splunk> 4 rookies

aws

splunk> a CISCO company | aws

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

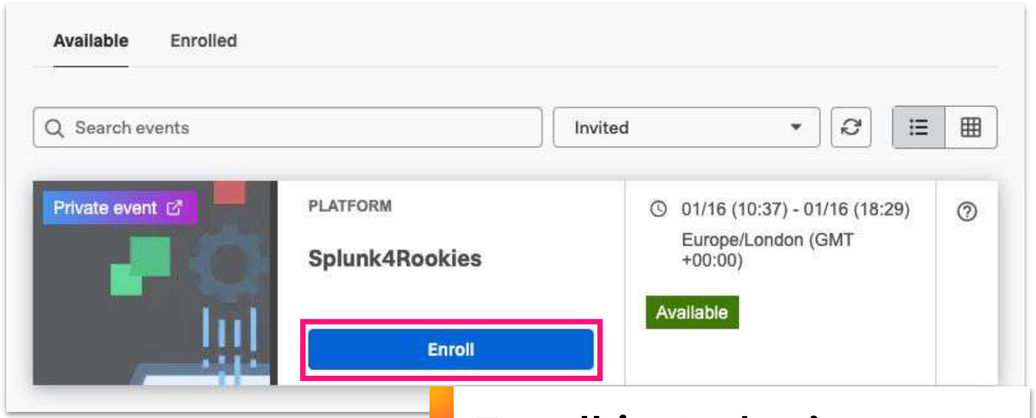
Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide:
   https://splk.it/S4R-AWS-Lab-Guide

   > Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
   https://splk.it/S4R-AWS-Attendee

Goal



Enroll in today's event

Explore how to secure and monitor AWS environments & applications with Splunk

Workshop Agenda

Assumption Alert
Attendees have a basic understanding of Splunk and how Splunk works

Splunk & AWS Overview

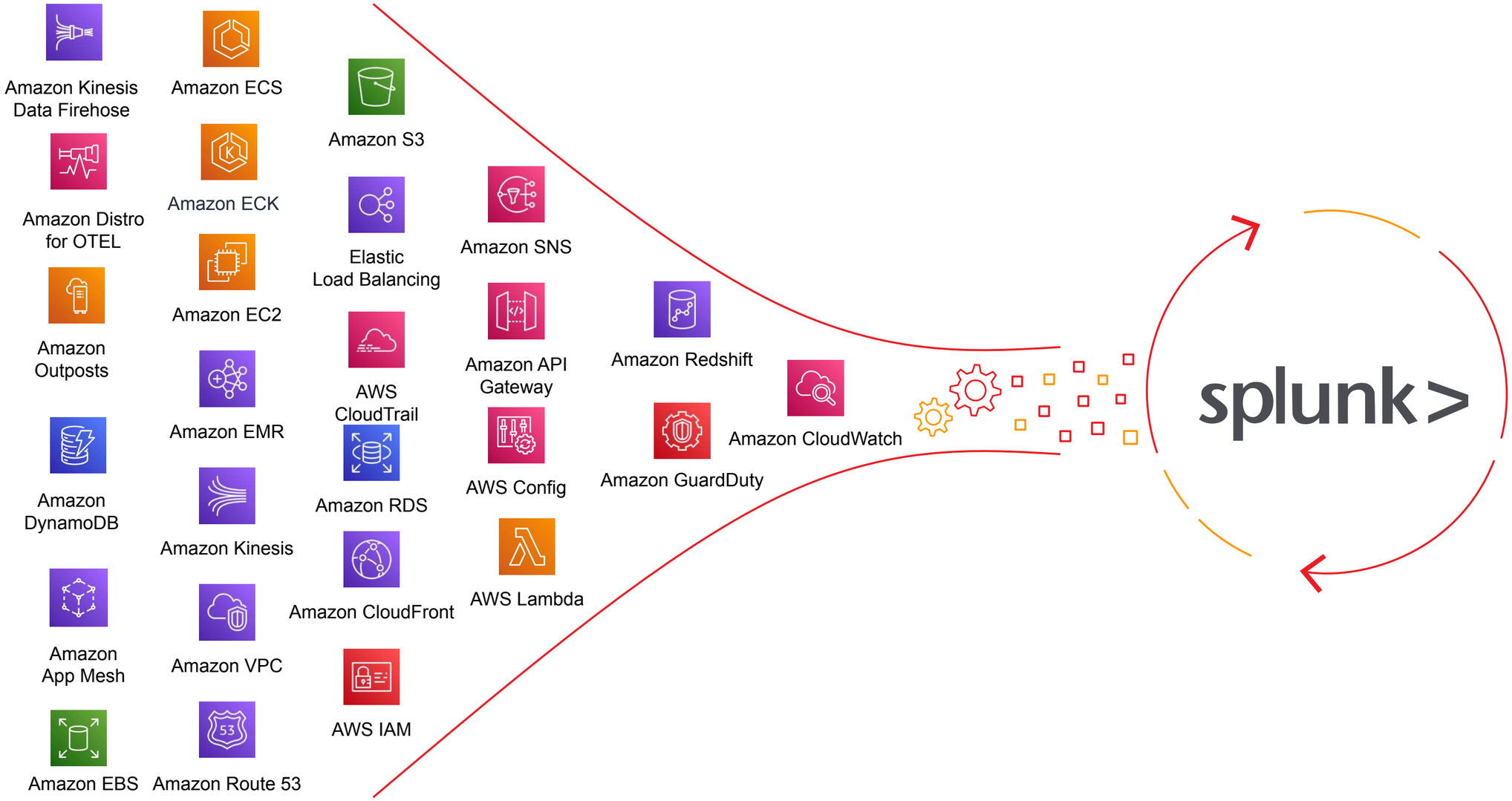
- Building digital resilience with Splunk & AWS
- Getting AWS data into Splunk
- Splunk for AWS Security
- Splunk for AWS Observability

Hands-on-Lab

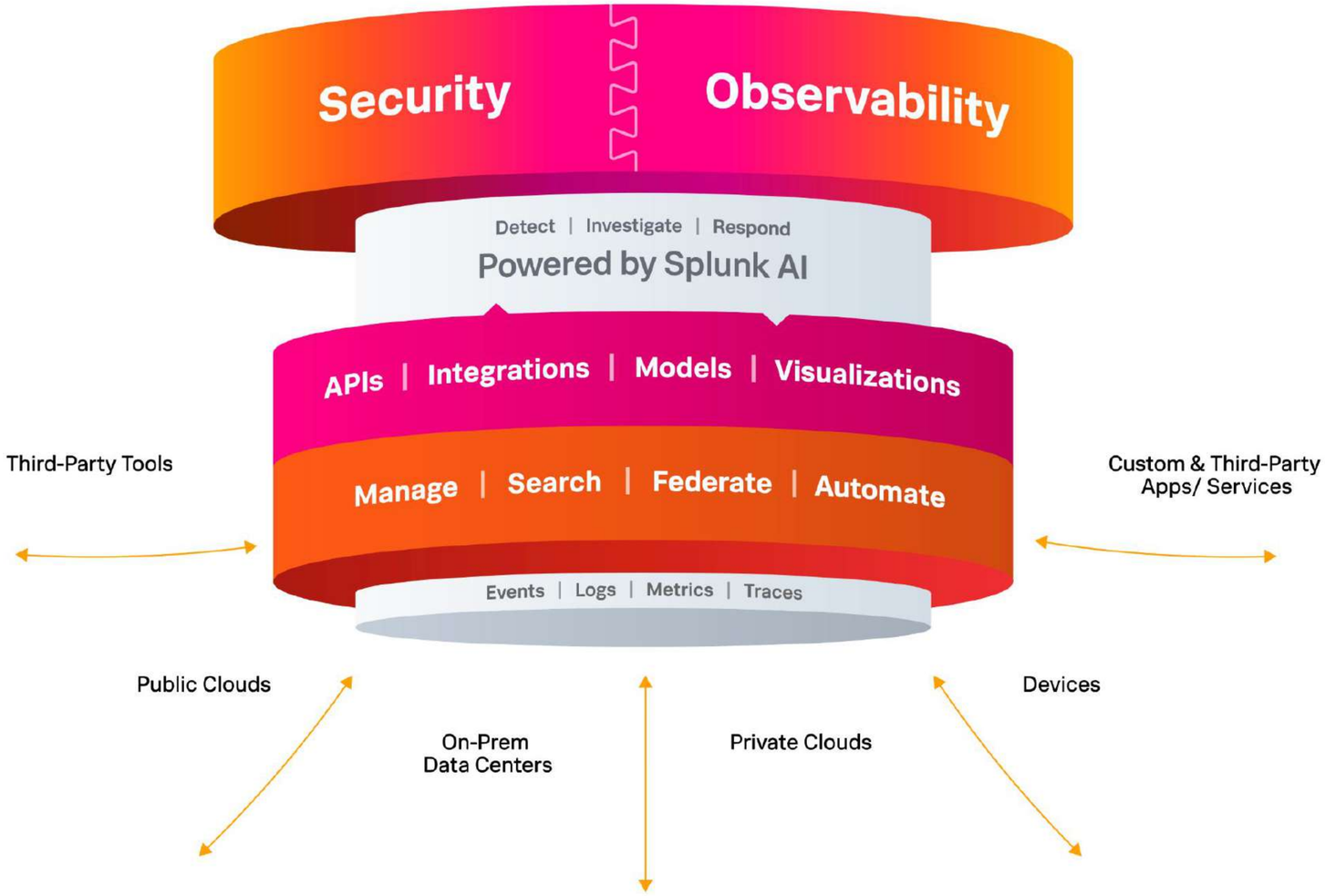
- Using Splunk with AWS Security Services
- Using Splunk to Monitor AWS

Splunk + AWS, Better Together

Splunk helps AWS customers to both secure and monitor their critical AWS environments & apps



The Unified Security and Observability Platform



Splunk Portfolio

Use Cases Apps

Splunkbase

2100+
apps available on Splunkbase

~1K
Add-ons for data source integrations

2400+
Community partners

Observability

- Splunk IT Service Intelligence™
- Splunk Observability Suite
- Splunk Infrastructure Monitoring
- Splunk Application Performance Monitoring

Security

- Splunk Enterprise Security™
- Splunk Attack Analyzer
- Splunk User Behavior Analytics™
- splunk> SOAR

Splunk Core

Cloud + On Premises

splunk>cloud™

splunk>enterprise

aws aws aws

Splunk Runs on AWS

SaaS

splunk>cloud

- Available in 16 regions globally
- 100% Uptime SLA
- Government & Industry compliance certifications
- Available via Marketplace

Self-Managed

splunk>enterprise

- Deploy on EC2 instances
- Quickstart with AWS CloudFormation
- Government & Industry compliance certifications
- Available via Marketplace

AWS & Splunk: Driving business outcomes with an integrated approach

Security monitoring

Advanced threat detection

Insider threat detection

Compliance and data privacy

Incident investigation and forensics

Incident response

Cloud Monitoring

Infrastructure Monitoring

Application Performance Monitoring

Incident Response

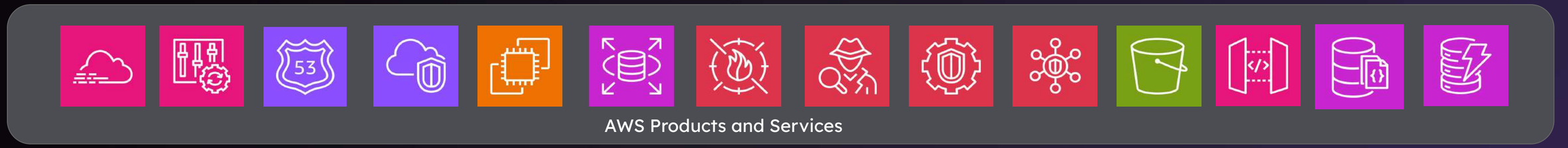
Log Analysis

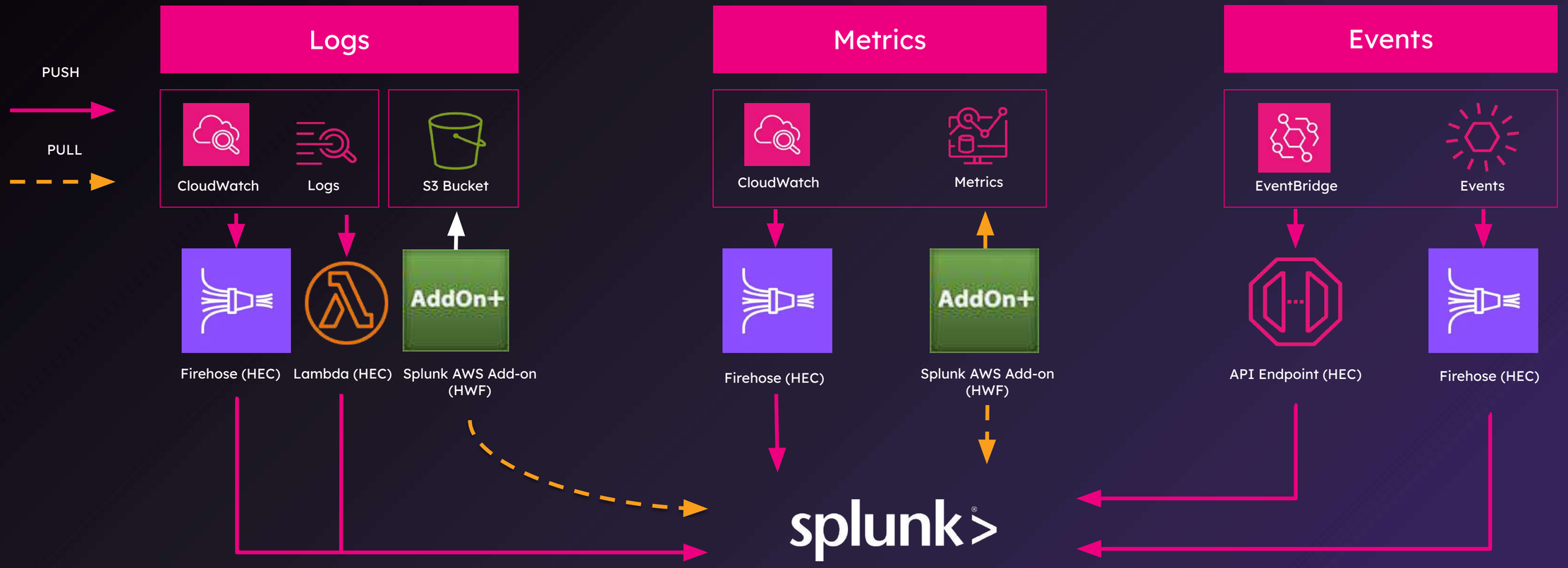
Cloud Migration

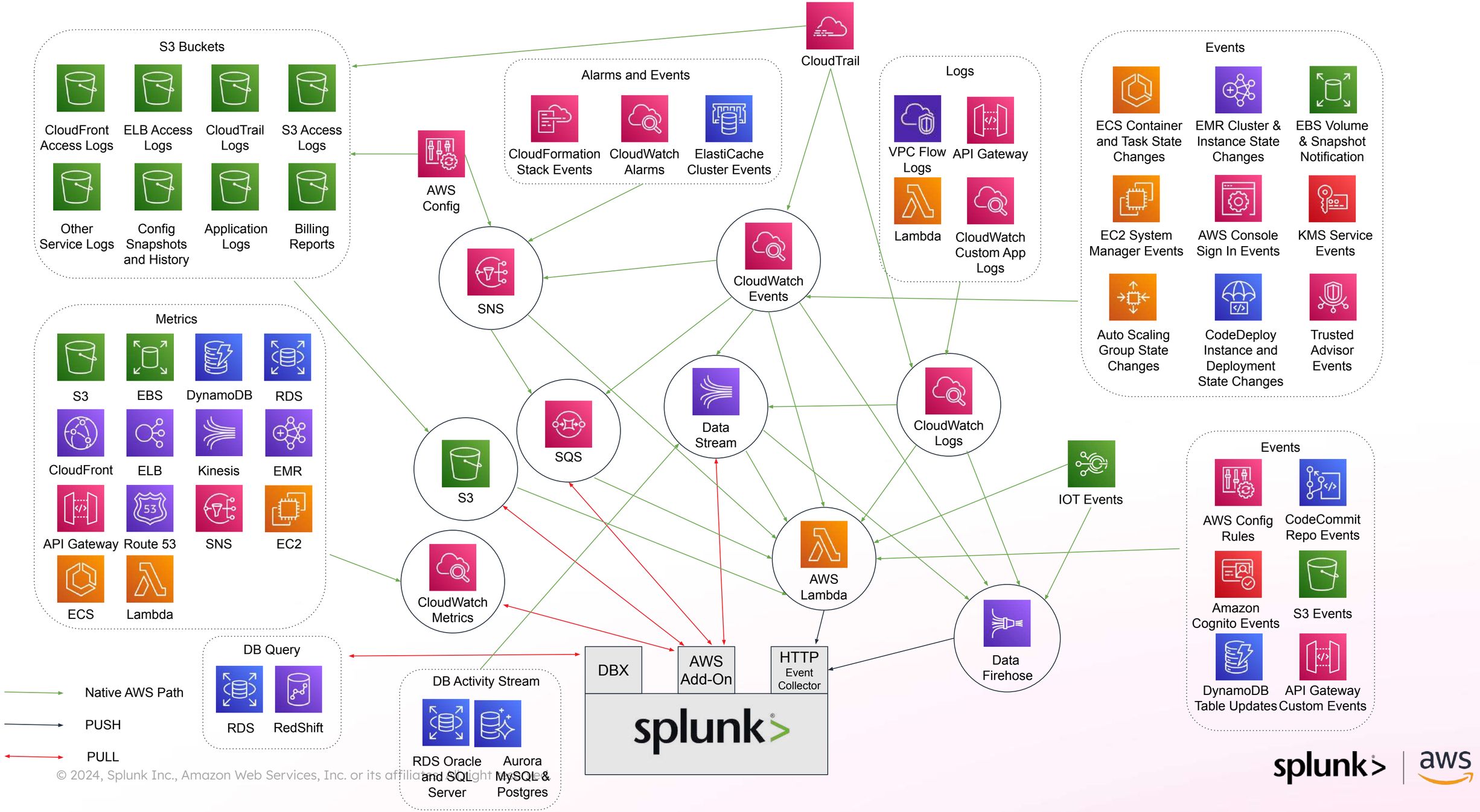
splunk> | aws

Getting AWS Data into Splunk

How AWS data gets into Splunk

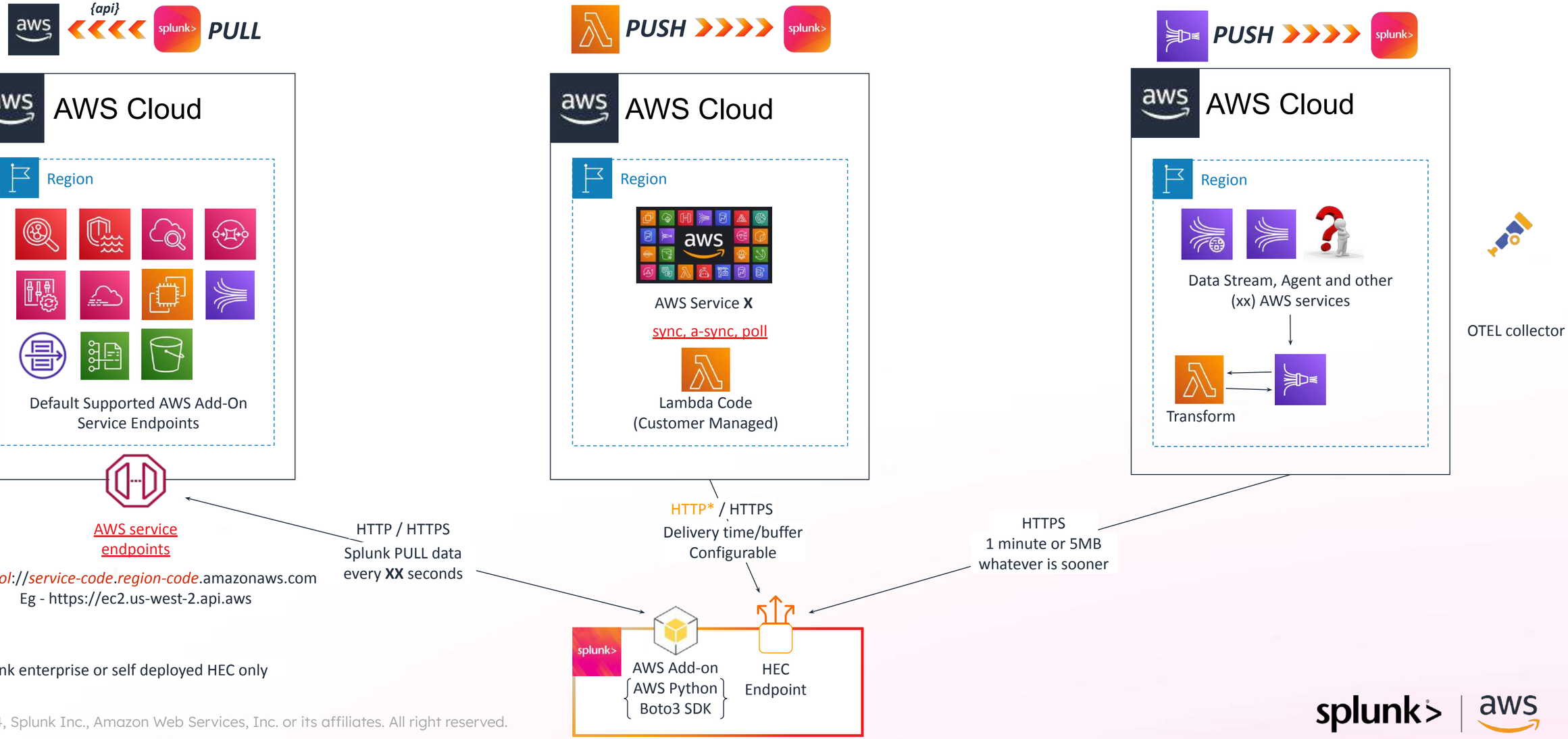






AWS Integration Methods with Splunk

Everything in Threes (3)



HTTP* : Splunk enterprise or self deployed HEC only

Splunk Add-On for AWS

What is the Splunk Add-on for AWS?

Splunk developed Add-on allows you to ingest data across AWS data sources, facilitating the integration of AWS data into your Splunk platform deployment.

The Add-on also includes AWS specific Sourcetypes that can be used with other ingestion methods.

The Add-on is using a PULL is a method of getting data. In this instance we are effectively saying Splunk is the one asking for the data. We are initiating the data request.

splunk>

PUSH (FIREHOSE) and what is it?

PUSH (Firehose) Method

FUN FACT: Splunk was the first company to support firehose as a native endpoint for AWS.

PUSH Firehose is a method of sending the data into Splunk via using a highly scalable enterprise grade streaming service called Data Firehose.

Because it is sending data to Splunk into the HEC endpoint we consider this a PUSH method, ie we are receiving the data.

Data firehose is generally thought of as the preferred method when available for more enterprises as it offers SaaS scale with enterprise resilience including HEC acknowledgement allowed for better guaranteed data delivery.

Other Methods of Getting Data into Splunk

Lambda

- Lambda is a method of sending the data into Splunk via Code
- Sends data to Splunk into the HEC endpoint
- Some companies today have a lambda first policy

Data Manager

- Used with Splunk Cloud Only
- Onboard AWS service data via Splunk interface
- Does not include all AWS data sources

Splunk & AWS:

Security

AWS and Splunk enhance security for the cloud through the shared responsibility model

Customers are responsible for security “in” the cloud

- CUSTOMER DATA
- PLATFORM, APPLICATIONS, IDENTITY, & ACCESS MANAGEMENT
- OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
- CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
- SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
- NETWORKING TRAFFIC PROTECTION (ENCRYPTION INTEGRITY, IDENTITY)

splunk>

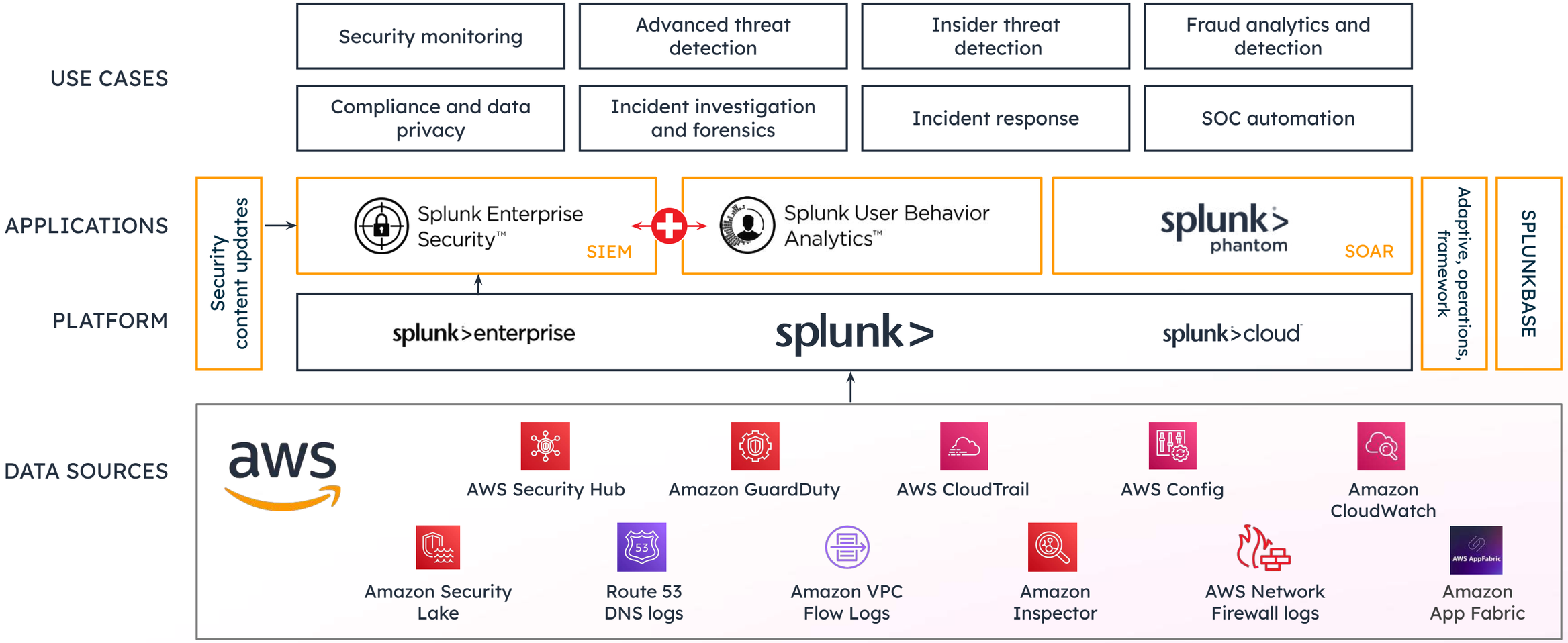
AWS

AWS is responsible for the security “of” the cloud

- SOFTWARE
  - COMPUTE
  - STORAGE
  - DATABASE
  - NETWORKING
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
  - REGIONS
  - AVAILABILITY ZONES
  - EDGE LOCATIONS

splunk> | aws

Splunk Security Operations Suite ingests AWS data sources across common security use cases

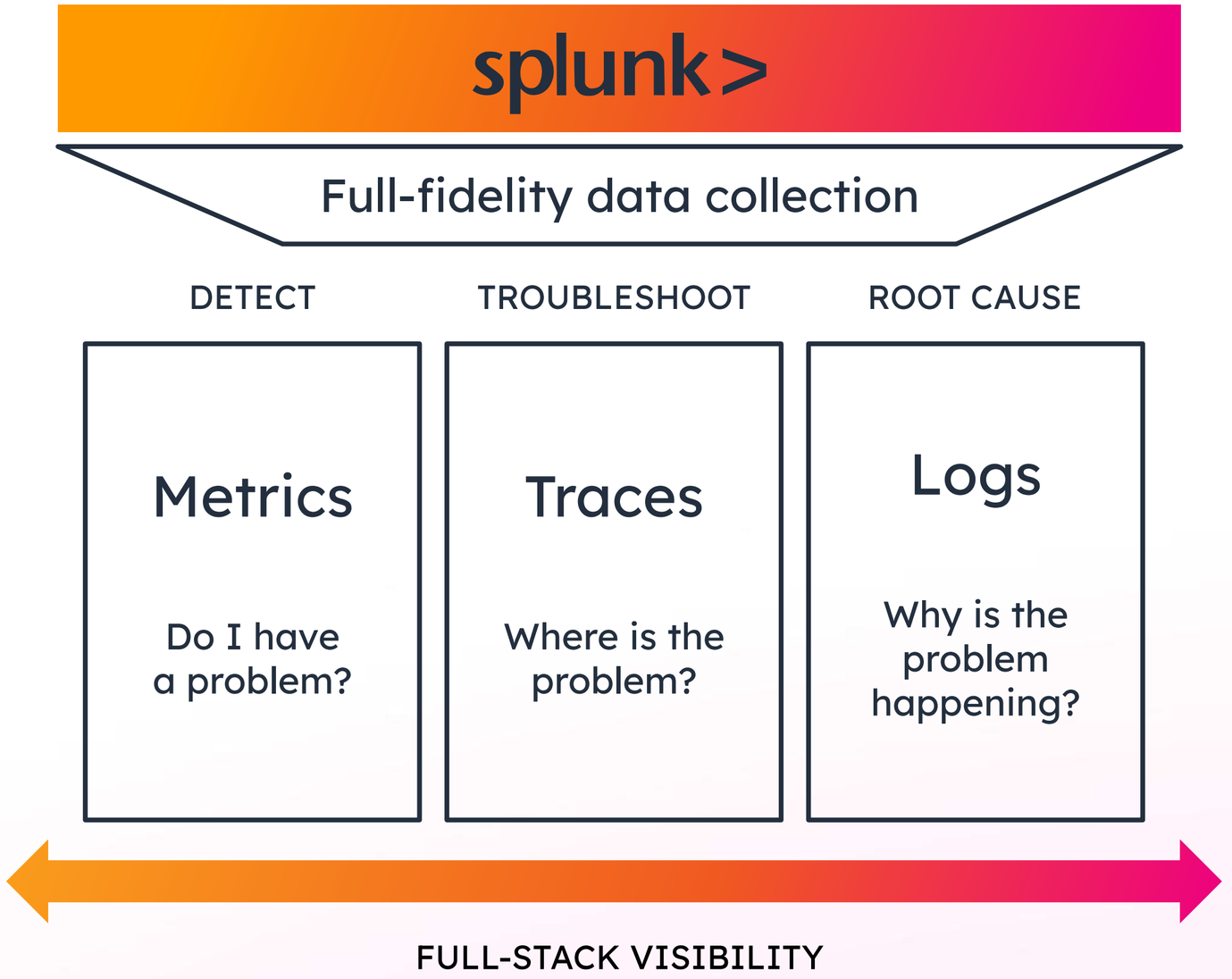


Splunk & AWS:

Observability

Splunk takes a data-driven approach to observability

Full-stack visibility and contextual insights into the behavior of critical business and operational systems



splunk> | aws

Deep visibility into AWS services


Amazon Elastic Kubernetes Service


Amazon Elastic Container Service


AWS Outposts


Amazon EC2


AWS Lambda


AWS Lambda Extensions


AWS Lambda Function Wrappers


Amazon CloudWatch


Amazon RDS


Amazon DynamoDB

Amazon Route 53


Amazon Redshift


Amazon CloudFront


AWS App Mesh


Elastic Load Balancing


Amazon Simple Storage Service (S3)


Amazon Elastic Block Store


AWS Distro for OpenTelemetry

splunk> | aws

Hands On

Setup & Explore Environment

splunk> a CISCO company

Splunk's Search Processing Language (SPL)

Search Terms

Commands

```
index=main action=purchase | stats count by status | rename count as "number of events"
```

Pipe character: Output of left is input to right

Functions

e.g. `index=main action=purchase` `| stats count by status` `| rename count as "number of events"`

i	Time	Event
>	16/01/2024 11:03:08.000	27.102.0.0 - - [16/Jan/2024 11:03:08] "GET /cart.do?action=view&product_id=MCB-5&JSESSIONID=SD6SL6FF10ADFF3 HTTP 1.1" 200 3453 "http://www.buttercupenterprises.com/product.screen?product_id=DFS-2" "Mozilla/5.0 (Linux; Android 12.0.0; SM-A546B Build/A546BXXU1AWB7) AppleWebKit/537.36 Chrome/114.0.5735.61 Mobile Safari/537.36 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 388 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	131.178.233.243 - - [16/Jan/2024 11:03:08] "POST /product.screen?uid=5ac99574-edc7-417d-ad38-df91f883d280&product_id=PP-5&JSESSIONID=SD7SL3FF6ADFF8 HTTP 1.1" 200 2311 "http://www.buttercupenterprises.com/product.screen?product_id=PP-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 Chrome/107.0.5304.122 Safari/537.36" 703 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.4 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=881e7945-8fd6-4a55-94c1-880f668ea048&product_id=BW-3&JSESSIONID=SD1SL6FF5ADFF6 HTTP 1.1" 400 3158 "http://www.buttercupenterprises.com/product.screen?product_id=BS-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 Version/15.0 Mobile/19A346 Safari/602.1" 602 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.5 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=8a9dfff3-2e4f-4ea6-aef6-088cdb412b8e&product_id=BW-3&JSESSIONID=SD8SL1FF4ADFF1 HTTP 1.1" 505 1310 "http://www.buttercupenterprises.com/product.screen?product_id=CM-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/113.0.5672.92 Safari/537.36" 977 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined

status	count
200	850
400	81
401	76
402	50
403	57

status	number of events
200	850
400	81
401	76
402	50
403	57

Want to know more? Check out:
Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef
Search manual: https://splk.it/SplunkSearchManual

Apps and Add-ons

- 2100+ free apps and add-ons available from https://splunkbase.splunk.com/
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs

Apps

Content designed to bring fast time-to-value from your data in Splunk, including pre-built dashboards, reports, alerts, visualisations and workflows

Add-ons

Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

Splunk Dashboards

Classic Dashboards (Simple XML)

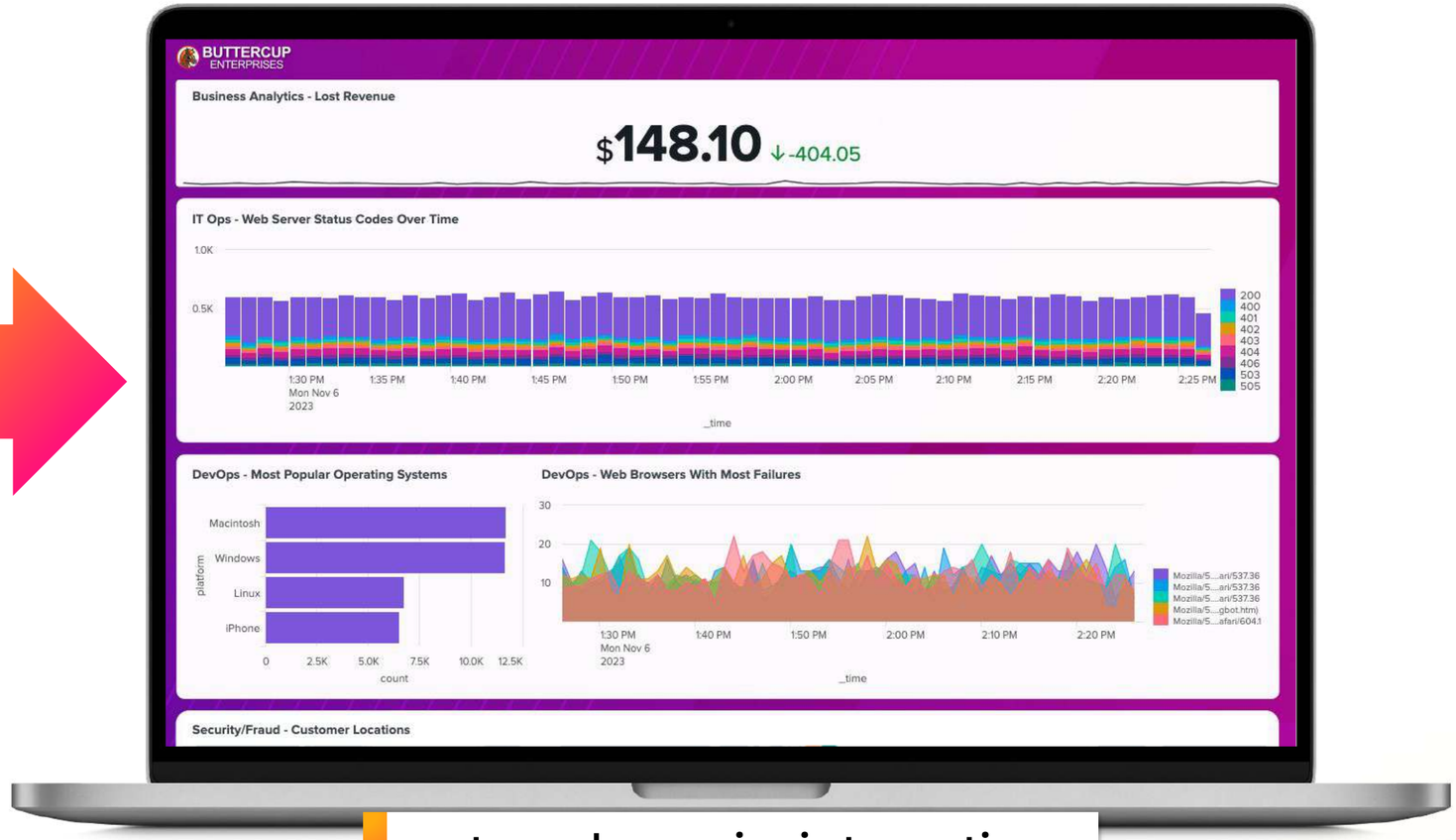
- Easy to deploy a **wide variety of visualisations**, but **hard to craft a story**
- **Flexible and extensible**, but **time consuming** to build something truly beautiful (e.g. custom JS, CSS)
- **PDF export loses look/feel** of dashboard

Dashboard Studio

- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images**, **text boxes**, **shapes**, **lines** and **icons**, with **intact PDF export**
- **No custom code** required

Objective for Today

Go from messy machine data…



…to a dynamic, interactive dashboard!

Today’s Scenario

Your Company

- Buttercup Enterprises is a large national online retailer operating in the US, which sells a variety of books, clothing and other gifts through its online webstore hosted on AWS
- Buttercup Enterprises have recently invested in Splunk to help secure and monitor its applications and AWS environments.

Your Role

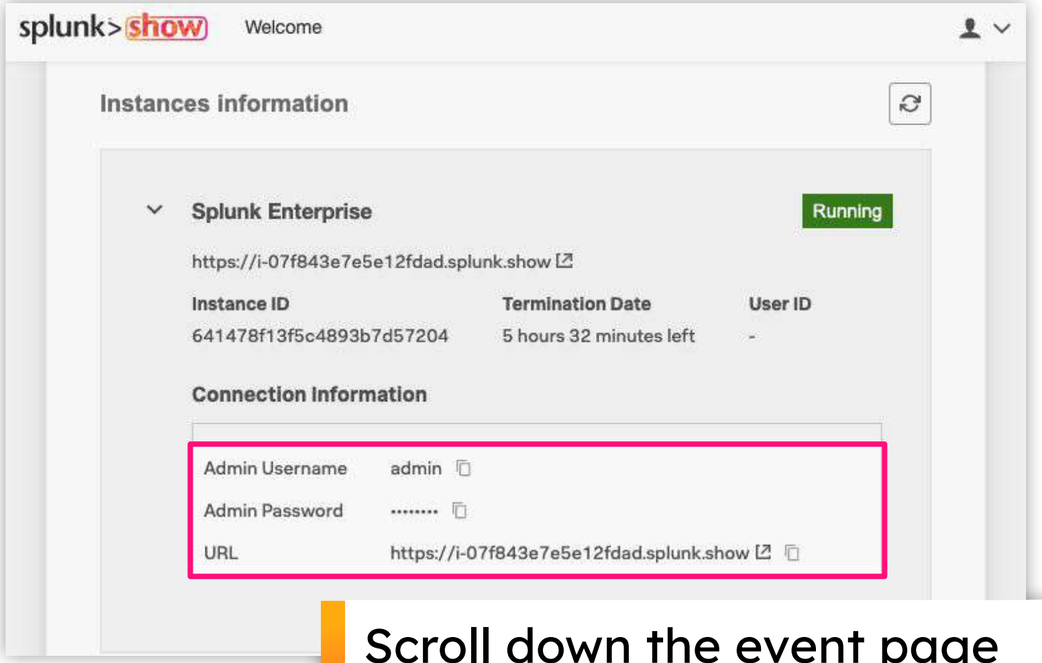
- You are one of the chosen few: a Splunk power user!
- Your responsibility is to provide insights to users throughout the company
- You are tasked with providing insights for the security team and IT Ops team

Exercise 1

Explore Splunk

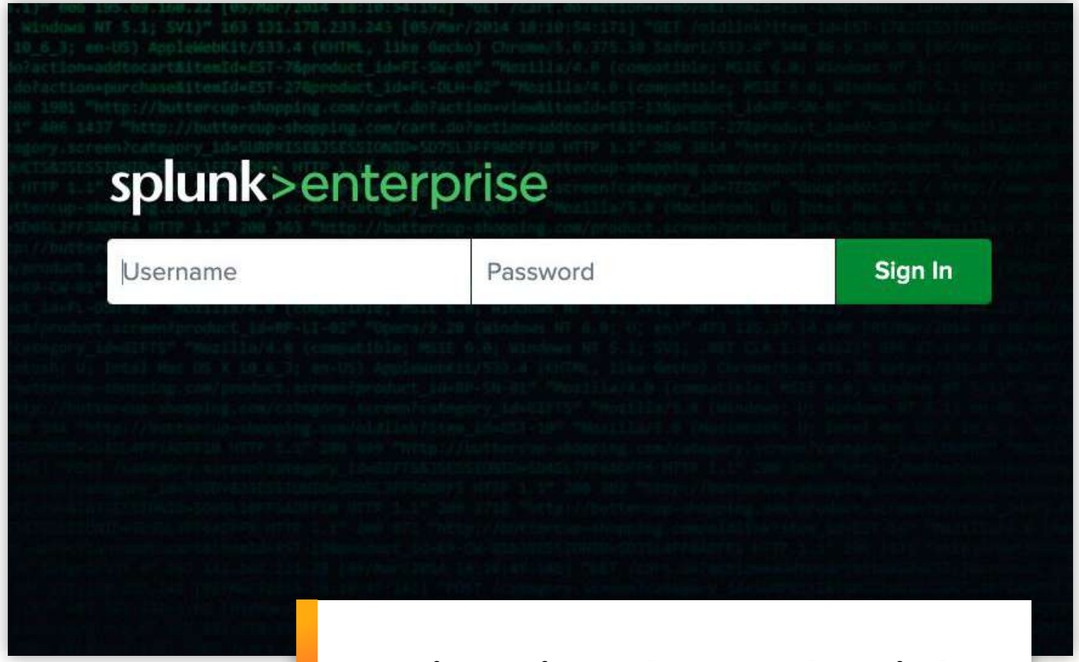
Login to Splunk

Locate your instance URL and credentials in the Splunk Show event
https://show.splunk.com



Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

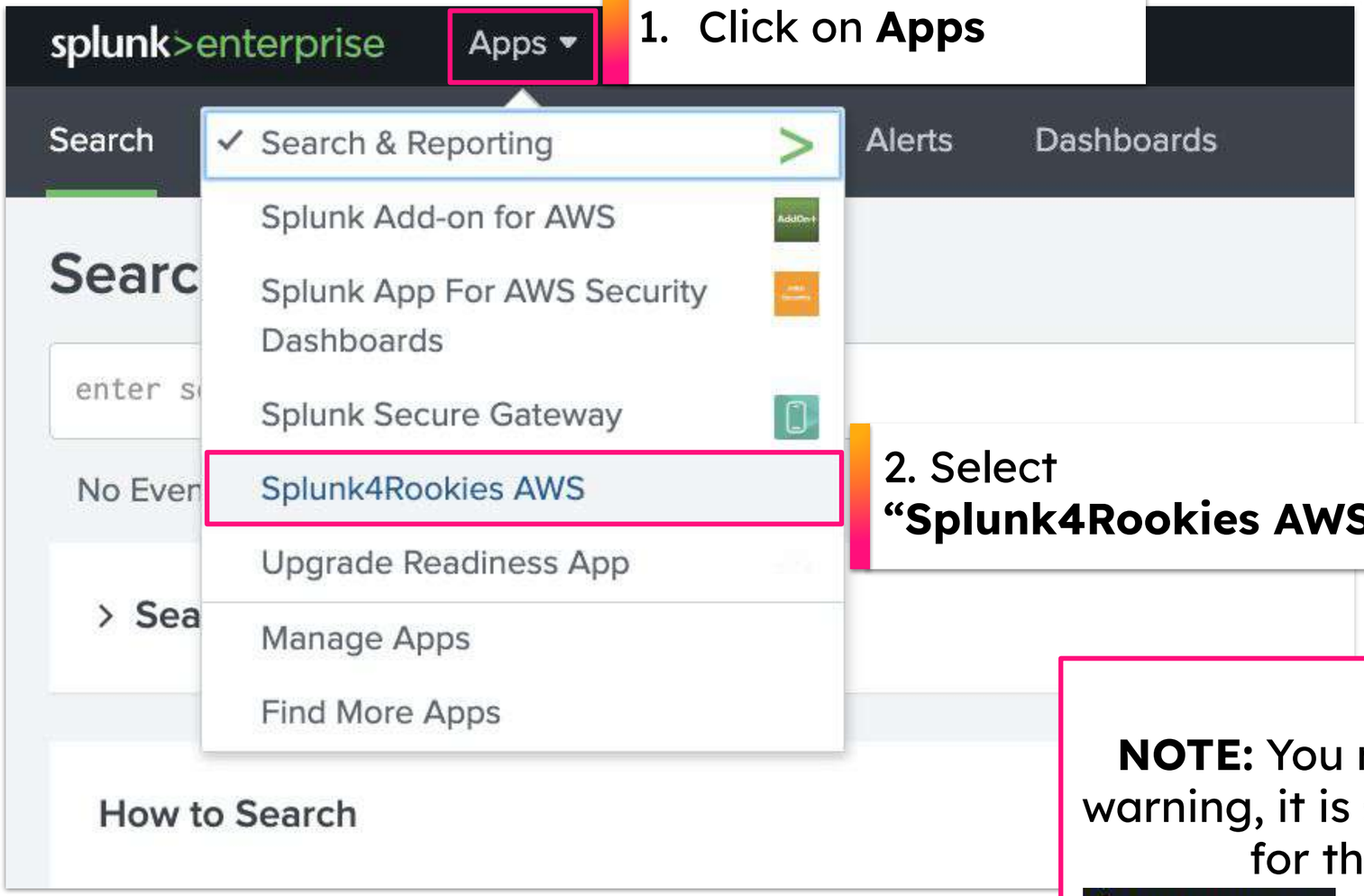
Log in to your Splunk instance



Login using the credentials from Splunk Show

1

Lets First Go to the AWS App

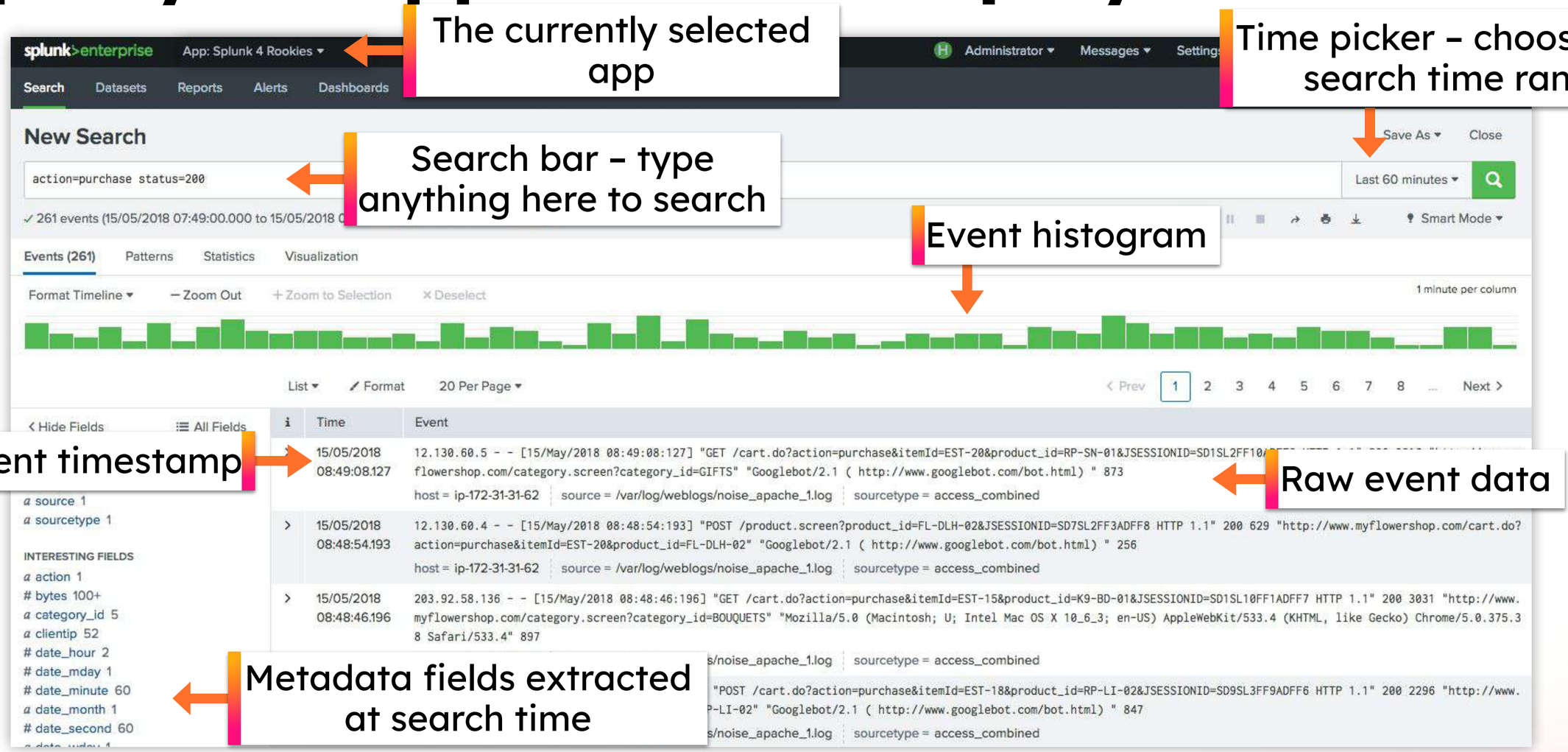


1. Click on **Apps**

2. Select **“Splunk4Rookies AWS”**

NOTE: You may see this warning, it is safe to ignore for the labs

Open your app and have a play!



Start Exploring Your Data

Example searches:

`sourcetype=*`	Explore the AWS services that are sending data to Splunk
`error`	Search for events that contain “Error”
`error*`	Expand search with a wildcard. Do the # of sourcetype change?

Explore the events from the different AWS services

- What fields are the same?
- Can you gain any information from any of the services?

Explore the logs and look for interesting fields

Exercise 2

VPC Flow Logs

VPC Flow Logs

What are they and when should I ingest into Splunk?

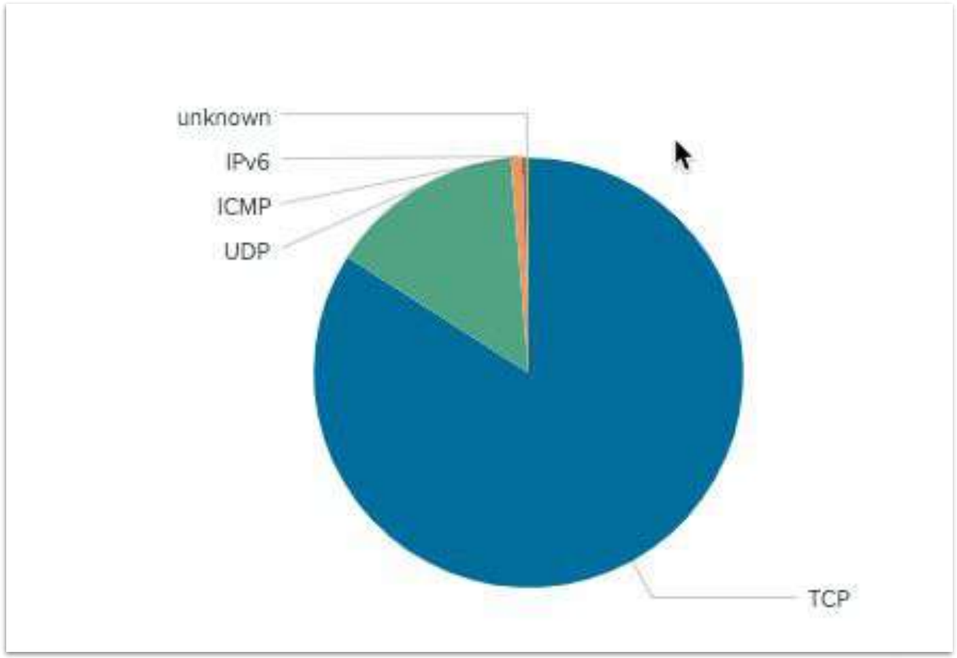
- Allows capture of IP traffic in/out of network interfaces in a VPC
- Helps with:
  - Diagnosing restrictive security group rules
  - Monitoring traffic into and out of your instance
  - Determining direction of traffic
- Can ingest into Splunk or query using Amazon Security Lake and Federated Analytics

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

VPC Example in Splunk

> 8/11/20 4:35:20.000 PM
2 058441036840 eni-026393b403a7aa371 10.0.0.208 52.119.178.64 56008 443 6 4 160 1597163720 1597163730 ACCEPT OK
host = 204.236.168.170:8088 | source = lambda:SplunkVPCFlow | sourcetype = aws:cloudwatchlogs:vpcflow

Type	Field	Value	Actions
Selected	host	204.236.168.170:8088	
	source	lambda:SplunkVPCFlow	
	sourcetype	aws:cloudwatchlogs:vpcflow	
Event	account_id	058441036840	
	action	allowed	
	aws_account_id	058441036840	
	bytes	160	
	dest	52.119.178.64	
	dest_ip	52.119.178.64	
	dest_port	443	
	duration	10	
	dvc	eni-026393b403a7aa371	
	end_time	1597163730	
	eventtype	vpcflow (cloud communicate network traffic)	
	interface_id	eni-026393b403a7aa371	
	log_status	OK	
	packets	4	



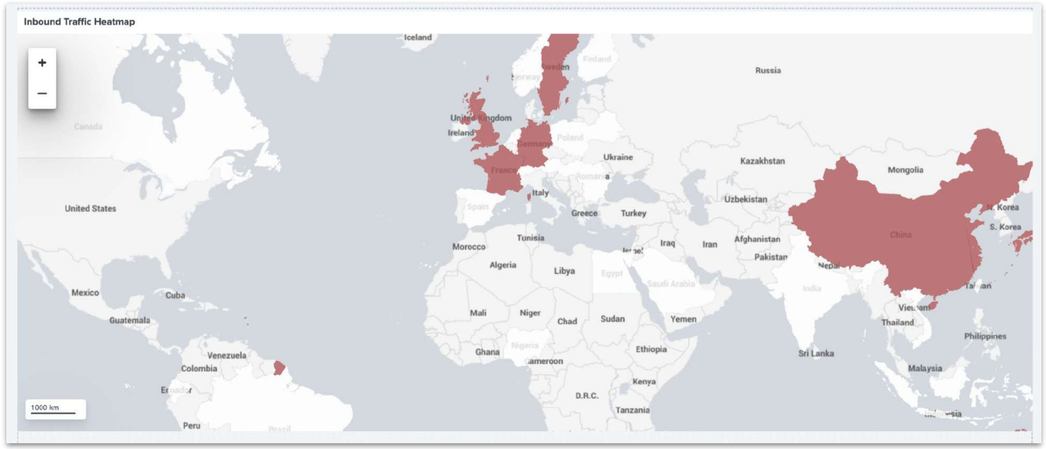
Security Team

Investigate VPC Flow logs

Tasks

1. Explore VPC Flow Logs using Splunk
2. Identify countries that are the top talkers?
3. Explore countries of interest
4. Create heatmap of the traffic
5. Create dashboard and save heatmap

Goal



Dig into VPC

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
```

i	Time	Event
>	8/11/20 4:35:20.000 PM	2 058441036840 eni-026393b403a7aa371 10.0.0.208 52.119.178.64 56008 443 6 4 160 1597163720 1597163730 ACCEPT OK host = 204.236.168.170:8088 source = lambda:SplunkVPCFlow sourcetype = aws:cloudwatchlogs:vpcflow
>	8/11/20 4:35:20.000 PM	2 058441036840 eni-026393b403a7aa371 104.143.92.220 10.0.0.208 7711 443 6 206 77970 1597163720 1597163730 ACCEPT OK host = 204.236.168.170:8088 source = lambda:SplunkVPCFlow sourcetype = aws:cloudwatchlogs:vpcflow
>	8/11/20 4:35:20.000 PM	2 058441036840 eni-026393b403a7aa371 10.0.0.208 10.0.2.230 8088 18834 6 4 239 1597163720 1597163730 ACCEPT OK host = 204.236.168.170:8088 source = lambda:SplunkVPCFlow sourcetype = aws:cloudwatchlogs:vpcflow

Investigate VPC Flow Logs

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
```

Explore the logs and look for interesting fields

iplocation Information

The iplocation command extracts location information from IP addresses by using 3rd-party databases. This command supports IPv4 and IPv6 addresses and subnets that use CIDR notation.

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip | stats count by Country | sort - count
```

Country	count
United States	9236
Russia	1306
Czechia	1253
Netherlands	947
China	519
Germany	456
France	289
Canada	226
Seychelles	145
Ukraine	121
United Kingdom	101
Poland	75

Traffic Flow (bytes) from Countries

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| stats sum(bytes) as bytes by Country
| sort -bytes
```

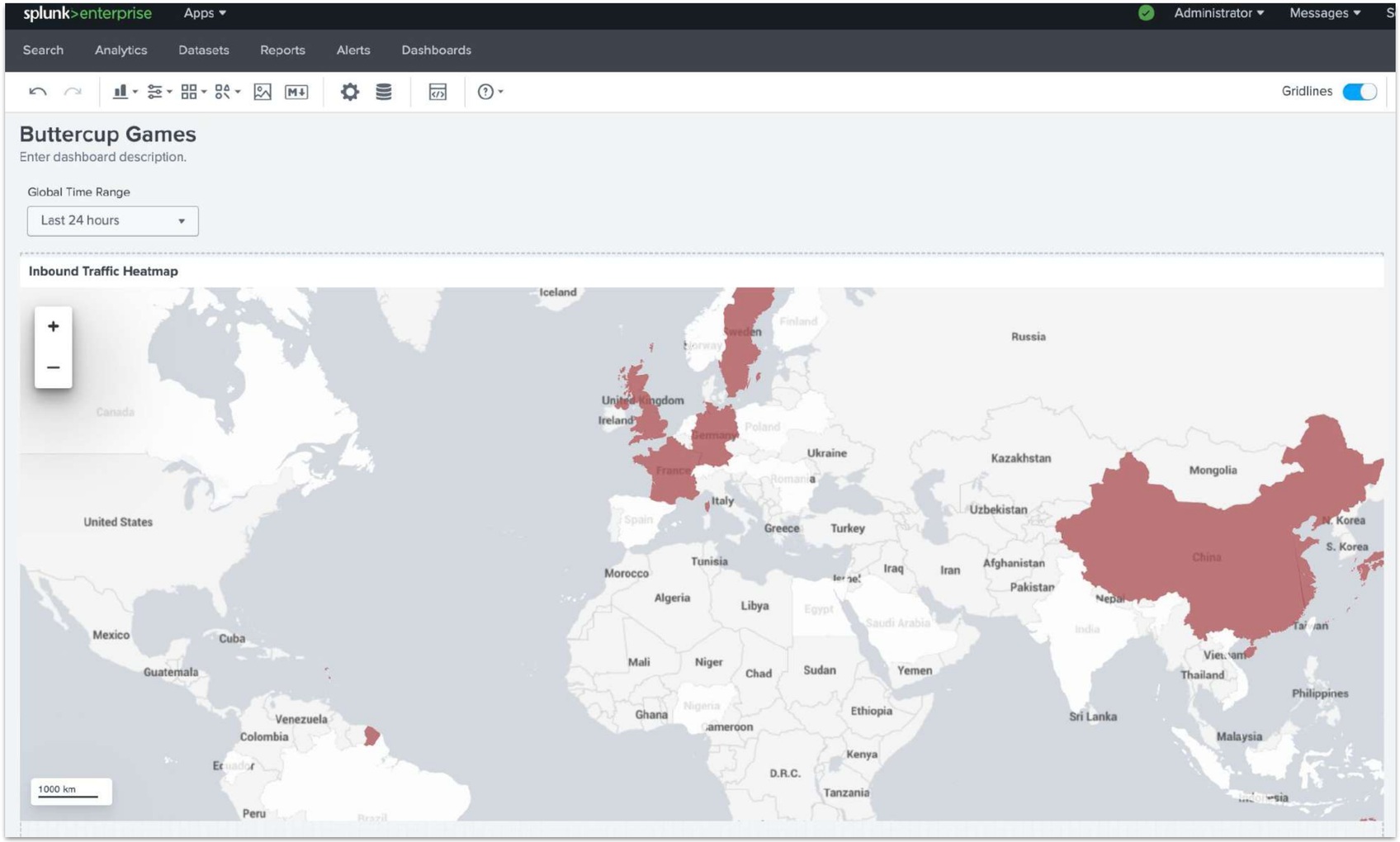
Country	bytes
United States	980946514
China	235648
Germany	193956
Netherlands	158735
Russia	85580

Create Heatmap of Traffic

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| search Country!="United States"
| stats count by Country
| geom geo_countries featureIdField="Country"
```

LAB EXERCISE 1 TASK 4 5 MINS

Create new dashboard and add heatmap



What do we know so far?

- VPC Flow logging is enabled:
  - Default VPC logging has been turned on, no customizations
- `iplocation` adds a ton of useful information:
  - Most traffic is coming from the US
  - Significant traffic is coming from China, Russia, and the Netherlands
  - Frothly has been attacked in the past by adversaries which use tools in both Russia and the Netherlands (see appendix for Diamond Model)

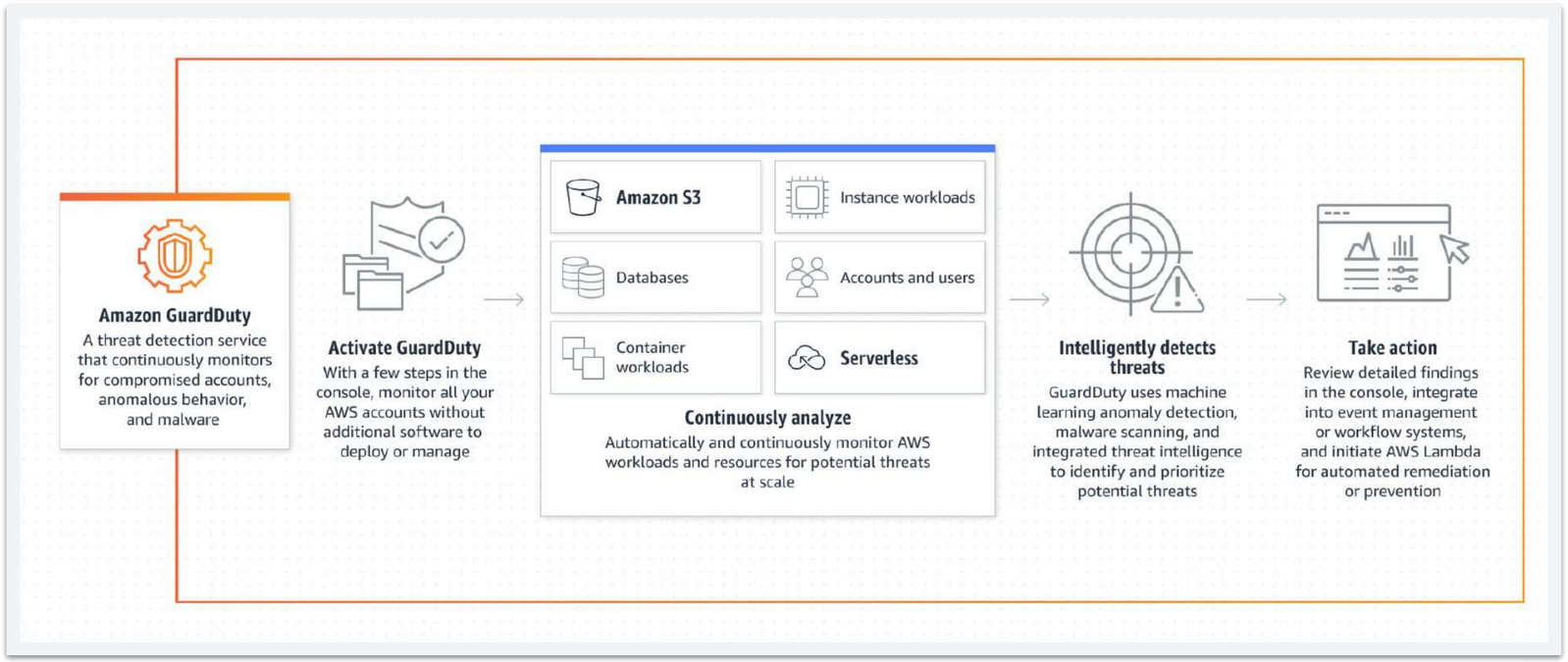
Amazon Guard Duty

What is it and what should I enable it?

An AWS workload protection service that keeps an eye a set of AWS services

Services Available: S3, EKS, ECS, EC2, RDS and Lambda

More Info: https://aws.amazon.com/guardduty/



Amazon Guard Duty

Protect AWS accounts with intelligent threat detection

AWS Config

What is it and what should I enable it?

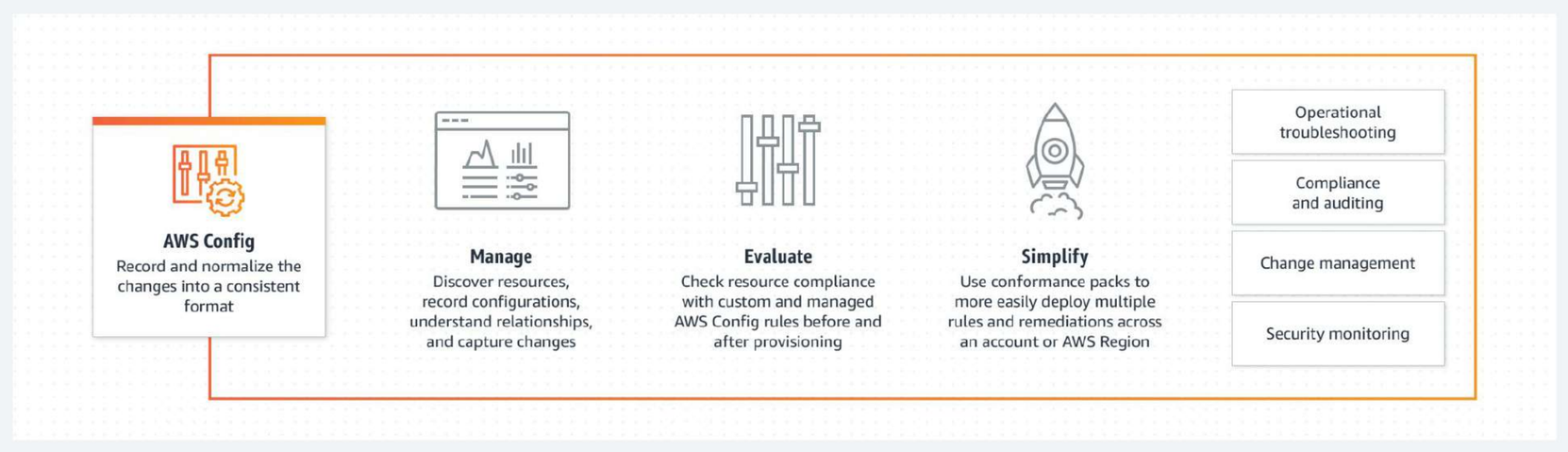
Keep track of configuration and relationship changes to your AWS services over time with AWS Config. Supported resource types.

Optionally set up rules to flag when a resource becomes non compliant.

AWS Config also has an ability to do ahoc config snapshots (CLI/API only). These are also stored in the same S3 bucket in a different folder.

In Short: Use AWS Config to detect (record) what resources are configured or misconfigured overtime. Good for auditing and alerting on configuration changes.

More Info: https://aws.amazon.com/config/



AWS Config

Get a detailed view of the configuration of AWS resources inside your AWS accounts

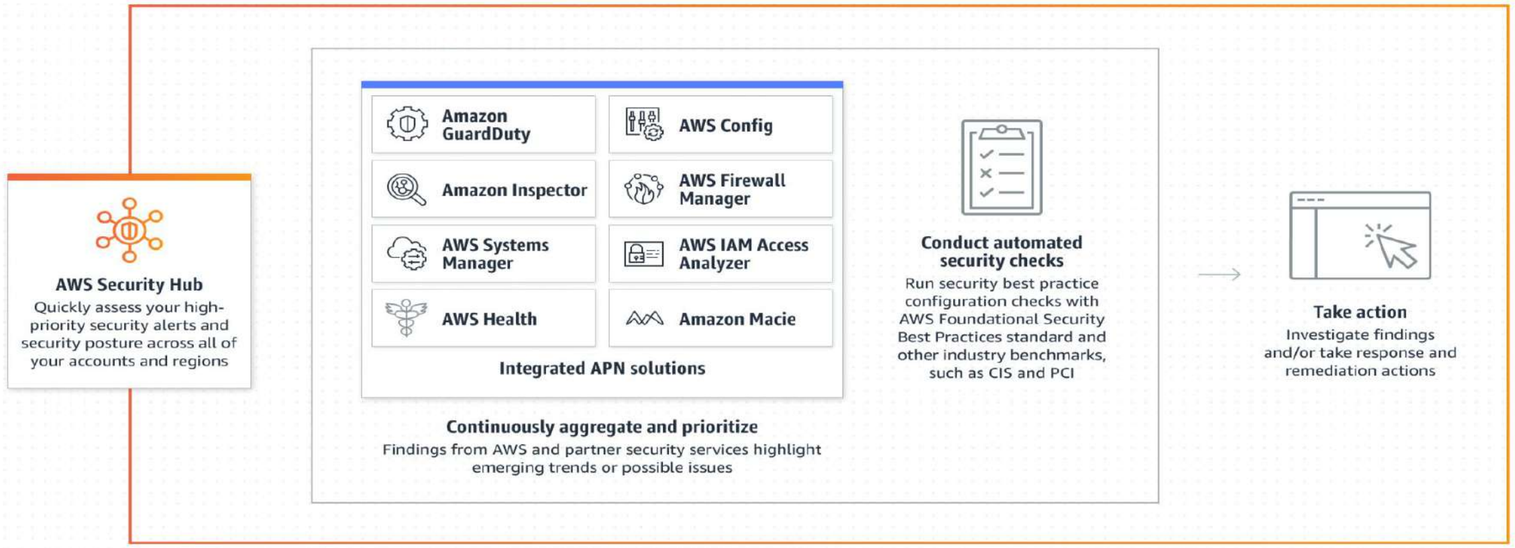
AWS Security Hub

What is it and what should I enable it?

Security Hub enables users to aggregate security findings from a number of different AWS sources into a central hub. This allows security teams to take actions via investigations or automated responses.

In Short: A cloud security posture service that performs automated security best practice checks.

More Info: https://aws.amazon.com/security-hub/



Amazon Guard Duty

Integration point for AWS security services to allow AWS users to conduct audits or automate security actions

AWS CloudTrail

What is it and what should I enable it?

CloudTrail enables AWS cloud administrators to track user activity (API calls). CloudTrail is a critical service for security of your AWS cloud.

CloudTrail enables you to tack:

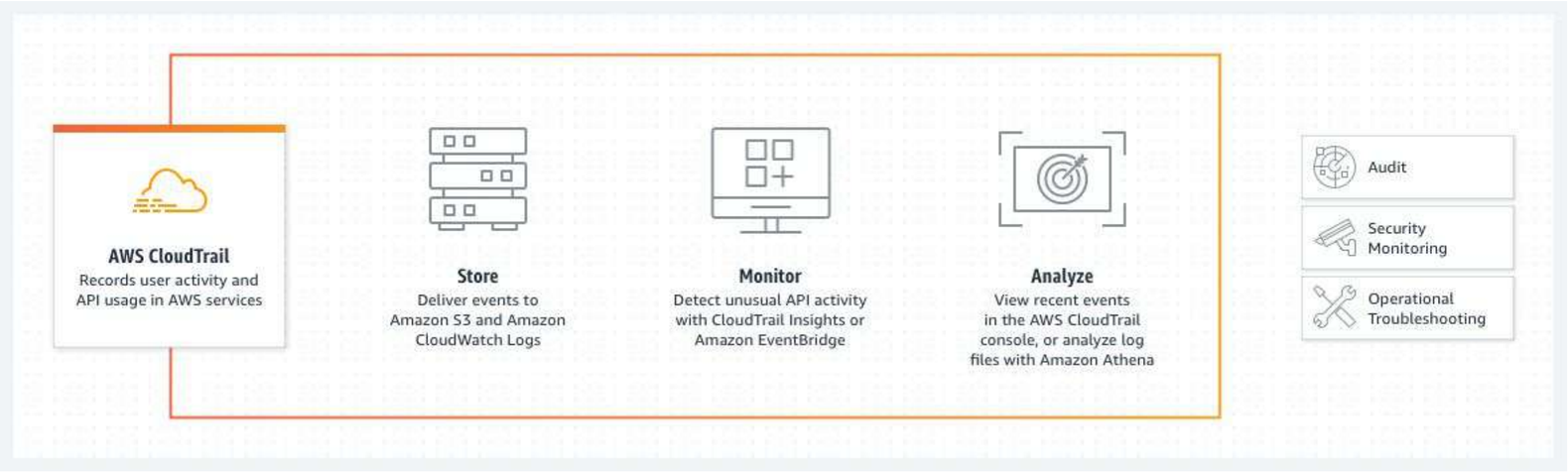
Management events: Control plane actions such as creating S3 bucket

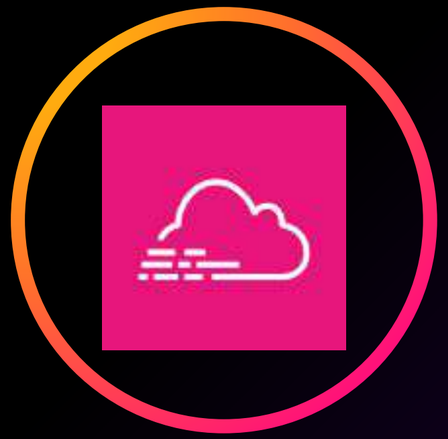
Data events: Data plane actions such as reading and writing to S3

Insight events: Identity and response to unusual activity with API calls

In Short: When a user interacts with an AWS account that usage (API call) is logged to either a local or centralised audit account.

More Info: https://aws.amazon.com/cloudtrail/





AWS CloudTrail

Track usage of your AWS account(s) to enable better auditing, compliance and security on your AWS account or organization

Exercise 3

Cloudwatch Logs

Amazon CloudWatch

What is it and should I ingest into Splunk?

- Monitors AWS resources and the applications you run on AWS in real time.
- Collect and track metrics and logs for your resources and applications and ingest into Splunk
- Use Amazon Data Firehose to push Cloudwatch data into Splunk

https://docs.aws.amazon.com/cloudwatch/

Example Amazon CloudWatch in Splunk

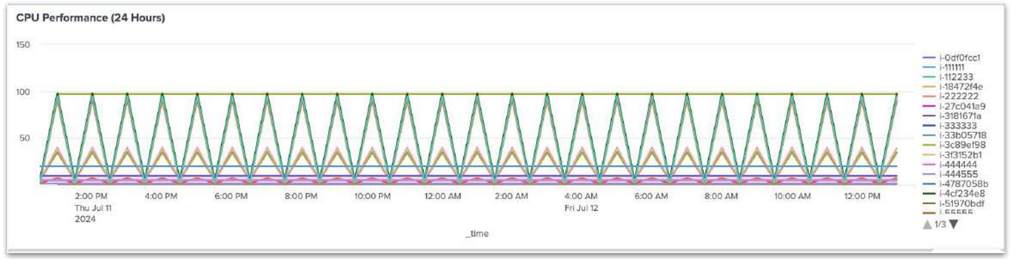
IT Operations Team

Monitor CPU performance for instances in your AWS Account

Tasks

1. Explore Cloudwatch data in Splunk
2. Monitor CPU performance for all instances in account
3. Create line chart to show performance for last 60 minutes & 24 hours
4. Add your chart your dashboard

Goal



Dig into Amazon CloudWatch

```
sourcetype=aws:cloudwatch
```

i	Time	Event
>	7/12/24 1:37:12.000 PM	{ [-] Average: 0.4 Maximum: 1 Minimum: 0 SampleCount: 5 Sum: 2 Unit: Count account_id: 063605715280 metric_dimensions: FunctionName=[hello-world-lambda6],Resource=[hello-world-lambda6] metric_name: Errors period: 300 timestamp: 2024-07-12T13:37:12Z } Show as raw text host = 127.0.0.1 | source = ap-southeast-1:AWS/Lambda | sourcetype = aws:cloudwatch

Investigate Amazon CloudWatch

```
index=main sourcetype="aws:cloudwatch"
```

Explore the logs and look for interesting fields

Monitor CPU performance

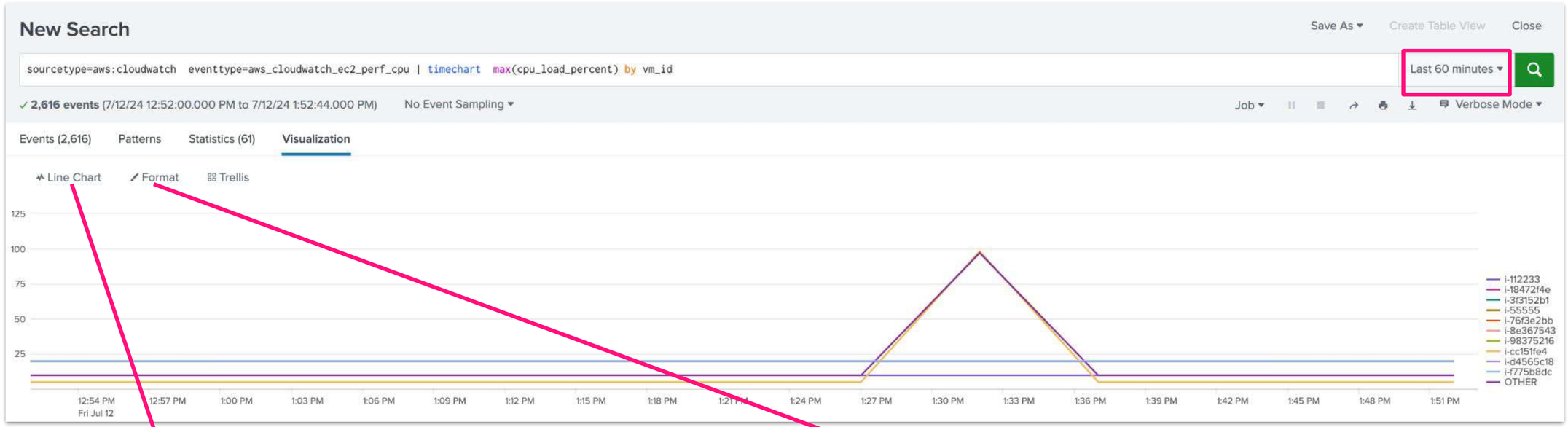
```
sourcetype=aws:cloudwatch  eventtype=aws_cloudwatch_ec2_perf_cpu
| timechart max(cpu_load_percent) by vm_id
```

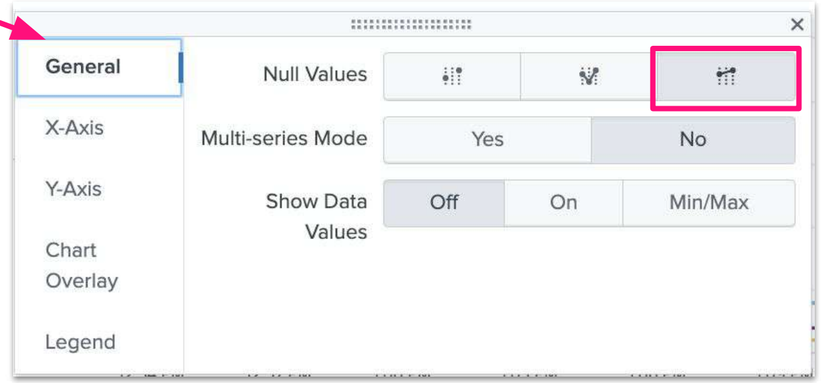
Monitor CPU Performance

20 Per Page ▾ Format Preview ▾

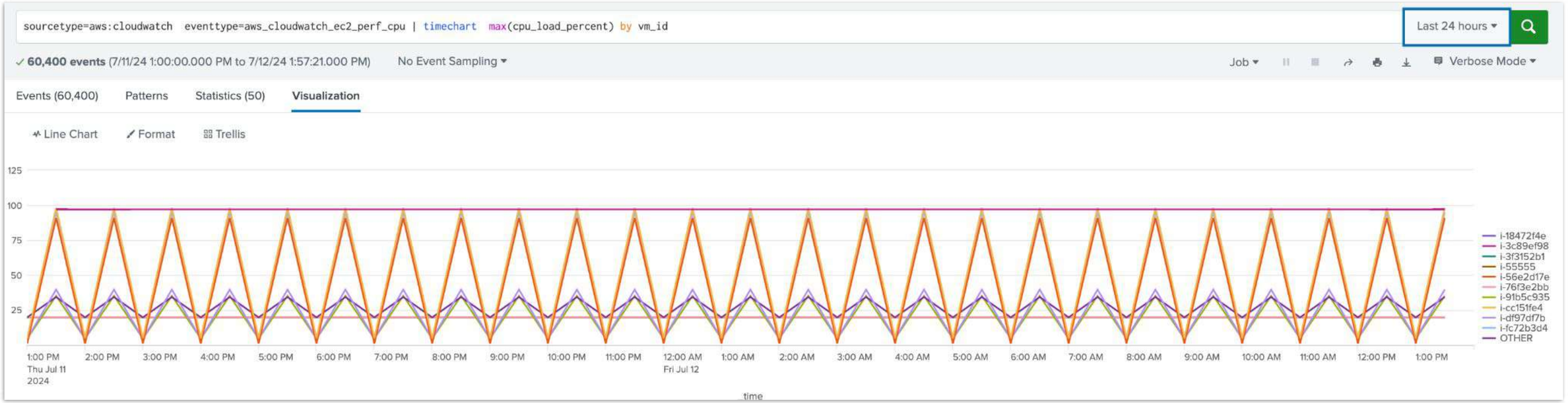
_time	i-18472f4e	i-3c89ef98	i-3f3152b1	i-55555	i-56e2d17e	i-76f3e2bb	i-91b5c935
2024-07-11 13:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 13:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 14:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 14:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 15:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 15:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 16:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 16:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 17:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 17:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 18:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 18:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 19:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 19:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 20:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 20:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000
2024-07-11 21:00:00	19.78333333328677		19.78333333328677	19.78333333328677	1.120312794434308	19.78333333328677	4.518306010928476
2024-07-11 21:30:00	19.78333333328677	97	19.78333333328677	19.78333333328677	90.870000000000000	19.78333333328677	35.180000000000000

Visualize CPU Performance in a Line Chart

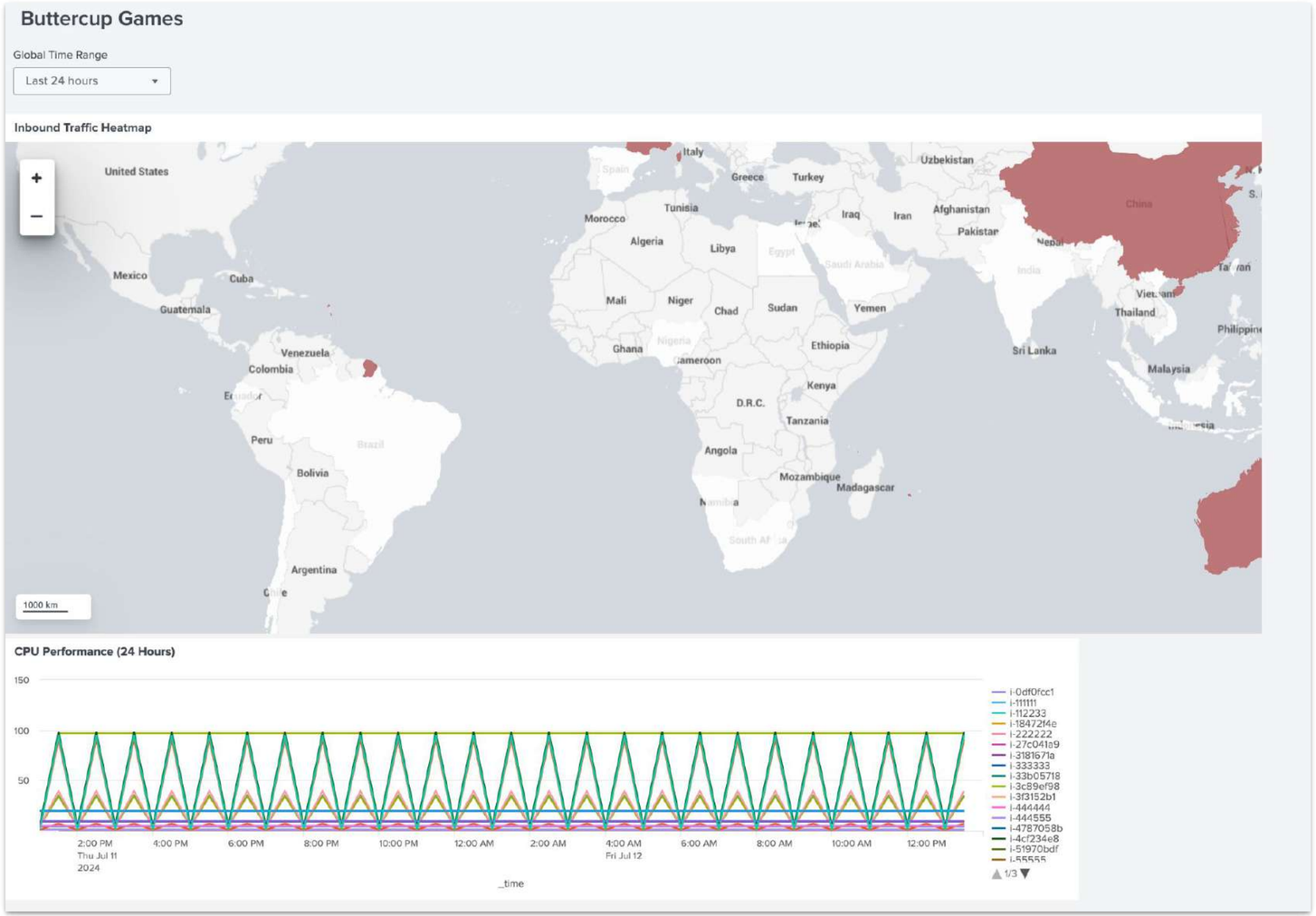




Create 24 Hour View



Add to dashboard



Demo

- Splunk Add-On for AWS
- Splunk App for AWS Security
- Splunk IT Essentials Learn

Apps and Add-ons

- 2100+ free apps and add-ons available from https://splunkbase.splunk.com/
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs

Apps

Content designed to bring fast time-to-value from your data in Splunk, including pre-built dashboards, reports, alerts, visualisations and workflows

Add-ons

Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

Splunk Resources

Where to go after today's workshop

Splunk Events

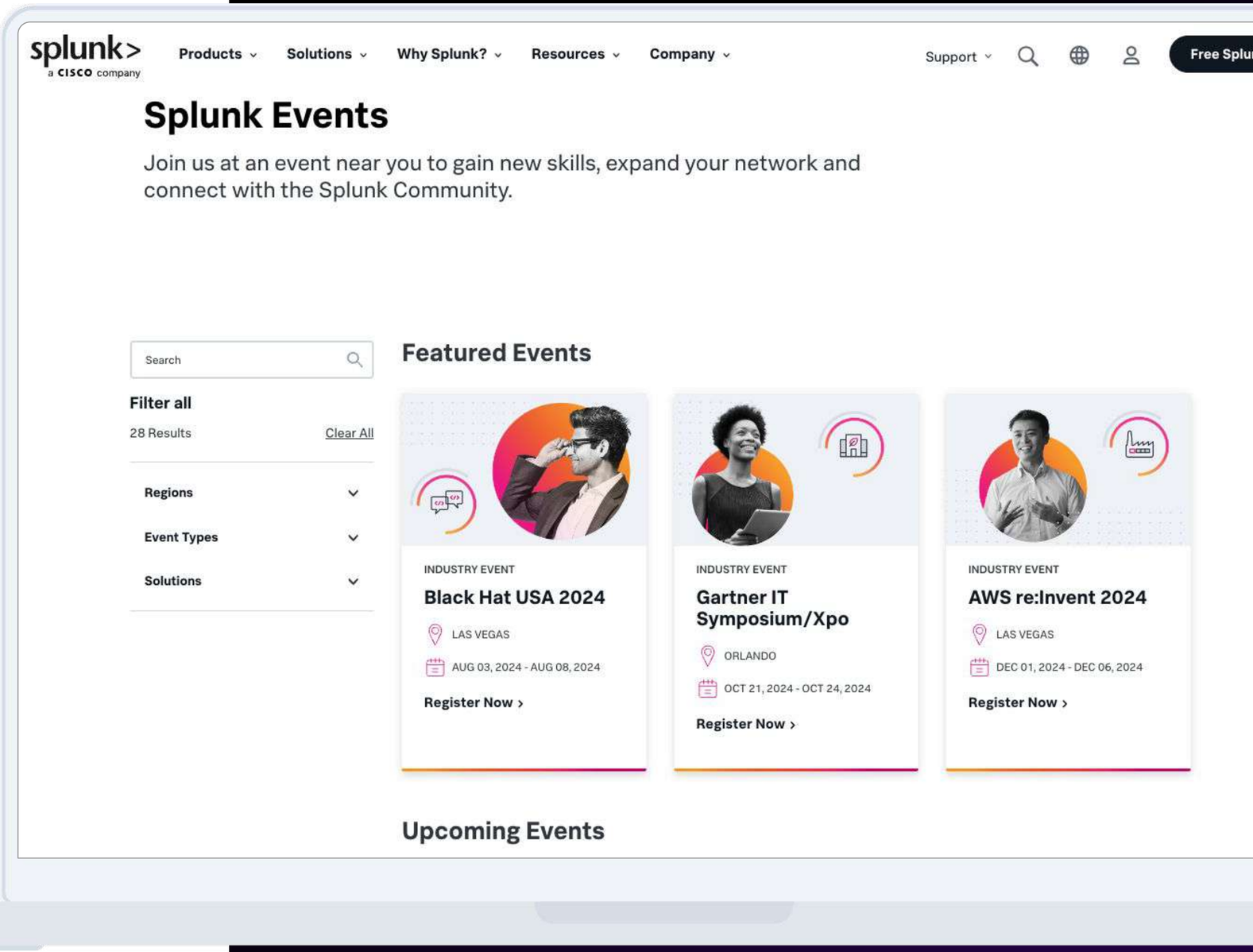
https://splunk.com/events

- Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

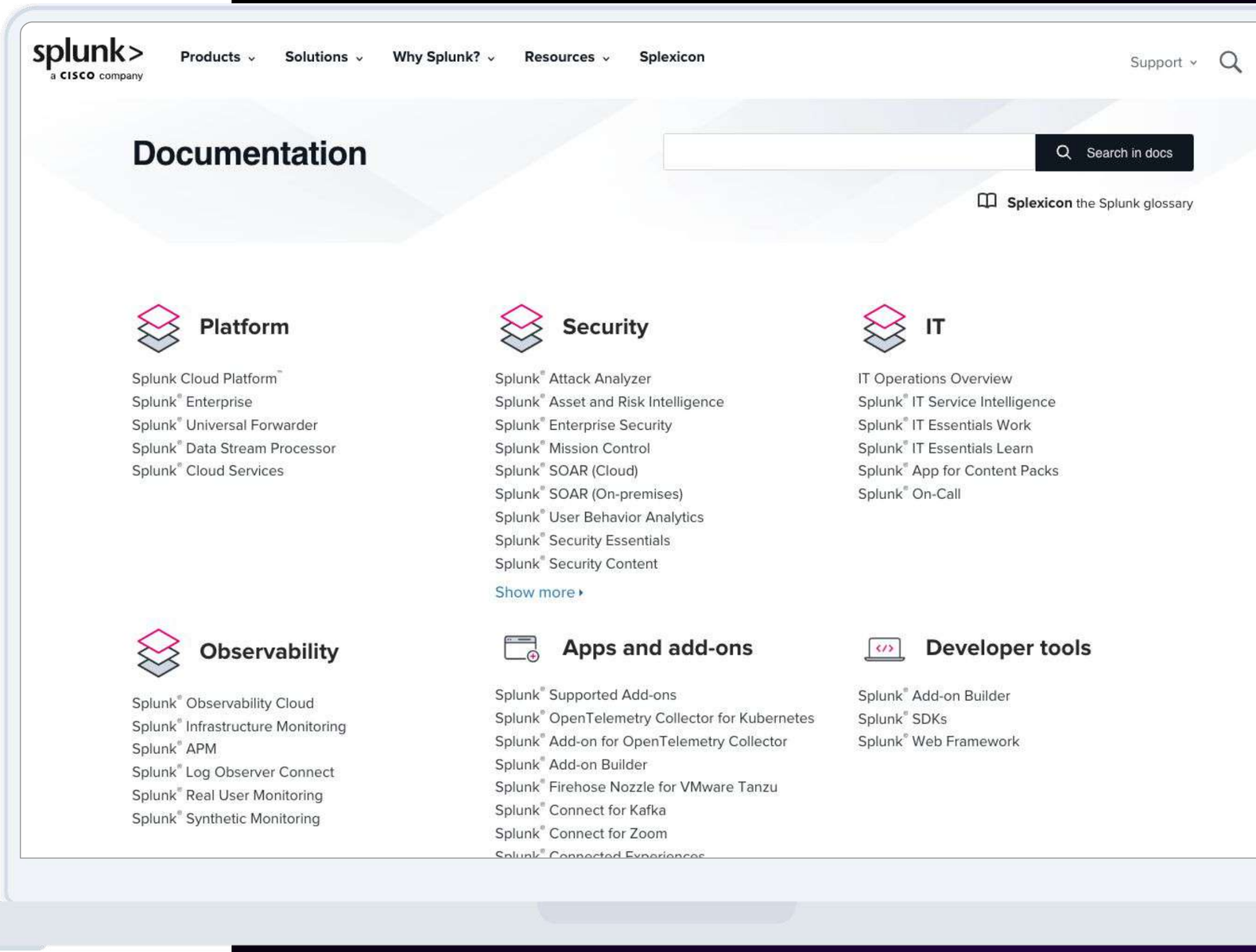
- Join us at .conf!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



Documentation

https://docs.splunk.com

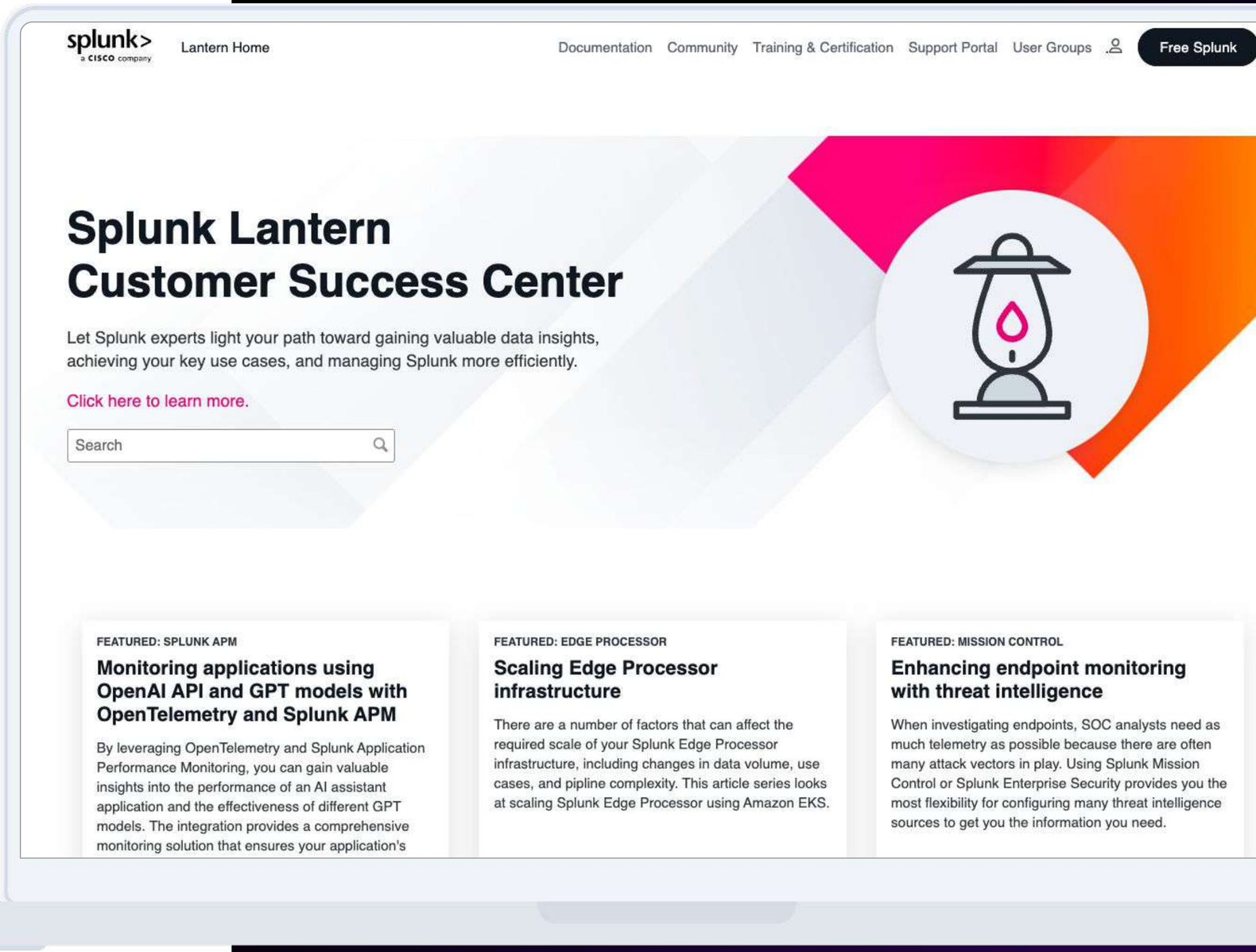
- Search reference for SPL
- Step-by-step tutorials
  Search:
  https://splk.it/SplunkSearchTutorial
  Dashboard Studio:
  https://splk.it/SplunkDashStudioTutorial
- Product references
- Procedures/guides
- And more!



Splunk Lantern

https://lantern.splunk.com

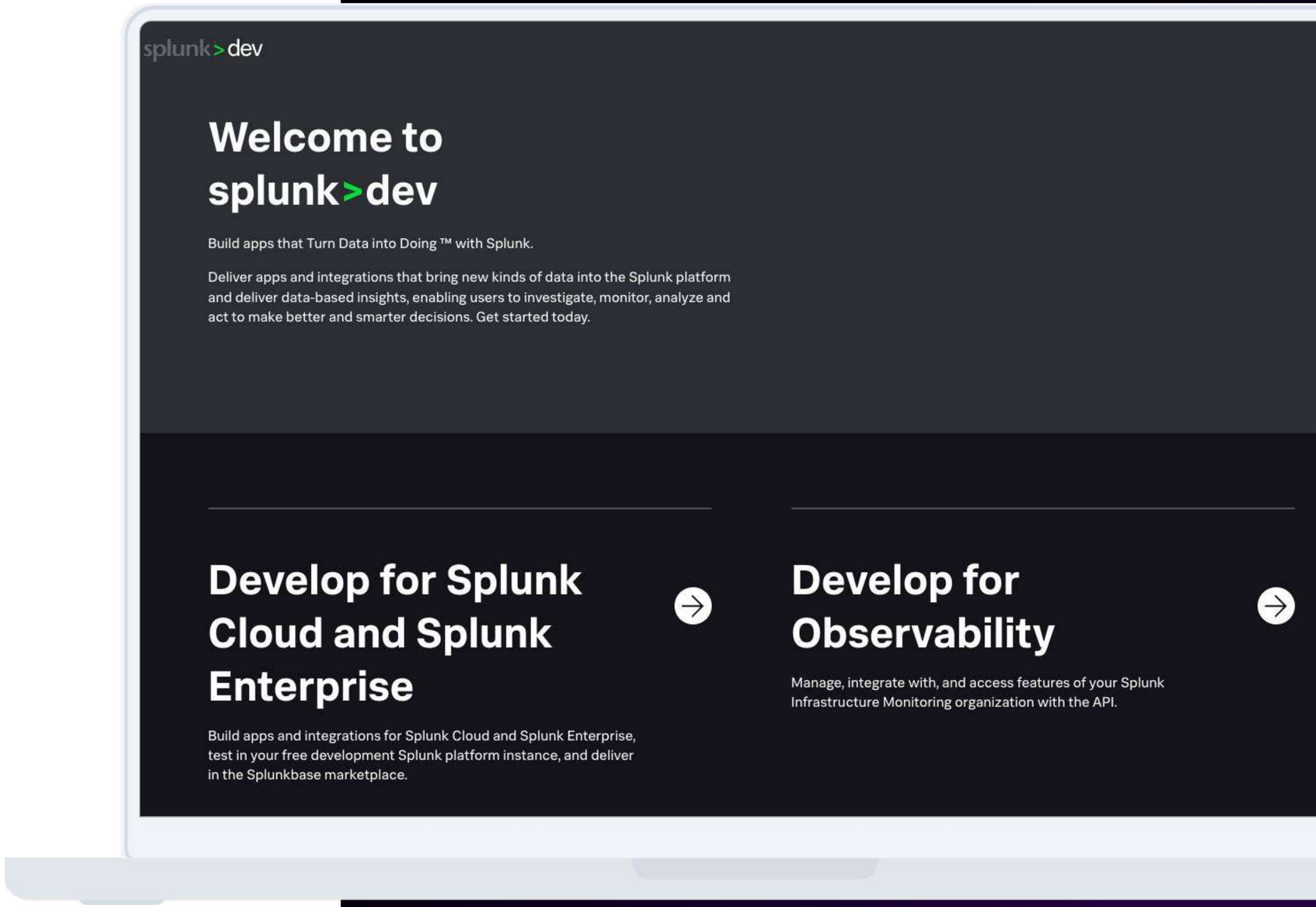
- Use case library
- Product tips
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to increase the value of Splunk across your organisation



Developer Resources

https://dev.splunk.com

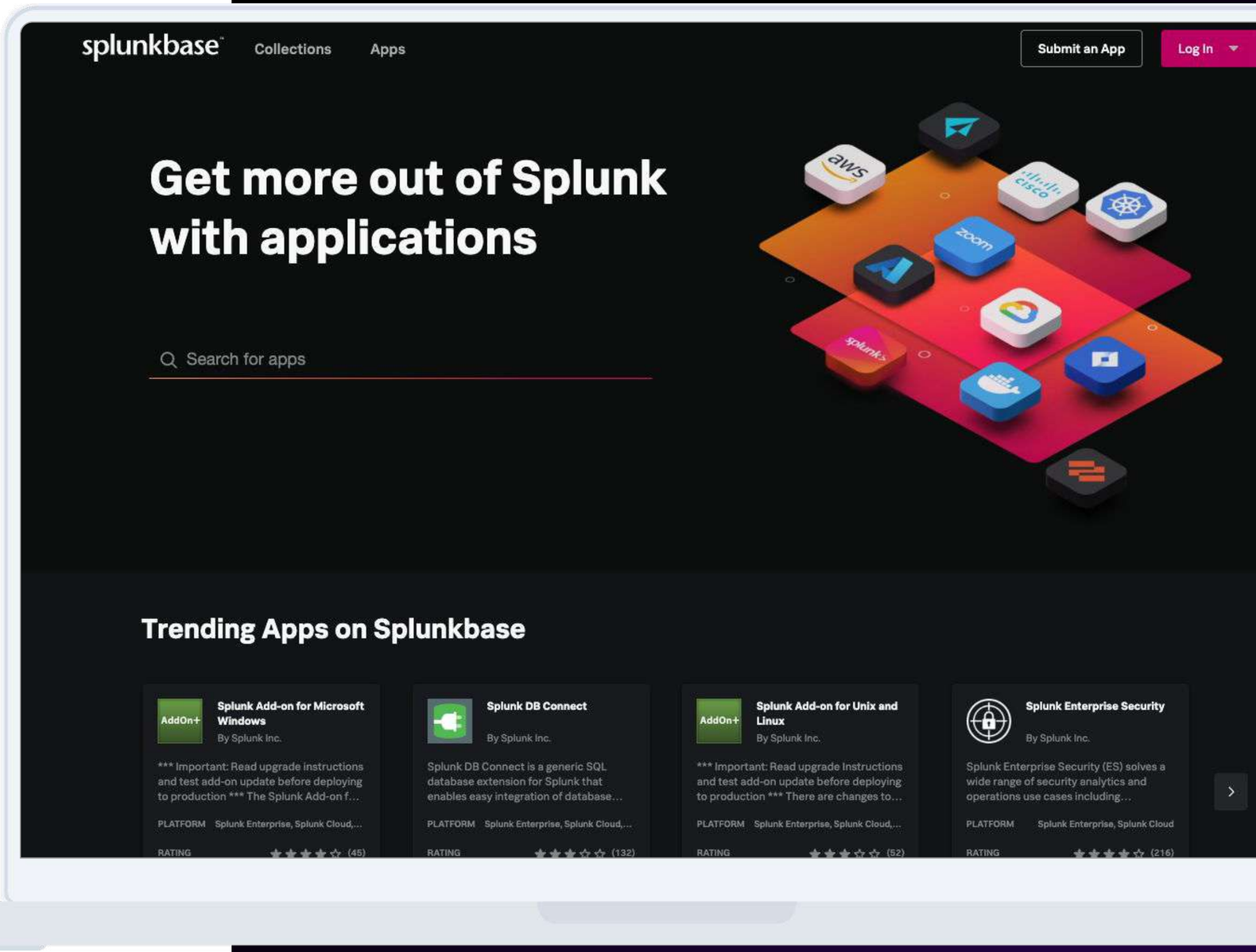
- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

https://splunkbase.splunk.com

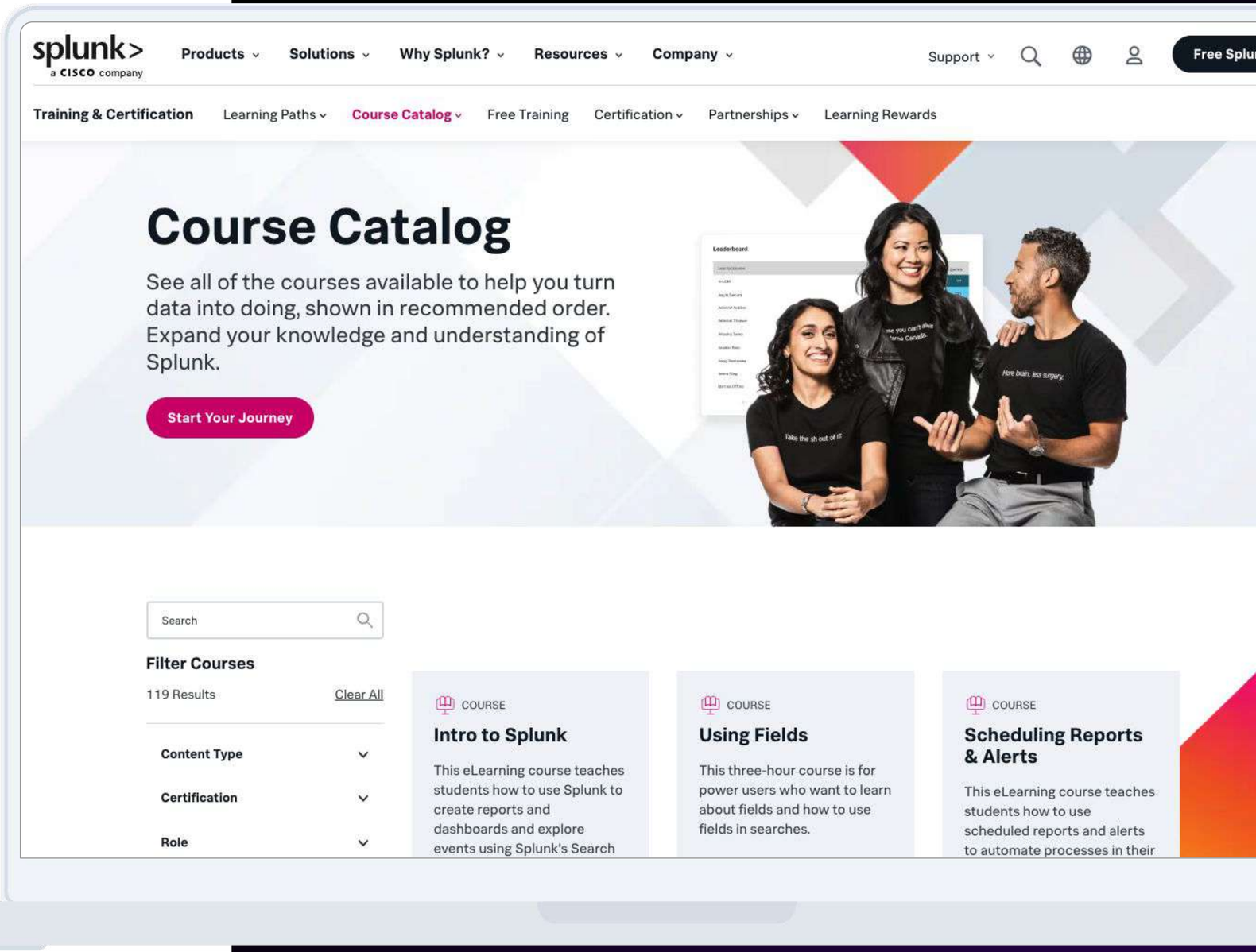
- 2100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



Training & Certification

https://splunk.com/training

- Online education classes
  Instructor-led and self-paced eLearning
- Certification tracks for different roles
  User, Power User, Admin, Architect and Developer
- Splunk Education Rewards
  Complete training and receive points that you can redeem for Splunk swag!
- Free education!
  Single-subject eLearning courses to kick start your Splunk learning



Thank you

splunk> a CISCO company