



Splunking the Clouds: finding the needle in AWS & Azure

Daniel BARBU – Manger of Security @ Adobe | **Uzoma OGBONNA** – Cloud Security Engineer @ Adobe



Start with the WHY



AWS vs. Azure

Description	Amazon Web Services	Microsoft Azure
Billing container	Account	Subscription
Management & Monitoring	Cloud Watch	Azure Diagnostics + App Insights
Infrastructure as Code	Cloud Formation	Azure Resource Manager
Grouping Mechanism	Resource Groups	Resource Groups
User Interface	Console	Portal
Object storage	S3 Service	Blob Storage
Compute/Virtual Servers	EC2	Virtual Machines
Networking	Virtual Private Cloud	Virtual Network
Access Control	Identity and Access Management	Role Based Access Control

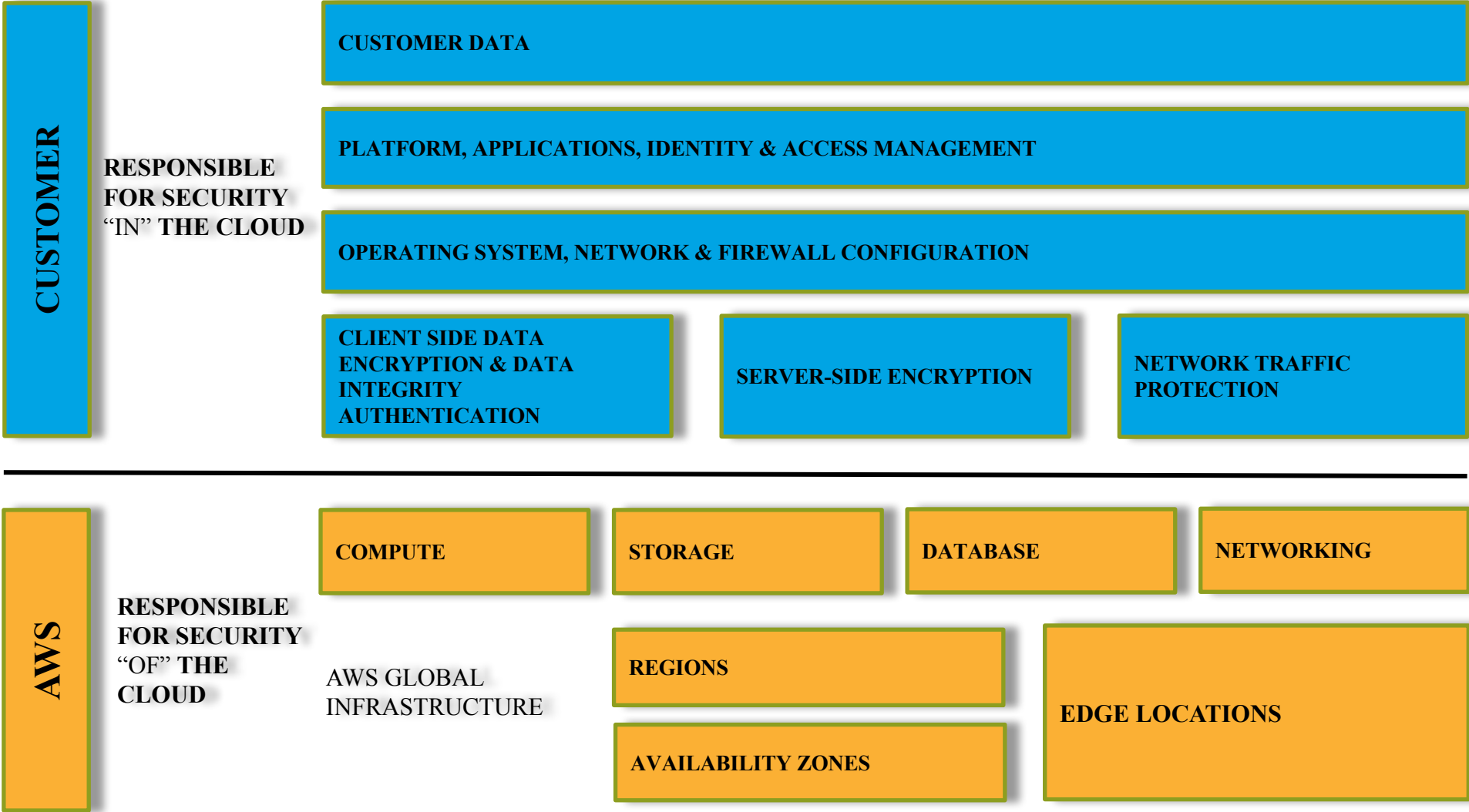
AWS vs. Azure: Security Services

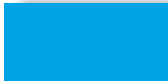
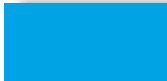

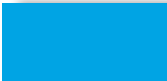
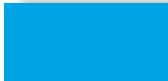
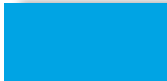


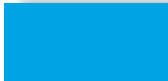
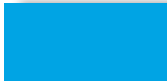


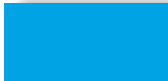
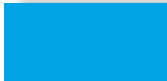

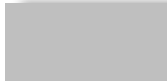
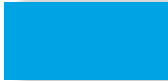

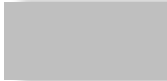
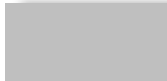
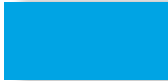

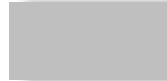
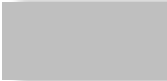
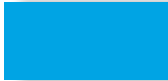
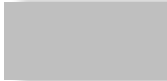
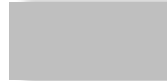
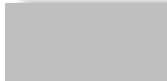
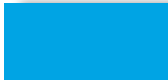
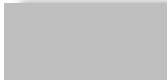
Category	AWS Service	Azure Service
Authentication and authorization	Identity and Access Management MFA	Azure AD/Role-based access control MFA
Securing key and secrets	Key Management Service CloudHSM	Key Vault
Firewall	Web Application Firewall	Web Application Firewall (preview)
Security assessment	Inspector	Security Center
Security best practices	Trusted Advisor	Advisor (Preview)
Directory	Directory Service	Azure Active Directory Azure AD B2C Azure AD DS

Journey through the clouds



Shared Responsibility Model

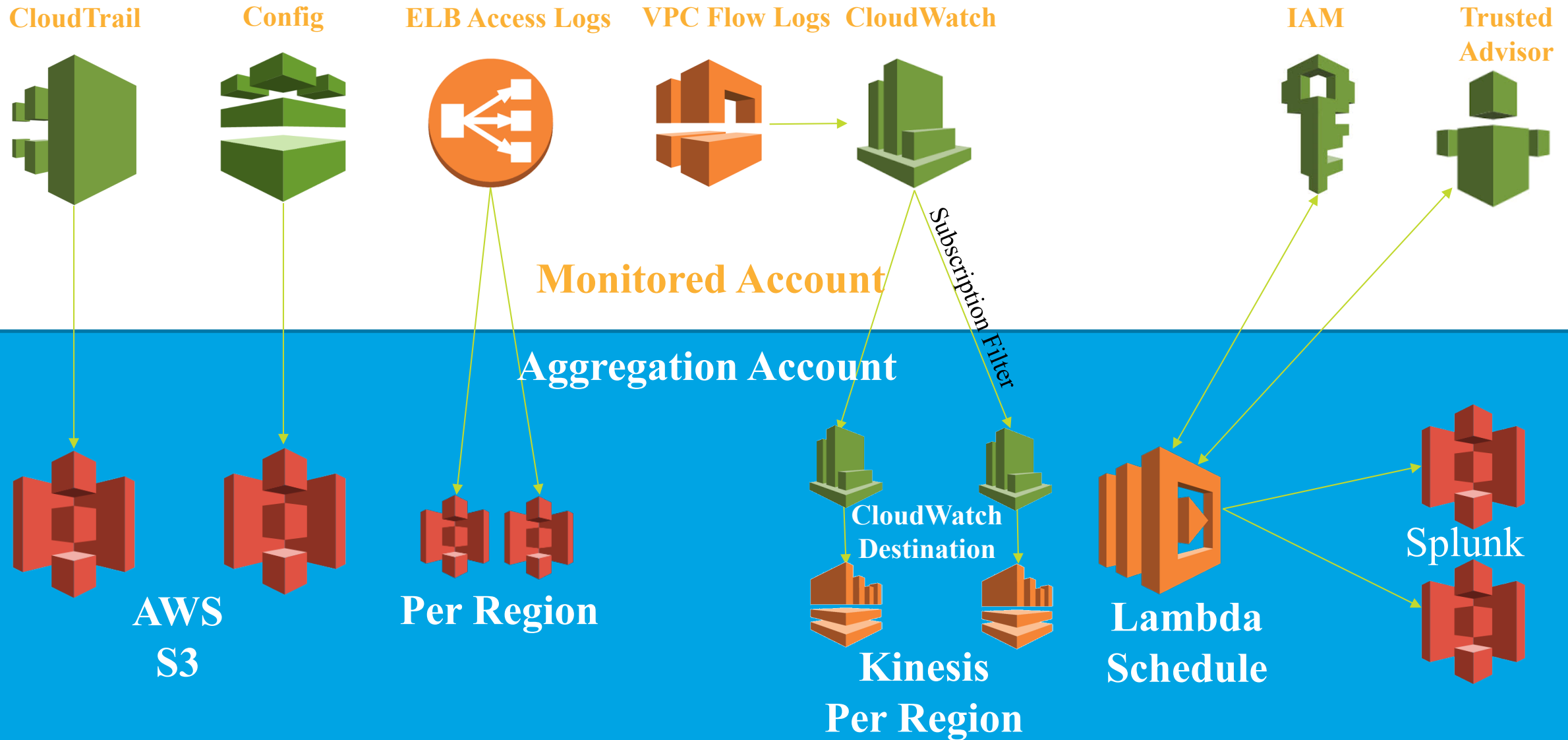


Responsibility	On-Prem	IaaS	Paas	SaaS
Data classification & accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host infrastructure				
Physical security				
		Cloud Customer		 Cloud Provider



Back to the haystack

How will you monitor?



What do you collect?

Category	AWS Service	Azure Service
Authentication and authorization	Identity and Access Management MFA	Azure AD/Role-based access control MFA
Configuration	AWS Config	Azure Resource Config
Audit	AWS Cloudtrail	Azure Audit
Security assessment	Inspector	Security Center
Security Advisor	Trusted Advisor	Advisor (Preview)
Network flows	ELB Access Logs VPC Flow Logs	Network Watcher

What do you do with it?

- Content Development:
 - Alerts
 - Dashboards
 - Lookups
 - Workflows
 - Reports
 - Adaptive and Automated responses

Why?

- **Find it before the boogey man does!**
- *misconfigurations, intrusion monitoring, baselining*
- *triage, forensics, deep diving*



Splunk IT!

Getting through the storms



Never Design OR Implementation

Design (Cloud Flaws)

☐

Name

Group ID

Group Name

VPC ID

Description

☐

sg-

default

vpc-

default VPC security group

Security Group: sg-

Description

Inbound

Outbound

Tags

Edit

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Security Group: sg-

Description

Inbound

Outbound

Tags

Edit

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	

Implementation (Human Error)

- Virtual Machines without a Network Security Group (Azure)
- Weak Security group configs (AWS & Azure)
- Non MFA Login (AWS)
- Key Rotation / Compromised Keys
- Too permissive IAM policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Id": "test4",  
4   "Statement": [  
5     {  
6       "Sid": "Test",  
7       "Effect": "Allow",  
8       "Principal": "*",  
9       "Action": [  
10        "s3:GetObject",  
11        "s3:ListBucket"  
12      ],  
13      "Resource": [  
14        "arn:aws:s3:::defcampbucket",  
15        "arn:aws:s3:::defcampbucket/*"  
16      ]  
17    }  
18  ]  
19 }
```

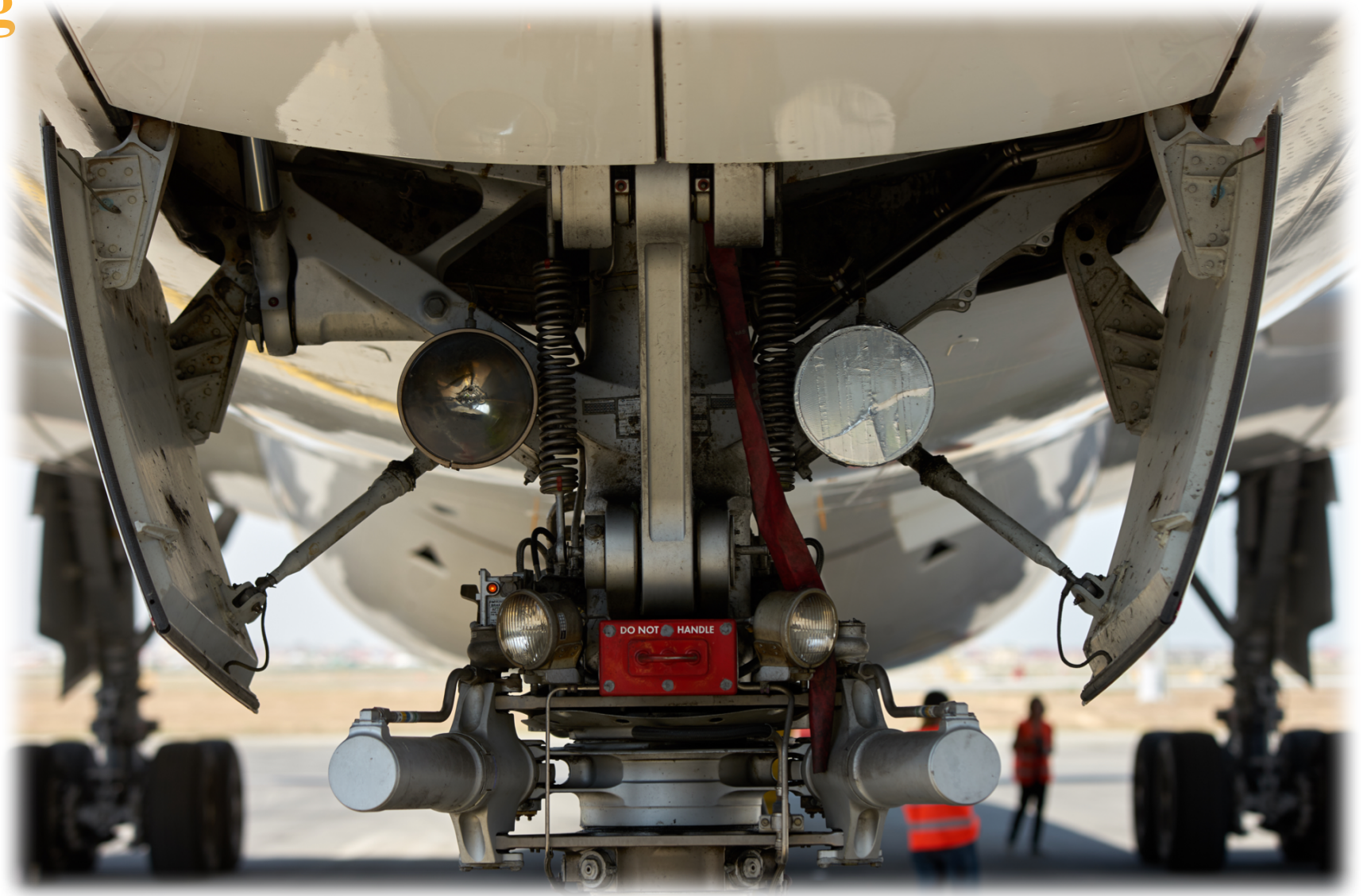
Security Group: sg-

Description Inbound Outbound Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	SSH FROM ANYWHERE

Prepare for landing



AWS Data - Before

```
> 10/26/17 9:10:20.000 PM { [-]
  ARN: arn:aws:ec2:us-west-2: :security-group/sg-1
  availabilityZone: Not Applicable
  awsAccountId: ?
  awsRegion: us-west-2
  configuration: { [-]
    description: For use only with Zerus testing
    groupId: 
    groupName: Zerus-Purple
    ipPermissions: [ [+]
  ]
    ipPermissionsEgress: [ [+]
  ]
    ownerId: 
    tags: [ [+]
  ]
    vpcId: vpc-1
  }
  configurationItemCaptureTime: 2017-06-29T23:39:36.166Z
  configurationItemStatus: OK
  configurationItemVersion: 1.2
  configurationStateId: 1498779576166
  configurationStateMd5Hash: ad0da55d430bb5ebb83fe70fb7e1880
  relatedEvents: [ [-]
  ]
  relationships: [ [-]
    { [-]
      name: Is contained in Vpc
      resourceId: vpc-
      resourceType: AWS::EC2::VPC
    }
  ]
  resourceId: sg-
  resourceName: Zerus-Purple
  resourceType: AWS::EC2::SecurityGroup
  snapshot_id: 2fe36ea2-f2cd-46b3-ace7-72eef0931d64
  snapshot_time: 1509048617.218747
```



AWS Data - After

AWS Monitoring

Edit

Export

...

AWS Console Logins without MFA

Event Time	AWS Account ID	Account Description	User	User Type	ARN
2017-10-26T09:14:26Z	432143214321	Test Account 4	root	Root	arn:aws:iam::432143214321:user/root
2017-10-26T20:22:39Z	123412341234	Test Account 1	uzo-test	IAMUser	arn:aws:iam::123412341234:user/uzo-test

Security Groups allowing traffic from 0.0.0.0/0

AWS Account ID	Account Description	Ticket Queue	Security Group	Port	Protocol	Description	ENI/Instance/VPC
432143214321	Test Account 4	SEC	sg-654321	22	TCP	Allow SSH	eni-123456
123412341234	Test Account 1	SEC	sg-123456	3306	TCP	For MySQL	i-222222

Weak Bucket ACL's

AWS Account ID	Account Description	Resource Name	Url	Bucket Owner	Permission
432143214321	Test Account 4	test-bucket-1	test-bucket-1.s3.amazonaws.com	Bob	AuthenticatedUsers:Read
123412341234	Test Account 1	test-bucket-2	test-bucket-2.s3.amazonaws.com	Jane	AllUsers:Read

AWS Old Keys

1m ago

AWS Account ID	Account Description	User	Access Key 1 Active	Access Key 1 Last Rotated	Access Key 2 Active	Access Key 2 Last Rotated
432143214321	Test Account 4	root	True	2016-11-02T21:04:54+00:00	False	2016-03-15T16:47:57+00:00
123412341234	Test Account 1	bob	False	2013-03-03T18:55:13+00:00	True	2015-08-02T18:09:27+00:00

AWS Notables / Alerts

- SSH Key created offsite
- Threat Activity Detected
- Short Lived User accounts
- Non Federated / non-MFA login
- VPC Flow Possible Outbound Port Scanning
- Globally exposed S3 buckets
- Account with X number of sockets (100+)

Search

```
index=aws sourcetype=aws:cloudtrail tag=authentication action=success eventName=ConsoleLogin
"additionalEventData.MFAUsed"=No "userIdentity.type"!=FederatedUser NOT "additionalEventData
.SamlProviderArn"=* NOT src_category=*
| rex field=userIdentity.arn "^.*\/(?P<src_user>[^\$]+)$"
| eval user=coalesce(if(userName!="unknown",userName,src_user),"unknown")
| lookup dnslookup clientip AS src OUTPUT clienthost AS src_dns
| iplocation src prefix=src_
| rename src_City as src_city, src_Country as src_country, src_lon as src_long
| eval type="alert"
| eval subject="AWS Console Login non federated non mfa."
| eval service="cloudtrail"
| eval body="The user "+user+" initiated a "+eventName+" event for account " + aws_account_id
| eval desc="AWS CloudTrail Logging Non Federated Non MFA Console Login Detected for source not tagged as
an Adobe asset"
| eval tag="alert"
| `get_event_id`
| `map_notable_fields`
```


Azure Data - Before

i	Time	Event
✓	11/3/17 3:39:51.000 PM	<pre>{ [-] id: /subscriptions/[REDACTED]/resourceGroups/uzoTest/providers/Microsoft.Compute/virtualMachines/uzoTestVm location: northeurope name: uzoTestVm properties: { [-] availabilitySet: { [+] } diagnosticsProfile: { [+] } hardwareProfile: { [+] } networkProfile: { [+] } osProfile: { [-] adminUsername: uzo computerName: uzoTestVm linuxConfiguration: { [+] } secrets: [[+]] } provisioningState: Succeeded storageProfile: { [+] } vmId: 4d05fd70-636d-4ec8-89cf-428dd3a26b2e } resources: [[-] { [-] id: /subscriptions/[REDACTED]/resourceGroups/uzoTest/providers/Microsoft.Compute/virtualMachines/uzoTestVm/extensions/OmsAgentForLinux location: northeurope name: OmsAgentForLinux properties: { [+] } type: Microsoft.Compute/virtualMachines/extensions }] subscriptionId: [REDACTED] type: Microsoft.Compute/virtualMachines }</pre>

Parsing Azure data

```
sourcetype="azure:resource" type="Microsoft.Network/networkSecurityGroups" | dedup name
```

Last 7 days ▾



```
| spath output=SG_Parse path=properties.securityRules{}  
| mvexpand SG_Parse  
  
| spath input=SG_Parse output=sg_name path=name  
| spath input=SG_Parse output=sg_ruleName path=properties.priority  
| spath input=SG_Parse output=sg_priority path=properties.priority  
| spath input=SG_Parse output=sg_access path=properties.access  
| spath input=SG_Parse output=sg_direction path=properties.direction  
| spath input=SG_Parse output=sg_sourceAddress path=properties.sourceAddressPrefix  
| spath input=SG_Parse output=sg_sourcePort path=properties.sourcePortRange  
| spath input=SG_Parse output=sg_destinationAddress path=properties.destinationAddressPrefix  
| spath input=SG_Parse output=sg_destinationPort path=properties.destinationPortRange  
  
| eval Rule=sg_access+", "+sg_direction+", "+sg_sourceAddress+": "+sg_sourcePort+", "+sg_destinationAddress+": "+sg_destinationPort+", "+sg_priority  
| rex mode=sed field=Rule "s/\*/ANY/g"  
| table name,sg_name,Rule | stats list(sg_name) as "SG Name", list(Rule) as "Rule (Access, Direction, Source IP:Source Port, Destination IP: Destination Port, Priority)"  
| by name
```

✓ 2 events (10/19/17 11:00:00.000 PM to 10/26/17 11:15:46.000 PM) No Event Sampling v

Job ▾ || ■ ↶ 🖨 ⬇ ⚡ Fast Mode ▾

Events Patterns Statistics (1) Visualization

100 Per Page Format Preview

name	SG Name	Rule (Access, Direction, Source IP:Source Port, Destination IP: Destination Port, Priority)
APPSNSG	HTTP	Allow, Inbound, ANY:ANY, ANY:80, 100
	default-allow-ssh	Allow, Inbound, ANY:ANY, ANY:22, 1000

IP / VM Name / Security Group

52.

Last 7 days ▾

Hide Filters

Resource Group	Display Name	Jira Queue	Subscription ID
Azure_test_uzo	DMa/Sandbox shared R&D (AZR0002)	OI	09d29343-ed9a-4ad8-baa3-25e147d2d48a

Virtual Machine Info

!

VM Name ▾	Admin Username ▾	Operating System ▾
-----------	------------------	--------------------

WebVM1	demouser	Canonical 14.04.5-LTS
--------	----------	-----------------------

NIC - Security Group Configuration

.169.198.213

!

name ▾	SG Name ▾	Rule (Access, Direction, Source IP:Source Port, Destination IP: Destination Port, Priority) ▾
--------	-----------	--

APPSNSG	HTTP default-allow-ssh	Allow, Inbound, ANY:ANY, ANY:80, 100 Allow, Inbound, ANY:ANY, ANY:22, 1000
---------	---------------------------	---

🔍

⬇

i

↺

17m ago

Recent Related Notables (Last 7 days)

_time ▾	rule_name ▾	src ▾	dest ▾	owner ▾	status_label ▾
---------	-------------	-------	--------	---------	----------------

2017-10-25 10:45:12	Azure Weak Security Group			unassigned	New
---------------------	---------------------------	--	--	------------	-----

Turbulence

- No packet-level visibility
- No ability for signature-type traffic detection
- Configuration data doesn't exist for all resource types.
- Configuration data has embedded arrays and are JSON format.
- Creating the logic, alerts falls on the Security team



Happy Landing

- Familiarity with the security and policy checks
- Self Enrollment
- Entirely Passive
- Automatable audits & ticketing
- Automatic Field Extractions
- Integrates with correlation rules
- Extensible Auditing



Future Plans

- Automation & Orchestration
- Artificial Intelligence & Machine Learning
- Intelligence Driven Operations



Thank you!



Adobe