Splunk To A Cure:

Be Inspired By A Lifesaving Use Case Of Managing T1 Diabetes. See Critical Notifications, Visualizations, And Correlated Analysis

Steve Hogan

Splunk Staff Engineer, Splunk

Disclaimer

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

Opening

- See how Splunk is being leveraged to intelligently overcome daily obstacles through:
  - Critical alert notifications using simple, but intelligent Splunk Searches
    - *How intelligent alerting can cut through the noise, and truly provide lifesaving responses*
  - Strategic real-time to historical trending analysis
  - Correlating cross-data to reach the goal of a Type 1 Cure.
    - *How correlating cross-data can be leveraged for reaching an ultimate resolution*
- *Goal: To inspire, educate, and cooperate.*

Agenda

- Diabetes - Key Definitions
- Splunk To A Cure - Splunk Application
- Diabetes Data
- Intelligent Splunk Alerting
- Intelligent Splunk Trending Analysis
- Correlation - Finding Contributing Factors
- Shout Out
- Conclusion

Key Diabetes Definitions

Key Diabetes Definitions

- ***Insulin:***
  - Without insulin, cells cannot absorb sugar (glucose), which they need to produce energy.
- ***Type 1 vs. Type 2:***
  - **Type 1** (5-10% of Diabetics):
    - Pancreas ***Does Not*** produce Insulin (Autoimmune Disease)
  - **Type 2** (90-95% of Diabetics):
    - Pancreas ***Does*** Produce Insulin, but not the right way (Mostly managed through Diet)

Key Diabetes Definitions

Blood Sugar Value (***BG*** - blood glucose) ***:***

- Is the amount of glucose (sugar) present in the blood

Hyperglycemia (BG High *">170 mg/dl"*) ***:***

- Is a condition in which an excessive amount of glucose circulates in the blood plasma.
- *Action Term:* ***Correction*** = Give Insulin

Hypoglycemia (BG Low *"<70 mg/dl"*) ***:***

- Is when blood sugar decreases to below normal levels
- *Action Term:* ***Treatment*** = Give Sugar/Glucose

CGM (Continuous Glucose Monitor):

- Medical Device that collects BG values using a worn transmitter.
- *Example –* Dexcom CONTINUOUS GLUCOSE MONITORING

Insulin Pump (insulin delivery system)

- Medical Device that delivers continuous Insulin**,** Basel Rate, or ad-hoc Insulin for meal/***Correction***, Bolus**.**
- *Example –* 

A1c:

- Measurement of successful Diabetes Management.

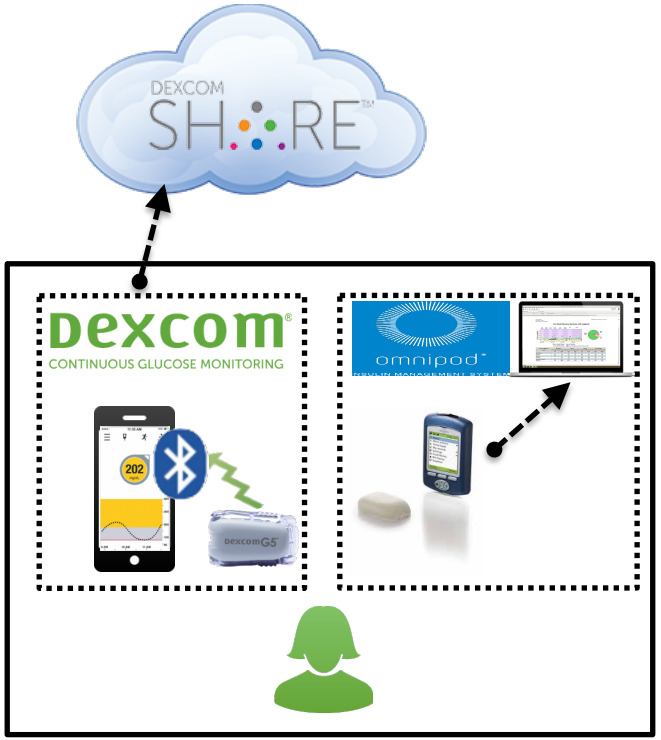
Splunk To A Cure

Splunk To A Cure

- ***Description:*** *Splunk Application for assisting with Diabetes management. This application can be leveraged for gathering and managing Blood Sugar (BG) data from CGM (Continuous Glucose Monitoring), Insulin Pumps and other relevant data sources.*
- ***Why I created the Application?***
  - *I am a recently new parent to a daughter who has Type 1, after getting caught up with currently available management solutions, the geek in me took over to Rejoice on what is provided, but do my best to improve daily management for my family.*

Diabetes Data

Diabetes Data



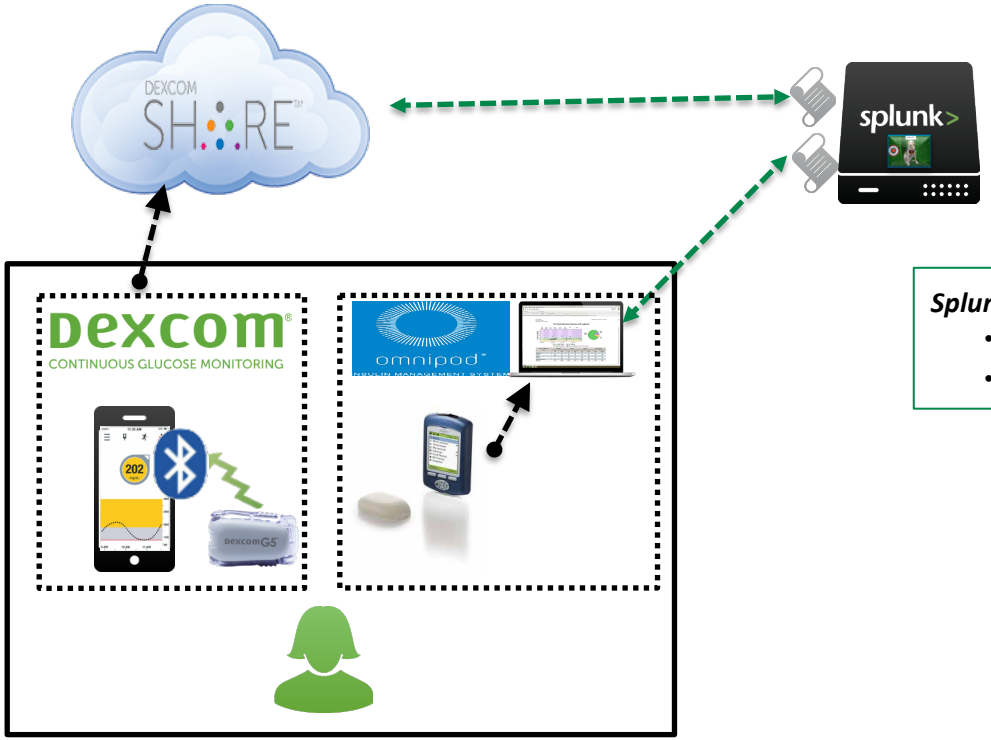
CGM (Continuous Glucose Monitor) – dexcom CONTINUOUS GLUCOSE MONITORING

- *Data Location:*
  - *Dexcom Share Cloud*
- *Key Data Values:*
  - BG Value
  - Direction

Insulin Pump (insulin delivery system) – omnipod

- *Data Location:*
  - ***Abbott Diabetes Care CoPilot®** exported daily reports*
- *Key Data Values:*
  - *Pump Settings:*
    - *Basal Rate*
    - *IOB – Insulin On Board*
  - *Logbook:*
    - *Bolus (Carbs, Insulin, Type (Meal or Correction)*
    - *Temp Basal*
    - *Activity or Event*
    - *Meal Details*

Diabetes Data Inputs



Splunk Scripted Input **–**

- *Python Script – Dexcom Share API*
- *PowerShell Script – Extract and Index Co-Pilot exported reports.*

Intelligent Splunk Alerting

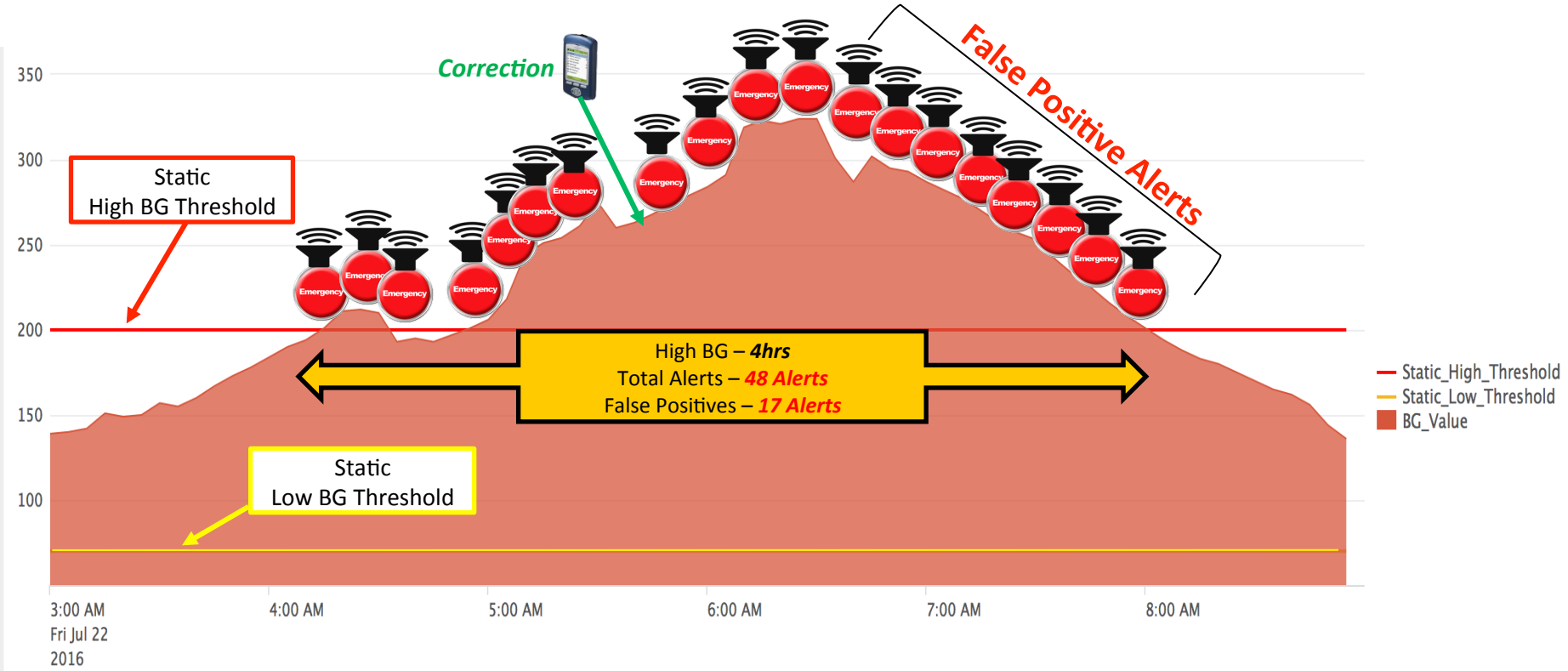
Intelligent Splunk Alerting

Why Static Thresholds Alone don't Work!!

- Medical Diabetes Devices and Static Thresholds:
  - **Problem:**
    - Most Diabetes Management medical devices use static thresholds for alerting notifications
      - *Ex.* ***High BG*** *(>170 mg/dl) or* ***Low BG*** *(<70 mg/dl)*
  - **Results:**
    - *False Positive Alerts:*
      - Unneeded and eventually tuned out acknowledgement.
    - *False Negatives:*
      - Missed Rapid Descents/Accents, sometimes forcing strenuous catchup to stabilize.

Intelligent Splunk Alerting

Static Thresholds – False Positive Example



Intelligent Splunk Alerting

Static Thresholds – False Positive Results In.....

Extremely Sleep Deprived Parents....

Intelligent Splunk Alerting
Removing False Positives With Splunk

- ***Leveraging Simple Splunk Commands:***
  - **Solution:**
    - Reduce Alert Frequency and False Positives (*Suppress Alerts after* ***Correction*** *or* ***Treatment***)
  - ***Splunk Commands Used:***
    - ***reverse:*** Reverses the order of the results.
    - ***autoregress:*** Calculate *auto regression*, or the *moving average*, by copying one or more of the previous values for *field* into each event.
    - ***tail:*** Returns the last N number of specified results.
  - ***Basic Example High BG - Splunk Search:***

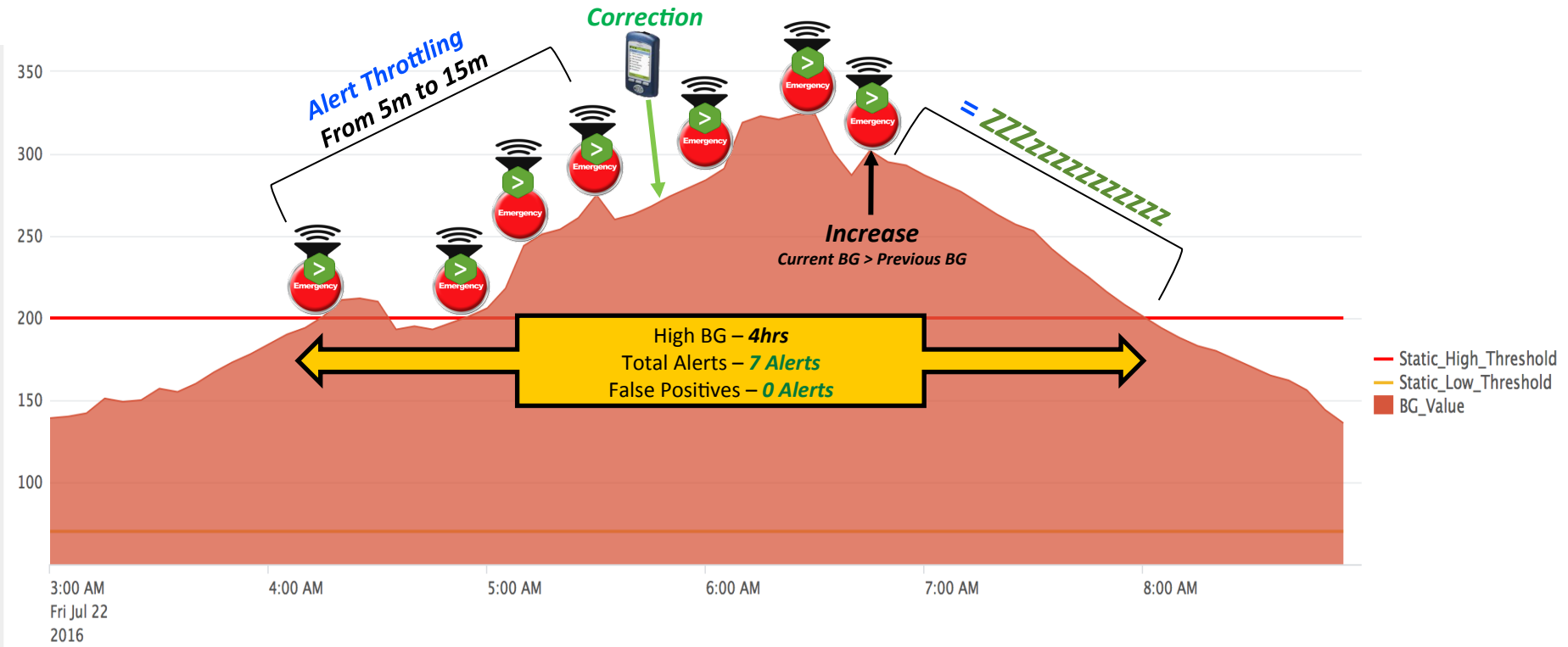
```
index=cure_data
| reverse
| autoregress BG
| eval bg_trigger_flag = if(BG > BG_p1,"True","False")
| tail 1
```

- Get previous *BG (Field: BG_p1)*
- Create alert Trigger Flag
- Use Splunk Alert's ***Custom Trigger Condition***
  - ***search bg_trigger_flag = "True"***.
- Get the last result

_time	BG	BG_p1	bg_trigger_flag
2016-07-30 07:16:24	221	190	True

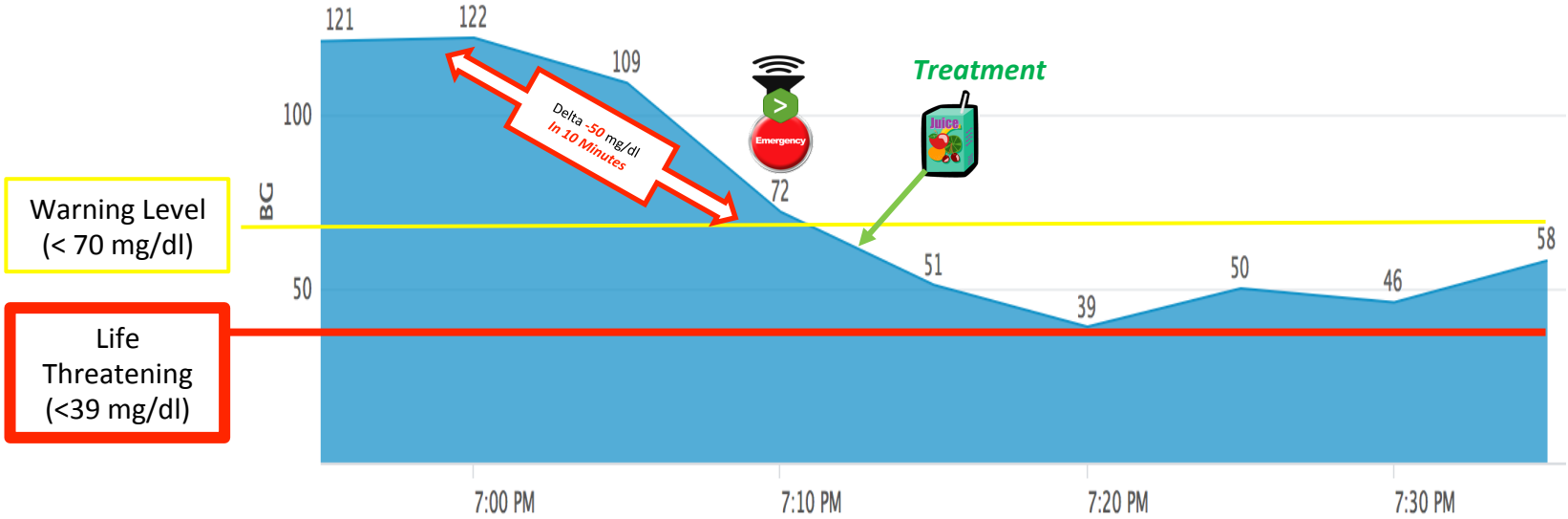
Intelligent Splunk Alerting

Removing False Positives With Splunk



Intelligent Splunk Alerting
Avoiding False Negatives With Splunk

- ***False Negatives:***
  - **Problem:**
    - Alert when extreme BG Increases or Decreases occur within a short time period.
      - Not Within Warning Range, "YET"
      - If Not Caught early, lengthy catchup or Life Threatening levels reached.



Splunk Intelligent Alerting
Avoiding False Negatives With Splunk

- ***Splunk Commands:***
  - Use *reverse*, and *autoregress* to get historical values, then use *eval* for getting and analyzing delta.

```
index=cure_data
| reverse
| autoregress BG p = 1-3
| eval BG_Total_Delta = BG - BG_p3
| eval BG_Range = if(BG<180 AND BG>70, "True","False")
| eval bg_trigger_flag = if(BG_Range=="True" AND
(BG_Total_Delta > 45 OR BG_Total_Delta<-45)),"True","False")
| tail 1
```

Get previous *BG's (p=1-3)* new *BG_p1, BG_p2, BG_p3* fields.

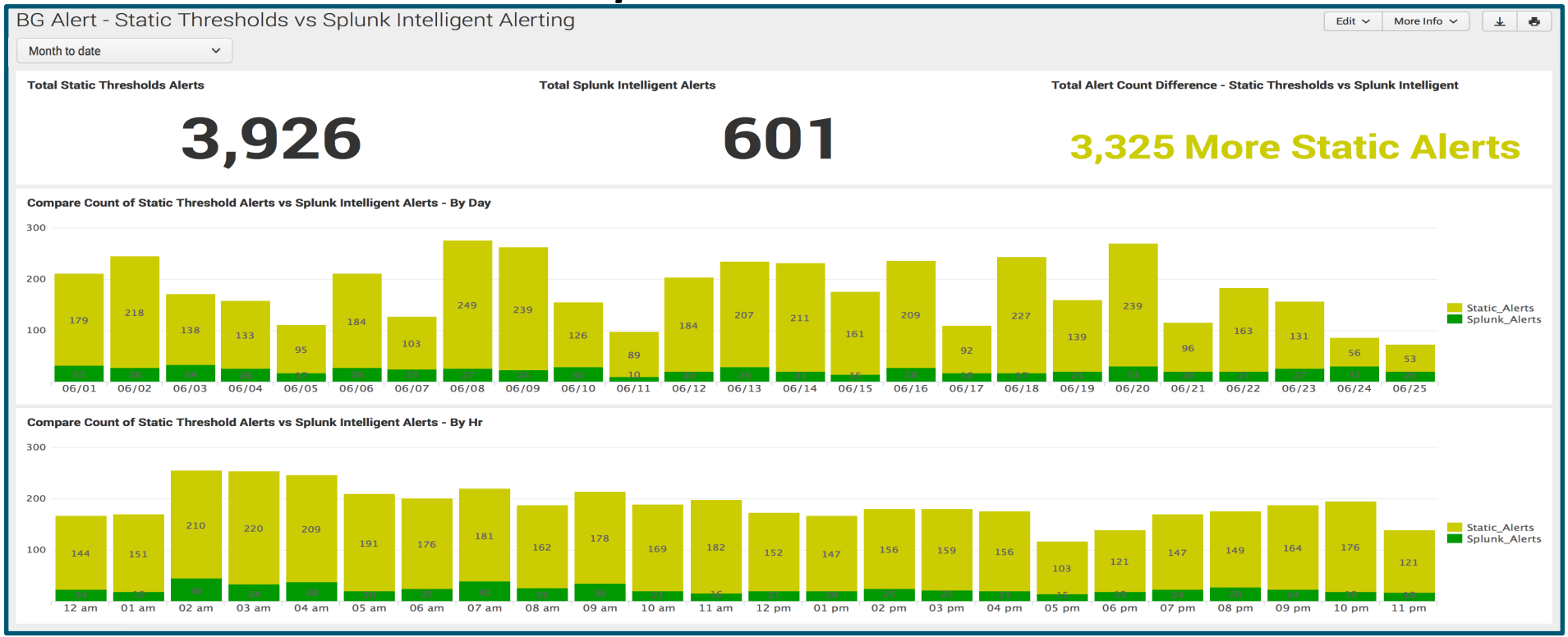
Get Delta between Current BG and the 3rd Previous BG. Used for getting rate of change.

Check BG Range, to only Alert for drastic Changes that have not already generated an alert.

Set Alert Trigger Flag if BG Change is greater than 50, and Current BG is within "Non-Standard Alerting Range".

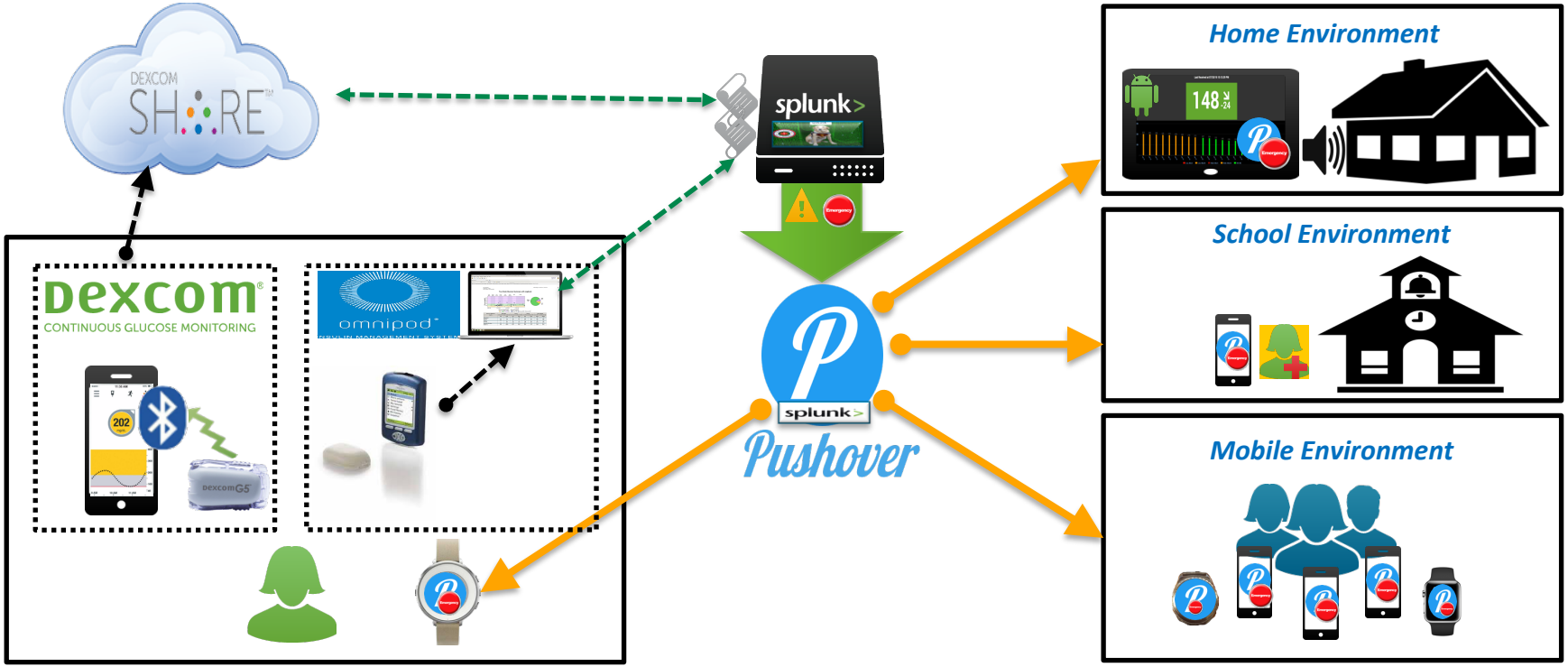
Intelligent Splunk Alerting

Comparison Results



Intelligent Splunk Alerting

Intelligent Notifications



Intelligent Splunk Alerting
Intelligent Notifications

- ***Formatting Events:***
  - **Problem:**
    - Streamline Notification content to make quick, but precise decisions.
  - ***Splunk Resolution:***
    - *Leverage **Pushover Splunkbase App**, and **Splunk's Search** Language.*
    - Use *reverse*, and *autoregress* to get historical values, then use *eval* and *makemv* to format it for the Pushover Notification.
      - *makemv:* Converts a single valued field into a multivalue field by splitting it on a simple string delimiter, which can be a multi-character. Alternatively, splits field by using a regex.

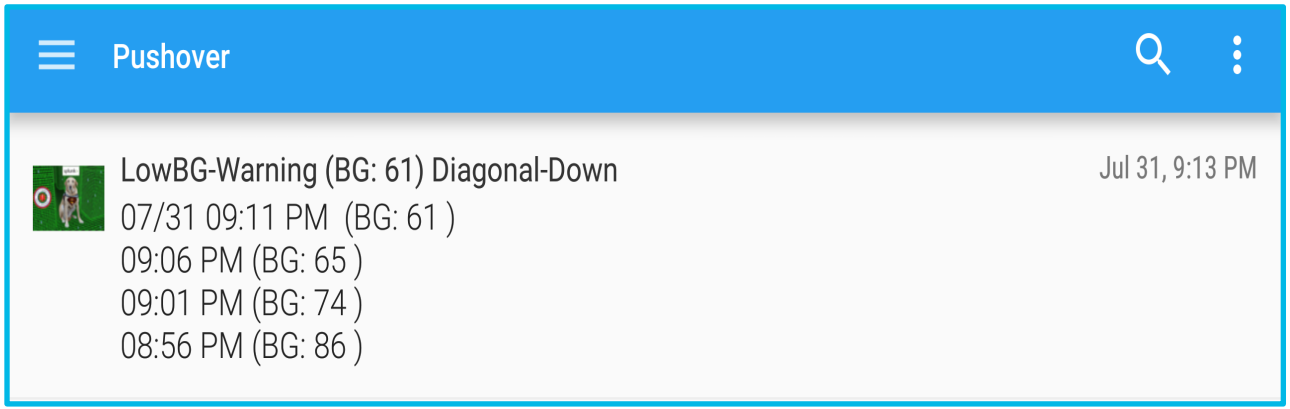
Intelligent Splunk Alerting
Intelligent Notifications

```
index=cure_data
| reverse
| autoregress bg p=1-4
| eval bg_time=_time
| autoregress bg_time p=1-4
| eval bg_time_period=strftime(bg_time, "%m/%d %I:%M %p")
| eval bg_n_p1=strftime(bg_time_p1, "%I:%M %p")." (BG: ".bg_value_p1." )"
| eval bg_n_p2=strftime(bg_time_p2, "%I:%M %p")." (BG: ".bg_value_p2." )"
| eval bg_n_p3=strftime(bg_time_p3, "%I:%M %p")." (BG: ".bg_value_p3." )"
| eval bg_history=bg_time_period."  (BG: ".bg_value.")|".bg_n_p1."|".bg_n_p2."|".bg_n_p3
| eval Severity_Title=Severity." (BG: ".bg.") ".Direction
| makemv delim="|" bg_history
| eval bg_trigger_flag=if(bg<bg_p1,"True","False")
| fields + _time bg_history Severity_Title
| table _time,Severity_Title,bg_history
| tail 1
```

Build Title and Summary fields for Notification

Intelligent Splunk Alerting
Intelligent Notifications

- ***Leveraging Pushover.net notifications:***



- ***Splunk Search Results:***

Severity_Title	bg_history
LowBG-Warning (BG: 61) Diagonal-Down	7/31 09:11 PM (BG: 61) 09:06 PM (BG: 61) 09:01 PM (BG: 74) 08:56 PM (BG: 86)

Splunk Intelligent Trending Analysis

Splunk Intelligent Trending Analysis

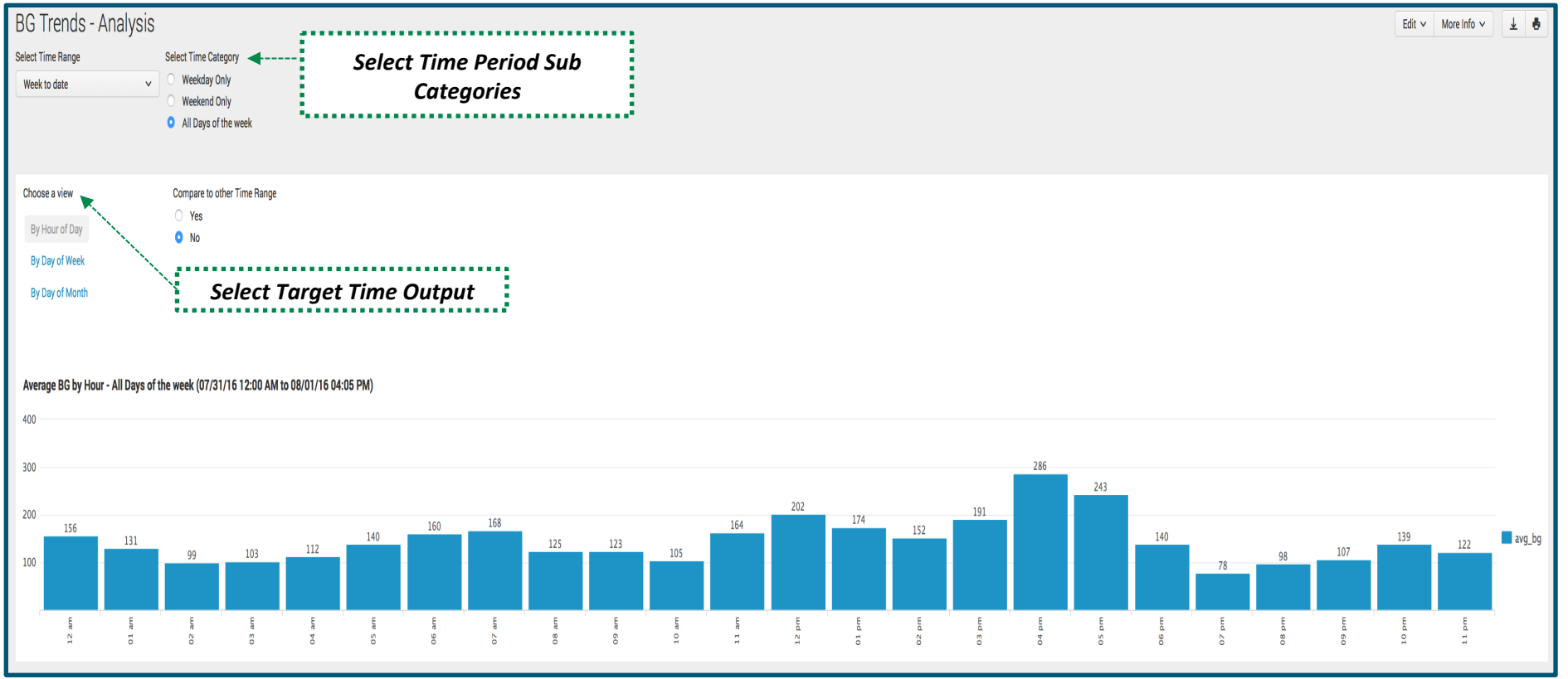
Problem/Need:

- Need to analyze historical trends to determine:
  - Pump Basal Rate Settings
    - Night/Daytime
    - Events and Activities
  - Appropriate Bolus - Meals
  - Education and verification of care givers
- Assist with meeting BG Target Ranges:
  - ***BG:*** 70mg < - - < 170mg
  - ***A1c:*** 7.5%

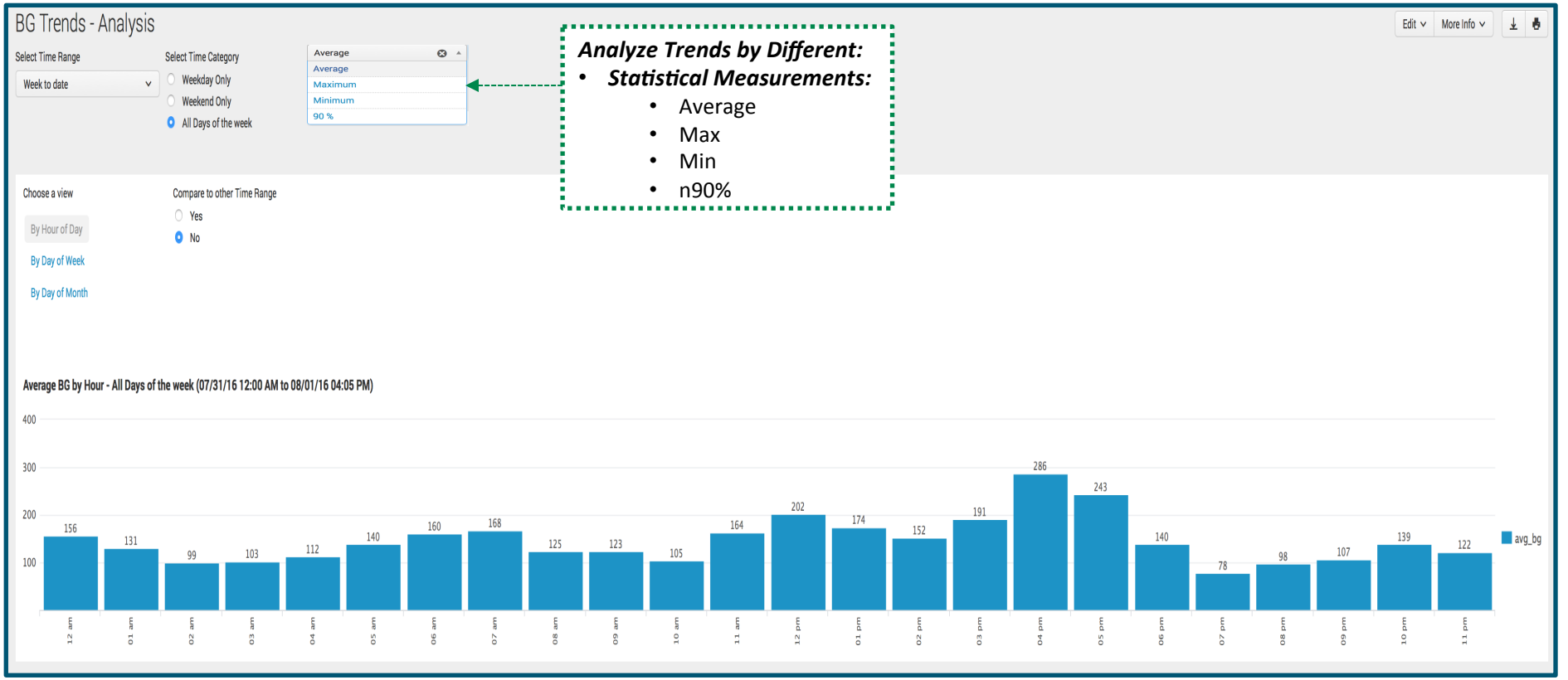
Solution - BG Trending Dashboard:

- Dashboard for Analyzing BG Values for:
  - All Days/Weekday/Weekends
  - By hour of day, Day Of Week, and Day of Month
  - Comparing against a different time period.

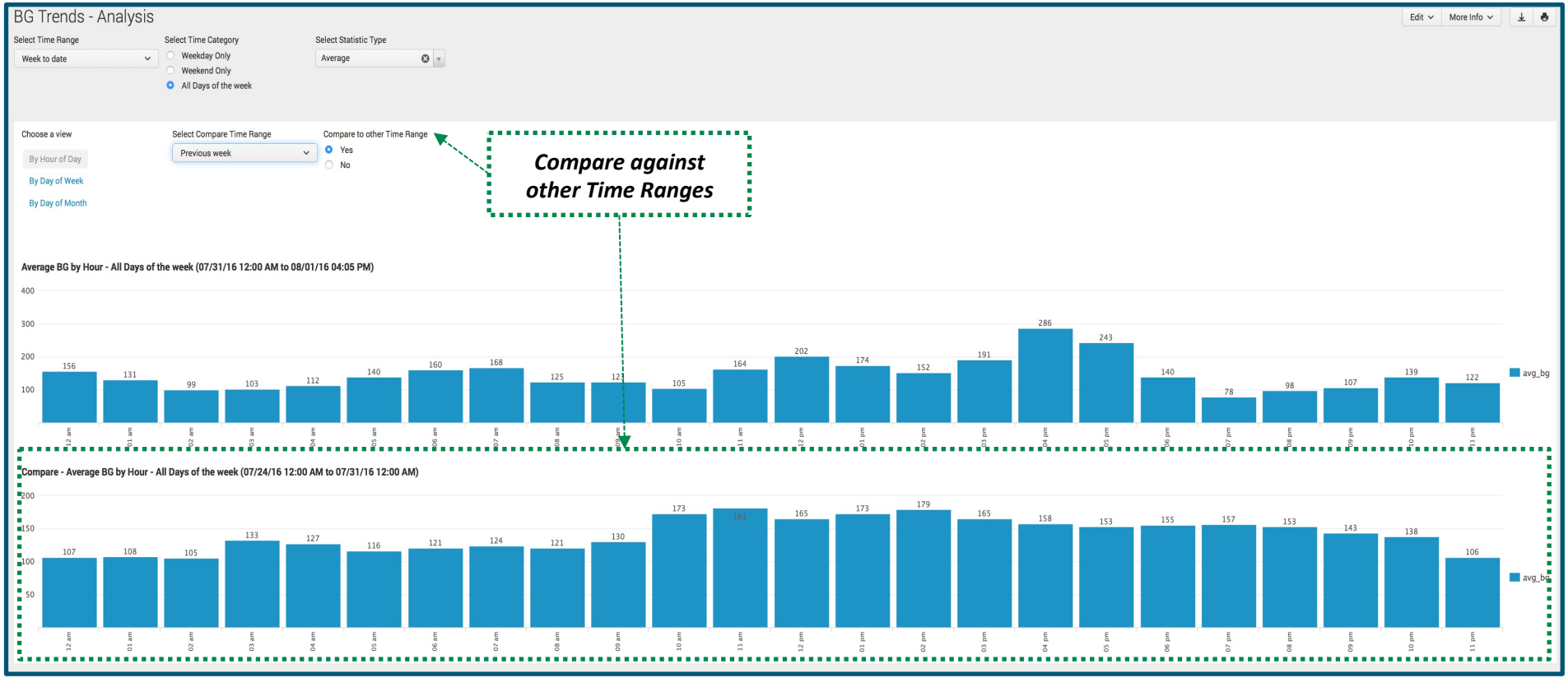
Splunk Intelligent Trending Analysis



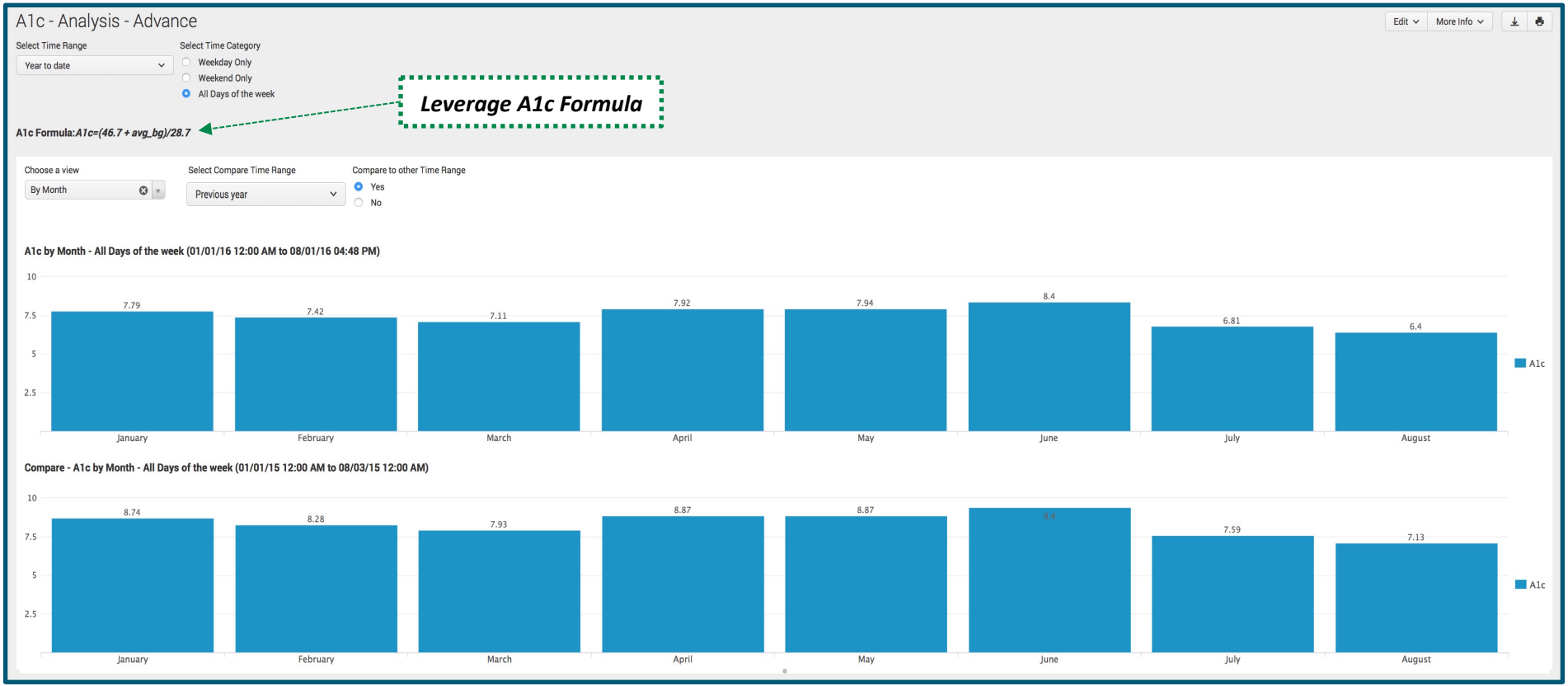
Splunk Intelligent Trending Analysis



Splunk Intelligent Trending Analysis



Splunk Intelligent Trending Analysis



Correlation Of Other Data

Correlation
Finding Contributing Factors

Need:

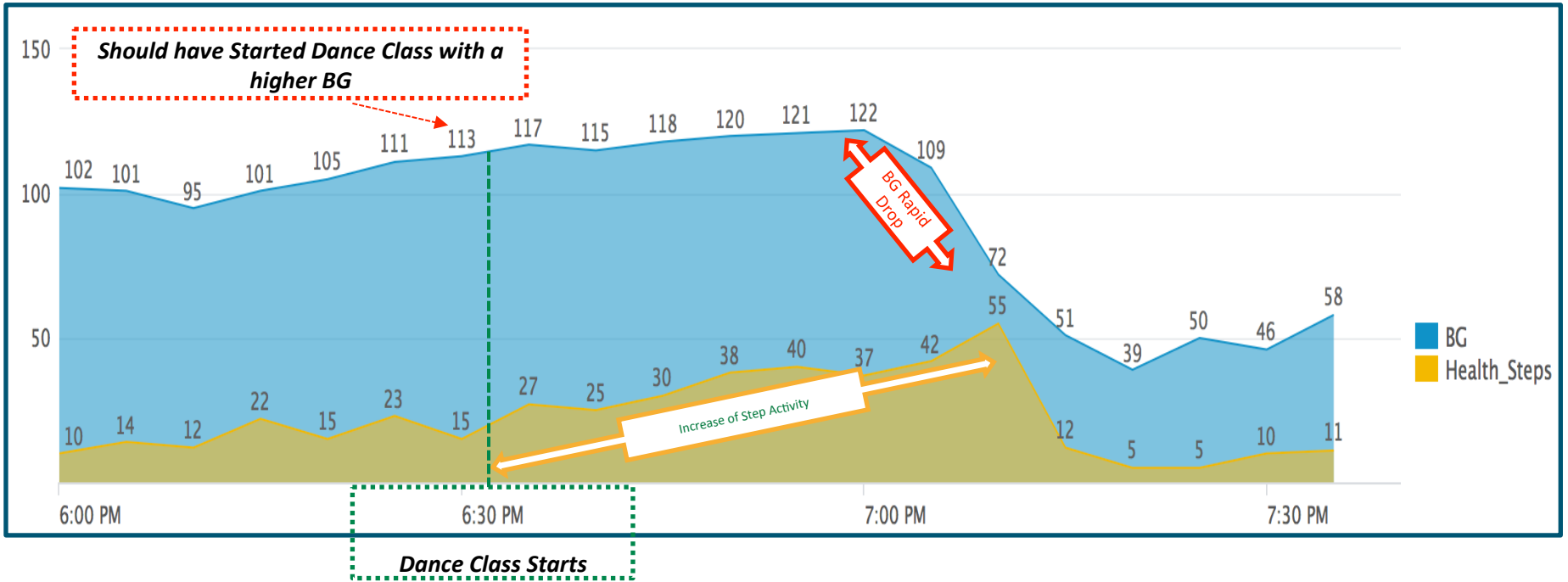
- A way to correlate *non-diabetic data* with *diabetic data* for:
  - Positive/Negative affects on successful Diabetic Management.
  - Ultimately, to find the "Cure Needle" in this "VICIOUS DISEASE Haystack"

Current Non-Diabetic Data Analyzed:

- Pebble Health → Apple Health Kit:
  - Steps, Activity Duration
- Weather Data using:  TA for Wunderground
- USDA Food Composition Databases: (http://www.ars.usda.gov/services/docs.htm?docid=1328)
  - Assist with "Carb Counting"
  - Analyze other nutritional elements, instead of just Carbohydrates.

Correlation
Finding Contributing Factors

Example – Correlating Pebble Watch Step counts with CGM BG Data



Shout Out

Shout out

NIGHTSCOUT
#WeAreNotWaiting

- Facebook: http://www.facebook.com/groups/cgminthecloud
- Website: http://www.nightscout.info

dexcom
CONTINUOUS GLUCOSE MONITORING

omnipod

CIRCLES OF BLUE

- Website: http://circles-of-blue.winchcombe.org/

splunk>

Conclusion

Conclusion

To wrap this up, hopefully you:

- .. have been inspired by Splunk's power behind this real world use case.
- ..have gained some basic, but critical knowledge of Diabetes.
- ..learned how to take your alerts to an "Intelligent Level", and who know's, maybe getting you some extra "ZZZzzzzzzzz's"
- ..can view trends with your data, and retrieve key intelligence from them for improving stability with your data management needs.
- ..are thinking how you can leverage "other-data" for finding contributing factors to your data obstacles.

BUT MOST IMPORTANT, I hope I opened a few community channels that could help me ***SPLUNK TO A CURE!!***

THANK YOU

splunk>

Appendix A: More Info on Diabetes Management

Type 1 and Type 2:

- ***Type 1:***
  - 5%-10% of people who have diabetes.
  - Auto Immune Disease - The body's immune system destroys the cells that release insulin, eventually eliminating insulin production from the body.
  - Can develop at any age.
  - Without insulin, cells cannot absorb sugar (glucose), which they need to produce energy.
  - There are many myths about what people with diabetes can and can't eat. The reality is there are no "off-limits" foods.
- ***Type 2:***
  - 90% - 95% of people who have diabetes.
  - Most people with type 2 diabetes do not take insulin.
  - Can develop at any age, most commonly in adults, but type 2 diabetes in children is rising.
  - The body isn't able to use insulin the right way. This is called insulin resistance.
  - As type 2 diabetes gets worse, the pancreas may make less and less insulin (Insulin Resistance)

**Used References: http://www.m.webmd.com, http://www.diabetes.org*

Appendix A: More Info on Diabetes Management

Blood Sugar Value (***BG*** - blood glucose) ***:***

- Normal Blood Sugars. A normal fasting (no food for eight hours) blood sugar level is between 70 and 99 mg/dL.
- A normal blood sugar level two hours after eating is less than 140 mg/dL.

Hyperglycemia (BG High):

- *Description:* Technical term for **high** blood glucose (blood sugar). High blood glucose happens when the body has too little insulin or when the body can't use insulin properly.
- *Action:* **Correction** = Insulin (Shot or via Pump Bolus).

Hypoglycemia (BG Low):

- *Description:* Is a condition characterized by abnormally **low** blood glucose (blood sugar) levels, usually less than 70 mg/dl.
- *Action:* **Treatment** = Sugar (Juice, Glucose Tab, etc)

CGM (Continuous Glucose Monitor):

- This tool uses a sensor to measure the level of glucose in your body every 10 seconds. It sends the information to a cell phone-sized device called a "monitor" that you wear. The system automatically records your average reading for up to 72 hours. The device isn't meant for day-to-day checks or long-term self-care. It doesn't replace your standard blood sugar test. It's only used to spot trends in your levels.

Insulin Pump (insulin delivery system)

- **Basel Rate:** A small, constant, background supply of insulin (called a basal rate) is delivered automatically at a programmed rate, all day and night.
- **Bolus:** An extra dose of insulin can be delivered when you need it to match the carbohydrates in a meal or snack or to **correct** a high blood glucose.

A1c:

- The A1C test gives you a picture of your average blood glucose (blood sugar) control for the past 2 to 3 months. The results give you a good idea of how well your diabetes treatment plan is working.

**Used References: http://www.m.webmd.com, http://www.diabetes.org*