Bank of America
Security by Design

Derrick Barksdale
Jason Gillam
Costs of Correcting Defects


- Requirements
- Design
- Coding
- Testing
- Maintenance
The Three P’s

- **Product**: Design and build security into our product
- **People**: Cultivate a security mindset in our people
- **Process**: Embed security throughout our process

Security By Design
# The Three P’s

<table>
<thead>
<tr>
<th>People</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Security fundamentals training</td>
<td>✓ Executive/leadership security briefings</td>
</tr>
<tr>
<td>✓ Secure coding training</td>
<td>✓ Socialize security resources and materials</td>
</tr>
<tr>
<td>✓ Security by Design team integration with development and production support teams</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Design security into our product from the beginning: Requirements &amp; Design</td>
<td>✓ Assure security through security testing frameworks</td>
</tr>
<tr>
<td>✓ Design security into our application architecture</td>
<td>✓ Assure security through automated or manual source code analysis and review</td>
</tr>
<tr>
<td></td>
<td>✓ Assure security through live application vulnerability scanning and ethical hacking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Development teams engage the Security by Design team during the Requirements phase</td>
<td>✓ Security check list must be completed by the development team</td>
</tr>
<tr>
<td>✓ Schedule pre-production assessments</td>
<td>✓ Execute security source code analysis</td>
</tr>
<tr>
<td>✓ Triage, track and remediate vulnerabilities during development lifecycle</td>
<td>✓ Triage, track and remediate post production vulnerabilities</td>
</tr>
</tbody>
</table>
Enterprise Security Assessment Cycle

Assessments
- Static Analysis
- Dynamic Analysis
- Manual Ethical Hacks
- Frequent High Volume Scans

Remediation
- Prioritize work based on risk
- Schedule to software release
- Code

Verification
- Retest to verify remediation
Security By Design Integrated with SDLC

- Security Engagement
- Risk Assessment Questionnaire
- Requirements
- Production
  - Targeted MEH
  - Dynamic Analysis
- Design
  - Architectural Risk Analysis
  - Design Review
- Coding
  - IDE Plugins
  - Code Review
- Testing
  - Static Analysis
  - Self-Service
- Production

Bank of America
Security by Design Team Elements

- Security by Design
  - Consulting
  - Engineering
  - Risk & Compliance
Project Engagement:
• Obtain and review the security engagement packet
• Security by Design issues a risk summary report to the Technical Delivery Manager once the security engagement packet is reviewed to ensure potential pitfalls are avoided
• Enter the information in the Security by Design dashboard

Risk Assessment:
• Review the Requirements and High Level Design to ensure key security metrics and design elements are identified.
• Assess the risk of the project (design level assessment) based on the following factors:
  ✓ Third party involvement in coding
  ✓ Connections to external partners
  ✓ Customer facing applications with multiple trust boundaries
  ✓ Size and complexity of the project
  ✓ Number of delivery teams involved
  ✓ New technologies being introduced
Remediation of Security Defects:
• Direct: we fix
• Indirect: we consult while app team fixes

Design & Code Activities:
• Design Reviews
• Code Reviews
• Development/Management of Utility Code (e.g. common validation routine)

Testing:
• Self-Service Static Analysis
• Self-Service Dynamic Analysis
• Targeted Manual Ethical Hack
Application Assessments:
• Risk Rates defects identified for remediation
• Coordinates with Global Information Security assessments team to schedule live application assessment:
  ✓ Ethical Hack (manual /automated)
  ✓ High Frequency Scan

Remediation Tracking:
• Responsible for reporting to channel execs
## Progress and outlook

### What we are seeing
- A decrease in number of application defects during assessments.
- A decrease in severity of the defects found during assessments.
- A better understanding of security best practices across development teams.
- Remediation of security defects before code reaches production.

### What we are doing
- Digging deeper into application functionality and business logic.
- Engaging earlier in the SDLC.
- Beginning to understand, quantify, and remediate risk across additional channels.
- Continue to enhance Security by Design.
Questions?