McAfee
Product Security Practices

12 October 2017

Importance of Security

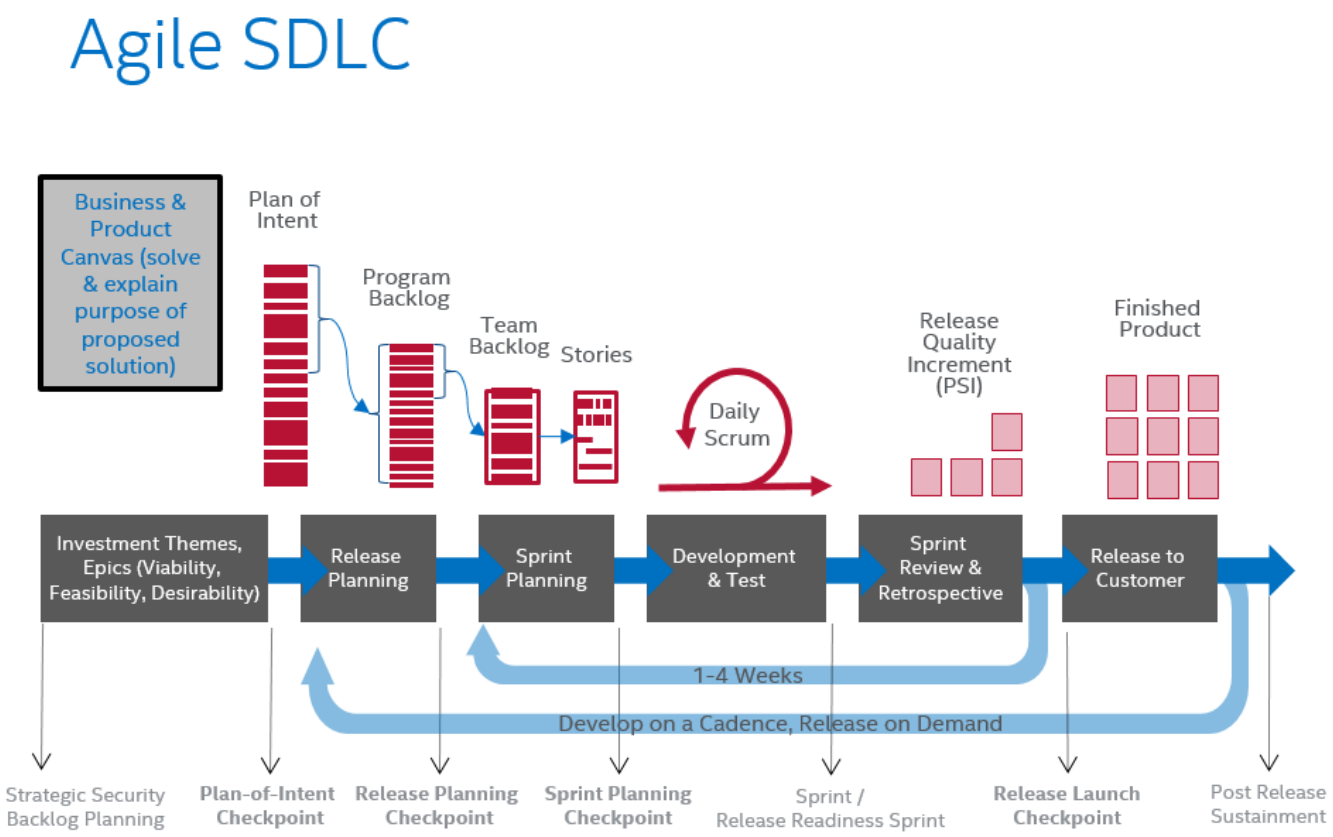
At McAfee (formerly Intel Security) we take product security very seriously. Our practices include designing for both security and privacy, in software and applications. We have rigorous product security policies and processes designed to proactively find and remove software security defects, e.g. security vulnerabilities. We understand that our products must not only fulfill the stated function to help protect our customers, the McAfee software itself must also aim to protect itself from vulnerabilities and attackers. McAfee strives to build software that demonstrates resilience against attacks.

We also understand that our customers may, from time to time, wish to review our product security practices so that they may make their own risk-based decisions on how best to use our products and to fulfill any due diligence responsibilities they may have.

Specific policies and practices can vary by product. The summary of practices described in this statement apply to all McAfee and Intel Security branded products.

Software Development Lifecycle (SDLC) at McAfee

All of McAfee's software is developed using the Agile methodology or Continuous Integration Continuous Delivery (CICD). These agile practices are referred to as the Agile Software Development Lifecycle (SDLC). The Waterfall methodology is no longer used. At McAfee, the SDLC is referred to as the Product Lifecycle Framework (PLF) v2.

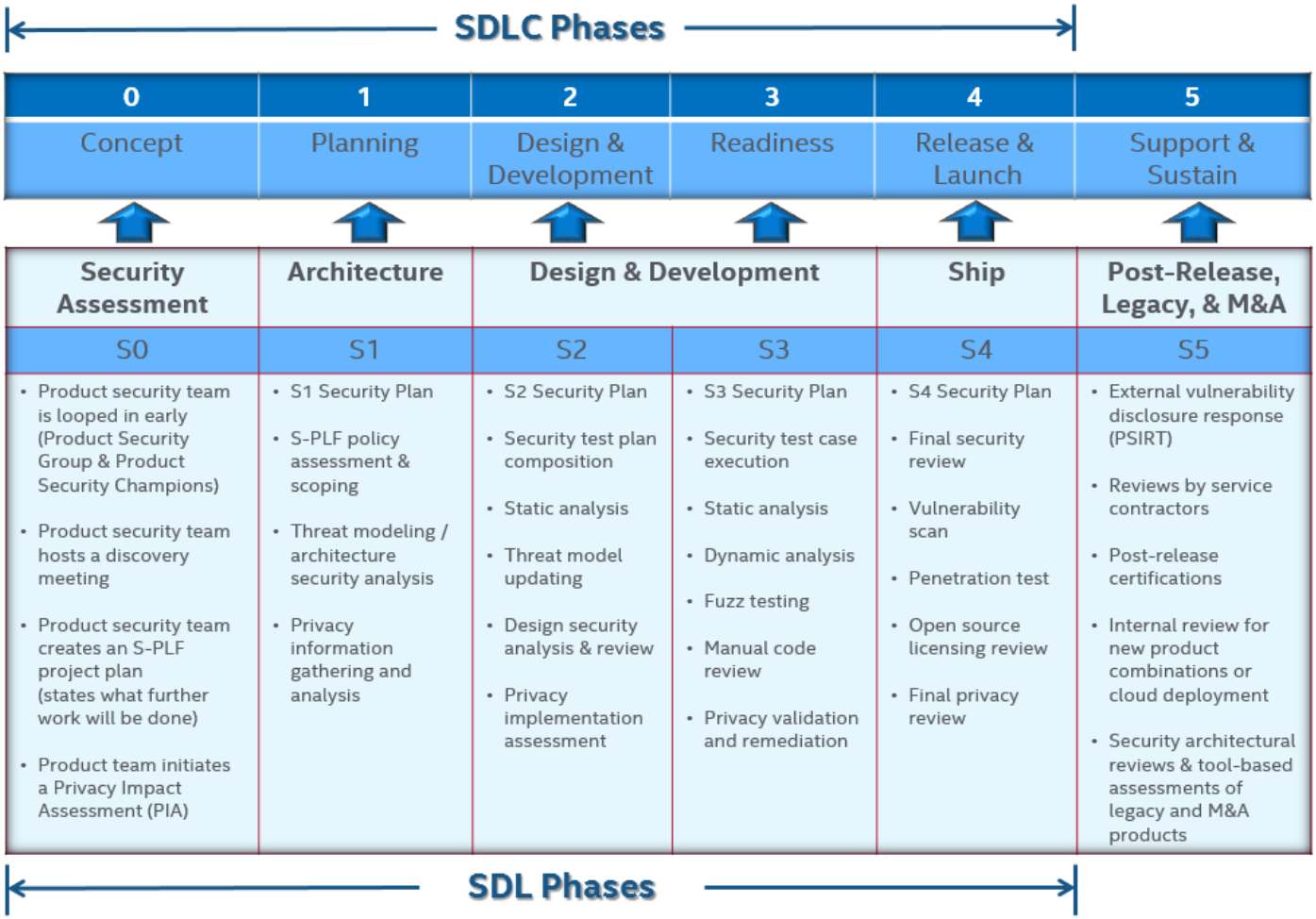


Security Development Lifecycle (SDL) at McAfee

In line with IT and application development industry standards such as ISO/IEC 27001, 27002, and 27034, BSIMM, and SAFECode, McAfee product development has processes designed to adhere to a Security Development Lifecycle (SDL).

- McAfee's SDL is called the Agile SDL

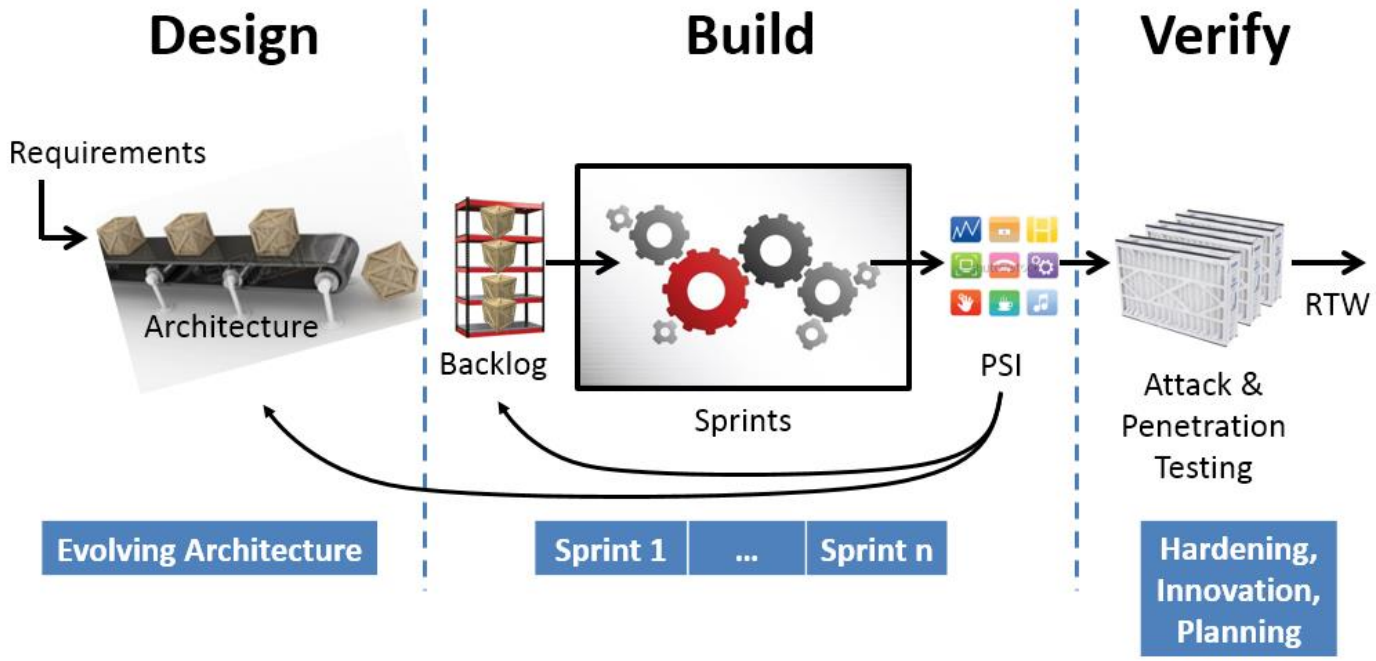
The following paragraphs describe, at a high level, the McAfee SDL process.



The chart above was developed for a traditional Waterfall SDLC. This chart has been adapted and redefined for McAfee's Agile SDL. Security and privacy tasks are integrated into McAfee's Agile SDL as a seamless, holistic process designed to produce software that has appropriate security and privacy built into it. While the following description may appear to apply only to Waterfall development, the same set of security tasks are performed across the iterations of Agile just as they may be performed in discreet phases during Waterfall. McAfee encourages full engagement by product security engineers and architects within Agile sprints to ensure that security and privacy are integral parts of the Agile process.

High Level Agile SDL

For a new product, the security process typically begins at project initiation. A seasoned security architect or McAfee Product Security Champion (PSC) assesses a proposal for its security implications. The output of this engagement is any additional security features that will be added for software self-protection so that the software can be deployed in accordance with the different security postures of McAfee's customers.

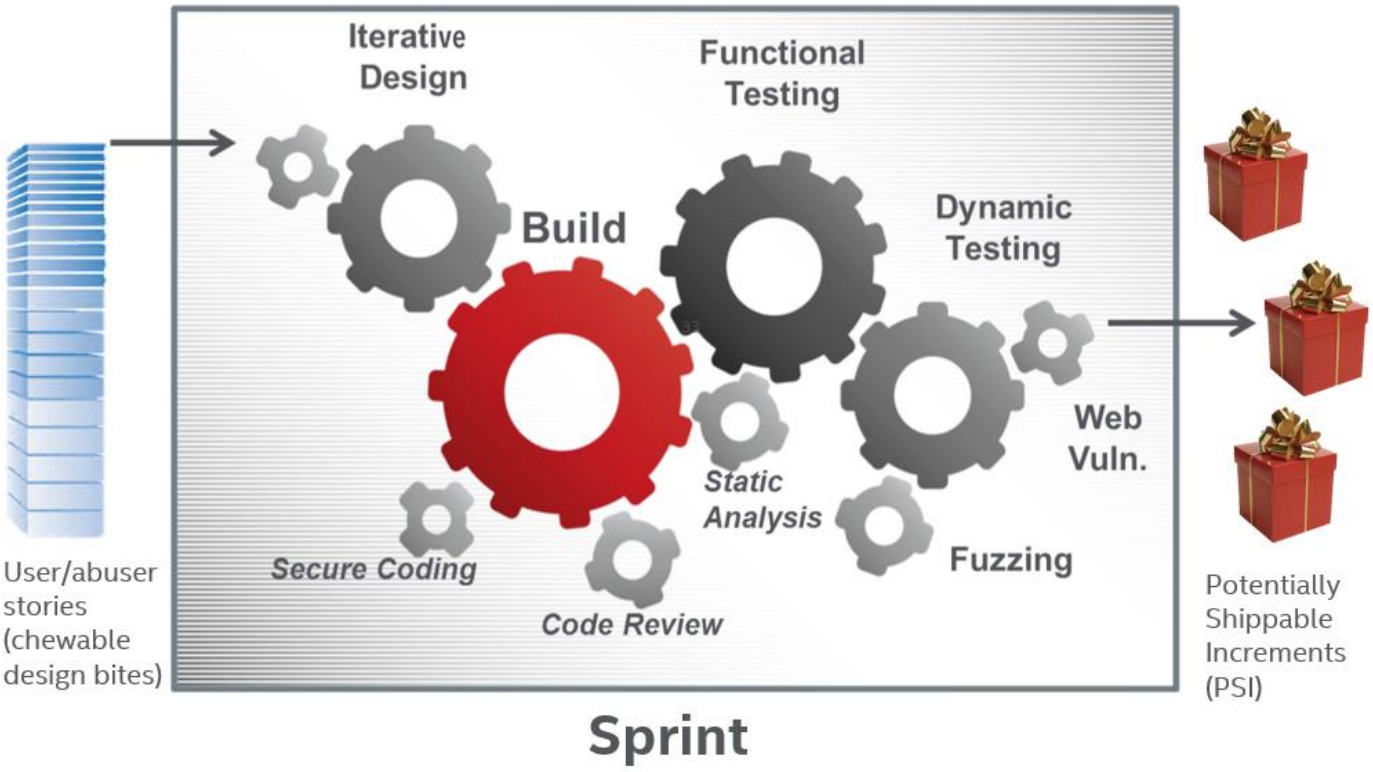


Agile SDL

Any project that involves a change to the architecture of the product is required to go through a security architecture review. The proposed architectural changes are analyzed for security requirements, as well as analyzed within the whole of the architecture of the product for each change's security implications. A threat model is created or updated. The output of this analysis will typically be the security requirements that must be folded into the design that will be implemented. An architecture review may be a discreet event or may be accomplished iteratively as the architecture progresses (Agile).

The Agile SDL requires that designs that contain security features or effects are reviewed to make sure that security requirements will be built correctly. The PSC signs off when the design meets expectations. All functional items, including security design elements, are included in the thorough functional test plan. Like architectural reviews, a design review may be a discreet event or may be accomplished iteratively when design work occurs (Agile).

In tandem with architecture and design reviews, privacy reviews are conducted. A Privacy Impact Assessment (PIA) is performed to determine if any additional privacy activities are required to protect personal data. Privacy reviews cover the whole lifecycle of personal data and often extend beyond the product collecting the data and include backend systems and infrastructure.



Agile SDL Activities

In summary, the Agile SDL technical activities defined for each product release include:

- SDL.T01 Security Definition of Done (DoD)
- SDL.T02 Security Architecture Review
- SDL.T03 Security Design Review
- SDL.T04 Threat Modeling
- SDL.T05 Security Testing and Validation
- SDL.T06 Static Analysis (SAST)
- SDL.T07 Dynamic Analysis – Web Apps (DAST)
- SDL.T08 Fuzz Testing
- SDL.T09 Vulnerability Scan
- SDL.T10 Penetration Testing
- SDL.T11 Manual Code Review
- SDL.T12 Secure Coding Standards (includes cryptography)
- SDL.T13 Open Source and 3rd Party Libraries
- SDL.T14 Vendor Management (includes software legal compliance)
- SDL.T15 Privacy
- SDL.T16 Operating Environment

Product Security Champions

At McAfee, we foster industry standard secure coding practices. To that end, McAfee University and our McAfee Learning Management System (LMS) contains many courses on building software securely. Developers are expected to pursue ongoing developer education. Self-training is encouraged.

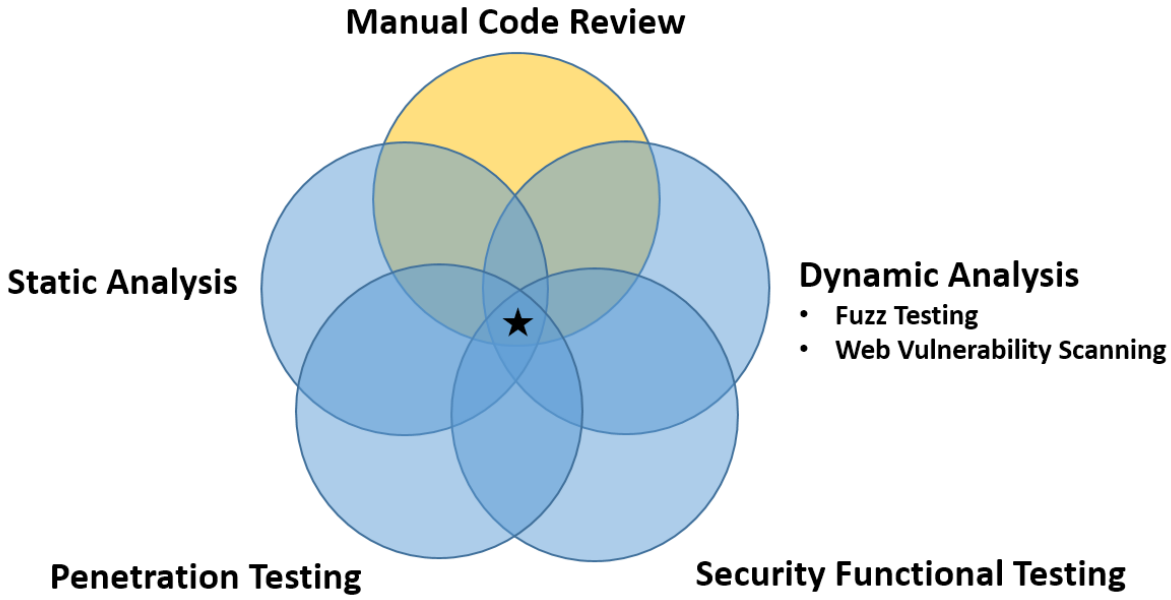
In addition, Product Security Champions (PSCs) are assigned to each product line. PSCs are functionally equivalent to the industry title, “Security Architect”. Our 90+ PSCs performs the SDL activities and help to confirm that every part of the product security process is applied appropriately.

We also have Product Security Evangelists (PSEs), engineers who have demonstrated a passion for software security, but have less experience or are often in Quality Assurance. Our 35+ PSEs are available to assist with secure coding, as well as providing security tool expertise.

"Trust And Verify"

Alongside each developer's responsibility to produce secure code, McAfee has a "trust and verify" attitude. All new code must go through a manual code review. For non-sensitive and/or noncritical functions, this code may solely go through peer review. Critical and/or sensitive changes are also reviewed by staff with a sufficient level of expertise to assess critical changes.

Making use of overlapping complementary approaches, we employ several tools and automation to find security defects that may slip through manual code review. All code must be statically analyzed (unless no static analyzer exists for the language or environment). All web code is expected to undergo a web vulnerability scan. Other forms of input are routinely fuzz tested. High severity issues must be fixed before release. Medium severity issues are prioritized then fixed or mitigated in future patches and product releases. Low severity issues are usually addressed in future product releases.



Complimentary Security Testing

Critical customer-premise releases may additionally be put through a third-party penetration analysis on a case-by-case basis before release. All hosted systems are routinely vulnerability scanned and penetration tested by our Information Security (InfoSec) department or by a third-party engaged by them.

We believe that the foregoing is a solid plan in line with industry standards and best practices. Since no computer system can be absolutely secure, McAfee makes no claim that the Agile SDL will prevent any particular issue or any collection of issues. McAfee reevaluates and updates its SDL policies and process on a regular basis.

McAfee Policies

McAfee believes that customer relations are best served through open, transparent dialog. We encourage customer engagement, including requests about our software security process.

There are some limitations as to what we may share. For instance, we never share our source code outside of McAfee's direct control. Also, we never make available the list of vulnerabilities that are found as a result of our own internal investigations or from any of our automated testing tools. After internally discovered vulnerabilities have been addressed in a hotfix, patch or new product release all medium and high severity issues are document in product release notes and/or a security bulletin.

It is important to note that any scan of McAfee's production systems will be considered an attack. Response to perceived attack will be rapid and decisive. Please coordinate your needs with your account manager. Availability of test systems is subject to customer need, customer cost, and timing.

Software Security Tools

McAfee engineering teams apply an appropriate combination of tools depending upon the target programming language, architecture, and the execution run-time. These tools are a combination of internally developed, vendor purchased, and open source tools. We may provide a list of utilized tools upon request.

Notice

No computer system can be absolutely secure. McAfee 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 McAfee. McAfee makes no warranty that any hardware products or software products will protect against all possible security threats, including intentional misconduct by third parties. McAfee is not liable for any downtime or service interruption, for any lost or stolen data or systems, or for any other damages arising out of or relating to any such actions or intrusions.

Points of Contact

- Dr. James Ransome, Director, Product Security Group, PSIRT, and Application Security, McAfee
- Harold Toomey, Sr. Product Security Architect, McAfee

Glossary

Agile SDL **Agile Security Development Lifecycle**
A software development methodology that condenses the traditional waterfall methodology delivery cycles into weeks instead of month. Used by over 95% of McAfee's software development teams.

PIA **Privacy Impact Assessment**
A privacy review conducted on all products to determine if additional privacy activities are required before a product is release.

PLF **Product Lifecycle Framework**
McAfee's SDLC.

PSC **Product Security Champion**
A senior security architect within McAfee responsible for all security related activities for a given product line.

PSE **Product Security Evangelist**
Engineers who have demonstrated a passion for software security, but are not as experiences as their PSC. They assist the PSCs.

PSI **Potentially Shippable Increment**
An agile term that means that each unit produced from a series of Sprints has a quality of completion. A governance checkpoint determines each release. PSCs participate in release decisions. There is no mandate to release a PSI.

PSIRT **Product Security Incident Response Team**
The team within McAfee that responds to product vulnerabilities in shipping products. They work with the discoverer and engineering to develop and deliver a patch and accompanying security bulletin. The vulnerability's severity (CVSS score) determines our fix response time (SLA). http://www.mcafee.com/us/threat-center/product-security-bulletins.aspx.

SDL **Security Development Lifecycle**
The security aspects of an SDLC.

SDLC **Software Development Lifecycle**
Describes the processes, activities and deliverables for developing, testing and shipping software.