An Overview of InterSystems Secure Development Lifecycle

Executive Summary

The InterSystems Secure Development Lifecycle (SDLC) helps ensure that secure products and services are delivered to customers and end-users. The SDLC reduces the exposure customers face while using InterSystems products and services.

InterSystems is commitment to creating, maintaining and delivering secure products by following best practices in the software industry. New cybersecurity threats are emerging every day and they are becoming more sophisticated--these threats present new challenges that are shared by vendors and customers alike. The InterSystems SDLC is made up of the following seven categories of security practices:

- Foundational Practices
- Product Security Requirements
- Designed with Security in Mind
- Secure Development
- Security Testing and Verification
- Secure Delivery
- Maintenance and Incident Response

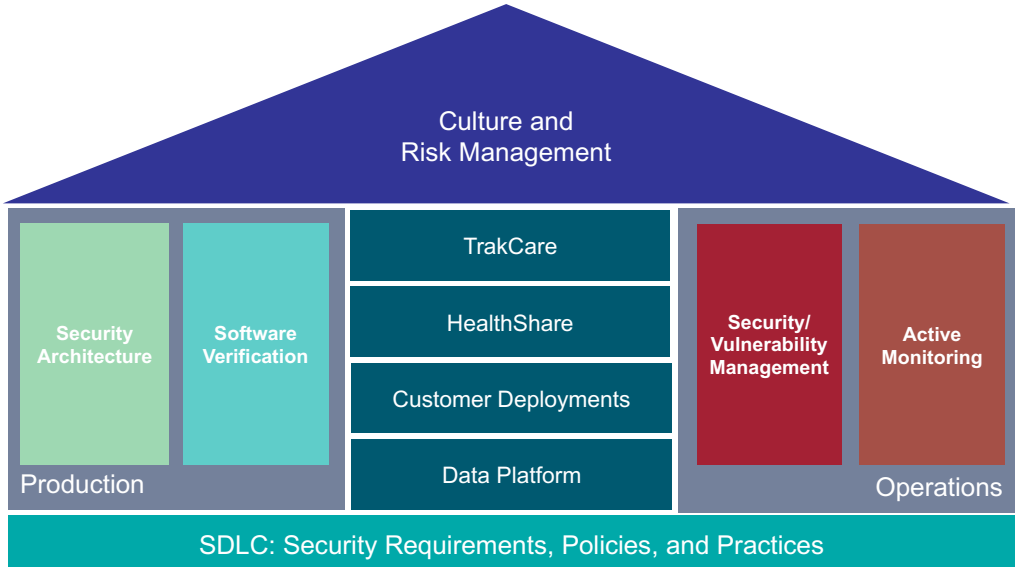
This white-paper describes how the SDLC fits into the InterSystems Security Engineering and Architecture (SEA) framework and then it provides an overview of the security practices in the InterSystems SDLC. Following these SDLC practices, InterSystems is able to deliver products and services with the highest possible security posture.

InterSystems®
Security Engineering and Architecture

FOSTERING A "CULTURE OF SECURITY" IS KEY TO EVERYTHING WE DO. IT EMBODIES THE SPIRIT OF OUR SECURE DEVELOPMENT LIFECYCLE.

The Security Engineering and Architecture Framework

The Security Engineering and Architecture (SEA) Framework is a conceptual model that illustrates how InterSystems executes the practices defined in the SDLC. In other words, the SDLC is the foundation on which the InterSystems approach to product security is built.



The InterSystems Security Engineering and Architecture Framework

In the SEA framework, InterSystems executes the foundational SDLC in various business functions. On the left side of the framework, we include business functions related to the production of our products and services such as security architecture and software testing and verification. On the right side of the framework, we include operational aspects of the business functions such as our incident response program and active monitoring efforts.

The middle of the framework recognizes that the various lines of business and deployment methodologies have different requirements that modify the execution of the SDLC.

Finally, the SEA framework is capped by practices related to fostering a culture of security. Tools and metrics associated with managing the InterSystems security complement the product security culture. The rest of this document focuses on the specific areas of the SDLC.

Foundational Practices

The InterSystems SDLC begins with several foundational elements that facilitate the seamless execution of the other practice areas. The foundational practice area provides the structure and tools necessary to actively manage product security efforts across the company.

The following practices are included in the foundational area:

- An executive sponsor responsible for security
- Infrastructure and systems to track security related risks and tasks
- General secure awareness training provided across the company and training on secure development practices provided to software developers
- Corporate policies include security elements and are followed across the company including in human resources, IT operations, as well as technical development and operations
- The Security Engineering and Architectural (SEA) business function serves as a product security center of excellence. The SEA maintains the SDLC and coordinates efforts related to the execution of the SDLC.

Product Security Requirements

Product security requirements in practice are cross-functional in nature and driven by a stakeholders across the company. For example, the InterSystems product management team has a dedicated employee that is not only focused on managing security issues, but this individual reviews all new features with a security lens. The SEA defines security requirements that engineering teams follow and the quality assurance team defines security testing objectives (execution is a different practice area). Additionally, the Global Trust Organization leads efforts to classify any data that will be stored or accessed by InterSystems employees and makes sure proper security controls are in place. Finally, the security architecture team, engineering and Global Trust Organization collaborate on risk assessments on all new development efforts.

THE INTERSYSTEMS SECURE DEVELOPMENT LIFECYCLE INCORPORATES FEEDBACK LOOPS FROM OUR CUSTOMERS AND THE INDUSTRY TO HELP EVOLVE AND ADDRESS NEW THREATS IN THE ENVIRONMENT.

Designed with Security in Mind

In order to ensure that all our practices are designed with security mindset, our security engineering and architecture team provides a set of security design requirements to the development teams to reference. Intersystems has made a subset of these security requirements available in the development guidelines section of our public secure coding practices policy.

As part of the design process, a group of dedicated security engineers update or create new threat models to review changes in the product architecture with a “hacker mentality” to determine how features might be abused to affect the confidentiality, integrity, or availability of the system.

Secure Development

All system development activities are performed in specialized development environments which are isolated from any customer environment. Intersystems developers follow the secure coding practices policy, a version of which is publicly available.

InterSystems has a dedicated release engineering organization which maintains the creation and deployment of code releases. These systems which orchestrate the build and release pipelines are regularly inspected for unauthorized modification or changes which may compromise the security posture of the delivered software or service. An inventory of third-party software is cataloged in a software bill of materials which is published on our public third-party products web page. This bill of materials is tied to a threat intelligence feed to help manage new security risks in our supply chain.

Security Testing and Verification

InterSystems has a long history of conducting security and functional tests. InterSystems has been evolving the continuous integration platform for over 20 years and it was designed to regularly build each product and platform, perform automated testing, and securely archive the results. In addition to automated testing, a team of security engineers review the results from a variety of commercial static (SAST) and dynamic application security testing (DAST) tools and perform regular penetration testing.

Secure Delivery

Every InterSystems product undergoes a final leadership review before they are release either in sprint reviews or in a dedicated release readiness review. The director of quality assurance, director of product management, and engineering executives review all known issues before they sign off on the release. When possible, each release is cryptographically signed after the security posture reviewed via automated and manual procedures. Every build artifact is hashed and archived--regardless of whether it is an internal, ad-hoc, or public release.

Maintenance and Incident Response

The security landscape is every changing and new threats emerge every day. If a product or service does not continue to evolve to address new threats, the security posture quickly degrades and creates security risks to its users. InterSystems maintenance and incident response practices help ensure that new risks in the environment are monitored, tracked, and addressed. This includes collecting feedback from our customers through our worldwide response center (WRC) and from other external stakeholders through our product security incident response team (PSIRT). More information on how to contact our PSIRT is provided on our PSIRT website.

Cloud Services

InterSystems has adopted a DevSecOps approach to delivering cloud based services. While the mechanisms and systems may vary the practice areas in the SDLC are still executed in an agile software development methodology.

About InterSystems

Established in 1978, InterSystems is the leading provider of data technology for extremely critical data in healthcare, finance, supply chain and other industries. Its cloud-first data platforms solve scalability, interoperability, and speed problems for large organizations around the globe. InterSystems is committed to excellence through its award-winning, 24×7 support for customers and partners in more than 80 countries. Privately held and headquartered in Cambridge, Massachusetts, InterSystems has 25 offices worldwide.

For more information, please visit **InterSystems.com/GT/**

InterSystems®
Security Engineering and Architecture