How to Turn Crisis Into Opportunity
Brad Arkin | Senior Directory, Product Security & Privacy
Brief Introduction

- **Current Gig:**
  - The “one neck to choke” at Adobe
  - ~300 products & services, ~4000 dev staff
  - Proactive (SPLC), reactive (PSIRT), & communications

- **Also:**
  - SAFECCode board member
  - Advisory boards for BSIMM, SAP, Veracode, etc.

- **Previously:**
  - RST/Cigital, @stake/SYMC
Set the Stage
Vulnerability/CVE Counts Grow Dramatically

Adobe's security woes continue as new exploits found in Reader, Flash

by Lee Mathews on July 24, 2009 at 04:00 PM

FILED UNDER: security

flickr user rjfalco
JBIG2 Vuln in Adobe Reader Makes the Nightly News (Feb 2009)
Solve the Business Problem!

- Some analogies:
  - The dog catches the car.
  - You’re handed a blank check.
- Someone asks the security guy what to do.
  - Now what!? 
Project Level: More Maturity is Seen with Earlier Engagement
Culture Change for Scale
ASSET Certification Program

Secure Software Engineering Certified White Belt

Secure Software Engineering Certified Brown Belt

Secure Software Engineering Certified Green Belt

Secure Software Engineering Certified Black Belt
Adobe Secure Product Life Cycle (SPLC)

Community engagement

TRAINING AND CERTIFICATION
- Concepts and process
- Defensive coding
- Security testing

RESPONSE
- Incident response protocols
- Regular patch cadence
- Update management

PLANNING
- Health assessment
- Risk assessment
- Threat landscape analysis

SHIP
- Readiness review
- Response plan
- Developer resources and education

DESIGN
- Security architecture
- Design review
- Threat modeling

TESTING
- Fuzz testing
- Threat mitigation validation
- Third-party testing

IMPLEMENTATION
- Static and dynamic analysis
- Secure compiler flags
- Secure coding guidelines
Questions?

- Visit us at:
  - www.adobe.com/security

- Twitter:
  - @BradArkin