

To the Cloud! Software Security Evolution at Adobe

Brad Arkin

Sr. Director, Product & Services Security
Adobe Systems

Security in
knowledge



Fall of 2011 (Then)



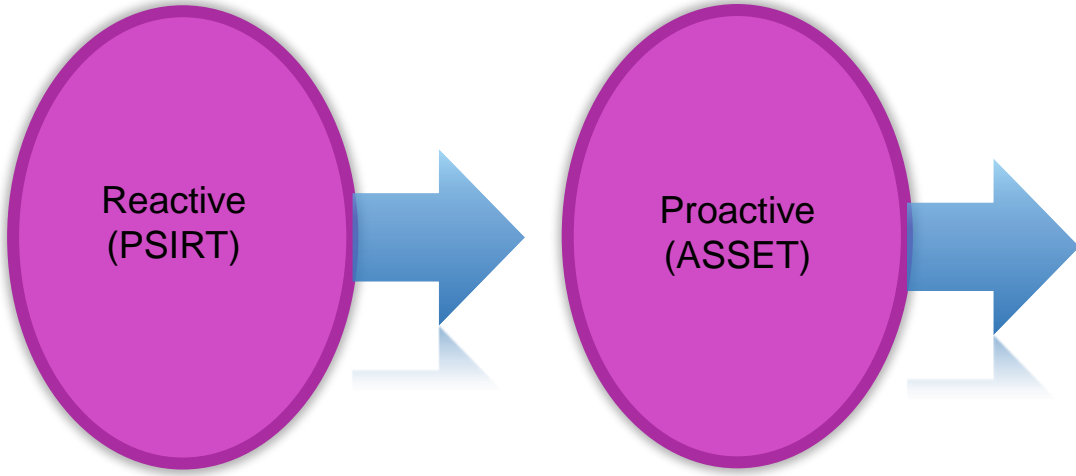
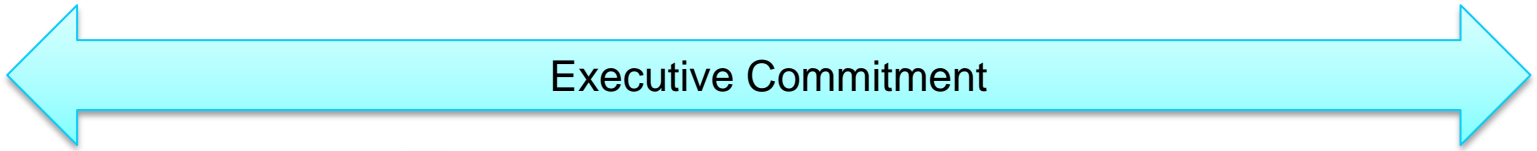
— Then: Key Problems

1. APT attacks leveraging 0-day exploits in Adobe software
2. “Un-coordinated” security researcher activity
3. CVE counts in Adobe Product Security Bulletins

— Then: Key Resources

- ☑ Product Security Team
- ☑ Strategy:
 - ☑ Exploit cost
 - ☑ Effective response
- ☑ Secure Product Lifecycle (SPLC) for Runtimes
- ☑ Security Training
- ☑ Product Security Incident Response team (PSIRT)
- ☑ Metrics
- ☑ Security Community (inside and outside Adobe)

Then: Our Security Commitment



Security-trained engineers across all product lines

Then: Our Security Strategy

Make exploits
hard to create

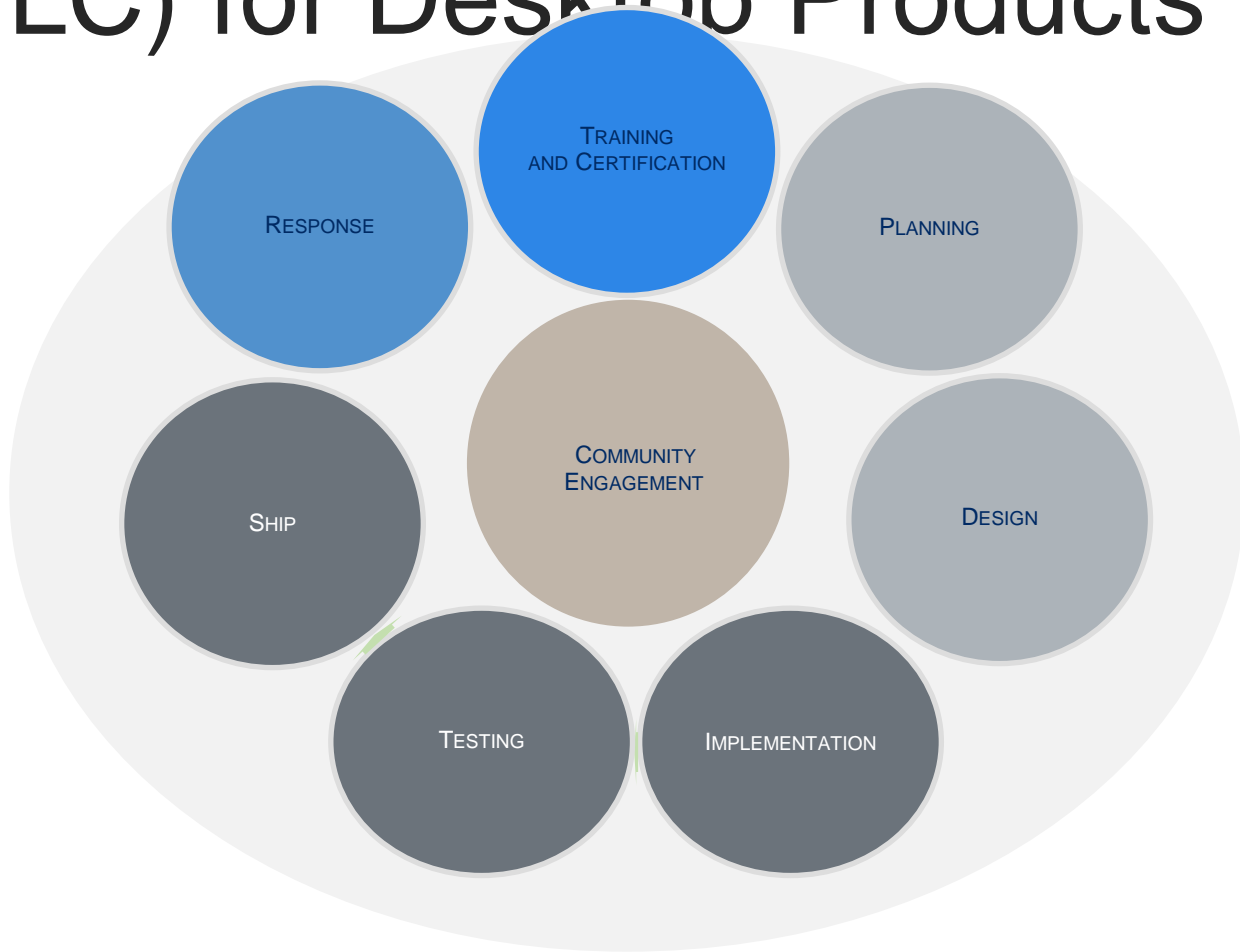
Defense in depth

Once created,
quickly drive the
value to zero

React efficiently,
mitigations

Transparent communication on what we are doing

Then: Secure Product Lifecycle (SPLC) for Desktop Products



Then: Training

Secure Software Engineering
Certified White Belt



Secure Software Engineering
Certified Brown Belt



Secure Software Engineering
Certified Green Belt



Secure Software Engineering
Certified Black Belt



— Then: Response



— Then: Metrics for Desktop Incident Response

Goal metrics for response:

- ▶ Average age of open incidents <90
- ▶ Response for zero days <20 days

Then: Community



de
e in Code
egrity

— In November 2011...



MelBaw


— New Assignment: Secure Hosted Services Oh No!



— New Assignment: Secure Hosted Services

What to do?

- ▶ Different:
 - ▶ skills
 - ▶ process
 - ▶ mindset
 - ▶ timeframes



New Leadership Challenge!

Now: Secure Hosted Services launched



Adobe Marketing Cloud



Adobe Creative Cloud

— Key Problems







Then:

1. APT attacks leveraging 0day exploits in Adobe software
2. “Uncoordinated” Security Researcher activity
3. CVE counts in Adobe Product Security Bulletins

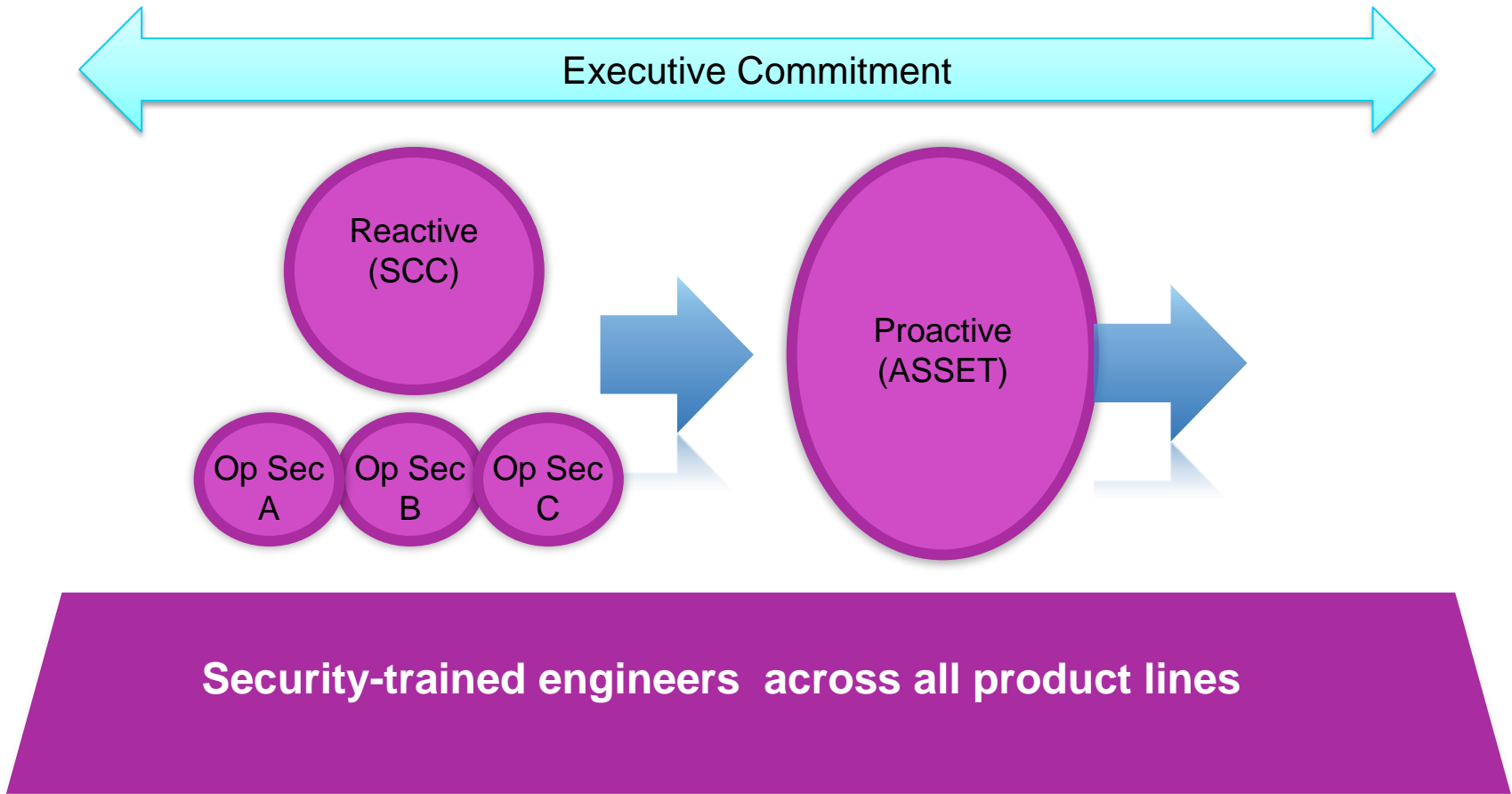
Now:

1. Security Operations / Monitoring
2. Governance
3. Authentication

Then and Now: Key Resources

<input checked="" type="checkbox"/> Product Security Team		Expanded team with SaaS expertise
<input checked="" type="checkbox"/> Strategy Strategy Exploit cost Effective response		Attack difficulty Effective monitoring & response
<input checked="" type="checkbox"/> SPLC for Runtimes		SPLC for SaaS
<input checked="" type="checkbox"/> Security Training		Security training for SaaS
<input checked="" type="checkbox"/> PSIRT Coordination Center (SCC)		Security
<input checked="" type="checkbox"/> Community (inside and outside Adobe)		Community (inside and outside Adobe)

Now: Our Security Investment



Now: Our Security Strategy

Make attacks
hard
to carry out

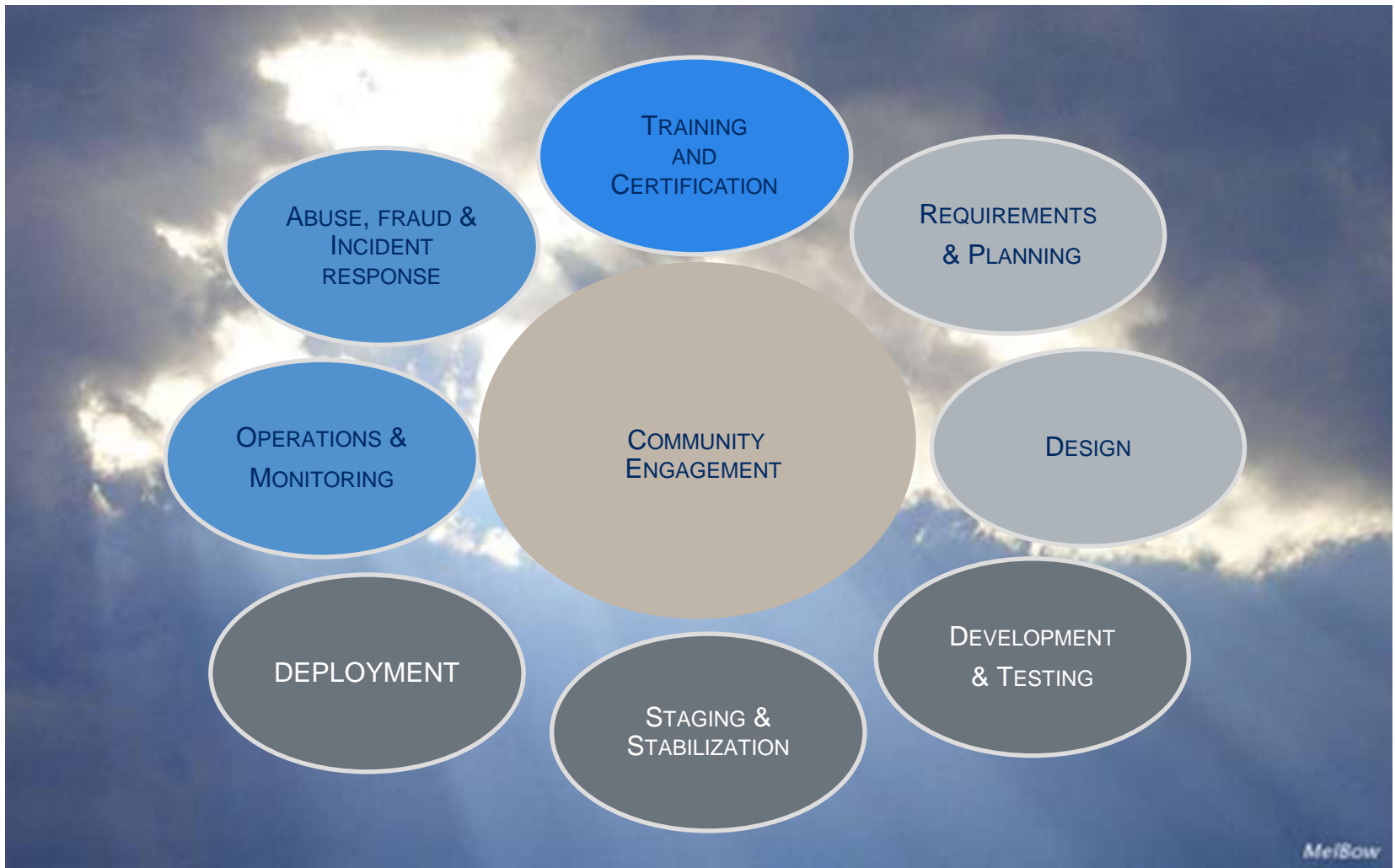
Defense in depth

Once attacked:
quickly detect,
respond, &
eradicate

Monitoring, react
efficiently

Transparent communication on what we are doing

Now: SPLC for SaaS



MeiBow

Now: SaaS Specific Training Added



— Now: Response (Security Coordination Center)

- ▶ Added centralized incident response coordination
- ▶ Improve internal monitoring and detection of issues
- ▶ Monitor external sources to gather information
- ▶ Provide cross-functional consistency for processes
- ▶ Interface with Legal, PR, Marketing, ...

— Now: Response Metrics

Goal metrics for response:

- ▶ Response time for high priority issues <5 days
- ▶ Response time for SaaS incidents measured in minutes/hours

Governance

- ▶ Universe consists of three distinct demographics
 - ▶ Product engineering teams
 - ▶ Adobe IT
 - ▶ 3rd party vendors

- ▶ Tools
 - ▶ Dashboards & Roadmaps
 - ▶ Automation
 - ▶ Policy

— Authentication

- ▶ Implementation
 - ▶ Password storage
 - ▶ Account alerts based on activity
 - ▶ Long list of pending features
- ▶ Offline interaction
 - ▶ Response to the “Mat Honan” problem
- ▶ Real-time monitoring
 - ▶ Defensive actions in response to suspicious activity

Now: Community



le
n Code
grity

Summary

- ▶ Change can be scary
- ▶ Leverage what you already have/modify to fit new needs
- ▶ Acknowledge when a new approach is required
- ▶ Identify all related and interested parties
- ▶ Take advantage of existing strengths
- ▶ Build out process where needed
- ▶ Emphasize efficient communication
- ▶ Employ benchmarks and reporting dashboards

Resources

- ▶ Security portal (customers and channel partners):
<http://adobe.com/security>
- ▶ Advisories and updates
<http://www.adobe.com/support/security>
- ▶ ASSET blog: <http://blogs.adobe.com/asset>
- ▶ PSIRT blog: <http://blogs.adobe.com/psirt>
- ▶ Documentation wiki:
<http://learn.adobe.com/wiki/display/security/Home>
- ▶ Adobe Security on Twitter: @AdobeSecurity
- ▶ My Twitter Handle: @BradArkin



Adobe