CLOUDSEC RULES
EVERYTHING AROUND ME
WHOAMI

- Kyle Dickinson
- Twitter: @KyleHaxWhy
- Cloud Security Architect - Koch Industries
- SANS Instructor – SEC545 Cloud Security Architecture & Operations
WHAT’RE WE DOIN’?

• Refresher on Cloud Concepts
• Logging
• Configuration Management
• Identity and Access Management
• 3@F?46C E@ 3@5J8F2C5
• Takeaways
HEY YOU, GET OFF MY CLOUD...

- Shared Responsibility Model IaaS/PaaS/SaaS
- Infrastructure-as-a-Service (IaaS)
  - Amazon EC2
  - Azure VM
- Platform-as-a-Service (PaaS)
  - Heroku
  - Azure SQL
- Software-as-a-Service (SaaS)
  - Office 365
## Shared Responsibility Model

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance &amp; data governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patches &amp; Upgrades</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Customer**
- **Cloud Provider**
LOGGING
AWS LOG SERVICES AT A GLANCE

• CloudTrail
  – Who/What/Where/When/How
• VPC FlowLogs
  – North/South NetFlow monitoring
  – VPC Mirroring
• CloudWatch
  – Metrics
  – Alarms
AWS CLOUDTRAIL EXAMPLE

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDATMCUXEGKNPMPSIPJ6",
    "arn": "arn:aws:iam:: 12345678901: user/--- ",
    "accountId": 12345678901,
    "userName": "--- "
  },
  "eventTime": "2019-06-06T00:23:48Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?
state=hashArgs%23&isauthcode=true",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "07c7d20e-e514-478b-b89f-62ad623afccb",
  "eventType": "AwsConsoleSignIn",
  "recipientAccountId": "12345678901"
}
```
“CHECK YOURSELF BEFORE YOU WRECK YOURSELF” – ICE CUBE
CENTRALIZE CLOUDTRAIL LOGS

- Benefits:
  - Ships logs out of account
  - Enables single ingestion point
  - Reduces # of buckets in environment
VISUALIZING AWS CLOUDTRAIL

AWS Cloudtrail: Summary

Total Events
268,533
(a few seconds ago)

Root User Logins
0
(a few seconds ago)

Console Login Sources

<table>
<thead>
<tr>
<th>Value</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>npf13ccc7.dynkbo.deutschland.de</td>
<td>31.19</td>
<td>204,190</td>
</tr>
<tr>
<td>144-163-167-45.nlrk.centurylink.net</td>
<td>33.33</td>
<td>1</td>
</tr>
</tbody>
</table>

Top AWS Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Value</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>eu-west-1</td>
<td>93.20</td>
<td>250,264</td>
<td></td>
</tr>
<tr>
<td>us-west-1</td>
<td>3.25</td>
<td>8,723</td>
<td></td>
</tr>
<tr>
<td>us-east-1</td>
<td>2.63</td>
<td>7,667</td>
<td></td>
</tr>
<tr>
<td>us-west-2</td>
<td>0.91</td>
<td>2,450</td>
<td></td>
</tr>
<tr>
<td>eu-central-1</td>
<td>0.01</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

Others

<table>
<thead>
<tr>
<th>Region</th>
<th>Value</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-southeast-1</td>
<td>0.00%</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ap-northeast-2</td>
<td>0.00%</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ap-south-1</td>
<td>0.00%</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ca-central-1</td>
<td>0.00%</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

(a few seconds ago)
## Visualizing CloudTrail S3 Logs

### AWS Cloudtrail: S3
Overview of AWS S3 activity based on Cloudtrail data.

Drag widgets to any position you like in unlock/edit mode.

#### Total S3 Events
- **254,926** events

#### Top S3 Event Names
<table>
<thead>
<tr>
<th>Value</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 5 values</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GetObject</td>
<td>95.53%</td>
<td>228,226</td>
</tr>
<tr>
<td>PutObject</td>
<td>5.42%</td>
<td>13,827</td>
</tr>
<tr>
<td>UploadPart</td>
<td>3.21%</td>
<td>5,400</td>
</tr>
<tr>
<td>HeadObject</td>
<td>1.04%</td>
<td>2,837</td>
</tr>
<tr>
<td>DeleteObject</td>
<td>0.26%</td>
<td>652</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ListObjects</td>
<td>0.19%</td>
<td>494</td>
</tr>
<tr>
<td>ListBucket</td>
<td>0.13%</td>
<td>322</td>
</tr>
<tr>
<td>CopyObject</td>
<td>0.13%</td>
<td>330</td>
</tr>
<tr>
<td>CompleteMultipartUpload</td>
<td>0.11%</td>
<td>273</td>
</tr>
<tr>
<td>GetBucketLocation</td>
<td>0.09%</td>
<td>23</td>
</tr>
<tr>
<td>CreateMultipartUpload</td>
<td>0.08%</td>
<td>195</td>
</tr>
<tr>
<td>ListParts</td>
<td>0.06%</td>
<td>156</td>
</tr>
<tr>
<td>GetObject</td>
<td>0.06%</td>
<td>142</td>
</tr>
<tr>
<td>GetBucket</td>
<td>0.04%</td>
<td>114</td>
</tr>
<tr>
<td>GetBucketLocation</td>
<td>0.04%</td>
<td>114</td>
</tr>
<tr>
<td>GetBucketWebsite</td>
<td>0.04%</td>
<td>114</td>
</tr>
<tr>
<td>GetBucketPolicy</td>
<td>0.04%</td>
<td>114</td>
</tr>
</tbody>
</table>

#### Top Error Messages
<table>
<thead>
<tr>
<th>Value</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 5 errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The requested range is not satisfiable</td>
<td>61.10%</td>
<td>4,658</td>
</tr>
<tr>
<td>The specified key does not exist</td>
<td>22.56%</td>
<td>1,500</td>
</tr>
<tr>
<td>Access Denied</td>
<td>3.00%</td>
<td>199</td>
</tr>
<tr>
<td>Object lock configuration does not exist for this bucket</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The CORS configuration does not exist</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The specified bucket does not have a website configuration</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The server-side encryption configuration was not found</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The replication configuration was not found</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The public access block configuration was not found</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The TagSet does not exist</td>
<td>1.72%</td>
<td>114</td>
</tr>
<tr>
<td>The bucket policy does not exist</td>
<td>1.29%</td>
<td>86</td>
</tr>
<tr>
<td>We encountered an internal error. Please try again</td>
<td>0.62%</td>
<td>7</td>
</tr>
</tbody>
</table>

#### Top S3 Regions
- **Top 5 regions**
  - eu-west-1: 94.47% 240,835
  - us-west-1: 3.21% 8,185
  - eu-west-2: 2.31% 5,954
  - us-east-1: 0.08% 12

*a few seconds ago*
VISUALIZING VPC FLOWLOGS
“HEY – WE SHOULD LOOK FOR THESE EVENTS!”

- Root User Activity
- MFA being disabled
- CloudTrail being disrupted
- Security Groups permitting unrestricted access
- Activity performed in uncommon regions
- Bucket Policy changes
- …and the list keeps growing!
CONTINUOUS COMPLIANCE
AS SHADOW I.T. FADES. THE SHADOW ACCOUNT IS BORN

• Accounts created with personal cards
• Risks are:
  – No Data Governance
  – No Security Controls
  – <Insert Doomsday Scenario Here>
AWS CONFIG

• Continuous Monitoring
• Change Management
• Compliance Standards
• Multi-account Management and Remediation
“CHECK YOURSELF BEFORE YOU WRECK YOURSELF” – ICE CUBE
PROWLER

• Created by Toni Blyx
• Used for AWS auditing
• Can perform
  – CIS Benchmark Checks
  – GDPR
  – HIPAA
• Digital Forensics Readiness!? – Great for validation!
SECURITY MONKEY

- Created by Netflix
- Monitors AWS, GCP, OpenStack
- Uses cross-account role authentication
REDLOCK

- SaaS Platform that monitors Azure, AWS, GCP
- HIPAA, GDPR, PCI, NIST, SOC II, CIS, custom signatures
- Cross-Account Role Authentication
- Well documented API
IAM
SWITCH-ROLE METHOD

- Leverages federated identity/SSO
- Scalable
- Auditable
IAM BEST PRACTICES

• MFA…MFA…MFA!
  – Root Account
  – Console Users
• Federate Identity
• User Lifecycle Policy
  – Leverage Tags
  – Automation
BOUNCER TO BODYGUARD
PROACTIVE ENABLEMENT

- Transform how Security is perceived
- Enable development teams
- Understand developer needs
- Adapt to multiple solutions
WHAT TO DO NEXT

• Strategize Logging
• Incident Response Teams/Investigations have appropriate access
• Continuous Compliance solution
• Asset Inventory
• Automation!
• Work with Development teams