You knew the job was dangerous when you took it!

Defending against CS malware

Presented By:

Doug Cavit
Microsoft

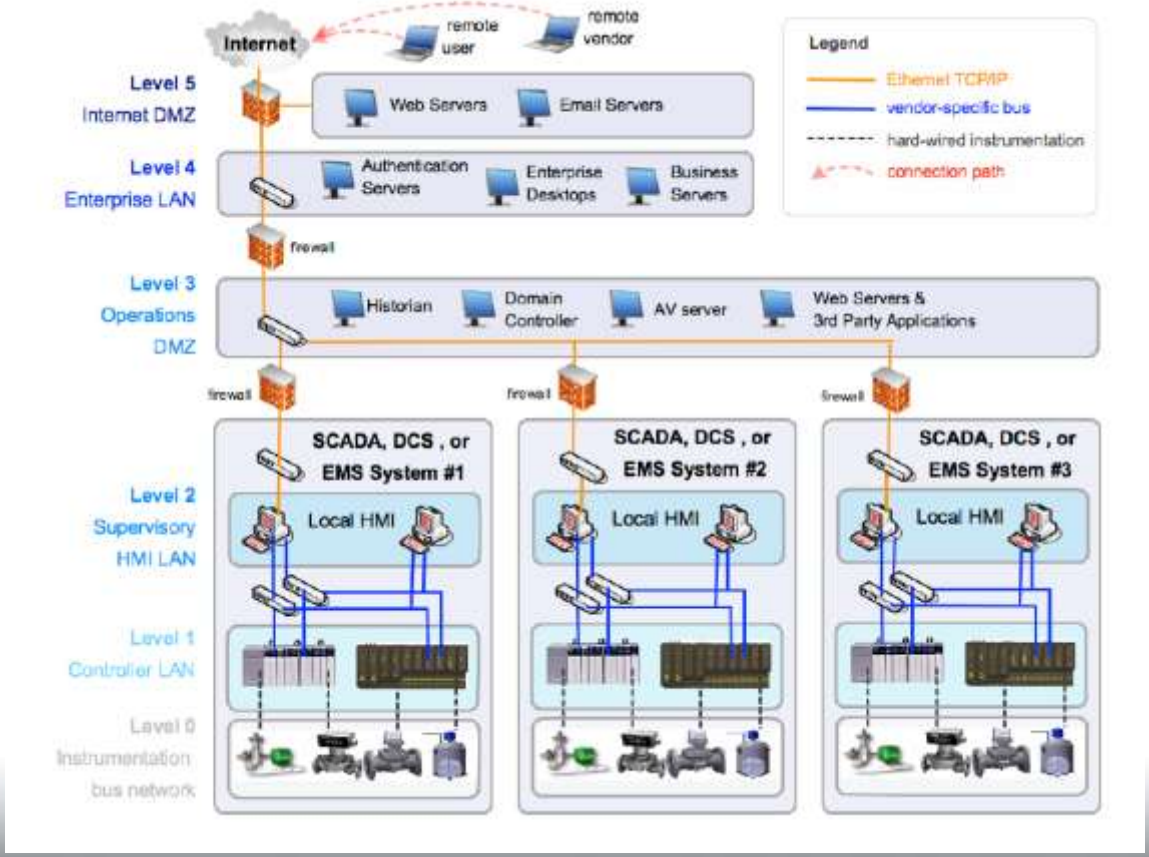
OSIsoft®

NERC HILF 6/10

"Adequately addressing vulnerabilities will also require close coordination with technology vendors and developers. Ensuring protections are "***built-in***" to system components purchased by asset owners as opposed to requiring a "***bolt-on***" solution in the future will significantly enhance the security of the system."

Threats Via ISA S99 Model

- Almost half of the vulnerabilities are found in the Operations DMZ which is also a pathway from the Level 5 to the lower level systems



Stuxnet Learnings

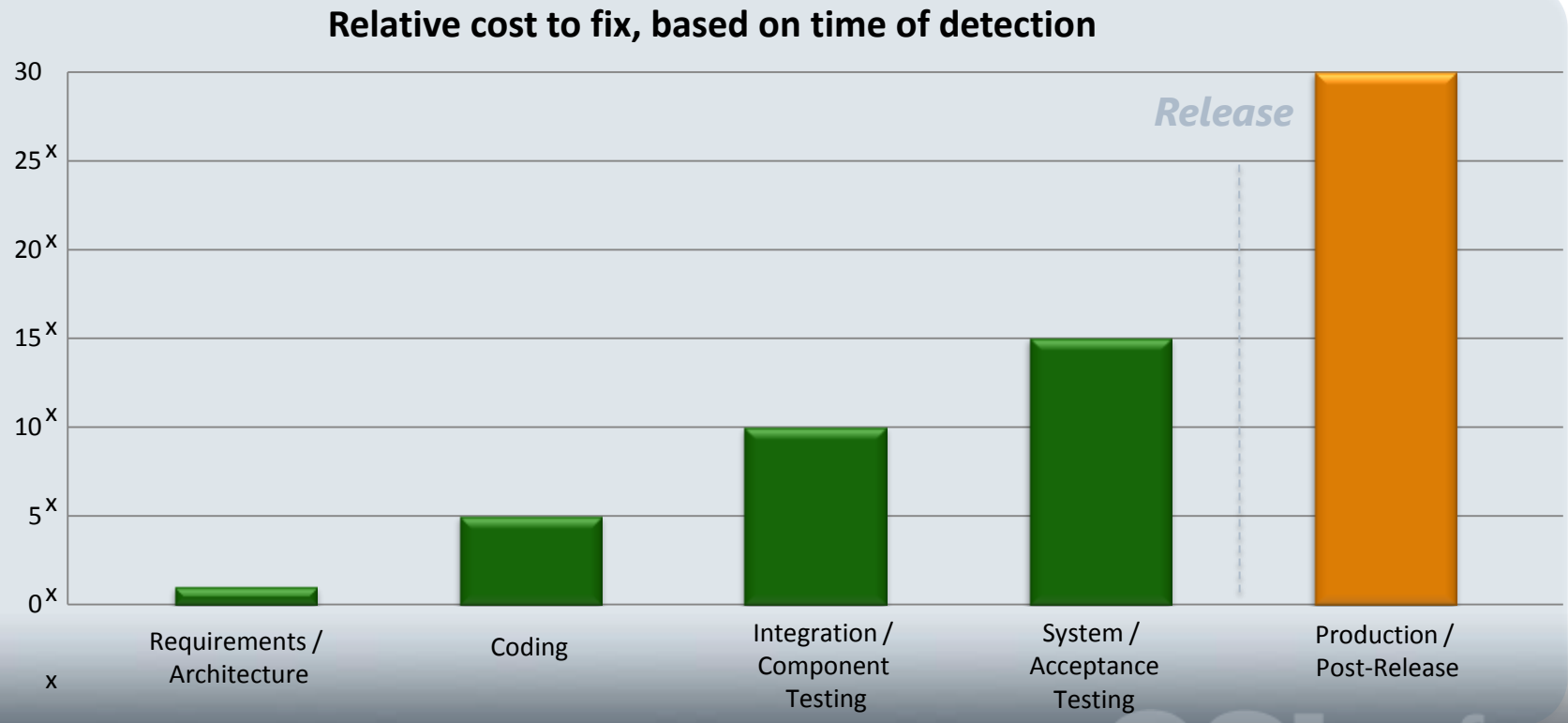
- New, undiscovered Windows vulnerability
- Stolen 3rd party root certificates
- Hard coded DB password in control app
- Issues in software updating policies
- Gaps in response planning & capabilities

MidAmerican SDL Story

- Suffered web data breach in May ‘08
- Surveyed industry best practices and choose SDL
- Began crash program in training, design, tooling, QA practices
- Reshaped engineering culture
- 15,000 issues to less than 100 in 18 months
- 20% more dev productivity now than before
- Recent 3rd party audit found no significant issues
- New corporate standard practice

Software bugs are expensive

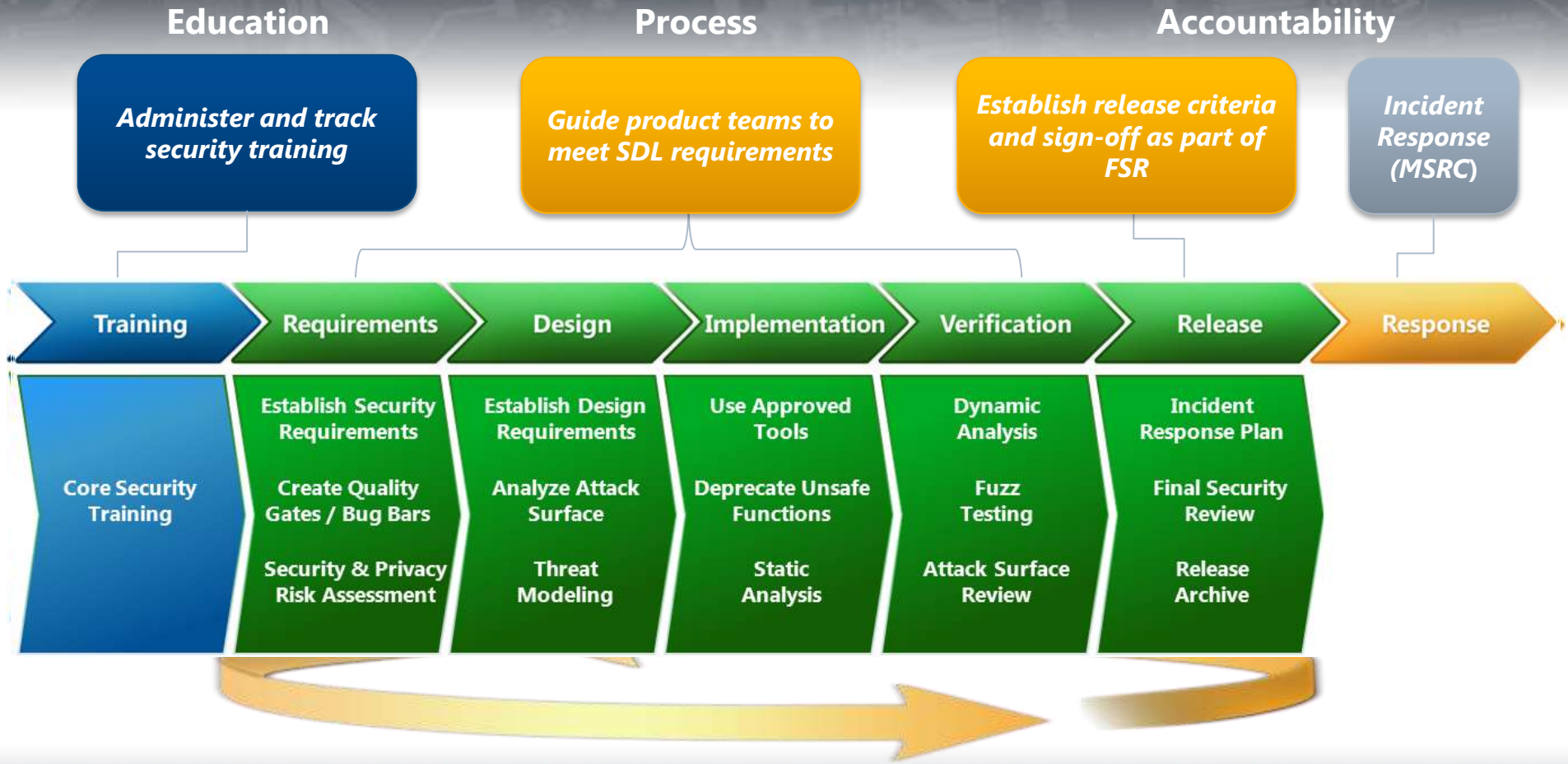
Code fixes performed *after release* can cost up to *30 times* more than fixes performed during the design phase.



Source: National Institute of Standards and Technology

Working to protect our users…

Reduce vulnerabilities, *limit* exploit severity



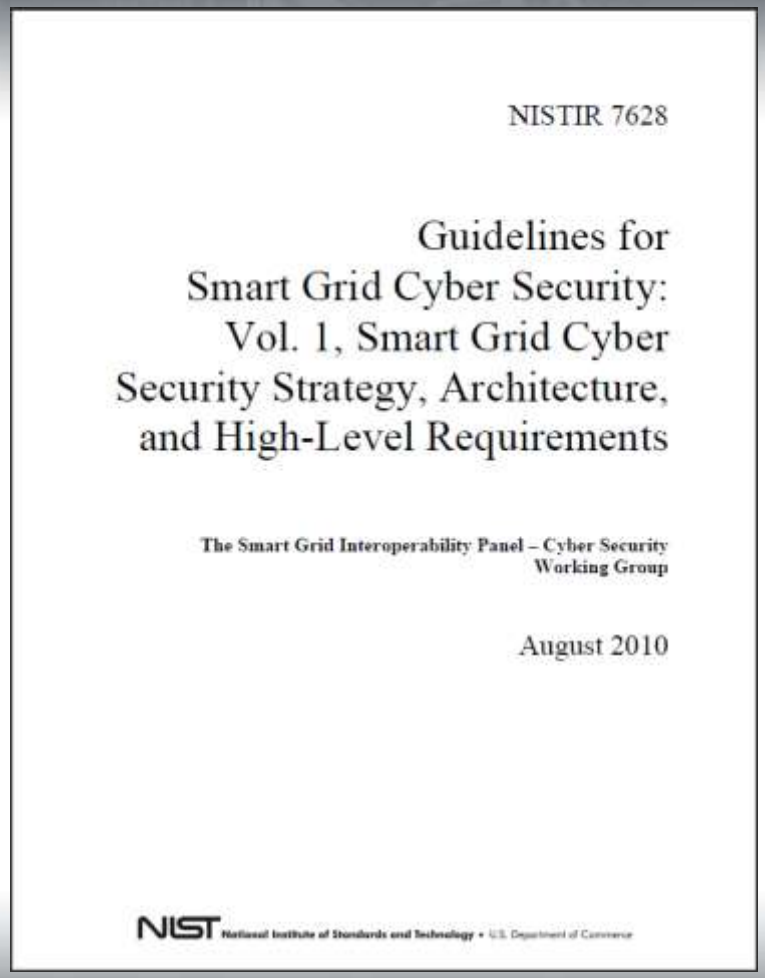
Ongoing Process Improvements – 12 month cycle

OSIsoft®

Motivation for Action

- The application space is under attack, things are bad, and getting worse
  - Users now expect security *without* having to pay for it
- Software security and holistic development practices are becoming a competitive differentiator
  - Procurement
- Showing up in government regulations
  - DISA STIG
  - NIST Smart Grid Requirements
  - NERC/CIP & NERC/HILF
- Failure to show forward momentum will lead to unintended consequences and loss of consumer trust

NIST – Smart Grid Cyber Security Guidelines



SG.SA-8 Security Engineering Principles

Requirement

The organization applies security engineering principles in the specification, design, development, and implementation of any Smart Grid information system.

Security engineering principles include:

1. Ongoing secure development education requirements for all developers involved in the Smart Grid information system;
2. Specification of a minimum standard for security;
3. Specification of a minimum standard for privacy;
4. Creation of a threat model for a Smart Grid information system;
5. Updating of product specifications to include mitigations for threats discovered during threat modeling;
6. Use of secure coding practices to reduce common security errors;
7. Testing to validate the effectiveness of secure coding practices;
8. Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements;
9. Creation of a documented and tested security response plan in the event vulnerability is discovered;
10. Creation of a documented and tested privacy response plan in the event vulnerability is discovered; and
11. Performance of a root cause analysis to understand the cause of identified vulnerabilities

Call to Action

- “Defense in Depth” has to mean something
- Implement a holistic security process
- Software updating at every level matters
- “Security through obscurity” is over
- Ask hard questions about your supply chain’s security processes
- Root cause analysis and process change are critical

Resources

SDL Portal

http://www.microsoft.com/sdl

SDL Blog

http://blogs.msdn.com/sdl/

SDL Process on MSDN (Web)

http://msdn.microsoft.com/en-us/library/cc307748.aspx

Simplified Implementation of the Microsoft SDL

http://go.microsoft.com/?linkid=9708425

Resources

Energy Sector Guidance

[Smart Energy Reference Architecture (SERA)]

Threat Modeling in Infrastructure

[IT Infrastructure Threat Modeling Guide]

Thank You!

OSIsoft®