Today’s Agenda

● The State of AWS Cloud Security / Top 10 Problems
  ○ Ben Hagen

● Morning Presentations
  ○ Will Bengston ~ Netflix
  ○ Steve Woodrow ~ Lyft
  ○ Mark Hillick ~ Riot Games
  ○ Thomas Vachon ~ Harvard University

● Afternoon Training
  ○ Part 1 ~ AWS Security Fundamentals, Bringing it all together
  ○ Part 2 ~ Programmatic AWS / Lambda / Events
The State of Cloud Security
A well architected & instrumented AWS environment is more secure than its counterpart in a datacenter. (*)
(*) but only if you know what you’re doing.
Meaning ... the state of cloud security SHOULD BE BETTER
Top 10 AWS Security Risks
1. Insecure use of developer credentials
2. Publicly accessible S3 buckets
3. Improper use of default configurations
4. Access controls do not follow principles of least privilege
5. Misconfigured network constructs
6. Lack of appropriate logging and monitoring
7. Lack of inventory management
8. Domain hijacking
9. Lack of a disaster recovery plan
10. Manual account configuration
Bonus!

To sum things up ...

- We’ve covered 10 common mistakes organizations make ... there are more
- But the opportunities and advantages of public cloud environments can be worth it
- As security professionals we must understand the technology and environment we are securing
- In the case of AWS this translates to a fundamental understanding of how AWS works and how you can instrument and manage not only the security features of your account, but the account itself towards your organization’s security goals
Thank you!