RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CRWD-W02

Building and AppSec Program with Sun Tzu, the Dalai Lama and Honey Badger

Dan Cornell

CTO

Denim Group

@danielcornell

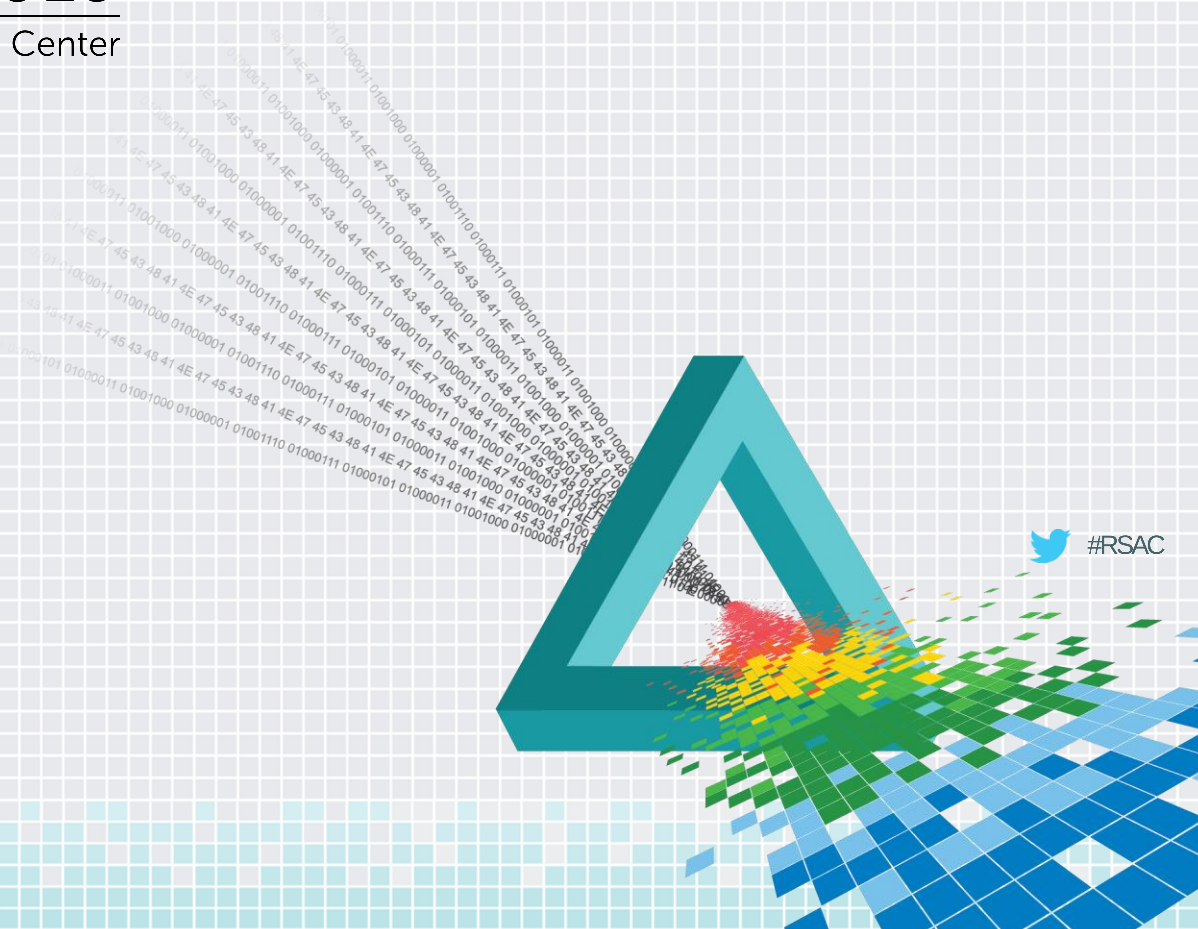
Agenda

- Housekeeping
- Sun Tzu and Information Security
- How About Application Security?
- The Dalai Lama and Application Security
- Summary
- Apply

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Housekeeping



#RSAC

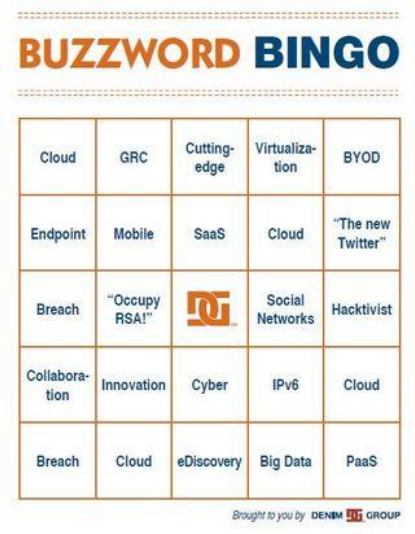
Simpsons Already Did It

- As with any good topic information security…

…Jericho covered it first

http://attrition.org/security/rant/fsck_sun_tzu/

Since Jericho Actually Reads Stuff. . .



BUZZWORD BINGO

Cloud	GRC	Cutting-edge	Virtualiza-tion	BYOD
Endpoint	Mobile	SaaS	Cloud	"The new Twitter"
Breach	"Occupy RSA!"		Social Networks	Hacktivist
Collabora-tion	Innovation	Cyber	IPv6	Cloud
Breach	Cloud	eDiscovery	Big Data	PaaS

Brought to you by DENIM GROUP

http://www.denimgroup.com/blog/denim_group/2012/02/rsa-buzzword-bingo.html

http://attrition.org/security/rebuttal/rebuttal-cornell_denimgroup_rsa_bingo.html

http://www.denimgroup.com/blog/denim_group/2012/03/buzzword-bingo-all-my-words-come-back-to-me-in-shades-of-mediocrity.html

. . .Clean Room

Didn't read the attrition.org article

(Though I will have to check it out when the talk is over)

What To Expect

Cherry-picked quotes used in a context I find useful. . .

. . .for both Sun Tzu and Dalai Lama

If you were hoping to use this presentation to complete your doctoral dissertation. . .

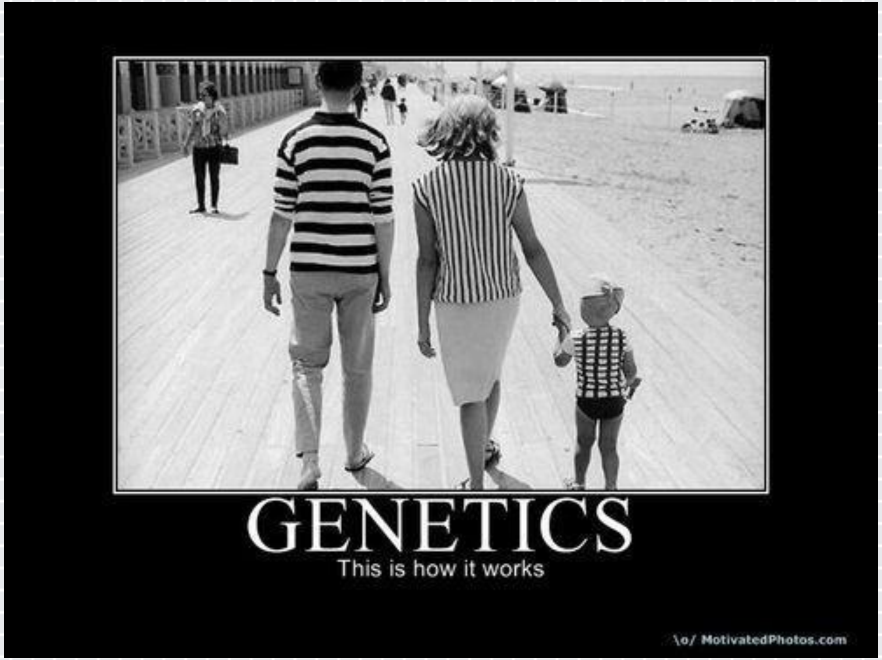
You will be disappointed or You will have a shaky dissertation

That Said. . .

I want to talk about perspective

And some of the fundamental metaphors security professionals use to approach their work

And the stories they use to communicate and inspire one another



The Gold Standard Sun Tzu Quote for InfoSec

If you know the enemy and know yourself,
you need not fear the result of a hundred battles.
If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself,
you will succumb in every battle.

-Art of War, Chapter 3

His (Supposed) Training Methods

Training the king’s harem to be soldiers

Some Advice Too Many Take (Halfway) To Heart

“A military operation involves deception. Even though you are competent, appear to be incompetent. Though effective, appear to be ineffective”

-Art of War, Chapter 1

“Pretend inferiority and encourage his arrogance”

-Art of War, Chapter 1

#RSAC

Sun Tzu and Information Security

Thinking “Security” Has An End

“What is essential in war is victory, not prolonged operations”

Art of War, Chapter 2

Thoughts on “Capturing” Attackers

“In the practical art of war, the best thing of all is to take the enemy’s country whole and intact; to shatter and destroy it is not so good. So, to, it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them”

Art of War, Chapter 3

Hacking Back

“One defends when his strength is inadequate, he attacks when it is abundant”

Art of War, Chapter 4

“The quality of decision is like the well-timed swoop of a falcon which enables it to strike and destroy its victim”

Art of War, Chapter 5

Security Through Obscurity

“Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness”

Art of War, Chapter 6

Problems Communicating With "The Business"

"The general that hearkens to my counsel and acts upon it, will conquer: let such a one be retained in command! The general that hearkens not to my counsel nor acts upon it, will suffer defeat: - let such a one be dismissed!"

-Art of War, Chapter 1

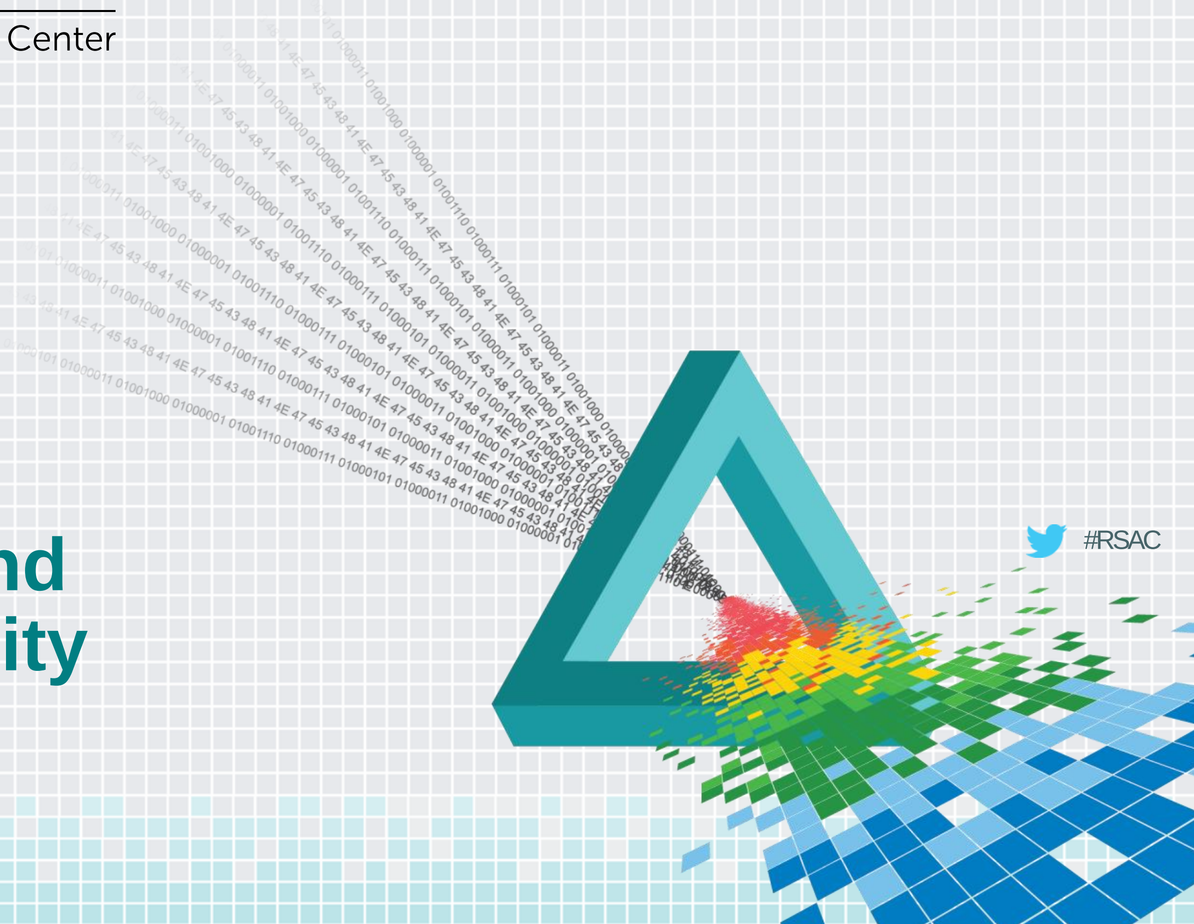
How About Application Security?

An InfoSec Perspective on Developers

“If these developers would just stop writing such sh*tty code, all our lives would be a lot better”

-Some Security Curmudgeon, BSides Austin, 2011

Developers And Overzealous InfoSec Folks



#RSAC

The Dalai Lama and Application Security

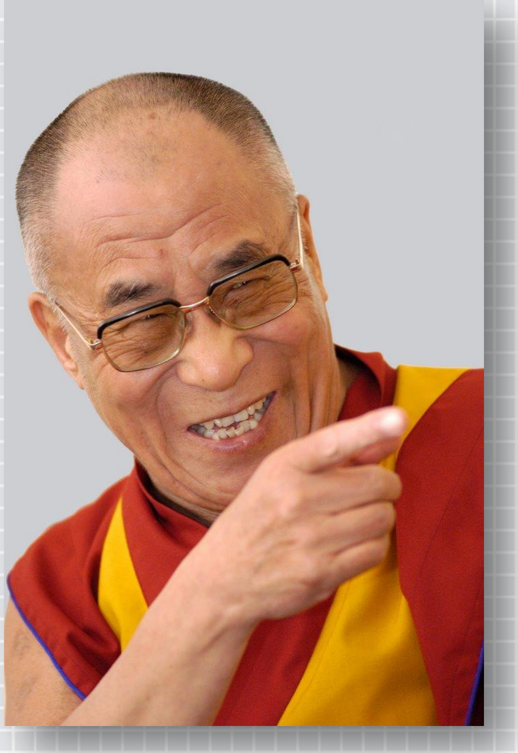
Get Your Mind Right

“My true religion is Kindness”

-Kindness, Clarity and Insight, 1984

“I feel that the essence of spiritual practice is your attitude toward others”

-Catherine Ingram interview, 1988



Get Your Mind Right

- What are the *true* risks to your business?
  - Physical, financial, strategic
  - Not just information assets

- How well are developers' activities aligned with the business
  - Features, functions, timelines

Empathy and Compassion

"I believe all suffering is caused by ignorance"

-Nobel acceptance speech, 1989

"Compassion and tolerance are not a sign of weakness, but a sign of strength"

-Words of Wisdom, 2001

Empathy and Compassion

- What are your developers actually doing?
- Why are they doing it?
- How can you support them *and* advance your goals?

Understand Developer Tools

- Coding (IDE)
- Testing (Unit tests, acceptance tests)
- Workload tracking (Defect trackers, change management)
- Automation and orchestration (Continuous integration)
- Metrics

Be Flexible and Data-Driven

“My confidence in venturing into science lies in my basic belief that as in science so in Buddhism, understanding the nature of reality is pursued by means of critical investigation”

-The Universe in a Single Atom, 2005

“If science proves some belief of Buddhism wrong, then Buddhism will have to change. In my view, science and Buddhism share a search for the truth and for understanding reality. By learning from science about aspects of reality where its understanding may be more advanced, I believe that Buddhism enriches its own worldview”

-New York Times, 2005

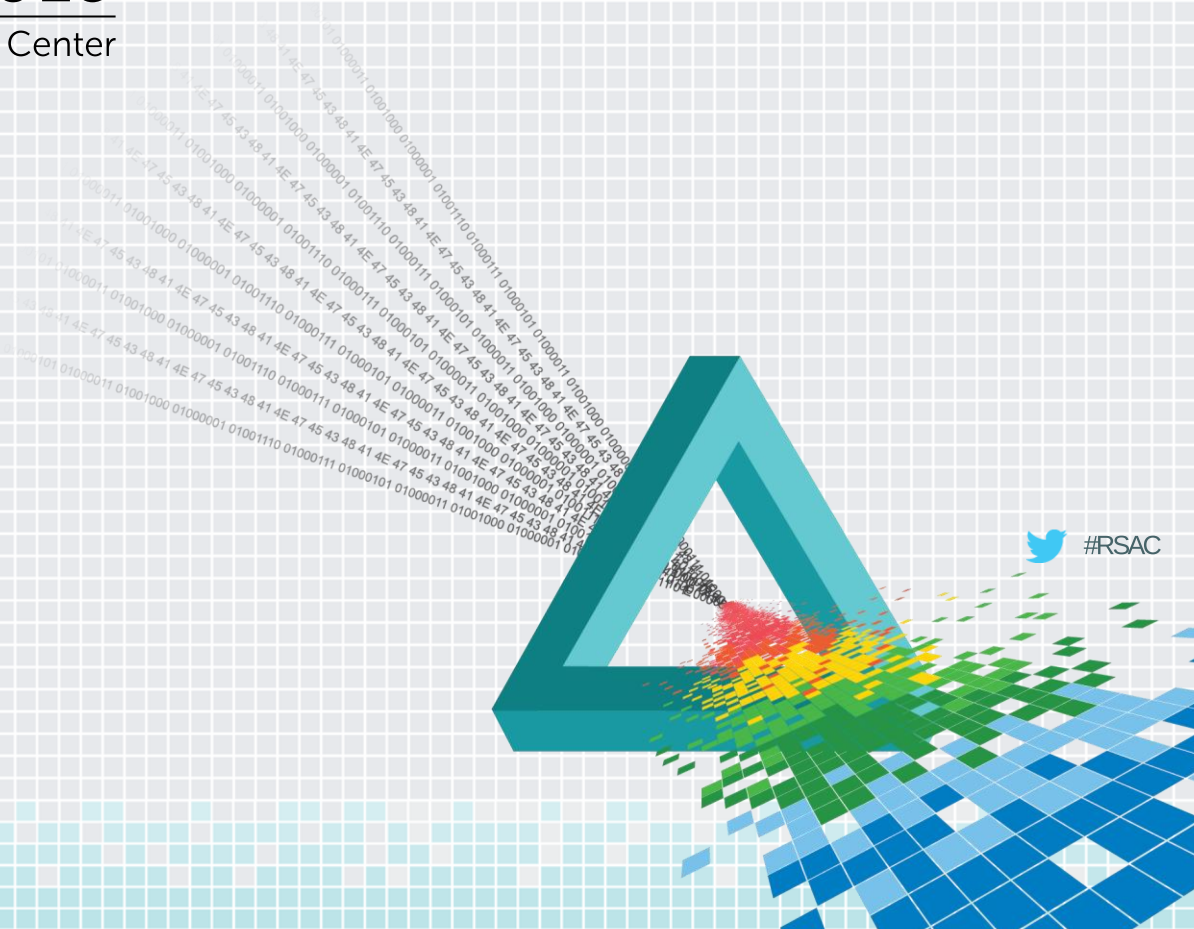
Be Flexible and Data-Driven

- What things are you doing “because we have always done it this way?”
  - And how does that distort your budget and resourcing?

- What value are you getting from the technologies you have deployed?

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Apply

Applying These Concepts

- When you get back to the office:
  - Take a development manager to lunch
  - Find out how they manage their workload
  - Find out their big process/tool initiatives for the next quarter/year

- In the next 3-6 months:
  - Run some lightweight metrics to see if your app security program “makes sense”
  - Run some security “lunch and learn” events for developers

And We'll Close with This

Contact

Dan Cornell

CTO, Denim Group

dan@denimgroup.com

@danielcornell