Splunking AWS For End-To-End Visibility

Randy Young

Principal Product Manager, Splunk

Jove Zhong

Director of Engineering, Splunk

.conf2016

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Splunk & Amazon Web Services
- Splunk Engineering Internal Insights
- Demo
- Q & A

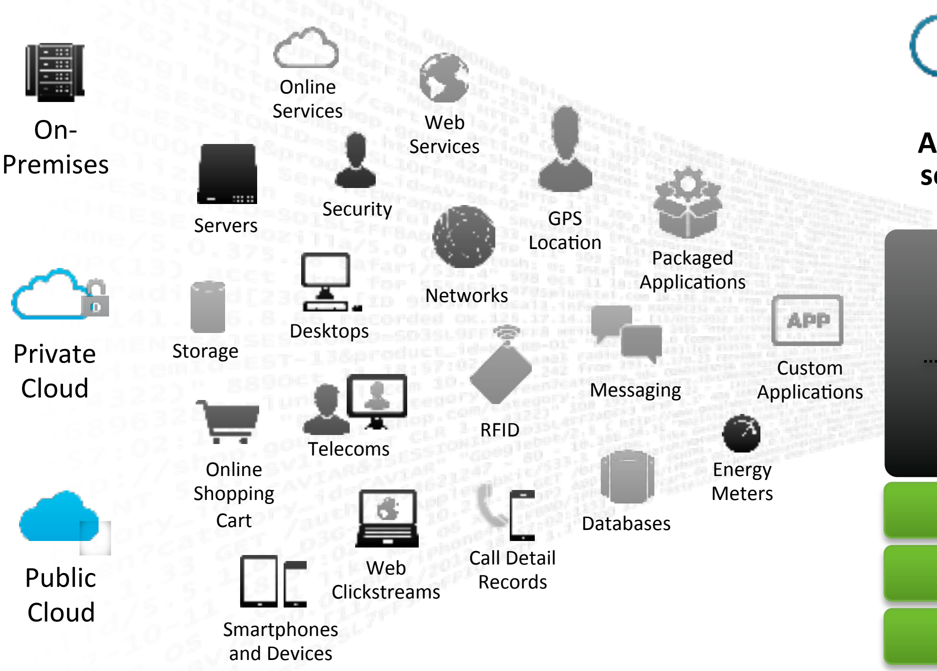
What Can Splunk Do For My AWS Environment?

.conf2016

splunk>

Splunk: Industry Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume



On-Premises

Private Cloud

Public Cloud

Online Services

Web Services

Servers

Security

GPS Location

Networks

Packaged Applications

Storage

Desktops

Messaging

Custom Applications

RFID

Telecoms

Online Shopping Cart

Energy Meters

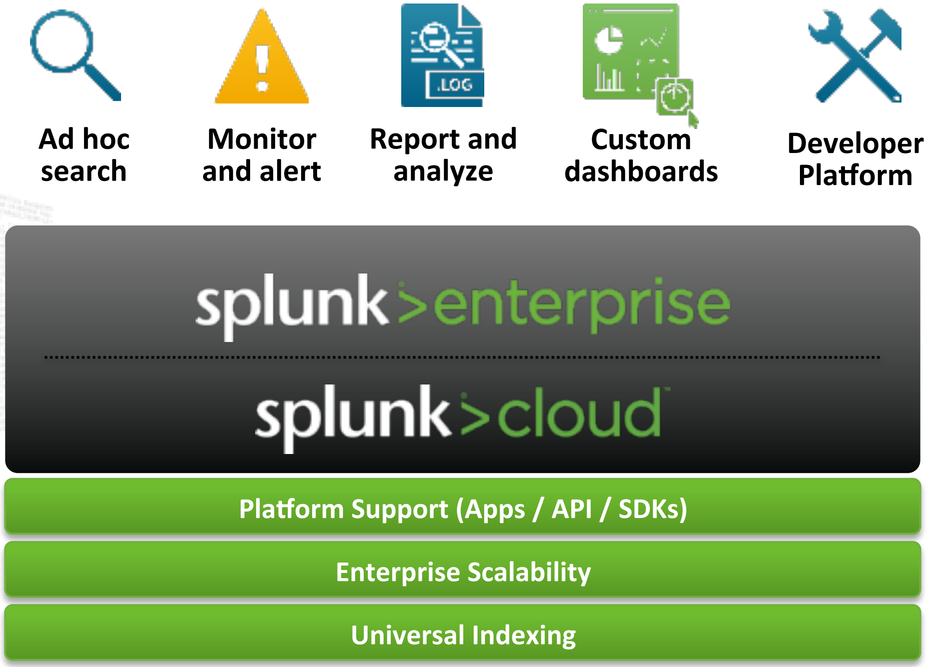
Databases

Web Clickstreams

Call Detail Records

Smartphones and Devices

Answer Any Question



Ad hoc search

Monitor and alert

Report and analyze

Custom dashboards

Developer Platform

splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Splunk Runs **On** And **With** AWS

Delivery Models

As a Service on AWS

splunk>cloud

SOC2 Type II Certified

splunk>light

For small IT teams starts $90/mo

Software

splunk>
Enterprise on AWS

Splunk Core + Enterprise
Security & ITSI available

splunk>light

For small IT teams starts $75/mo

Apps and Integrations

splunk>
Cloud Services Apps

Splunk Add-on for AWS

Splunk App for AWS

Specific Integrations

Config, CloudTrail, CloudWatch, VPC Flowlogs, Lambda: AWS IoT, AWS Kinesis: AWS Cloudformation

Splunk Runs **On** And **With** AWS

Delivery Models

As a Service on AWS

splunk>cloud

SOC2 Type II Certified

splunk>light

For small IT teams starts $90/mo

Software

splunk>
Enterprise on AWS

Splunk Core + Enterprise
Security & ITSI available

splunk>light

For small IT teams starts $75/mo

Apps and Integrations

splunk>
Cloud Services Apps

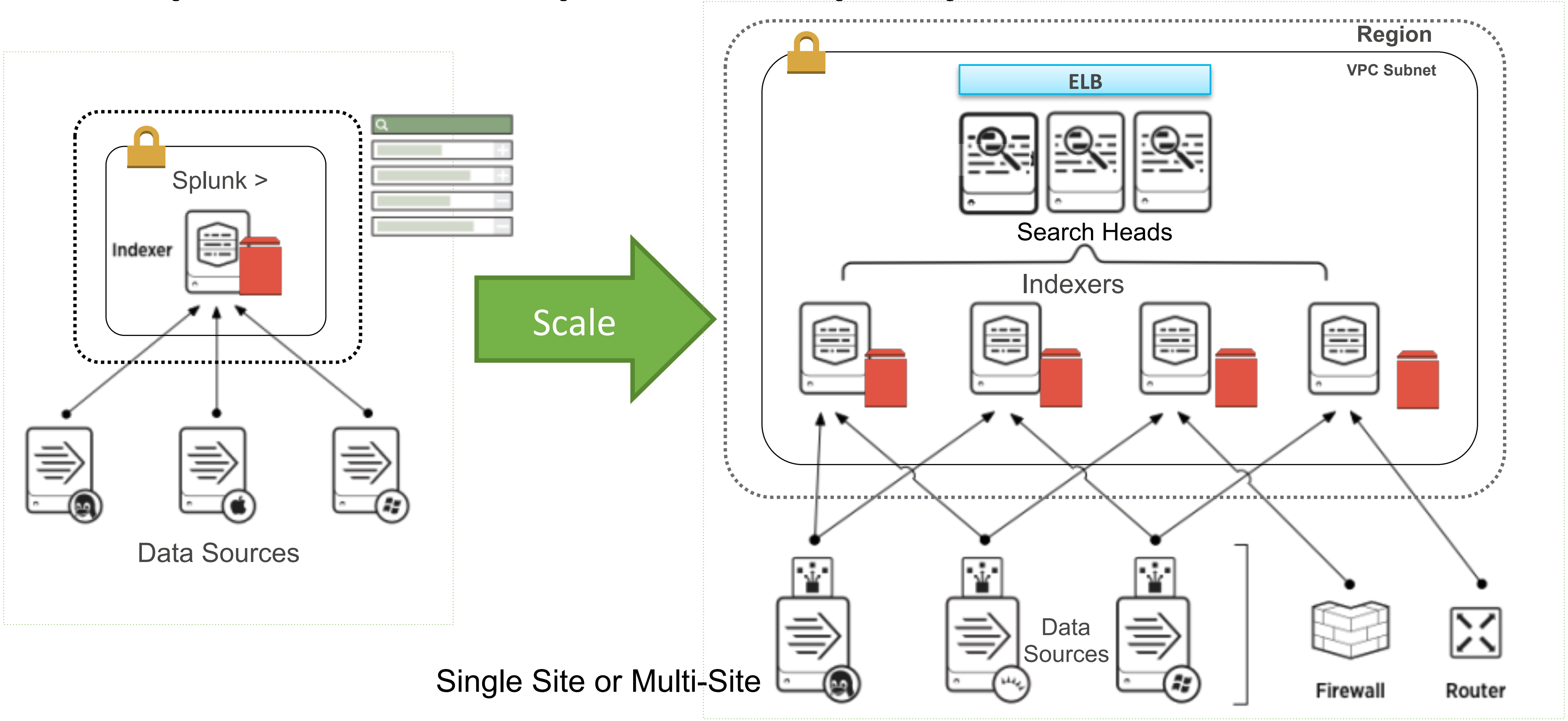
Splunk Add-on for AWS

Splunk App for AWS

Specific Integrations

Config, CloudTrail, CloudWatch, VPC
Flowlogs, Lambda: AWS IoT, AWS
Kinesis: AWS Cloudformation

Splunk Enterprise Deployment On AWS



Single Site or Multi-Site

Splunk Runs **On** And **With** AWS

Delivery Models

As a Service on AWS

splunk>cloud

SOC2 Type II Certified

splunk>light

For small IT teams starts $90/mo

Software

splunk>
Enterprise on AWS

Splunk Core + Enterprise
Security & ITSI available

splunk>light

For small IT teams starts $75/mo

Apps and Integrations

splunk>
Apps & Integrations

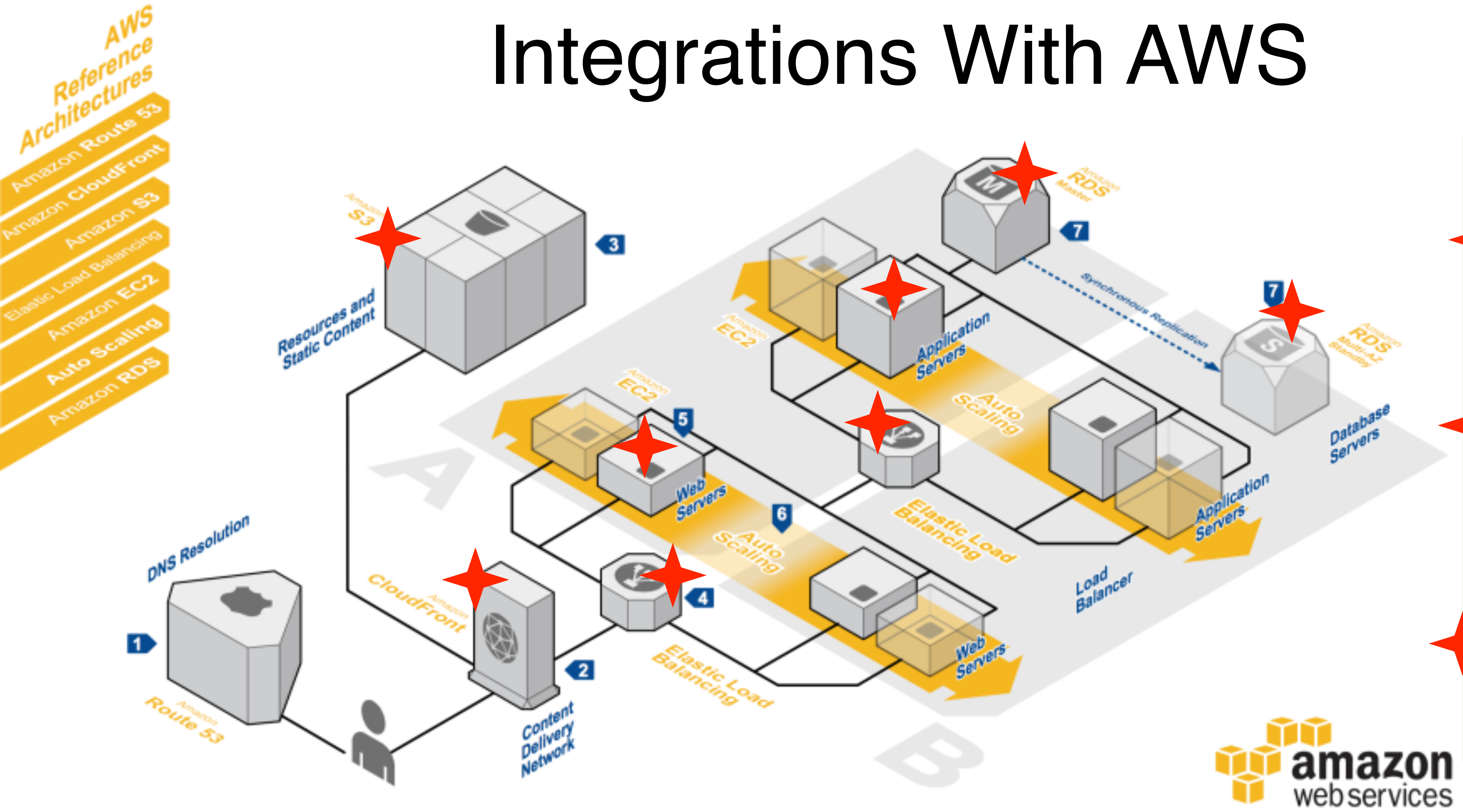
Splunk Add-on for AWS

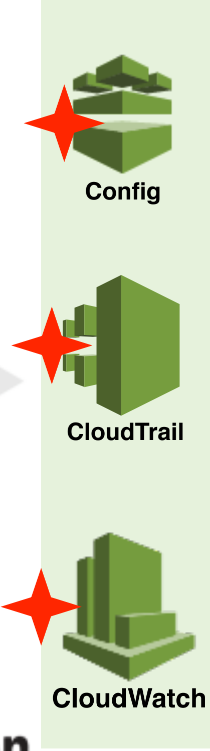
Splunk App for AWS

Specific Integrations

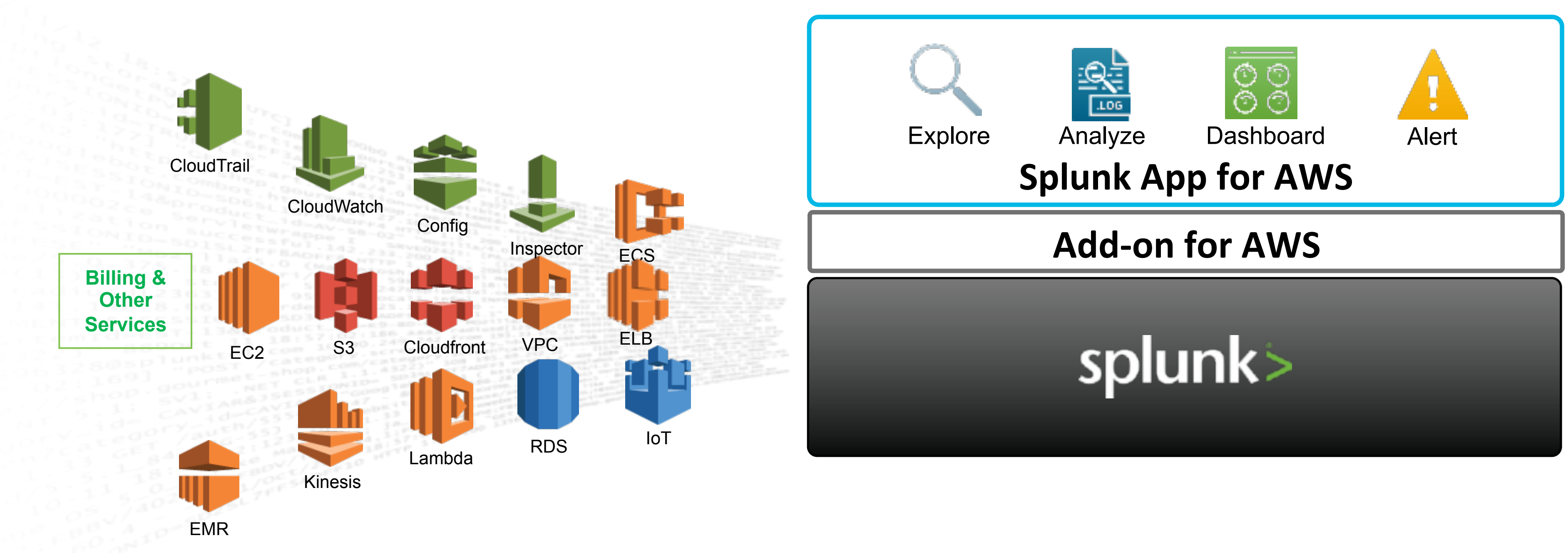
Config, CloudTrail, CloudWatch, VPC
Flowlogs, Lambda: AWS IoT, AWS
Kinesis: AWS Cloudformation

Integrations With AWS





Splunk Insights for AWS Data



CloudTrail

CloudWatch

Config

Inspector

ECS

Billing & Other Services

EC2

S3

Cloudfront

VPC

ELB

RDS

IoT

Lambda

Kinesis

EMR

Explore

Analyze

Dashboard

Alert

Splunk App for AWS

Add-on for AWS

splunk>

Sample Use-cases For AWS Data

Operations Intelligence

- What is my EBS footprint and posture across all my accounts and all my regions?
- Who started/stopped/restarted what instances and when?
- What EC2 instances are underutilized and perhaps overprovisioned?
- What is the traffic volume into my VPC and where is it originating from?
- Why are certain resources unreachable from certain subnets/VPCs?
- List resources with missing or non-conforming tags?
- Etc.

Security Intelligence

- Who added that rule in the security group that protects our application servers?
- Where is the blocked traffic into that VPC coming from?
- What was the activity trail of a particular user before and after that incident?
- Alert me when a user imports key-pairs or when a security group allows all ports
- What instances are provisioned outside of a VPC, by whom and when?
- What security groups are defined but not attached to any resource?
- Etc.

Easy Ways To Use AWS With Splunk

Jove Zhong

Splunk Developer & AWS Admin

.conf2016

splunk>

Now You Have All This Data… What Do You Do With It?

- HR Director: Happy Friday afternoon
- You: (smiles nervously)
- HR Director: Joe was let go today. Close his account. I want to get an email if his account does anything strange this week
- You: (nods nervously)

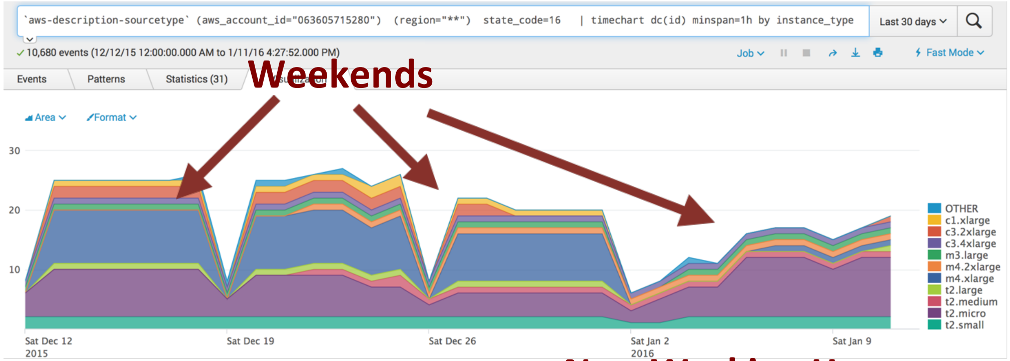
Save as Alert > Email Action

```
sourcetype=aws:cloudtrail userIdentity.userName=joe|table _time event*
user*
```

Now You Have All This Data… What Do You Do With It?

- CFO: Happy Friday afternoon
- You: (smiles nervously)
- CFO: Our production AWS subaccount's spending is on track. But I need to cut of 1/3 of your development subaccount
- You: !#*$%&

AWS Tag Based Instance Auto Start/Stop

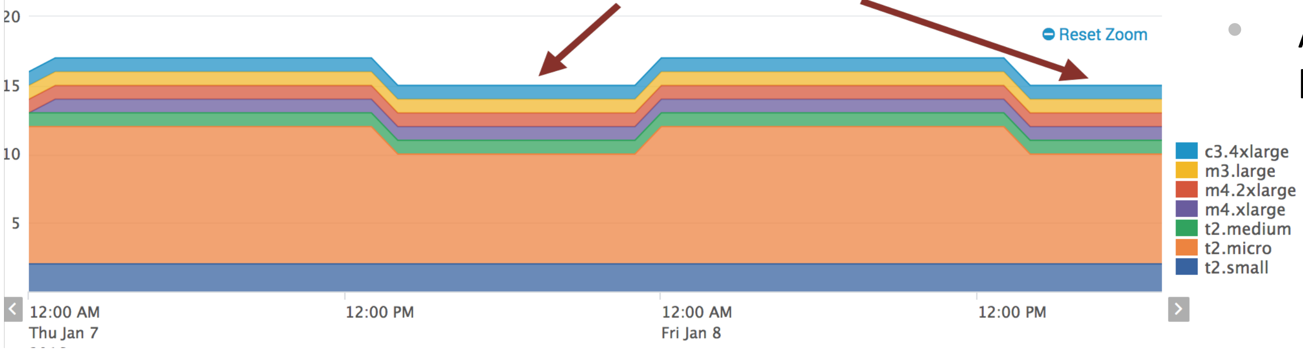


```
`aws-description-sourcetype` (aws_account_id="063605715280") (region="**") state_code=16 | timechart dc(id) minspan=1h by instance_type
```

✓ 10,680 events (12/12/15 12:00:00.000 AM to 1/11/16 4:27:52.000 PM)

Weekends

Non-Working Hours



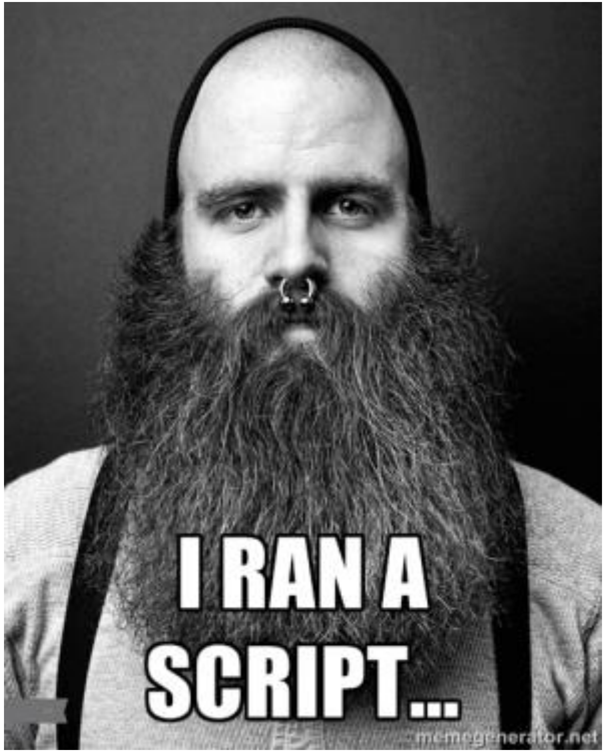
Receipts:

1. Create IAM user ‘robot’
2. Install AWS CLI on splunk host
3. Define tag: PowerSave=LongRun/RareRun/Normal on each instances
4. Create splunk alert
   - CRON, run in morning/night
   - SPL to search instances by tag
   - Alert action to call AWS CLI to batch start/stop instances

Save 40% dev cost!

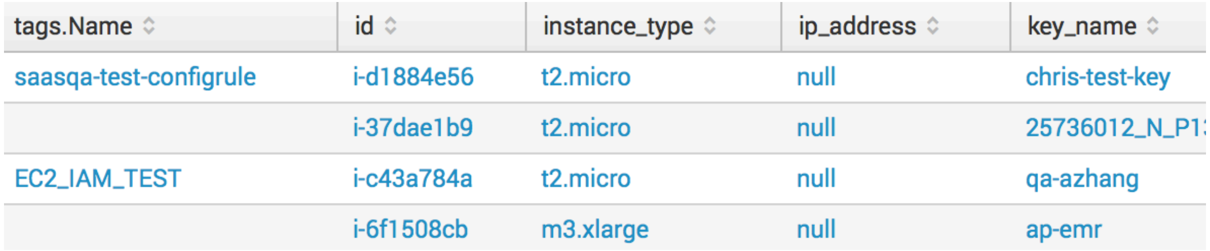
Now You Have All This Data… What Do You Do With It?

- Dev: I am going to run. Happy Friday afternoon
- You: !#*$%&
- Dev: BTW, I ran a script and created a bunch of untagged EC2 Instances. Can you help me find them?



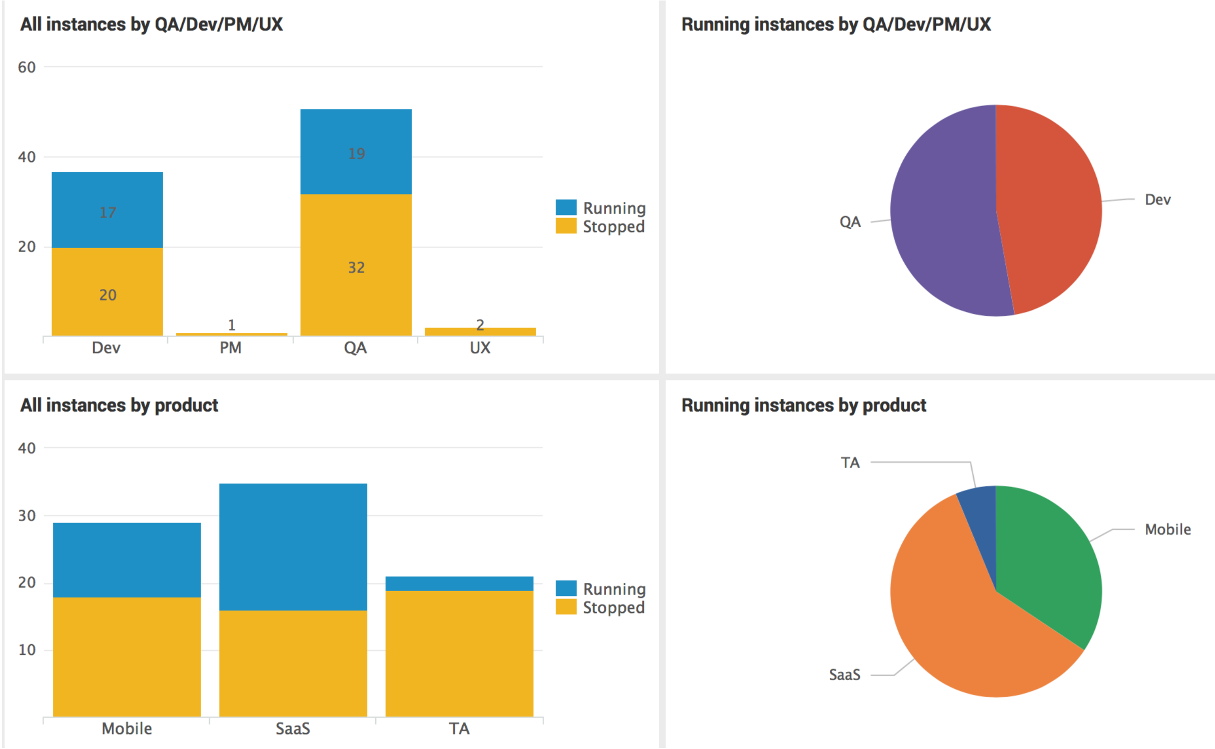
Tag AWS Resource Properly

- Find untagged EC2 instances
  – sourcetype=aws:description source="*:ec2_instances" NOT "tags.Name"=*| table region id instance_type ip_address key_name
- Define a naming conventions for EC2 instance and enforce it
  – DLA_Jove_testEC2Cmd. D: Dev, L: Linux, A: AWS project
  – <Role><OS><Project>_<Owner><Note>
  – sourcetype=aws:description source="*:ec2_instances" (NOT "tags.Name"=*) OR ("tags.Name"=* tags.Name!=Q* tags.Name!=D* tags.Name!=P* tags.Name!=U*)



tags.Name	id	instance_type	ip_address	key_name
saasqa-test-configrule	i-d1884e56	t2.micro	null	chris-test-key
	i-37dae1b9	t2.micro	null	25736012_N_P1
EC2_IAM_TEST	i-c43a784a	t2.micro	null	qa-azhang
	i-6f1508cb	m3.xlarge	null	ap-emr

Just Use The “Name” Tag



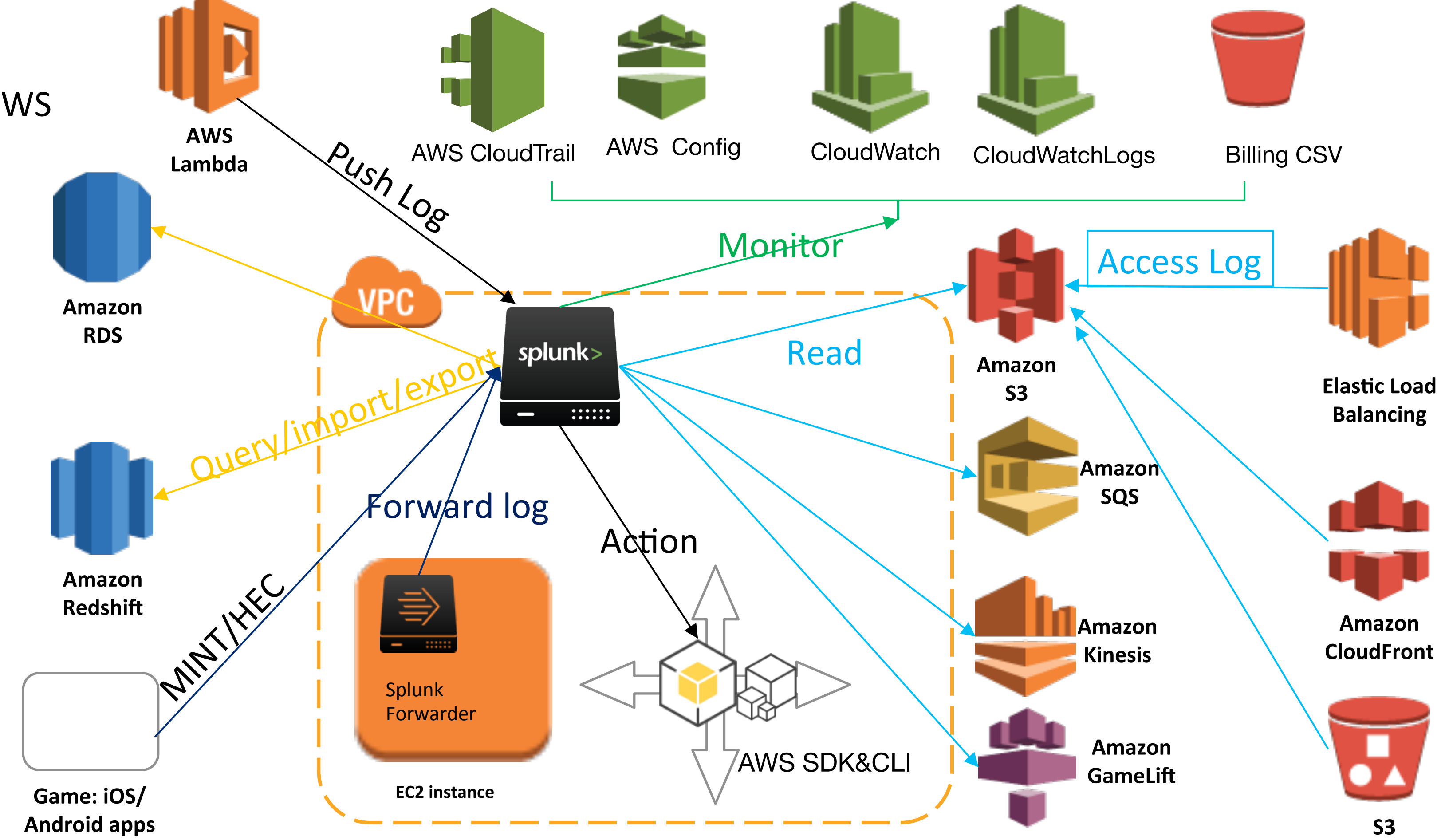
All instances by QA/Dev/PM/UX

Running instances by QA/Dev/PM/UX

All instances by product

Running instances by product

Splunking anything on AWS



Splunk App For AWS: DEMO

.conf2016

splunk>

Splunk App For AWS: The Data

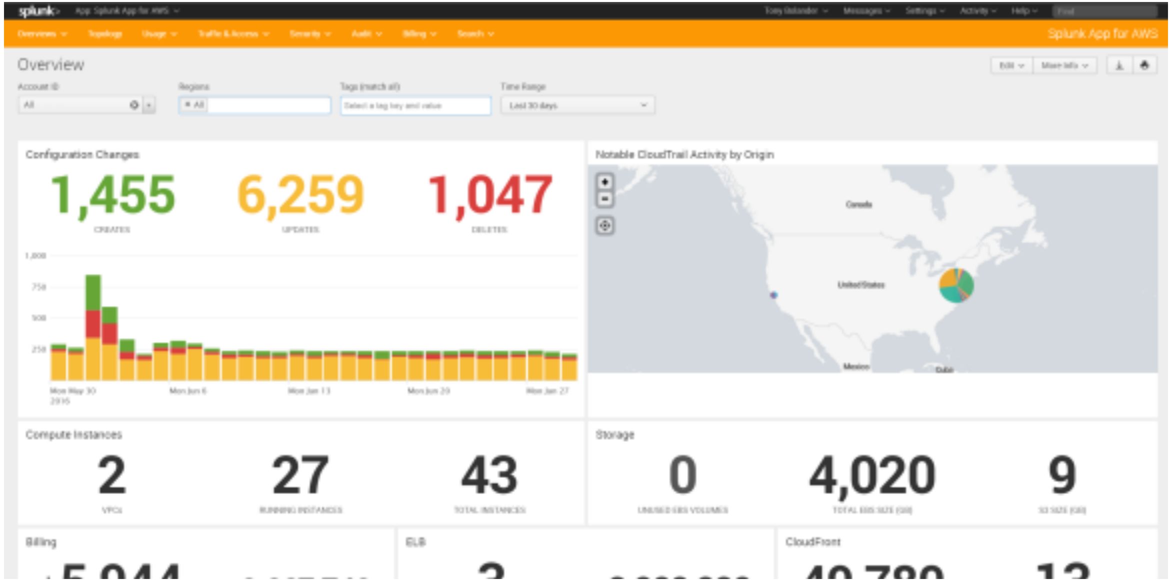
- **AWS Cloudtrail**
  - Service that records AWS API calls for your account and delivers activity logs
  - Provides data to enable security analysis, resource change tracking, compliance auditing, and troubleshooting
- **AWS Config & Config Rules**
  - Service that provides resource inventory, configuration history and configuration change notifications
  - Config Rules enables creation of rules to auto-check AWS configurations
  - Provides data to enable resource discovery, service relationships, change tracking & troubleshooting
- **Amazon Cloudwatch**
  - Service that collects AWS system metrics and log files
  - Offers ability to stream logs via Amazon Kinesis
  - Provides data to enable utilization & health reporting for services such as EC2, EBS, & RDS
- **Amazon Cloudwatch VPC Flow Logs**
  - Service that enables capture of IP traffic information to/from VPC network interfaces
  - Data stored and accessible from AWS Cloudwatch Logs
  - Provides data used to troubleshoot undesired traffic behavior for both operational and security use cases
- **Amazon Inspector**
  - Automated security assessment service to help improve security and compliance of apps on AWS
  - Provides data from knowledge base and security findings based on security best practices
- **AWS Access Logs**
  - **Elastic Load Balancing (ELB)** – Provides data on load balancer requests to anlayze traffic patterns
  - **Cloudfront CDN** – Provides data about every user request received from Cloudfront
  - **S3** – Provides data about a single access request and can be used for security and access audits
- **AWS Billing**
  - Current Month via Cloudwatch metrics
  - Monthly Detailed Billing for Capacity Management

Splunk App For AWS: The Value

- Increase visibility into AWS resource utilization & user activity **across all accounts**
- Ensure adherence to security and compliance standards with audit reporting
- Understand AWS environmental dependencies via interactive topology visualization
- Monitor VPC traffic utilization for additional patterns & security insights
- Cost Optimization through Monthly and Detailed Billing Dashboards

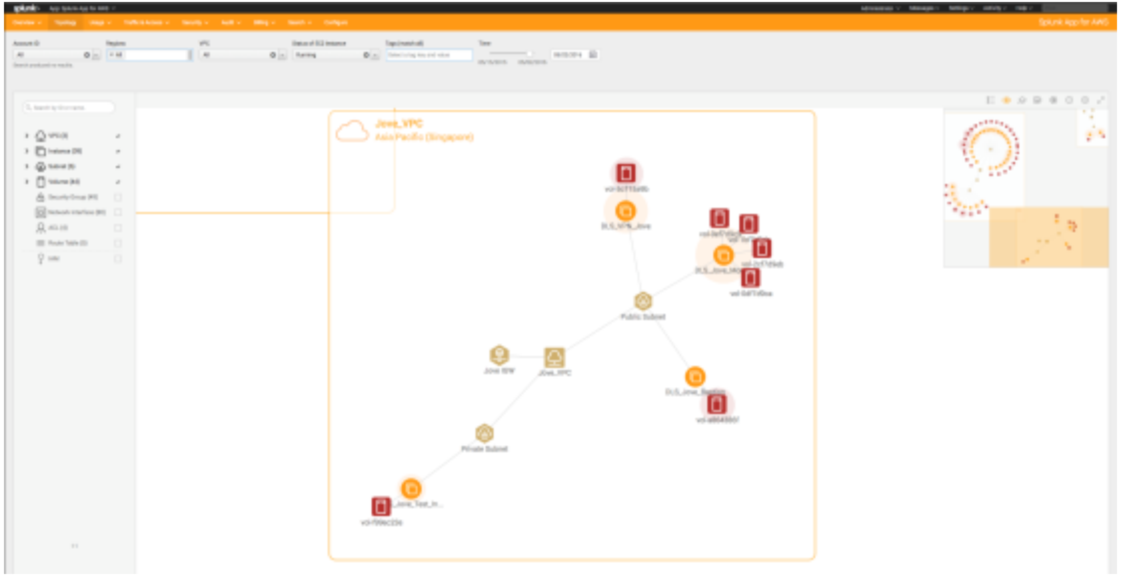
Overview For Splunk App For AWS

- The overview page highlights the following information:
  - Configuration changes
  - Cloudtrail Activity by Origin
  - Compute Instances
  - Storage Instances
  - Monthly Billing
  - ELB Instances
  - Cloudfront Requests
- Drill down to gain additional insights



AWS Topology

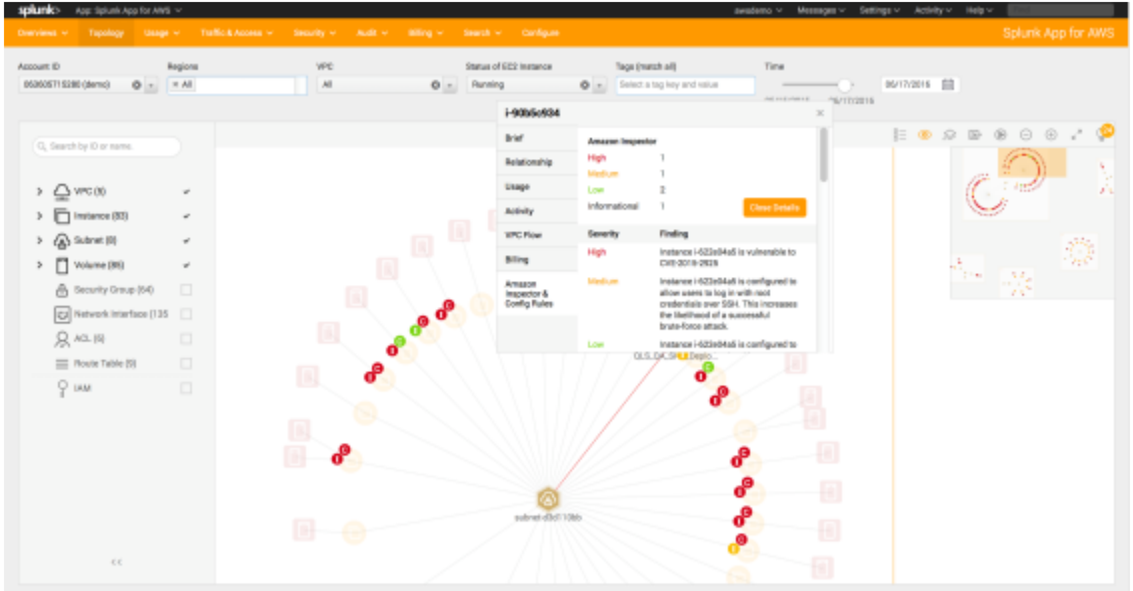
- Topology view gives holistic view of current & historical AWS deployment
- Maps relationships between components
- Clickable layers add visual priority/ severity for key services
- Snapshot topology and/or Playback how environment was built over time



Powered by AWS Config Data

AWS Topology - Expanded Visuals

- Click on resource or apply layers to see correlated data including:
  - Metrics Overview
  - Relationships via Config
  - Resource Usage via Cloudwatch Metrics
  - Audit Activity via Cloudtrail
  - VPC Flow via Cloudwatch Logs
  - Resource Billing
  - Inspector assessment details
  - Config Rules compliance details



i-90b5c934

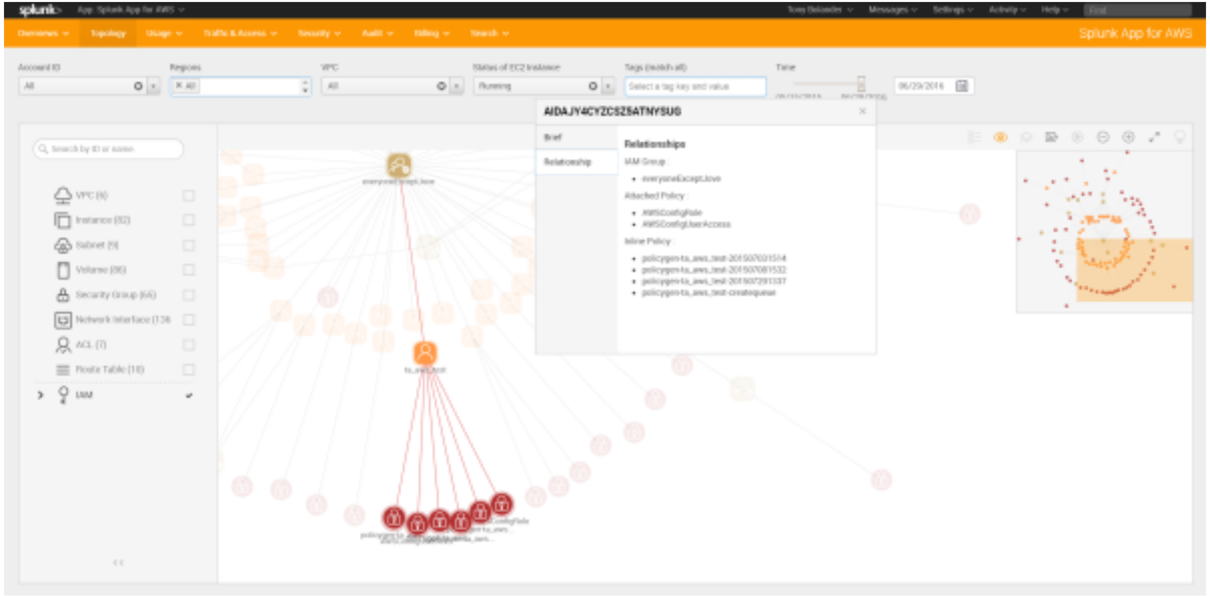
Amazon Inspector

High	1
Medium	1
Low	2
Informational	1

Severity	Finding
High	Instance i-523e04a5 is vulnerable to CVE-2016-2828
Medium	Instance i-523e04a5 is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.
Low	Instance i-523e04a5 is configured to

AWS Topology - IAM

- IAM Topology view uses AWS Config to provide a comprehensive view of Identity and Access Management Information
- Provides visual way to manage IAM Users, Groups and Policies
- Select entity of interest to see IAM relationships



AIDAJY4CYZCSZ5ATNYSUG

Relationships

IAM Group :

- everyoneExceptJove

Attached Policy :

- AWSConfigRole
- AWSConfigUserAccess

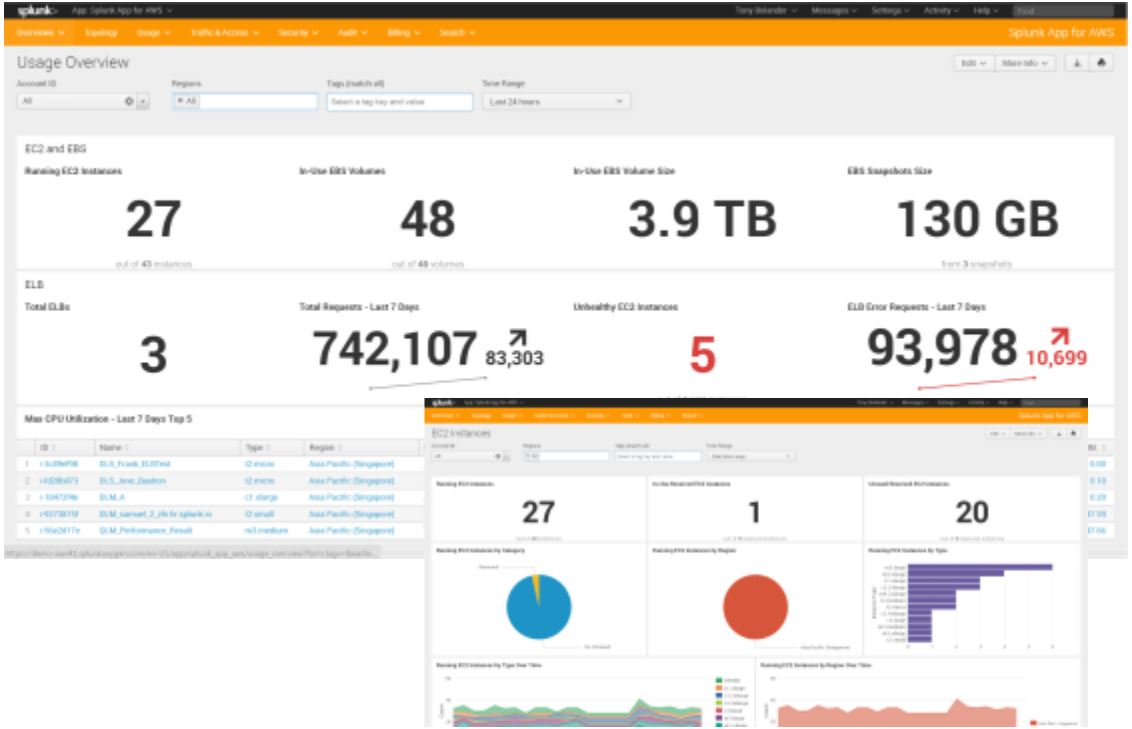
Inline Policy :

- policygen-ta_aws_test-201507031514
- policygen-ta_aws_test-201507081532
- policygen-ta_aws_test-201507291337
- policygen-ta_aws_test-createqueue

Powered by AWS Config Data

Amazon EC2 & EBS Usage Overview

- In one glance, review your EC2 usage and EBS Volume details
- Click through dashboards for details on individual EC2 instances and EBS Volumes
- Drill down further into raw search and original metrics



Usage Overview

Account ID: All
Regions: All
Tags (match all): Select a tag key and value
Time Range: Last 24 hours

EC2 and EBS

Running EC2 Instances: 27 (out of 43 instances)

In-Use EBS Volumes: 48 (out of 48 volumes)

In-Use EBS Volume Size: 3.9 TB

EBS Snapshots Size: 130 GB (from 3 snapshots)

ELB

Total ELBs: 3

Total Requests - Last 7 Days: 742,107 ↗ 83,303

Unhealthy EC2 Instances: 5

ELB Error Requests - Last 7 Days: 93,978 ↗ 10,699

Max CPU Utilization - Last 7 Days Top 5

	ID	Name	Type	Region
1	[illegible]	DLS_Frank_ELBTest	t2.micro	Asia Pacific (Singapore)
2	[illegible]	DLS_Jane_Daston	t2.micro	Asia Pacific (Singapore)
3	[illegible]	DLM_A	c1.xlarge	Asia Pacific (Singapore)
4	[illegible]	DLM_samuel_2_ubi hr splunk.io	t2.small	Asia Pacific (Singapore)
5	[illegible]	DLM_Performance_Result	m3.medium	Asia Pacific (Singapore)

EC2 Instances

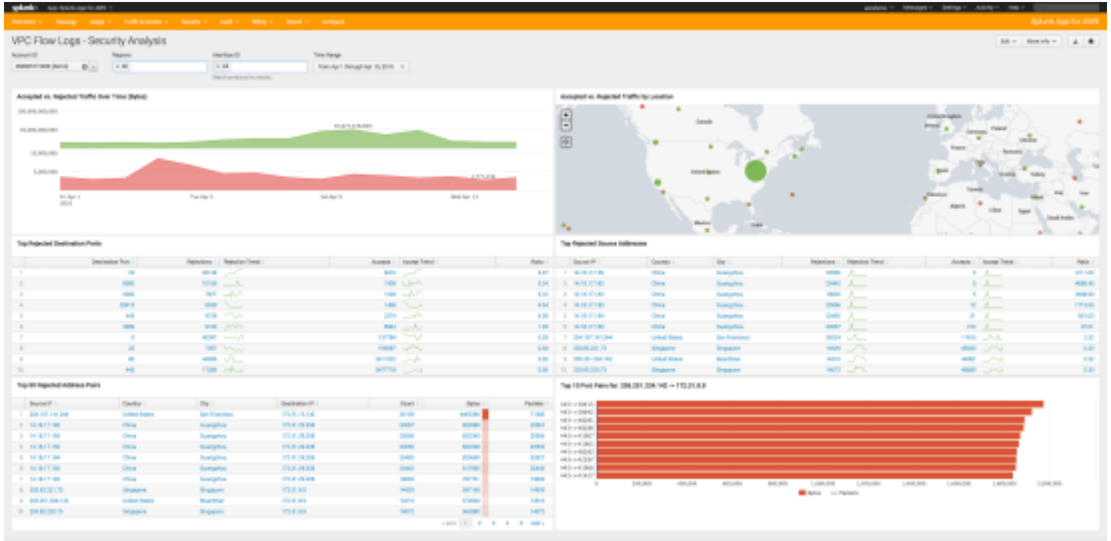
Running EC2 Instances: 27

1

20

Amazon VPC Flow Data – Traffic & Security

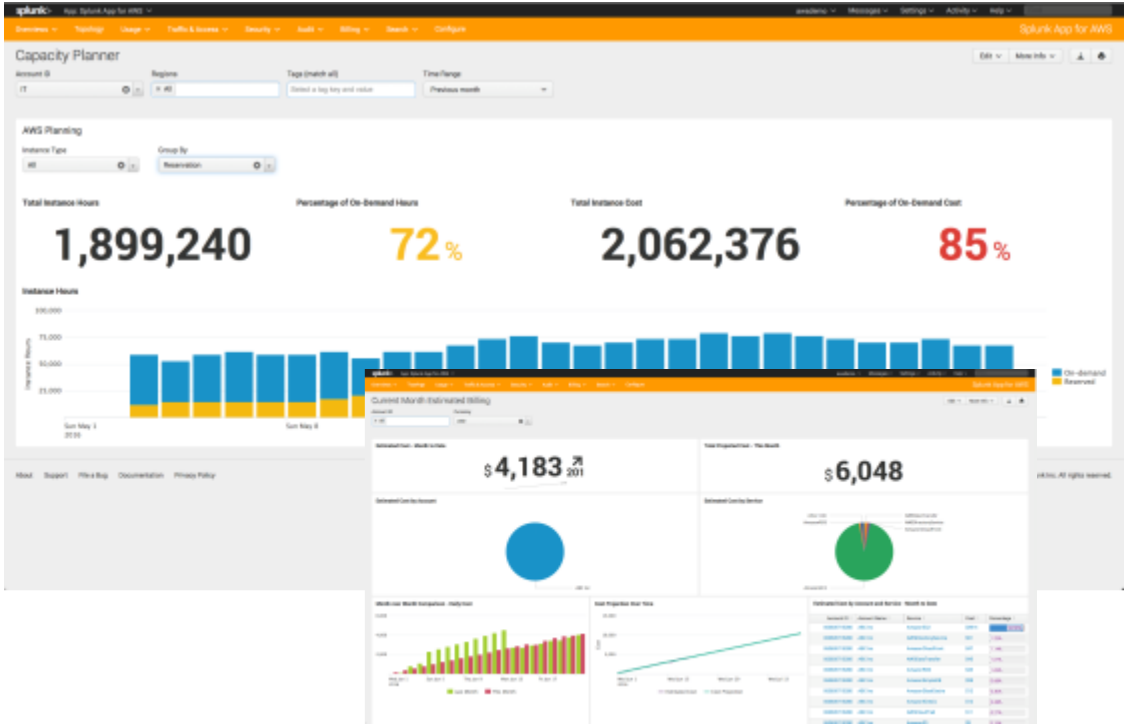
- Utilizes VPC Flow Logs for Security & Traffic Analysis
- Drill down into rejected vs. accepted traffic by source location
- See top source / destination and IP Addresses and ports
- Visualize VPC traffic by interface, time, and location



VPC Flow Logs - Security Analysis

AWS Billing & Capacity Planning

- Month-to-Date billing and End-of-Month projections
- Detailed Historical Billing Dashboard available using Monthly AWS Detailed billing reports
- Capacity Planner gives additional clarity on AWS On-Demand vs Reserved Instance spend



Capacity Planner

Account ID: IT

Regions: × All

Tags (match all): Select a tag key and value

Time Range: Previous month

AWS Planning

Instance Type: All

Group By: Reservation

Total Instance Hours: 1,899,240

Percentage of On-Demand Hours: 72 %

Total Instance Cost: 2,062,376

Percentage of On-Demand Cost: 85 %

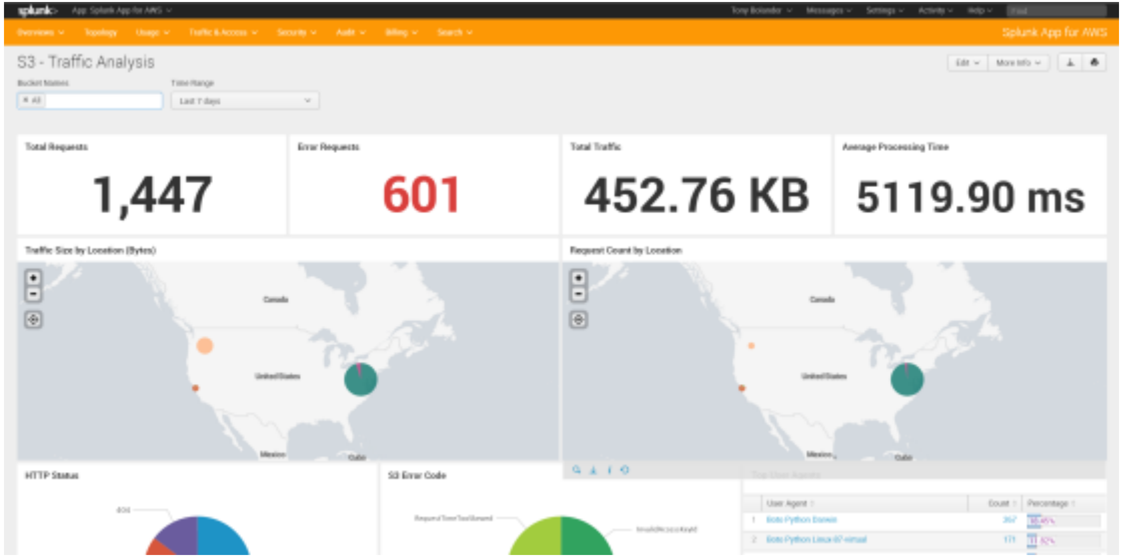
Current Month Estimated Billing

$4,183 201

$6,048

Amazon S3 Access

- Utilizes S3 Access logs to provide visibility on the health, requests, and traffic volume handled by S3 bucket objects
- Aggregations by requester, user-agent, and error codes
- Provides insights for troubleshooting, security and general product/business analytics.



S3 - Traffic Analysis

Bucket Names: × All

Time Range: Last 7 days

Total Requests: 1,447

Error Requests: 601

Total Traffic: 452.76 KB

Average Processing Time: 5119.90 ms

Traffic Size by Location (Bytes)

Request Count by Location

HTTP Status

S3 Error Code

RequestTimeTooSkewed

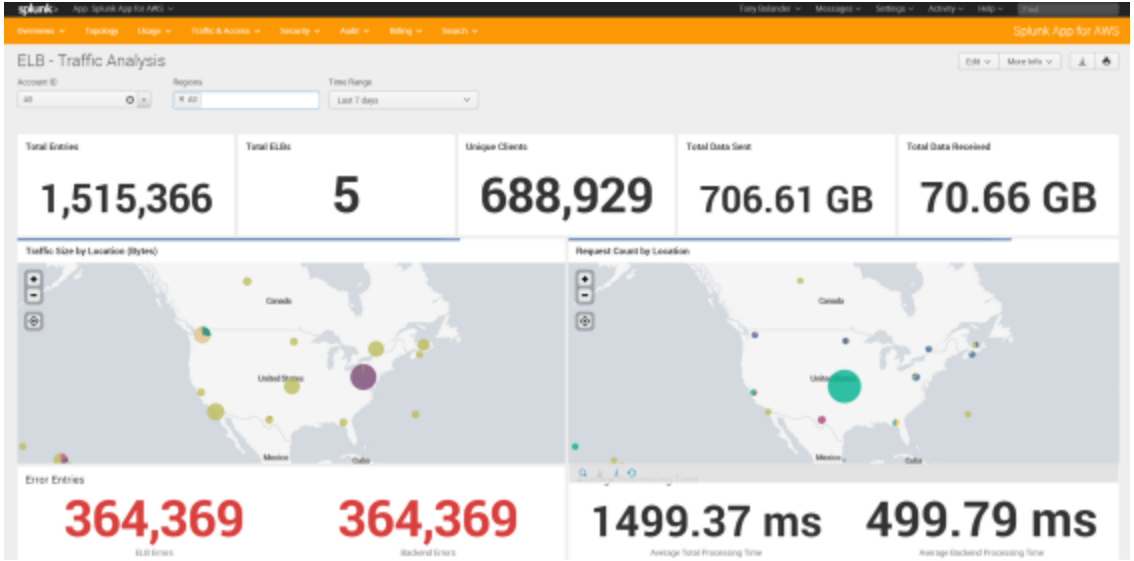
InvalidAccessKeyId

Top User Agents

	User Agent	Count	Percentage
1	Boto Python Darwin	367	[illegible]
2	Boto Python Linux-97-virtual	171	11.82%

AWS Elastic Load Balancer

- Utilizes ELB access logs to provide visibility on ELB health, latency and request volume
- Client and server side errors are surfaced (HTTP 4XX-5XX errors) by account and region



ELB - Traffic Analysis

Account ID: All

Regions: All

Time Range: Last 7 days

Total Entries: 1,515,366

Total ELBs: 5

Unique Clients: 688,929

Total Data Sent: 706.61 GB

Total Data Received: 70.66 GB

Traffic Size by Location (Bytes)

Request Count by Location

Error Entries

364,369 ELB Errors

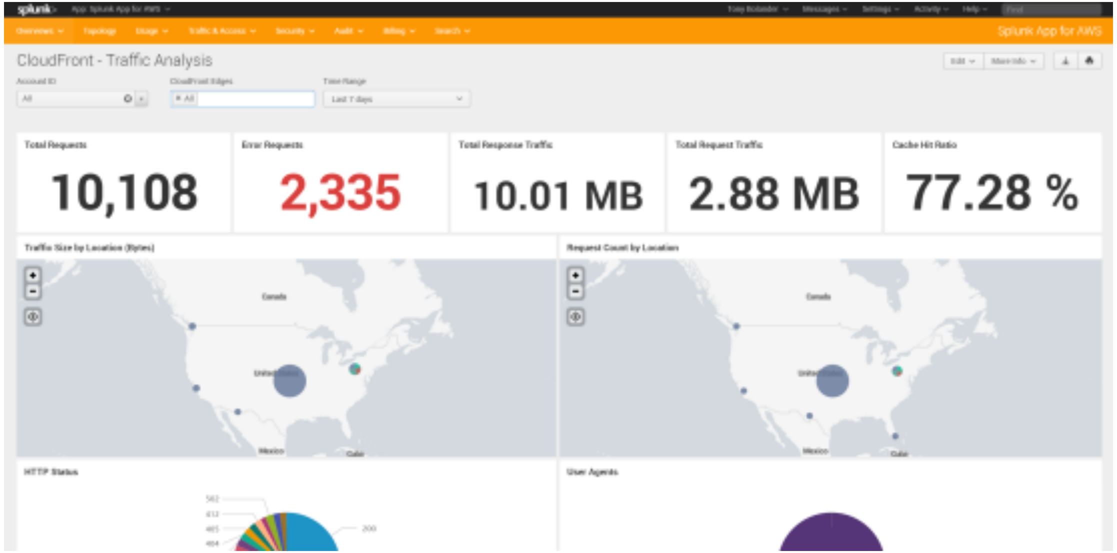
364,369 Backend Errors

1499.37 ms Average Total Processing Time

499.79 ms Average Backend Processing Time

Amazon Cloudfront CDN

- Utilizes Cloudfront access logs to display visitor information per edge location, referrers, cache hits/misses and traffic volume
- Provides operational utility by adding visibility to errors, latency, distribution
- Provides business insights such as geo location of visitors, user agents and referrers



CloudFront - Traffic Analysis

Account ID: All

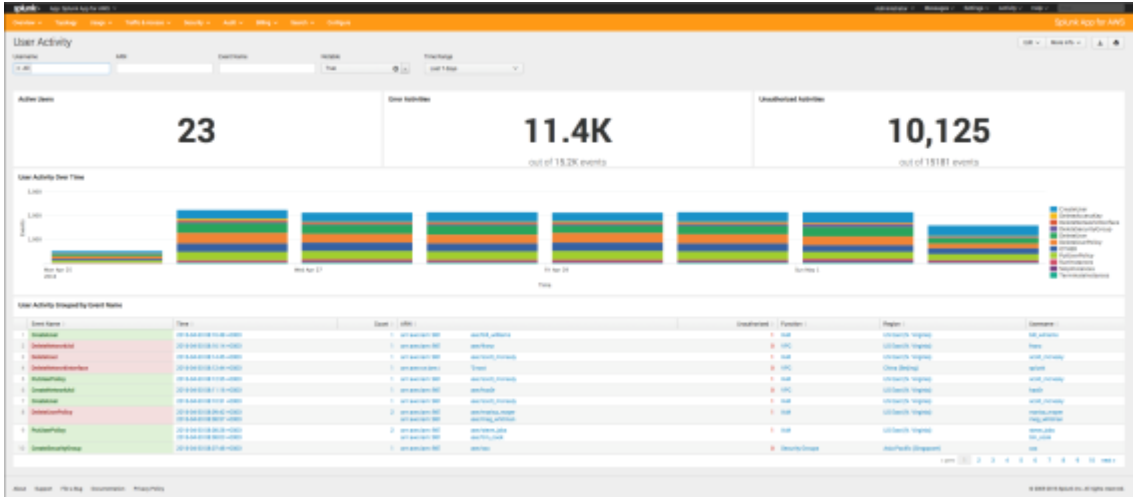
CloudFront Edges: All

Time Range: Last 7 days

Total Requests	Error Requests	Total Response Traffic	Total Request Traffic	Cache Hit Ratio
10,108	2,335	10.01 MB	2.88 MB	77.28 %

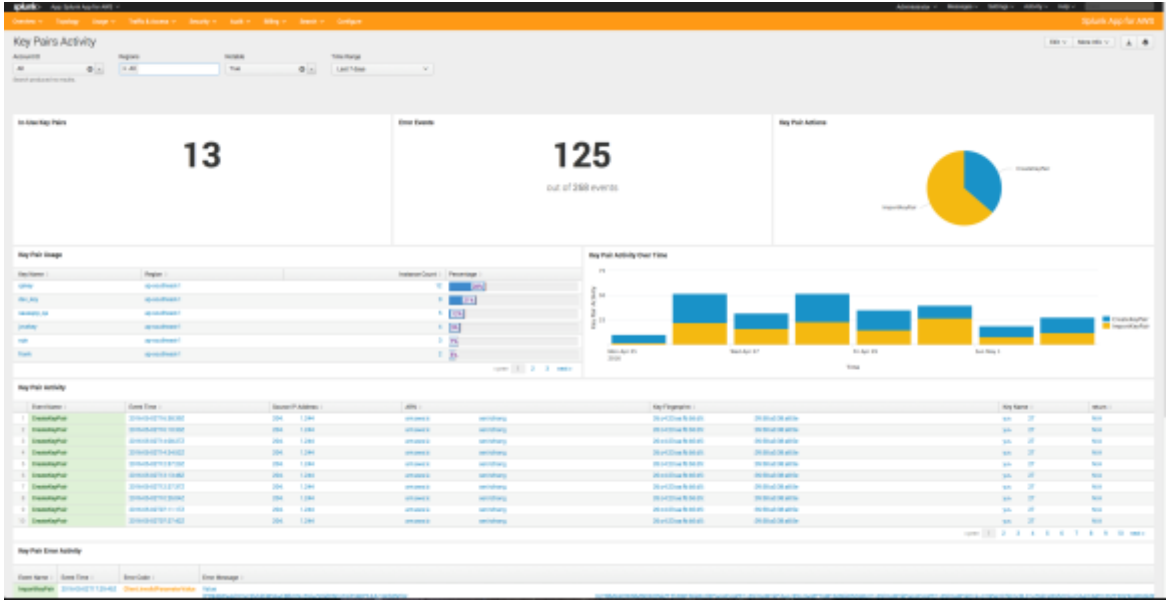
AWS User & IAM Activity

- Utilizes Cloudtrail data to quickly see the number of active users logged into the system
- Get alerted on Unauthorized user activities and create additional alerts for any user action
- See what ARN's are being used to access services and the correlated functions



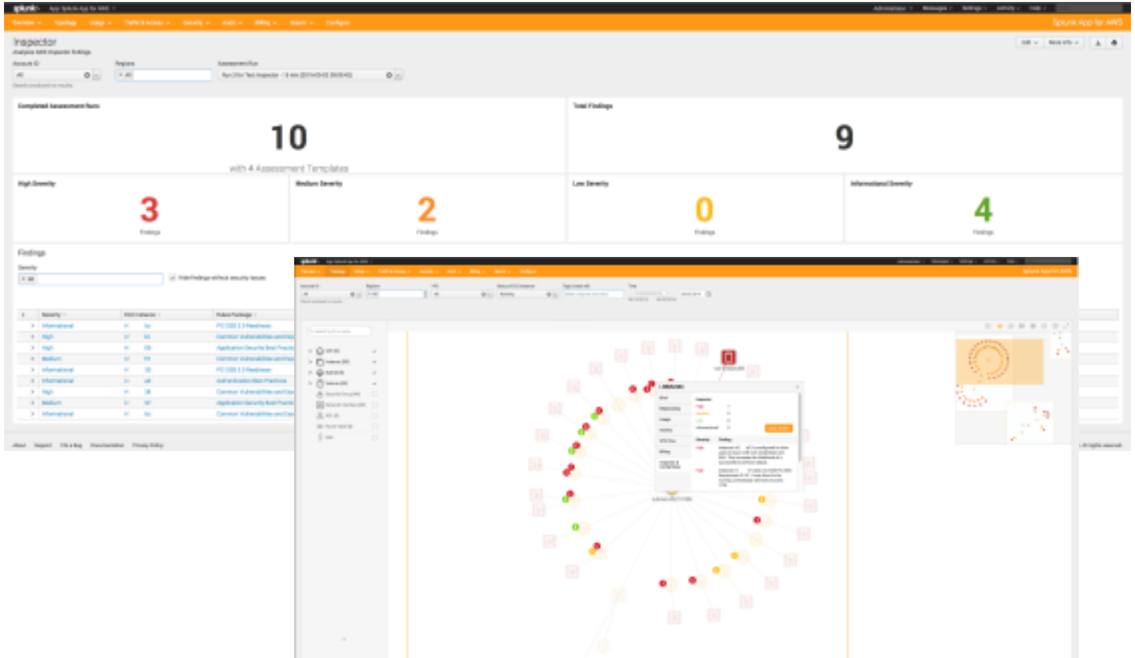
AWS Key Pairs Activity

- Utilizes Cloudtrail data to quickly see number of In-Use Key Pairs, Error events and actions
- Reports on Key Pair usage by Region and activity over time



Amazon Inspector

- Utilizes Amazon Inspector findings to present comprehensive dashboard
- Findings are also overlaid on AWS resource based on severity



Inspector

Completed Assessment Runs

10

with 4 Assessment Templates

Total Findings

9

High Severity

3

Findings

Medium Severity

2

Findings

Low Severity

0

Findings

Informational Severity

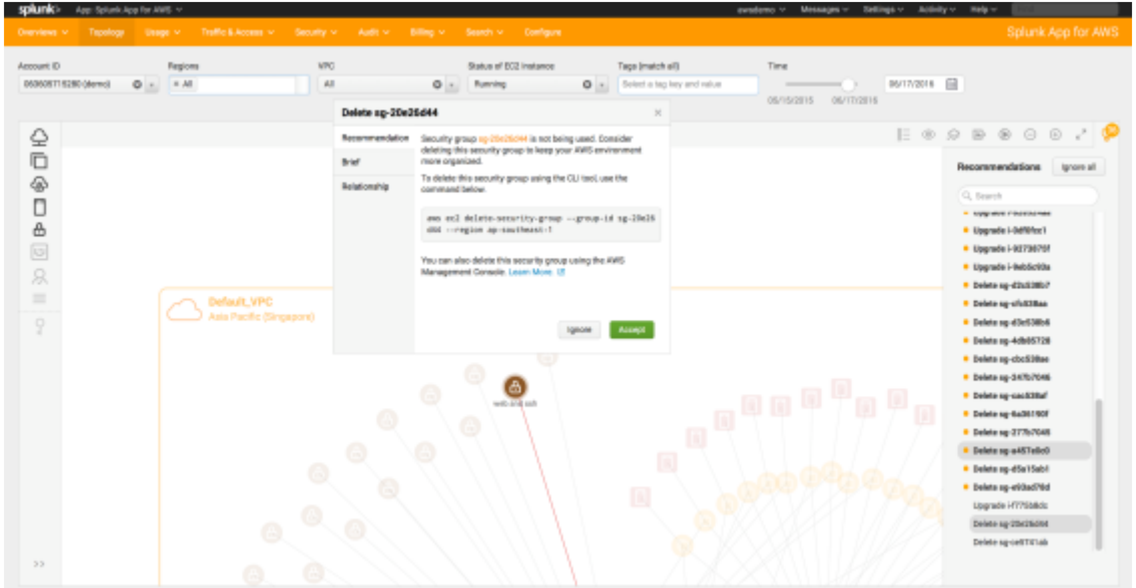
4

Findings

Findings

Recommendation Engine (Preview)

- Utilizes correlated data and machine learning to make resource recommendations
- Preview recommendations shipped in v4.2 include
  - Upgrade EC2 instance
  - Downgrade EC2 instance
  - Delete Security Group



Delete sg-20e26d44

Recommendation

Brief

Relationship

Security group sg-20e26d44 is not being used. Consider deleting this security group to keep your AWS environment more organized.

To delete this security group using the CLI tool, use the command below.

```
aws ec2 delete-security-group --group-id sg-20e26
d44 --region ap-southeast-1
```

You can also delete this security group using the AWS Management Console. Learn More

Ignore Accept

Getting Started

- Create a Splunk account using your Amazon email: https://www.splunk.com/page/sign_up
- Access and set up on your own EC2 instance via a Cloudformation template by following these directions. This environment will include the Splunk App for AWS to easily visualize for Config, Cloudtrail, Cloudwatch Metrics, VPC Flow Logging, S3, and Billing

  or

  Download Splunk>Enterprise for your laptop and then set-up the Splunk App for AWS & AWS Technology Add-On to easily visualize for Config, Cloudtrail, Cloudwatch Metrics, VPC Flog Logging, S3, and Billing
- For personal demos requiring a larger license please aws-info@splunk.com to request for **Not-For-Resale** License or request access to AWS EC2 environment available through David Potes (potesd@amazon.com)
- Be sure to take 4.5 hour self-paced Using Splunk tutorial + Review Splunk>Docs and Splunk>Apps for more

THANK YOU

.conf2016

splunk>