



The Security Division of EMC

Panel: *SwA Practices - Getting to Effectiveness in Implementation*

(EMC's Evolution of Product Security
Assurance)

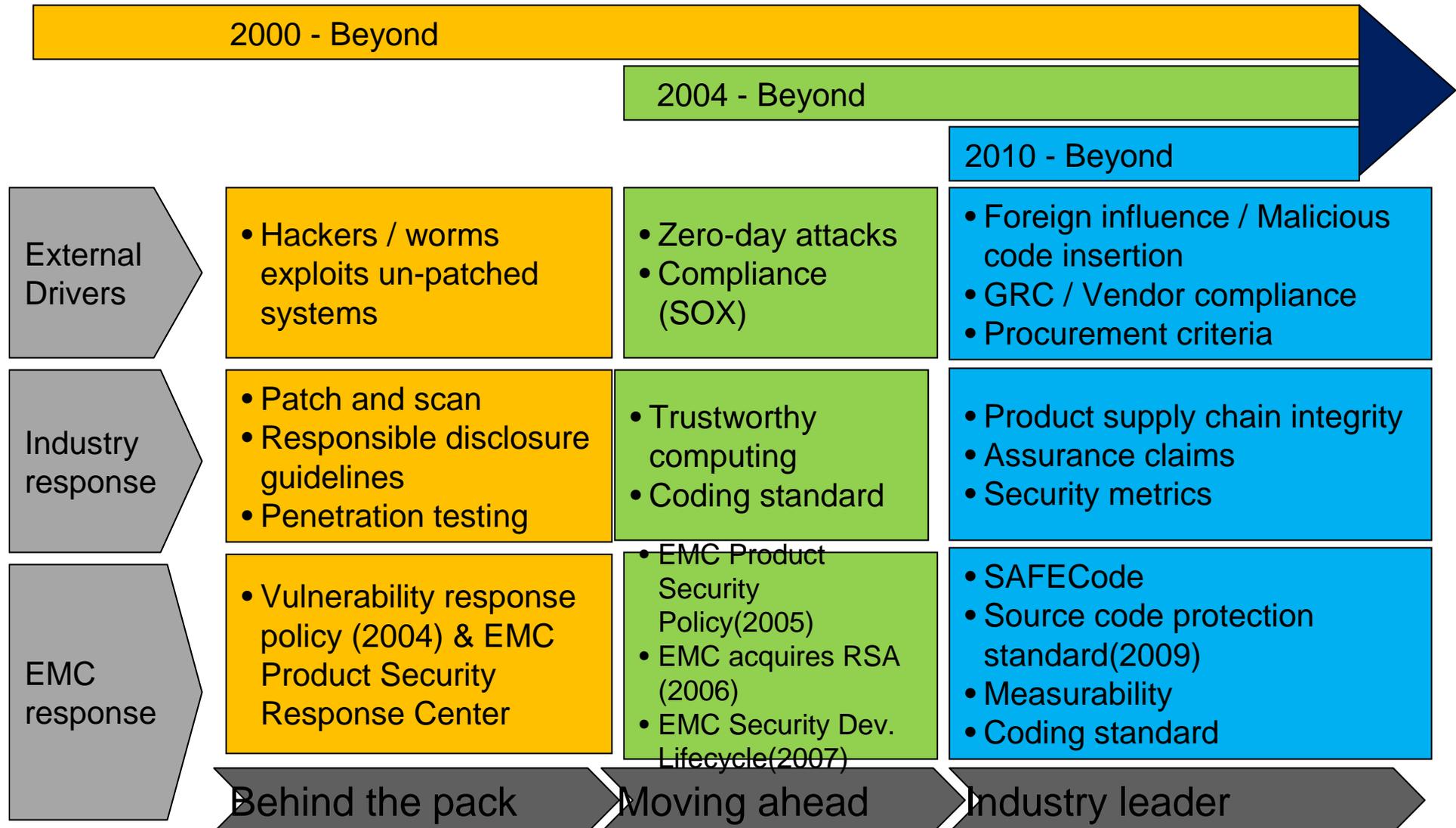
Dan Reddy, CISSP, CSSLP
EMC Product Security Office

Software Assurance Forum
Gaithersburg, MD
September 29, 2010

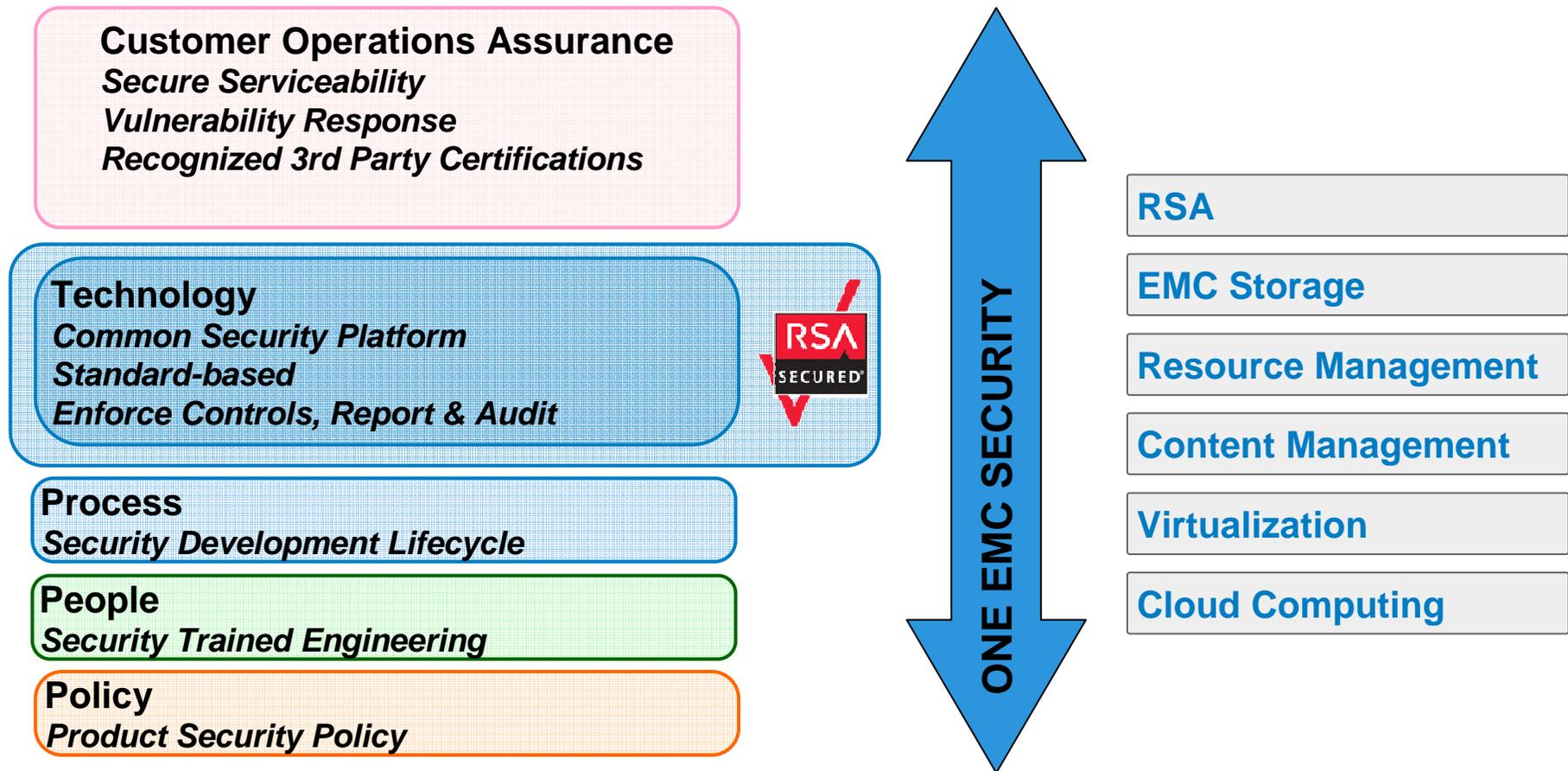


The Security Division of EMC

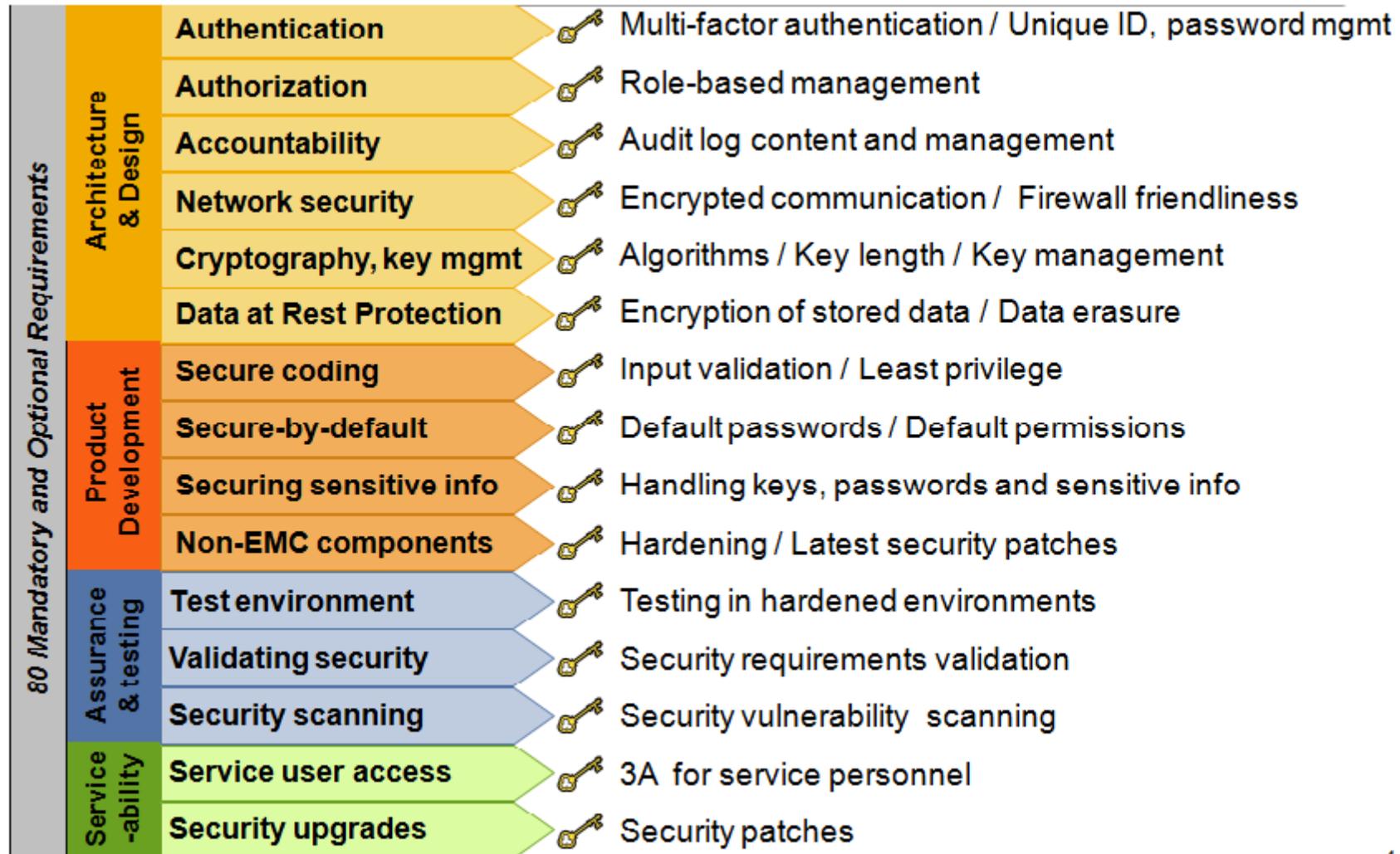
The Evolution of Product Security Assurance



EMC's Approach to Deliver a Secure Information Infrastructure

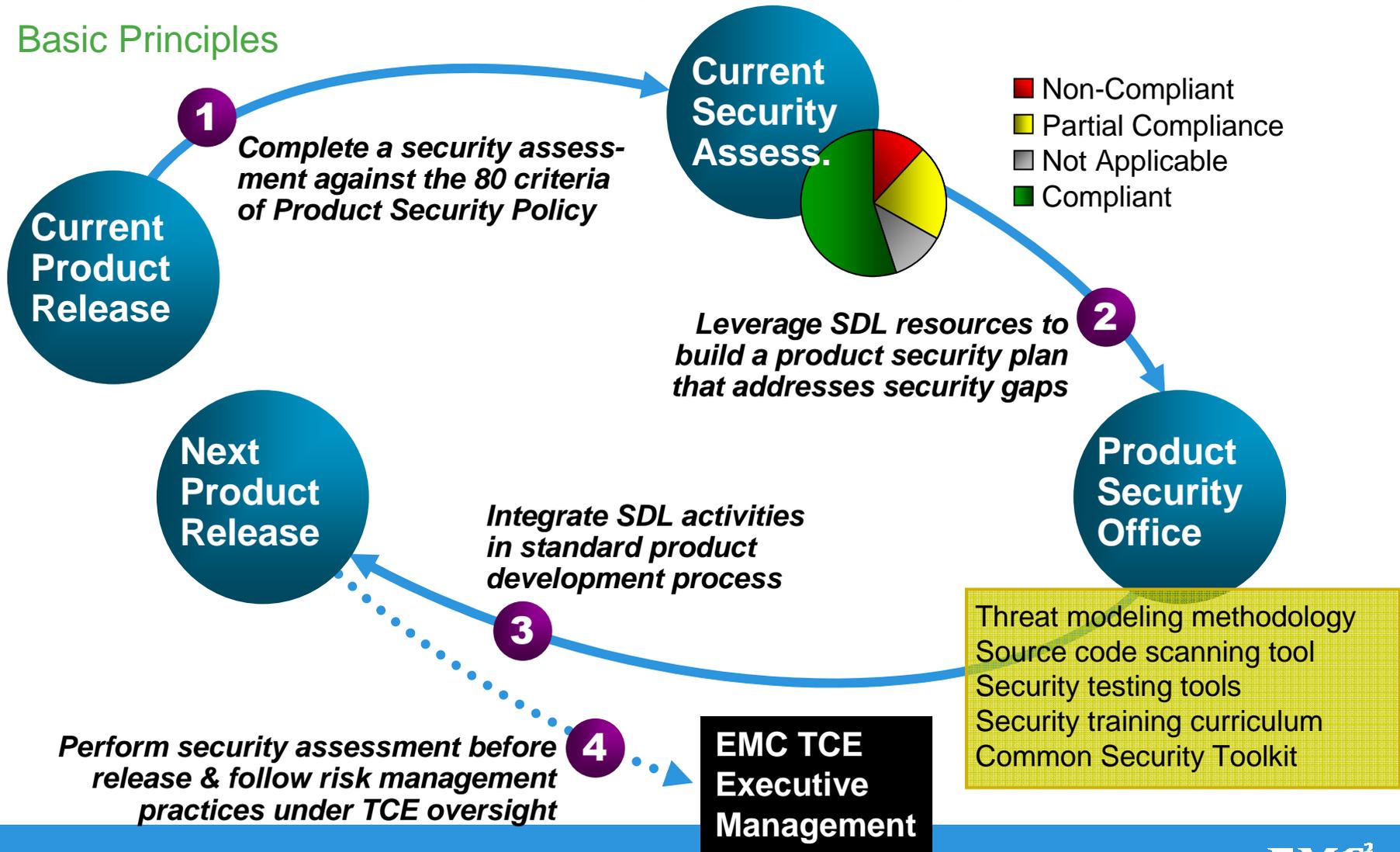


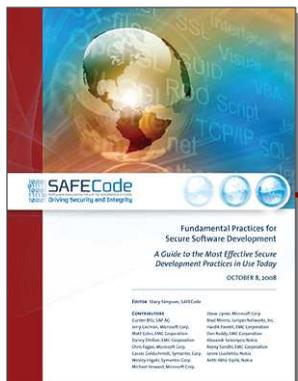
Policy: EMC Product Security Policy (v.2)



Process: EMC Product Security Development Lifecycle (SDL)

Basic Principles





Secure Software Development



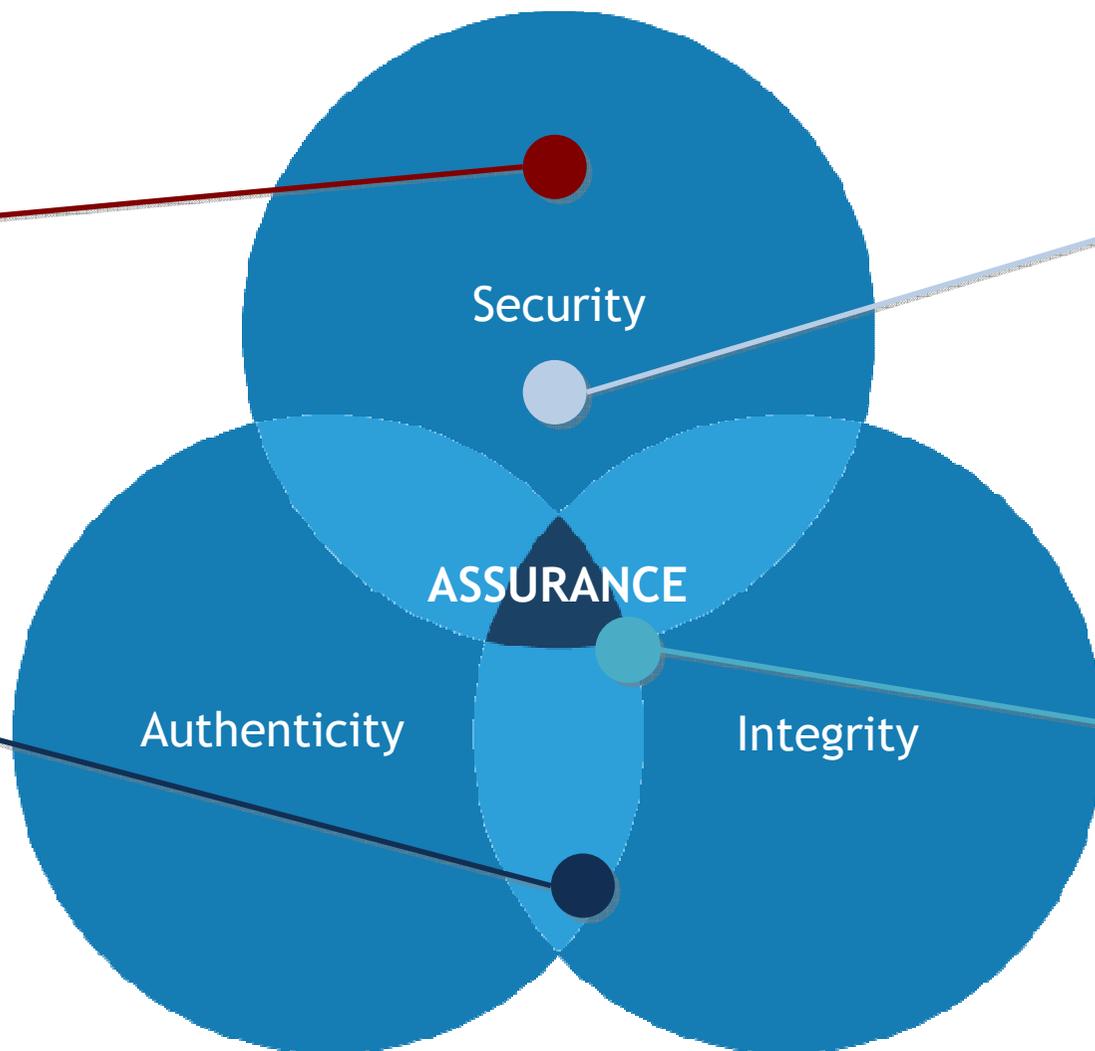
Training



Software Integrity Best Practices



Software Integrity Controls in Supply Chain



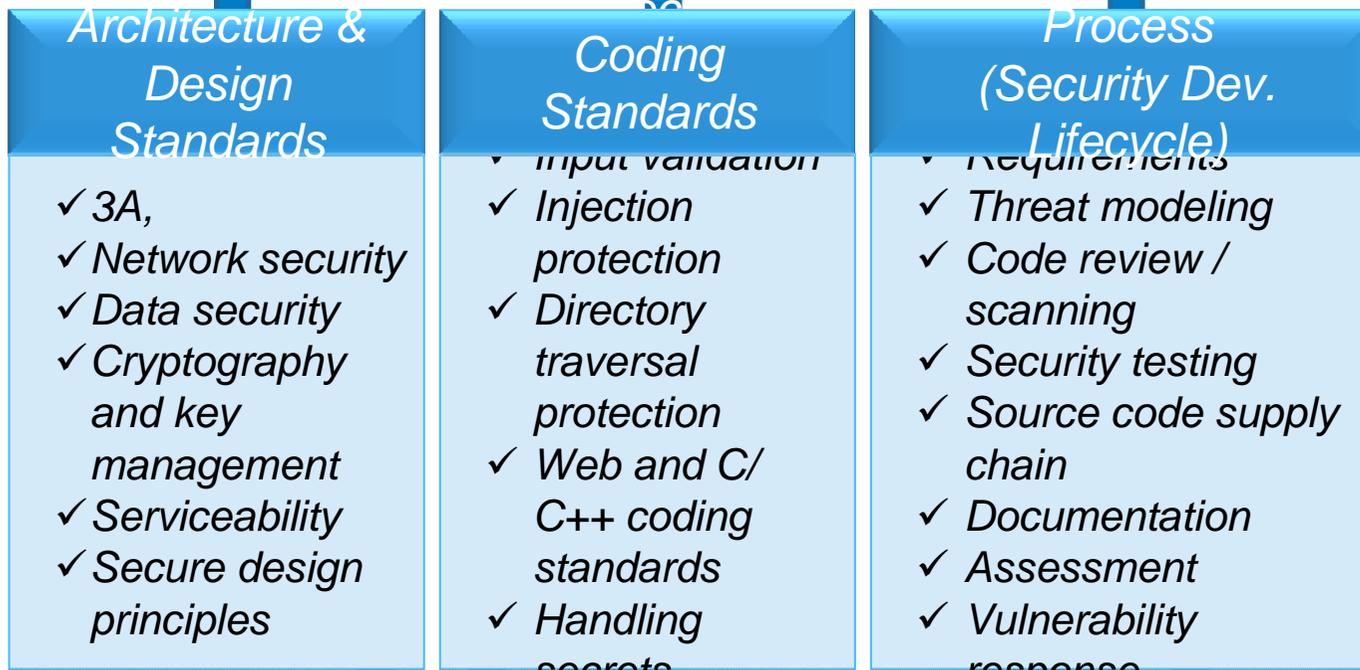
EMC/RSA Approach to Measuring Product Security and Organization Maturity



The Security Division of EMC

PRODUCT SECURITY POLICY

Maintained by RSA / Sets EMC-wide standards for product



PRODUCT GAPS



PROCESS GAPS

KEY METRICS

PRODUCT RISK (4 levels)

ORG MATURITY (4 levels)

Lessons learned

- Use organization maturity to set organization adoption roadmaps
 - 1) Vulnerability resp.
 - 2) Assessment
 - 3) Commercial testing
 - 4) Threat modeling
 - 5) Full process
- Be prescriptive with functional standards
- Use metrics as management tools
 - Executive dashboards
 - Cost avoidance per gap





The Security Division of EMC

THANK YOU

