Vulnerability Management & DevSecOps & the Cloud

Oh My!

Patricia Smith
VP, Chief Information Security Officer

Tabrez Naqvi
Sr. Manager, Security Operations
COUNTRIES WORLDWIDE

25+ COMPANIES

100+ COUNTRIES WORLDWIDE

Cox Automotive™

TRANSFORMING THE WAY THE WORLD BUYS, SELLS, OWNS AND USES CARS
<table>
<thead>
<tr>
<th>Monthly Service Appointments Xtime 2016</th>
<th>Monthly Average 3.8M+</th>
<th>OF ALL CAR BUYERS 67%</th>
</tr>
</thead>
<tbody>
<tr>
<td>OF ALL CAR BUYERS Use Autotrader or KBB.com 67%</td>
<td>ACTIVE U.S. DEALERS 22,000+</td>
<td>VEHICLE VALUES SOLD ANNUALLY $57B+</td>
</tr>
<tr>
<td>22,000+ ACTIVE U.S. DEALERS On the Dealertrack Network</td>
<td>60+% OF U.S. FRANCHISE DEALER WEBSITES Operated by Dealer.com</td>
<td>Through Manheim</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>47.7M+ UNIQUE VISITORS</th>
<th>3.8M+ MONTHLY SERVICE APPOINTMENTS Xtime 2016 Monthly Average</th>
<th>43M+ FINANCED TITLES Managed By Dealertrack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly on 13,000+ Dealer.com Websites</td>
<td>48% OF ALL U.S. CARS SOLD Submitted to Lenders with Dealertrack Technology</td>
<td>100+ COUNTRIES Across 6 Continents Global DMS Clients</td>
</tr>
</tbody>
</table>

Cox Automotive™ A leading provider of products and services that connect the automotive ecosystem worldwide
Storm of acquisitions
Challenges

• Some Agile/DevOps
• Varying levels of maturity
• 25+ Independent businesses
• 350+ Scrum teams
• 650+ AWS accounts
• 40+ Datacenters
• 100’s of Internet-facing applications
• 1000’s of microservices
• Lack of standardization across businesses
Somewhere, over the rainbow...

- Cloud-first strategy
- 5 data centers
- DevSecOps/Shift left
- Security as a Service
- Automation
- Standardized technologies and processes

Cox Automotive™
The promise of the Cloud:

- Scalable
- Flexible
- Reliable
- Cost reduction
- High performance
- Increased efficiency
- More secure
The Cloud: it’s great but... what about:

- Tracking assets
- Security testing
- Tracking vulnerabilities
- Access management
- Segregation of duties
- Configuration standards
- Resiliency

Cox Automotive™
The Cloud

It can be scary and confusing
Integrating the same old security processes into the new world will not work.
Make security easily accessible and consumable. Put it in the hands of your engineering teams so they can make it a part of their processes.
Amazon Machine Image Scanning

Scheduled Function

Puts msg on Amazon SQS

Amazon SNS

Triggers a build passing AMI-ID

AWS.Linux AMI
Windows AMI
RHEL AMI

Q.17
Q.2.17

Amazon marketplace

Jenkins

SOC

Job initiated

Terraform state files

Terraform IaC to launch EC2 instance based on new AMI-ID

GitHub

Amazon S3 Bucket

Agent binaries and other scanning artifacts

OS fingerprint plus config info are sent for analysis and NVD scoring

AWS Linux EC2

Windows EC2

RHEL EC2

T2 Burstable performance instance (t2.micro or min. required by OS+Agent)

Approved list updated (add/remove/alert)

Amazon DynamoDB table with Current CAI-approved AMIs

CloudSploit inspects AWS infrastructure for AMIs and reports against Dynamo DB list

Cox Automotive™
Future Plans

Qualys at Cox Automotive
- Near real-time alerts (Slack/Rally/JIRA)
- Approved AMI Marketplace

Cultural Shift
- Partnership (Engineering and Security)
- Shared Goals
Thank You

Cox Automotive

Patricia Smith
VP, Chief Information Security Officer

Tabrez Naqvi
Sr. Manager, Security Operations