

DC/4

DAYCONF~~OUR~~//DAYTONSECURITYSUMMIT 2010////



Defending the undefendable

Bruce Potter

bpotter@pontetec.com

Intro

- ▶ By day
 - Co-founder and CTO – Ponte Technologies
- ▶ By night
 - Founder of The Shmoo Group, help with ShmooCon
- ▶ Written some books, write articles, on Ed board of some IEEE pubs
- ▶ Don't believe anything I say

We'll have the desert first

Doing things right is necessary....
but not sufficient

Threats

- ▶ Evolved dramatically
 - APT has been thrown around a lot recently
- ▶ Modern attacks are:
 - Not really that “advanced”
 - Definitely “persistent”
 - A real “threat” for a wide variety of enterprises
- ▶ Attacks come right through the front door
 - Very hard to stop

Threats

- ▶ Evolved dramatically
 - APT has been thrown around a lot recently
- ▶ Modern attacks are:
 - Not really that “advanced”
 - Definitely “persistent”
 - A real “threat” for a wide variety of enterprises
- ▶ Attacks come right through the front door
 - Very hard to stop

Defenses

- ▶ Have not evolved
 - Boundary protection
 - Firewalls
 - AV
 - Anti-spam
 - Proxy?
 - Other options are not widely deployed
 - Core protection
 - AV
 - Patch/version management
 - Compliance?
 - Right.. Check boxes are like multiple choice in HS

A View of Current Threat

Highly Targeted
Insider Threat

Skilled,
Motivated

General
Purpose

Org Crime, Indust.

Worms, virus,

Written Off

Or at least basically
ignored. Very
difficult with
today's
technology.

“Solved” Problem

AV, AS, IDS, Firewalls.
These tools are highly
automated and geared
towards compliance.

A View of Current Threat

Highly Targeted
Insider Threat

Skilled,
Motivated

General
Purpose

Org Crime, Indust.

Worms, virus,

Written Off

Or at least basically
ignored. Very
difficult with
today's
technology.

???

Requires some manual
work as well as a
different set of
tools than is
currently available.

“Solved” Problem

AV, AS, IDS, Firewalls.
These tools are highly
automated and geared
towards compliance.

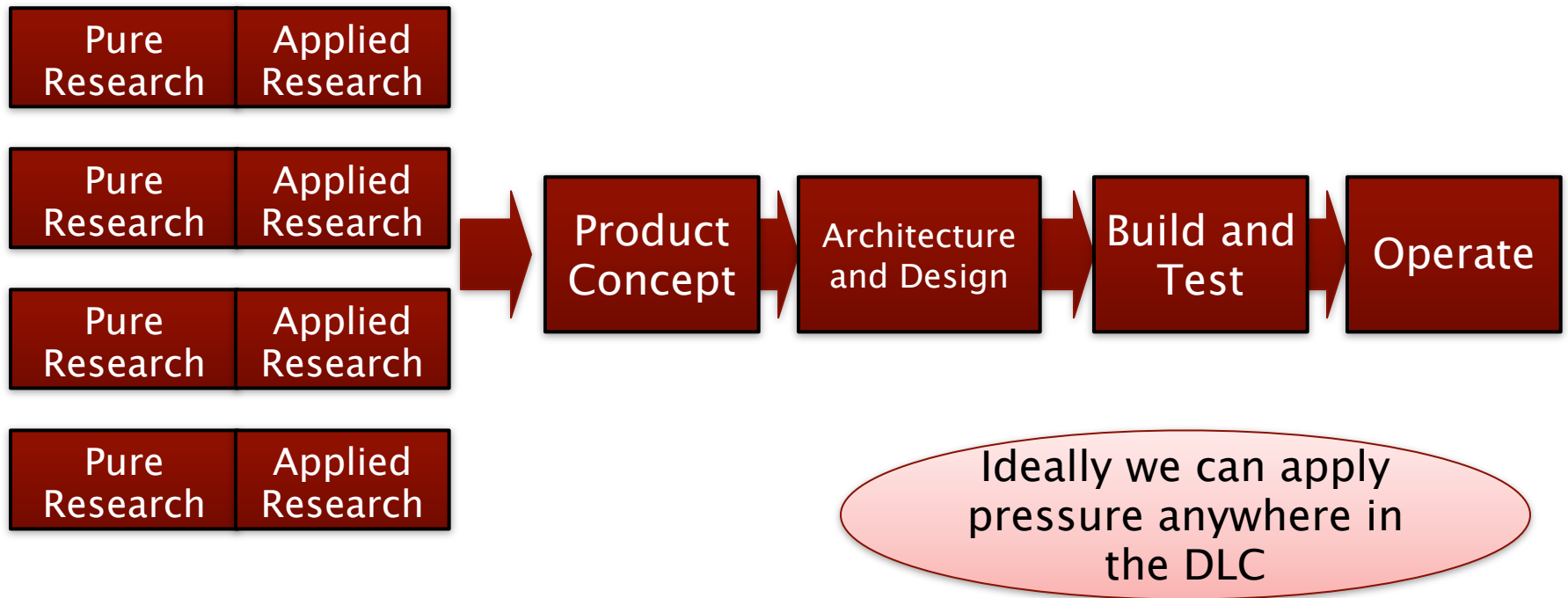
Metrics on how bad IT is

- ▶ “Outgunned: How Security Tech is Failing Us” – Information Week, Greg Shipley
 - 54% of all malware is “customized”
 - 71% and 79% of organizations claimed attacks evaded IDS and AV, respectively
- ▶ “All your iFrames Point to us” – Provos (Google) et al
 - 5% of the web is overtly malicious. There are no “safe” sites
 - AV averages 50% effectiveness against drive bys
- ▶ Verizon’s Data Breach Report
 - Org’s that are PCI compliant are 50% less likely to suffer a breach
 - WTF. That’s supposed to be positive reinforcement for PCI?

Sad Reality

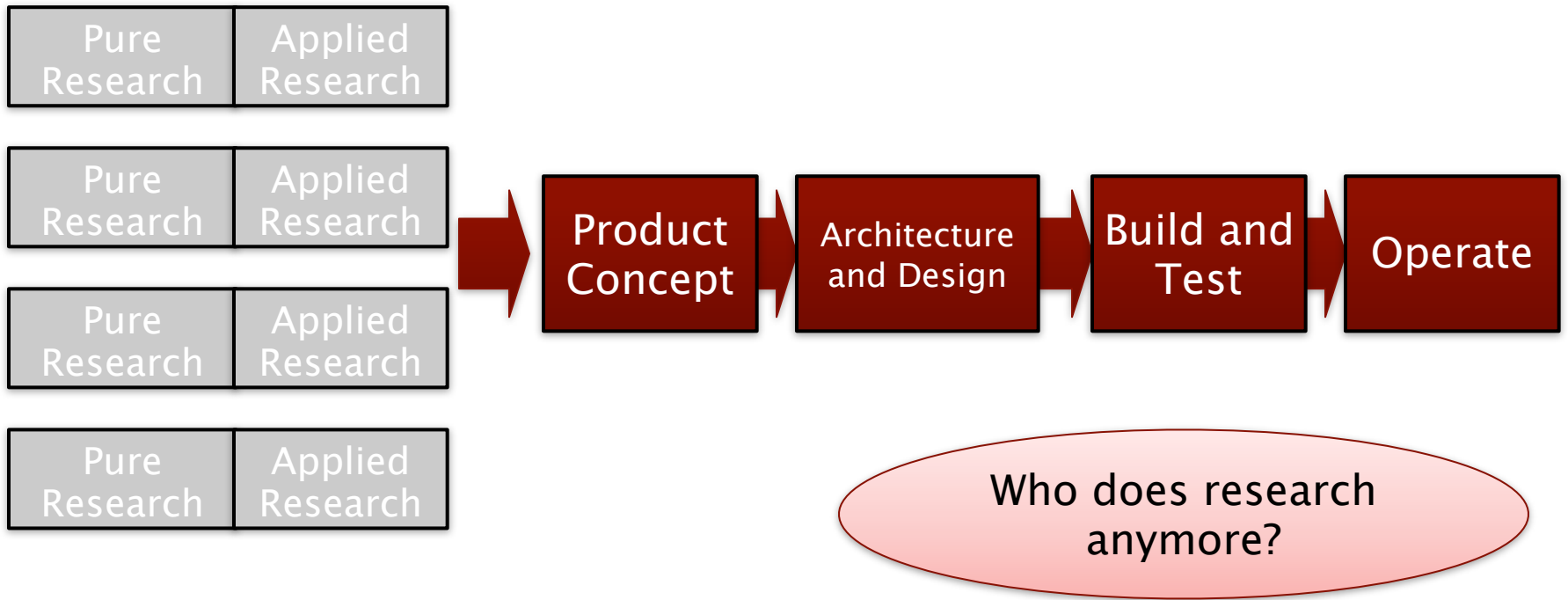
- ▶ Attackers can make it through whatever defenses you have in place
 - And if you're a target, they will
- ▶ In the last few months, this message has really started to take hold
 - Great. Word is getting out... So now what?

Where to fix the problem...



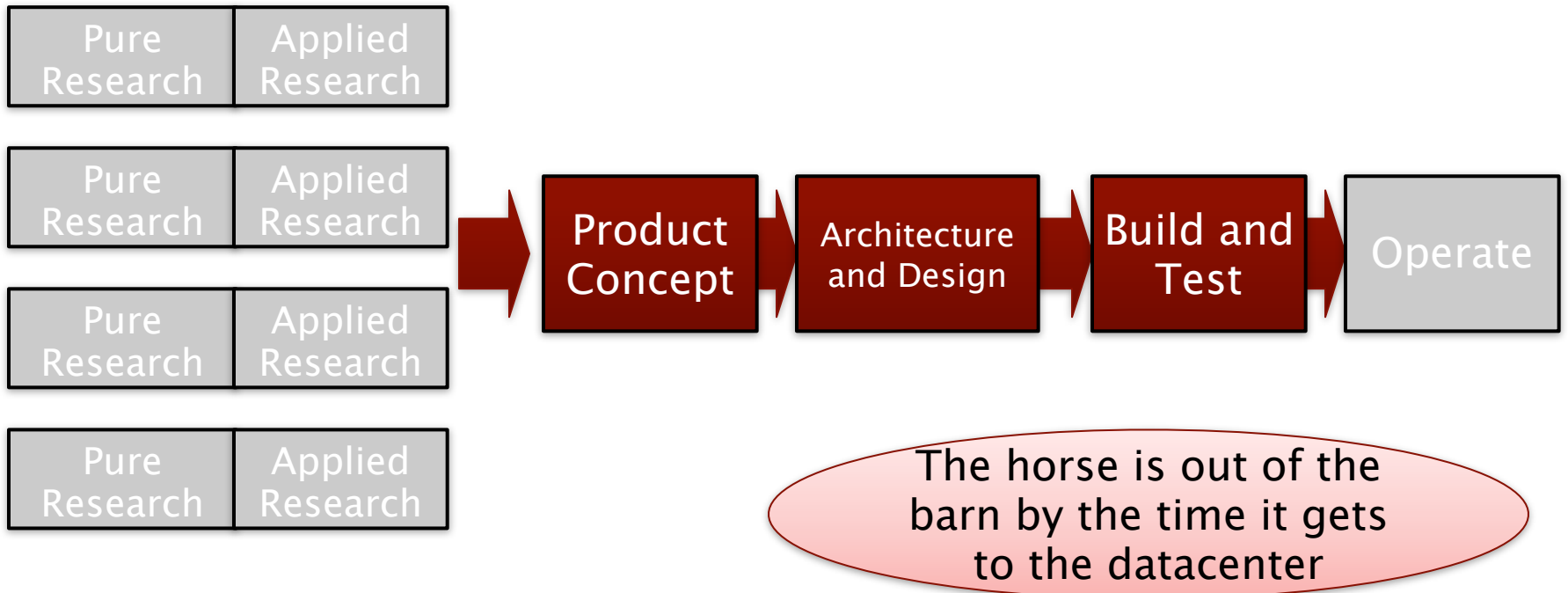
Product Development Lifecycle

Where to fix the problem...



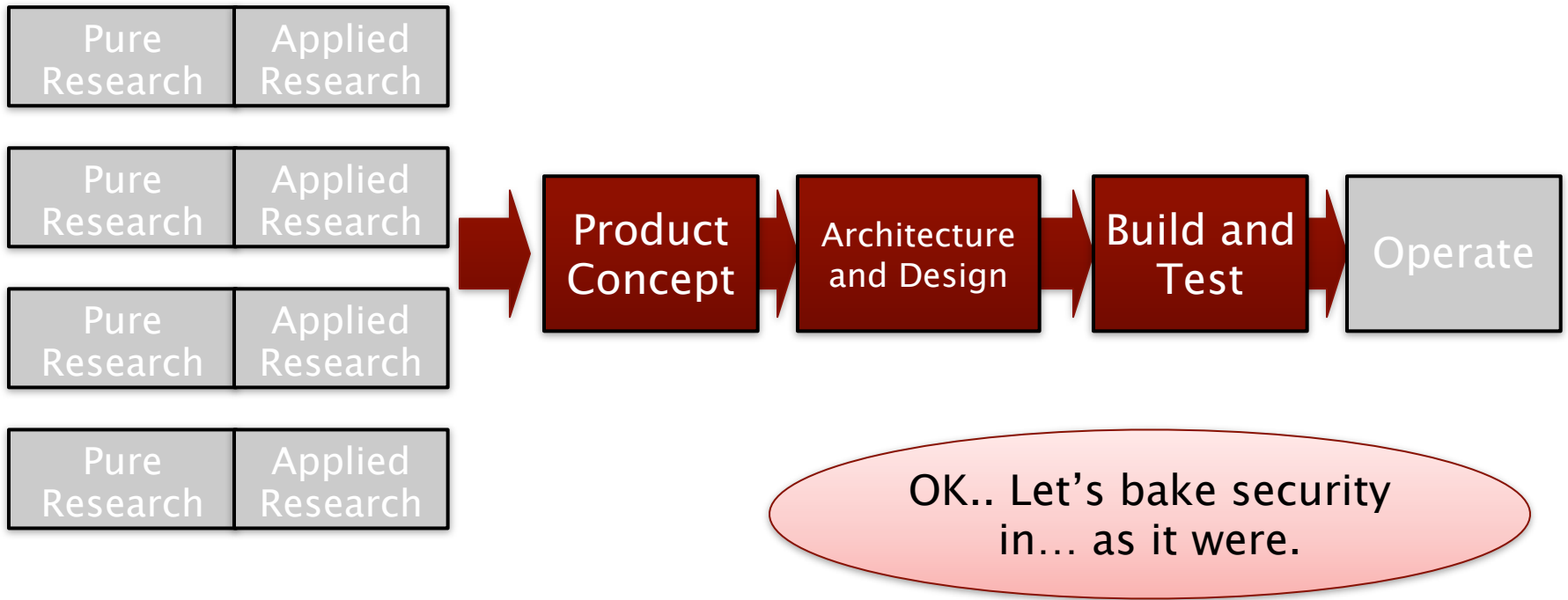
Product Development Lifecycle

Where to fix the problem...



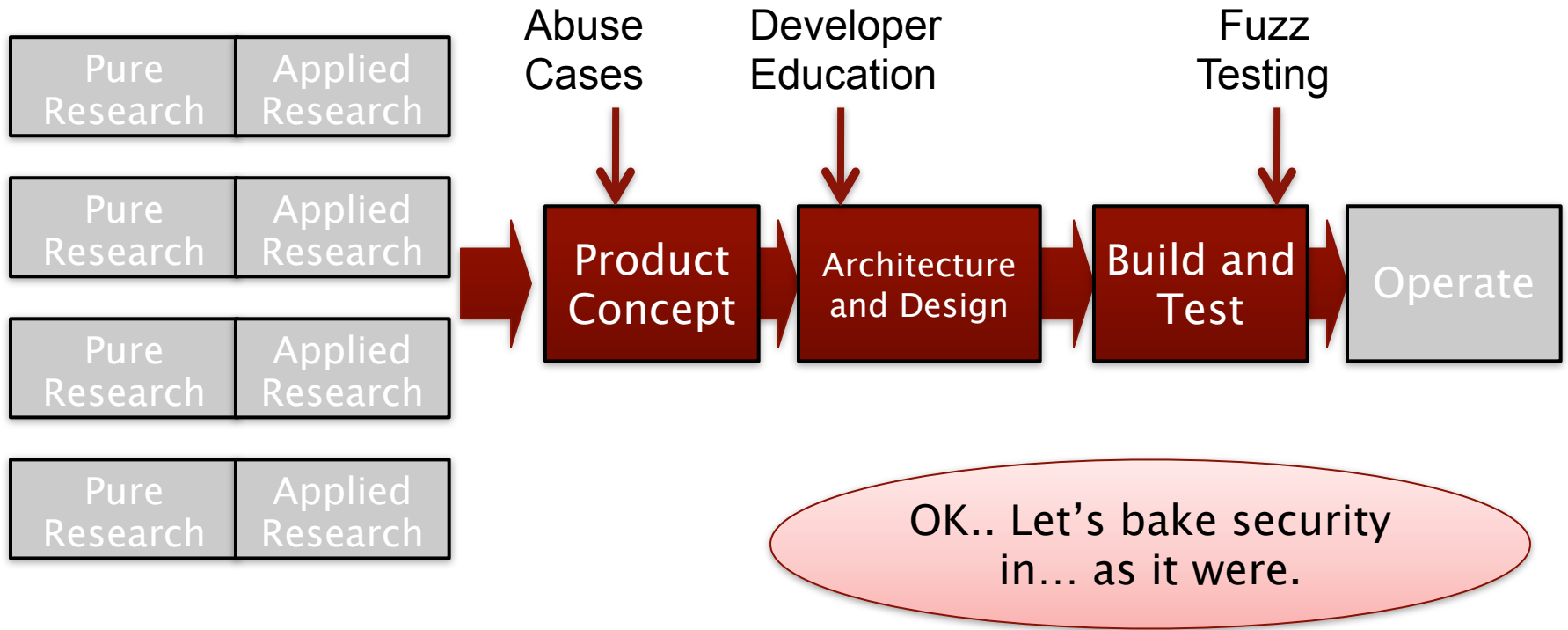
Product Development Lifecycle

Where to fix the problem...



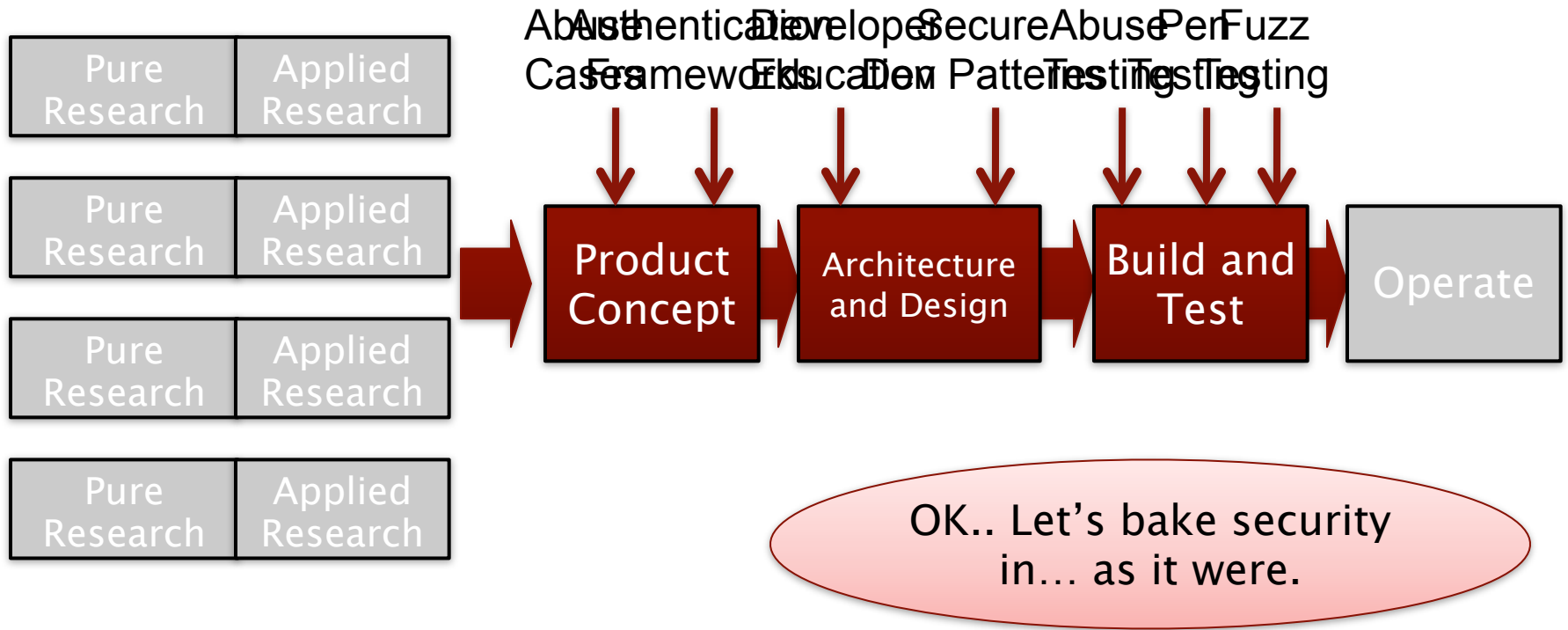
Product Development Lifecycle

Where to fix the problem...



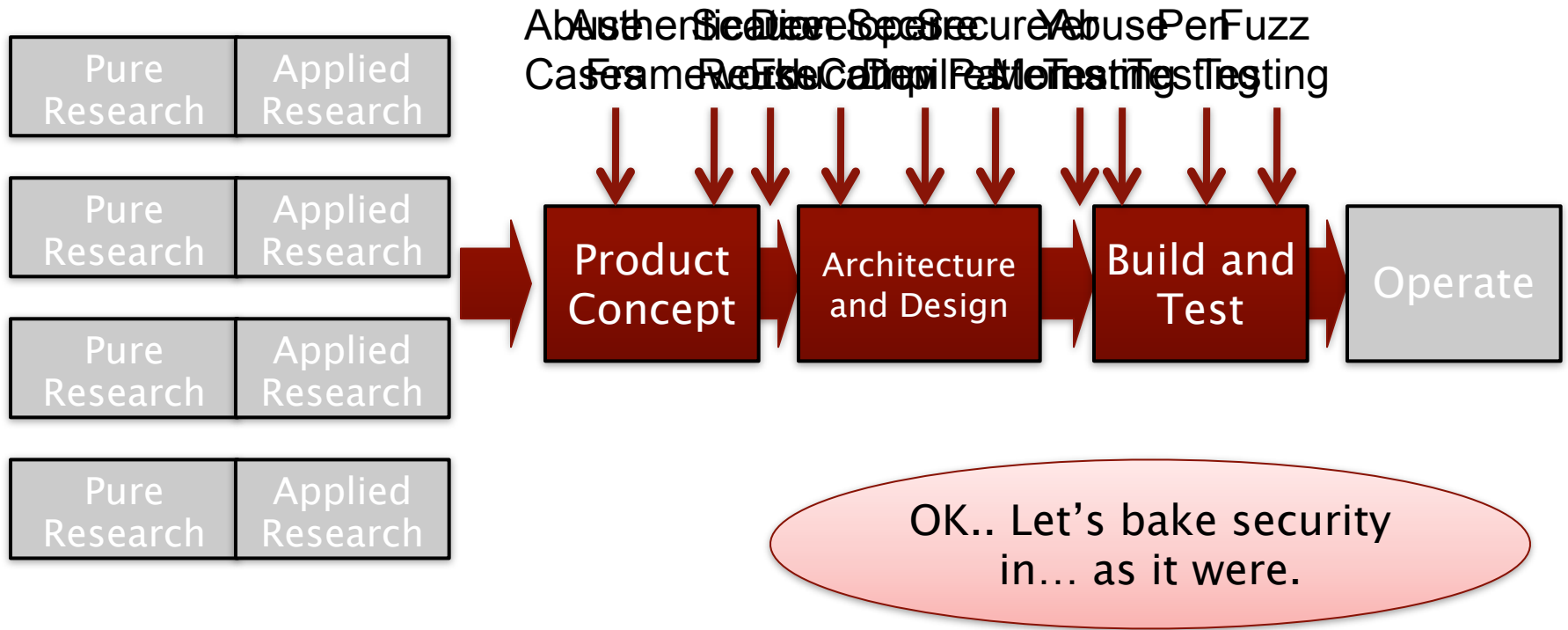
Product Development Lifecycle

Where to fix the problem...



Product Development Lifecycle

Where to fix the problem...



Product Development Lifecycle

Where to fix the problem...



2010!
RESEARCH!
FAILURE!

OK.. Let's bake security in... as it were.

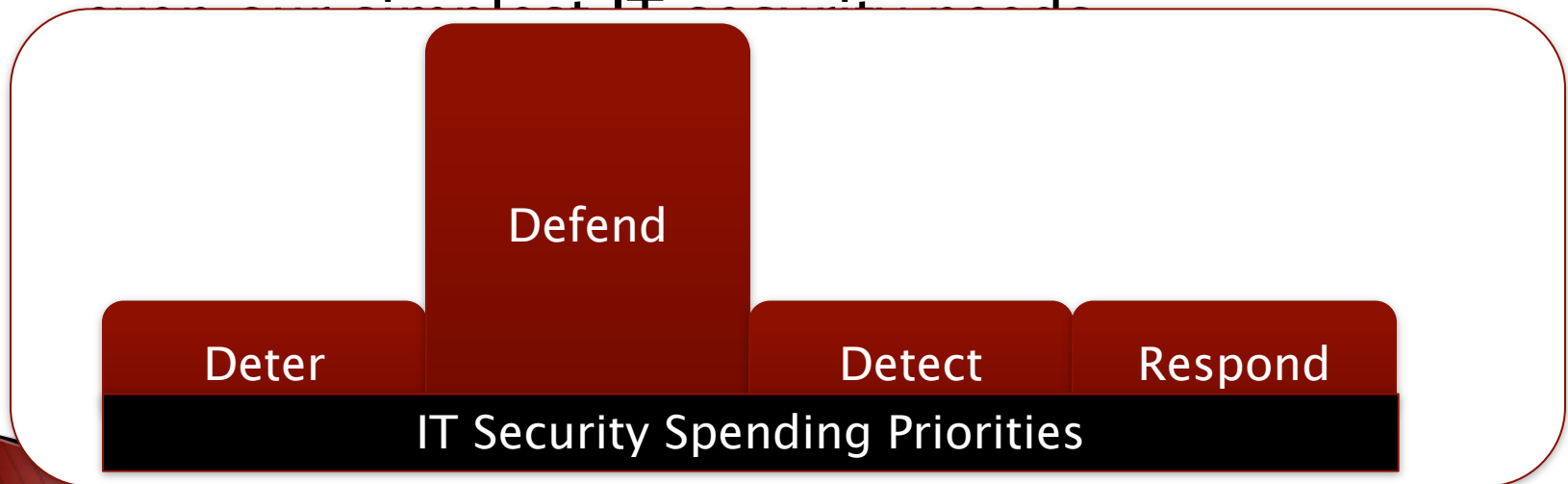
Product Development Lifecycle

Responding – Operations

- ▶ Detection is the new battle ground
 - And I don't mean IDS...
- ▶ But do you really want to pay for detection?
 - IT is a discriminator.. Is security?

Wait! What about buying detection products?

- ▶ IT Security is a multibillion dollar industry...
 - That has been investing in a failed set of products for the last 2 decades
 - HUGE spending on preventing attacks, but it fails
 - Detection (ie: analysis) hasn't been a spending priority ergo products haven't been built to address



Practical Operational

- ▶ Fix authentication as best you can
 - Two factor if you can.. At least get rid of LM
- ▶ Isolate, Isolate, Isolate
 - Provide internal boundaries, especially managed from unmanaged
- ▶ Assume attackers will (and have) breached your borders
 - Focus on detection
 - Netflow, log analysis, integrity management, etc. (not IDS)

A Parable on Integrity Management.. As it were...

Responding – New Technologies

- ▶ Trusted Computing
- ▶ Capabilities-based security
- ▶ End-to-end attribution

- ▶ Honestly... a huge reinvestment in basic computer science needs to occur.

New Big New Challenge TM

- ▶ Educating businesses about the new reality
 - How do you justify your IT security spend when you know your defenses are going to be compromised?
- ▶ Need to focus on the whole lifecycle
 - ... against all odds... it's a very hard sell
 - Few metrics, working against conventional wisdom, seems like security without regard for business, etc...

Prevent
attack

- Deter

Stop
attack

- Defend

Find
attack

- Detect

Recover
service

- Respond

And now, the beginning...

- ▶ Don't believe anything I say...

bpotter@pontetec.com