Case Study: The Evolution of EMC’s Product Security Office

Dan Reddy, CISSP, CSSLP
EMC Product Security Office
The Evolution of EMC Product Security

2000-2004

External Drivers

- Hackers / worms exploit unpatched systems

Industry Response

- Patch and scan
- Responsible disclosure
- Penetration testing

EMC Response


2005-2009

- Zero-day attacks
- Compliance (SOX, Federal)

Industry Response

- MSFT Trustworthy computing
- Coding standard

EMC Response

- EMC acquires RSA (2006)
- First Common Criteria certified product (2007)

2010-Beyond

- Foreign influence / Malicious code insertion
- GRC / Vendor compliance
- Procurement criteria

Industry Response

- Product supply chain integrity
- Assurance claims
- Security metrics

EMC Response

- SAFECode
- Source code protection standard (2009)
- Measurability
- Coding standard

Behind the pack

Moving ahead

Industry leader
EMC’s Approach to Deliver a Secure Information Infrastructure

Coordinated by a central Product Security Office

Customer Operations Assurance
  Secure Serviceability
  Vulnerability Response
  Recognized 3rd Party Certifications

Technology
  Common Security Platform
  Standard-based
  Enforce Controls, Report & Audit

Process
  Security Development Lifecycle

People
  Security Trained Engineering

Policy
  Product Security Policy

ONE EMC SECURITY

Symmetrix
Unified Storage
Backup & Replication
Storage Software Group
Content Management
RSA
Virtualization
Cloud Computing
EMC Product Security Maturity Model: Based on Risk

**Optimized**
- Vulnerability root-cause analysis
- Coding standard is followed
- Assessment is validated by QA or external penetration test
- Regularly scheduled security patches
- Security certification like Common Criteria & FIPS 140-2
- Machine readable documentation

**Integrated**
- Engineers are trained
- Program Management tracks security activities
- Security Requirements
- Threat modeling at design phase
- Embedded component inventory
- Source code analysis and triage
- Vulnerability response plan
- Malware scanning
- Security testing & STIG scanning
- Security Bug tracking and evaluation
- Security Configuration Guide
- Vulnerability response plan
- Vulnerability regression testing
- Security Patches and patch communication
- Assessment before GA includes all unremediated issues discovered during threat modeling, source code analysis, vulnerability scanning, and security testing

**Proactive**
- Scorecard before release
- Risk escalation process followed
- Vulnerability response team members identified
- Product Security Liaisons identified (PSMO rep and Security Engineering Advocates)
- Vulnerability Scanning performed
- Embedded Component security alert tracking

**Reactive**
- All Activities reactive to external pressures
EMC / RSA Approach to Measuring Product Security and Organization Maturity

**PRODUCT SECURITY POLICY**
Maintained by RSA / Sets EMC-wide standards for product security

- 3A, Network security
- Data security
- Cryptography and key management
- Serviceability
- Secure design principles

**Coding Standards**
- Input validation
- Injection protection
- Directory traversal protection
- Web and C/ C++ coding standards
- Handling secrets

**Process (Security Dev. Lifecycle)**
- Training
- Requirements
- Threat modeling
- Code scanning
- Security testing
- Source code supply chain
- Documentation
- Assessment
- Vulnerability response

**PRODUCT RISK LEVELS**
- **Critical**: Requires executive sign-off
- **High**: Requires remediation in next release
- **Medium**: Requires monitoring
- **Low**

**ORG MATURITY LEVELS**
- **Reactive**: Customer risk is unknown
- **Proactive**: Customer risk is understood
- **Integrated**: Customer risk is controlled
- **Optimized**: Customer risk is minimized

**KEY METRICS**

**PRODUCT RISK (4 levels)**

**ORG MATURITY (4 levels)**