Developing an Application Security Strategy for Large Enterprise Systems

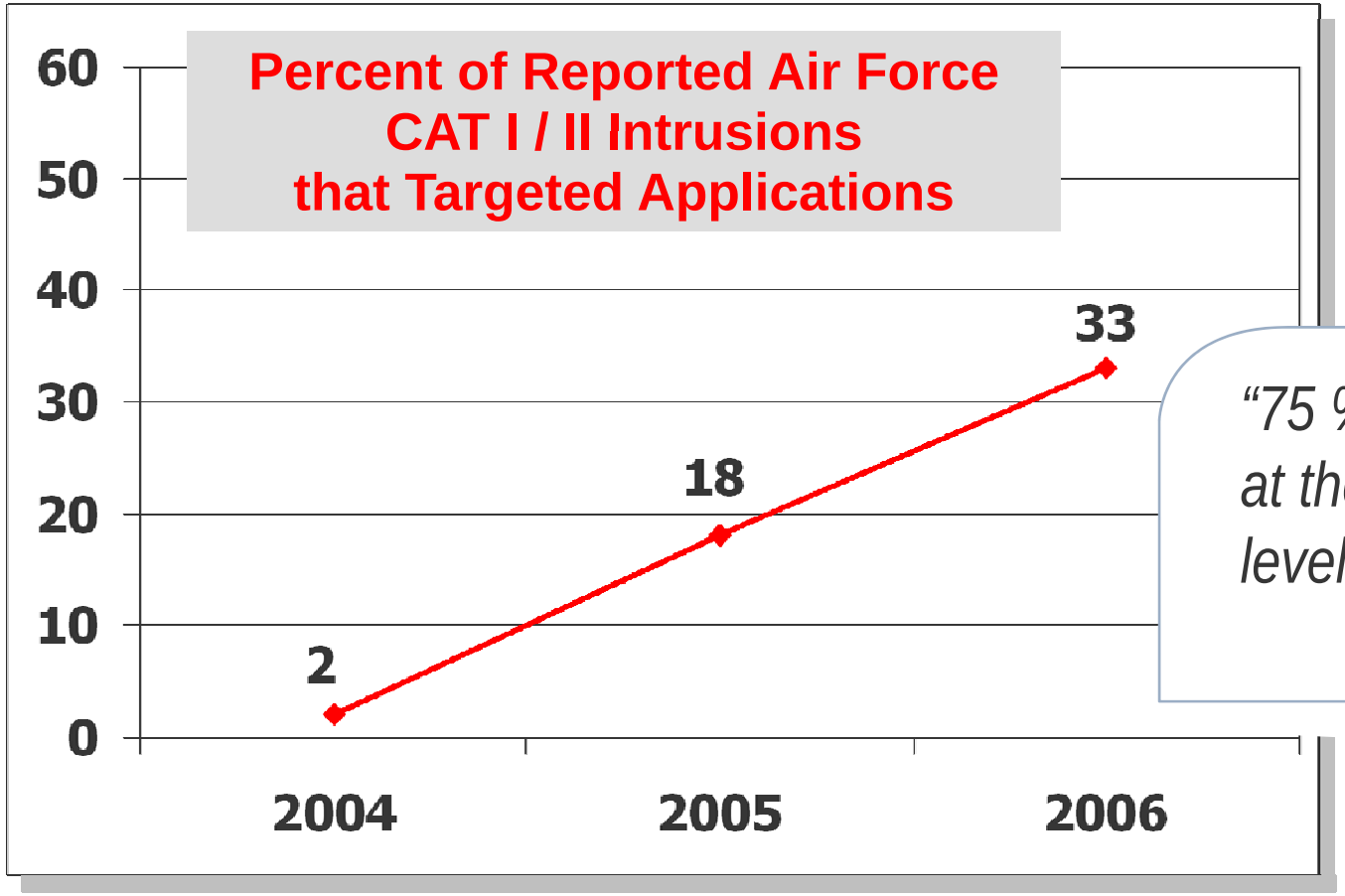
Major Bruce C Jenkins (USAF, Ret.)

San Antonio OWASP, 06 Sep 2007

Overview

- **Organizational Context**
- Deployment Challenges and Assumptions
- Getting Down to Business

Security Wake-up Call



"75 % of hacks occur at the application level…"

Gartner

Dec 2005

FORTIFY SOFTWARE

Security Wake-up Call

May 2005: Air Force Assignment Management System (AMS) Compromised

- Unauthorized individual accessed valid user account
- Initiated Password Reset
- Downloaded 33,000 personnel records

System Access Controls Complied with Published Guidance

FORTIFY SOFTWARE

Systems Development Profile

- **Program Management Offices: 50+**
- **Software Developers: 600-900**
- **Automated Information Systems: 120+**
- **Programming Languages: 12+**
- **Source Lines of Code: 40M+**

Quick Fix Countermeasures

- **Activated 554 ELSW Crisis Action Team**
  - Program Management Offices
  - Security Analysts
  - AFOSI Liaison to the AFNOSC-NOD
- **Top-to-Bottom Review of all Wing Apps**
  - Review Password Reset Procedures*
  - Revalidate Privileges*
  - Review of System Audit Logs*
  - Reduce Concurrent Log Ons
- ***Develop Long-term Security Strategy***

*AFMAN 33-223 Requirements

FORTIFY SOFTWARE

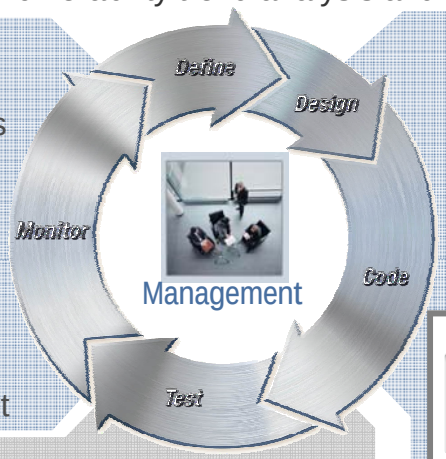
Way Ahead: Securing the SDLC

Centralized Project Management
Vulnerability trend analysis and reporting; view multiple projects, all mission areas

Application Defense
Monitor, prevent and report on intrusion attempts against applications / databases

Security Ops Team

Application Virtualization
"Wrap" legacy apps in virtual environment for low-cost SDC compliance

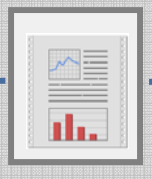


Developers

Source Code Analysis (SCA)
Proactive security with targeted, accurate analysis tuned for low false positives

PR

Security Testers



Build Server

Code Auditing
Pre-build security auditing and analysis of application's entire code base

Penetration Testing
Scripted, controlled external probing of the application's security features

RunTime Analysis
Black box integration testing and vulnerability analysis

Security Leads / Auditors

FORTIFY SOFTWARE

Overview

- Organizational Context
- **Deployment Challenges and Assumptions**
- Getting Down to Business

Challenges and Assumptions

- **Challenges – Some you can change, most you cannot; however, if necessary, you can work around all of them**
  - Cultural
  - Financial
  - Political
  - Time Constraints (schedules)
  - Internal Policy
  - Personal
- **Assumptions**
  - Everyone above you in the food chain is on board
  - You have at least *some* resources

Overview

- Organizational Context
- Deployment Challenges and Assumptions
- **Getting Down to Business**

Getting Down to Business

Success is often the result of taking a misstep in the right direction.

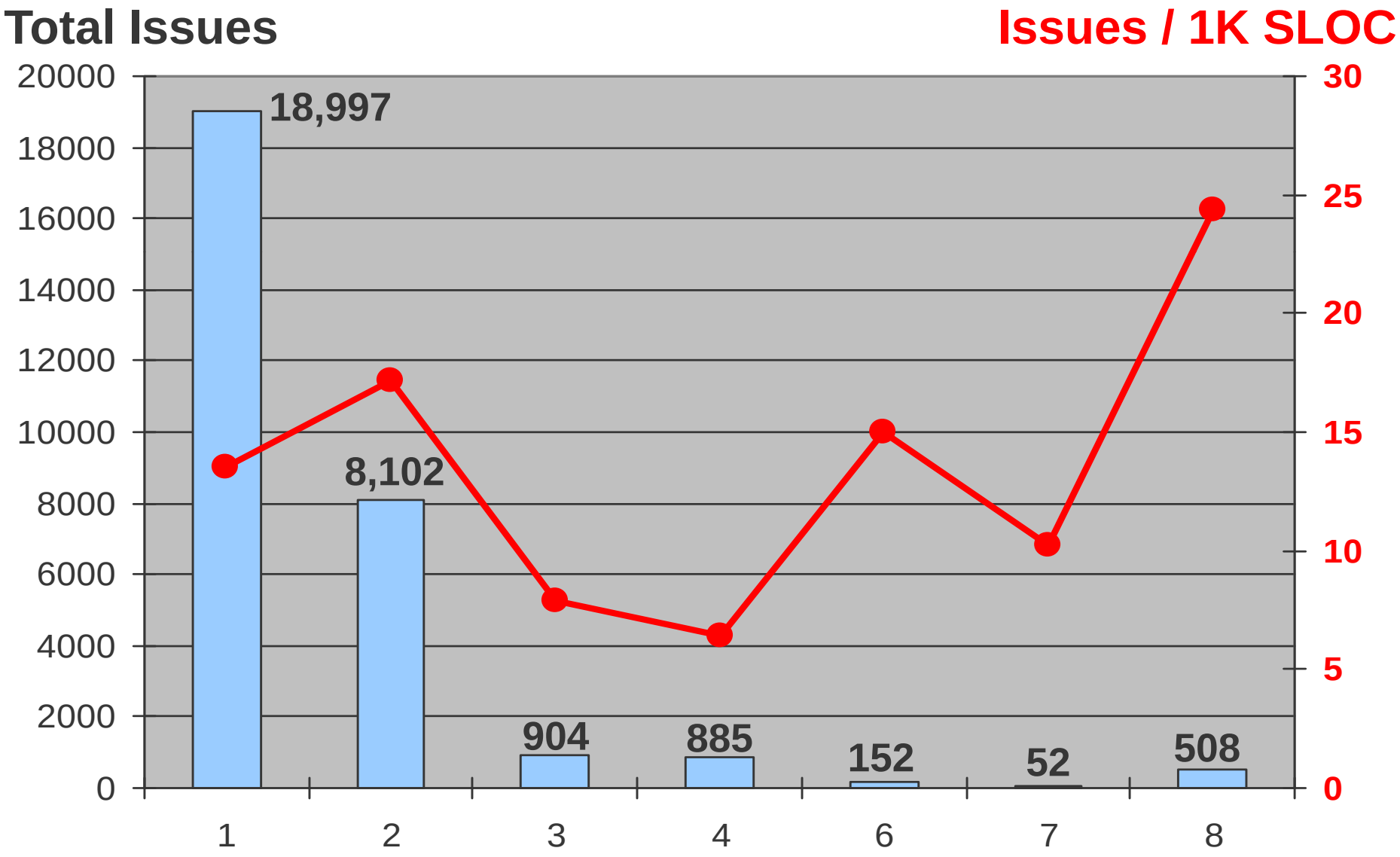
-- Al Bernstein

Getting Down to Business

1. **Determine the Strategic Objective**
2. **Deal with the Challenges**
3. **Identify your Champions… and your Detractors**
4. **Sell Hard to Key Leaders**
5. **Sell Soft to Developers**
6. **Target Early Successes**
7. **Conduct Lessons Learned**

Take Baby Steps… but do something!

Data are just data—don't be overwhelmed....



Questions?