RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CSV-W05R

CLOUD SECURITY ESSENTIALS 2.0

Full Stack Hacking & Recovery

Shannon LIetz
Director, DevSecOps & Security Eng
Intuit
@devsecops

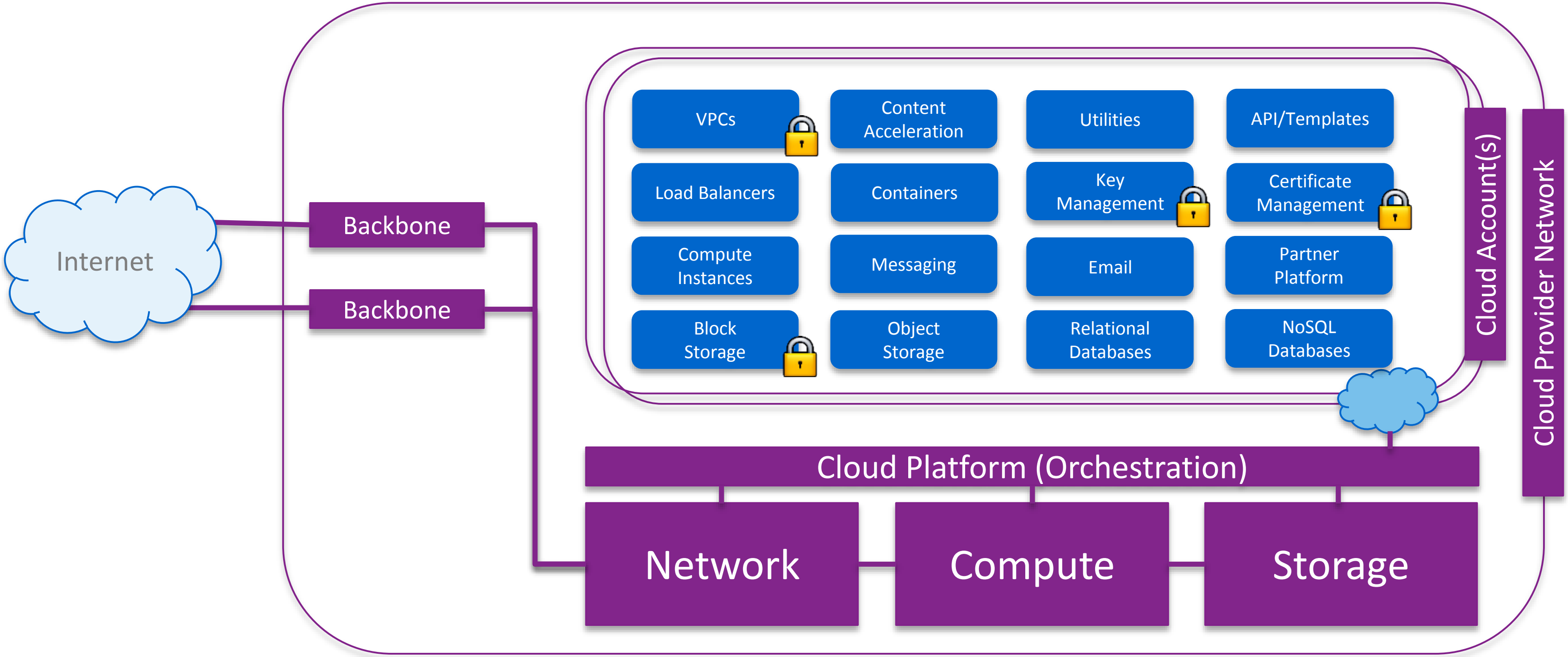
Javier Godinez
Principal DevSecOps Architect
Intuit

#RSAC

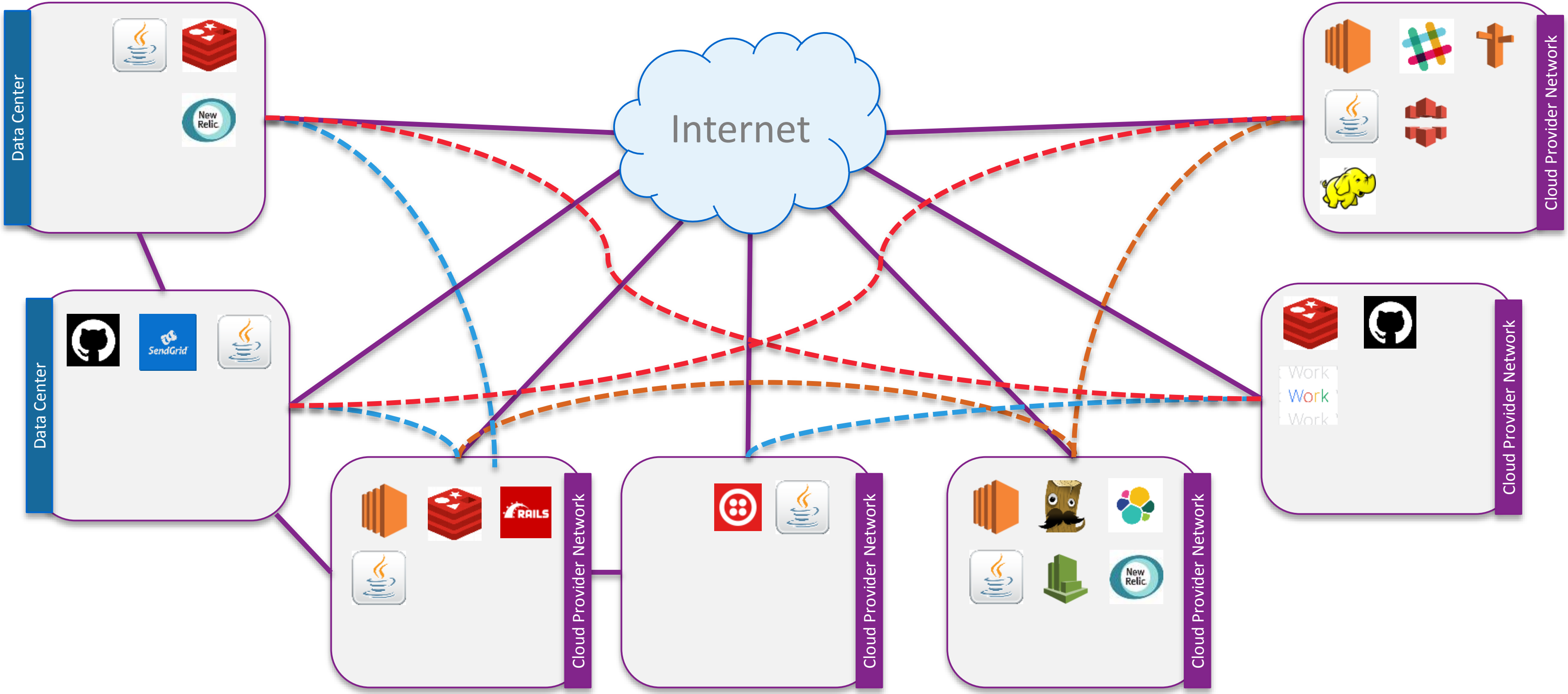
Overview

- A Basic Introduction – Cloud Hack Lab
- Attack Harness, Enumeration and Testing Tools
- Cloud Forensics at Scale
- Opportunities for Tools

The Basic Cloud Model

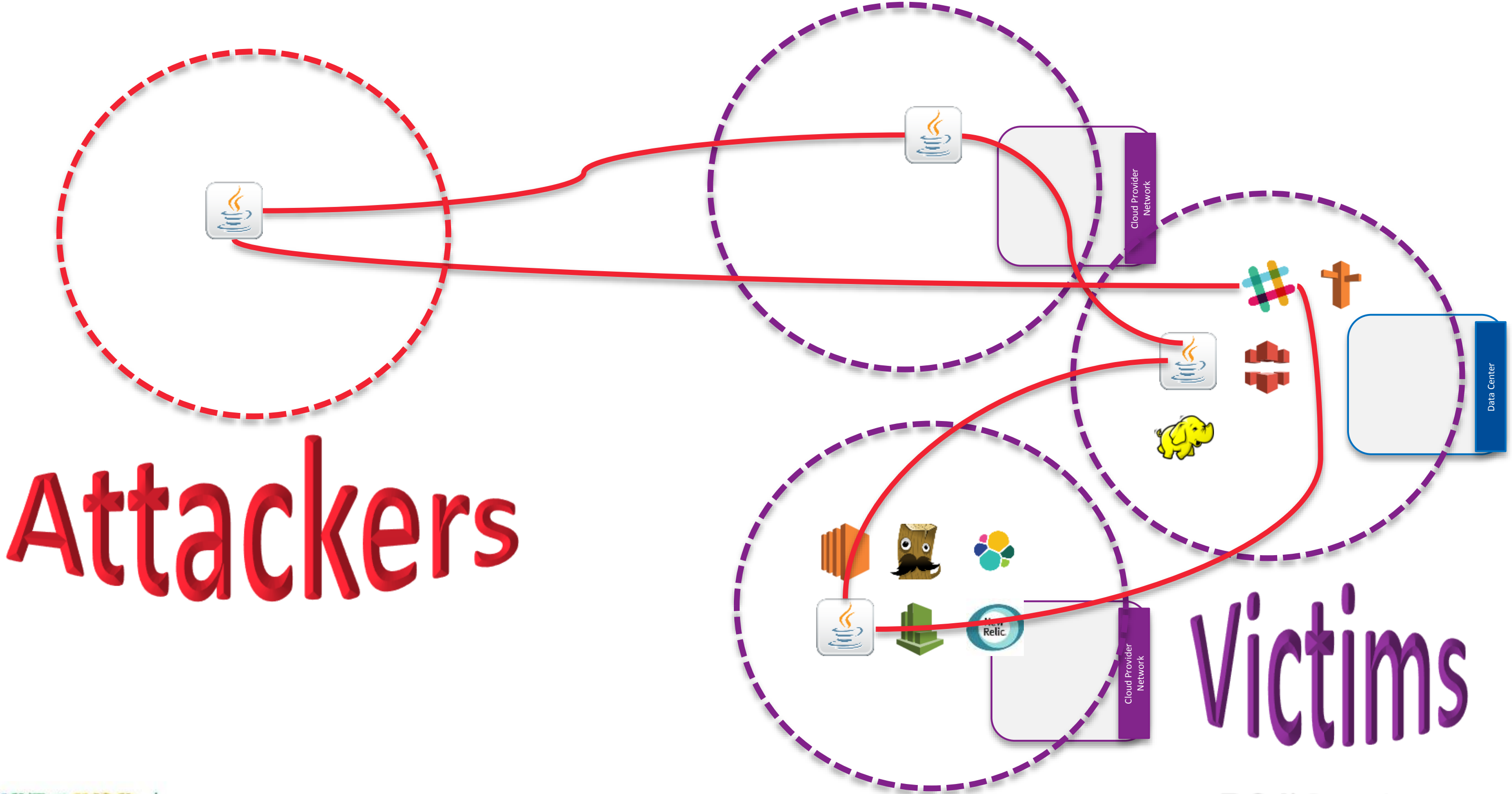


Reality...

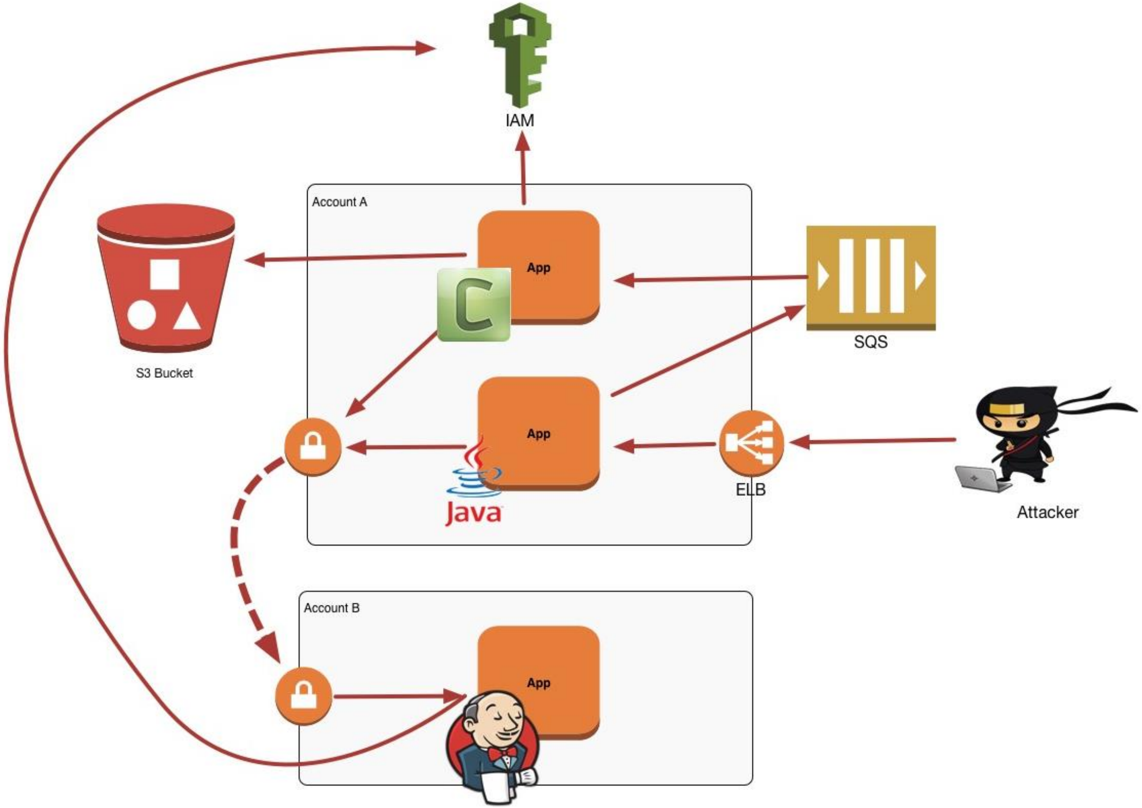

Data Center
New Relic
Internet
Cloud Provider Network
Data Center
SendGrid
Work
Work
Work
Cloud Provider Network
RAILS
Cloud Provider Network
Cloud Provider Network
New Relic
Cloud Provider Network

UH… WE’RE NOT IN {KANSAS} ANYMORE

Attack Surface is Much Less Obvious



Cloud Hack Lab

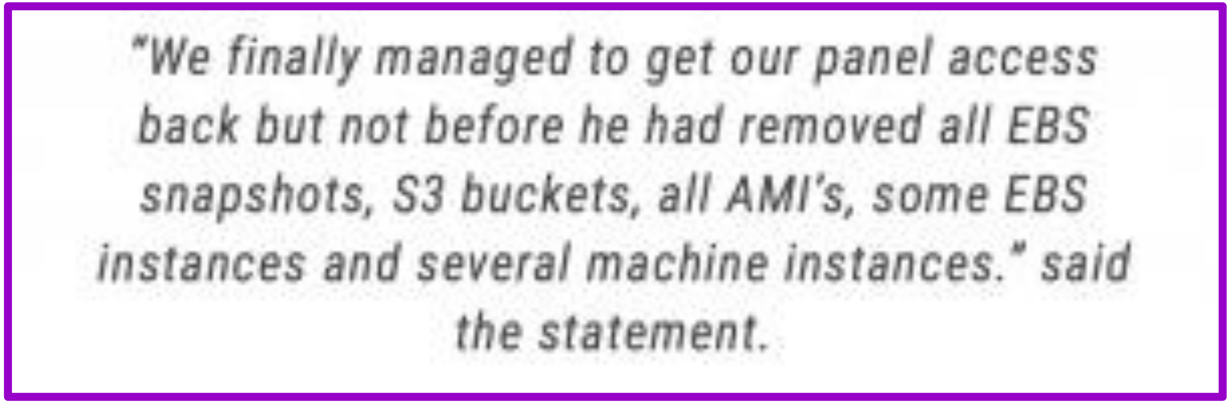


Cloud Hack Lab Demo

Blast Radius is a real thing…

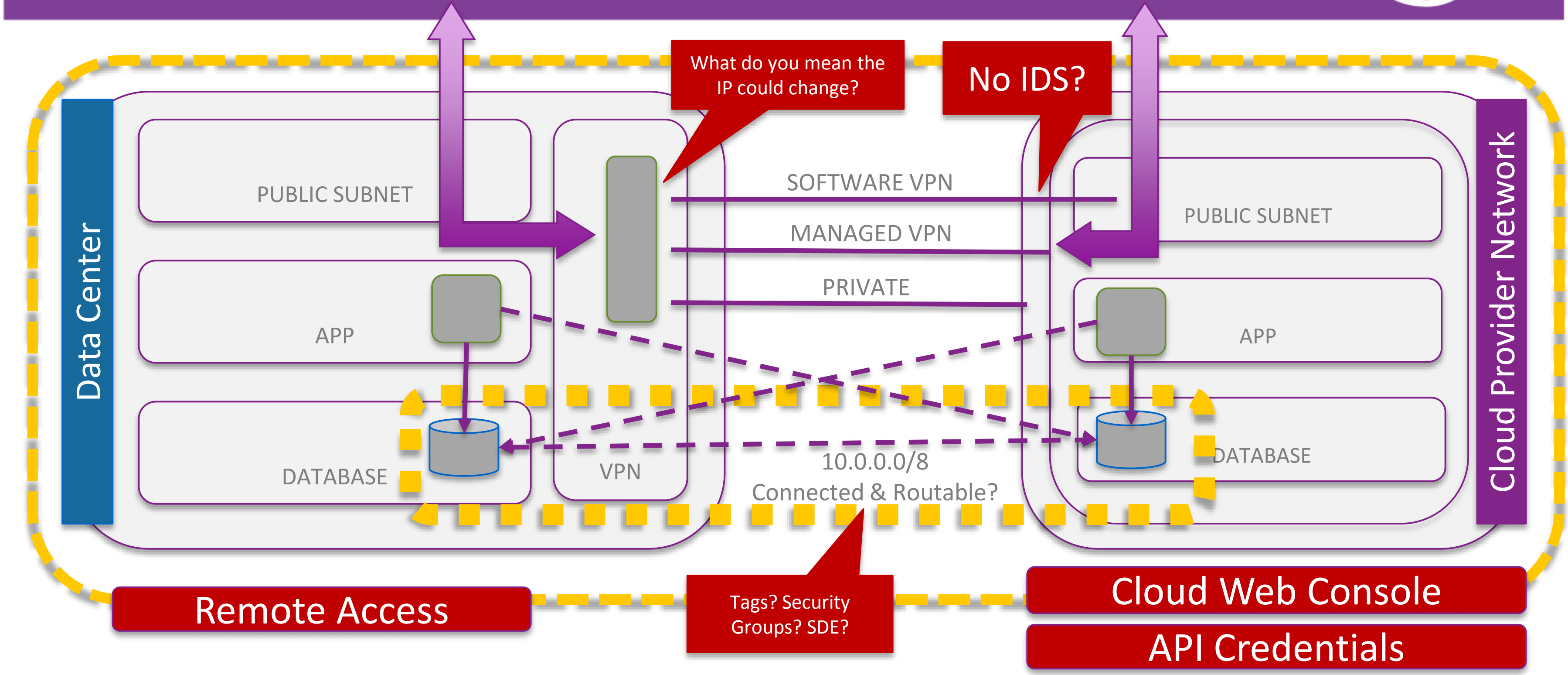
R.I.P.

Code Spaces



"We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances." said the statement.

Direct Connections/VPNs to Clouds are evil!



What do you mean the IP could change?

No IDS?

Remote Access

Tags? Security Groups? SDE?

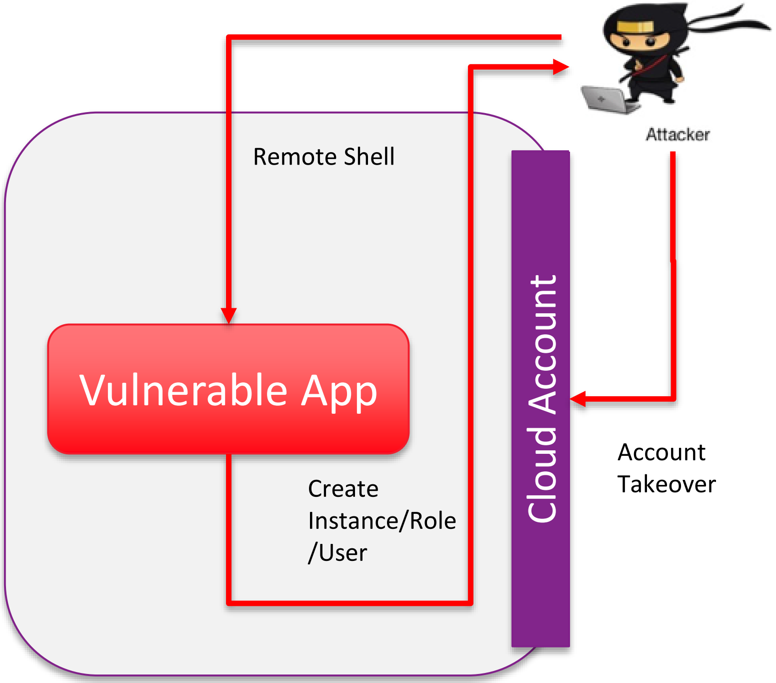
Cloud Web Console

API Credentials

"NEW" BOUNDARY HAS ALL THE WEAKNESSES OF BOTH AND MIXES TWO DIFFERENT SECURITY MODELS!

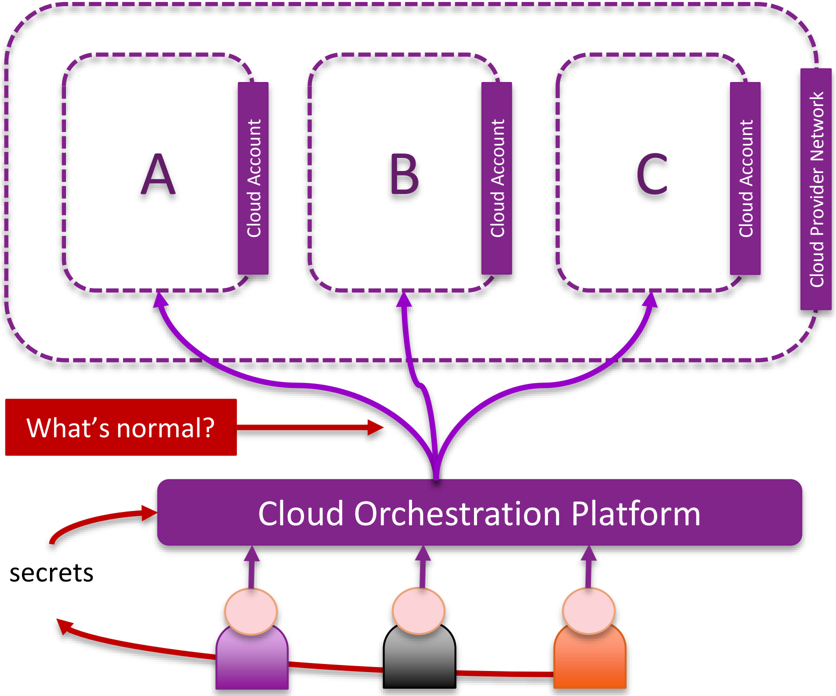
Cloud Lateral Movement …

- An Application vulnerability can lead to a Cloud Account Takeover
- Most apps require traditional defense in depth which doesn’t apply to cloud apps
- Baselines are really important and drift management essential



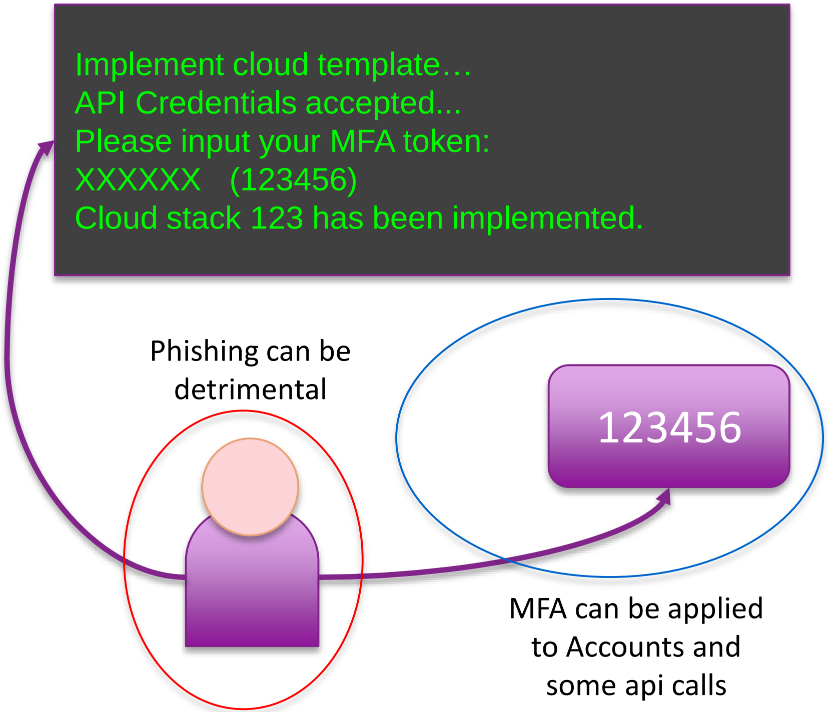
Beware of Orchestrators…

- Orchestration creates blast radius because it centralizes the deployment/security for cloud workloads.
- Tools that ***act on behalf*** usually require credentials and create blindspots.
- Non-native tools require specialized skills and make it difficult to gain context on what the right behavior should be.



MFA is a MUST!

- Passwords don’t work.
- Passwords aren’t enough to protect infrastructure.
- API Credentials and Roles can be misappropriated
- Most Cloud Environments and Apps have one level of access
- On some cloud platforms it is possible to make roles work only when MFA is provided and for certain actions to require MFA



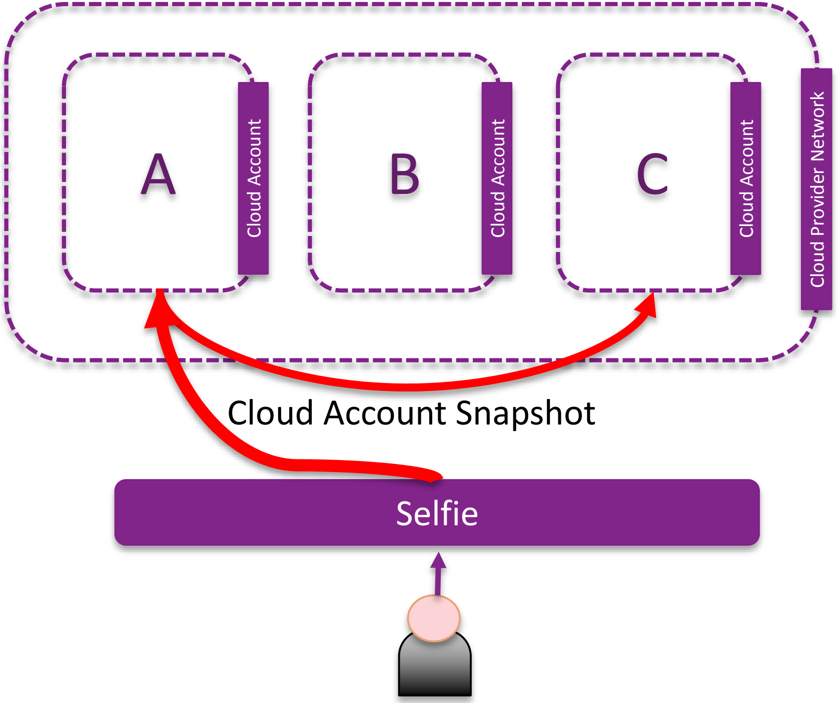
```
Implement cloud template…
API Credentials accepted...
Please input your MFA token:
XXXXXX   (123456)
Cloud stack 123 has been implemented.
```

Phishing can be detrimental

MFA can be applied to Accounts and some api calls

Selfie for Forensics

- Full Account Snapshot (Roles, Instances, Managed Services)
- Used to determine what happened along with Audit Trails
- Ability to clone and perform sandbox analysis



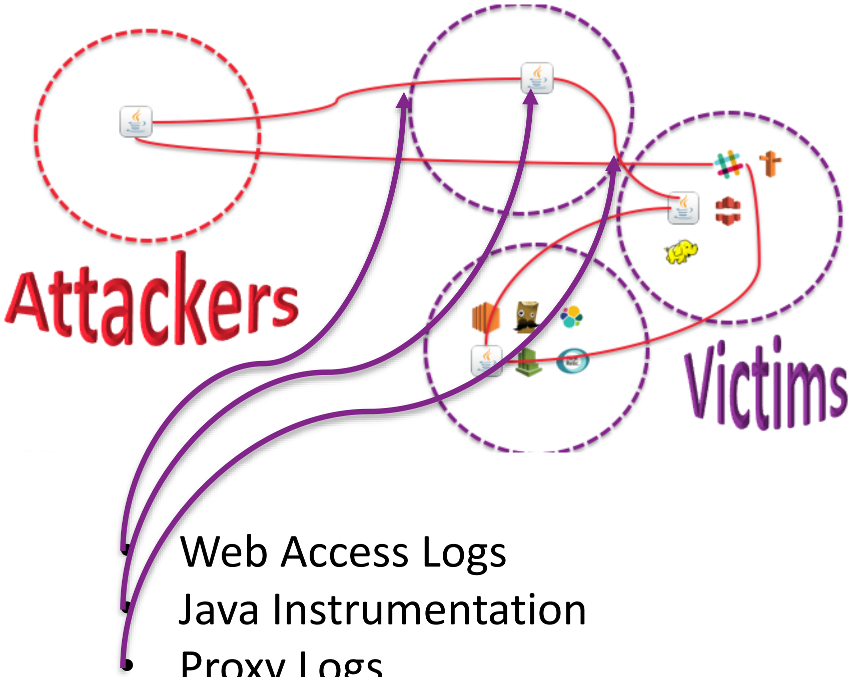
Cloud Forensics Demo

Missing Tools of the Trade

- Enumeration tools for API discovery and drift detection are few and far between
- Scanners are missing Cloudy capabilities, ie. Credential Discovery, API Integrations, Pathway Enumeration
- Varying levels of resources and 3rd party add-ons create visibility challenges
- Permissions are not granular enough and role inheritance is missing
- Hard to create coarse grained controls to allow for innovation
- Network monitoring and controls are not easily passed to cloud customers

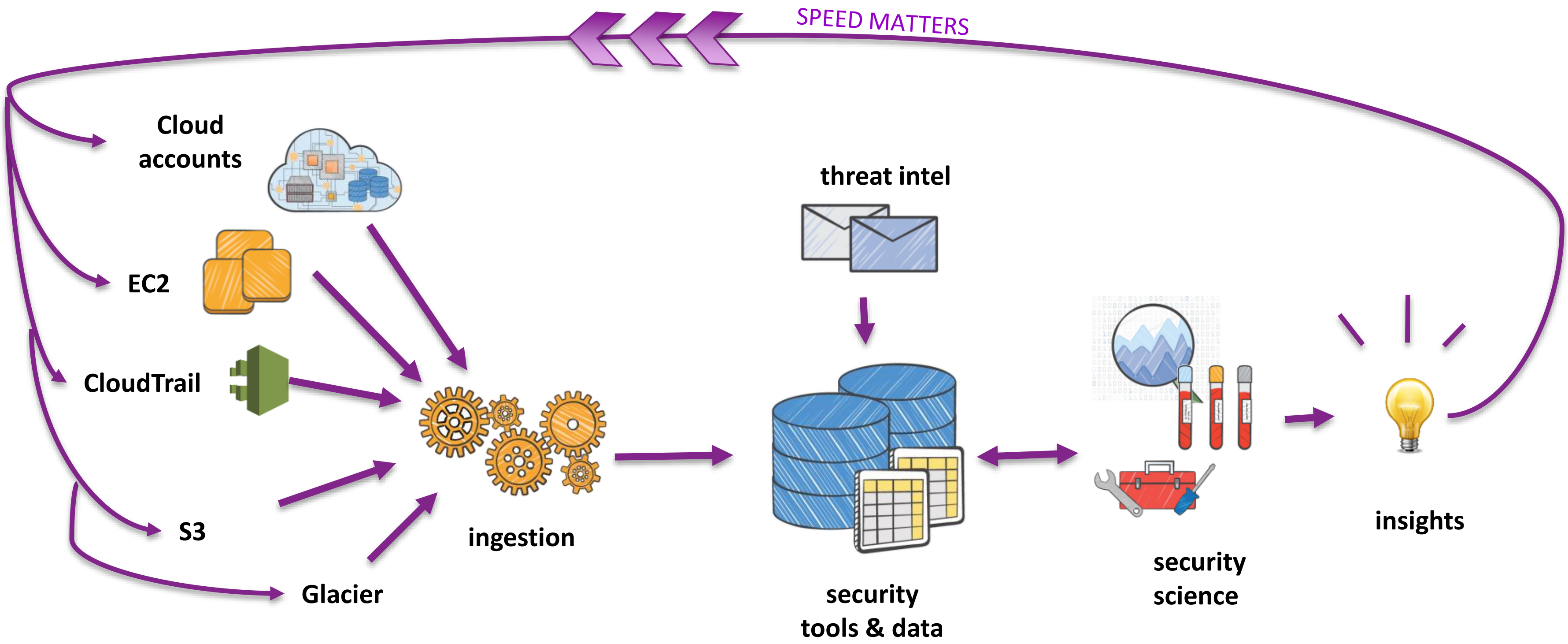
Cloud Security is a Big Data Challenge…

- DevOps + Security is the biggest big data challenge ahead.
- Use Attack Models and choose the right Data Sources to discover attacks in near real-time.
- Develop a scientific approach to help DevOps teams get the security feedback loop they have been looking for.



- Web Access Logs
- Java Instrumentation
- Proxy Logs
- DNS Logs

Cloud Security Feedback Loop



Security as Code… gotta do it.

Apply what you learned today…

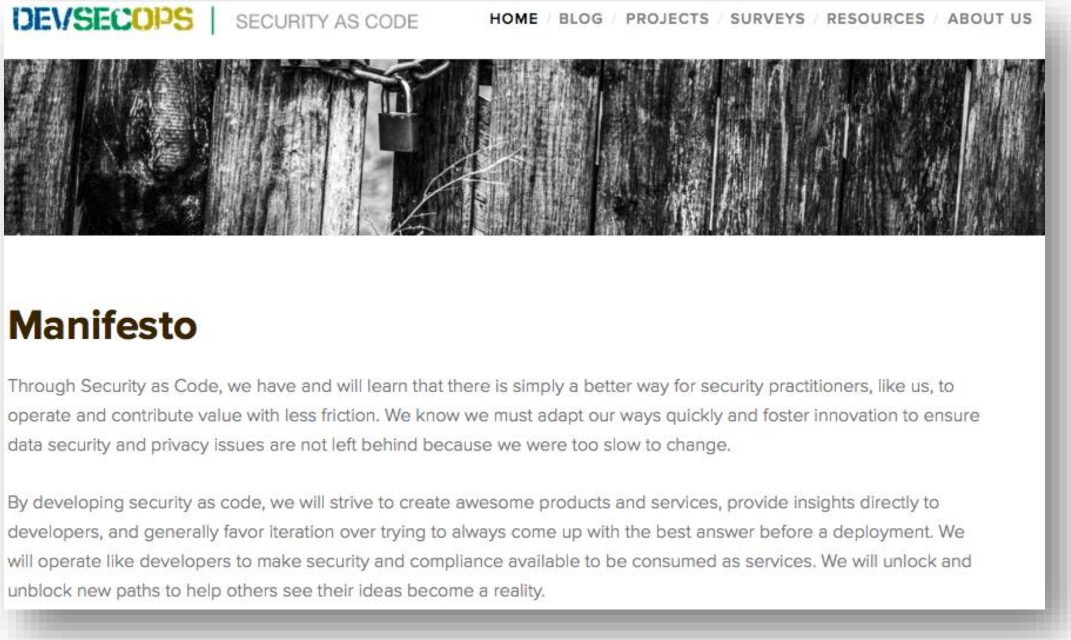
- **Next week you should:**
  - Understand how your organization is or plans to use cloud providers
  - Identify cloud workloads and virtual blast radius within your organization
- **In the first 3 months following this presentation you should:**
  - Begin to build Security as Code skills and run cloud security experiments to understand the issues
  - Develop Crawl-Walk-Run plans to help your organization build security into cloud workloads
- **Within 6 months you should:**
  - Cloud workloads have been instrumented for known security issues and flagged during the Continuous Delivery of software to the cloud
  - Your group has begun to test using Red Team methods and automation to ensure end-to-end security for your cloud workloads
  - Remediation happens in hours to days as a result of automation

Get Involved & Join the Community

- devsecops.org
- @devsecops on Twitter
- DevSecOps on LinkedIn
- DevSecOps on Github
- RuggedSoftware.org
- Compliance at Velocity

Join Us !!!

Spread the word!!!


DEVSECOPS | SECURITY AS CODE
HOME / BLOG / PROJECTS / SURVEYS / RESOURCES / ABOUT US

Manifesto

Through Security as Code, we have and will learn that there is simply a better way for security practitioners, like us, to operate and contribute value with less friction. We know we must adapt our ways quickly and foster innovation to ensure data security and privacy issues are not left behind because we were too slow to change.

By developing security as code, we will strive to create awesome products and services, provide insights directly to developers, and generally favor iteration over trying to always come up with the best answer before a deployment. We will operate like developers to make security and compliance available to be consumed as services. We will unlock and unblock new paths to help others see their ideas become a reality.