

Where We Were, Are and Going

The Start

- Lack of reciprocity in authorization and assessment results
- Resource intensive
- Redundant and duplicative activities
- Inconsistent policy and process implementation
- Lack of automation (for both workflow and testing tools)
- Lack of standardized documentation and artifacts to facilitate informed decisions
- Three-year "Paperwork Drill"

Current Capability

- Enabled reciprocity and information sharing
- Improve security postures (architecture and information)
- Streamline processes and improve end-product quality
- Uniform set of policies and practices
- Consistent implementation and use of automated tools
- More effective resource allocation; reduce costs
- Continuous monitoring

Coming Up

- Product Awareness and Security Life Cycle Integration
- Threat Modeling with Enterprise Architectures
- Real Time Visibility at Multiple Levels
- Dynamic and Rapid Security Implementation Cycles
- Continued Cooperation and Integration of Resources
- End to End Security Through Technologies