SECURE DEVELOPMENT

At Motorola Solutions, our philosophy is that security needs to be injected into every phase of development - from before a developer even touches a keyboard, all the way to after a product is in a customer's hands. Each step of the traditional Software Development Lifecycle (SDLC) has security activities that must be completed, and whether we are using agile or waterfall methods, each activity slots into one of the six phases of our Secure SDLC (S-SDLC):

- Training
- Requirements
- Design
- Implementation
- Verification
- Release & Response

TRAINING

The first phase of the S-SDLC is Training. Before any code gets written, our developers receive relevant and current security related training to become aware of common vulnerabilities and how to avoid them. Our training is aligned to the NIST Cybersecurity Workforce Framework (NICE) and our dedicated cybersecurity education team works to make sure our developers have the resources they need to securely write applications. This includes on demand, computer based trainings, instructor led "boot camps", and up-to-date internal resources and references.

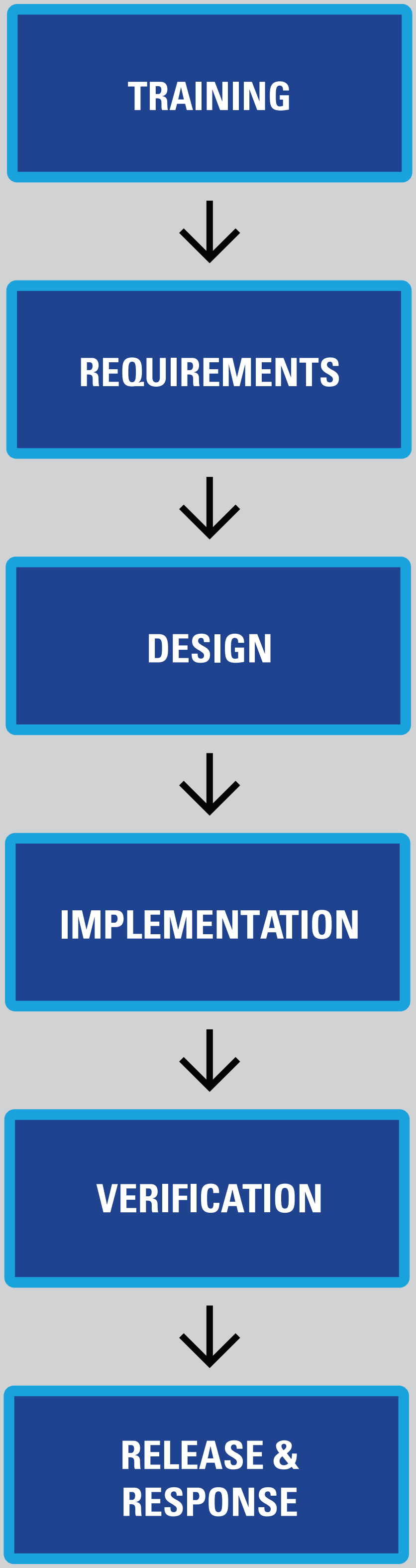
The training "phase" is continuous - our developers never stop learning, and we continue to invest in developing our cybersecurity training. Our belief is that the easiest security bug to fix is the one that never gets made in the first place.

REQUIREMENTS

In a traditional SDLC, the requirements phase is where developers spend a lot of time understanding the exact needs and goals of the customer. In the Requirements phase of our Secure SDLC, we inject high level security requirements that must be taken into account throughout the remainder of the development lifecycle. Our dedicated product Governance, Risk and Compliance program blends risk-based and compliance-based security requirements to put relevant and actionable security guidelines, checklists and best practices in the hands of our engineers and developers. It's important for development teams to understand cybersecurity risk and mitigation options in all aspects of product development. We maintain and provide up-to-date standards, approved frameworks, checklists and guidance that can be followed all the way through the development lifecycle.

DESIGN

As development begins, the design phase of the Secure SDLC is where cybersecurity requirements and controls are being baked in to our products and applications. We perform security architecture reviews of all new products and features, which includes in-depth technical questions and discussions around data flows, security boundaries, and "defense in depth" controls. Threat modeling is also performed at this phase, which may include an in-depth threat model of a brand new solution, or an update to an existing feature. For development teams that follow agile practices, the output of these activities can be documented as security requirement stories and negative use cases.



IMPLEMENTATION

We integrate automated security scanning in our pipelines to provide rapid feedback to developers as they work to implement new features. Our goal is to discover security vulnerabilities as early as possible, and by running scans and checkers in the developers' normal Continuous Integration and Continuous Delivery (CI/CD) pipelines, we can often provide near immediate feedback on code defects, open source usage and dynamic scan results.

We also strive to integrate security testing into traditional unit and integration testing by writing custom test cases based on the stories created during the design and requirements phases.

VERIFICATION

As code is built and the release date approaches, we perform verification of our security requirements through both manual and automated processes. We use industry standard vulnerability scanning tools on completed systems in test labs to identify vulnerabilities and misconfigurations that made it past the implementation phase.

We also have a dedicated red team which performs regular penetration tests and "ethical hacking" of our systems and applications to emulate real attackers to identify flaws and vulnerabilities in our systems after they are built. Lastly, our scanners and processes check our products against regular industry standards, such as CIS Benchmarks and DISA STIGS.

RELEASE AND RESPONSE

The final phase of the Secure SDLC is an ongoing commitment to the security of our products post-release and throughout their entire lifetime. Automated and manual release gates and checklists are in place to ensure products and applications have passed all security checks before being released. After release, we continue to test and probe for weaknesses and vulnerabilities. Our public bug bounty program, external vulnerability scanning process and dedicated threat intelligence team are all used to identify and discover vulnerabilities which may arise in our products after release. Continuous threat monitoring in our cloud and on-prem environments also detect and alert in near real time if any suspicious behavior is detected. All of this leads to the security of our products through regular patching and release cycles.

For more information, please visit us on the web at:
www.motorolasolutions.com/trustcenter

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**