RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Secure Cloud Development Resources with DevOps

SESSION ID: CSV-F01

Andrew Storms & Eric Hoffmann

Andrew Storms - Director of DevOps
Eric Hoffmann – Director of QA
CloudPassage

CloudPassage

Teach Old Dogs New Tricks

- Applying old thinking to using the cloud for DevOps means:
  - You are non-compliant and will never be compliant.
  - Devs are smart and will find ways to work around security roadblocks.
- You simply cannot bolt on old security tactics and “hope”

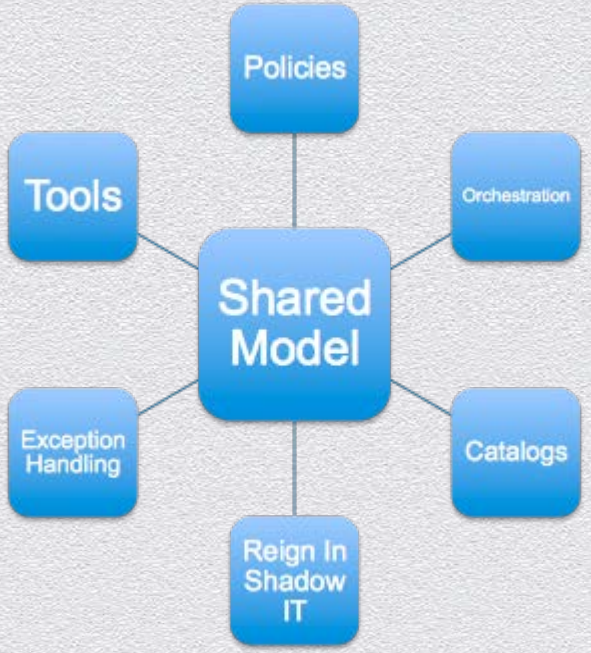
Shared Responsibility Model

Merge DevOps + Shared Responsibility Models

- Requires coordination, inter-company & cross functional groups
- Requires leadership, training & champions
- Requires shared vision & objectives

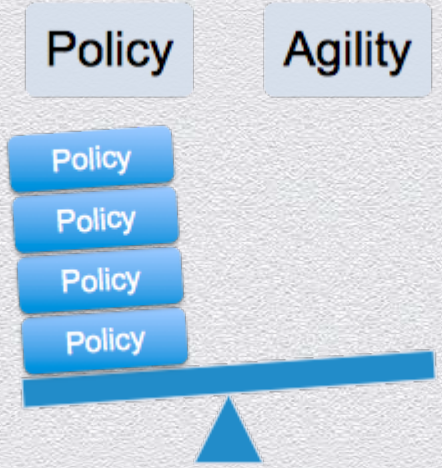
Delivering The Shared Responsibility Model

1. Policies
2. Handling exceptions
3. Service catalogs
4. Orchestration
5. Reign in shadow IT
6. Tools



Policies

- Define Your Policies
  - What policies are needed?
  - SANS templates
- Specific Cloud Vendor Tools & Interfaces
  - AWS mgmt console roles, groups, etc
  - AWS firewall groups
  - Require MFA



Policy Management

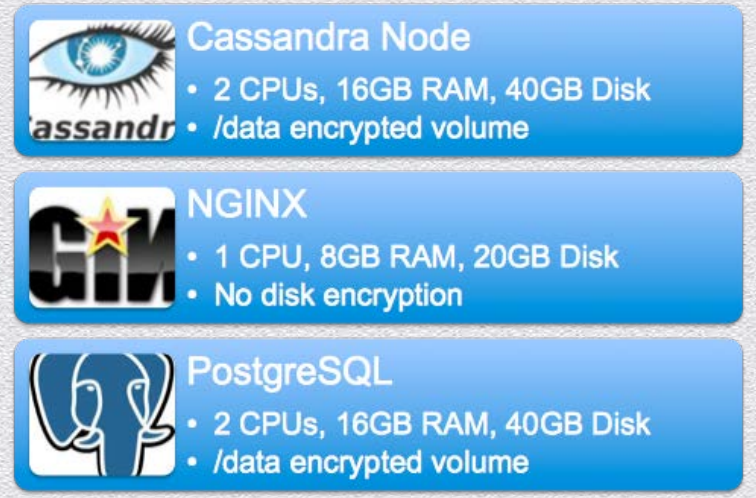
- Get Buy-In and Agreement
  - No vacuums allowed in policy definition
  - Security, ops, dev, audit, management teams
  - “Bake-in” your policies with orchestration
- Policy Violators
  - Define up front what happens when someone deviates from policy
- Intentional or Approved Violator?
  - What if someone NEEDS to go out of policy?

The Dreaded, But Common Exception Cases

- How To Address Exceptions
  - Use cross functional teams, champions, visions & leaders
  - Pre define the ideal case of what should happen
- Be Agile, Use Existing Toolsets
  - Leverage existing security approved tools
  - Keep it public, let ops, dev & security review

The Service Catalog

- Create A Service Catalog
  - Predefined sets of system images
  - Meets security controls
  - Adheres to the company policies
- The One Stop Shop
  - Used by all departments
  - Used within all practices (Dev, Test, Modeling, Etc)

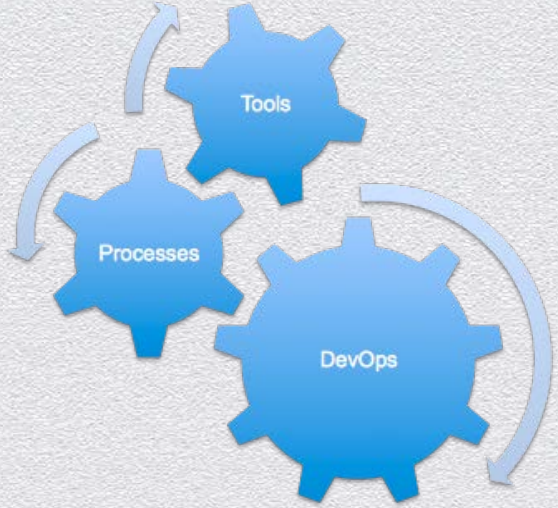


Orchestration

- The Automated Service Catalog
  - Can be predetermined image
  - Can be predetermined recipes
  - Always use APIs
- Single toolset. Single Interface
  - Make available to everyone
  - Teach everyone to use

Orchestration - Shared Tools

- Make It Available To Everyone
  - Encourage everyone to develop & improve
  - Check into your source code system
- Security Can Audit & Approve & Improve
  - Peer review
  - Internal audit



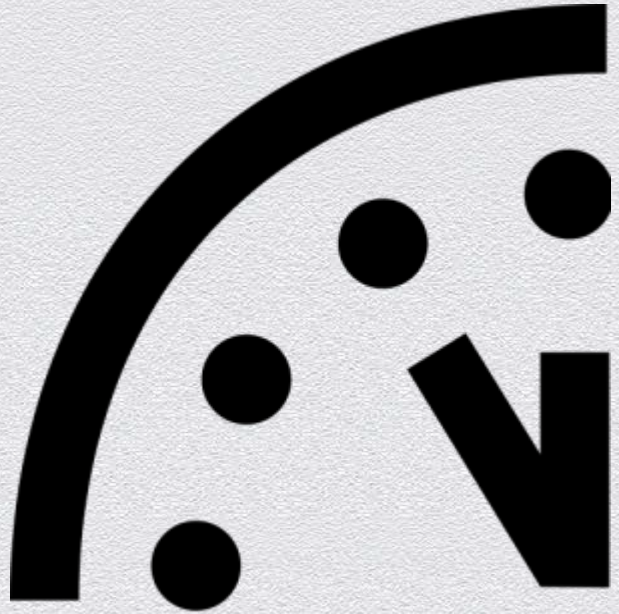
Reign in Shadow IT

- Dev, QA & Others Are Playing IT & Ops
  - Ops isn't delivering the goods in time
- Choke Points Are Bad. Enablers Are Good
  - Need to understand user's needs and deliver them
  - Allow everyone do what they do best
- Understand That Dev and Ops Have Similar Skills
  - This is DevOps after all

What the Cloud Promises

- Economies of scale…
- Self-provisioning agility...
- Servers compromised in 4 hours…

Priceless

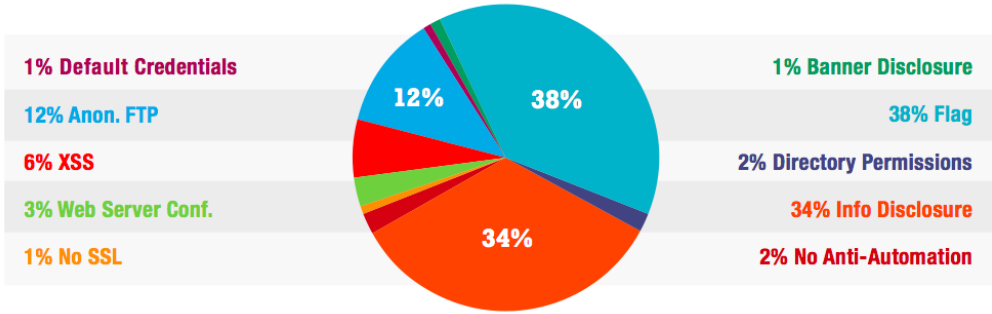


- Live Server Exploitation Exercise
  - Zero to little server security configuration applied
  - Server fully compromised by a single individual in four hours

What We Learned From The Gauntlet Report

- Require Basic Security Tools & Policies For Cloud Servers
  - Access controls
  - Monitoring
  - Alerting

Figure 7: Types of bug submissions, by Percent



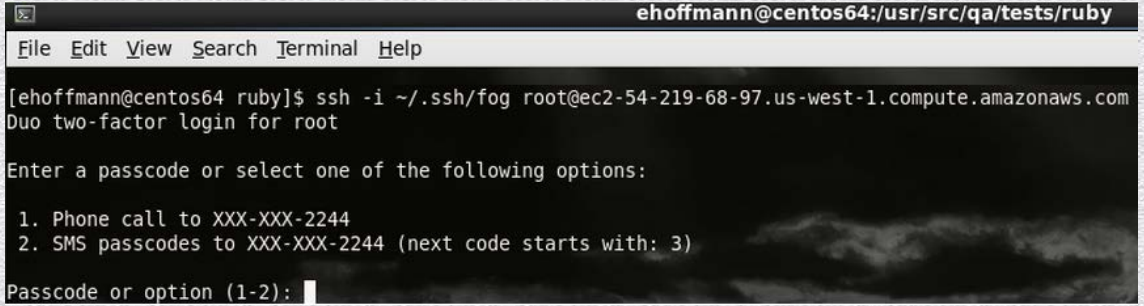
Access Control Tools

- Require Stronger Passwords
  - Linux PAM system-auth settings
  - Windows policy settings
  - L0phtCrack
- Multi Factor
  - Duo security
  - Google authenticator

Access Controls With Orchestration

Making Use Of Multi Factor Authentication… REQUIRE IT!

- Policy creation
- Duo security
- Chef, Puppet
- AWS MFA



CloudPassage

#RSAC

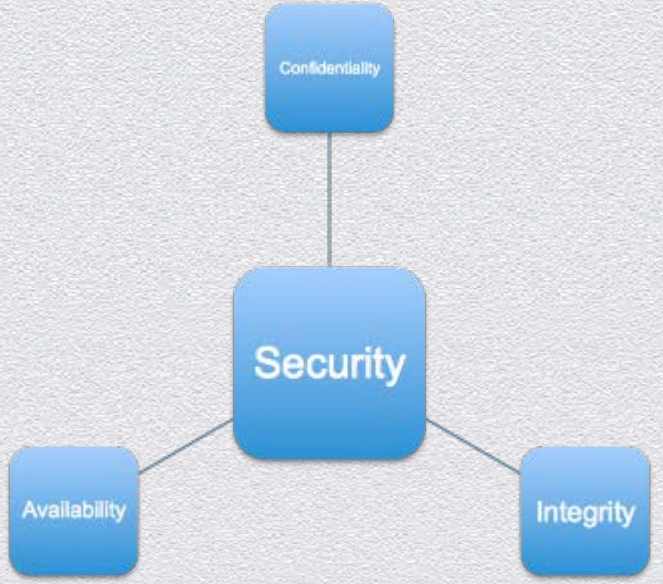
RSACONFERENCE2014

Monitoring & Alerting

- Monitoring Is A Big Space To Cover
  - Server uptime, performance etc.
  - Inventory, usage, costs
- Server, Application Watch Services
  - Cloud vendor specific offerings
  - De Facto: Nagios, Munin, Cacti

Monitoring & Alerting - The CIA Triad

- Availability
- Continuous Monitoring
- Change Alerting



Monitoring & Alerting

- Log Review & Alerting

Monitoring & Alerting

- Stats & App Performance

Monitoring & Alerting

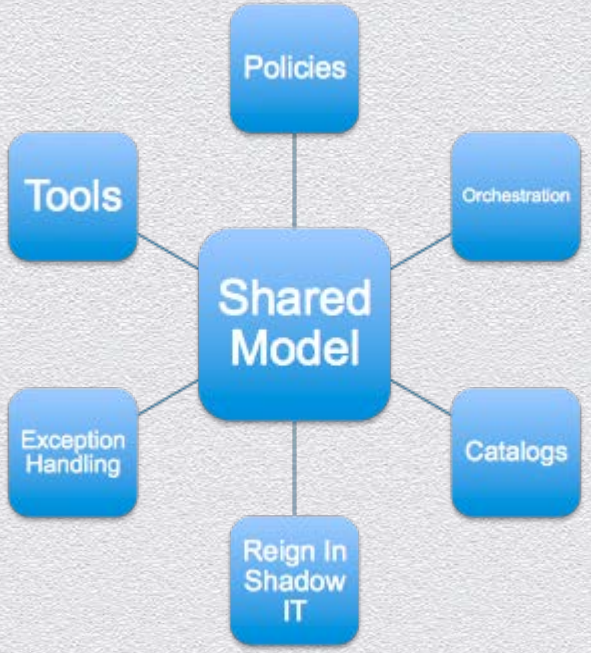
- Overall Usage & Costs

Sum This Up

1. Adoption of cloud resources by development teams has created a security problem.
2. The self-service and on-demand nature of the cloud increases the company attack surface
3. Traditional castles and walls were outdated long ago.
4. Get your head out of sand and do something now. Its not too late, but never is not an option.

Sum This Up

1. Extend the shared responsibility model internally
2. 5 Steps to delivering secure development in the cloud
3. Tool talk



Take Action – Only You Can Prevent Bad Things

- Where do you sit in the development and/or security processes?
- Create real and useful security policies.
- Use orchestration in delivery of a secure eco system.
- Use service catalogs to pre build approved systems.
- Make use of the various available existing services.

Questions?

Andrew Storms @St0rmz, astorms@cloudpassage.com

Eric Hoffmann, ehoffmann@cloudpassage.com