

splunk®

.conf2017

© 2017 SPLUNK INC.

# Fake Data for Real Apps

SimData as a new Simulated Data Generator

David J. Cavuto, CISSP | Principal Product Manager, Data Ecosystem

David Poncelow | Senior Software Engineer, Data Ecosystem

Date | Washington, DC

# 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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

# Cavuto Bio



- ▶ Bell Labs
  - Principal Engineer - Lucent VPN Firewall
- ▶ AT&T
  - Network security and analytics
- ▶ Narus
  - Product Manager – Narus Cyber Analytics
- ▶ Splunk
  - Sales Engineer, Security SME
  - Principal Product Manager – Splunk App for Stream
  - Principal Product Manager – Data Ecosystem Area
- ▶ David J. Cavuto  
dcavuto@splunk.com

# History of Data Simulation at Splunk

---









# Next Steps in Data Simulation: SimData

---

SimData Concepts and Execution













# DSL Syntax (v0.8)

Yes, it's an eye chart

```

entity <entity-class-name> {
  init { assignment; [assignment;] };
  every (time) { statement };
  on <message-class-name> { statement };

  send <message-class-name> { parameters }
[in (time)];
  respond { parameters } [in (time)];
  emit <event-class-name> { format-parameters
};

  /* this defined a function for invoking as
self.method() */
  /* and can use 'send', 'emit'. In the right
scope 'respond' too. */

  method <method-class-name>([parameters]) {
statement };
};

message <class-name> { message-parameters };

event <class-name> { statement };

debug( format-parameters );

scene {
  connect {
    {
      fromEntity: <entity-class-name>;
      messageType: <message-class-name>;
      toEntity: <entity-class-name>;
    } [, {
    fromEntity: <entity-class-name>;
    messageType: <message-class-
    name>;
    toEntity: <entity-class-name>;
  } ]
}

-----
message-parameters:
  required: <field-name> [,<field-name>];
  optional: <field-name>=<default-value>
[,<field-name>=<default-value>];

parameters:
  <field-name>: evaluation;

format-parameters: (TBD)

statement:
  [statement;]
  [expression;]

expression:
  [assignment;]
  [<method-invocation>;]
  [<send-invocation>;]
  [<respond-invocation>;]
  [<emit-invocation>;]
  [<debug-invocation>;]
  [<conditional>;]

conditional:
  if (<evaluation> <comparison> <evaluation>)
then { statement } [ else { statement } ]

assignments:
  <variable> = evaluation;

time:
  numeric-evaluation (milliseconds | seconds
| minutes | hours)

evaluation:
  expression that evaluates to a type object

numeric-evaluation
  expression that evaluates to a numeric
scalar type

langauge builtins: (more TBD)
  random(<range>)
  now
  false
  true
  self
  if/else
  milliseconds
  seconds
  minutes
  hours

range: (low,high)
  numeric-evaluation, numeric-evaluation
  time, time

```







# Examples and Demonstration

---

Some syntax and a live simulation





# Sample Splunk Events

3 of 559,618 events matched [No Event Sampling](#) Job ▾ ▮ → ⏏ ⏴ ⏵ ⚙ Smart Mode ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 10 milliseconds per column

List ▾ Format ▾ 20 Per Page ▾

<a href="#">&lt; Hide Fields</a> <span style="margin-left: 20px;">☰ All Fields</span>	i	Time	Event
	>	9/7/17 3:35:01.000 PM	2017-09-07T15:35:01.6 userID=837 got response code=200 sessionID=c808e135-ea9c-4754-935b-148e4d251967 host = localhost:8088   source = user   sourcetype = httpevent
Selected Fields <a href="#">a host</a> 1 <a href="#">a source</a> 3 <a href="#">a sourcetype</a> 1	>	9/7/17 3:35:01.000 PM	2017-09-07T15:35:01.2 Database Replied with status=ok connectionID=358d3b60-1792-4788-a95b-72ae619ad7f7 host = localhost:8088   source = webserver   sourcetype = httpevent
Interesting Fields <a href="#"># code</a> 1 <a href="#">a connectionID</a> 1 <a href="#"># CPU_percent</a> 1 <a href="#"># disk_percent</a> 1 <a href="#"># duration</a> 1 <a href="#">a index</a> 1 <a href="#"># linecount</a> 1 <a href="#">a punct</a> 3 <a href="#">a sessionID</a> 1 <a href="#">a splunk_server</a> 1	>	9/7/17 3:35:00.000 PM	2017-09-07T15:35:00.8 Query Successful. connectionID=358d3b60-1792-4788-a95b-72ae619ad7f7 CPU_percent=0 disk_percent=0 duration=1 host = localhost:8088   source = database   sourcetype = httpevent







# Q&A?

Questions from the Audience



# Thank You

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk> .conf2017