities that are involved in validation include:

- Black-box testing: Testing the software functionality without knowing its internal structure or code
- White-box testing: Testing the software functionality knowing its internal structure or code
- Unit testing: Testing the individual software components or units
- Integration testing: Testing the interaction and integration of different software components or units

As mentioned earlier, the validation phase is not only necessary but critical for several compelling reasons:

Risk reduction: SSDLC validation ensures that security measures are integrated at every stage of software development. By identifying and addressing vulnerabilities early, the risk of security breaches, data leaks, and cyberattacks is significantly reduced.

Cost savings: Fixing security issues after deployment is far more expensive than preventing them during development. SSDLC validation helps catch security flaws early, saving both time and resources.

Customer trust: Secure software and product development inspires confidence in users. Organizations that prioritize security demonstrate commitment to protecting customer data, as well as fostering trust and loyalty.

Threat landscape: Cyberthreats evolve rapidly. SSDLC validation adapts security practices to address emerging risks, keeping software resilient against new attack vectors.

Business continuity: A security breach can disrupt operations, damage reputation, and lead to financial losses. SSDLC validation safeguards business continuity.

In summary, SSDLC validation is not just a process; it's an investment in robust, trustworthy solutions that benefit organizations, users, and the digital ecosystem. Ciena strives to ensure a world-class security program based on industry standards, such as the National Institute of Standards and Technology (NIST) and ISO 27001, so our customers can focus on their business objectives.

Ciena has secure product development processes in place to ensure that new releases deliver consistent product security. Secure validation processes work in conjunction with the other defined secure-development processes to ensure product security.