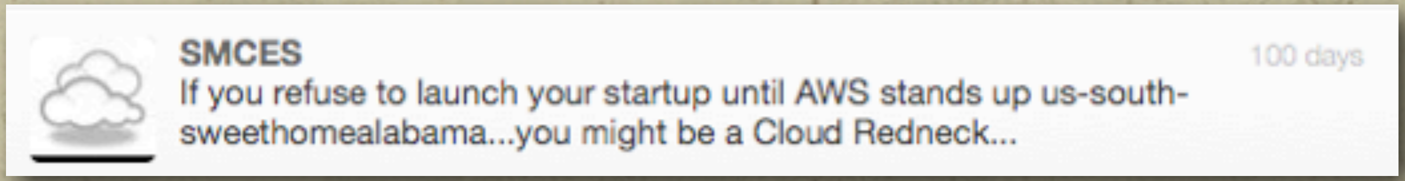
SH*T MY CLOUD EVANGELIST SAYS...

...JUST NOT TO MY CSO

ABOUT @BEAKER:

- I’m an a*hole with a blog (rationalsurvivability.com)
- Global Chief Security Architect for a company who provides networking & security widgets to SP’s & Enterprises
- Love Cloud & particularly fond of those that do my bidding in a manner commensurate with my OCD-driven need to manage outcomes in a reasonably predictable way



SMCES

100 days

If you refuse to launch your startup until AWS stands up us-south-sweethomealabama...you might be a Cloud Redneck...

<< @SMCES

DEFINING THE PROBLEM

IT’S A TRAP!

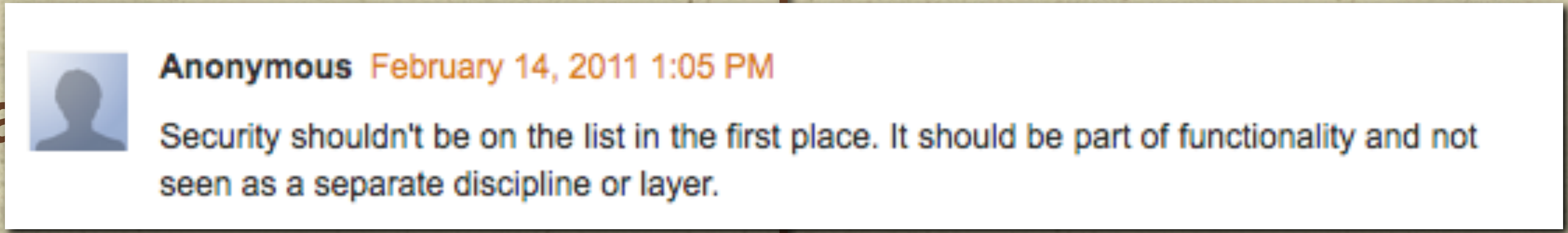
DEVELOPER PRIORITIES*	VS	SECURITY PRIORITIES
1. Functions and features as specified or envisioned		1. Security
2. Performance		2. Compliance
3. Usability		3. Uptime
4. Uptime		4. Performance
5. Maintainability		5. Functions and features as specified or envisioned
6. Security		6. Usability/Maintainability

**Mark Curphey - The Great Security Divide - Part 1 & John Wilander - Security People vs Developers*

DEVELOPER PRIORITIES* VS SECURITY PRIORITIES

1. Functions and features as specified or envisioned
2. Performance
3. Usa
4. Uptime
5. Maintainability
6. Security

1. Security
2. Compliance
4. Performance
5. Functions and features as specified or envisioned
6. Usability/Maintainability



Anonymous February 14, 2011 1:05 PM

Security shouldn't be on the list in the first place. It should be part of functionality and not seen as a separate discipline or layer.

**Mark Curphey - The Great Security Divide - Part 1 & John Wilander - Security People vs Developers*

@SMCES... VS ...SECURITY

- Cloud is **more secure**; security is more integrated and it's everyone's responsibility
- The Golden Rule: **Design for fail**
- Cloud is **more agile, costs less** and delivers more value, more quickly & flexibly and without capital costs
- The only "**True Cloud**" is Public, pay-per use, multi-tenant platforms. All else are "**False Clouds**"
- Legacy IT organizational hierarchy and siloed operations is dead. Long live Shadow IT and **DevOps...or NoOps**
- Automation enables simplicity, scalability, agility, resiliency and better security; **Availability is the priority**

- Cloud is **less secure** because developers can't detect & prevent basic threats, let alone complex, adaptive and emerging adversaries; See OWASP Top 10 vs APT
- Security is penalized severely for failure & is **expected never to fail** (even though it does)
- Cloud encourages bypassing controls, promotes **reckless operations** and will ultimately **cost more** to clean up the mess
- Private Clouds, extending in limited fashion to Public clouds will provide a controllable, **hybrid architecture** we can secure
- Compliance will have the last laugh when you bypass security and bad things happen; **Separation of Duties & Least Privilege**
- Abstraction yields "simplexity" and complex System Failures due to automation in security will be catastrophic; **Fail CLOSED**

WHAT'S MISSING?

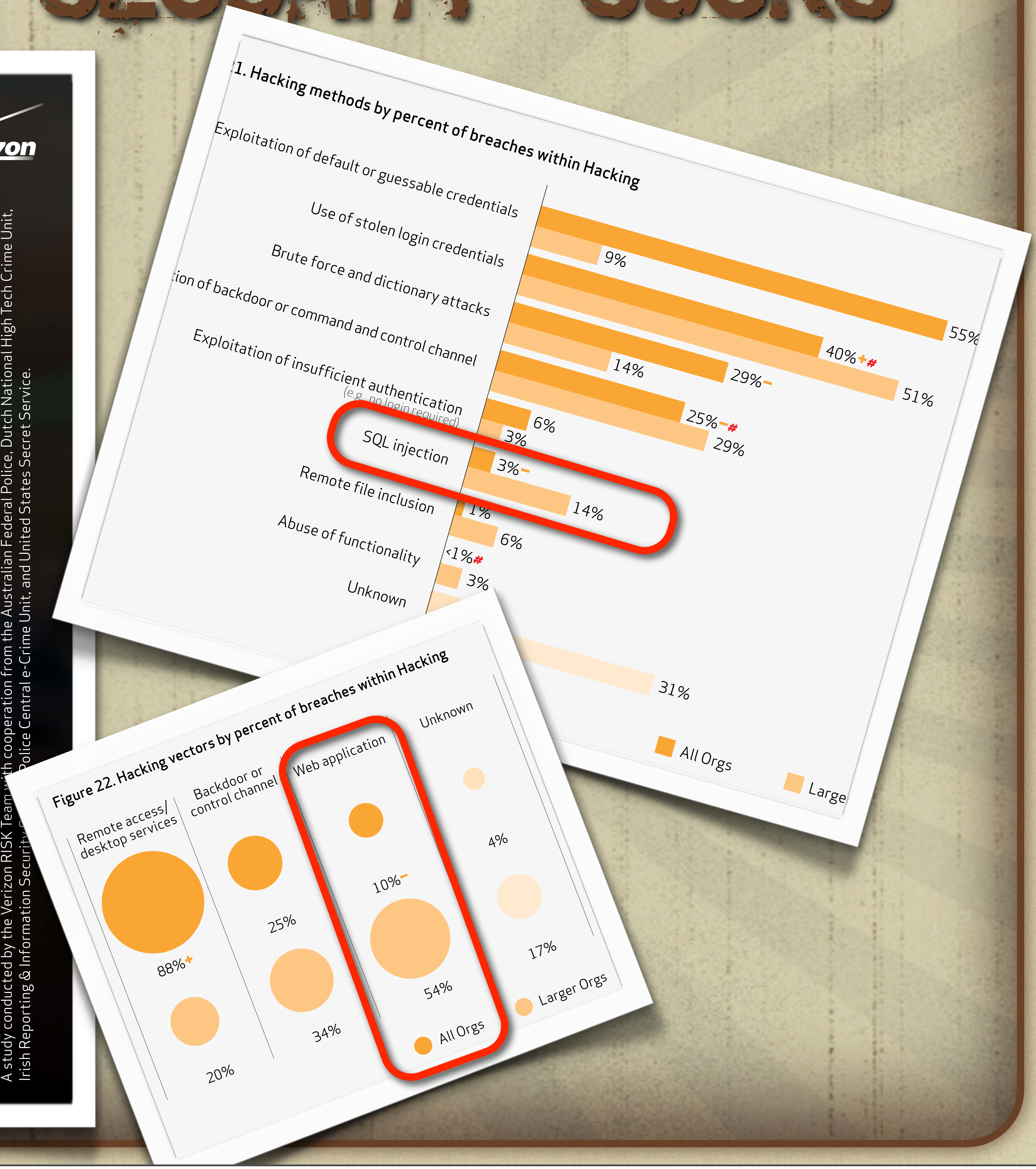
- Instrumentation that is inclusive of security
- Intelligence and context shared between infrastructure and applistructure layers
- Maturity of "automation mechanics" and frameworks
- Standard interfaces, precise syntactical representation of elemental security constructs < We need the "EC2 API" of Security
- An operational methodology that ensures a common understanding of outcomes & "Agile" culture in general
- Sanitary Application Security Practices

NASTY BITS

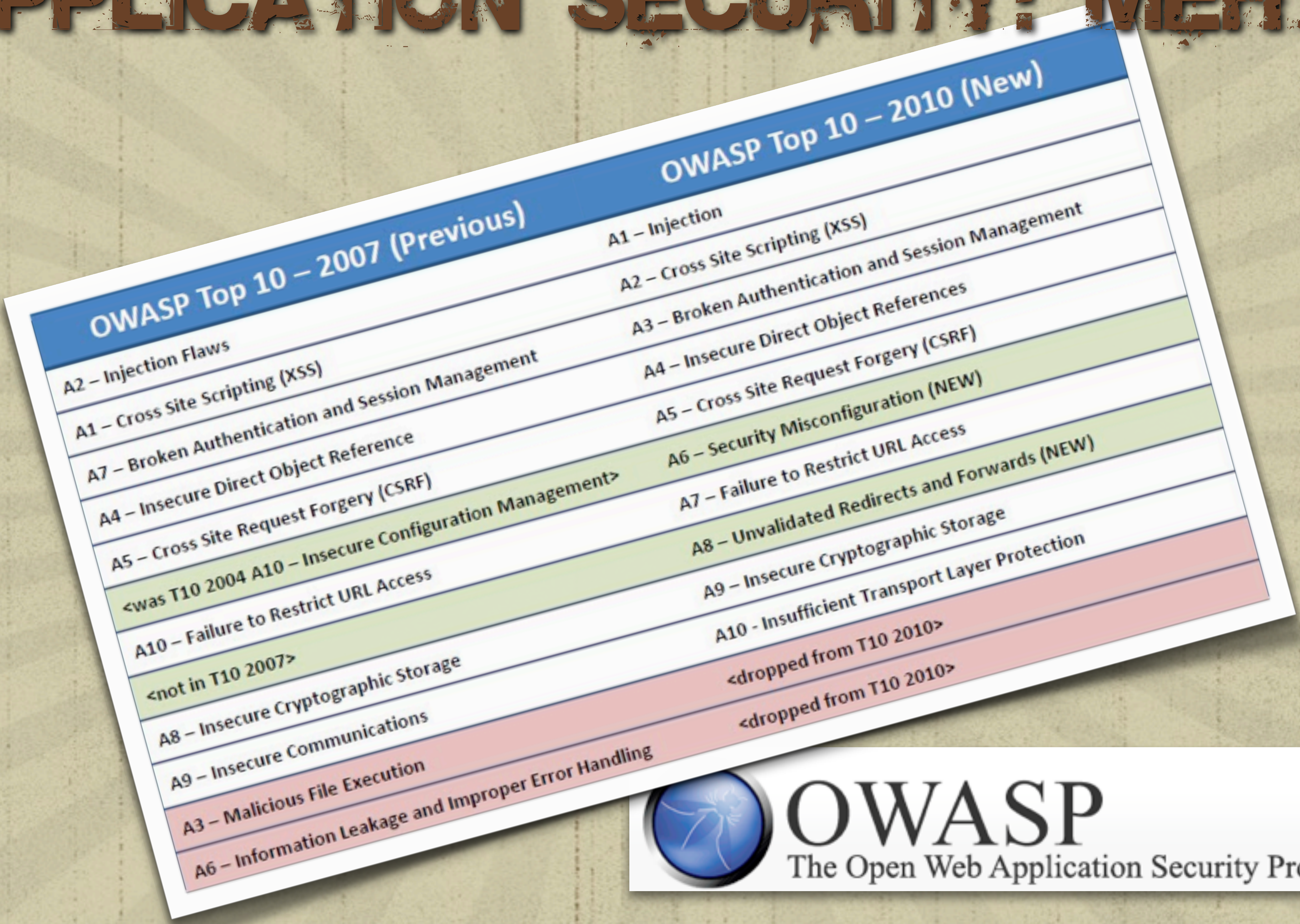
"INFORMATION SECURITY" SUCKS

2012 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security … Police Central e-Crime Unit, and United States Secret Service.



APPLICATION SECURITY: MEH

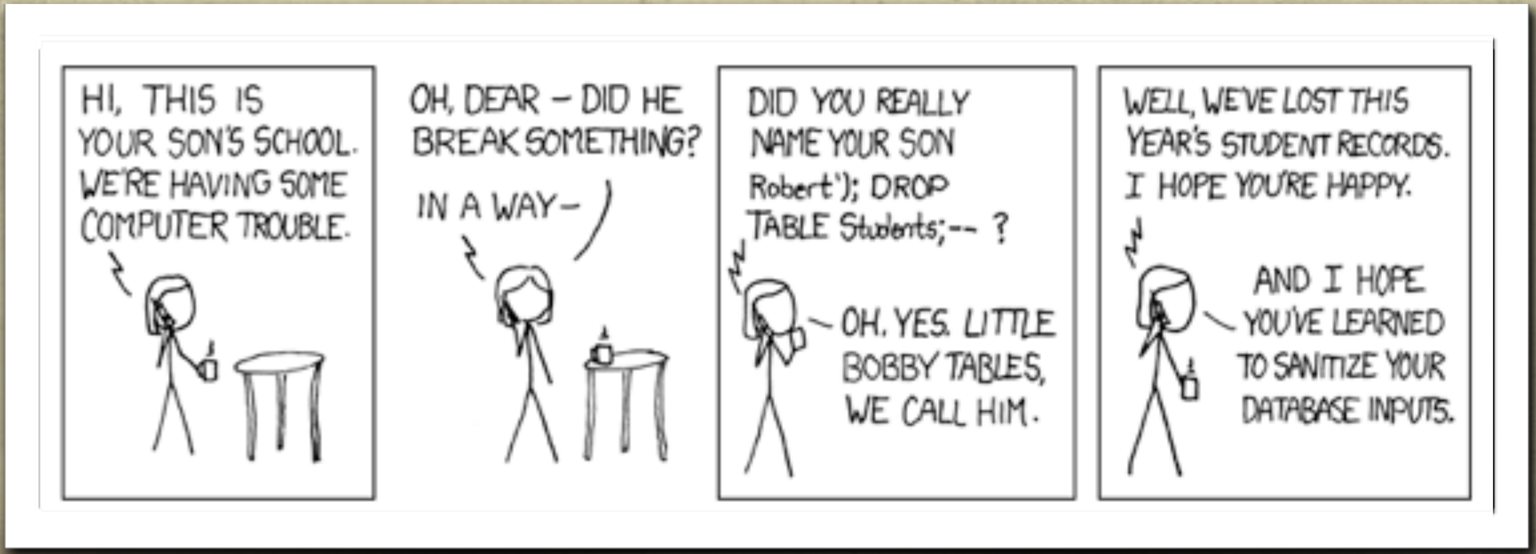


OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

OWASP
The Open Web Application Security Project

API SECURITY SUCKS HARDER

- Most Security Drones can’t spell XML
- ...they rarely use SOAP
- ...they don’t get REST
- SSL and Firewalls: the breakfast of champions


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

FOOL! YOU FELL VICTIM TO ONE OF THE CLASSIC BLUNDERS!

- Never Get Involved In a Cloud War In Asia
- Never Go In Against a Dutchman When APIs Are On the Line!

* You Can Order Iocaine Powder On Amazon - Free Shipping With Prime!

FOOL! YOU FELL VICTIM TO ONE OF THE CLASSIC BLUNDERS!

- Never Get Involved In a Cloud War In Asia
- Never Go In Against a Dutchman When APIs Are On the Line!

* You Can Order Iocaine Powder On Amazon - Free Shipping With Prime!

SH*T MY CLOUD EVANGELIST <u>FAILS</u> TO SAY...

CENSORED

AS ILLUSTRATED BY GEORGE'S 7 DIRTY WORDS

THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

...Of Cloud Security

SCALABILITY

- Distributed Networked System problems are tough; Distributed Networked System Security problems are tougher

- “Traditional” security doesn’t scale across distributed software-driven architecture; policies disconnected from workloads...more complicated as we go from IaaS > PaaS

- Unfortunate reconciliation of Metcalfe’s Law vs. Moore's Law vs. HD Moore’s Law (Casual Attacker power grows at the rate of Metasploit)

- Security is not programmatic & leveragable automation across heterogenous systems in security is LULZ

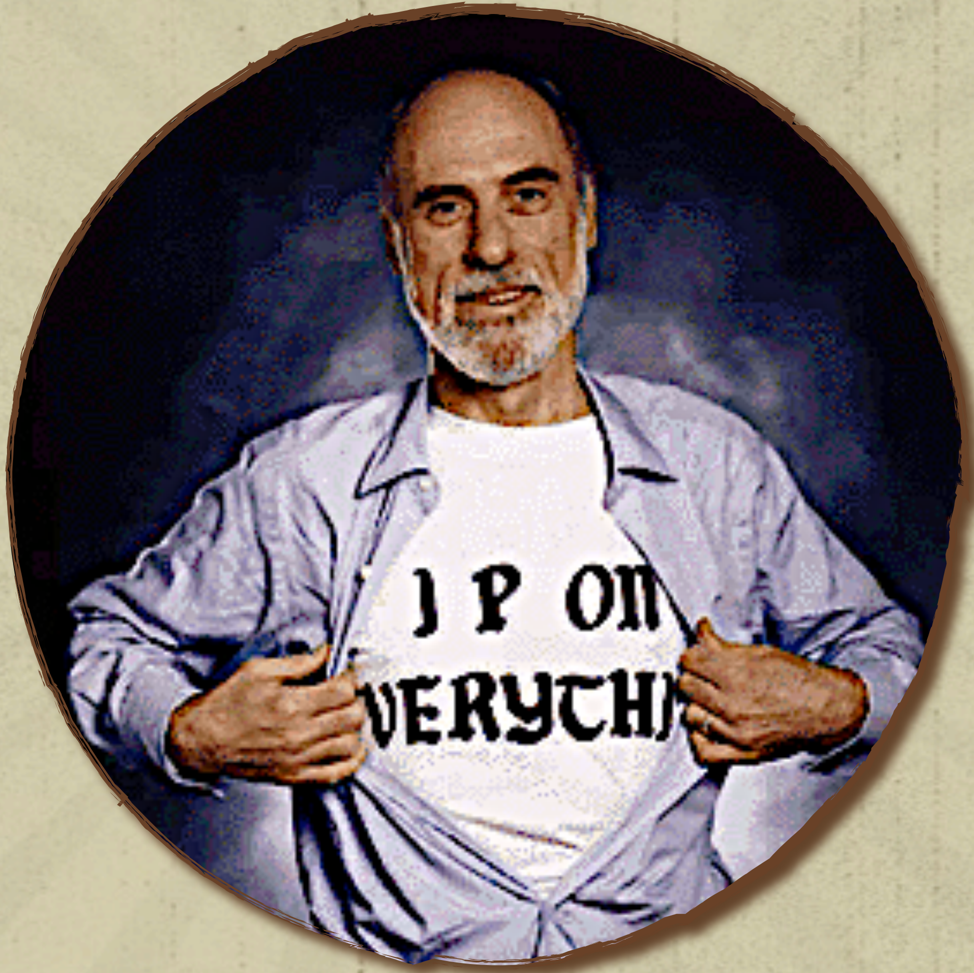
SECURITY @SCALE

- It doesn't. The MeatCloud giveth, the MeatCloud taketh away...
- Beyond Gb/s, Connections/s, flows, etc., security requires the notion of context, policy, and potentially state...eventual consistency doesn't work with security
- The Self-Defending {network | application} is complicated simultaneously with the concepts of "data gravity" and mobility

CLOUD: THE REVENGE OF VPN AND PKI

HINT: CLOUD SECURITY IS MORE THAN OVERLAY ENCRYPTION & MULTI-FACTOR AUTHENTICATION MECHANISMS

HE P'S ON EVERYTHING...



Everything's Connected

DO NOT POKE THE BEAR

If You Think A Noogie Is Bad, Try the Wedgie!

PORTABILITY

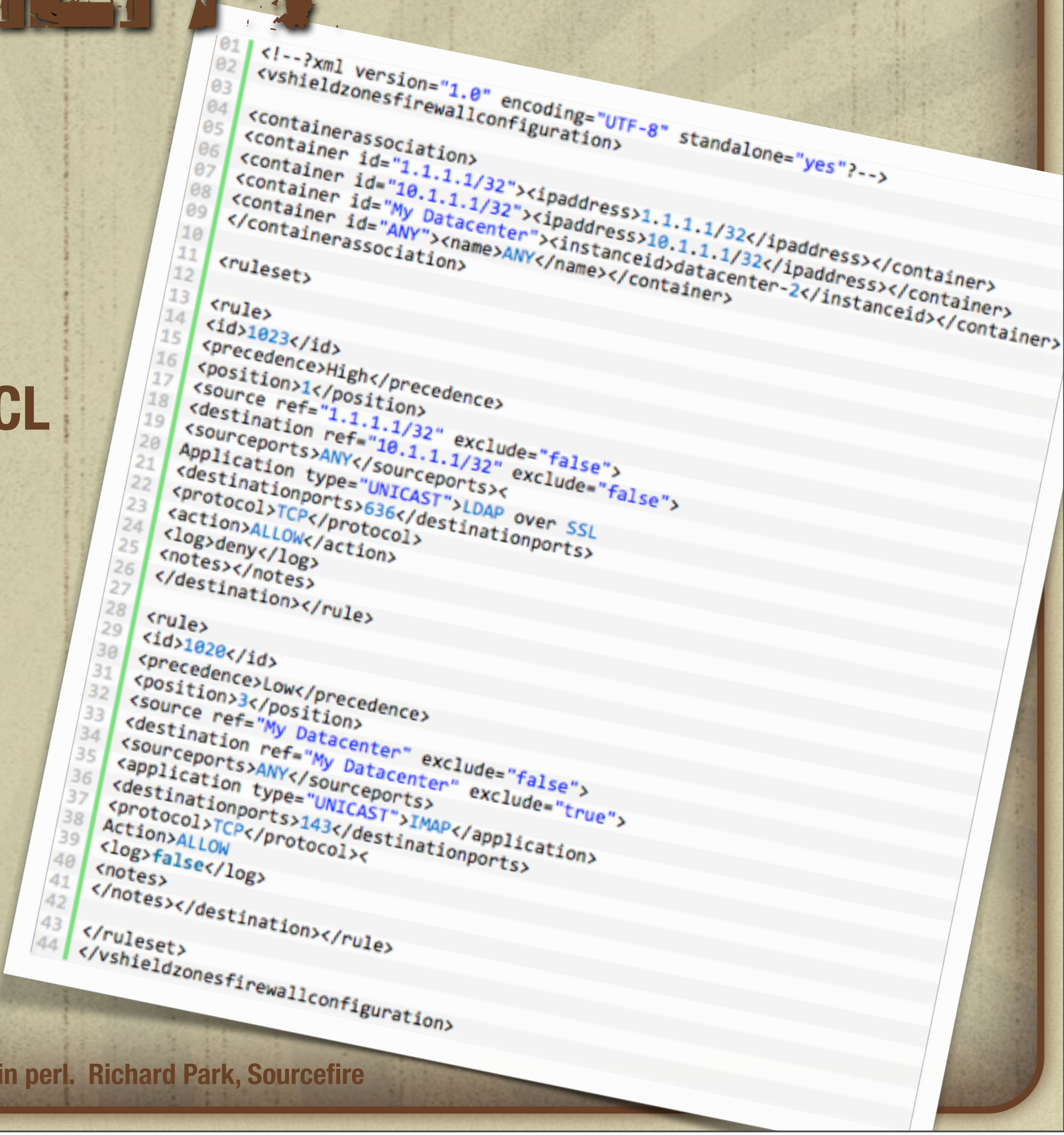
- If we don’t have consistency in standards/formats for workloads & stack insertion, we’re not going to have consistency in security; Lack of consistent telemetry

- Inconsistent policies and network topologies make security service, topology & device-specific...flatter means responses to “network” attacks must be dealt with by the application...or not

- Abstraction has become a distraction

PORTABILITY

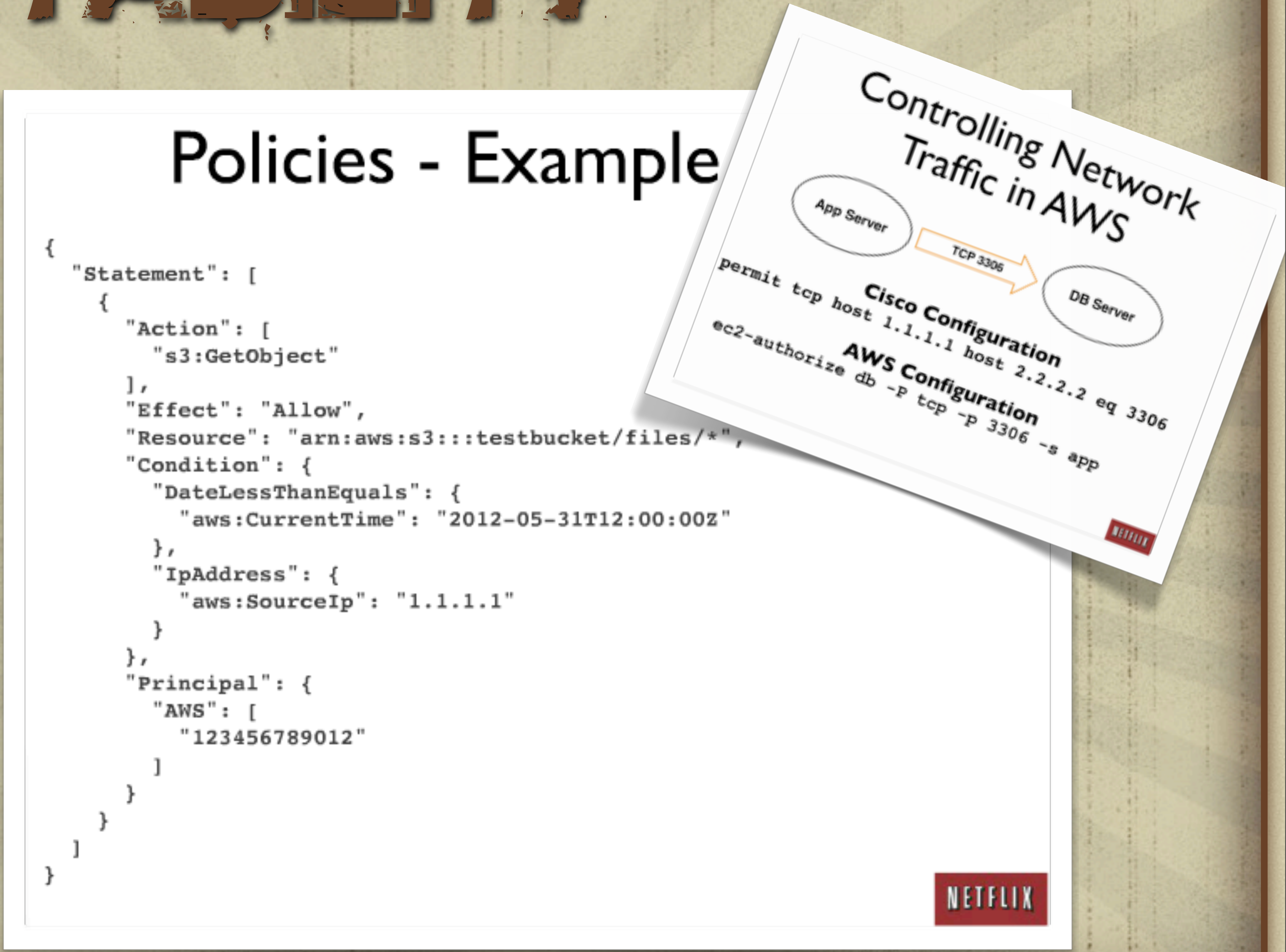
- Dude, Where's My IOS ACL 5-Tuple!?



```
<!--?xml version="1.0" encoding="UTF-8" standalone="yes"?-->
<vshieldzonesfirewallconfiguration>

<containerassociation>
<container id="1.1.1.1/32"><ipaddress>1.1.1.1/32</ipaddress></container>
<container id="10.1.1.1/32"><ipaddress>10.1.1.1/32</ipaddress></container>
<container id="My Datacenter"><instanceid>datacenter-2</instanceid></container>
<container id="ANY"><name>ANY</name></container>
</containerassociation>

<ruleset>

<rule>
<id>1023</id>
<precedence>High</precedence>
<position>1</position>
<source ref="1.1.1.1/32" exclude="false">
<destination ref="10.1.1.1/32" exclude="false">
<sourceports>ANY</sourceports><
Application type="UNICAST">LDAP over SSL
<destinationports>636</destinationports>
<protocol>TCP</protocol>
<action>ALLOW</action>
<log>deny</log>
<notes></notes>
</destination></rule>

<rule>
<id>1020</id>
<precedence>Low</precedence>
<position>3</position>
<source ref="My Datacenter" exclude="false">
<destination ref="My Datacenter" exclude="true">
<sourceports>ANY</sourceports>
<application type="UNICAST">IMAP</application>
<destinationports>143</destinationports>
<protocol>TCP</protocol><
Action>ALLOW
<log>false</log>
<notes>
</notes></destination></rule>

</ruleset>
</vshieldzonesfirewallconfiguration>
```

PORTABILITY

- ...or this:



Policies - Example

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::testbucket/files/*",
      "Condition": {
        "DateLessThanEquals": {
          "aws:CurrentTime": "2012-05-31T12:00:00Z"
        },
        "IpAddress": {
          "aws:SourceIp": "1.1.1.1"
        }
      },
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

Controlling Network Traffic in AWS

Cisco Configuration

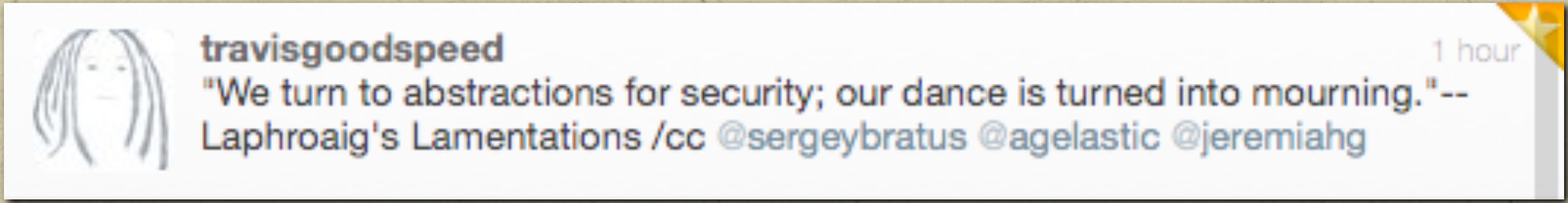
```
permit tcp host 1.1.1.1 host 2.2.2.2 eq 3306
```

AWS Configuration

```
ec2-authorize db -P tcp -p 3306 -s app
```

FUNGIBILITY

- Fundamentally, we need reusable and programmatic security design patterns; Controls today are CLI/GUI based



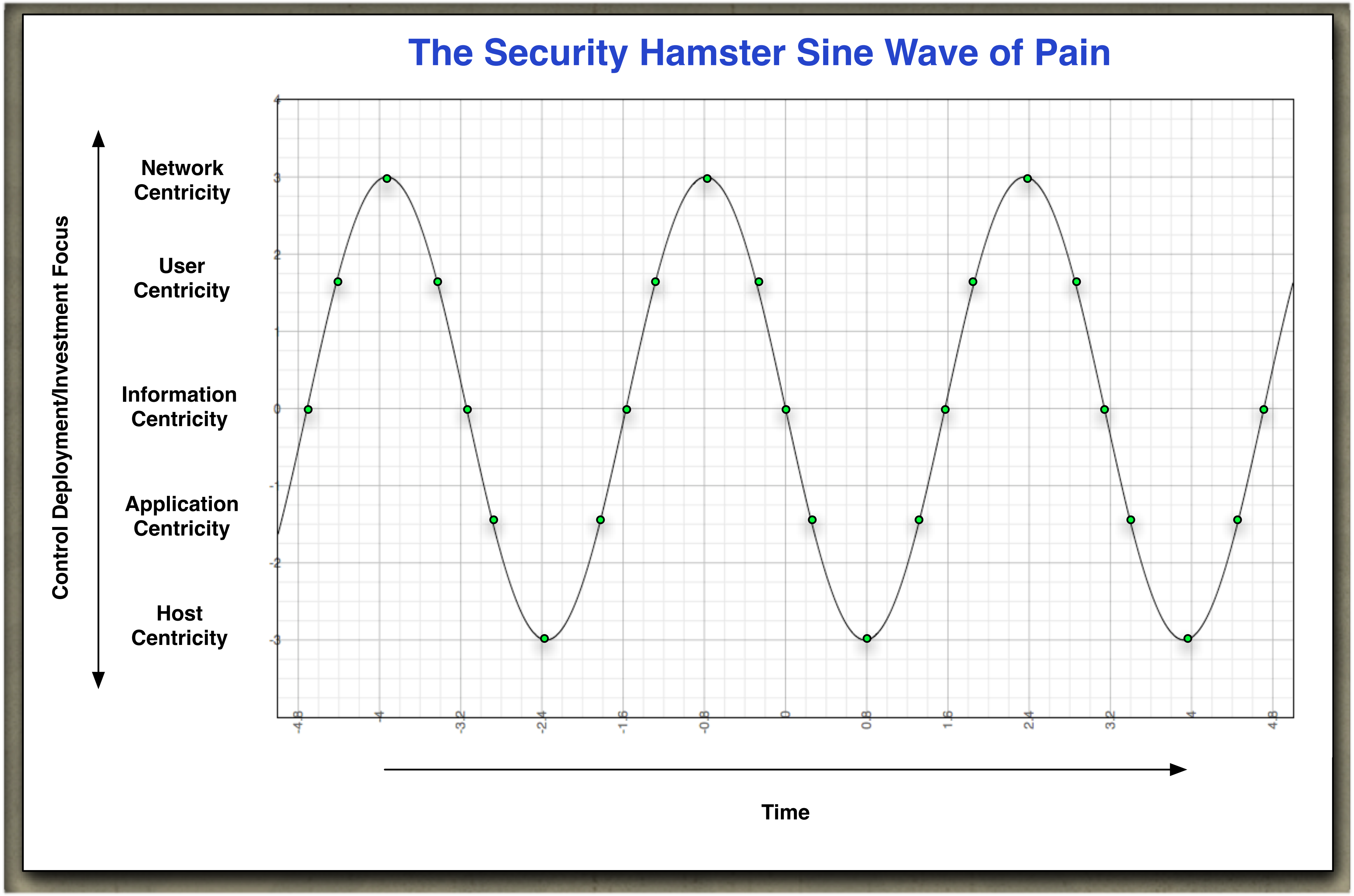
travisgoodspeed

"We turn to abstractions for security; our dance is turned into mourning."-- Laphroaig's Lamentations /cc @sergeybratus @agelastic @jeremiahg

- Each level of "the stack" means security controls can't be reused and are "slice" specific (more on this in a minute)
- If we're having trouble digesting IaaS, guess what PaaS does to the conversation?

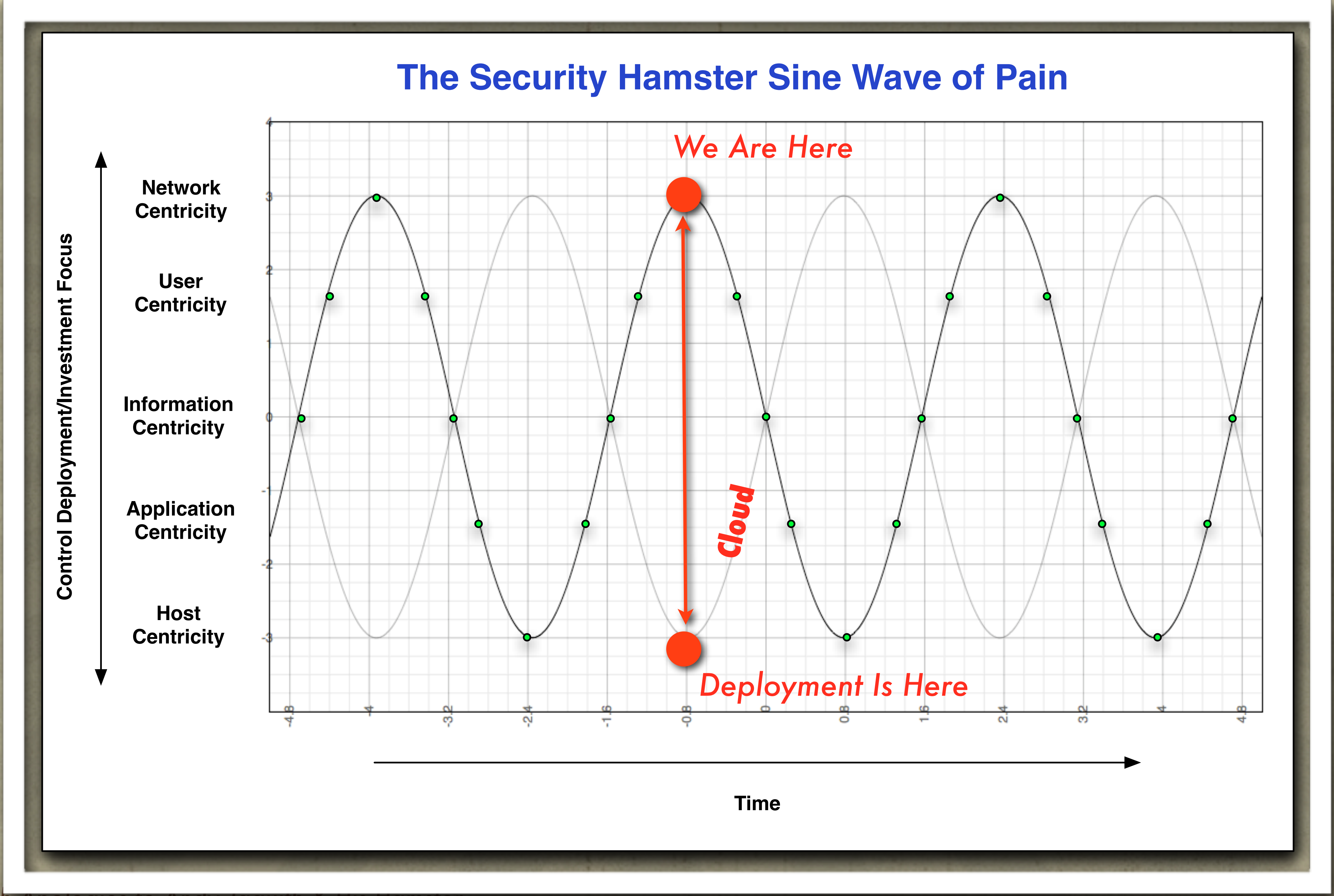
THE PROBLEM IS ALWAYS HAMSTERS

THE HAMSTER SINE WAVE OF PAIN...*



* *With Apologies to Andy Jaquith & His Hamster...*

THE HAMSTER SINE WAVE OF PAIN...*



* *With Apologies to Andy Jaquith & His Hamster...*

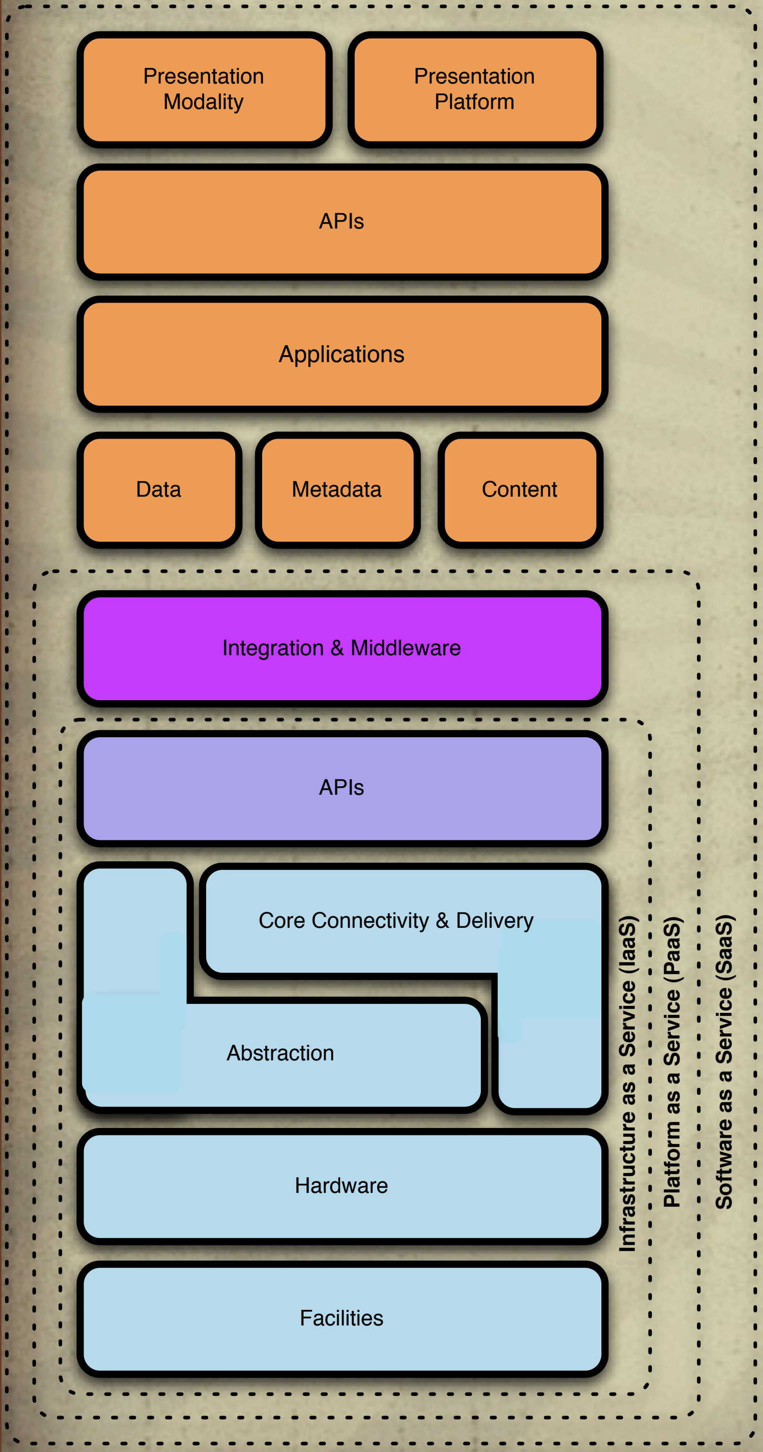
COMPLIANCE

- Security != Compliance and “security” doesn’t matter
- Regulatory compliance and frameworks don’t address emerging/disruptive innovation quickly enough - or at all
- How do we demonstrate compliance against measurements that don’t exist?
- Lack of automation for gathering audit/compliance artifacts

MAPPING THE MODEL TO THE METAL

Find the Gaps & Manage the Risk!

Cloud Model



Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Config. Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-Based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability MgMt
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

ISO

COBIT

COST

- Built-in or bolted on? Either way, it ain't free, or when it is, you get what you pay for and when it's not, you often don't

- It's a squeezing the balloon problem depending on where the stack focus is; CapEx v OpEx

- Device or service centric - costs shift, but management and quality/stability cost you in the long run

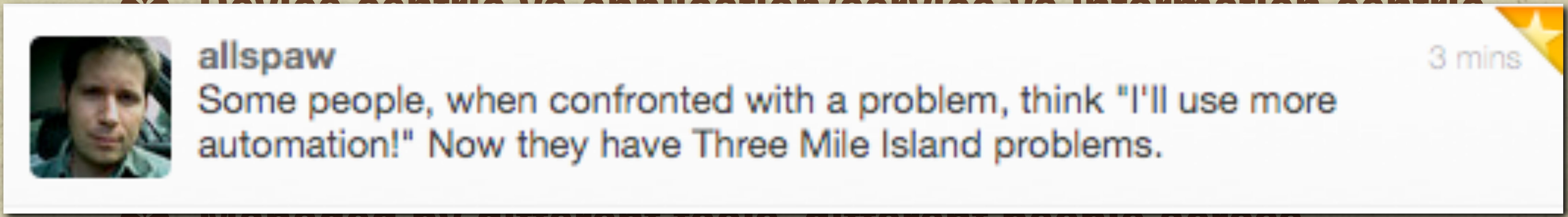
- Operational experience and expertise is expensive

MANAGEABILITY

- Security might be everywhere, but consistent management, visibility and instrumentation is not
- Device centric vs application/service vs information centric security poses challenges
- Managed by different tools, different people across discipline slices
- Differences in Deployment & Delivery Models
- APIs & Automation need nurturing

MANAGEABILITY

- Security might be everywhere, but consistent management, visibility and instrumentation is not
- Device centric vs application/service vs information centric



allspaw

3 mins

Some people, when confronted with a problem, think "I'll use more automation!" Now they have Three Mile Island problems.

- Managed by different tools, different people across discipline slices
- Differences in Deployment & Delivery Models
- APIs & Automation need nurturing

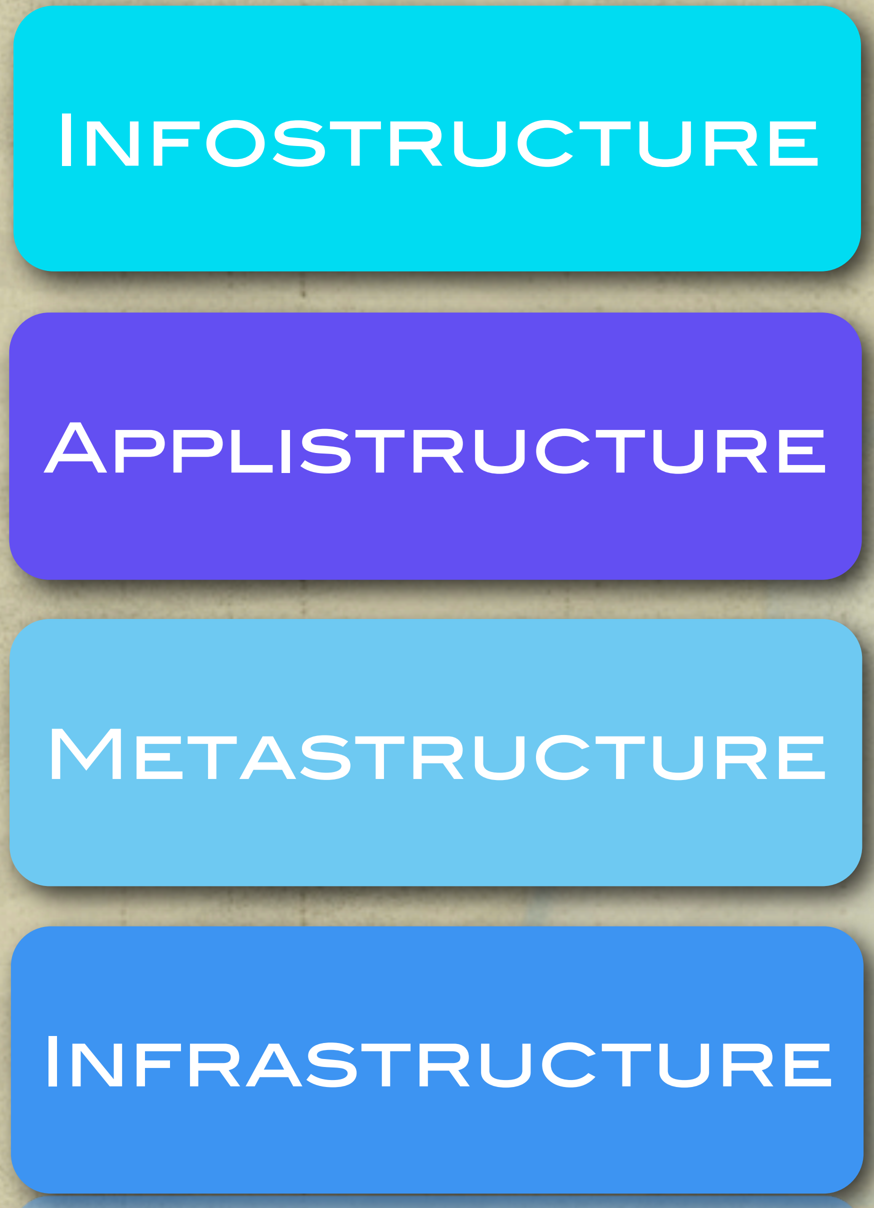
TRUST

- Trust models in computing are horribly warped and based on 40 year old approaches that continue to deteriorate (See: DAC, Multi-User OS, SSL Certs, DNS, etc.)
- Adding more abstraction & stirring in mobility makes the security problem more obtuse and operationally opaque
- We don’t have a consistent way to measure and compare trust levels, so we hope instead
- ...so, we don’t “trust” the Cloud...

...WHEN YOU THINK ABOUT IT

- Client/Server Computing broke our security models
- We transitioned from "secure" operating systems with mandatory access control security models to discretionary access control and kernel/user modes with lousy process isolation. Server Virtualization was an attempt to fix that.
- If you think about it, Cloud (PaaS) reapportions the "user" mode to a web browser on one end and "kernel" on the other with mandatory access control across platforms that are designed around process isolation and programmatic security models
- When done right, we realize the "re-centralization" of computing via cloud platforms and the distribution of consumption via web browsers

The Stack


Infostructure

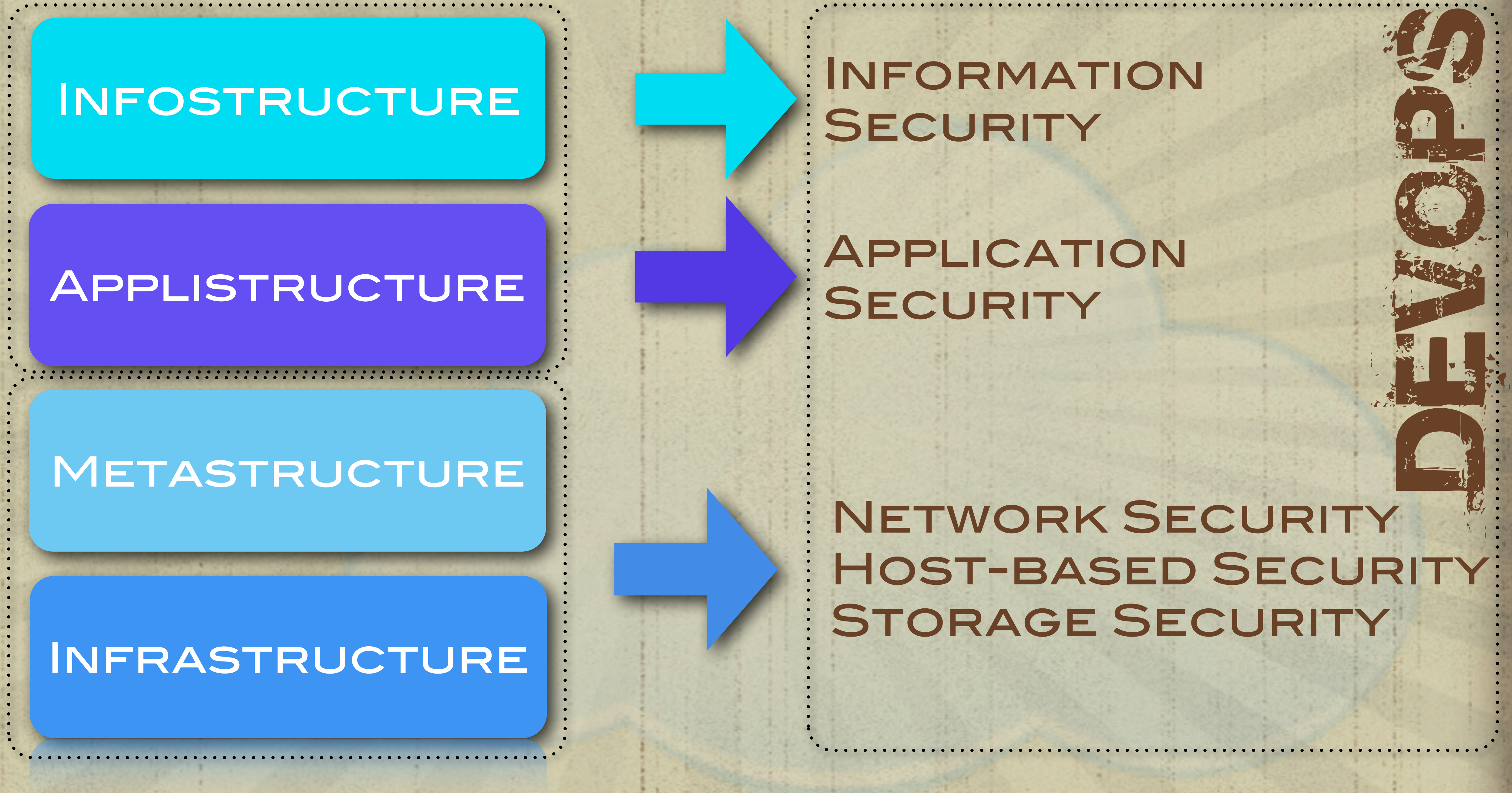
Applistructure

Metastructure

Infrastructure

- Content & Context -
  Data & Information
- Apps & Widgets -
  Applications & Services
- Glue & Guts -
  IPAM, IAM, BGP, DNS, SSL, PKI
- Sprockets & Moving Parts -
  Compute, Network, Storage

THERE'S NO DISCIPLINE...



Infostructure

Applistructure

Metastructure

Infrastructure

Information Security

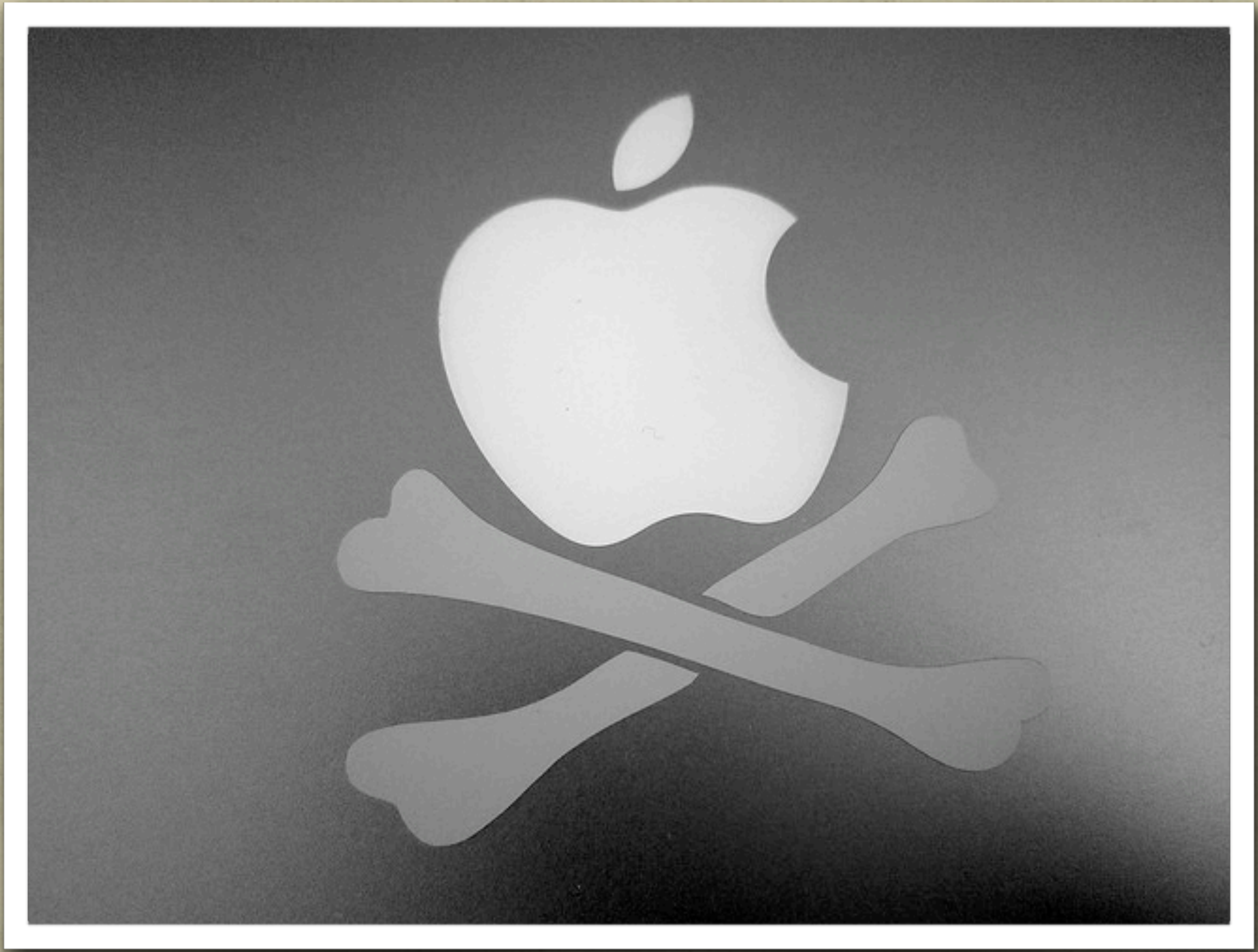
Application Security

Network Security
Host-based Security
Storage Security

DEVOPS

...IN OUR DISCIPLINE...

APPLE][VS MAC



THE DEVOPS DISCONNECT?

- Connectivity is what drove us from the original “Programmers Did It All” Model to the separate “Cylinders Of Excellence” we have today. Cloud is what’s pushing us back to it.
- Most DevOps teams don’t have dedicated security people, most enterprises do...see the problem?
- Making DevOps and “security” a religious/political debate versus a pragmatic, relevant and well-defined discussion of evolution instead of revolution is counter-productive
- We can’t afford a turf battle. This isn’t West Side Story.
- Besides, Security always has better knives (while you lot have better theme music and hipster dance moves)

BUT, BUT...NOT EVERYONE CAN BE A NETFLIX, ETSY, ZYNGA, ETC.

...NO, BUT EVERYONE SHOULD AIM TO BE...

PLATFORM, BITCHES!

- Today's Security Teams are invested in dealing with applications atop infrastructure that they own and protect with more infrastructure
- Developers are invested in iterating on software applications atop platforms that they own (and build, abstracted from infrastructure) and protect with more software
- See the difference? Help Security become invested in your platform; enroll them in your problem and they will help!

SECURITY
YOU'RE DOING IT WRONG

ANOTHER 7 WORDS...

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

1. Some
2. People
3. Forget
4. Cloud
5. Concerns
6. More (than)
7. Technology...

IF WE DON'T WORK TOGETHER WE CAN LOOK FORWARD TO:

- More Crappy, Uninformed Regulation/Law
- More FUD
- More Compliance Challenges
- More Privacy Concerns
- More Stupid Public vs. Private Cloud Battles & Stifled Progress
- More Turf Wars and an Ultimate Undermining Of Effort

IGNORANT AND SELF-RIGHTEOUS SECURITY TEAMS CAN BE EVEN MORE DANGEROUS THAN ATTACKERS

-- Vitaly Osipov (via Twitter on another topic completely ;)

EMPOWERED AND INFORMED SECURITY TEAMS CAN HELP ASSURE SUCCESS NOT IMPEDE IT.

-- Me

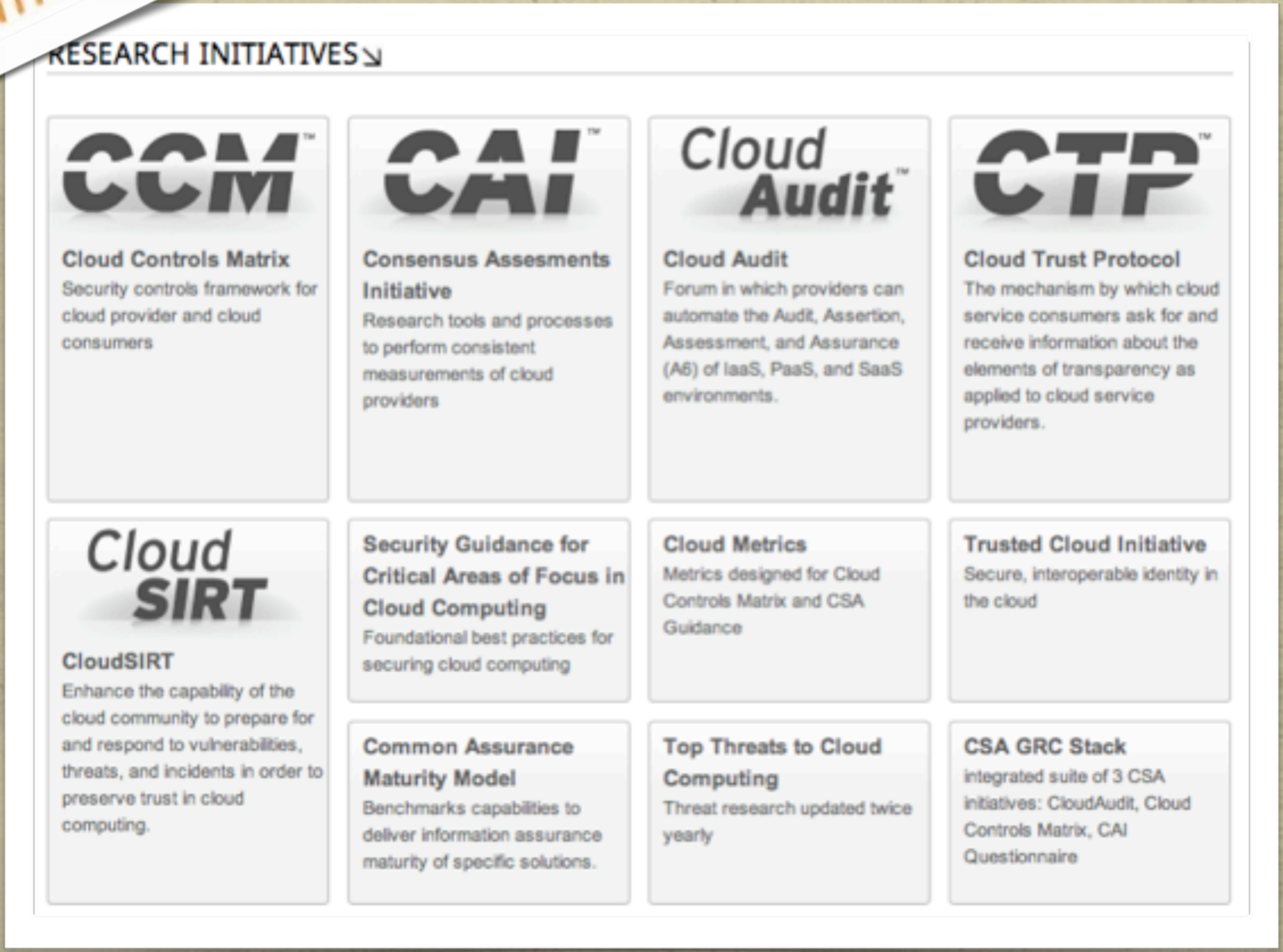
LET'S MAKE SECURITY: EFFICACIOUS, AUTOMATED, PROVABLE, USEABLE, RELIABLE, AND MANAGEABLE

LET'S ADD WHAT'S MISSING:

- Instrumentation that is inclusive of security
- Intelligence and context shared between infrastructure and applistructure layers
- Maturity of "automation mechanics" and frameworks
- Standard interfaces, precise syntactical representation of elemental security constructs
- An operational methodology that ensures a common understanding of outcomes & "Agile" culture in general
- Sanitary Application Security Practices

NEEDS DEVELOPERS/DEVOPS

CSA cloud security alliance



RESEARCH INITIATIVES↘

Cloud Controls Matrix
Security controls framework for cloud provider and cloud consumers

Consensus Assesments Initiative
Research tools and processes to perform consistent measurements of cloud providers

Cloud Audit
Forum in which providers can automate the Audit, Assertion, Assessment, and Assurance (A6) of IaaS, PaaS, and SaaS environments.

Cloud Trust Protocol
The mechanism by which cloud service consumers ask for and receive information about the elements of transparency as applied to cloud service providers.

CloudSIRT
Enhance the capability of the cloud community to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in cloud computing.

Security Guidance for Critical Areas of Focus in Cloud Computing
Foundational best practices for securing cloud computing

Cloud Metrics
Metrics designed for Cloud Controls Matrix and CSA Guidance

Trusted Cloud Initiative
Secure, interoperable identity in the cloud

Common Assurance Maturity Model
Benchmarks capabilities to deliver information assurance maturity of specific solutions.

Top Threats to Cloud Computing
Threat research updated twice yearly

CSA GRC Stack
integrated suite of 3 CSA initiatives: CloudAudit, Cloud Controls Matrix, CAI Questionnaire

HTTP://WWW.CLOUDSECURITYALLIANCE.ORG

IF WE DON'T GET THIS RIGHT...

...MANY CLOUD KITTEHS WILL PERISH AND @SMCES WILL CHURN SNARK

WINNING!

[Christofer] Hoff
choff@packetfilter.com
choff@juniper.net
@beaker
+1.978.631.0302

Other Presentations In The Series...

The Four Horsemen Of the Virtualization Apocalyps

Hoff | Blackhat

The Frogs Who Desired a King

A Virtualization & Cloud Computing Security Fable

Hoff | The Frogs Who Desired a King

Cloudifornication

Indiscriminate Information Intercourse Involving Internet Infrastructure

Hoff (@Beaker)

CLOUDINOMICON ::

IDEMPOTENT INFRASTRUCTURE, SURVIVABLE SYSTEMS & THE RETURN OF INFORMATION CENTRICITY

RELEVANT ADVANCES IN TOILETRY AND I.T. ::

FROM SQUAT POTS TO CLOUD BOTS - WASTE MANAGEMENT THROUGH SECURITY AUTOMATION

COMMODE COMPUTING