



SECURITY AND RISK MANAGEMENT IN AGILE SOFTWARE DEVELOPMENT

SATURN 2012 Conference (#SATURN2012)

Srini Penchikala (@srinip)

05.10.12

#WHOAMI

- Security Architect @ Financial Services Organization
- Location: Austin, TX
- Certified Scrum Master
- TOGAF 9 Certified Architect
- Co-Author: “Spring Roo in Action” Book
- Editor (InfoQ.com)



AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

AGENDA

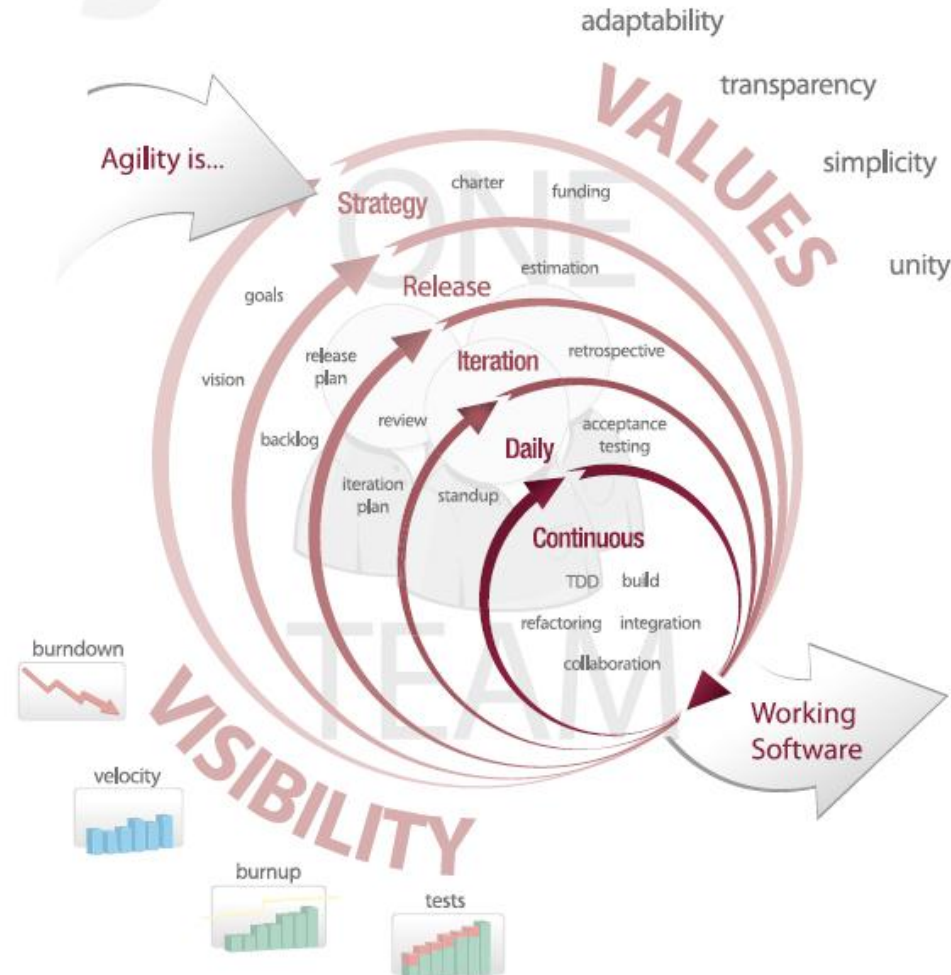
- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

PROGRAM

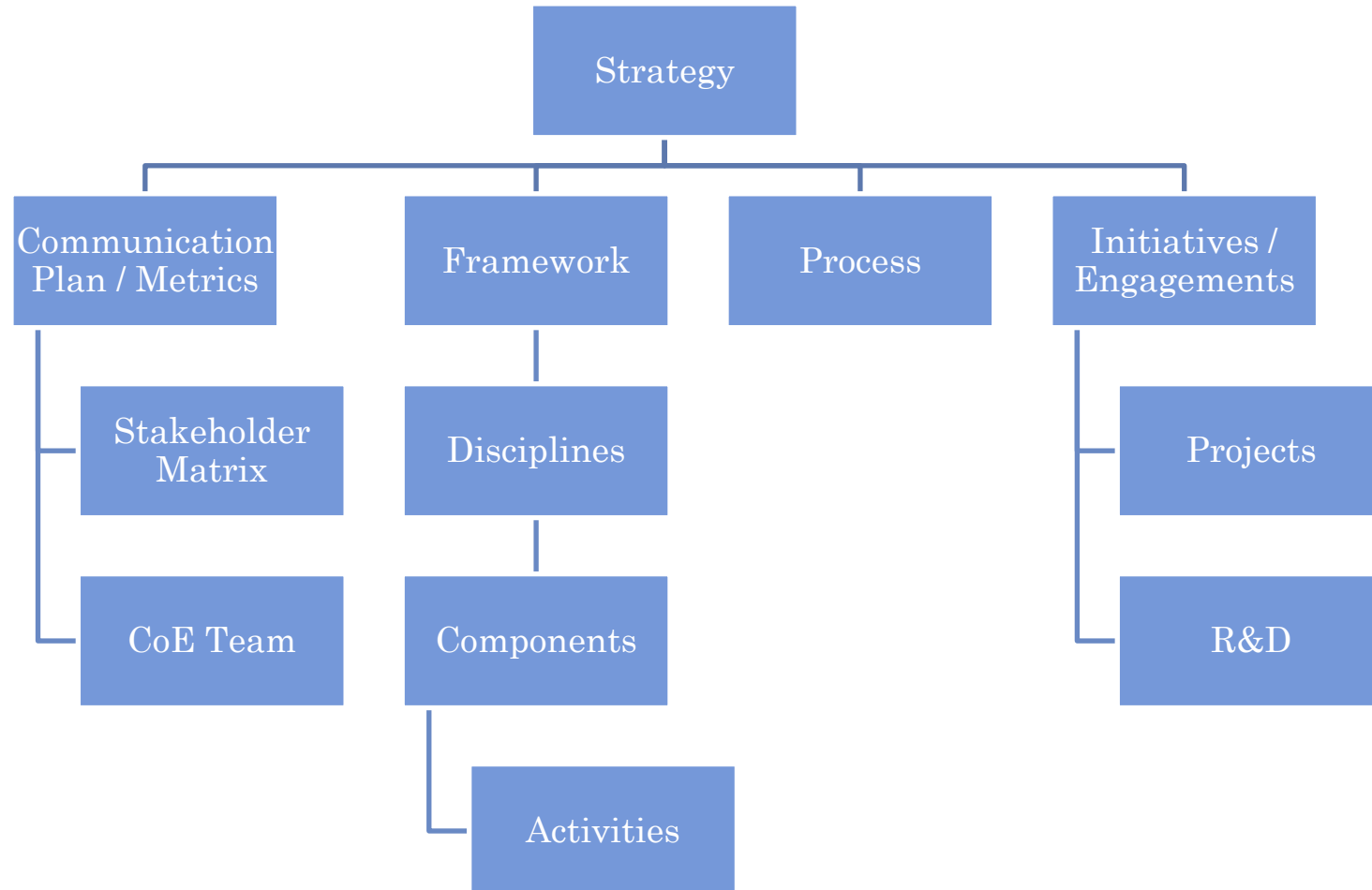
- *Goals:*
 - Security & Risk Management at Enterprise level
 - Build Security In
 - Sustainable Compliance
- Risk based Security Architecture Strategy
- Architecture Framework
- Process

ORGANIZATIONAL AGILITY

- Vertical:
 - Strategy
 - Portfolio
 - Project
 - Release
 - Iteration/Sprint
 - Daily Sprints
- Horizontal:
 - Process
 - People
 - Tools/Technologies



SECURITY ARCHITECTURE PROGRAM



AGENDA

- Security Architecture Program
- **Architecture Strategy and Framework**
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

FRAMEWORK

- Defines “Structure” and “Lifecycle” of the Architecture Strategy
- *Structure*: Framework Components
- Structure:
 - Disciplines
 - Components
 - Activities
- *Lifecycle*: Process Activities
- Components’ mapping with Process Activities

REFERENCE FRAMEWORKS

NIST 800-53

FISMA

TOGAF 9

Microsoft Secure
Development
Lifecycle (SDL)

BSIMM

SAFECode

OWASP
Standards

DISCIPLINES

Security
Assessment &
Authorization

Security
Architecture &
Design

Identity and
Access
Management
(IAM)

System &
Information
Integrity

Systems &
Communications
Protection

SIEM

Technologies
and Tools

Governance

COMPONENTS

Risk
Assessment

Threat
Modeling

Identification
and
Authentication

Data Security

Application
Security

Technologies
and Tools

Standards and
Best Practices

R&D

DISCIPLINES V. COMPONENTS

Security Assessment & Authorization

- Risk Assessment
- Regulatory Compliance

Architecture and Design

- Threat Modeling
- Reference Architecture and RI
- Model Driven Security

Identity and Access Management

- Identification and Authentication
- Access Control
- ESSO

System and Information Integrity

- Data Security
- Encryption
- Application Security

Governance

- Standards and Best Practices
- Reviews (Architecture, Design and Code)
- R&D

STANDARDS

- Standards at all levels of product development
 - Architecture
 - Design & Coding (based on OWASP Standards)
 - Technologies & Tools
- Standards Enforcement
 - Automatic scans
 - Manual Reviews
- Lifecycle:
 - Identify exceptions/waivers at beginning of project
 - Continuous feedback to refine standards (via Agile retrospectives)

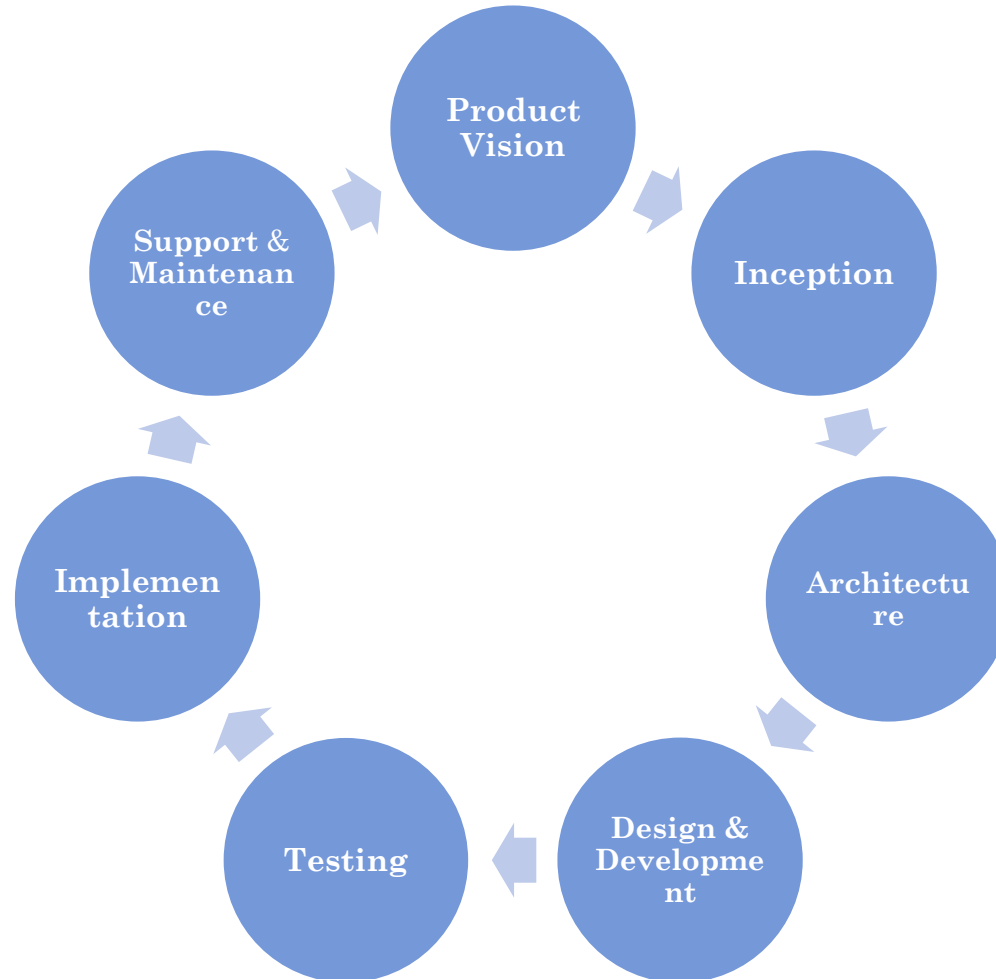
AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- **Development Process Changes**
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

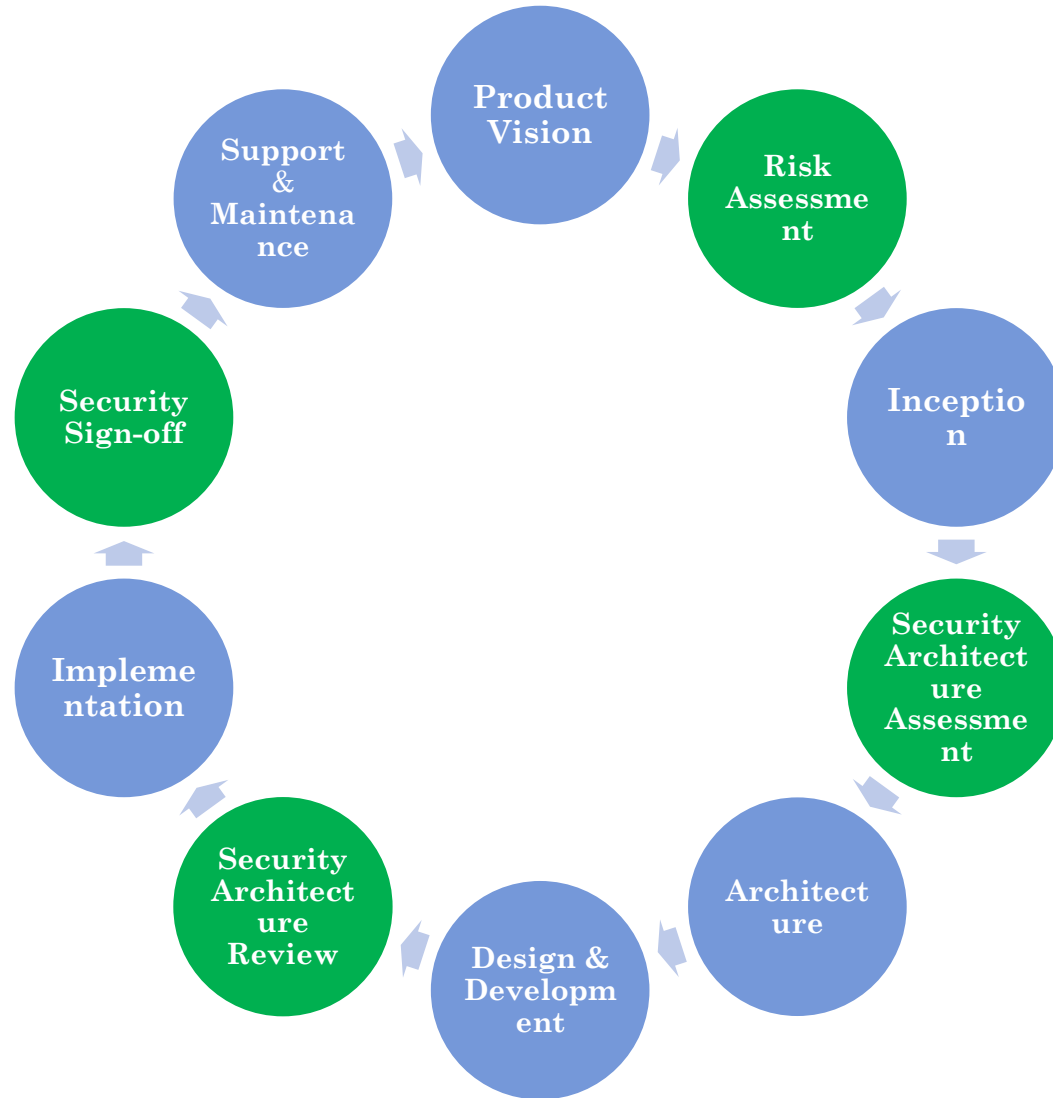
ARCHITECTURE LIFECYCLE PROCESS

- Integrate security risk assessment and management into all phases of product development
- Security touch-points with PMLC & SDLC processes
- Reviews to ensure architecture compliance
- Reviews v. Sign-offs

PRODUCT LIFECYCLE (PMLC)



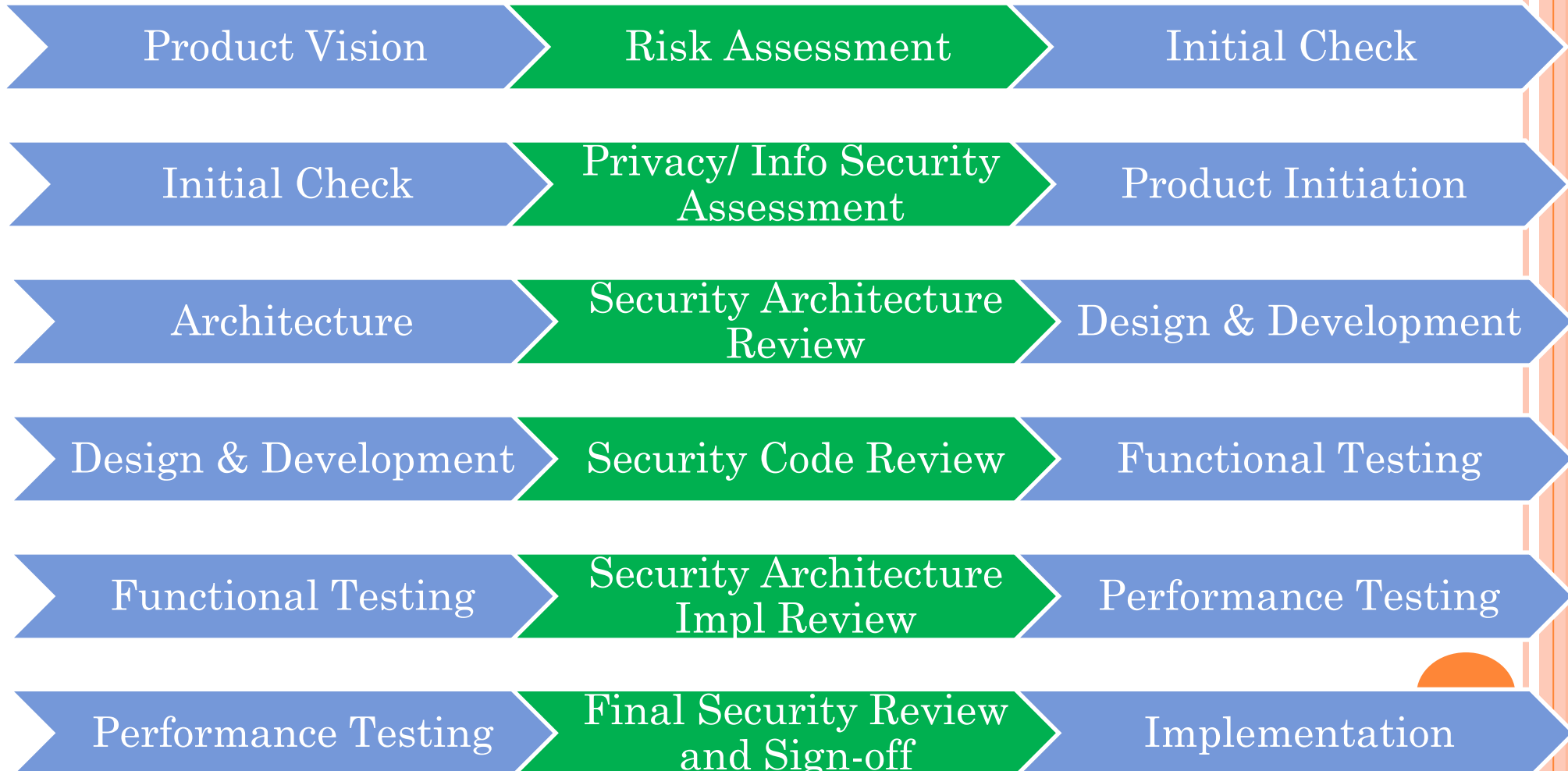
PMLC W/ SECURITY TOUCHPOINTS



AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- **Security and Risk Assessments**
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

ASSESSMENTS AND REVIEWS



AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- **Architecture Centers of Excellence**
- Training and Awareness
- Lessons Learned
- Conclusions

CENTERS OF EXCELLENCE

- Cross-team Security Architecture and Risk Management group
- Champion the management and governance of all aspects of security architecture program
- Core and Extended Teams
- Application, Security and Data
- Business and Technology

CoE CHARTER

- Risk Assessments
- Security Architecture and Design Consulting
- Communicate architecture decisions & guidelines to project teams
- Review & present security architecture related proposals to ARB
- Escalate critical security issues
- Awareness & Education (via Newsletters, Wiki, Brown Bag sessions)
- Security Training
- Security Reviews (Architecture, Design, and Development)
- Threat Modeling (Future)
- Guidance on Code Scans, Pre-deployment Scans & Penetration Testing
- Assist in product development and product acquisition

ENGAGEMENTS

- Collaboration between team members
- Communication at the right places in the process
- Security requirements & test cases during Sprint Planning
- Security architecture walk-throughs
- Architecture retrospectives (end of sprint)
- Projects, Initiatives, Ad-Hoc Consulting
- Governance Model
- Research Labs (for R&D)

AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- **Training and Awareness**
- Lessons Learned
- Conclusions

TRAINING AND AWARENESS

- Education focused - Learning v. Teaching
- Stakeholder specific
 - Business Analyst, Product / Project Manager
 - QA Testing Engineer
 - Technical Lead, Developer
 - DBA, Network Admin
- Topic/Module Specific
 - Requirements Management
 - Testing and Validation
 - Development: User Interface, Services, Data, SQL Injection, XSS
- Internal & External; Online & Classroom based

AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- **Lessons Learned**
- Conclusions

LESSONS LEARNED

- Manual architecture, design and code reviews
 - *Solution:* Automated Static & Dynamic Code Analysis Tool
- Skill set challenges
 - *Solution:* Enhancements to training program
- Assessments overhead
 - *Solution:* Refinements based on project experience

ROADMAP

- Current State: 2+ yrs since the start (3 yrs effort at the previous organization)
- Threat Modeling (Agile Version)
- Security & risk management aspects in:
 - Social Computing*
 - Mobile Development*
 - Cloud Computing
 - NoSQL Databases

* In progress

AGENDA

- Security Architecture Program
- Architecture Strategy and Framework
- Development Process Changes
- Security and Risk Assessments
- Architecture Centers of Excellence
- Training and Awareness
- Lessons Learned
- Conclusions

CONCLUSIONS

- Get commitment from Senior Mgmt. team
- Get involved in the strategic planning process
- Process and Standards are critical
- Automate the process as much as possible
- Agile governance model
- Community of best practices (CoE)
- “Agile or Security” v. “Agile and Security”
- “One Size Fits All” fits nothing

RESOURCES

- Agile Threat Modeling
(<http://www.infoq.com/articles/threat-modeling-express>)
- TOGAF
- SABSA
- The Building Security In Maturity Model (BSIMM)
(<http://bsimm.com>)
- Software Security: Building Security In by Gary McGraw
- Secure Programming with Static Analysis by Brian Chess and Jacob West
- Security Metrics
(<http://www.securitymetrics.org/content/Wiki.jsp>)

THANK YOU

○ Contact Information

- <http://www.infoq.com/author/Srini-Penchikala>
- srinipenchikala@gmail.com
- @srinip
- <http://srinip2007.blogspot.com>

○ Spring Roo in Action Book

○ Questions?

