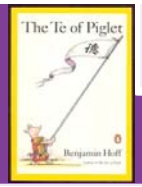

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center
Connect to Protect
CSV-W02
DevSecOps - The 道 of Security Science
Scott C. Kennedy
Security Scientist/Manager SSFTI
Cyber Security Team - Intuit
#RSAC

What is Tao? 道?



- Not a name for a 'thing'
  - An underlying natural order of the universe
  - Hard to grasp, easy to see.
- 道 = Radical 辶 (go forward/walk/walking)
  + 首 (head)
- Loosely understood as a concept of…
  - A road, way, path, or route
    - The way one goes somewhere
  - Or a doctrine, principle
    - The way one does or believes something

All quotes used in this text box are from ***The Complete Tao Te Ching***
Translated by Gia-fu Feng and Jane English, Vintage Books, 1989

How does this relate to IT/Security?

"The world is ruled by letting things take their course, it cannot be ruled by interfering." - **Tao Te Ching** (chapter 48)

Which works better? DevSecOps?

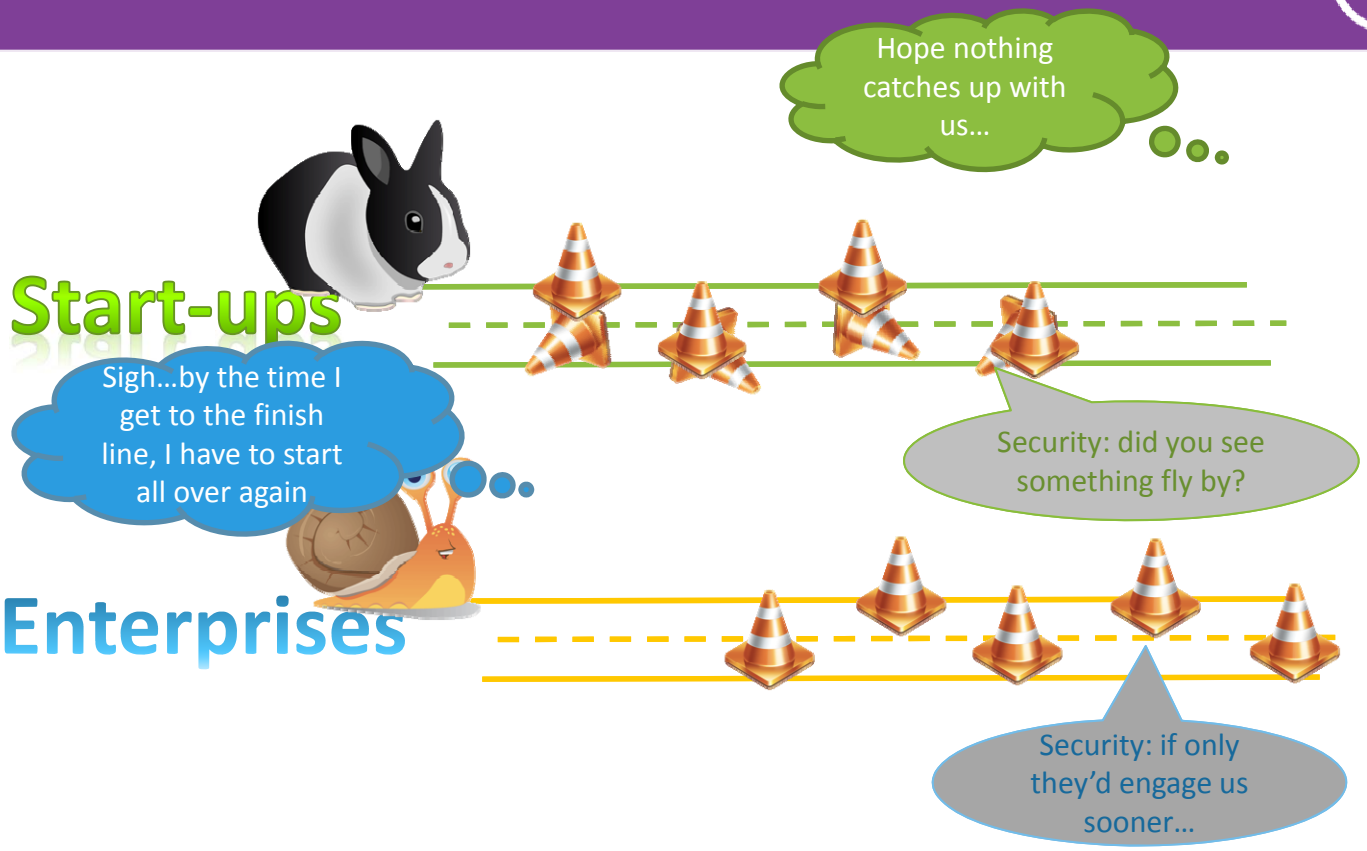
"Nothing is more soft and yielding than water, yet for attacking the solid and the strong, nothing is better." - **Tao Te Ching** (chapter 78)

What is DevSecOps?

- Agile discipline – Rugged Ops for Security
- Best of each security specialty in one framework
- Value provided to the business as security services
- Make it easy for business to take the right risks
- Reduce friction and disruptions with developers
- Continuous improvement mindset

"In dealing with others, be gentle and kind. In speech, be true. In ruling, be just. In daily life, be competent. In action, be aware of the time and the season. No fight: No blame. " - **Tao Te Ching** (chapter 8)

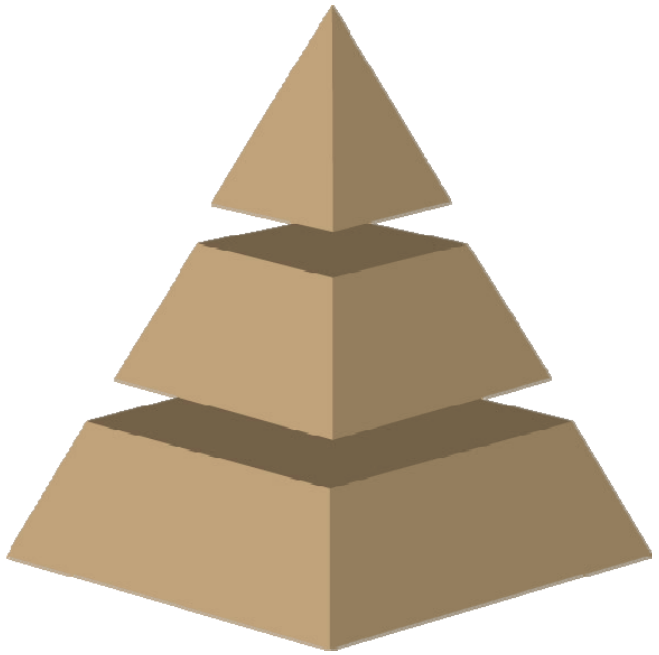
The Innovation Race



"The softest thing in the universe, Overcomes the hardest thing in the universe." - **Tao Te Ching** (chapter 43)

Step Zero: Establishing DevSecOps Principles

1. Customer focused mindset
2. Scale, scale, scale
3. Objective criteria and analysis
4. Proactive hunting & RedTeaming
5. Continuous detection & response



"If I have even just a little sense, I will walk on the main road and my only fear will be of straying from it. Keeping to the main road is easy, but people love to be sidetracked." - **Tao Te Ching** (chapter 53)

The Arts/Wushu of DevSecOps

DevSecOps

Security Engineering	Security Operations	Compliance Operations	Security Science
Experiment, Automate, Test	Hunt, Detect, Contain	Respond, Manage, Train	Learn, Measure, Forecast

"Empty yourself of everything. Let the mind become still. The ten thousand things rise and fall while the Self watches their return. They grow and flourish and then return to the source." - **Tao Te Ching** (chapter 16)

Security Science?

- From F.U.D. to facts
- Science is a fact-based examination
  - Theories established
  - Testable against real data
  - Revised and retested as the landscape changes…
  - Question -> Hypotheses -> Experiment -> Analyze -> Repeat
- Answers simple questions

"Knowing ignorance is strength; ignoring knowledge is sickness." - **Tao Te Ching** (chapter 71)

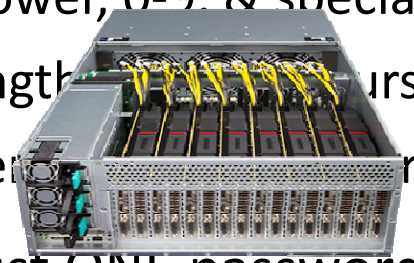
Examples of Security Science

- What is your Password policy? Why?
  - With an attacker with a budget of $10,000, we ought to set our minimum length to 12 characters if we rotate our Linux passwords every 90 days.
- How frequently do you need to patch/restack to avoid CVSS > 5.0?
  - With the Amazon RHEL image, historically it's been every 5.3 days.
  - With our smaller base RHEL image, historically it's been 10.5 days.
- Minimum Length of password vs. algorithm used to store it safely?
  - MD-5 = 19 characters against a $10,000 attacker budget
  - SHA-512 = 11 characters against a $10,000 attacker budget
  - Bcrypt = 8 characters against a $10,000 attacker budget

"The truly great man dwells on what is real and not what is on the surface." - **Tao Te Ching** (chapter 38)

Explain that password thing some more?

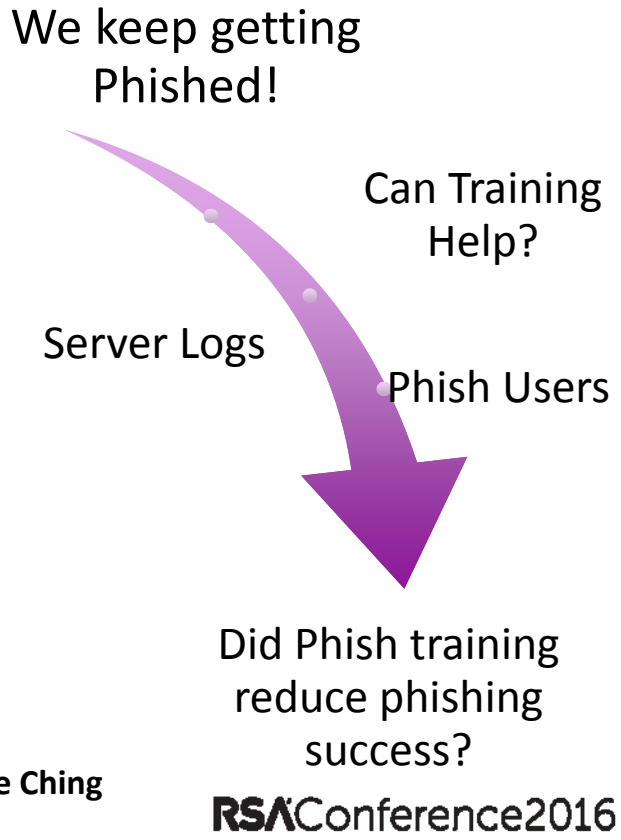
- With a budget of $10,000, what can an attacker do?
  - 79.362 billion MD5 hash attempts per second
  - 2.2362 billion SHA-512 hash attempts per second
- With that performance, the attacker can brute force
  - ***EVERY SINGL***UPPER, lower, 0-9, & special ch ord
  - rs in length urs
  - le rs
- Probability of cracking just ONE password that is t rotated?



"Seeing the small is insight; Yielding to force is strength. Using the outer light, return to insight, and in this way be saved from harm. " - **Tao Te Ching** (chapter 52)

How to start Security Science?

- Look at your company.
  - What questions need answers?
- Theorize a solution
  - How do you think to solve this?
- Gather data to investigate.
  - What sources do you need?
  - What are you missing? How to get it?
- Analyze data to confirm/dispute
  - Was your assumption, correct?



"Perseverance is a sign of will power. He who stays where he is endures." - **Tao Te Ching** (chapter 33)

How we started to find our own problems.

- Previously, established a Red Team to help elevate security issues
  - Rules of engagements were
  - ”Act like an attacker” but “Do
- Where to start?
  - Production hosts? Developme
- Red Team phished our own se
  - Had a very well crafted phish

From: Intuit Purchasing Card Team <Purchasing_Card_Team@intuit.com>
Date: September 12, 2015 at 4:02:36 PM PDT
To: Bogus Employee <bogus.employee@intuit.com>
Subject: Action Required: Pcard Fraudulent Activity

Hello Bogus,

Our records indicate that possible fraudulent activity has been detected on your credit card. Per Intuit's cardholder agreement, it is mandatory to verify the associated charges. Please update the database to accept or deny the charge.

Your credit card will be suspended if no action is taken by September 14th 2015.

Employee	Location	Expense Submitted	ER #	Merchant	Expense Type	Line Amount	Click for Record
Employee, Bogus	US	8/4/2015 21:38	ER83A4666	HOTELS.COM266987934512	Lodging	3,133.77	https://This_LooksReallyFake.html

Please be informed that your manager is copied on this email for visibility.

Thank you,

Intuit Purchasing Card Team

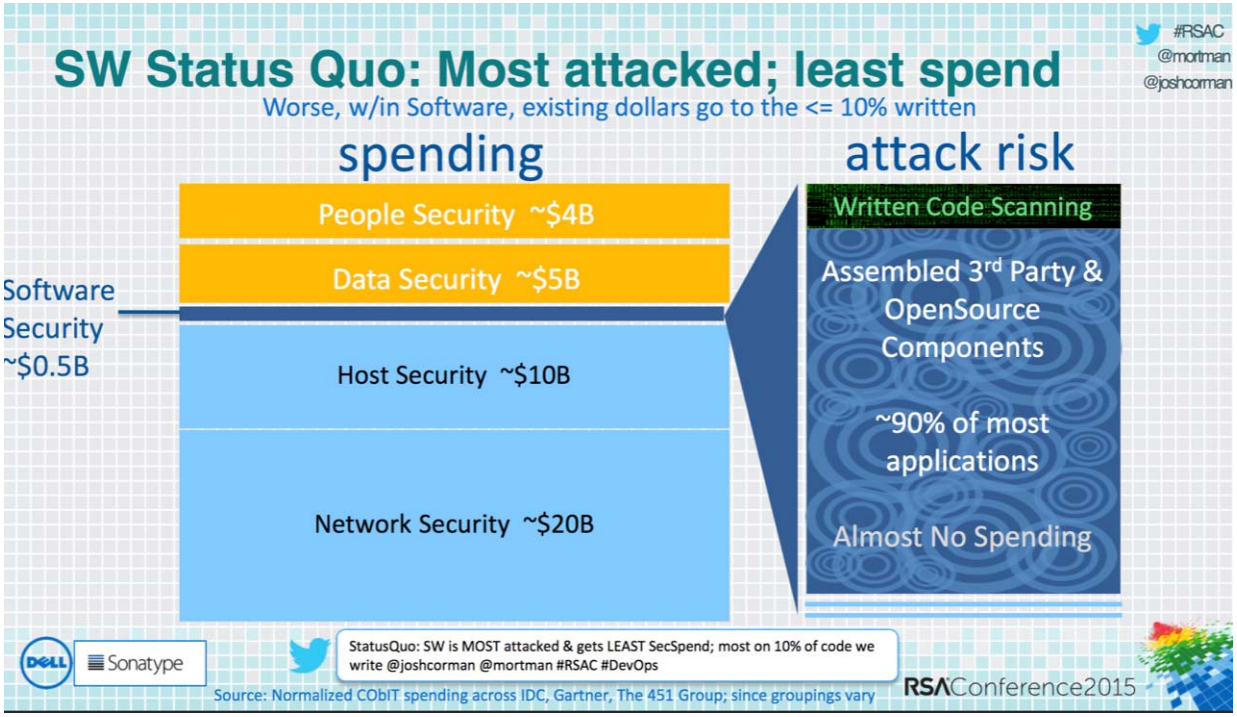
“Ruling the country is like cooking a small fish. Approach the universe with Tao, and evil is not powerful, but its power will not be used to harm others. ” - **Tao Te Ching** (chapter 60)

Phishing ourselves taught us…

- Achieved **54%** click through rate, with Security Professionals!
- Women are **25%** more likely than men to click
- **1/3** tested will click on a link, access a site and enter details, even when they suspect it is suspicious
- Existing security awareness/phishing training campaigns did not prevent this
- Need to better socialize “Red Team” actions

“In caring for others and serving heaven, There is nothing like using restraint. Restraint begins with giving up one's own ideas.” - **Tao Te Ching** (chapter 59)

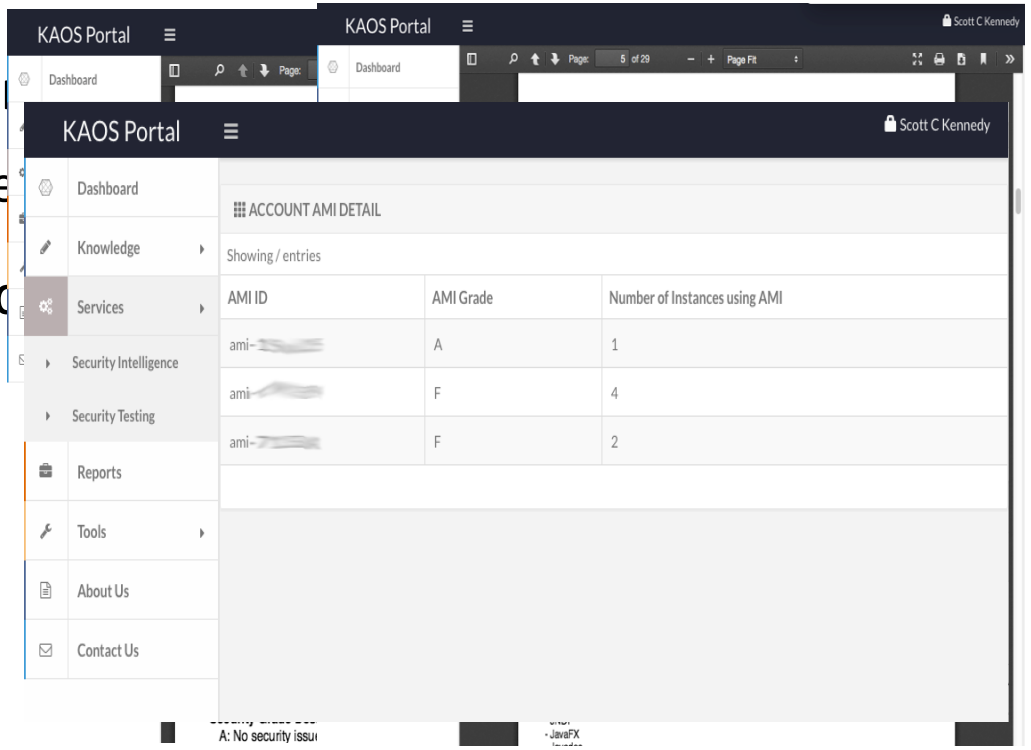
Where else can we use more Science?



"Knowing others is wisdom; Knowing the self is enlightenment. Mastering others requires force; Mastering the self needs strength. He who knows he has enough is rich. " - **Tao Te Ching** (chapter 33)

How to fix the lack of security spend?

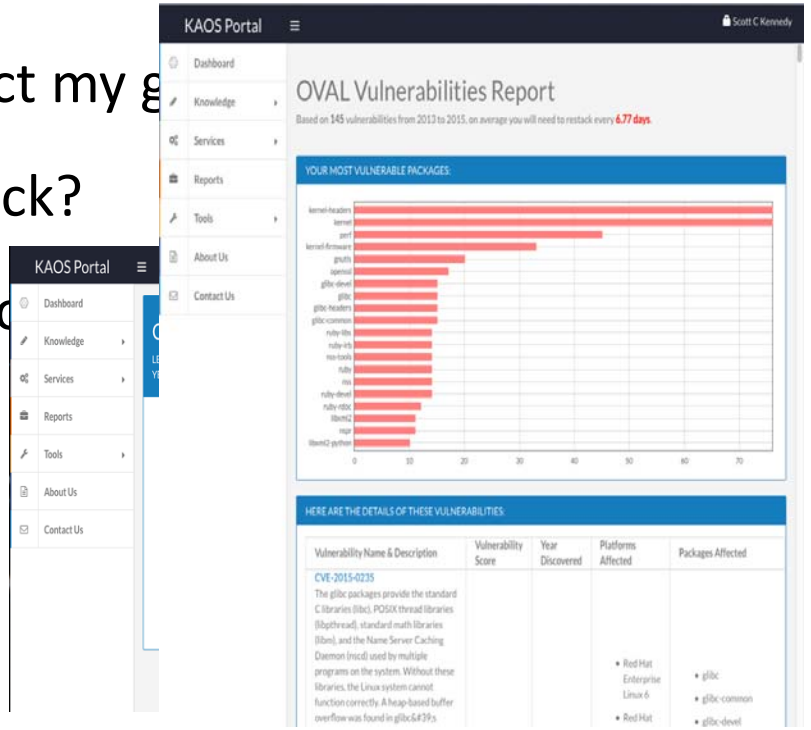
- Scoring/Grades are powe
  - Consistent and defensible
- Allows the Dev leader to
  - Why am I failing?
  - Where am I using that?



"A man is born gentle and weak; at his death he is hard and stiff. Green plants are tender and filled with sap; at their death they are withered and dry. Therefore, the stiff and unbending is a disciple of death; the gentle and yielding is a disciple of life." - **Tao Te Ching** (chapter 76)

Use Models to guide away from mistakes

- How do the decisions I make affect my g
- How frequently do I have to restack?
- What is the impact of package cho
  - Ruby or Python?
  - MySQL or Postgres?
  - Apache or Nginx?



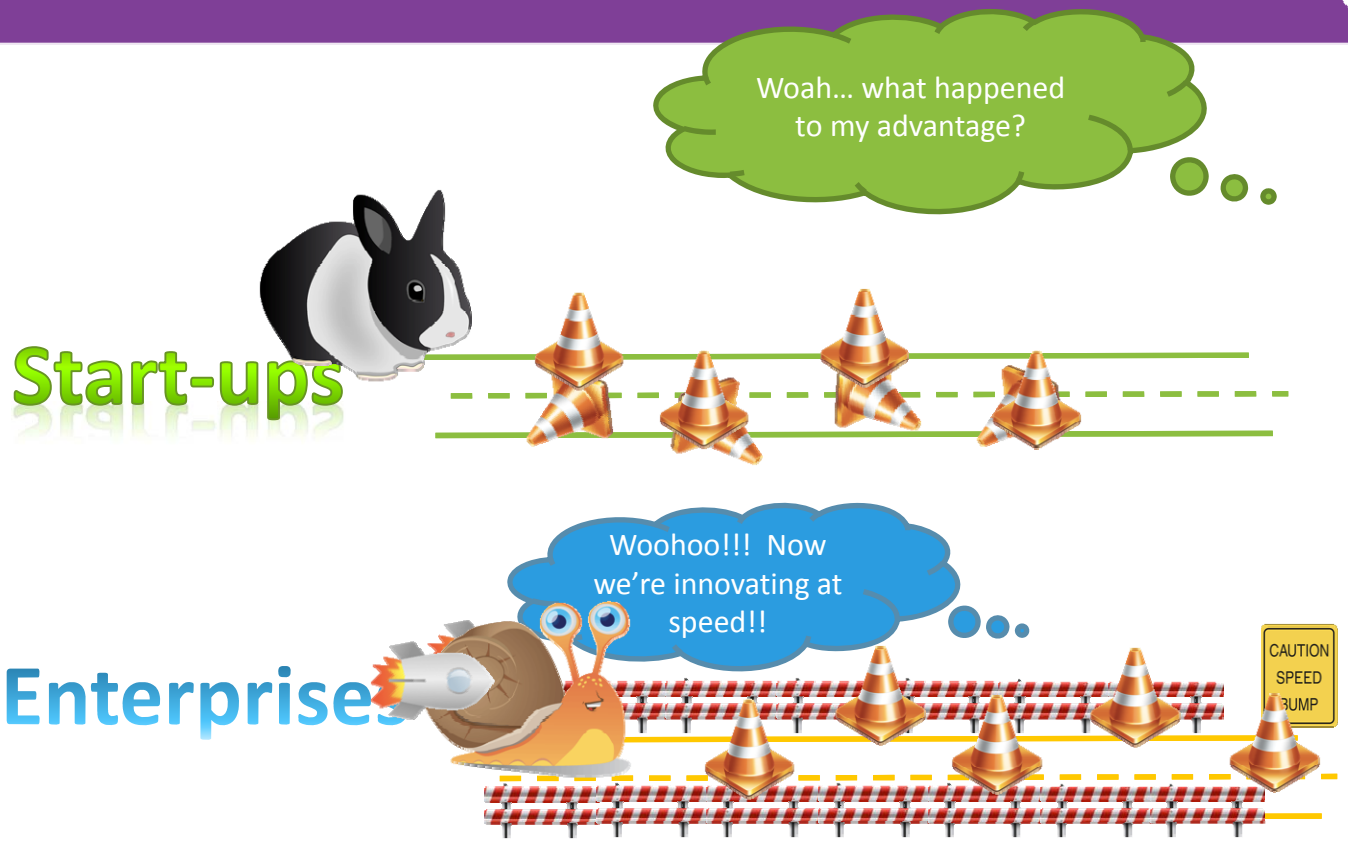
"The farther you go, the less you know. Thus the sage knows without traveling; He sees without looking; He works without doing." - **Tao Te Ching** (chapter 47)

Security Science can provide …

- Insights to steer policy creation
- Understanding to drive adoption
- Development goals to “move the needle”
- Analysis of existing data to uncover new “truths”

“A good walker leaves no tracks; A good speaker makes no slips; A good reckoner needs no tally. A good door needs no lock, yet no one can open it.” - **Tao Te Ching** (chapter 27)

The Innovation Race redux



"If I have even just a little sense, I will walk on the main road and my only fear will be of straying from it." - **Tao Te Ching** (chapter 53)

Apply What You Have Learned Today

- Next week you should:
  - Join the DevSecOps Community via LinkedIn and Twitter.
  - Start looking at how your company makes decisions in security.
- In the first three months following this presentation you should:
  - Choose a security science experiment to run in your organization.
  - Build a platform to collect the data to support/refute your experiment.
- Within six months you should:
  - Have a foundational data platform that supports basic security science decisions
  - Begin to provide results from your experiment

e pursuit of learning, every day something is acquired. In the pursuit of Tao, every
omething is dropped. Less and less is done, until non-action is achieved. When
ng is done, nothing is left undone." - **Tao Te Ching** (chapter 48)

Tie It Together: 道=path to understanding

- Security needs to switch from “NO!” to “Know!”
- Run your own experiments and test your hypotheses
- Share with your colleagues and customers.
- For more information on DevSecOps
  http://DevSecOps.org
  http://linkedin.com/grp/home?gid=6817408
  http://github.com/devsecops
  http://twitter.com/devsecops
- For more quotes from the Tao Te Ching

  http://terebess.hu/english/tao/gia.html

d binding requires no knots, yet no one can loosen it. Therefore the sage takes care
men and abandons no one. He takes care of all things and abandons nothing.” -
e Ching (chapter 27)