The Road to Rugged

Shannon Lietz
Let us know what you think

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

• 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?

• Case for change is very compelling!

• Planning != Good Code, Less Security Breaches

• Perfection takes too long to get wrong
This isn’t rugged or helpful...

- 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"
- Enter credentials
- Click "Next"
- Click "Next"
- Click "Finish"
And this just creates friction...

YOU

Hopefully it’s not going to be another round of “No’s”...

CISO

YOUR CUSTOMER

Why does it take so long for features?
Which makes everyone...

Bang
Head
Here
But - What if Security can be Rugged?

DevSec Ops:
- Security Engineering: Experiment, Automate, Test
- Security Operations: Hunt, Detect, Contain
- Compliance Operations: Respond, Manage, Train
- Security Science: Learn, Measure, Forecast
Let’s Get Rugged!!

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?

1. Cloud DNS Reveals Private IP of web server
2. Private IP of web server reveals detailed errors or admin interface
3. SSRF or XXE vulnerability exposes Metadata, revealing API Keys
4. API Key allow you to escalate privileges clone system root partition
5. Cloned system gets you SSH keys to app servers and API key with full access
6. With new credentials create trust relationship with external account and clone DB for quiet extraction
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

Account Grade:
B

Heal Account?
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

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

- Secure Components
- Scanners
- Instrumentation
Red Team Via
Security Engineering

• #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

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

- AWS accounts
- EC2
- CloudTrail
- S3
- Glacier
- Ingestion
- Threat intel
- Security tools & data
- Security science
- Insights
Emerging Security Trends

- 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
Please Remember to rate this session

Thank you!
Thanks!