LONDON
INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE 2015

goto; conference

The Road to Rugged

Shannon Lietz

goto; conference

Click ‘engage’ to rate session.

Rate **12** sessions to get the supercool GOTO reward

Join the conversation #gotoldn

Who I am

- 25+ years Technology and Security Experience
- Most of my career has been about being Rugged!
- Background in Security R&D
- Working with the Cloud before it was called the “Cloud”
- Manage my teams using DevOps and Scrum
- IR & Crisis Management

Disclaimer

goto; conference

- Mistakes happen
- The truth may be difficult to bear
- Unknown unknowns will get discovered
- Success means less 3am phone calls
- Security is a broad topic
- Rugged takes practice

Why is Rugged Important?

goto; conference

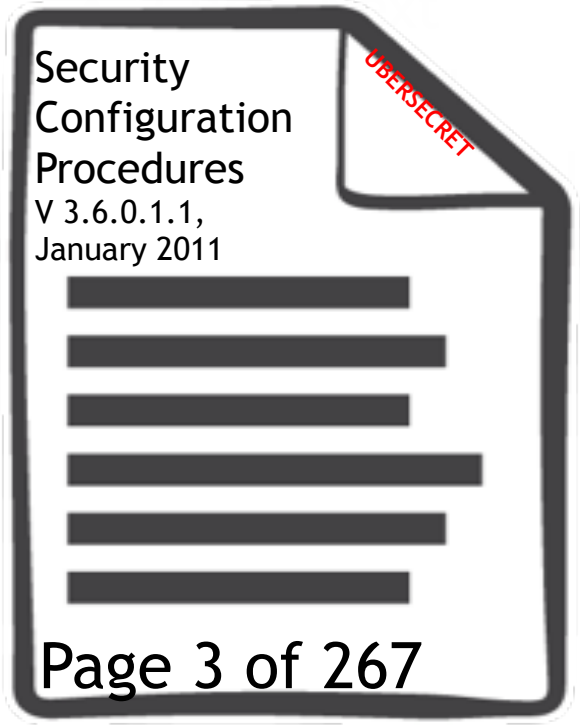
- Case for change is very compelling!
- Planning != Good Code, Less Security Breaches
- Perfection takes too long to get wrong

No one enjoys getting woken up to solve for someone else's mistakes, especially security breaches!!

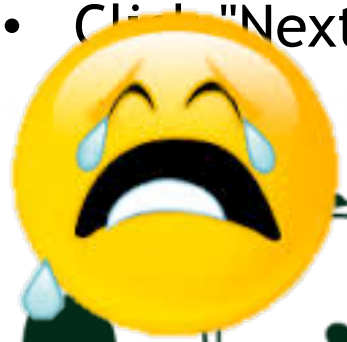
This isn't rugged or helpful...

goto; conference

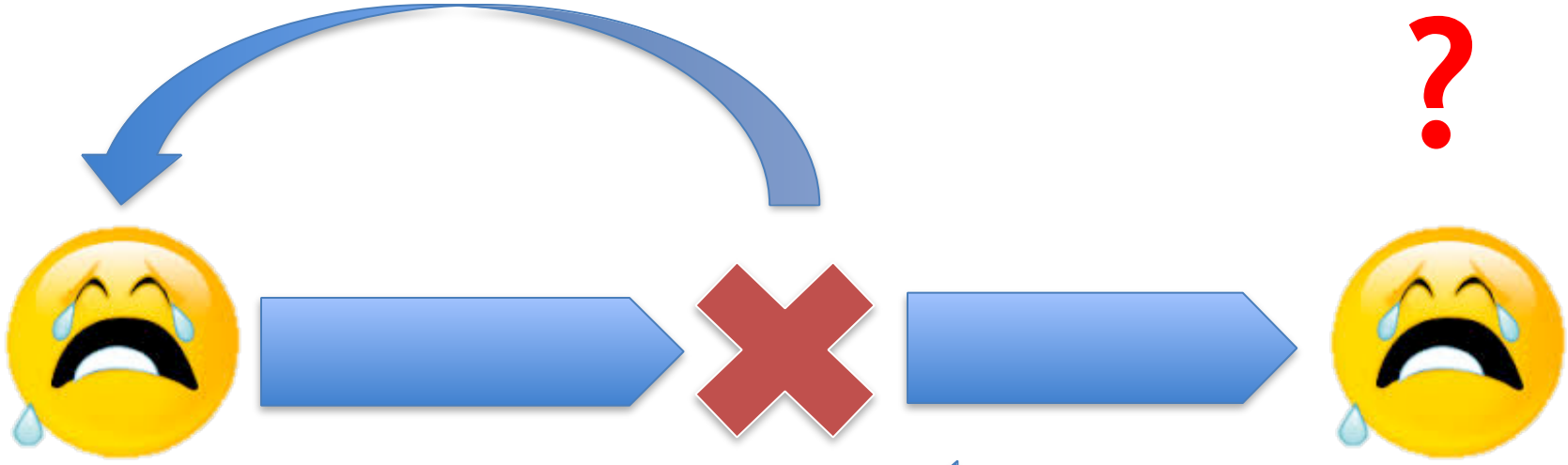
- Double-click installer
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"
- Click "Next"



Frozen in Time



And this just creates friction…



YOU

Hopefully it's not going to be another round of "No's"…

YOUR CUSTOMER

Why does it take so long for features?

CISO

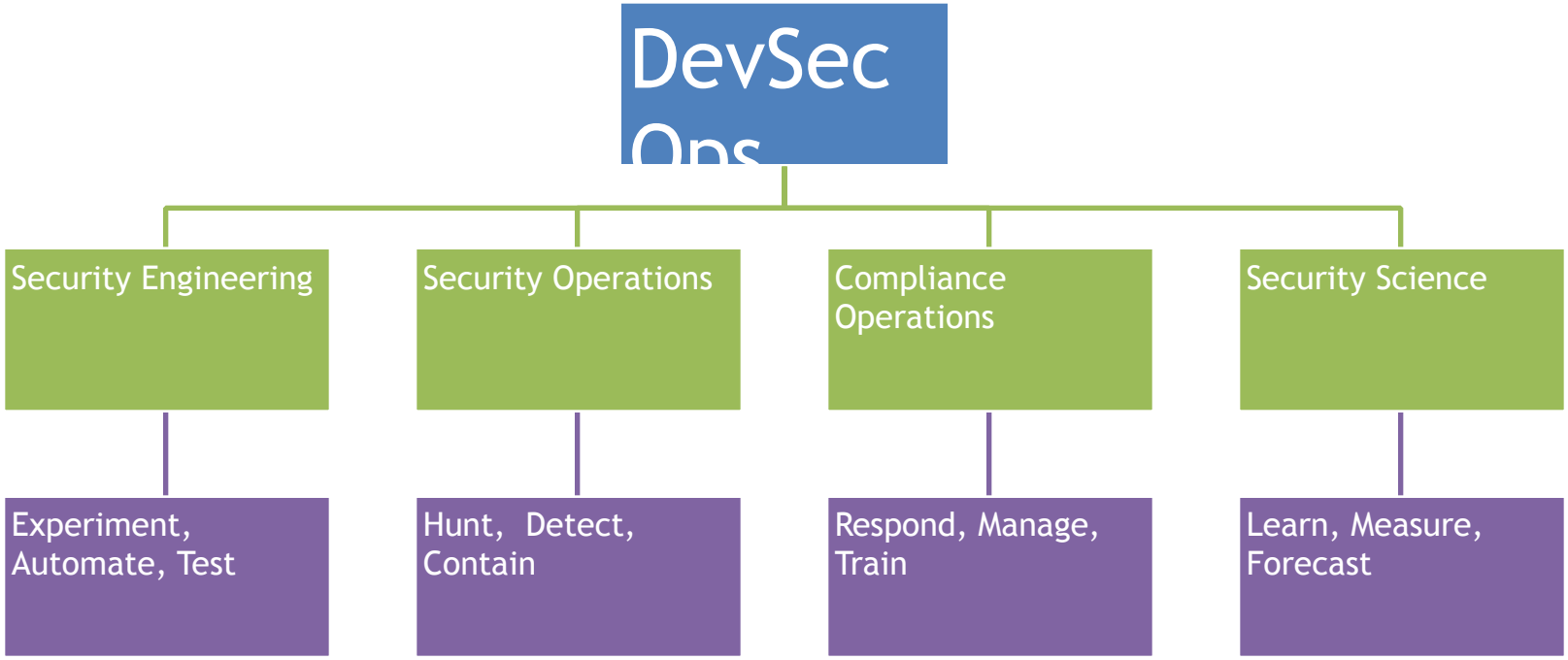
Which makes everyone...

goto; conference

Bang
Head
Here

But - What if Security can be Rugged?

goto; conference



Let's Get Rugged!!!

goto; conference

Problem Statement

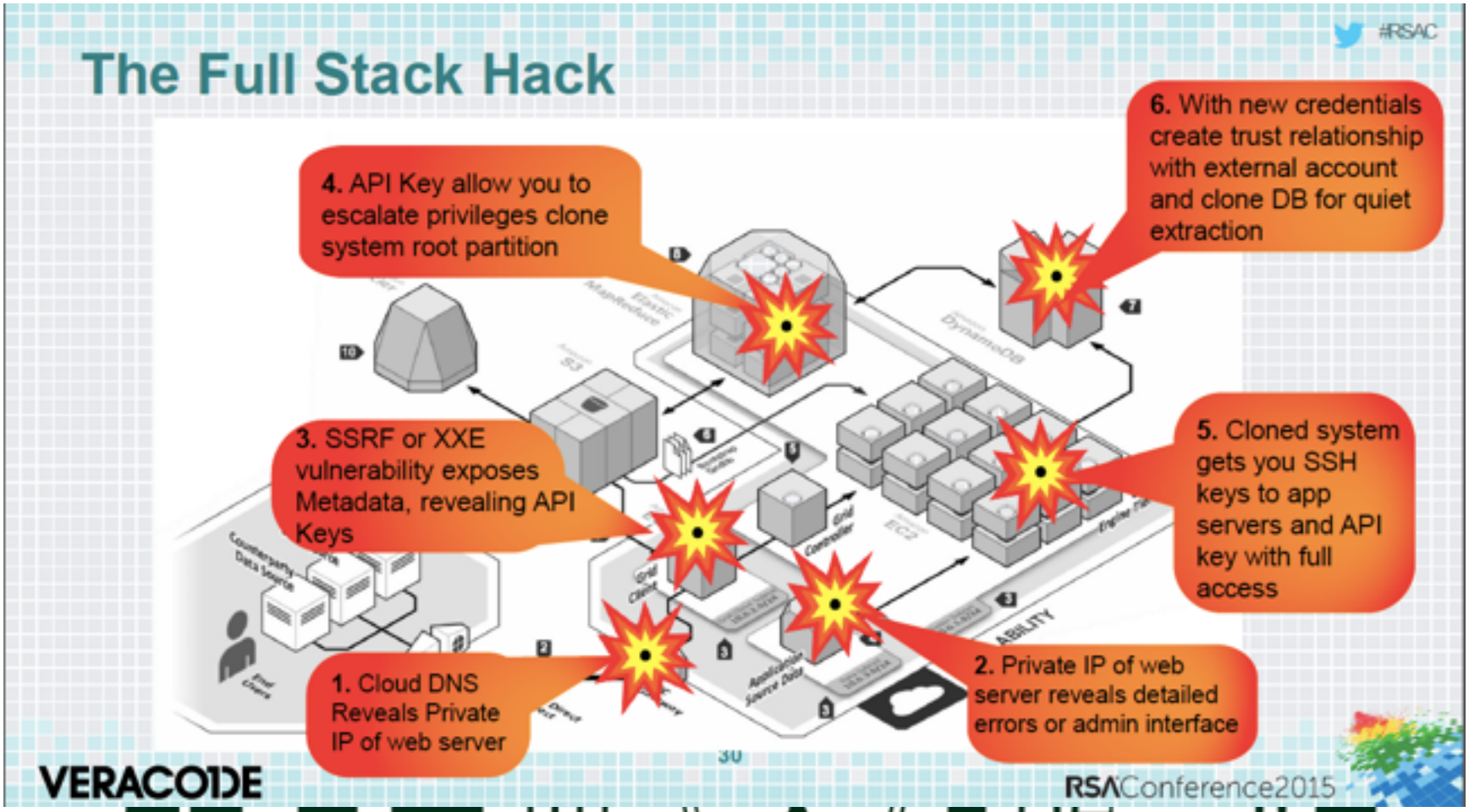
- DevOps requires continuous Deployments
- Fast decision making is critical to DevOps success
- Traditional Security just doesn't scale or move fast enough…

Welcome DevSecOps!!

- Customer focused Mindset
- Scale, Scale, Scale
- Objective Criteria
- Proactive Hunting
- Continuous Detection & Response

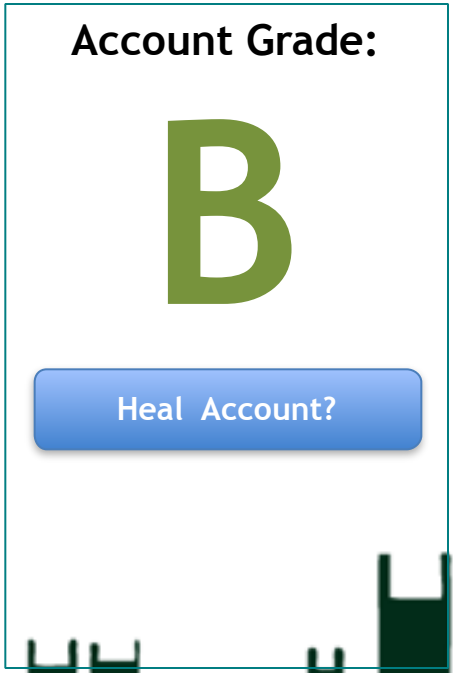
What if Security were no longer just theory?

goto; conference

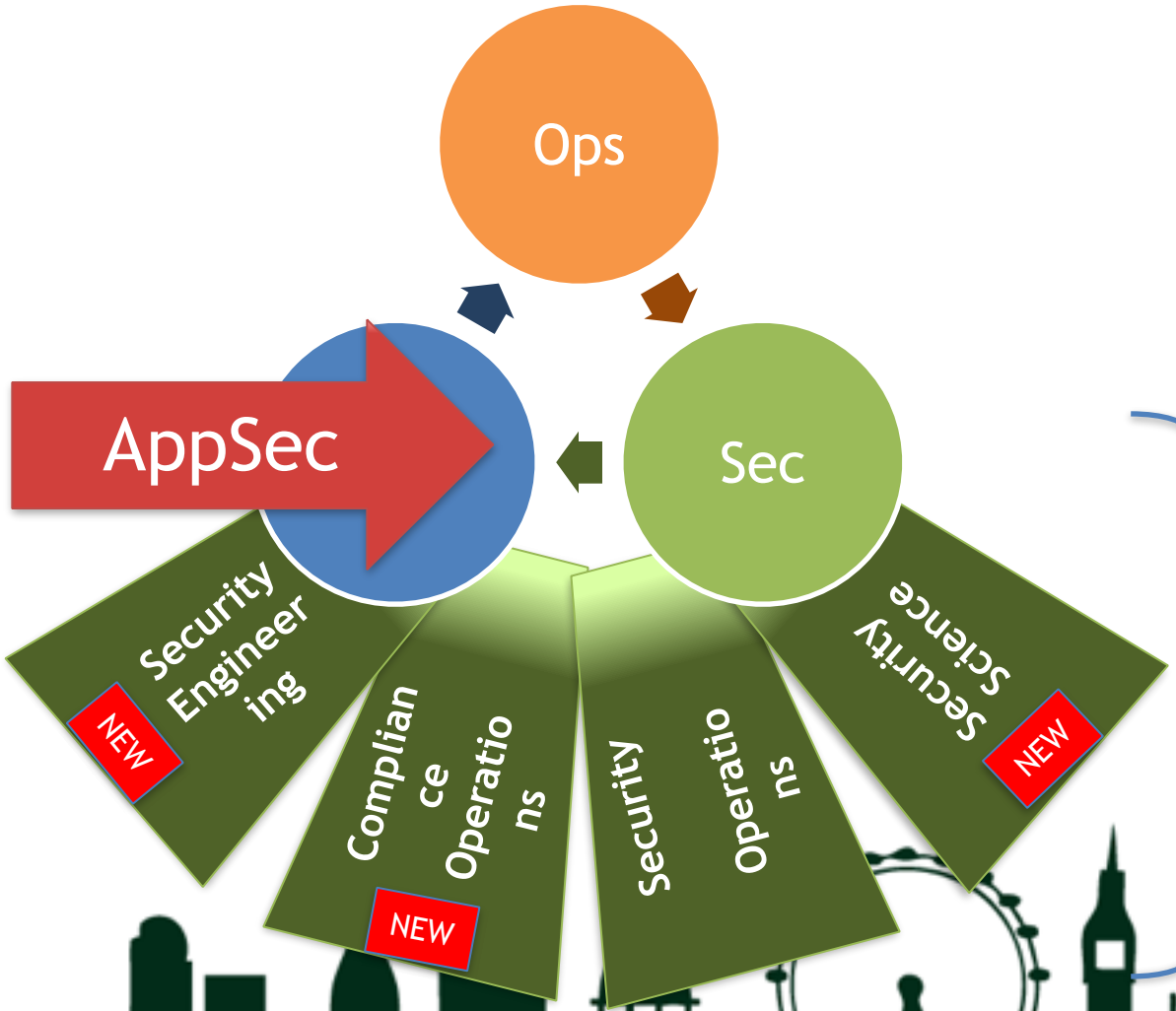


What if you could check Security via API? Or Self-Service?

```
begin
   (iam.client.list_role_policies(:role_name => role)[:policy_names]\
         - roledb.list_policies(role)).each do |policy|
    log.warn("Deleting Policy \"#{policy}\", which is not part of the approved baseline.")
    if policydiff("{}",
      URI.decode(iam.client.get_role_policy(\
        :role_name => role,
        :policy_name => policy
      )[:policy_document]),
      {:argv => ARGV, :diff => options.diff})
    end
    options.dryrun ? nil : \
      iam.client.delete_role_policy(
        :role_name => role,
        :policy_name => policy
      )
end
```



Sign me up! What's next?



- Security as Code
- Self-Service Testing
- Red Team/Blue Team
- Inline Enforcement
- Analytics & Insights
- Detect & Contain
- Incident Response
- Investigations
- Forensics

Migrate App Security into DevOps Teams

goto; conference

- Planning Security
- Testing Features for Security Defects
- Integrating Security Testing into CICD
- Remediating Security Issues

Secure Components

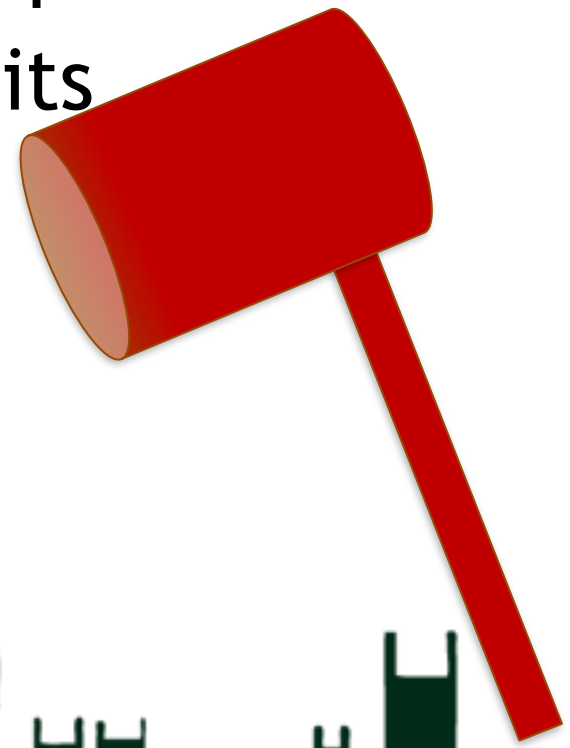
Scanners

Instrumentation

Red Team Via Security Engineering

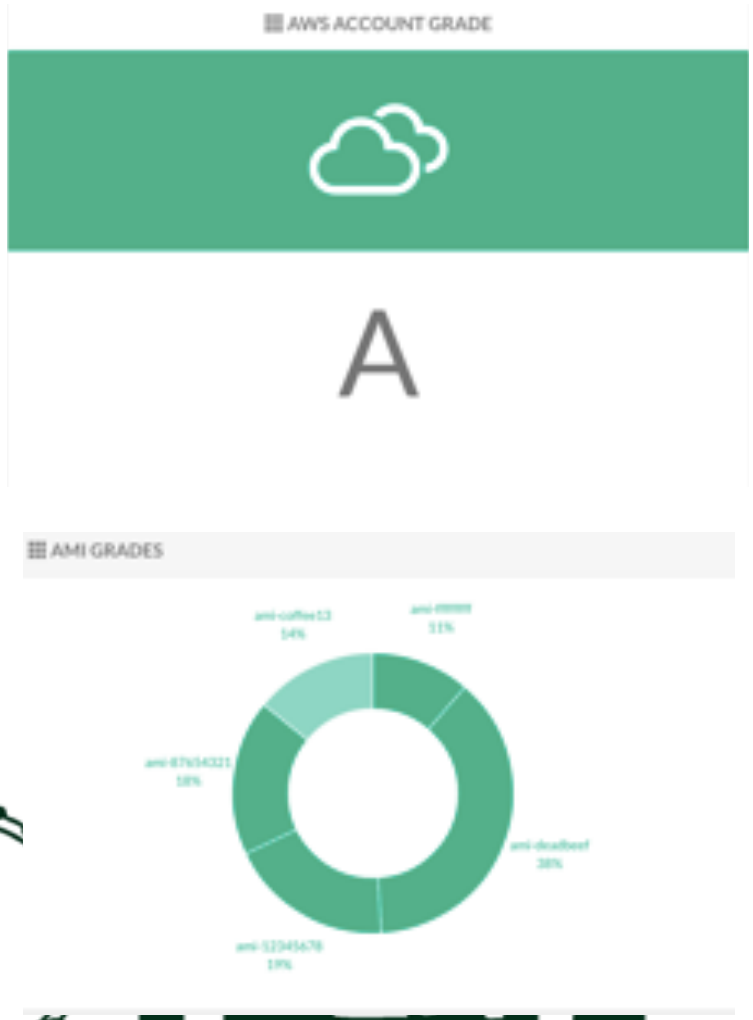
goto; conference

- #RedTeamMonday
- Developing Secure Code Components
- Reverse Engineering & Exploits
- Increased Education
- Mass Reconnaissance
- Scoring & Prioritization



Enforce in Real-time with Compliance Operations

- Metrics & Reporting
- Discover Compliance Issues in Real-time
- Improve maturity of controls
- Prepare for Security Operations & Red Team

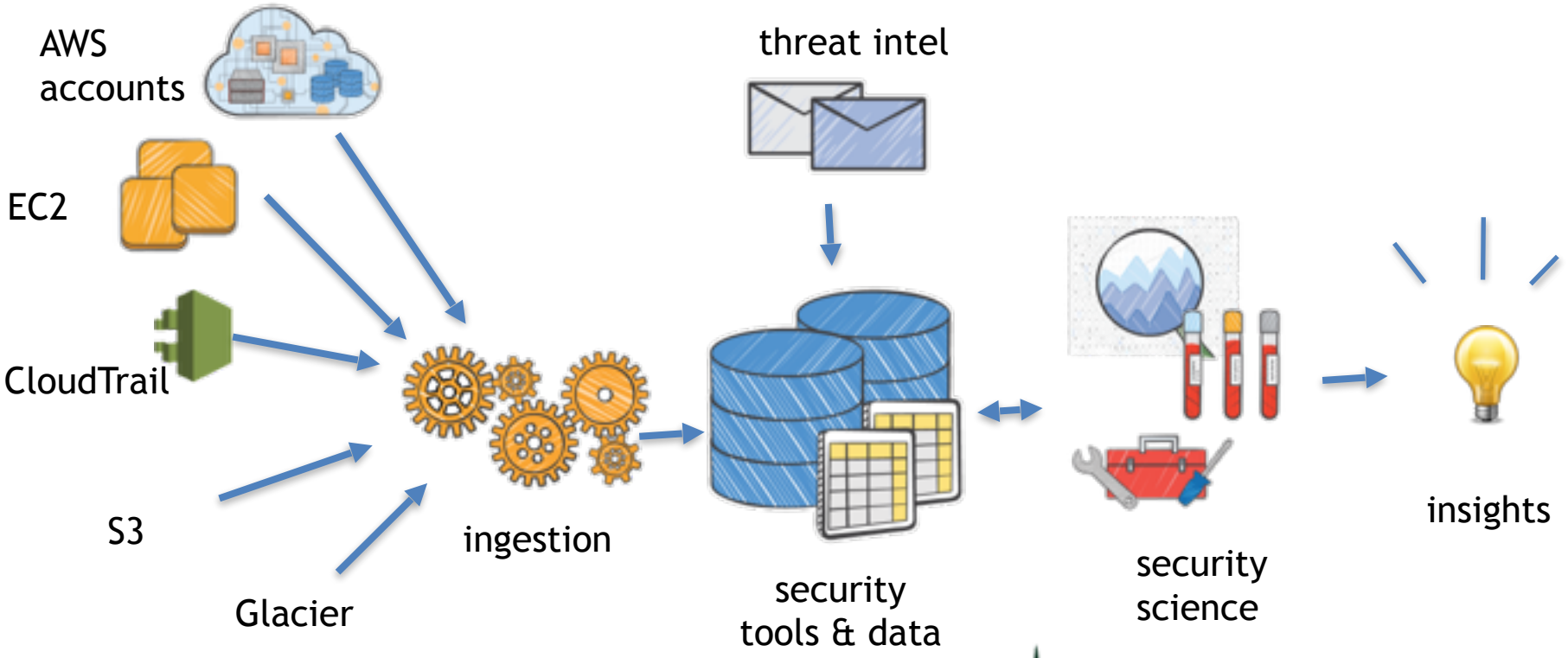


Blue Team via Security Operations

goto; conference

- Detect & Contain
- Research Red Team Events
- Keep Track of Threat Intel
- Develop Monitoring & Alerting
- Triage Events
- Perform Forensics

Data is Critical



Emerging Security Trends

goto; conference

- Shortage of Security Professionals
- Big companies are attempting to scale security to move faster: Facebook, Netflix, LinkedIn, AWS, Intuit
- Industry Leaders talking about the integration of DevOps & Security: Joe Sullivan, Jason Chan, Gene Kim, Josh Corman
- Introduction of DevSecOps at MIRCon in 2014
- SecDevOps at RSA 2015 was full day of dedicated content
- LinkedIn People Search: **36** DevSecOps, **13** SecDevOps, **11** DevOpsSec, **33k+** Cloud Security

goto; conference

Please

Remember to rate this session

Thank you!

Join the conversation #gotoldn

goto; conference

Thanks !

Join the conversation #gotoldn