SANS AppSec 2012

Panel: How to Build an AppSec Program Without Getting Fired

Michele D. Guel
Distinguished IT Engineer & Senior Security Architect/Advisor/Evangelist
Communication and Collaboration IT, Cisco

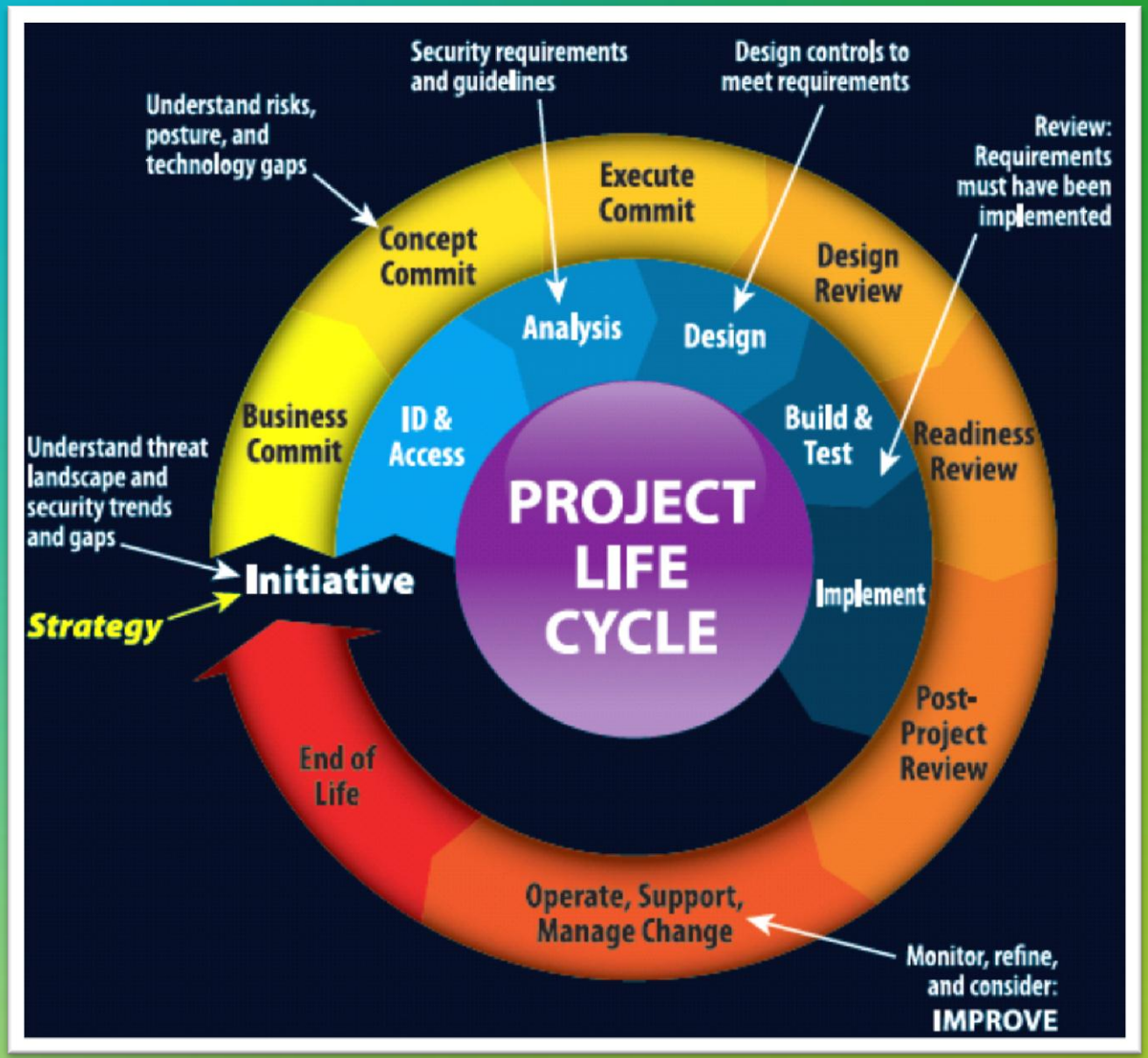
Who am I

- 16 year veteran of Cisco
- Founding member of what is now the Corporate Security Programs Office
- Have worked in multiple facets of information security for 23 years
- Was part of an “experiment” at Cisco to move security people out of corporate group – great learning's
- Total security geek and very passionate
- Current focus is How to Bake in Security and codify the practice

“How Do You Bake Security in the Application Development Process?”

Implement Project Governance

- Project must pass through each gate
- Critical questions at each gate
- Multiple steps of validation
- Security works hand in hand with implementation team.



Ask the Key Questions

1. What data is being collected, transacted on, transmitted, or stored, and for what purpose?
2. What is the highest sensitivity of the data, and the value of the data to the organization?
3. Internally or externally facing?
4. How are authentication and authorization being accomplished?
5. What are the communications channels between each component of the system and do they cross any network boundaries?
6. Does the solution involve an Application Service Provider, Data in the Cloud, SaaS, or an externally facing service or inclusion of 3rd party software?
7. Are there any regulatory laws or statutes that must be met?

Provide the right tools

- Secure coding classes for developers
- Security awareness and educations
- Security” socialization”- the business understand the importance and there is partnership
- Provide tools for early detection of coding issues
- Require a deep, intensive app vulnerability assessment prior to readiness review
- Manage the exceptions and follow-thru

Increase the Visibility

- Metrics and measures that matter
- Report up and across
- Give accolades where appropriate
- Learn from other teams

Thank You!