SOFTWARE SECURITY ASSURANCE SUMMIT
March 1, 2011 | Westin Huntsville | Huntsville, AL
T.E.N. presented by FORTIFY An HP Company

Software Security and Federal Compliance

Rob Roy
Federal CTO
HP Software

Who is Rob?

- French, not Scottish
- Yes, I've read the book, seen the movie, tasted the drink
- 10 years Navy – Comms and Crypto
- 20+ years hardware/software
  - Numerous startups
  - Big Co's – IBM, Oracle, Microsoft, HP
  - Focus on representing defense solutions

State of the Art 2011

- Appendix III to OMB Circular No. A-130
- FISMA
- NIST 800-53
- NIST 800-53A
- NIST 800-37
- NIST 800-64
- NIST 800-115
- DISA STIG Application Security
- DoDI 8510.01 (DIACAP)
- HSPD-7
- HSPD-12
- ICD 503

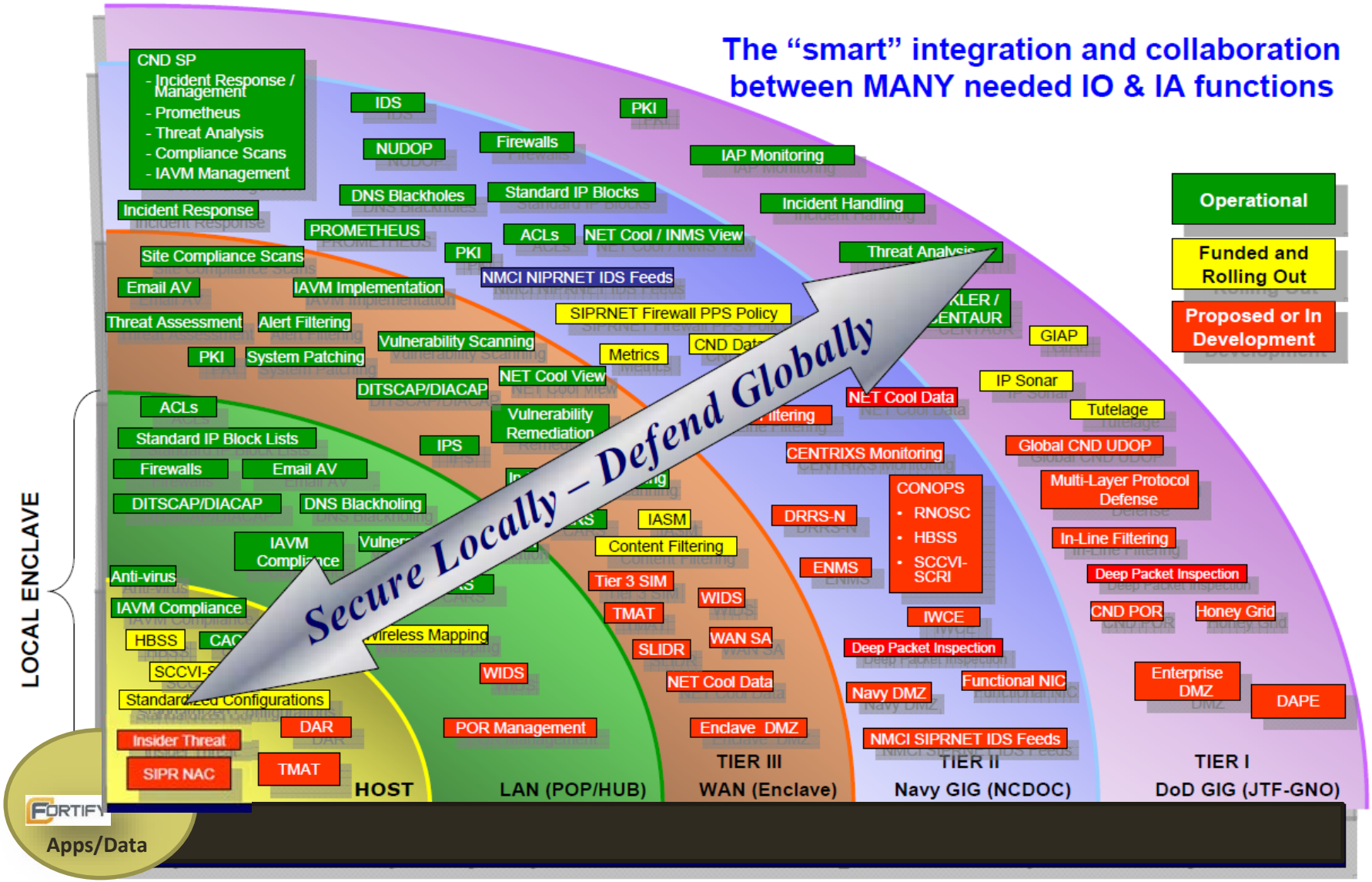
"…agencies should not bolt-on security afterwards…

*Frankly, security investments are **best when they are actually baked in to the systems** that we're looking at and not where they are treated as discrete investments across the board."*

Vivek Kundra
Federal CIO

TESTIMONY ON 2010 FEDERAL INFORMATION SECURITY AMENDMENTS ACT (H.R. 4900)
HTTP://WWW.NEXTGOV.COM/NEXTGOV/NG_20100325_7218.PHP?FBC_CHANNEL=1, 2/25/2010

DoD CND (and "Cyber") Defense in Depth

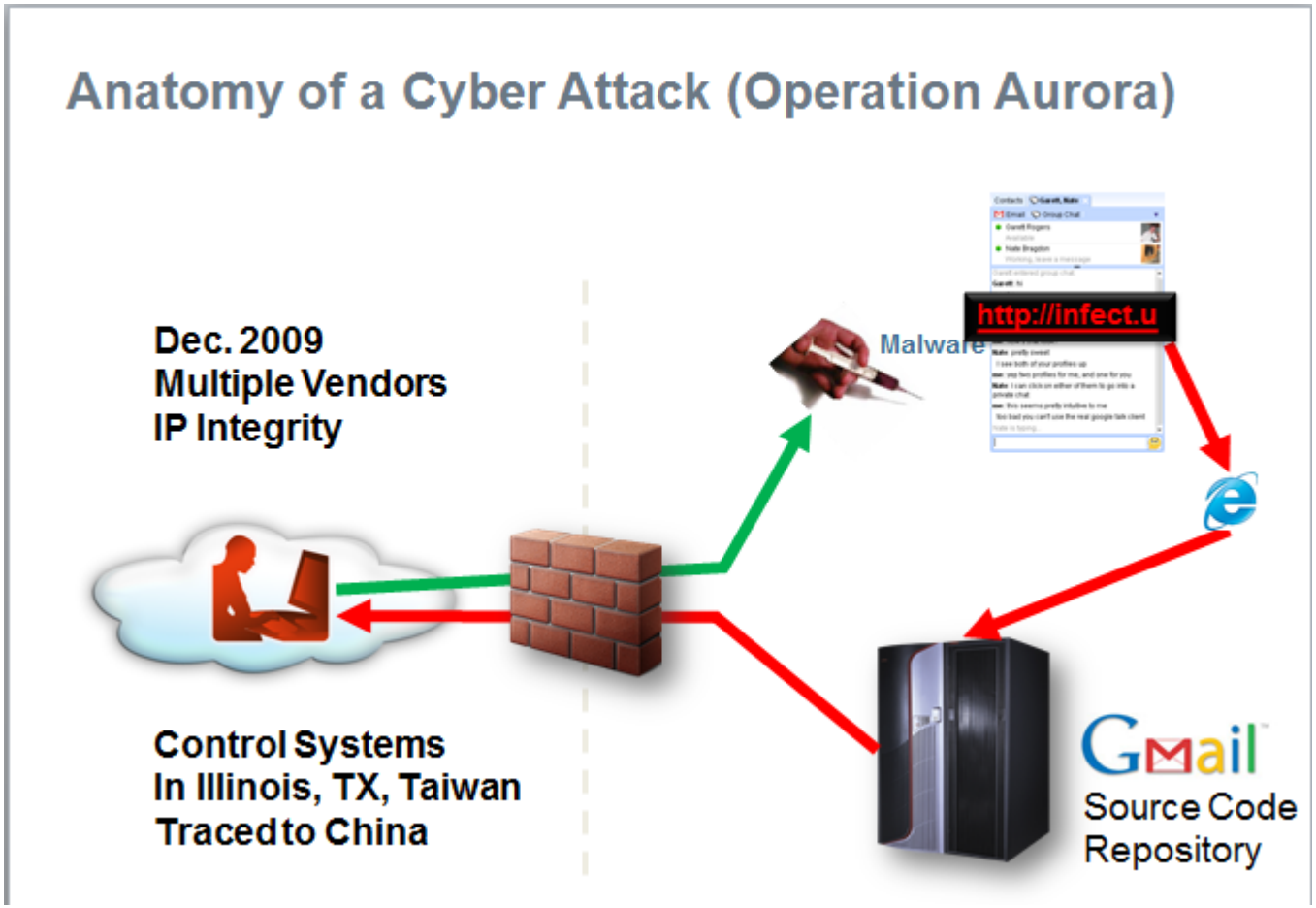


(From NCDOC briefs)

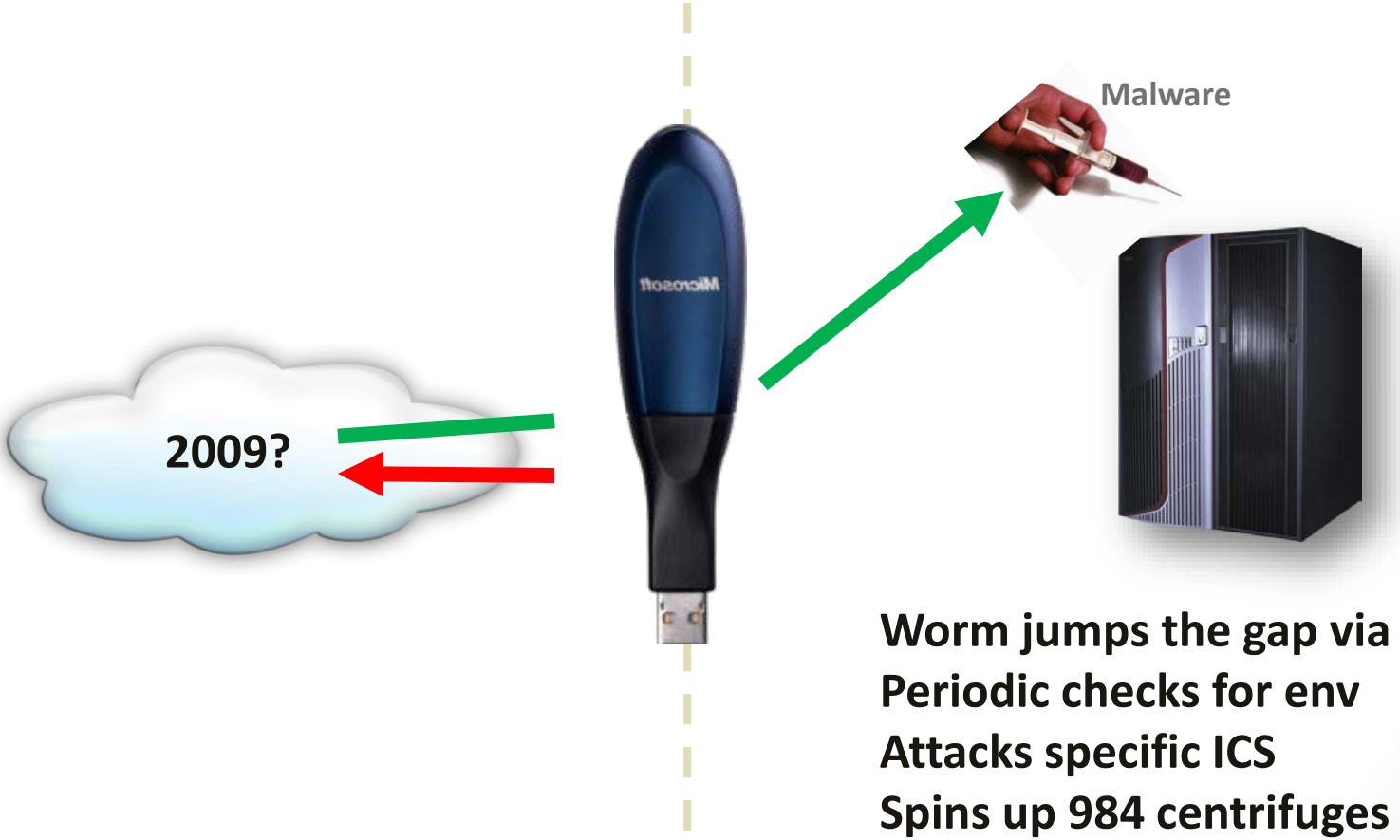
SSA Definition

- ***Software*** – the code that we develop, buy, or get for free
- ***Security*** – being free of dangers, threats, or vulnerabilities
- ***Assurance*** – positive declaration of justified confidence

Could This be You?



Anatomy of a Cyber Attack (Stuxnet)



Worm jumps the gap via USB
Periodic checks for env
Attacks specific ICS
Spins up 984 centrifuges
Displays fake status to control

Main Drivers?

- Financial
- **Intellectual Property**
- **Cyber Advantage**

Some Barriers to Adoption

- Education
- Cost
- Where to start

Foundation for an SSA Program

Critical SSA Practices

Forging an SSA Program

- ***Given:***
  - Federal regulations are splintered when it comes to software security
  - A complete SSA Program should account for all 12 key security practices
- ***Therefore:***
  - Formulate a set of controls (detective and preventative) for your organization
  - Map these controls back to regulations (where they exist) for compliance auditing
  - Implement the controls in your organization
  - Assess and monitor the controls continuously (and tune them as needed)

SOFTWARE SECURITY ASSURANCE SUMMIT
March 1, 2011 | Westin Huntsville | Huntsville, AL
T.E.N. presented by FORTIFY An HP Company

SSA Quick Wins & Getting Started

Governance

Education & Guidance

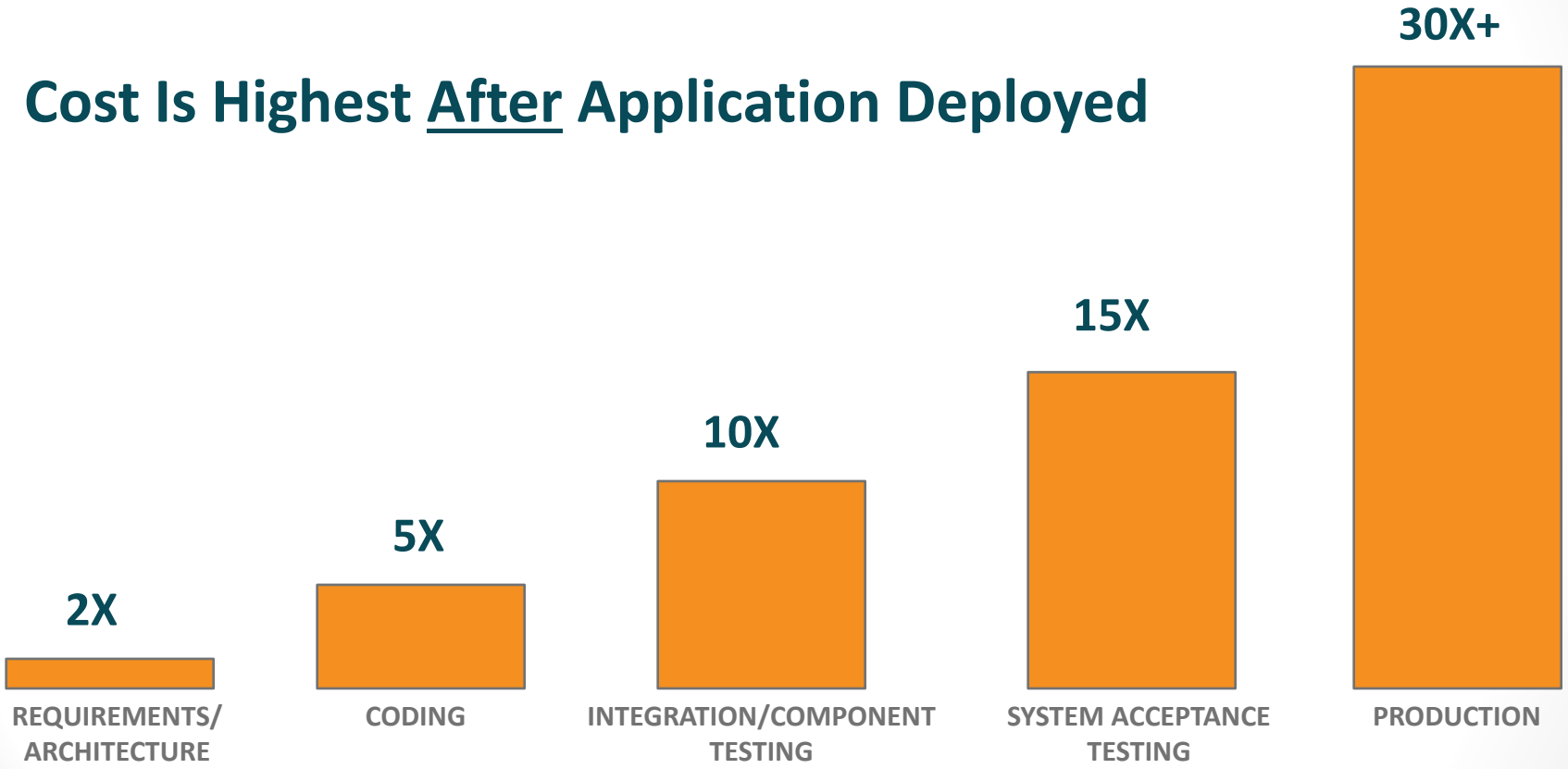
EG 1

- Educate ALL programmers
- Leverage HR for on-ramping of employees
- Budget time to bring legacy employees up to speed
- Develop project-specific guidance, e.g., How-Tos
- OWASP Top Ten 2010
- OWASP Development Guide

Cost of fixing vulnerabilities

Code Fixes After Release = 30X Fixes During Design

Cost Is Highest After Application Deployed



Source: NIST

Construction

Security Requirements

SR 1

SR 3

- Identify how common security tasks will be accomplished
- Integrate into the IDE and automate
- Identify and mitigate common weaknesses in chosen programming languages
- Specify requirements for protecting data at rest and in transit

Verification

Security Testing

ST 1

- Provide specific remediation advice !
- Perform security testing in QA
- Correlate black box and white box results
- Use automation to inform manual testing

Deployment

Vulnerability Management

VM 1

- Establish process for scanning and reporting on Web architecture
- Establish process for Web-architecture security incidents
- Establish process for inventory and tracking of applications

Go dos

- A journey of a thousand miles…
- Assess where you are today
- Develop a gap analysis
- Prioritize quick wins
- Understand the costs associated with inaction
- Champion software security policy
- Ensure that policy flows to contracts

?

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

-Sun Tzu