

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Splunk Platform Insights

A Guide for Network Engineers

Russell Uman
Cloud Staff Solutions Architect – Splunk Singapore
BRKGEN-1624

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKGEN-1624>

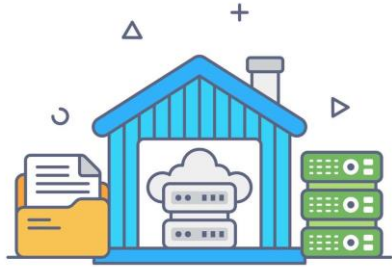


Splunk turns data into actions by making machine data accessible, usable and valuable

What is Splunk?

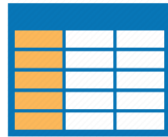
How do we help?

Data Classification

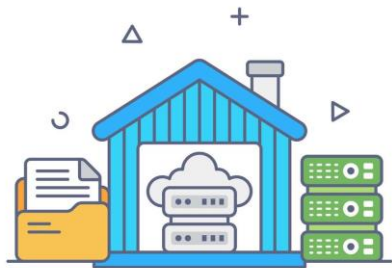


Data Warehouse

- Business
- Reporting

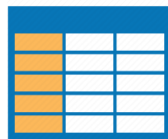


Data Classification



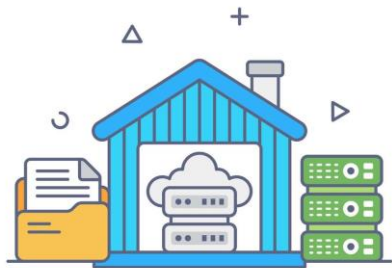
Data Warehouse

- Business
- Reporting



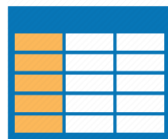
Files and Documents

Data Classification

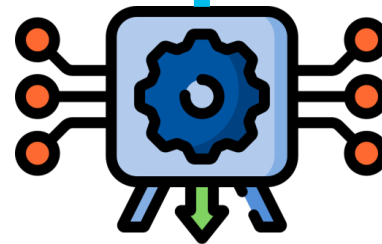


Data Warehouse

- Business
- Reporting



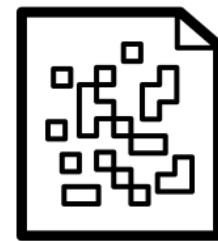
Files and Documents



Machine Data

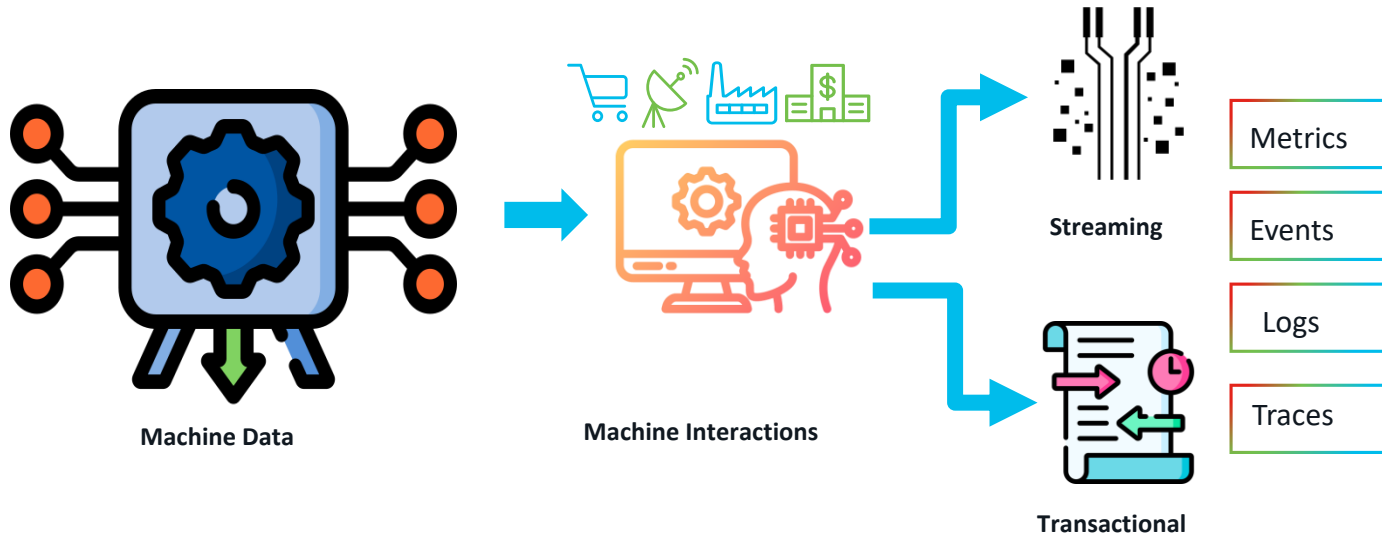
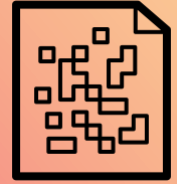


Messy



Unstructured

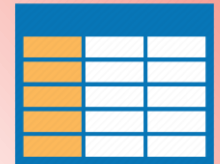
Machine Data “Valuable Complex Data”



Unstructured

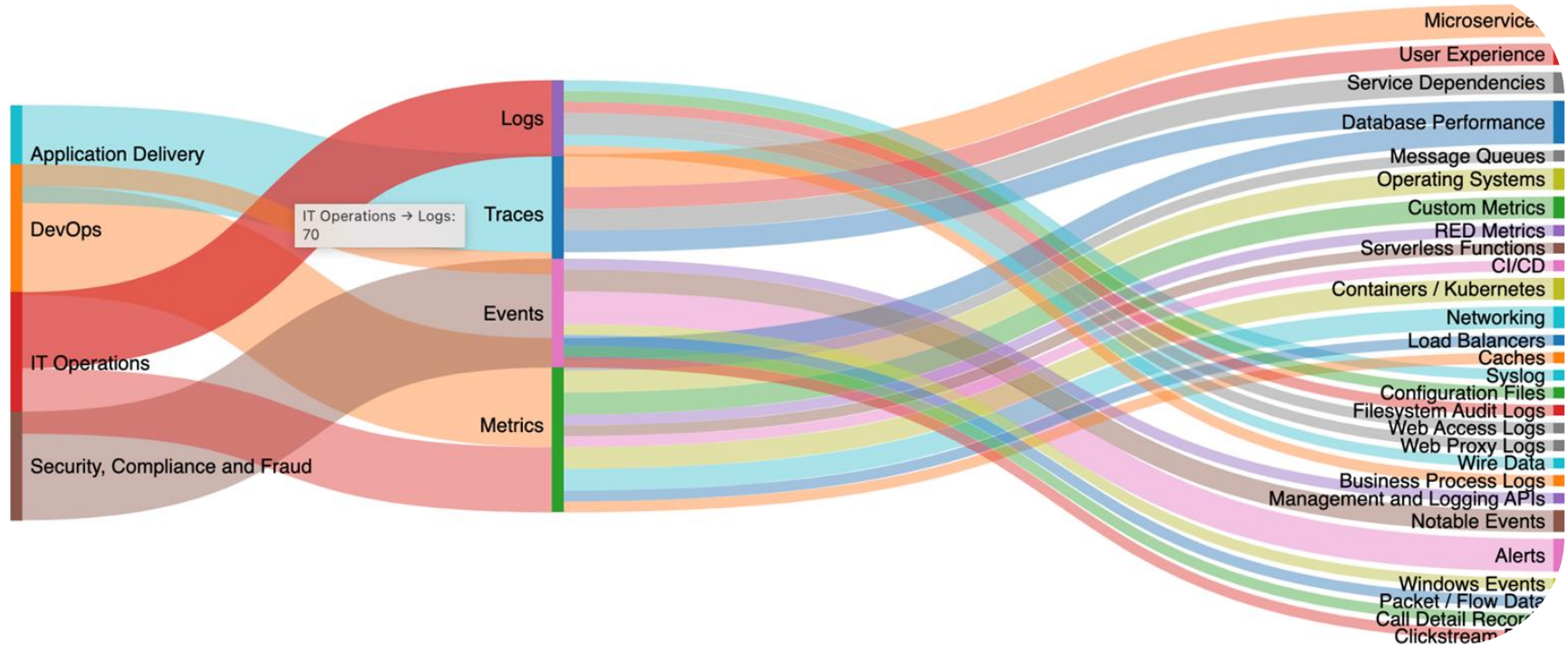


Messy



Structured
Semi - Structured

Multiple Use Cases On Common Data

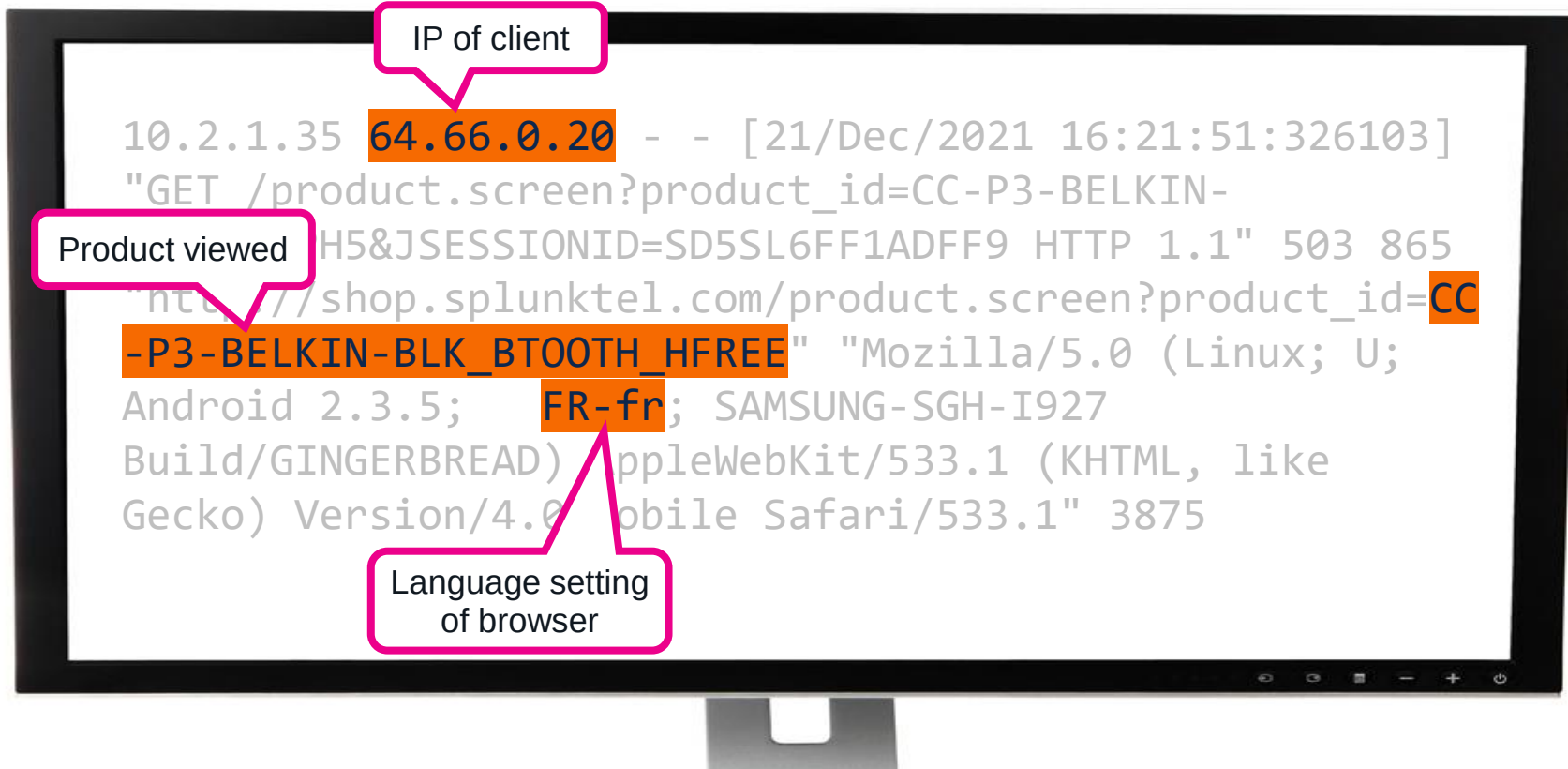


Machine Data is ~~Complex~~ VALUABLE!

```
10.2.1.35 64.66.0.20 - - [21/Dec/2021 16:21:51:326103]
"GET /product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
"http://shop.splunktel.com/product.screen?product_id=CC-
P3-BELKIN-BLK_BT00TH_HFREE" "Mozilla/5.0 (Linux; U;
Android 2.3.5; FR-fr; SAMSUNG-SGH-I927
Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1" 3875
```

Marketing Use Case:

Show the top products viewed by language



DevOps Use Case: Which mobile handsets should I test the most before releasing my new app?

```
10.2.1.35 64.66.0.20 - - [21/Dec/2021 16:21:51:326103]
"GET /product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
shop.splunktel.com/product.screen?product_id=CC
-P3-BELKIN-BLK_BT00TH_HFREE" "Mozilla/5.0 (Linux; U;
Android 2.3.5; FR-fr; SAMSUNG-SGH-I927
Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1"
```

Platform

Handset model

IT Operations Use Case: Which web pages are generating the most errors?



Splunk, since
2003.

CISCO *Live!*





Founded by 3 geeks (Rob, Michael and Erik)

Vision to make a tool to manage massive amount of machine logs as simple as you searching it on a webpage (GOOGLE FOR LOG SEARCH)

Splunk SIEM : Enterprise Security Launched

First premium app was launched to provide advance security data analytics and SIEM

Major feature updates across platform, security and o11y space

Data streaming was launched

Splunk Cloud Launched

O11y Cloud Launched



2003

2006

2012

2011

2013

2020

2024



Splunk 1.0 Launched

Splunk launched its first product, Splunk 1.0. It was marketed as a search engine for log files and machine data, enabling users to troubleshoot and monitor their IT systems.



Evolution of product : Splunk 1.0 to Splunk 4.0

- SPL Language for advance analysis
- Index optimisation for scale
- Data manipulation based searches
- Analytics and real time search
- Distributed search
- Splunk app base launch and APPS GENERATION AT SCALE STARTED

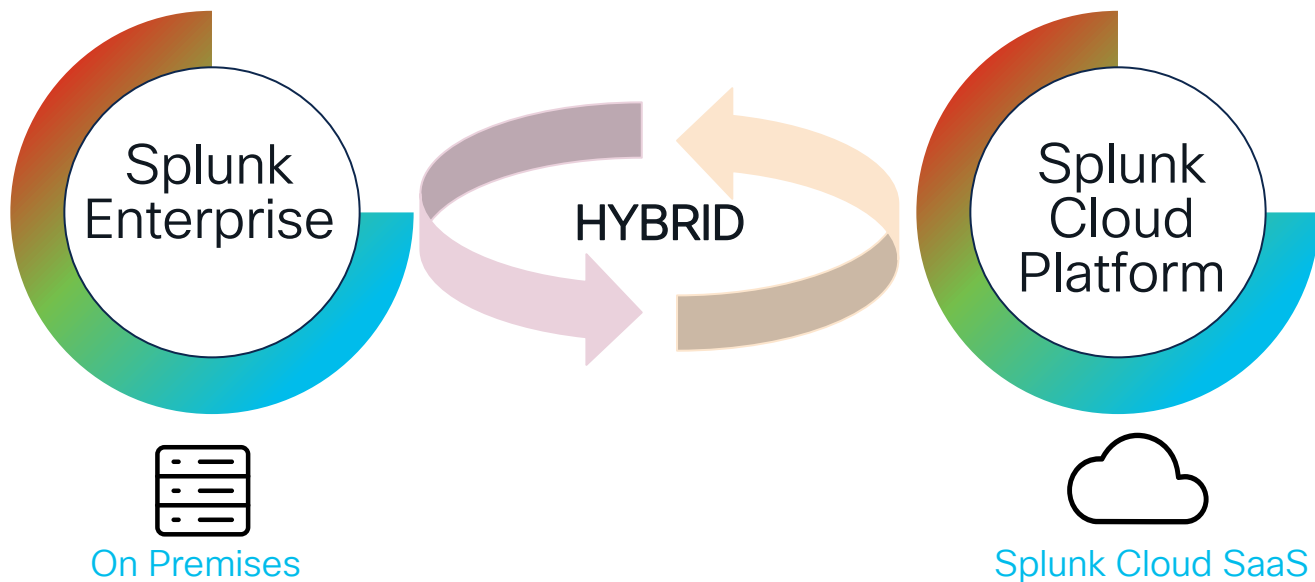
Product Evolution & Market Leadership

- ITSI Launched
- More than 8 acquisitions made (Phantom, SignalFx, Rocana etc)
- Emerged as technology leader in security, ITOps and o11y
- Splunkbase grown from 400 to 1800 apps
- Reached PB / day scale milestone

CISCO Live!

Splunk Platform

Deployment Choices



Splunk's way of
doing things.

CISCO *Live!*



Getting data in.

CISCO *Live!*



Forwarders

Universal Forwarder

- Inputs
 - File reader
 - Network (TCP/UDP)
 - Simple scripts
- Outputs
 - Splunk2Splunk
 - HEC
 - Raw/Syslog

Heavy Forwarder

- Data Collection
 - Complex scripts (modular inputs)
 - APIs
 - External databases



Receivers

Heavy Forwarder

- Intermediate forwarder to bridge networks or offload parsing.



Indexers

- Receive data, index data, and search data.
- Most parsing happens on the first receiver.

Splunk Connect For...

Syslog

- Containerized fast/efficient alternative to UF + Syslog server.

SNMP

- Containerized light-weight collector for SNMP sources.

Kubernetes

- Otel Collector for Kubernetes is a Helm chart that simplifies sending logs and metrics to K8s clusters to Splunk and Splunk IM.

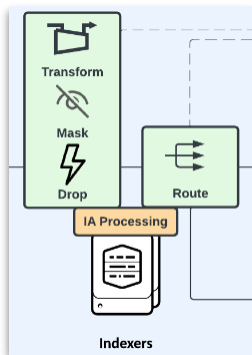
Splunk Stream

- Full-featured collector for network events
 - Passively capture streams of network data
 - Capture metadata and full packet streams for multiple network protocols
 - Collect NetFlow protocol data
- Runs as a component of a forwarder to collect local network data
- Runs as a stand-alone collector to capture wire data.

Ingest Actions

Transform & Control

Your Data



→Mask
→Filter & Drop
→Enrich
→Route
(Splunk, 3rd parties)

Create New Ruleset

ruleset_syslog

Clean up syslog and route to S3

Event Stream: syslog 33KB

Mask with Regex: // 0% | 33KB

Masking alters data that is to be indexed

Match Regular Expression: (user root)

Replace Expression: Enter a string value

Use [] etc to reference capture groups

Apply

+ Add Rule

Data Preview for Mask

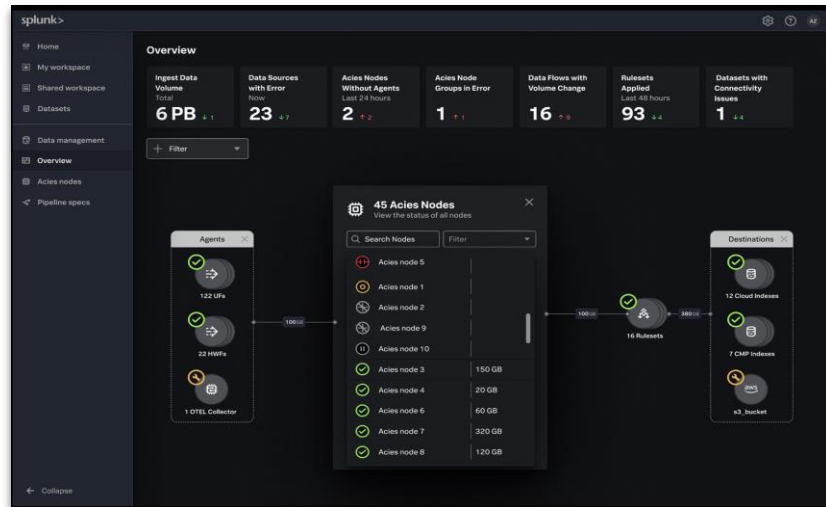
Time	Event	source	sourcetype
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Starting Session 196149 of user root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Started Session 196149 of user root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Starting User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Created slice User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Stopping User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Removed slice User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Starting Session 196147 of user root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Started Session 196147 of user root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Started Session 196146 of user root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Starting User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Created slice User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog
10/18/2021 9:09:32.000 AM	Oct 18 09:09:32 fool20 system: Stopping User Slice of root.	/localhome/abath/cluster_shc/splunk/var/spool/splunk/messages.log	syslog

Final Destination: Splunk Ingestion... 33KB

Edge Processor

Centrally managed next-generation data processor at the Edge.

- **Customer-managed edge instances** for ingest processing –Single command line deployment on hosts of your choice
- **Cloud-based control** plane for simple authoring and pipeline deployment
- Easy to author data processing **pipelines** with **data preview**
- **Visibility** of inbound and outbound streams, with metrics
- Serves as “**Intermediate Forwarding Tier**” for customers who need ingest processing at the edge

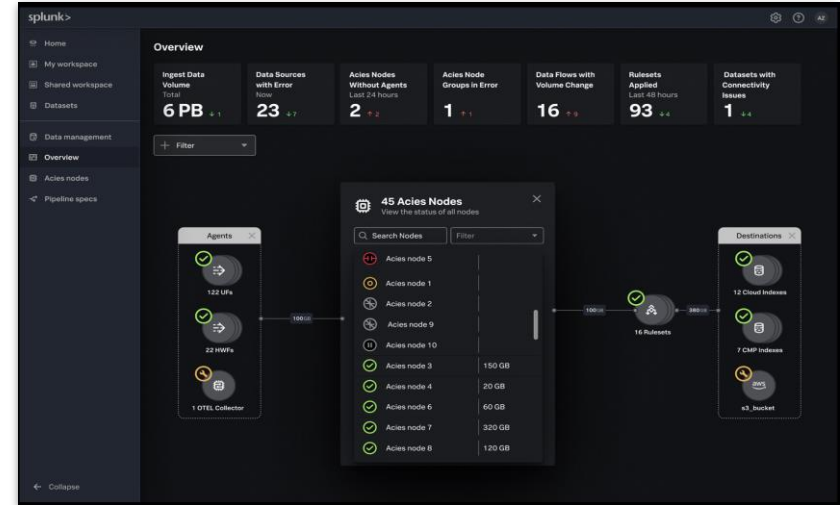


- Available to **Splunk Cloud customers** and supports both **Cloud and Enterprise deployments**
- **Supported processing**: filter, enrichment, transform, drop & routing
- **Supported data sources**: UF/HWF, HEC, Syslog
- **Supported destinations**: Splunk® Cloud Platform, Splunk® Enterprise, Amazon S3

Ingest Processor

Fully-managed next generation data processor

- Send data directly to Ingest Processor service.
- Easy to author data processing pipelines with **data preview**
- **Visibility** of inbound and outbound streams, with metrics



- Available to **Splunk Cloud customers** and supports **Cloud deployments**
- **Supported processing**: filter, enrichment, transform, drop & routing
- **Supported data sources**: UF/HWF, HEC, Syslog
- **Supported destinations**: Splunk® Cloud Platform, Splunk® Enterprise, Amazon S3

Data indexing.



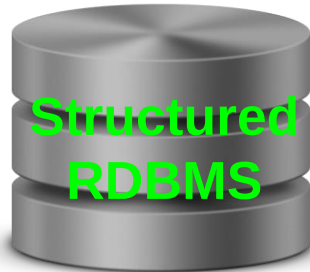
Splunk Approach to Machine Data

Traditional

Schema at Write

SQL

ETL



Splunk

Schema at Read

Search

Universal
Indexing

Unstructured
&
Structured

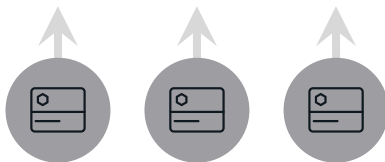
Volume Variety

Scales to PBs/Day

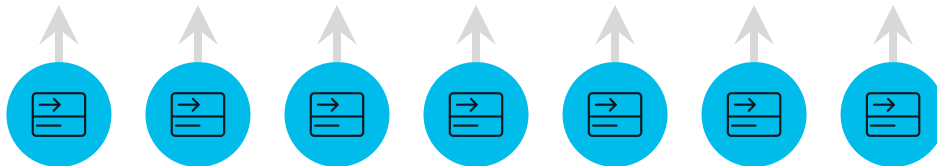
Enterprise-Class Scale, Resilience and Interoperability



Aggregate search results to **Splunk Search Heads**

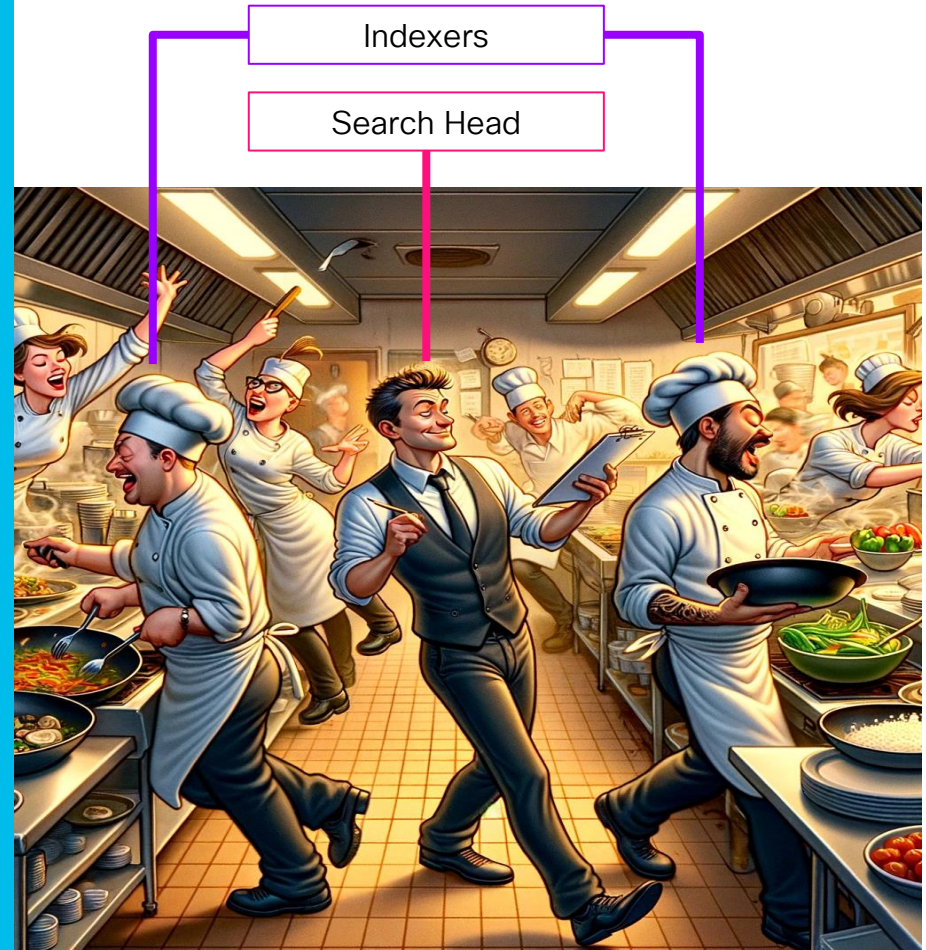


Auto load-balanced forwarding to **Splunk Indexers**



Send data from thousands of servers using any combination of **Splunk Forwarders**

Recipe to scale cooking process



Inside Universal Indexing

```
> 1/5/16 175.45.177.17 - - [05/Jan/2016 13:28:55:845080] "POST /search.php?1 AND (SELECT * FROM hr_employee_inf
1:28:55.845 PM D3SL1FF7ADFF9 HTTP 1.1" 504 44346 "http://m.acme.com/search.php?1 AND (SELECT * FROM hr_employee_info)
OS X; en_US) AppleWebKit (KHTML, like Gecko) Mobile [FBAN/FBForIPhone;FBAV/4.0.3;FBBV/4030.0;FBDV/iPhon
R/Pelephone;FBID/phone;FBLC/en_US;FBSF/2.0]" 9716
clientip = 175.45.177.17 | host = webserver-02 | source = /opt/apache/log/access_combined.log | sourcetype = access_combined
useragent = mozilla/5.0 (iPhone; U; CPU iPhone OS 5_0_1 like Mac OS X; en_US) AppleWebKit (KHTML, L...

> 1/5/16 175.45.177.7 - - [05/Jan/2016 13:28:55:807662] "POST /search.php?|((SELECT password FROM SYS.USERS WHERE
1:28:55.807 PM SESSIONID=SD3SL1FF7ADFF9 HTTP 1.1" 503 49818 "http://m.acme.com/search.php?|((SELECT password FROM SYS.
2.3.3; nl-nl; HTC_DesireHD_A9191 Build/GRI40) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile
clientip = 175.45.177.7 | host = webserver-02 | source = /opt/apache/log/access_combined.log | sourcetype = access_combined
useragent = mozilla/5.0 (Linux; U; Android 2.3.3; nl-nl; HTC_DesireHD_A9191 Build/GRI40) AppleWebKit/...

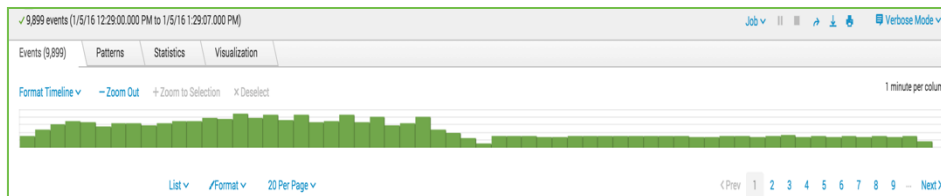
> 1/5/16 175.45.177.17 - - [05/Jan/2016 13:28:55:628252] "POST /search.php?uid=467359b9-48f3-4242-8512-40bcd8a
1:28:55.628 PM p://m.acme.com/<script type='text/javascript'>alert('pwd');</script>" "mozilla/5.0 (Linux; U; Android
```

Automatic event boundary identification

Automatic timestamp normalization

```
> 1/5/16 175.45.177.17 - - [05/Jan/2016 13:28:55:845080] "POST /search.php?1 AND (S
1:28:55.845 PM D3SL1FF7ADFF9 HTTP 1.1" 504 44346 "http://m.acme.com/search.php?1 AND (SEL
OS X; en_US) AppleWebKit (KHTML, like Gecko) Mobile [FBAN/FBForIPhone;FBAV/
R/Pelephone;FBID/phone;FBLC/en_US;FBSF/2.0]" 9716
clientip = 175.45.177.17 | host = webserver-02 | source = /opt/apache/log/access_combined.log
useragent = mozilla/5.0 (iPhone; U; CPU iPhone OS 5_0_1 like Mac OS X; en_US) AppleWebKit (KHTM
```

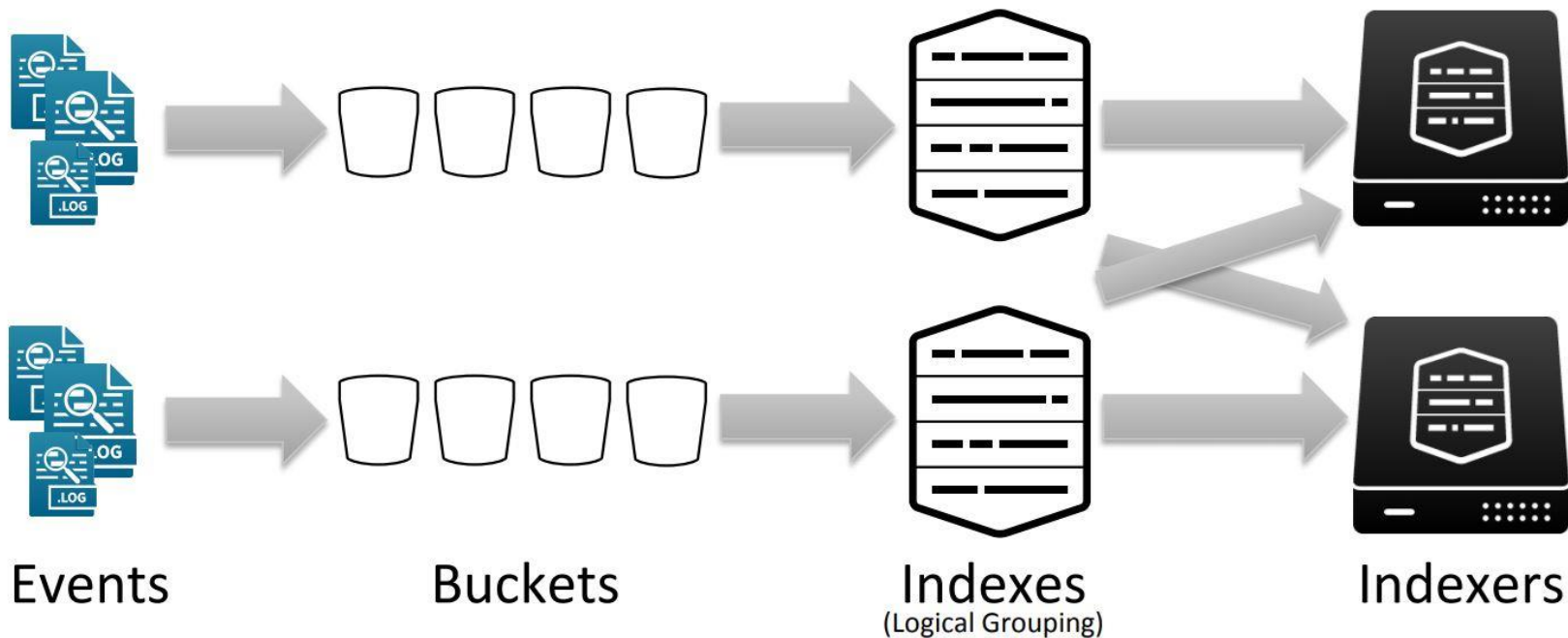
Accurate searching and trending by time across all data



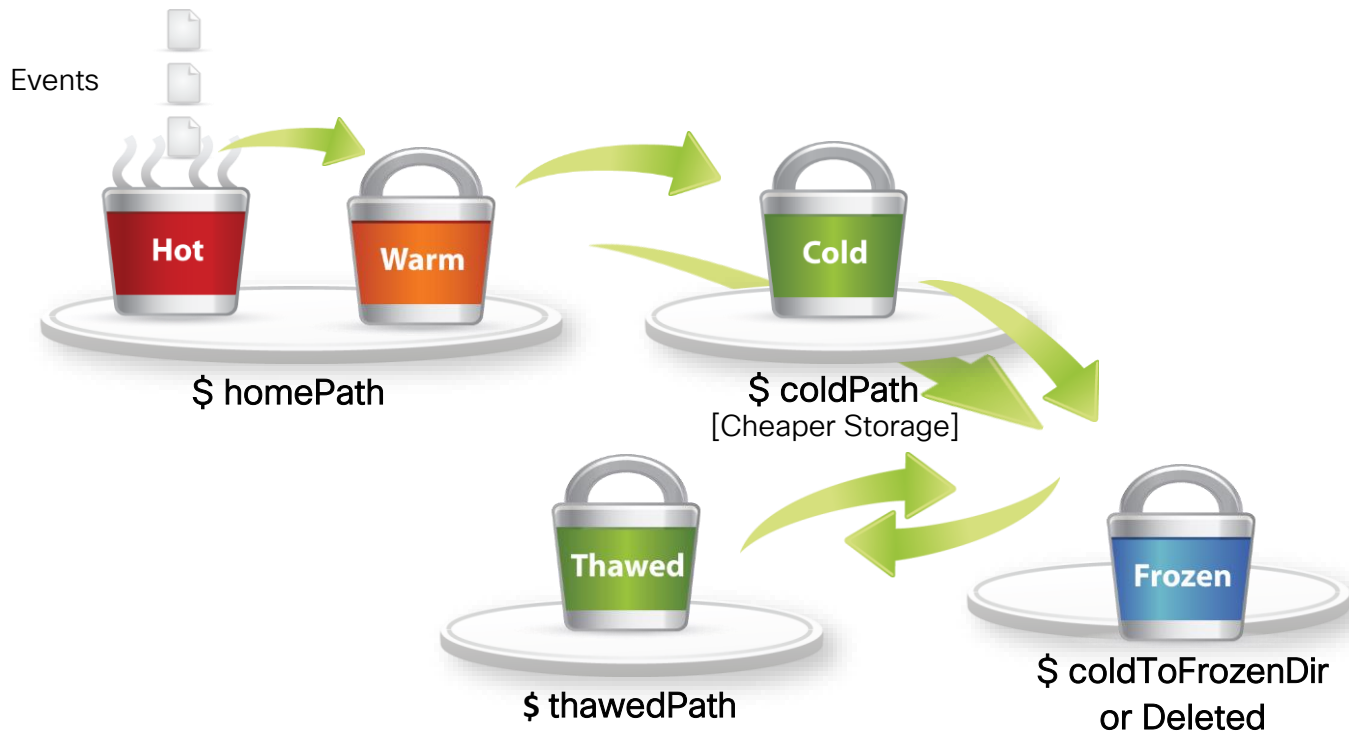
CISCO *Live!*

#CiscoLiveAPJC

How Splunk Stores Data



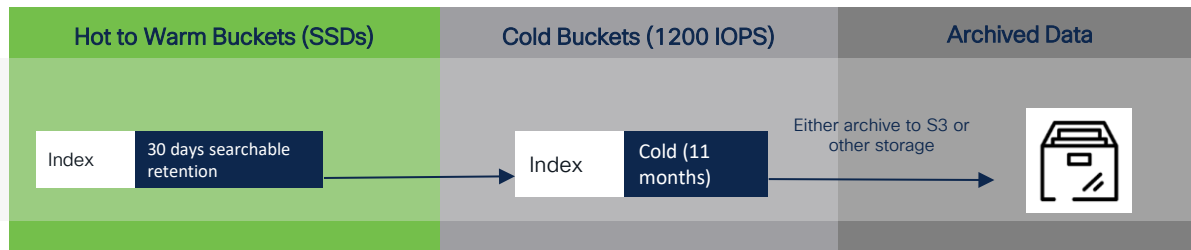
Splunk Storage : Bucket States



Splunk Storage Example

Index Configuration:

- 365 days total
- 30 days hot/warm
- Rest cold for 11 months, archive afterwards



What is in a Bucket



- Your events go here
- Journal.gz is made up of many smaller compressed slices
- Raw data is collected and saved into slices
 - ~128kb of uncompressed data make up a slice.

TSIDX



Time Series Index (C++)

- Inverted index optimized for time
- Two basic components

Lexicon

Arrays of information about events

Why: Given a time range and query, where's my matching data?

Raw Events
Jim likes Mickey
Suzie likes Donald
Pat likes Pluto



Unique terms from the raw events are written to the lexicon

Lexicon		Values Array	
Term	Postings List	Posting Value	Seek Address
Donald	1	0	34
Jim	0	1	87
likes	0,1,2	2	132
Mickey	0		
Pat	2		
Pluto	2		
Suzie	1		



The postings list tells us where we can find a specific term in the values array

The seek address tells us where we can find the matching event(s) in the journal.gz slices

TSIDX : Bloom Filters

Needle in a haystack

- Determines whether a term is likely to exist in the TSIDX of a bucket
 - False positives are possible, false negatives are not

Lexicon

Term
Donald
Jim
likes
Mickey

Each term from the lex is run
through a set of hashing algorithms



The output of each hash
sets a bit in the array to ON



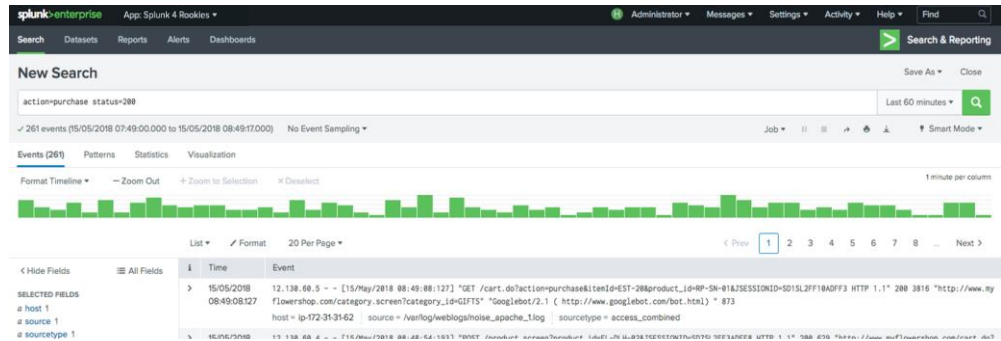
- Regardless of the # of terms, bit array size remains fixed
- Binary format
- Fast to read vs. TSIDX, which grows with more unique terms

Searching,
alerting,
reporting.

CISCO *Live!*



How Search Works



Search

index=world name=waldo glasses=yes | eval miles=km*0.62 | stats count by countries

Last 4 hours



Base Search

Retrieves & filters events

SPL Commands

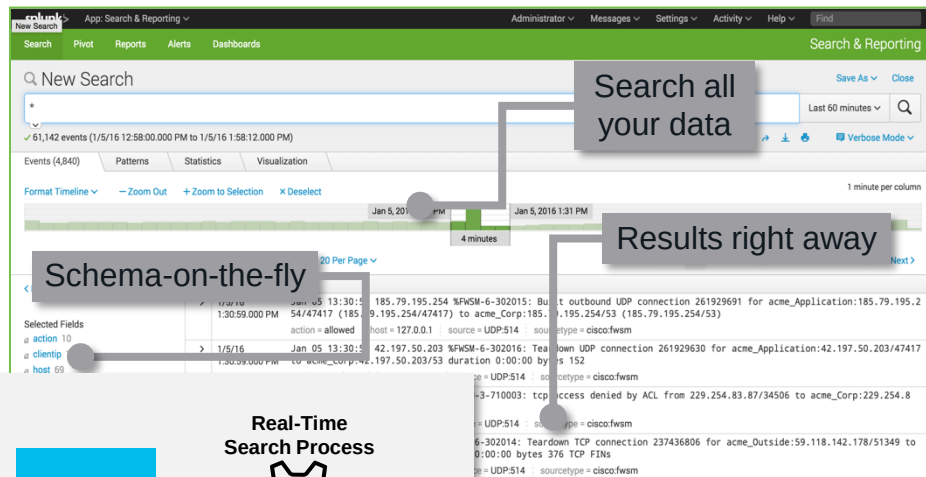
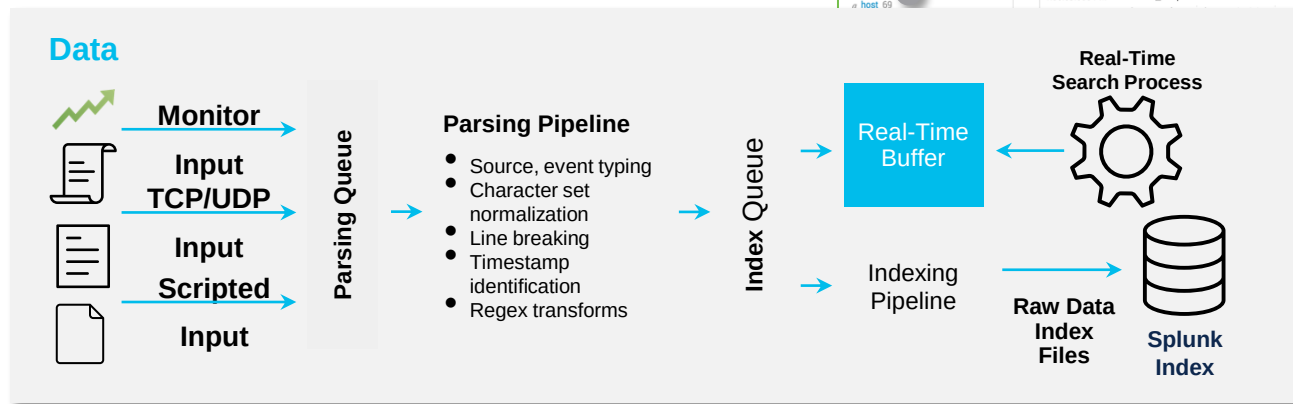
Evaluate, transform, and format events

Events are retrieved

Results move linearly through SPL commands

Search All Your Machine Data

- Real-time and historical data on-premises, in the cloud or both
- Over 200 commands including anomaly detection and machine learning

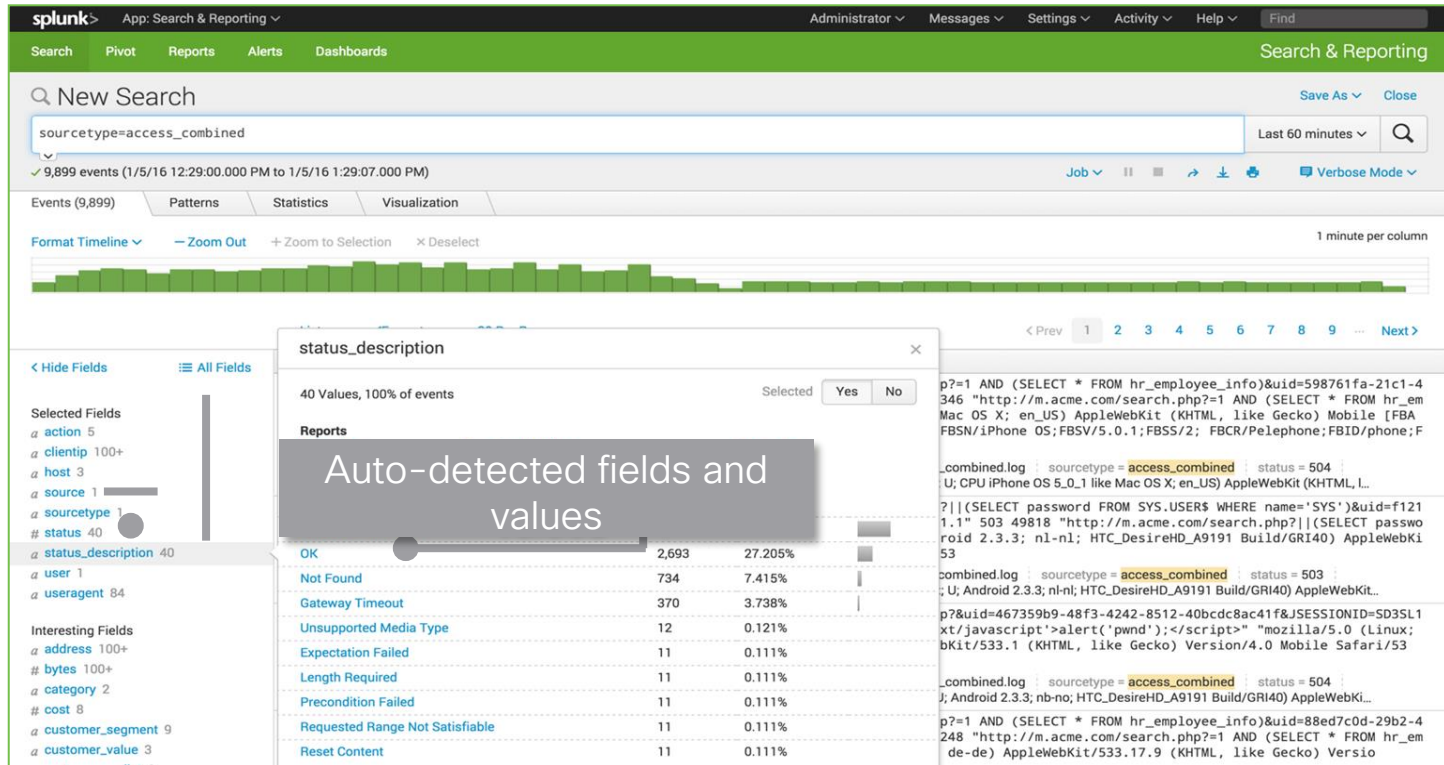


Event Sampling

The screenshot shows the Splunk web interface. At the top, the 'splunk' logo and 'App: Global Events' are visible. Below the navigation bar (Search, Pivot, Reports, Alerts, Dashboards), the 'New Search' section contains the search query 'index=gdelit hack OR breach'. Below the search bar, it indicates '78 events (3/9/14 2:34:49.000 PM to 3/9/16 2:34:49.000 PM)' and a 'Sampling 1 : 1,000' dropdown menu. The dropdown menu is open, showing options: 'No Event Sampling', '1:10', '1:100', '1:1,000' (selected), '1:10,000', '1:100,000', '1:346 (Custom)', and 'Custom...'. Below the search bar, there are tabs for 'Events (78)', 'Patterns', 'Statistics', and 'Visualizations'. The 'Events (78)' tab is active, showing a timeline visualization and a list of events. The list of events shows fields like 'Time', 'Actor1_Type', and 'Actor1Name'. The 'Selected Fields' section on the left lists fields like '# ActionGeo_Lat 57', '# ActionGeo_Long 59', 'a Actor1_Type 14', and 'a Actor1Name 59'.

- Sample Random Events
 - Powerful search option provides unbiased sample results
 - Useful to quickly determine dataset characteristics
 - Speeds large-scale data investigation and discovery

Schema-on-the-Fly



Extract Fields Anytime

Extract Fields

Select sourcetype Select sample **Select fields** Validate fields Save

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match.

web_iis_3 64.27.101.83 - - [18/Sep/2014 10:54:58:000000] "GET /cart.do?action=purchase&itemId=EST-19&product_id=BT-HS-JABRA-WAVE" "http://shop.splunktel.com/product.screen?product_id=BT-HS-JABRA-WAVE" "Mozilla/5.0 (Linux; U; Android 2.3.4; ja-jp; SonyEricc Gecko) Version/4.0 Mobile Safari/533.1" 3726

Show Regular Expression >

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its fields.

Events method status bytes

✓ 1,000 events (before 9/18/14 11:00:45.000 AM)

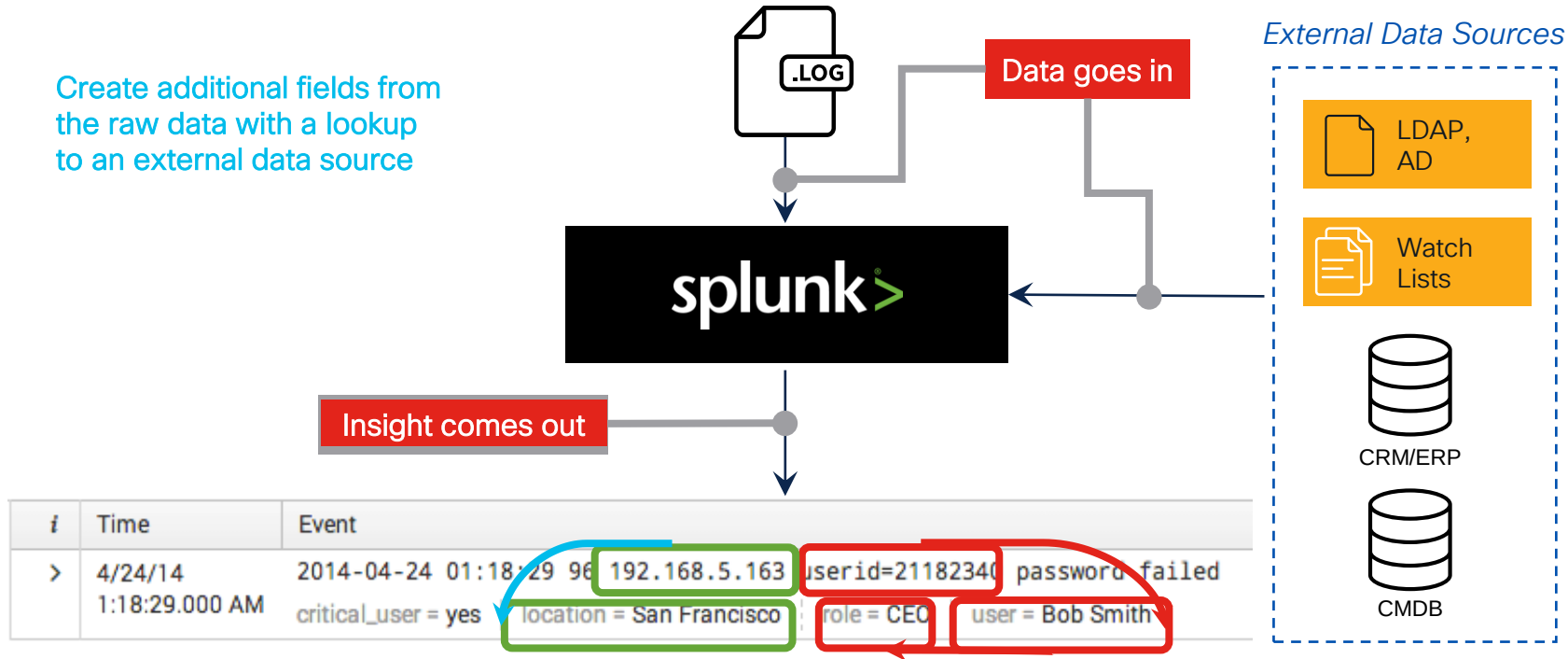
filter Apply Sample: First 1,000 events ▾ All events ▾ All Events Matches Non-Matches

✓ web_apache_2 64.27.101.65 - - [18/Sep/2014 10:56:59:000000] "POST /cart.do?action=purchase&itemId=EST-1&product_id=BA-MOPHIE-JUICEPACKAIR&JSESSIONID=SD3SL1FA700383 HTTP 1.1" 416 935 "http://shop.splunktel.com/product.screen?product_id=BA-MOPHIE-JUICEPACKAIR&JSESSIONID=SD3SL1FA700383" "Mozilla/5.0 (Linux; U; Android 2.1-update1; en-gb; Milestone Build/SHOLS_U2_02.36.0) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Mobile Safari/530.17" 3726

- Simple field extraction
 - Highlight-to-extract multiple fields at once
 - Apply keyword search filters
 - Specify required text in extractions
 - View diverse and rare events
 - Validate extracted values with field stats

Enrich Raw Data to Make It More Meaningful

Create additional fields from the raw data with a lookup to an external data source



Data Preparation & Analysis With Tables

Fast and simple analysis for a wide range of users

The screenshot shows the Splunk Search & Reporting interface. The top navigation bar includes 'App: Search & Reporting', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this is a green header with 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Table Dataset' and includes tabs for 'Preview Rows' and 'Summarize Fields'. A 'Commands' panel on the left shows SPL commands: `index=test`, `sourcetype=access_combined`, `fields="time","bytes","clientip","status","status_description","uid"`, `eval DateTime=strftime(_time, "%A %B %e, %Y %i:%M %p")`, `lookup "customer_info" uid OUTPUT "username","state","city","gender"`, and `eval "username" if(isnull(username), "unknown", username)`. A context menu is open over the 'clientip' field, showing options: 'Change Case...', 'Fill Null or Empty Values...', 'Replace Values...', 'Round Values', 'Remove Non-Numerical Values', 'Bucket...', and 'Eval Expression...'. The table data is displayed in columns: 'DateTime', 'clientip', 'IP', 'status', and 'status_description'. The 'clientip' column has a summary of 12,636 events (before 9/2/16) and a 'Matched type' of 99.87%. The 'IP' column has a summary of 107,115,121,147 and a 'Matched type' of 4.81%. The 'status' column has a summary of 200 and a 'Matched type' of 64.99%. The 'status_description' column has a summary of 1 and a 'Matched type' of 100.00%.

DateTime	clientip	IP	status	status_description
Wednesday, August 24, 2016 01:59	107.115.121.147	4.81%	200	OK
Wednesday, August 24, 2016 01:58	172.144.47.165	0.16%	Not Found	Not Found
Wednesday, August 24, 2016 01:58	114.183.149.172	0.16%	Service Unavailable	Service Unavailable
Wednesday, August 24, 2016 01:58	136.75.232.254	0.15%	Not Implemented	Not Implemented
Wednesday, August 24, 2016 01:57	0.134.99.193	0.13%	Temporary Redirect	Temporary Redirect
Wednesday, August 24, 2016 01:57	11.220.102.13	0.13%	Request-URI Too Long	Request-URI Too Long
Wednesday, August 24, 2016 01:56	152.132.210.188	0.13%	503	Payment Required
Wednesday, August 24, 2016 01:56	182.168.194.196	0.13%	307	Precondition Failed
Wednesday, August 24, 2016 01:55	154.160.48.22	0.13%	501	Created
Wednesday, August 24, 2016 01:55	158.42.245.110	0.13%	414	Gone
Wednesday, August 24, 2016 01:54	84.193.189.163	0.13%	402	Length Required
Wednesday, August 24, 2016 01:54	112.115.55.208	0.12%	412	Unauthorized
Wednesday, August 24, 2016 01:54	115.180.125.217	0.12%	201	Request Entity Too Large
Wednesday, August 24, 2016 01:54	116.22.111.230	0.12%	401	Non-Authoritative Information

- Tabular data views speed analysis for specialist and occasional users
- Intuitive interface to prepare and analyze data without using Splunk Search Processing Language (SPL)

Structured View Into Unstructured Data

ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.com.resource.ResourceException: ResourceDeadException: Could not get connection. The DBMS driver [Oracle JDBC Driver]Error establishing a connection to host and port: ACMEDB-01 (192.168.1.100) Reason: Connection refused

05/21 16:33:11.238 [CUSTID 10098213, ANI T7513ae51a6d092, Trunk T451.16] Failed login

05/21 16:33:11.238 [CUSTID 10098213, ANI T7513ae51a6d092, Trunk T451.16] Webserver ID

05/21 16:33:11.238 [CUSTID 10098213, ANI T7513ae51a6d092, Trunk T451.16] Amount

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CPU threshold

{actor:{displayName:"Go Boys!!",following:{CUSTID 10098213, friendsCUSTID 10098213, "http://dallascowboys.com/"},location:{lat:32.8333,lon:-96.7667,city:"Dallas, TX",objecttype:"place"},objecttype:"person",name:"Go Boys!!",statusCount:6072},body:"Just bought this POS device from the store. It doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objecttype:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}

Activity Log

Event Log

IT Ops					
Server Name	Uptime %	Avg Response Time	Errors	CPU	Disk
web_bc01	.88	35ms	1	22%	33%
web_bc02	.65	2990ms	43	100%	31%

Business Analytics						
Product ID	Number of Orders	Total Sales	Average Checkout time	Avg Site Visit Time	Abandoned Carts	CSAT
Prod A	301	\$6622	:45	3:04	301	60
Prod B	450	\$10350	:35	2:21	450	70

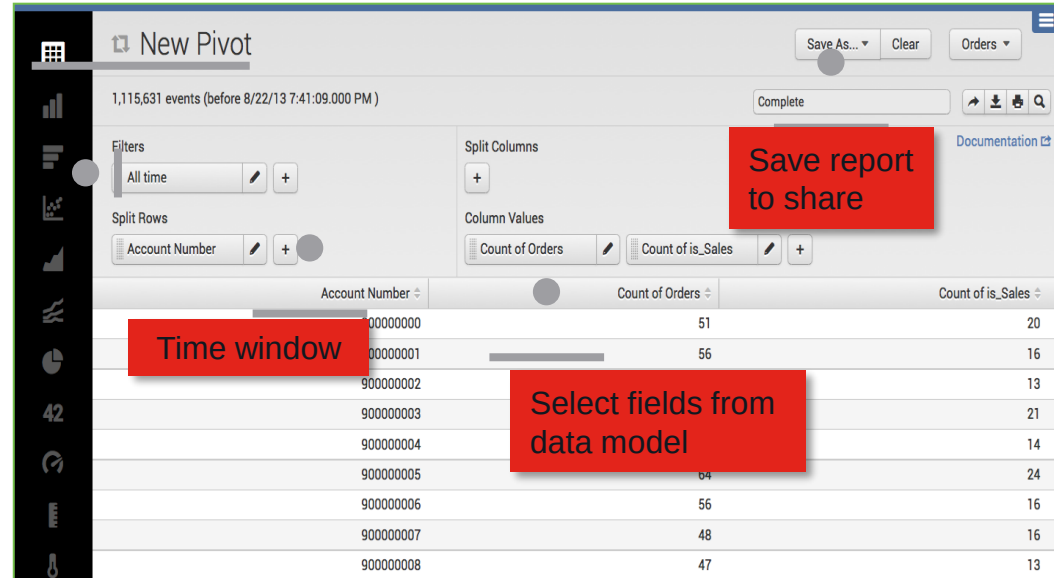
Security					
Server Name	IP Addr	Failed Logins	Security Event Logs	Network Activity	Notable Events
web_bc01	67.17.10.12	4	22	Normal	2
web_bc02	67.17.10.13	631	1030	Suspicious	13
web_bc03	67.17.10.14	12	27	Normal	0
prdstg_01	67.17.10.15	0	0	Normal	0
prddb_01	67.17.10.16	1	5	Normal	1

Table Datasets: Empower users with focused data views

Easy-to-Use Analytics

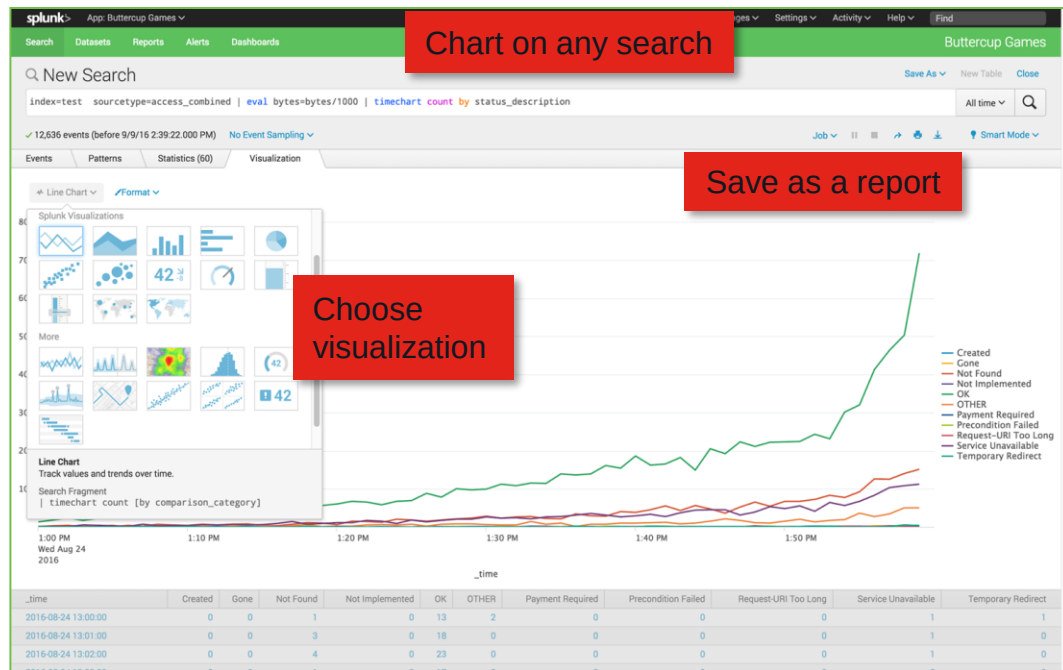
- Pivot
 - Drag-and-drop interface enables any user to analyze data
 - Create complex queries and reports without learning search language
 - Click to visualize any chart type; reports dynamically update when fields change

All chart types available in the chart toolbox

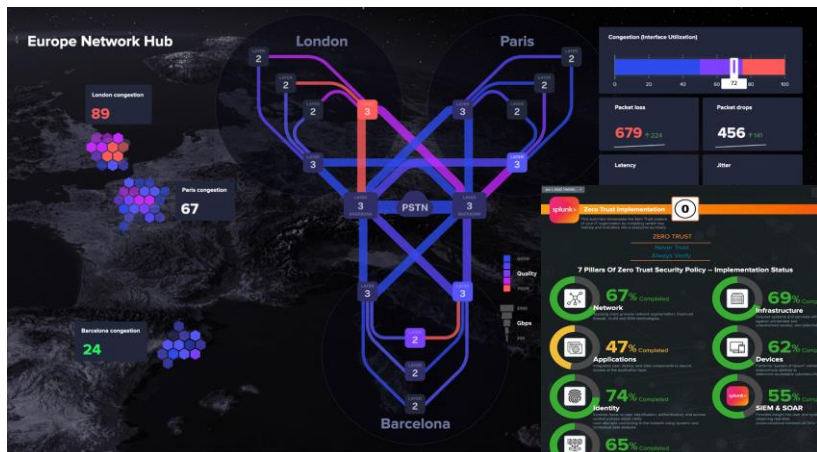
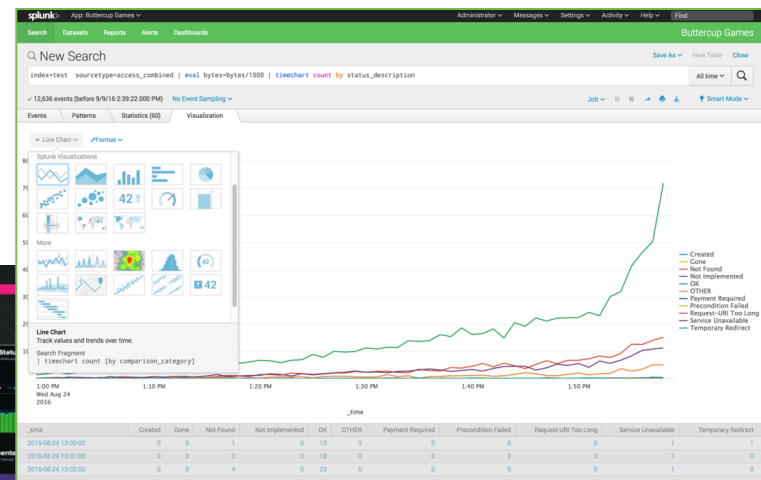


Dynamic Reporting

- Reports
 - Visually represent the results of a search
 - Run on an ad hoc basis or save the report to view later
 - Share it with others on the team or a different group
 - Add reports to a new or existing dashboard



Reporting & Visualizations



- Visualize Any Data
 - Open framework to create or customize any visual
 - Visuals shared via Splunkbase library
 - Available for any use: search, dashboards, reports
 - Visuals for IT, security, IoT and business analytics

Actionable Alerting

Alerts

- Create alerts based on any search
- Customize content and format of email alerts
- Trigger a script
- Custom Alert Actions
 - Allows packaged integration with third-party applications
 - Enable custom workflows
 - Developers can build, package and publish alert actions

The screenshot shows the 'Edit Alert' configuration window for an alert named 'Alert - Customer download failing'. The window is divided into several sections:

- Alert:** Alert - Customer download failing
- Enable Actions:** A checkbox labeled 'List in Triggered Alerts' is currently unchecked.
- Send Email:** A checkbox is checked. The 'To' field contains the email address '\$result.area_code\$.support@splunktel.com;'. The 'Priority' is set to 'High'. The 'Subject' field contains '\$name\$'. The 'Message' field contains a template: 'The customer with a phone number of \$result.n "\$result.track_name\$" by "\$result.artist_name\$". This dashboard may help diagnose: http://wimpy.splunk.com:8999/en-US/app/oidemo/customer_care?form.sourcetypeToken=\$result.mdn\$&earliest=\$job.searchEarliestTime\$&latest=\$job.searchLatestTime\$'.
- Include:** A grid of checkboxes for additional actions: 'Link to Alert' (checked), 'Link to Results' (unchecked), 'Search String' (unchecked), 'Inline Table' (unchecked), 'Trigger Condition' (checked), and 'Attach CSV' (unchecked).
- + Add Actions:** A dropdown menu showing various integration options: HipChat (Send HipChat room notifications), Run a script (Invoke a custom script), Send email (Send an email notification to specified recipients), ServiceNow (Create a ticket in ServiceNow), Slack (Send a message to a Slack channel), and Webhook (Generic HTTP POST to a specified URL).
- Buttons:** 'Cancel' and 'Save' buttons are at the bottom.

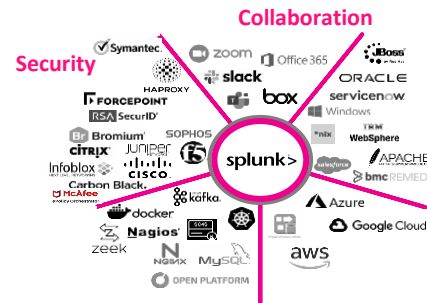
Apps and Add-ons

Apps

A packaged solution containing a collection of knowledge objects and extensions for a specific technology or use case

Add-on

An App that provides custom configurations or data inputs to support other Splunk apps. (ex. data ingestion and parsing.)



Public Apps

Splunk, Partner, and community developed Apps and TAs offered for community reuse*.

- Splunkbase apps vetted via App Inspect



Splunkbase

- 1,000+ Splunk Cloud Certified Public apps
- Splunk 1st-Party Apps are already vetted



App Inspect

Splunk AppInspect service automatically checks for security compliance of Splunk Apps



Private Apps

Customer developed Apps and TAs private to your organization.

- Private apps installed via Splunk Cloud UI or Admin Config Service (ACS)



Splunk Admin



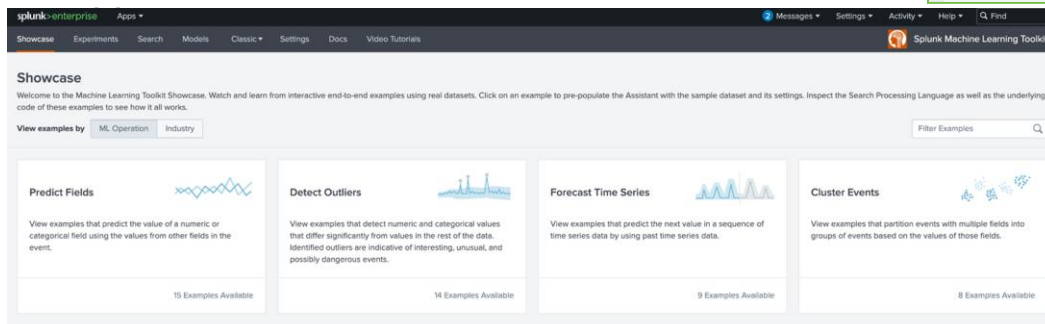
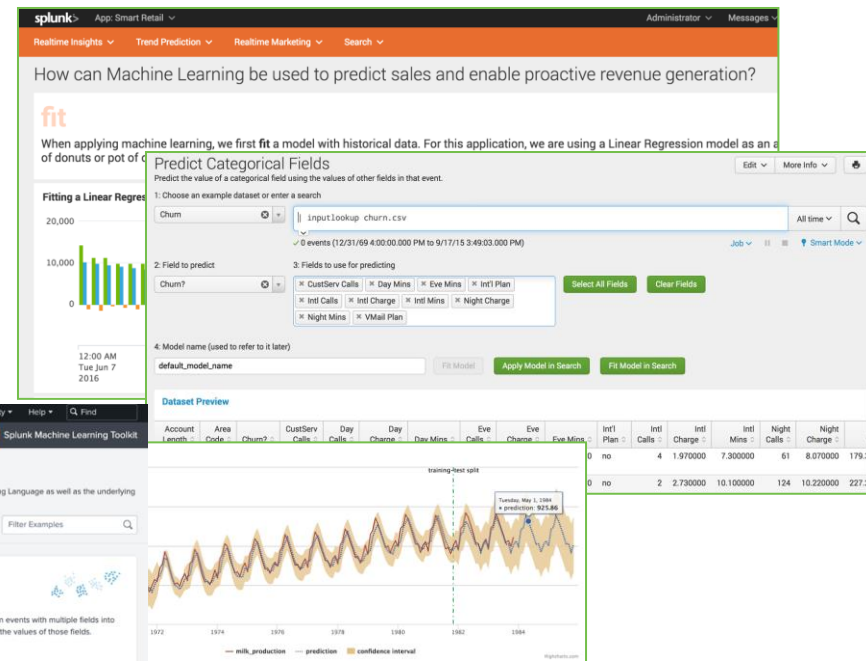
* Some Apps are offered as part of paid offerings.

Cisco Apps

 <p>Cisco ISE Custom Alert that can hit directly Cisco ISE API By WIMBO PRABA CANDRA SUCI</p> <p>The Splunk Add-on for Cisco ISE allows a Splunk to hit directly to Cisco ISE API to block mac-address via custom alerting....</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (3)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Cisco Enterprise Networking for Splunk By Cisco EN Programmability</p> <p>The **Cisco Enterprise Networking for Splunk Platform** presents visualizations in dashboards for different Cisco...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ☆☆☆☆☆ (0)</p> <p>DEVELOPER SUPPORTED APP</p>	 <p>Cisco Security Cloud By Cisco Security</p> <p>The Cisco Security Cloud application offers seamless integration for connecting your Cisco devices with...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (3)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Cisco Web Security Appliance (WSA) Insight By Pavel Prostin</p> <p>Visualize hidden Cisco Web Security Appliance (WSA) statistics, simplify troubleshooting, find performance...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ☆☆☆☆☆ (0)</p> <p>DEVELOPER SUPPORTED APP</p>	 <p>Cisco Catalyst Enhanced Netflow Add-on for Splunk By Salah Ramlawi</p> <p>The "Cisco Catalyst Enhanced Netflow Add-on for Splunk" provides Netflow element mapping for the Cisco Netflow...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ☆☆☆☆☆ (0)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Splunk Add-on for Cisco WSA By Splunk LLC</p> <p>The Splunk Add-on for Cisco WSA allows a Splunk software administrator to collect access and L4TM log data from...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (10)</p> <p>SPLUNK SUPPORTED ADDON</p>
 <p>Cisco Catalyst Add-on for Splunk By Cisco EN Programmability</p> <p>Cisco Catalyst Add-on for Splunk collects data for different Cisco Products - **Cisco Identity Services Engine**....</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ☆☆☆☆☆ (0)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Splunk Add-on for Cisco ASA By Splunk LLC</p> <p>The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA devices events to the Splun...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (18)</p> <p>SPLUNK SUPPORTED ADDON</p>	 <p>TA for Cisco CDR Reporting and Analytics By Sideview LLC</p> <p>This TA provides index-time settings to index and timestamp CDR and CMR data from Cisco CallManager and Cisco CUB...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ☆☆☆☆☆ (0)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Splunk Add-on for Cisco Identity Services By Splunk LLC</p> <p>The Splunk Add-on for Cisco ISE allows a Splunk software administrator to collect Cisco Identity Services Engine (ISE) syst...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (6)</p> <p>SPLUNK SUPPORTED ADDON</p>	 <p>Splunk Add-on for Cisco ESA By Splunk LLC</p> <p>The Splunk Add-on for Cisco ESA allows the Splunk software administrator to leverage Textmail, HTTP, Consolidated...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (5)</p> <p>SPLUNK SUPPORTED ADDON</p>	 <p>Cisco CDR Reporting and Analytics By Sideview LLC</p> <p>This commercial app, compatible with both Splunk Enterprise and Splunk Cloud, gives your team greatly increase...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (20)</p> <p>DEVELOPER SUPPORTED APP</p>
 <p>Cisco Secure eStreamer Client Add-On for Splunk By Cisco Security</p> <p>****Updates July 15th, 2024**** The current Cisco Secure Firewall app is going EOL, limited support will be...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (31)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Cisco Bug Search and Analytics By Pavel Prostin</p> <p>Cisco Bug Search and Analytics offers unrestricted filtering, summarization, and correlation capabilities for vulnerability...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (1)</p> <p>DEVELOPER SUPPORTED APP</p>	 <p>Cisco ACI App for Splunk Enterprise By Cisco Systems</p> <p>A flexible approach to monitoring your Cisco ACI and all other elements of your technology stack. This App for Cisco A...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (4)</p> <p>DEVELOPER SUPPORTED APP</p>	 <p>Splunk Add-on for Cisco UCS By Splunk LLC</p> <p>The Splunk Add-on for Cisco UCS allows a Splunk software administrator to collect UCS fault, inventory, and...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (9)</p> <p>SPLUNK SUPPORTED ADDON</p>	 <p>Cisco DNA Center Add-on By Cisco EN Programmability</p> <p>The Cisco DNA Center Add-on for Splunk allows a Splunk* Enterprise administrator to collect data from Cisc...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (6)</p> <p>DEVELOPER SUPPORTED ADDON</p>	 <p>Cisco ThousandEyes Add-on for Splunk By Avotrix Inc.</p> <p>Cisco ThousandEyes delivers the most comprehensive visibility into digital experience for applications and data...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (1)</p> <p>DEVELOPER SUPPORTED ADDON</p>

Splunk Machine Learning Toolkit

- **Assistants:** Guide model building, testing & deployment for common objectives
- **Showcases:** Interactive examples for typical IT, security, business, IoT use cases
- **SPL ML Commands:** New commands to fit, test and operationalize models
- **Python for Scientific Computing Library:** 300+ open source algorithms available for



Build custom analytics for any use case

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC