How REI Uses Intelligent Threat Detection and Edge Protection on AWS with Splunk

Rohit Pujari | Partner Solutions Architect, Amazon Web Services
Jae Lee | Product Marketing – Security Markets, Splunk
Wissam Ali-Ahmad | Technical Lead – Global Strategic Alliances, Technical Services, Splunk
David Bell | Manager – Infrastructure Cloud Services, REI
Rick Adams | Senior Systems Engineer, REI

September 11, 2018

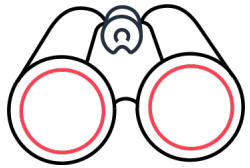
Forward-Looking Statements

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 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.

splunk> .conf18

Why is Security Traditionally so Hard?



Lack of
visibility

Low degree
of automation

The Most Sensitive Workloads Run on AWS

"We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance."

— John Brady, CISO, FINRA (Financial Industry Regulatory Authority)

"The fact that we can rely on the AWS security posture to boost our own security is really important for our business. AWS does a much better job at security than we could ever do running a cage in a data center."

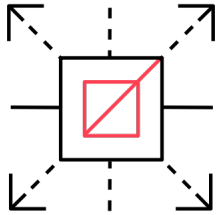
— Richard Crowley, Director of Operations, Slack

"With AWS, DNAnexus enables enterprises worldwide to perform genomic analysis and clinical studies in a secure and compliant environment at a scale not previously possible."

— Richard Daly, CEO DNAnexus

Move to AWS to Strengthen your Security Posture

Inherit global security
and compliance controls



Scale with superior
visibility and control

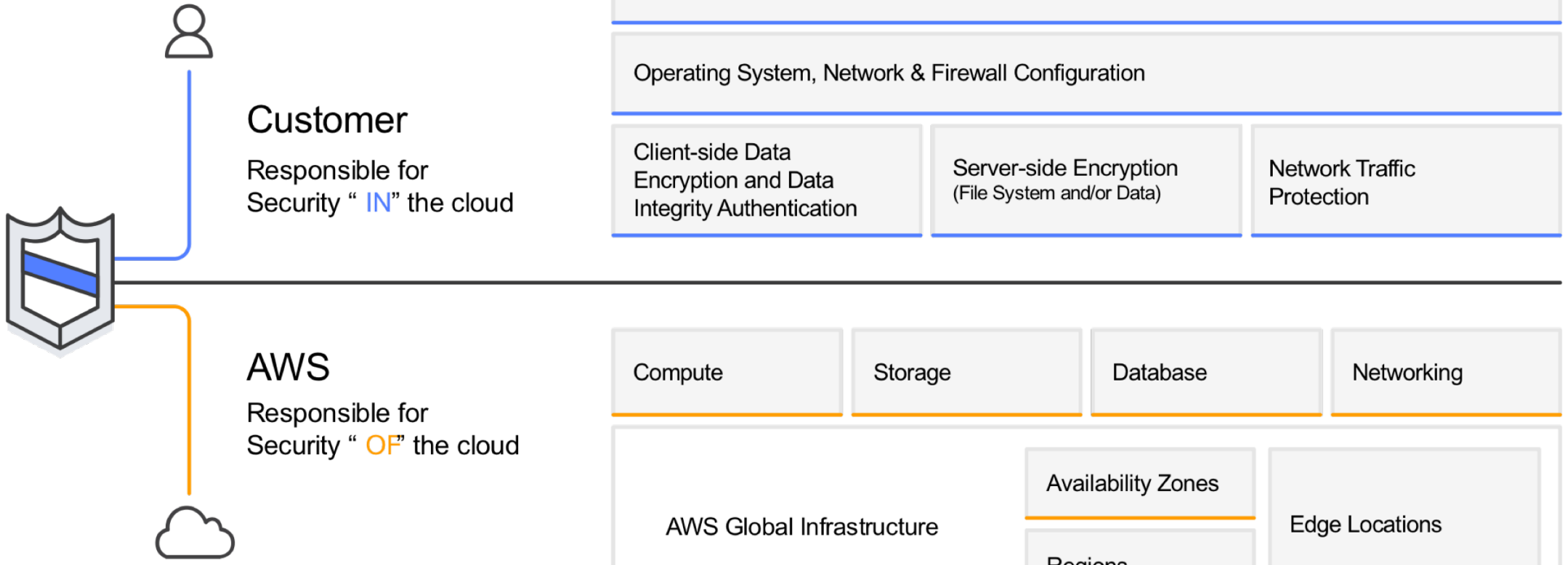
Highest standards for
privacy and data security

Automate with deeply
integrated security services

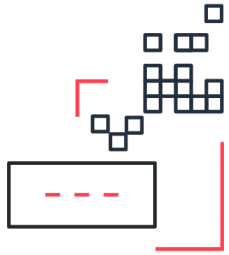
Largest network of security
partners and solutions

Inherit Global Security and Compliance Controls

Shared Security Responsibility



Highest Standards for Privacy

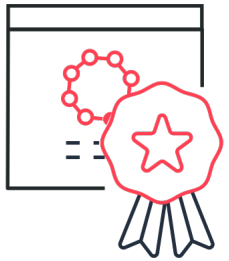


Meet data residency requirements

Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so.

Encryption at scale

Use keys managed by our AWS Key Management Service (KMS) or mange your own encryption keys with Cloud HSM using FIPS validated cryptography systems.



Comply with local data privacy laws

Control who can access content, its lifecycle, and disposal.

Access services and tools

Build compliant infrastructure on top of AWS.

End-to-End Security Visibility with Splunk

Jae Lee, Product Marketing | Security Markets, Splunk
Wissam Ali-Ahmad | Technical Lead – Global Strategic Alliances, Technical Services, Splunk

splunk> .conf18

Splunk and AWS Partnership

AWS re:Invent 2014 Keynote

“Splunk enables organizations to move to the cloud with confidence.”

“Splunk is all-in on AWS.”

Godfrey Sullivan, Splunk Chairman (formerly CEO)

CEO-CEO video: June 2016

“Our partnership with Splunk is incredibly important for our customers.”

“Customers love AWS agility with Splunk visibility.”

Andy Jassy, CEO, AWS

“AWS is at the heart of our cloud strategy.”

Doug Merritt, CEO, Splunk

AWS SF Summit Keynote: April 2017

“Like AWS, Splunk is customer obsessed. It is literally our number one company priority. Customer obsession makes partner alignment with AWS easy.

“It has never been easier to get centralized visibility across the cloud, hybrid, and on-prem environments.”

Doug Merritt, CEO, Splunk

splunk> .conf18

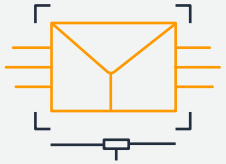
Thousands of Global Security Customers

splunk> .conf18

Costs of Data Breaches

(Global average costs per breach)

Detection + Escalation
(Global: $0.99M)



Notification
(Global: $0.19M)

Post-Breach Response
(Global: $0.93M)

Lost Business
(Global: $1.51M)

Average total cost of data breach
Global: $3.62M

Source: Ponemon Inst. 2017 Cost of Data Breach Study – United States and 2017 Cost of Data Breach Study - Global

splunk> .conf18

Splunk's Approach to AWS Migration

AWS Migration

Get visibility at all stages of the migration process – before, during and after.

Baseline performance and cost metrics.

Manage Hybrid Infrastructure

Hybrid infrastructure creates a complex monitoring environment. Splunk enables you to keep up.

One Consolidated Solution

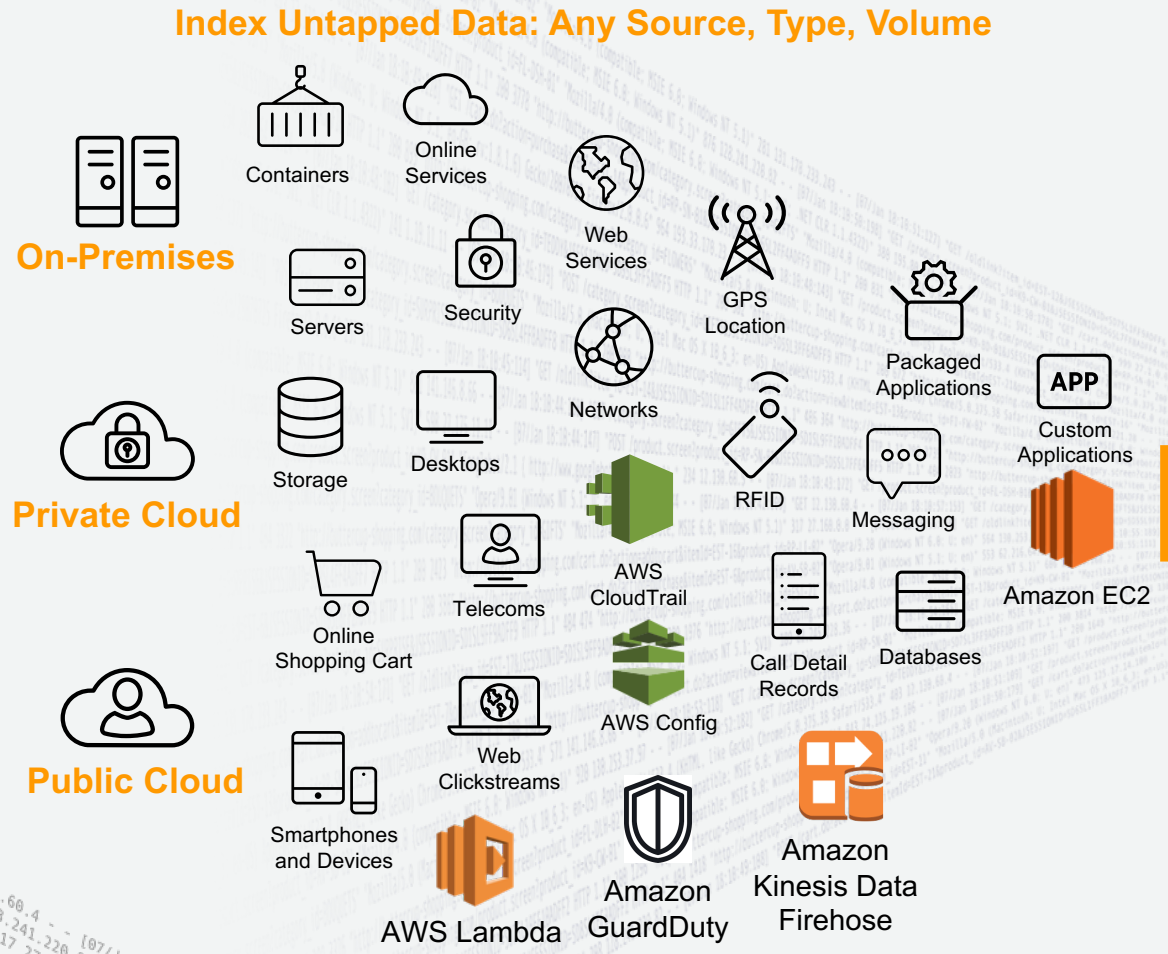
Manage security and IT Ops.

Monitor service-level down to system-level in a single view.

Cost, Capacity and Resource Management

Understand how resources are performing – measure against baselines – then optimize utilization and billing.

Splunk and AWS



AWS App & Add-on

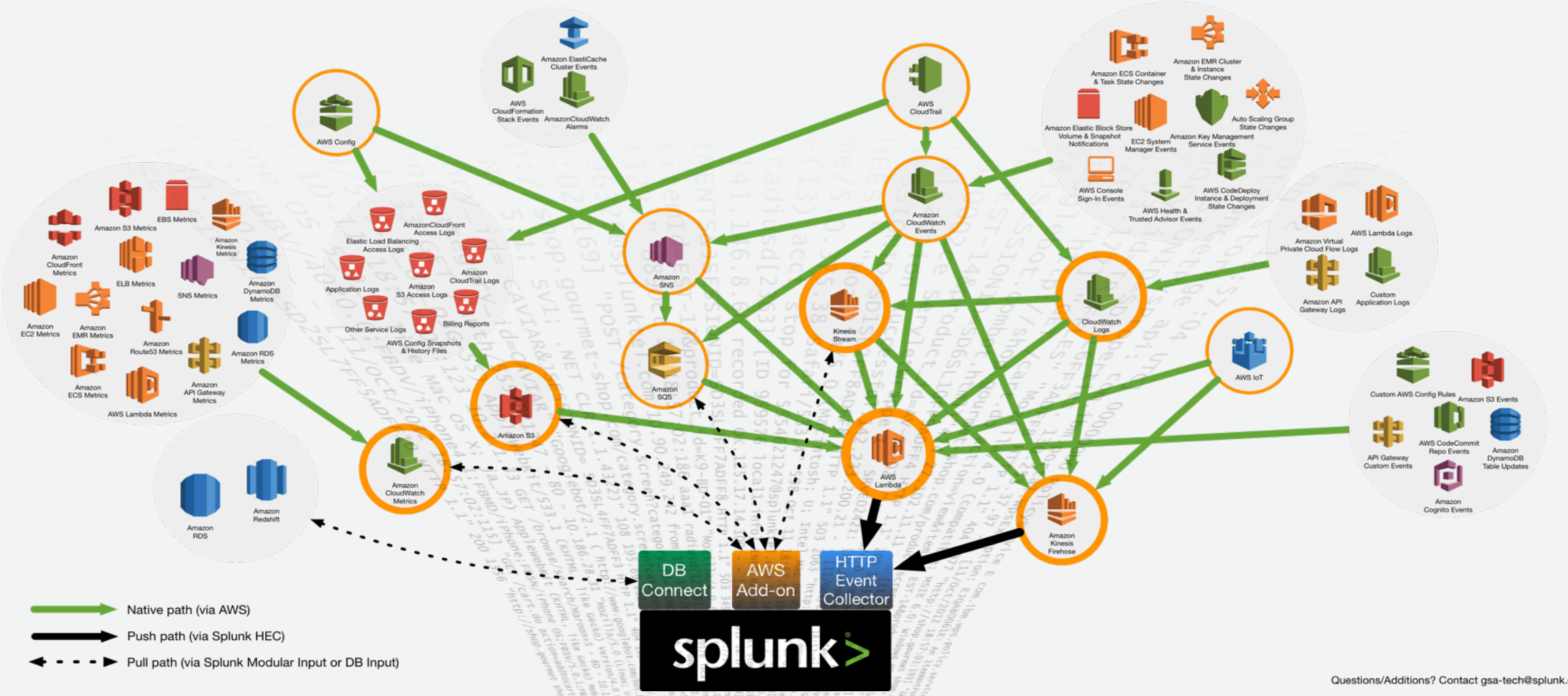
Real-Time Machine Data

splunk>

References – Coded fields, mappings, aliases
Dynamic information – Stored in non-traditional formats
Environmental context – Human maintained files, documents
System/application – Available only using application request
Intelligence/analytics – Indicators, anomaly, research, white/blacklist

splunk> .conf18

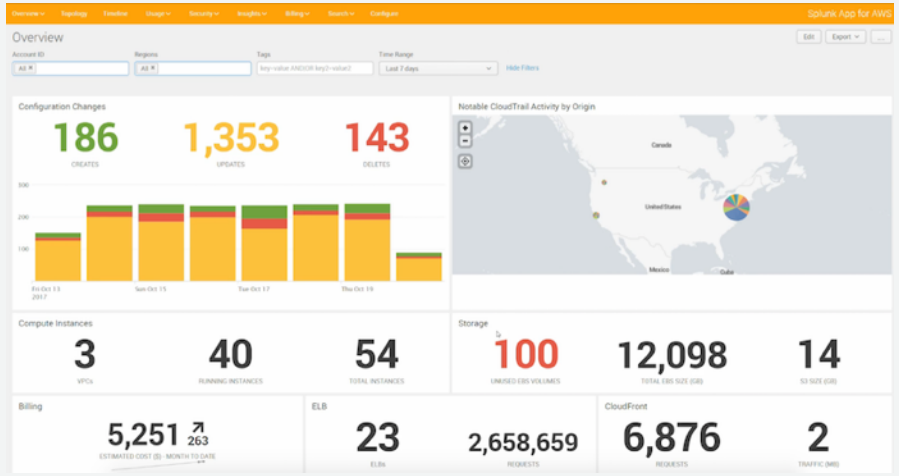
End State: Comprehensive AWS Visibility

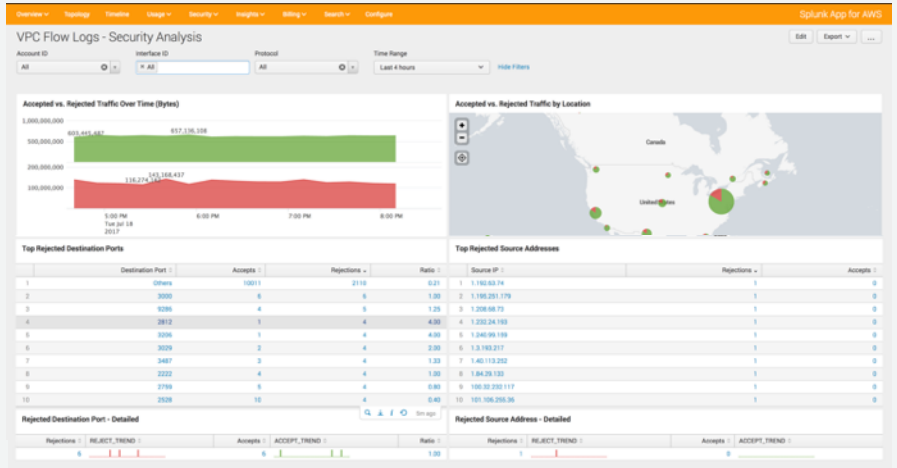


Questions/Additions? Contact gsa-tech@splunk.com

splunk> .conf18

Example Investigative Methods

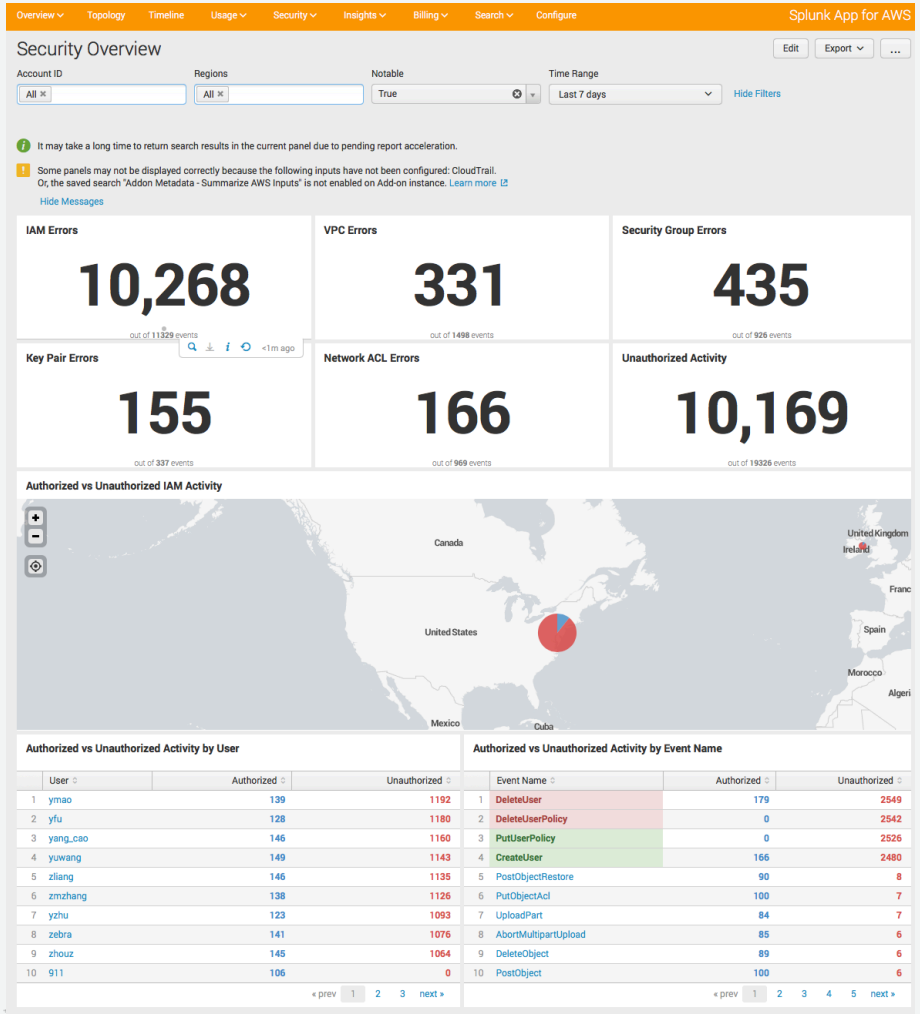




- Splunk App for AWS

- 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 an 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?

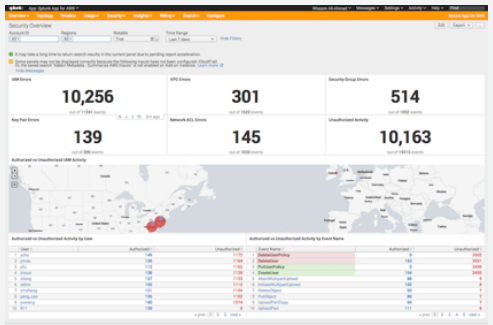
Examples: Basic Posture Methods



- Sudden change in the number of security group rules?
- Sudden change in the number of ACL modifications?
- Spike in error activity caused by unauthorized actions?
- Are there any publicly accessible Amazon S3 buckets?
- Any provisioning activity from an unusual country?
- API calls from users who have not made API calls before?
- First time a user provisioned an instance / account / etc.?

Splunk App & Add-on for AWS

App



Splunk Enterprise Security™

Add-on

Access

Anomaly

Amazon CloudWatch

AWS Config

Amazon S3

Adaptive Response

splunk> **Platform for Operational Intelligence**

aws

- Amazon S3
- Amazon EC2
- AWS CloudTrail
- AWS IAM
- Amazon CloudWatch
- AWS Config
- Amazon Kinesis
- AWS Lambda

splunk> .conf18

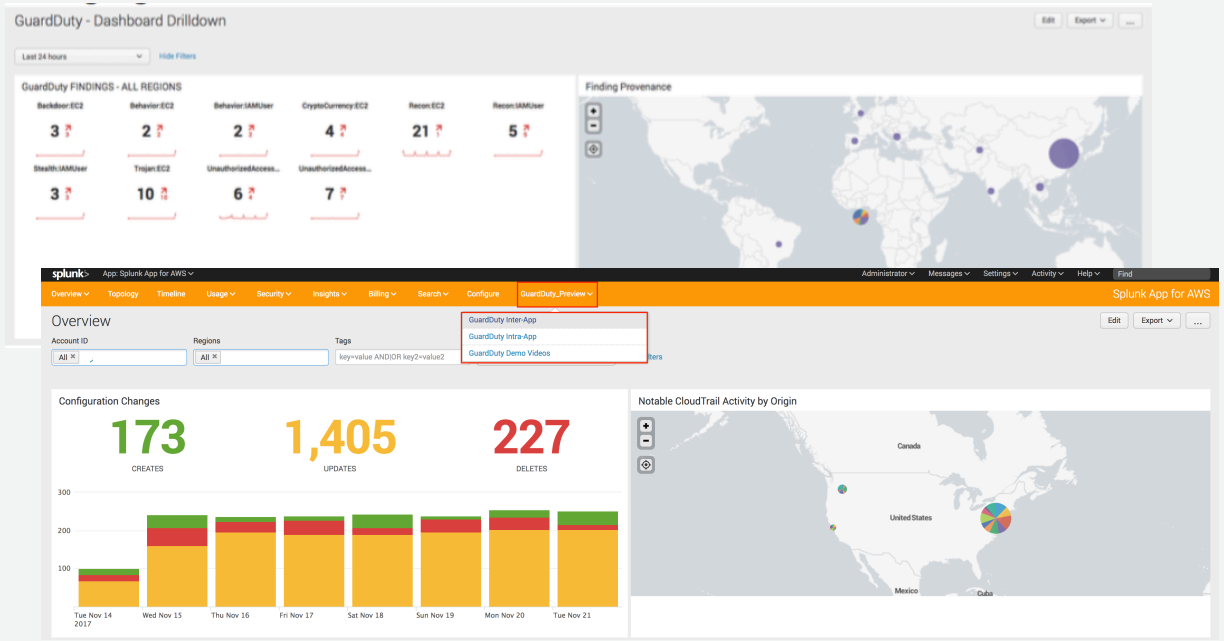
Amazon GuardDuty Add-on for Splunk

Amazon GuardDuty

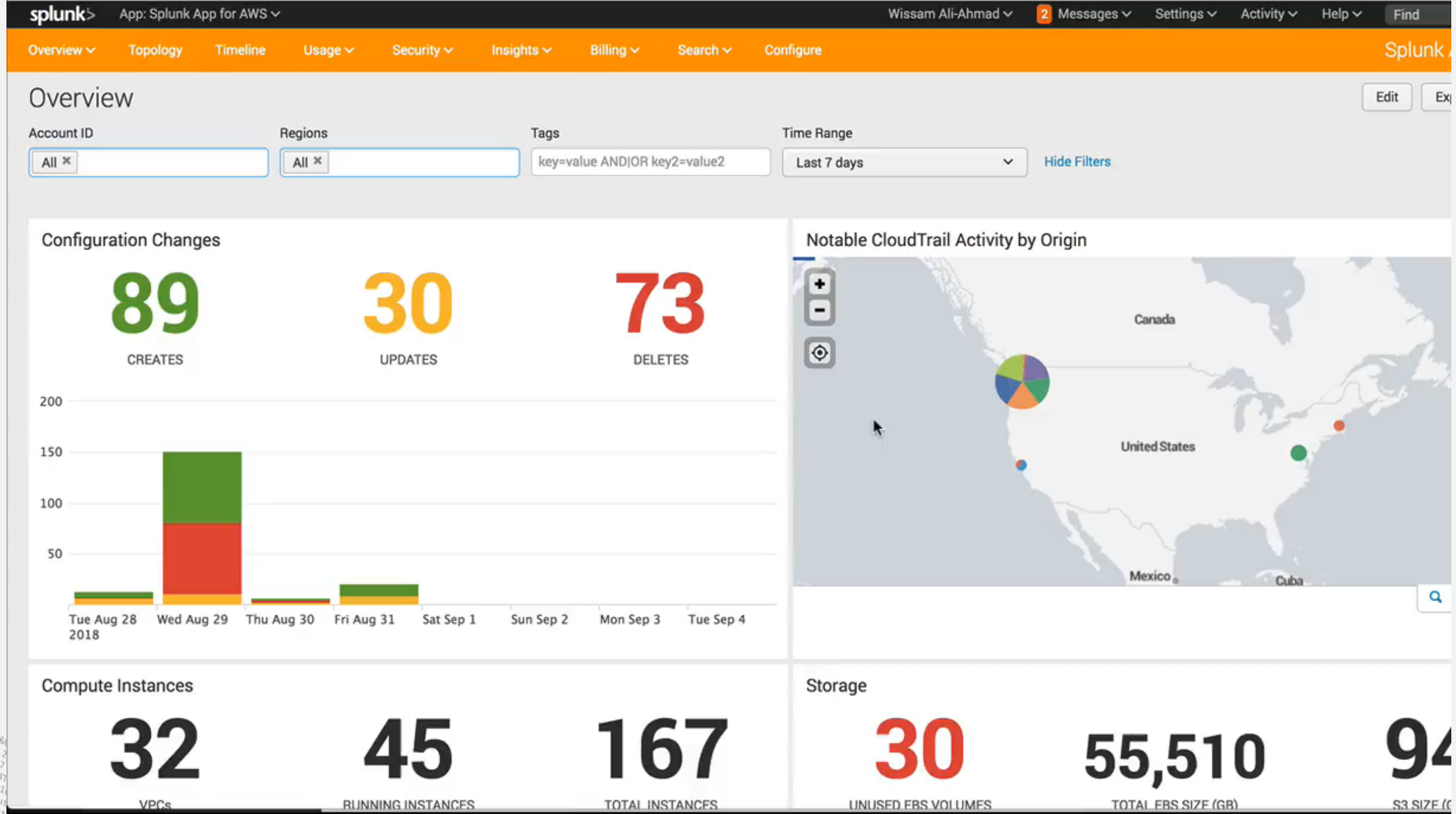
- Provides intelligent alerting on potentially malicious activity based on VPC flow logs + AWS CloudTrail data

Amazon GuardDuty Add-on for Splunk

- Prioritizes analyst time and investigations with aggregated alerts and correlation across availability zones
- Speeds response with additional context and data to fully scope and remediate



Video: How to configure Amazon GuardDuty events for Splunk
https://youtu.be/wlPfzUZMS6E?t=20s

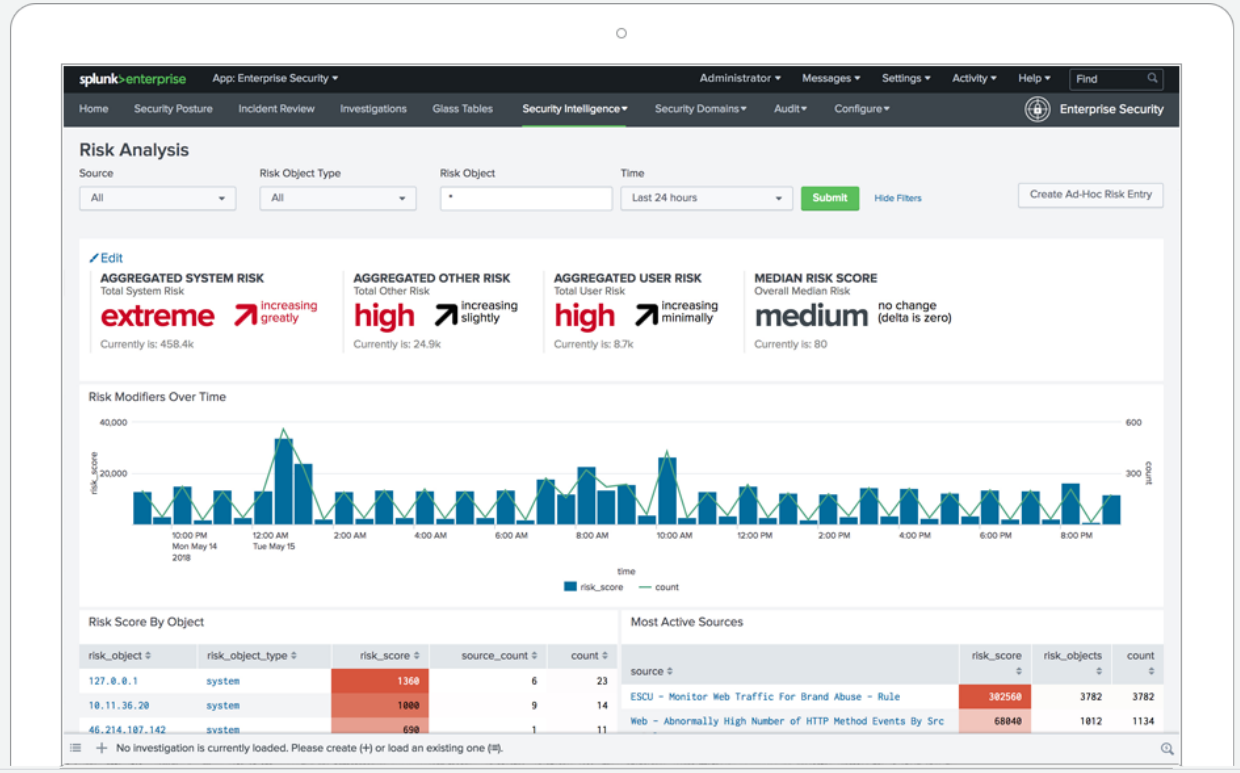

splunk> App: Splunk App for AWS
Wissam Ali-Ahmad
2 Messages
Settings
Activity
Help
Find
Overview
Topology
Timeline
Usage
Security
Insights
Billing
Search
Configure
Splunk
Overview
Edit
Account ID
All
Regions
All
Tags
key=value AND|OR key2=value2
Time Range
Last 7 days
Hide Filters
Configuration Changes
89
CREATES
30
UPDATES
73
DELETES
200
150
100
50
Tue Aug 28 2018
Wed Aug 29
Thu Aug 30
Fri Aug 31
Sat Sep 1
Sun Sep 2
Mon Sep 3
Tue Sep 4
Notable CloudTrail Activity by Origin
Canada
United States
Mexico
Cuba
Compute Instances
32
VPCs
45
RUNNING INSTANCES
167
TOTAL INSTANCES
Storage
30
UNUSED EBS VOLUMES
55,510
TOTAL EBS SIZE (GB)
94

Analytics-driven Security Investigation and Event Management (SIEM)

Splunk Enterprise Security (ES)

Combat threats with actionable intelligence and advanced analytics:

- Reduce time to detect
- Streamline investigations
- Respond rapidly



splunk> .conf18

AWS Serverless Repository

AWS Lambda blueprints for Splunk:

- 7 different Serverless Applications designed to help AWS customers easily send AWS data at scale to Splunk for further analysis and insights

AWS Adaptive Response (AR) action for Splunk:

- Serverless Applications for automated incident response and remediation for AWS triggered by Splunk analytics

https://github.com/splunk/splunk-aws-lambda-blueprints

Adaptive Responses:

Response	Mode	Time	User	Status
Stop performed on instance	lambda	2017-09-20T12:19:18-0700	system	✓ success
Instance snapshot/s complete	lambda	2017-09-20T12:18:34-0700	system	✓ success
Stop action started on instance	lambda	2017-09-20T12:18:34-0700	system	✓ success
Action request email sent	lambda	2017-09-20T12:18:03-0700	system	✓ success
Instance added to SSH only security group	lambda	2017-09-20T12:17:56-0700	system	✓ success
Instance snapshot/s (backup) started	lambda	2017-09-20T12:17:56-0700	system	✓ success
Instance tagged as 'Flagged by Splunk'	lambda	2017-09-20T12:17:54-0700	system	✓ success
step_function_snap	adhoc	2017-09-20T12:17:46-0700	system	✓ success
Notable	saved	2017-09-20T12:00:21-0700	nic	✓ success

Splunk is Available in AWS Marketplace

Options for Splunk Cloud & Splunk Enterprise

AWS Marketplace Ease of Sale

- Easily discover & deploy software & SaaS
- **Simplified buying process** and consolidated AWS Billing reduces time to procure
- **Automatic renewals**
- One consolidated AWS bill
- Potential impact and “draw-down” on AWS **EDP (Enterprise Discount Program) Contracts**

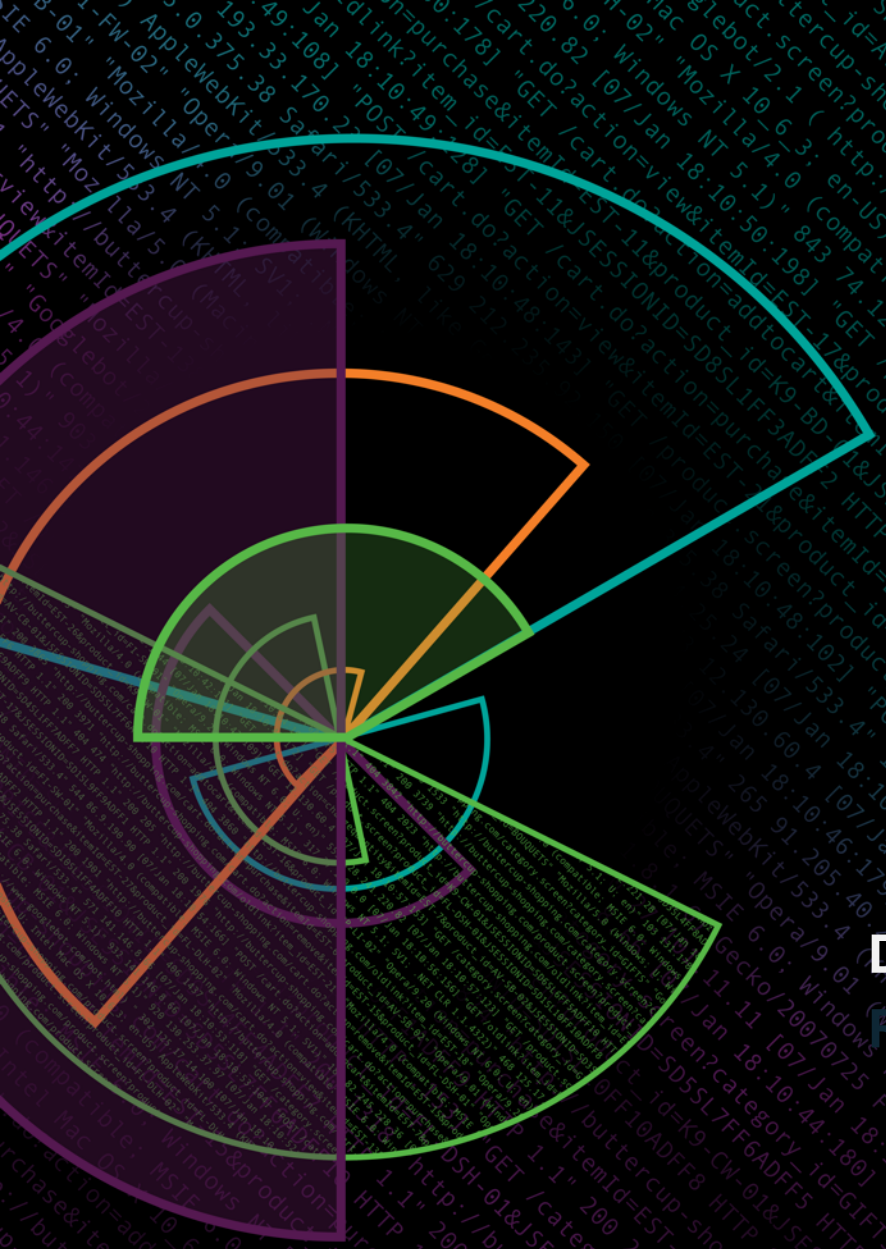
Explore AWS Marketplace

Splunk Specifics

- Annual contract subscriptions & automatic discount for multi-annual options
- Buy Splunk Cloud in **increments of 5GB to 100GB** across all supported regions
- Easily upgrade Splunk license
- **Marketplace seller private offers** available for larger index volumes, apps and add-ons
- **Splunk Enterprise licensing** available via AWS Marketplace seller **private offers**

New! Splunk Insights for Infrastructure Pay-as-You-Go

splunk> .conf18



REI Panel Discussion

David Bell | Manager – Infrastructure Cloud Services, REI

Rick Adams, Senior Systems Engineer, REI

splunk> .conf18

Company Overview

REI is a national outdoor retail co-op dedicated to inspiring, educating, and outfitting its members and the community for a lifetime of outdoor adventure and stewardship.

$2.6B

2016
Revenue

17M

Co-op
members

154

Retail stores
in 36 states

Challenges

REI needed to extend its security posture to include edge protection of its Amazon Virtual Private Clouds (VPCs) as it migrated application to AWS.

It was determined that REI previously lacked:

- A solid investigation workflow that included its AWS deployment
- A secure ingress path for migrating applications to AWS
- A clear path for implementing a DevSecOps practice across all REI accounts and VPCs

The AWS & Splunk Solution

AWS Services Used:

- Amazon Virtual Private Cloud
- AWS Application Load Balancer (ALB)
- Amazon GuardDuty
- AWS Config
- Amazon CloudWatch

Splunk Products Used:

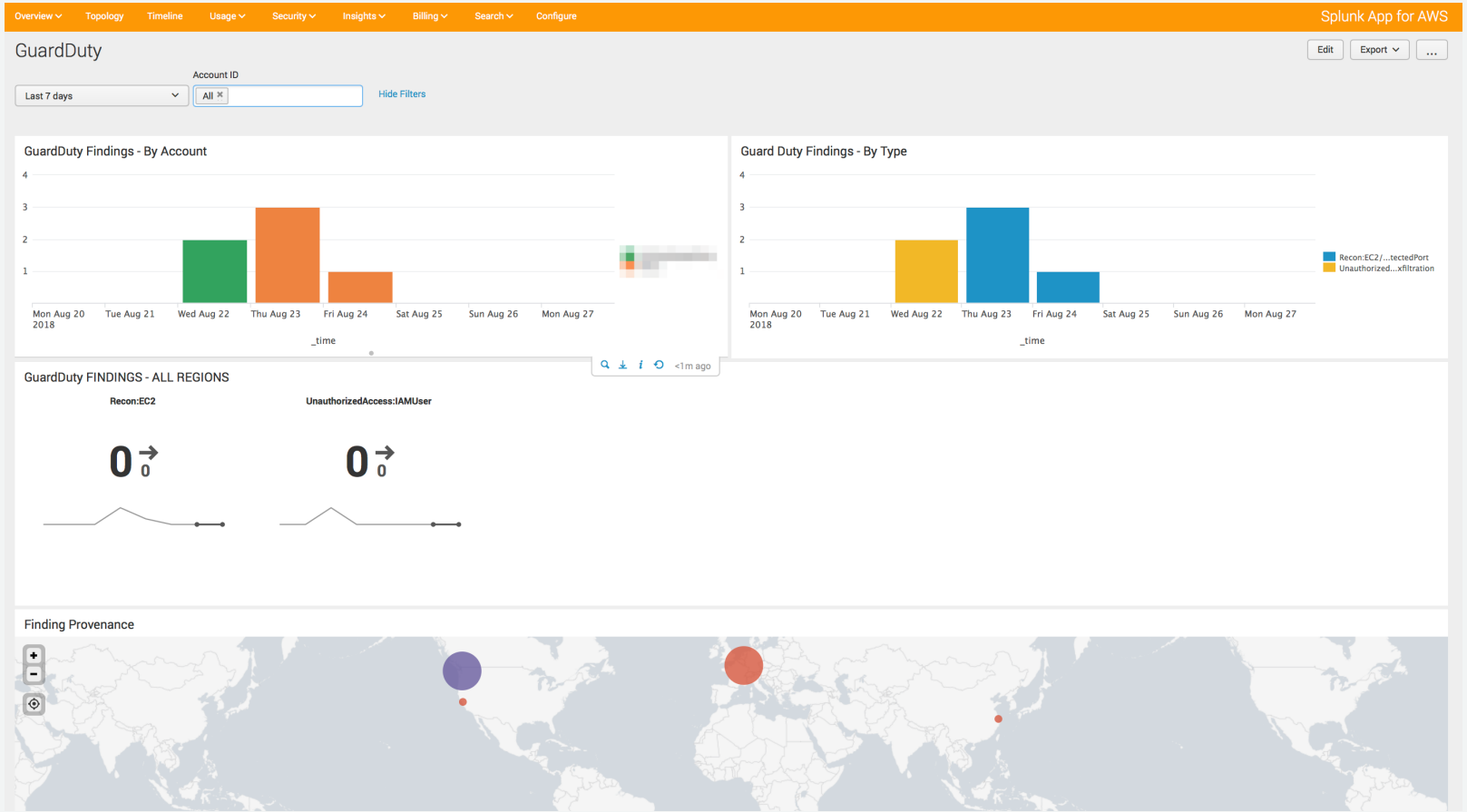
- Splunk Cloud
- Splunk Enterprise Security
- Amazon GuardDuty Add-on for Splunk
- Splunk App for AWS
- Splunk Add-on for Amazon Web Services

"The largest gain was through securing at the edge. This removed the need for individual dev teams to come up with edge protection models for public-facing endpoints. Splunk is helping us aggregate the Amazon VPC flow logs, AWS Application Load Balancer logs and Amazon GuardDuty logs for easy correlation, visualization and alerting."

David Bell, Manager, Infrastructure and Cloud Services, REI

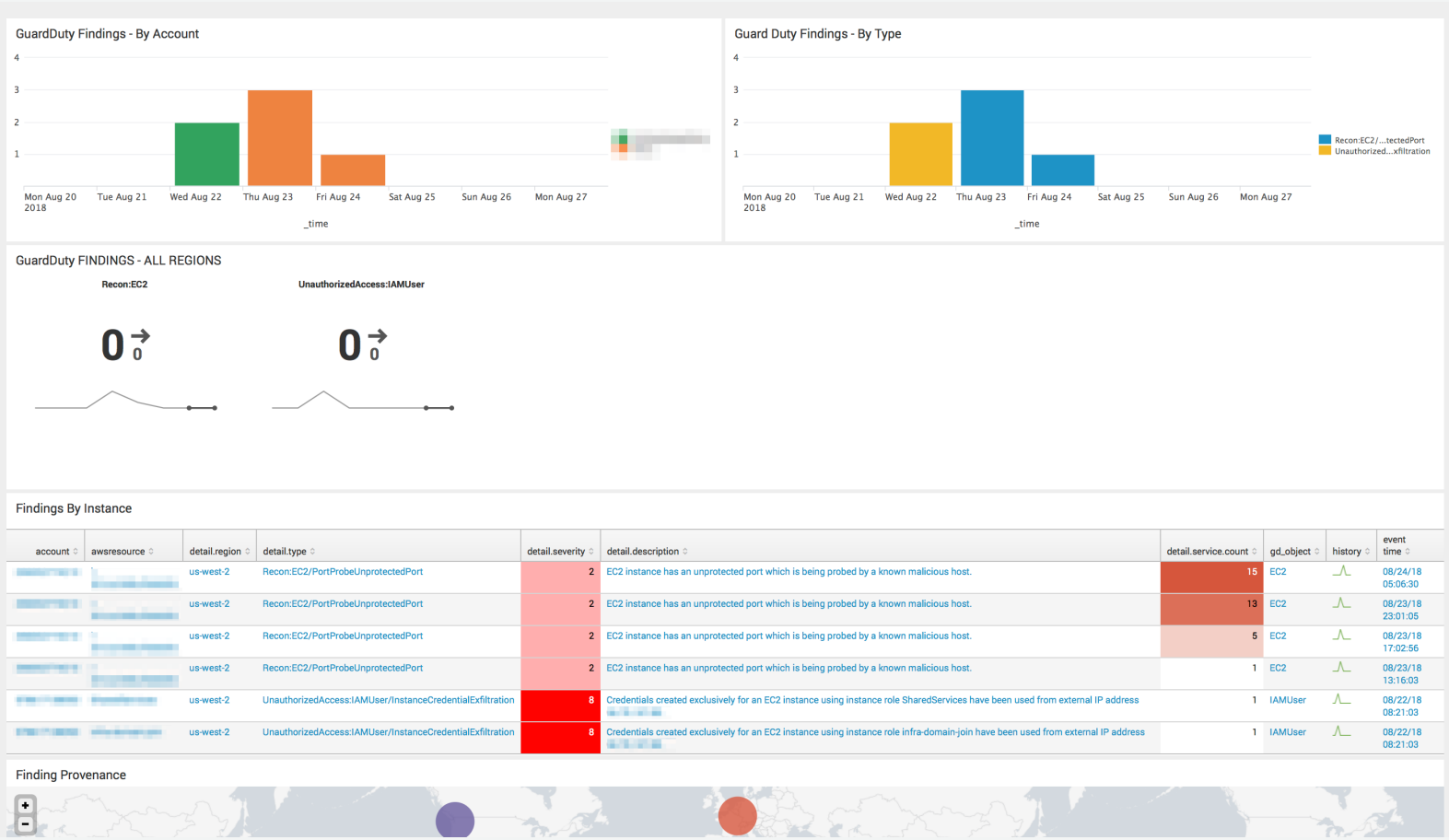
splunk> .conf18

Splunk GuardDuty Dashboard



- Moved Amazon GuardDuty findings to Splunk App for AWS to give security engineers a single source of information.
- Created panels to quickly see number of findings per account and overall numbers per finding type.
- Implemented dropdowns for time frame and to select individual AWS accounts.

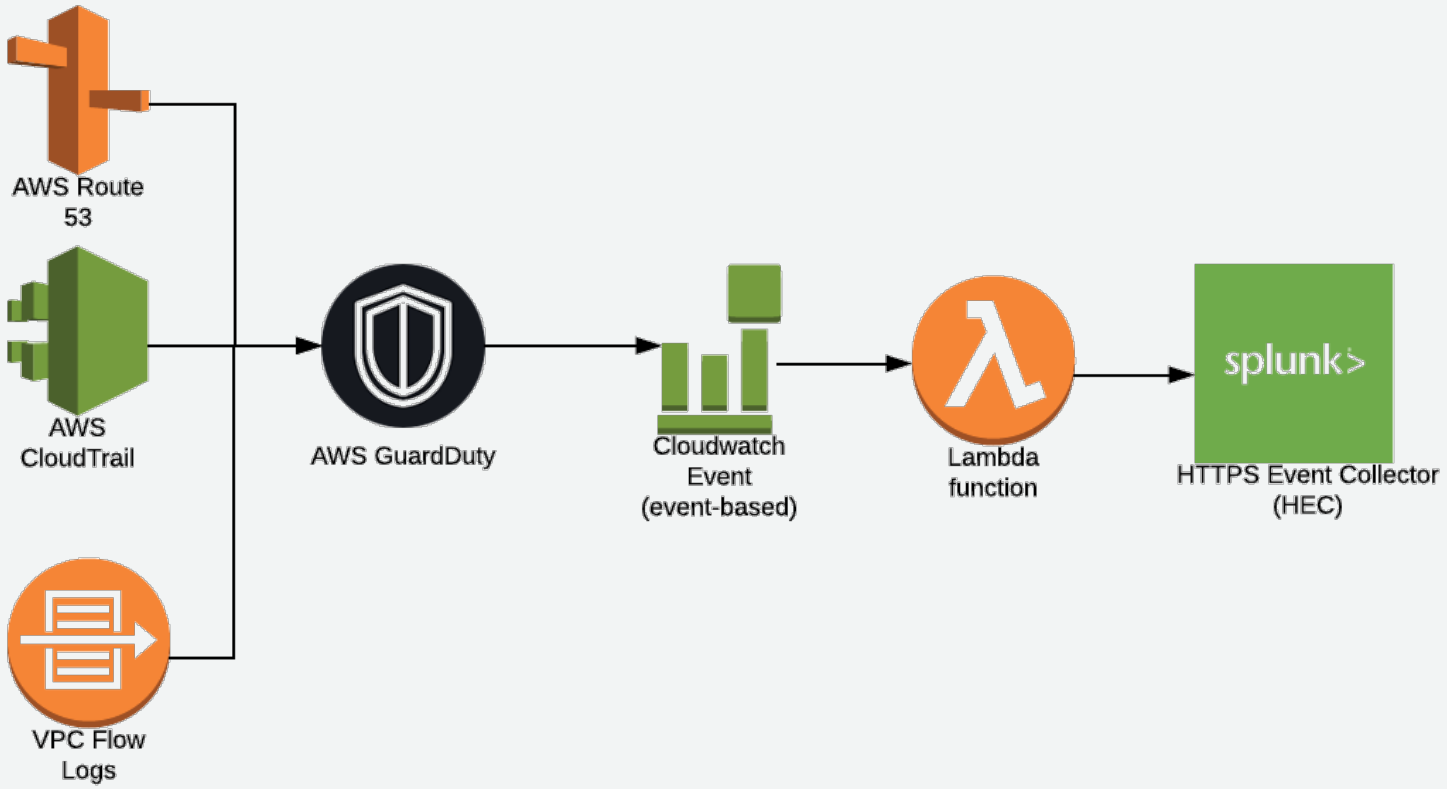
Splunk GuardDuty Dashboard



- Updated hidden drill down panel to work with new custom panels.
- Quickly gives security engineers information concerning AWS accounts, Amazon EC2 instances, and AWS IAM roles.

splunk> .conf18

Splunk GuardDuty Data Flow



- AWS GuardDuty analyzes information from Route 53, CloudTrail, and VPC Flow Logs.
- AWS Cloudwatch Event triggers a Lambda. Immediately for the first alert, every six hours afterwards.
- Lambda function sends CloudWatch data to a Splunk HTTPS Event Collector.
- Note: The Splunk Lambda blueprints and video was extremely helpful in getting this configured.

Business Benefits

REI gained:

Real-time visibility across applications, services, and security infrastructure

Threat intelligence, alerting, security monitoring, and troubleshooting

Enhanced edge security as applications migrate to AWS

Faster time-to-value and ease of use which reduces staffing challenges

Q&A

Thank You

Amazon GuardDuty Product Page https://aws.amazon.com/guardduty/
Amazon GuardDuty Add-on for Splunk https://splunkbase.splunk.com/app/3790/
Code: Splunk Lambda Blueprints https://github.com/splunk/splunk-aws-lambda-blueprints
Video: How to configure Amazon GuardDuty events for Splunk https://youtu.be/wlPfzUZMS6E?t=20s

Don't forget to rate this session in the .conf18 mobile app