How Real World Software Security Programs Work

'How has your program evolved over time?'

SANS What Works In Application Security Security Summit
March 2011
Where We Started

- Program staffed with Project Manager
- Sourced consulting help
  - Training materials & delivery
  - SDLC integration assistance
- Bought tools, expensive ones, and didn’t use them effectively
- Voluntary use of tools for code review
- Professional services to test external sites
• Ability to work 1:1 with developer peers
  – Awareness and consulting
  – Hands on guidance with tool usage
  – ‘Making the problems real’
• Tool-assisted static code analysis
• Pen testing
• Training
• Volunteer program was an abject failure
• Problem statement not well understood
• Cost and time pressures an additional barrier to adoption
• Software security deliverables built in to SDLC
• Deployment of achievable objectives
• Risk based approach
• Spent a lot of time looking for the perfect training - pretty good *is* good enough
• CBT is a crucial tool
• Hands-on experience key for early adopters
• Presentations, seminars, user groups are all opportunities to get the message out
• Videos, checklists, user guides
Where Do We Go From Here?

- Metrics and Reporting
- Ensuring security of outsourced development
- Effective management of Open Source vulnerabilities
Greg Ruddell
Director – Application Services
Information Security
RBC

greg.ruddell@rbc.com
(416) 348-4602