Meeting Halfway

Cloud Platform Security Through On-Prem Controls
IU’s Cloud Journey

- SaaS – *Almost* Cloud First
- IaaS/PaaS
  - Enterprise – crawling
  - Teaching – toddling
  - Research – walking
Origin Story
Concern about gaps raised
Early public cloud at IU

- Research
- Modest application experimentation
- Classroom use
Report requested

<table>
<thead>
<tr>
<th>PERSONAL HABITS</th>
<th>Oct. 31</th>
<th>Dec. 25</th>
<th>Jan. 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>correctly</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>correctly</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>correctly</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HANDS, NAILS, FACE, ETC.</th>
<th>Oct. 31</th>
<th>Dec. 25</th>
<th>Jan. 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>High and neat</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Mouth when coughing</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Clothing clean</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HANDKERCHIEF</th>
<th>Oct. 31</th>
<th>Dec. 25</th>
<th>Jan. 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hands and materials from mouth</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EVIDENCES OF GROWTH IN:</th>
<th>Oct. 31</th>
<th>Dec. 25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to express himself</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Learning to read</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Speaking clearly</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOOD WORK HABITS</th>
<th>Oct. 31</th>
<th>Dec. 25</th>
<th>Jan. 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working alone</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Doing purposeful work</td>
<td>S</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Finishing work</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>
Gap analysis

- Public cloud providers have similar controls
- IU is not using them systematically
- Left up the account owner to use and use properly
Call to Action
Charge given

- Create working group covering all relevant technical areas
- Develop strategies to bring controls into alignment
Cloud Security Working Group

- Exec Sponsor: Chief of Staff
- Chair: CISO
- Representation from:
  - Security
  - Policy
  - Networks
  - Support
  - Research Technologies
  - Learning Technologies
  - Enterprise Systems & Software
- Directional team
- Technical team
The process

- Scope would not include SaaS; it is dealt with in a separate process
The process

- Scope would not include SaaS; it is dealt with in a separate process
- Do we look for a single solution for the whole group of providers?
The process

- Scope would not include SaaS; it is dealt with in a separate process
- Do we look for a single solution for the whole group of providers?
- Do we focus on one vendor at a time?
The process

- Scope would not include SaaS; it is dealt with in a separate process
- Do we look for a single solution for the whole group of providers?
- Do we focus on one vendor at a time?
- If one, where do we begin?
The First Contestant
Google Cloud Platform (GCP)
Why GCP?

- GCP had fewer accounts than AWS or Azure
Why GCP?

- GCP had fewer accounts than AWS or Azure
- Security training was already scheduled
The process

- Training gave us...
  - a common vocabulary
The process

- Training gave us...
  - a common vocabulary
  - Understanding of the controls
The process

- Training gave us...
  - a common vocabulary
  - Understanding of the controls
- Subgroups dug into decision points on...
The process

- Training gave us...
  - a common vocabulary
  - Understanding of the controls
- Subgroups dug into decision points on...
  - Networking
The process

● Training gave us...
  ○ a common vocabulary
  ○ Understanding of the controls

● Subgroups dug into decision points on…
  ○ Networking
  ○ Identity and Access Management
End of Round One
The plan

IU Google Cloud Platform (GCP) Configuration Proposal 1.0

Table of Contents

OVERVIEW .................................................................................................................................................. 2

BASIC GOOGLE CLOUD PLATFORM (GCP) TERMINOLOGY ....................................................... 3

ORGANIZATION NODE ...................................................................................................................... 3
FOLDER .................................................................................................................................................. 3
PROJECT ............................................................................................................................................... 3
RESOURCE ............................................................................................................................................. 3
G-SUITE AND CLOUD IAM .................................................................................................................. 3
GOOGLE GROUPS ................................................................................................................................. 3
PERMISSIONS ....................................................................................................................................... 4
ROLE ..................................................................................................................................................... 4
PRIMITIVE ROLES .......................................................................................................................... 4
PREDEFINED ROLES ......................................................................................................................... 4
CURATED ROLES .................................................................................................................................. 4
CUSTOM ROLES ................................................................................................................................... 4
POLICY ................................................................................................................................................... 4
ORGANIZATION POLICY SERVICE .................................................................................................. 4
BILLING ACCOUNT/ BILLING ID ........................................................................................................... 5
SELF-SERVE ......................................................................................................................................... 5
CONTRACTED ....................................................................................................................................... 5
CREDITS ............................................................................................................................................... 5
The plan

● A balance between...
The plan

- A balance between…
  - Student exploration
The plan

● A balance between...
  ○ Student exploration
  ○ Teaching & Learning
The plan

- A balance between…
  - Student exploration
  - Teaching & Learning
  - Research
The plan

- A balance between…
  - Student exploration
  - Teaching & Learning
  - Research
  - Development
The plan

● A balance between…
  ○ Student exploration
  ○ Teaching & Learning
  ○ Research
  ○ Development
  ○ Enterprise workloads
The plan

● A balance between…
  ○ Student exploration
  ○ Teaching & Learning
  ○ Research
  ○ Development
  ○ Enterprise workloads
  ○ Sensitive data
The plan

● A balance between…
  ○ Student exploration
  ○ Teaching & Learning
  ○ Research
  ○ Development
  ○ Enterprise workloads
  ○ Sensitive data

● Leveraging native tools
The plan

- A balance between...
  - Student exploration
  - Teaching & Learning
  - Research
  - Development
  - Enterprise workloads
  - Sensitive data

- Leveraging native tools

- Sending data back to local tools
On to Round Two
Microsoft Azure

- Driven by request
- Starting with training
Networking Deep Dive
Backend services that require white-listing assume clients have known/fixed IP addresses.
What Have We Learned?
The “right” way

- There isn’t one.
- Your process can’t be done in isolation.
- Your solution must fit within the parameters of your institution.
- Think of the full account lifecycle.
- Include procurement and data governance.
Assumptions

- You must include use cases from Enterprise, Research, Teaching and Learning.
- Leaving out any one of them will prove costly in the long run.
Not all the best minds are in the room

- There is a lot of knowledge out in the higher ed community. Take advantage of it.
- EDUCAUSE Cloud Computing Community Group (CCCG)
  - Tomorrow 10:45AM to 12:15PM Room: W187b, Level 1
Resources

- Make sure both the decision-maker and technical teams are broad-based.
- Not only will the input be better, but you’ll ultimately expand cloud awareness and raise your organization’s overall Cloud IQ.
Resources

- Once you’ve figured out a plan, you need to have the resources to implement it
- That means staff to do the work
- And $$ to pay for the monitoring and controls
Best laid plans

- Despite your best efforts, you will get some things wrong
- Manage expectations
- Get back in the saddle after the inevitable mistakes
Questions?

Speakers:
Bob Flynn, Manager, Cloud Technology reflynn@iu.edu
Andrew Korty, Chief Information Security Officer ajk@iu.edu
Steven Wallace, Enterprise Network Architect ssw@iu.edu

IU GCP Plan:
http://go.iu.edu/2c0c

All Creative Commons images in the presentation were created with Haiku Deck