

# Your Systems Are Talking to You

Presenter:

George Sconyers

Senior Solutions Architect

Omega ATC

# Agenda

- Housekeeping
- Presenters
- About Conexus
- Presentation
- Q & A

# Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube ([youtube.com/conexxusonline](https://youtube.com/conexxusonline))
- Website Link ([conexxus.org](https://conexxus.org))

## Slide Deck

- Survey Link – Presentation provided at end

## Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: [info@conexxus.org](mailto:info@conexxus.org)

# Presenters

## Conexxus Host

Allie Russell

Conexxus

[arussell@conexxus.org](mailto:arussell@conexxus.org)

## Moderator

Kara Gunderson

Chair, Data Security Committee

POS Manager, CITGO Petroleum

[kgunder@citgo.com](mailto:kgunder@citgo.com)

## Speaker

George Sconyers

Senior Solutions Architect

Omega ATC

## Voice Assistant

Alexa

# About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards...
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy



# 2018 Conexxus Webinar Schedule\*

| Month/Date         | Webinar Title                                                                 | Speaker                       | Company                |
|--------------------|-------------------------------------------------------------------------------|-------------------------------|------------------------|
| May 24, 2018       | QIR in the World of Retail Petroleum                                          | Chris Bucolo<br>Todd Rosen    | ControlScan            |
| June 21, 2018      | How can we leverage data science to more effectively detect security threats? | Thomas Duncan<br>Ashwin Swamy | Omega ATC<br>Omega ATC |
| July 26, 2018      | Roadmap to a Vulnerability Disclosure Program                                 | Joe Basirico                  | Security Innovation    |
| August 23, 2018    | Moving Toward Outdoor EMV                                                     | Linda Toth                    | Conexxus               |
| September 20, 2018 | Your Systems Are Talking to You!                                              | George Sconyers               | Omega ATC              |
| November 2018      | Building a Scalable Security Engineering Team                                 | Joe Basirico                  | Security Innovation    |

# NACS Show

## October 7-10, 2018

### Las Vegas, NV

---

# TECHEEDGE

In partnership with CONEXXUS 

Booth 6147

Conexxus thanks our 2018 Annual Diamond Sponsors!

**mSHIFT.**

Relevant. Mobile. Solutions.



**GILBARCO  
VEEDER-ROOT**

**Stuzo**

**Cybera**<sup>®</sup>  
*Simplify Security and Networks*

**DIEBOLD  
NIXDORF**

# Your Systems Are Talking to You

Bringing Operational Intelligence  
to Convenience Retail



# Good Information – What is it exactly?

## FEATURES OF GOOD INFORMATION

|                |                                         |
|----------------|-----------------------------------------|
| Accurate       | Should be true and correct              |
| Complete       | No key facts missing                    |
| Timely         | Delivered on time and up-to-date        |
| Relevant       | Meets the need of the audience          |
| Cost Effective | Cost should be no more than the benefit |
| Meaningful     | Is it easy to understand                |

Source: Slide Player  
Communications in  
Administration

# Operational Intelligence

- Will be looking at OI specifically in convenience retail
- Many moving parts (systems) at stores
- Significant Security and Compliance Requirements
- Challenges
  - Limited access to information
  - Timely information often missing
- Gathering, analyzing and sharing information is key

# One Big Problem – Consoles For Everything



Source: Indiana Telephone

# Consoles Consoles and more Consoles!

- Secure Network Provider Portal
- Firewall / Router Mgmt
- Compliance / Vulnerability Scanning
- Applications Management
- Store Marketing Metrics
- Digital Signage
- Tank Readers
- HVAC & Refer / Freezer Monitoring / Management
- DVR and Camera Portal
- Lic Plate Reader / DO
- Car Wash Management
- HR - Time and Attend

# Compounded Complication and Confusion

- Departmental alignment of consoles
  - IT
  - Physical Security / Safety
  - Environmental, HVAC, Refrigeration / Freezers
  - Backoffice HR, fuel, ordering
  - Marketing
  - Compliance
- Outages of some systems often impact several others
- Difficulty in isolating failures and coordinating a fix

# Big Benefits to Breaking down Boundaries

- IT has networking data that is important to store management, marketing, or security
- Store to store routing used by delivery drivers can be used by IT and DMs using just their voice
- Store IoT door and motion sensor data can provide more than just security inputs as part of marketing analytics

# Console Access and Console Training = **Big \$\$\$**

- Many users need only basic status info
- To get basic status requires training and credentials
- Personnel rotation is relatively high
- Too expensive to train everyone on everything
- Expensive to administer access for everyone
- Some consoles are only available at HQ or only at the store or are a part of an “installed” application

# Consolidating Security AND Operations Data



Source: Splunk training materials



# Other operations data a SIEM can collect

- Application specific logs – logon / logoff / performance
- IoT Sensor Data
  - Pump and building Door cycles
  - Pump and aisle Motion
  - Temperature readings
- Payment transaction counts
- Wi-Fi intrusion detection / prevention visitor logs

# How can SIEM get operations data from my vendors?

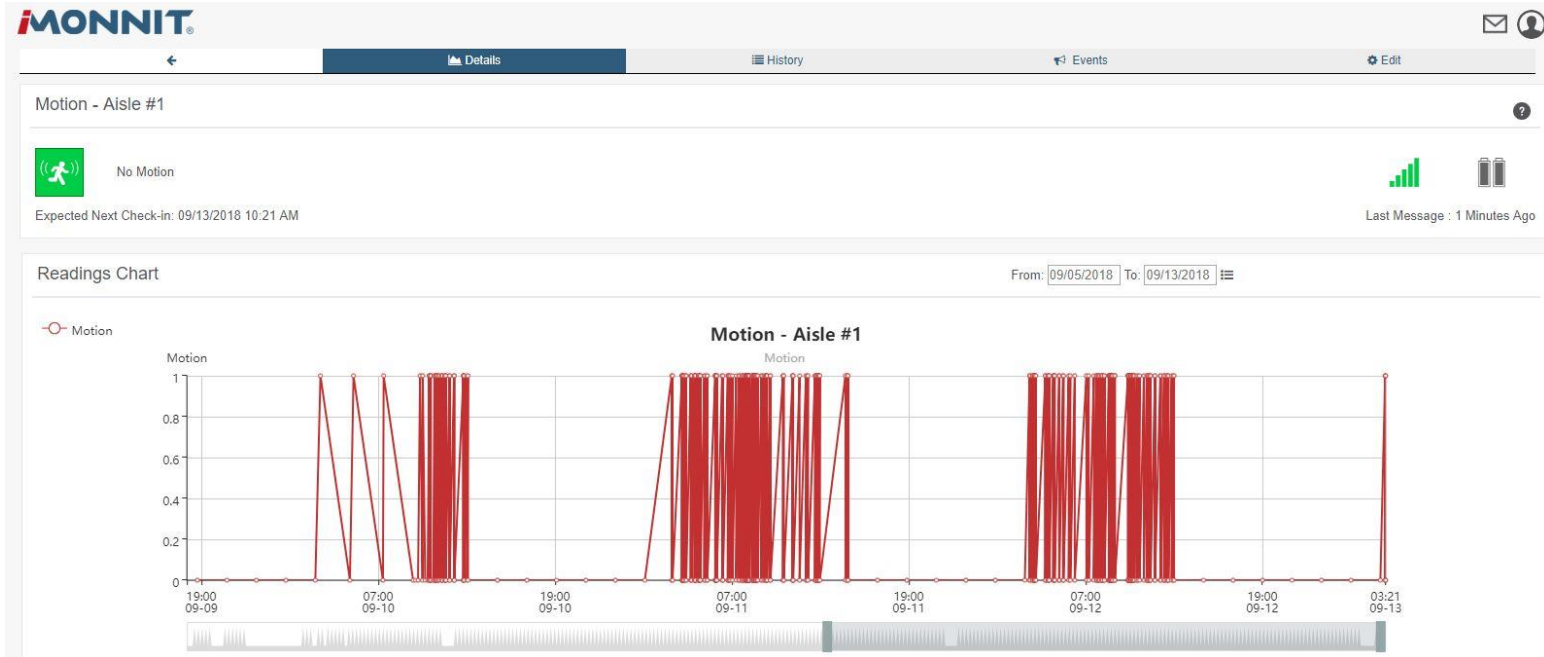
- APIs and Logging
  - Representational State Transfer (REST)
  - Web hooks
  - SYSLOGS
  - Proprietary text logs
- Data formatted in XML, JSON
- Provide basic or token based authentication

# Say what? How do we connect to our vendors again?



Source: Reddit – B-36 bomber, flight engineer station

# Motion Sensor Vendor Cloud Portal




# Configure our SIEM to collect the motion data

splunk > enterprise Apps ▾

## HTTP Event Collector

Data Inputs > HTTP Event Collector

1 Tokens App: All ▾ filter

| Name ▲                         | Actions                | Token Value ⇅                                                                                             |
|--------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------|
| monnit2<br>monnit2 event token | Edit Disable<br>Delete |  5f8-a23f-01caf8f9c4de |

Configure a webhook so vendor can send to our SIEM

## Configure Webhook

### How Webhooks Pass Data to Your Application

A webhook sends data to your application when data is received at the server. You can configure the URL, Headers, Cookies, and query parameters available to add after saving your connection string. Data is compiled as a JSON body and sent via HTTP POST.

|                                                                           |                                                                                    |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Base URL                                                                  | <input type="text" value="https://[REDACTED]001.com:8088/services/collector/raw"/> |
| Send gateway message                                                      | <input type="text" value="Only with sensor mes"/>                                  |
| Authentication                                                            | <input type="text" value="None"/>                                                  |
| <input type="button" value="Save"/> <input type="button" value="Delete"/> |                                                                                    |

Sending: Enabled  
Retries: Enabled

### Headers

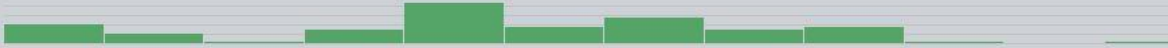
| Key                              | Value                              |                                    |
|----------------------------------|------------------------------------|------------------------------------|
| X-Splunk-Request-Channel         | [REDACTED]-847D-77833BD77132       |                                    |
| Authorization                    | [REDACTED]45f8-a23f-01caf8f9c4de   |                                    |
| <input type="text" value="Key"/> | <input type="text" value="Value"/> | <input type="button" value="Add"/> |

```
index=atcmnmit (sensorMessages{}.dataType=MotionDetect AND sensorMessages{}.dataValue=True) | timechart count
```

✓ 129 events (9/12/18 9:00:00.000 AM to 9/13/18 9:18:18.000 AM) No Event Sampling ▼

Events (129) Patterns Statistics (49) Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect



List ▼ ✎ Format 20 Per Page ▼

< Hide Fields ☰ All Fields

SELECTED FIELDS

a host 1  
a sensorMessages{}.dataType 3  
a source 1  
a sourcetype 1

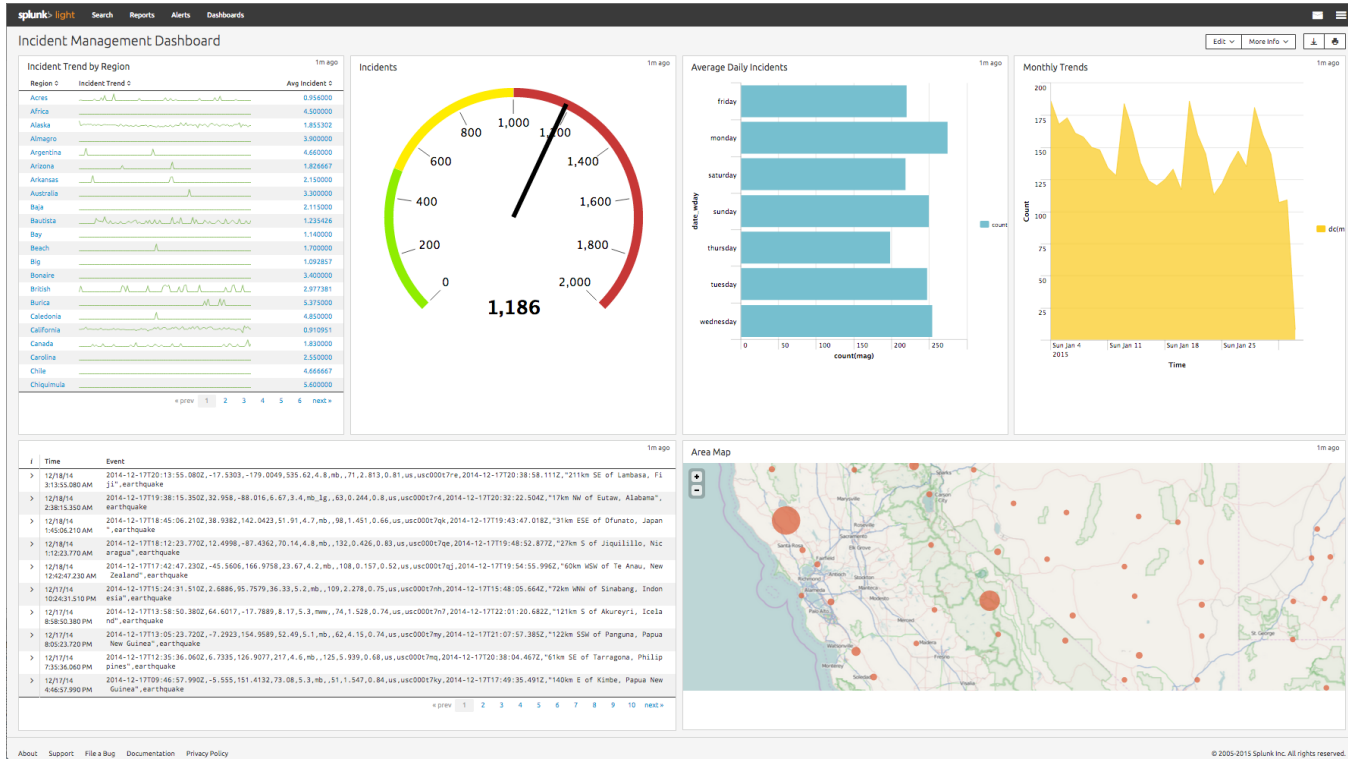
INTERESTING FIELDS

# gatewayMessage.accountID 1  
# gatewayMessage.batteryLevel 1  
# gatewayMessage.count 3  
a gatewayMessage.date 100+  
# gatewayMessage.gatewayID 1  
a gatewayMessage.gatewayName 1  
# gatewayMessage.messageType 1  
# gatewayMessage.networkID 1  
a gatewayMessage.pendingChange 1  
# gatewayMessage.power 1  
# gatewayMessage.signalStrength 1  
a index 1  
# linecount 1  
a punct 1  
# sensorMessages{}.applicationID 3  
# sensorMessages{}.batteryLevel 1

| i | Time                      | Event                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > | 9/13/18<br>8:54:25.000 AM | { [-]<br>gatewayMessage: { [+]<br>}<br>sensorMessages: [ [-]<br>{ [-]<br>applicationID: 101<br>batteryLevel: 100<br>dataMessageGUID: db15c6dd-91e3-4663-827a-5b02ad1293c5<br>dataType: MotionDetect<br>dataValue: True<br>messageDate: 2018-09-13 13:53:58<br>networkID: 50168<br>pendingChange: True<br>plotLabels: Motion<br>plotValues: 1<br>rawData: True<br>sensorID: 420956<br>sensorName: Motion - Aisle #1<br>signalStrength: 95<br>state: 2<br>}<br>]<br>} |

# All Motion Sensor data now in SIEM in standard JSON format

# SIEM Filters, Alerts, and Dashboards



Source: Splunk Answers



# Employees without SIEM Access and Training

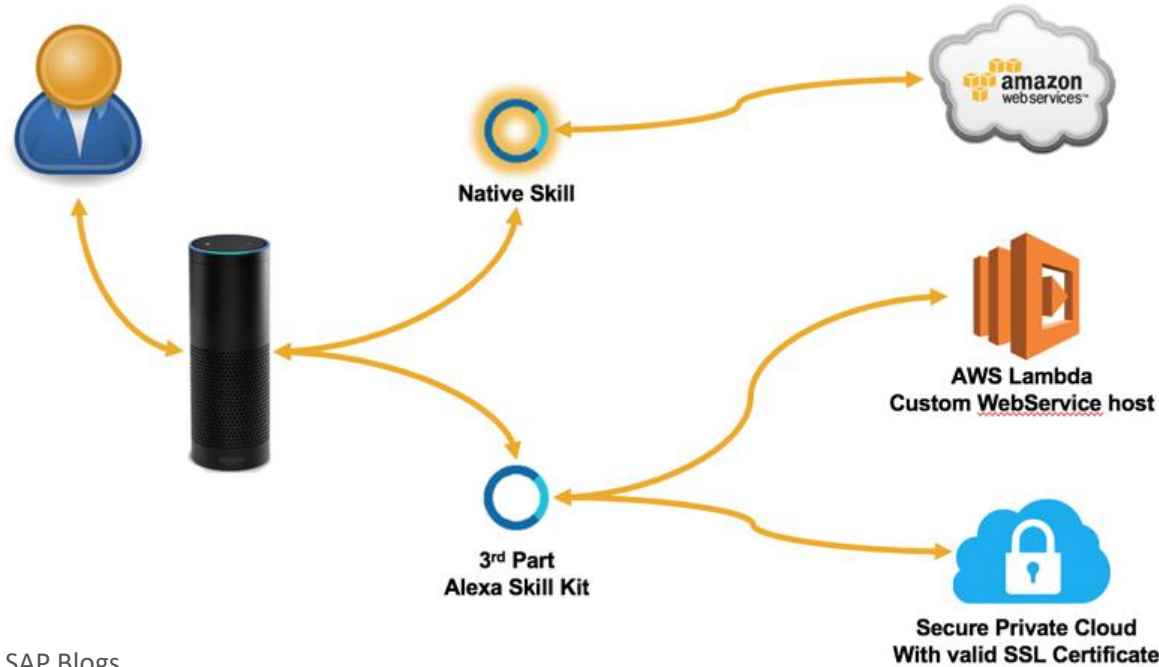


Source: ASPCA

# Operational Intelligence Delivery

- SIEM collects operational data from all available source
  - Store router syslogs
  - Remote Mgmt and Monitoring system
  - Ticketing system
- SIEM filters / alerts opens a tickets and emails vendor
- IT and vendor post comments to ticket
- Alexa Voice Assistant queries SIEM for ticket updates and reads them to the untrained user

# Alexa Native Skills vs. 3<sup>rd</sup> Party Skills



Source SAP Blogs

# What does Alexa look like to users?



Dot



Show

Echo  
(Several  
Variations)



Spot

Source: Amazon

# Protect and Accessorize!



Work smarter, not harder

[Shop now](#)

Electronics / iPad & Tablets / Tablet Accessories / All Tablet Accessories



## Fintie Protective Case for Amazon Echo (1st Generation) - Premium Vegan Leather Cover Sleeve, Mushroom Fantasy

★★★★★ [Write a review](#) [Fintie](#)

**\$11.99**

**Only 3 left!**

**Free shipping**

Arrives by Tuesday, Sep 25

Or get it by **Wed, Sep 19** with faster shipping [Options](#)

Qty:

1

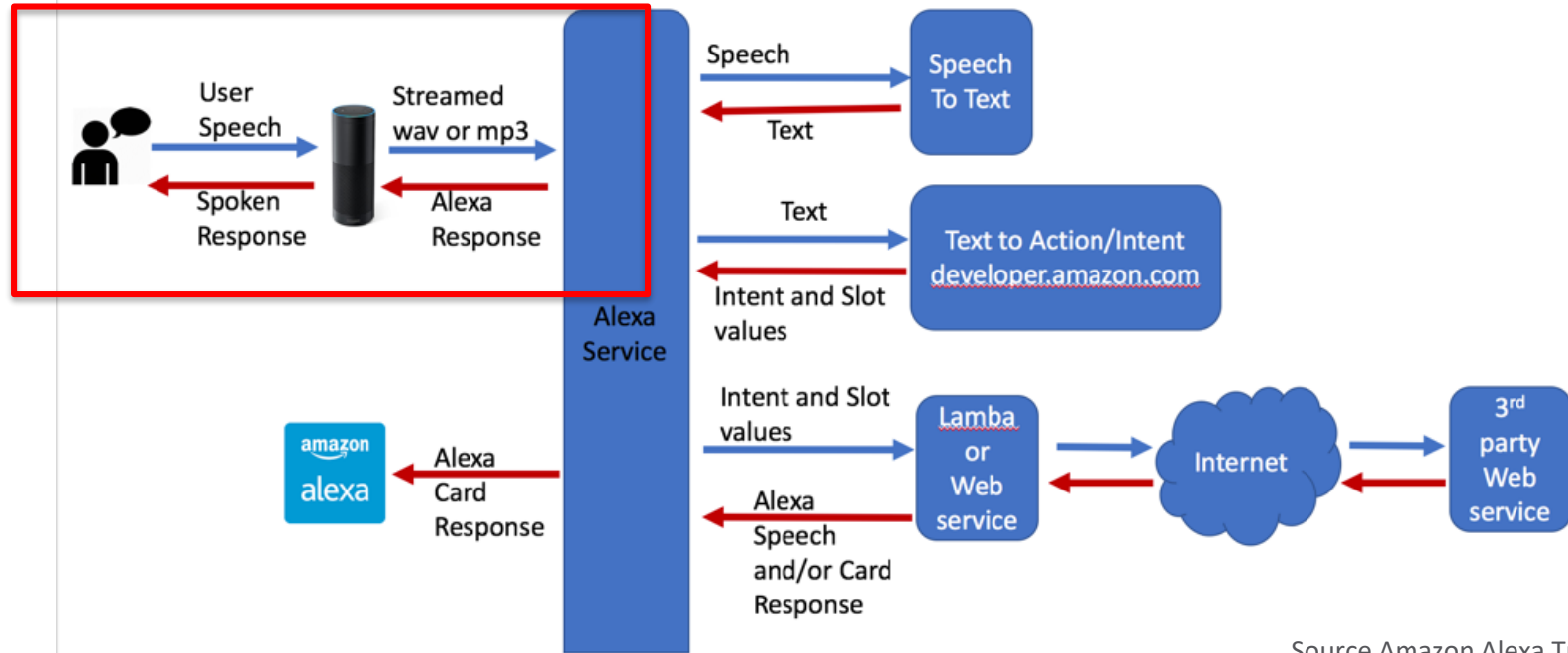
[Add to Cart](#)

[Feedback](#)

Source: Walmart

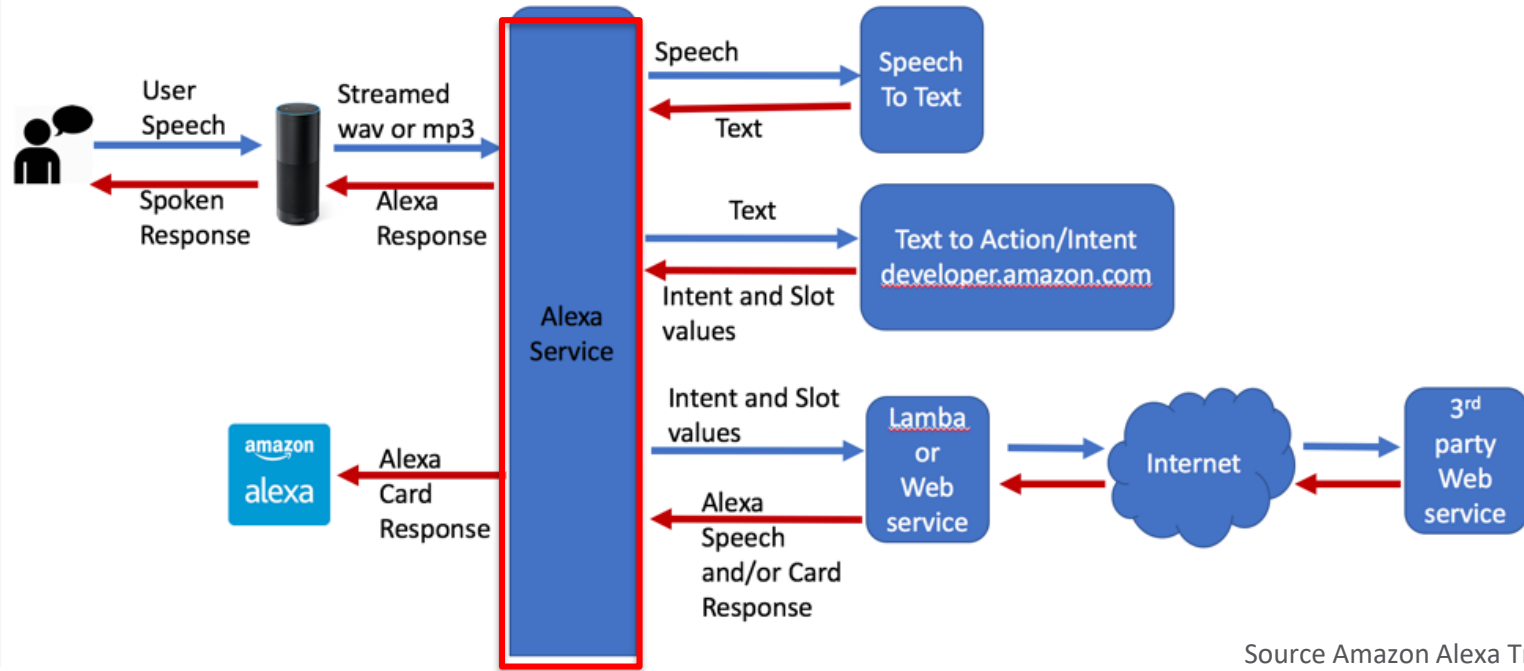
[Tell us if something is incorrect](#)

# Voice Assistant Behind the Scenes – the Skills



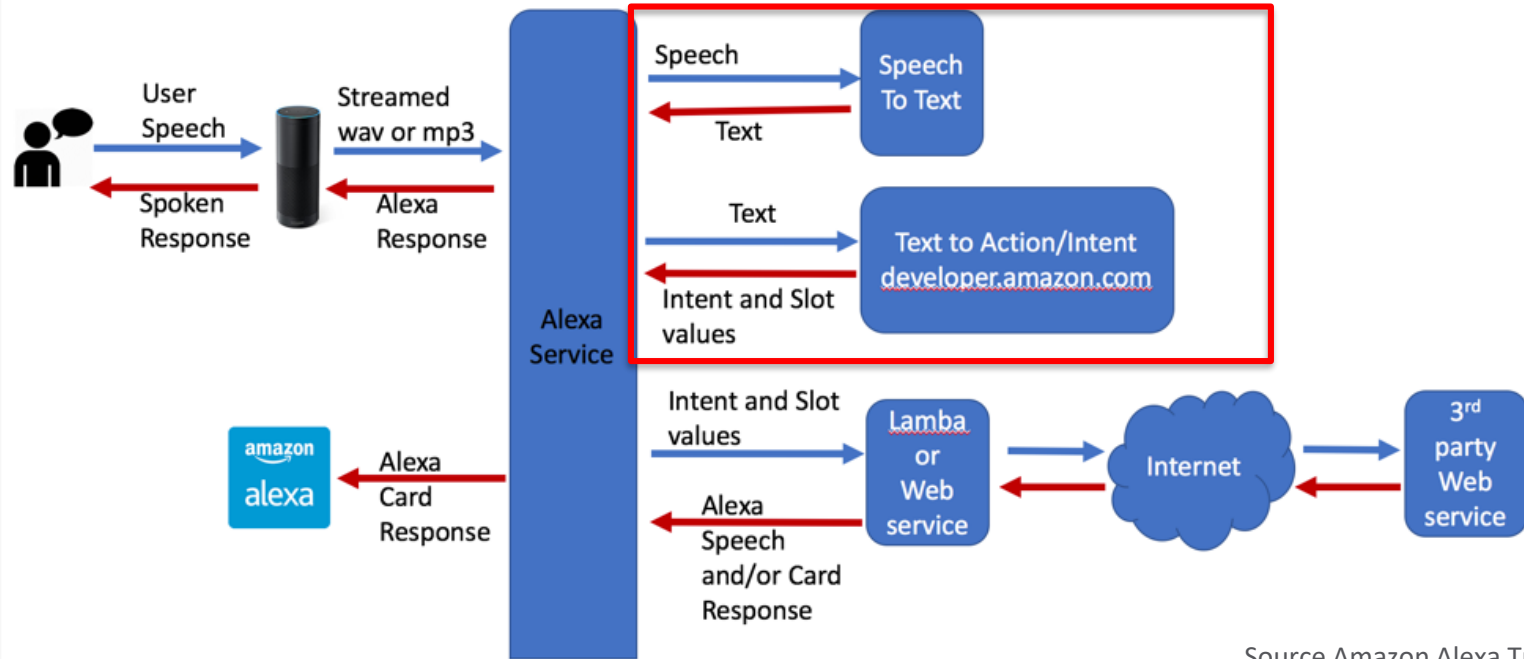
Source Amazon Alexa Training

# Voice Assistant Behind the Scenes – the Skills



Source Amazon Alexa Training

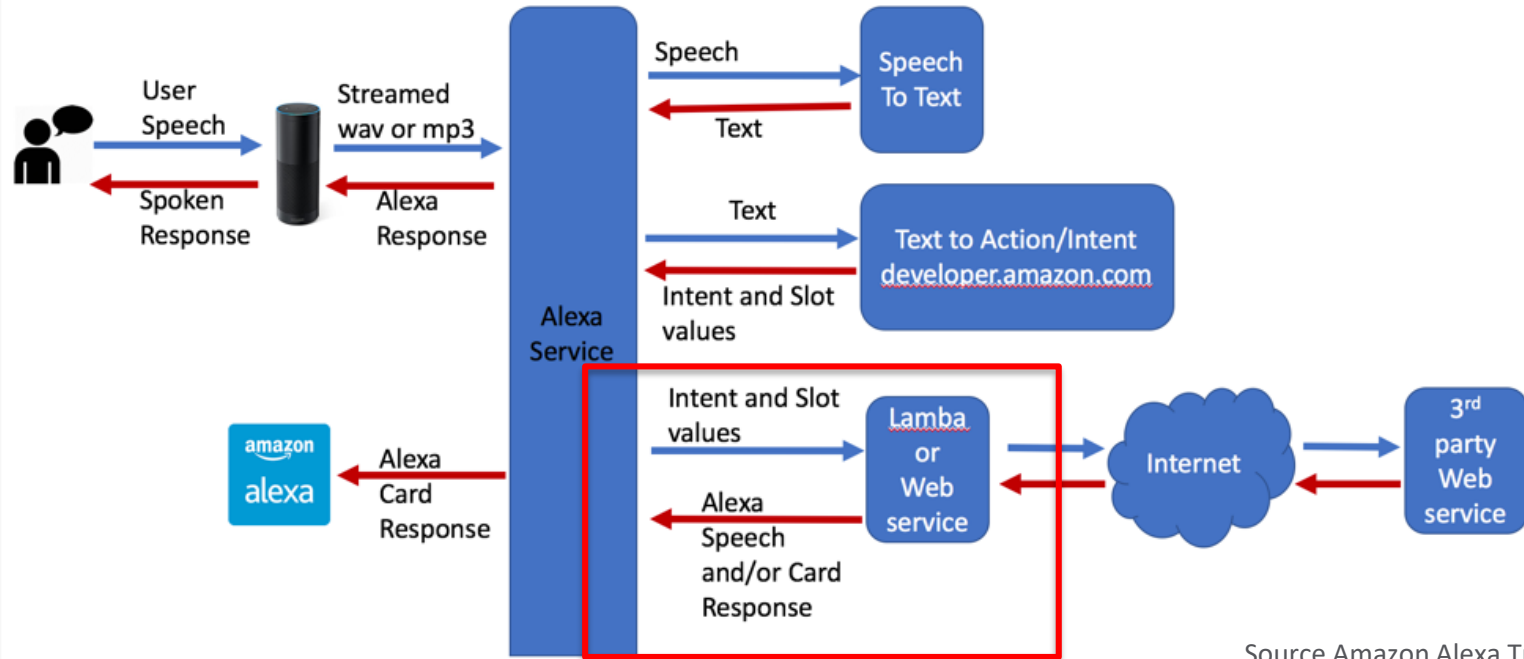
# Voice Assistant Behind the Scenes – the Skills



Source Amazon Alexa Training

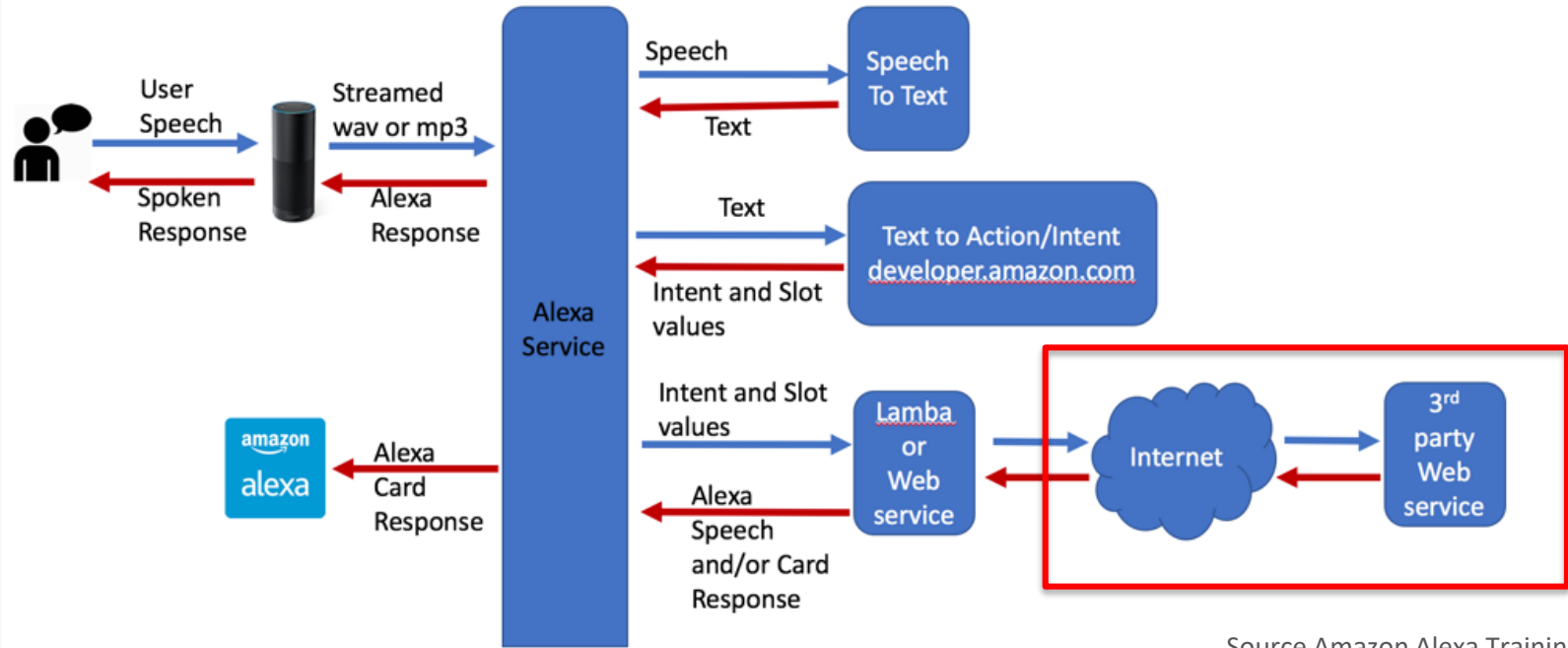


# Voice Assistant Behind the Scenes – the Skills

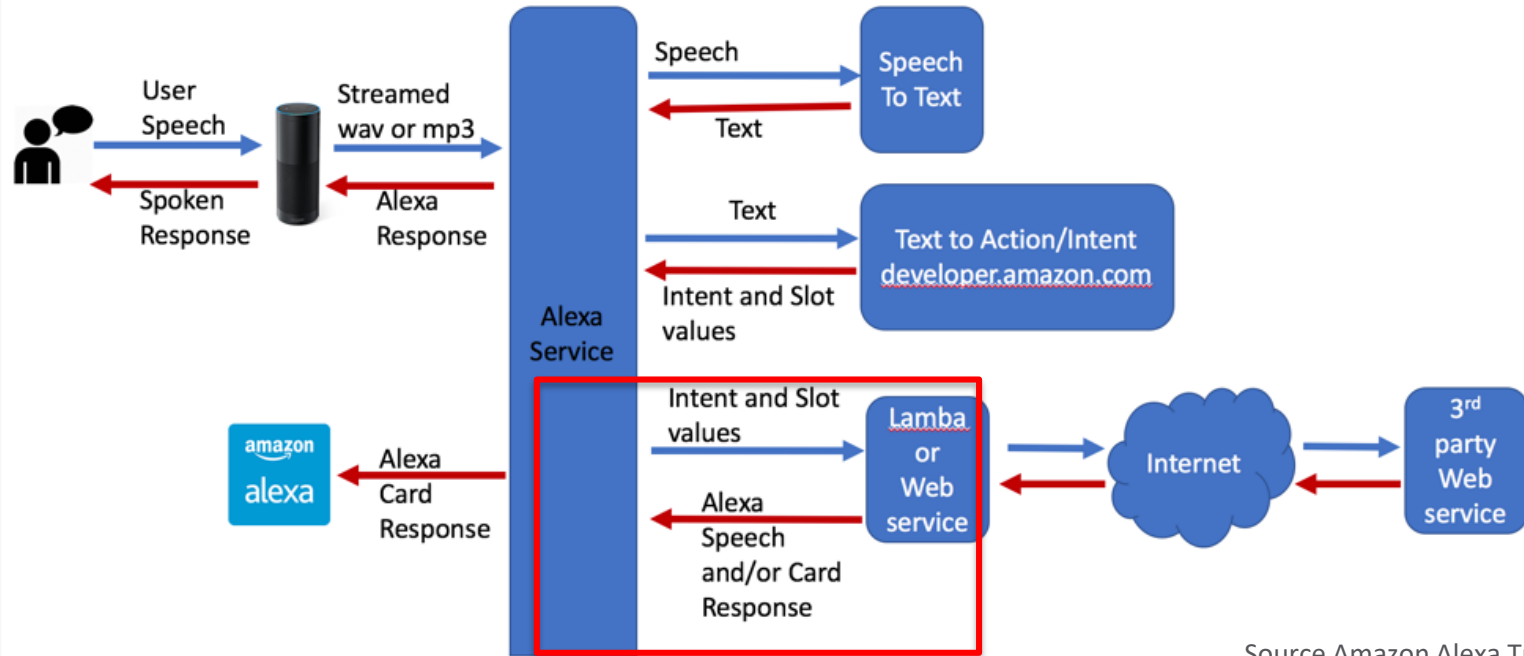


Source Amazon Alexa Training

# Voice Assistant Behind the Scenes – the Skills



# Voice Assistant Behind the Scenes – the Skills



Source Amazon Alexa Training

alexa developer console

< Your Skills OmegaAssistant Build Test Distribution Certification Analytics

English (US) Save Model Build Model

CUSTOM

Interaction Model

Invocation

Intents (6) + Add

openissues

Built-In Intents (5)

- AMAZON.FallbackIntent
- AMAZON.CancelIntent
- AMAZON.HelpIntent
- AMAZON.StopIntent
- AMAZON.NavigateHomeIntent

Slot Types (0) + Add

JSON Editor

Intents / openissues

Sample Utterances (6) ?

What might a user say to invoke this intent?

- what are the open issues
- what are my open issues
- what is going on
- what is happening
- wassup
- what's up

← Identify the Intent

Help train speech recognition to understand what the user wants by providing sample utterances

Keep in mind **all** ages, genders, cultural backgrounds

alexa developer console

< Your Skills Omega Status Build Test Distribution Certification Analytics

English (US) Save Model Build Model

CUSTOM

Interaction Model

Invocation

Intents (6) + Add

- generalstatus
- openissues
- storenumberstatus
  - storenumber
- Built-In Intents (3)
  - AMAZON.CancelIntent
  - AMAZON.HelpIntent
  - AMAZON.StopIntent
- Slot Types (1) + Add
  - AMAZON.NUMBER

Intents / storenumberstatus

Sample Utterances (13) ?

What might a user say to invoke this intent?

- store number {storenumber}
- store {storenumber}
- what's happening at store number {storenumber}
- what's happening at {storenumber}
- is there anything happening at store number {storenumber}

Intent Slots (1) ?

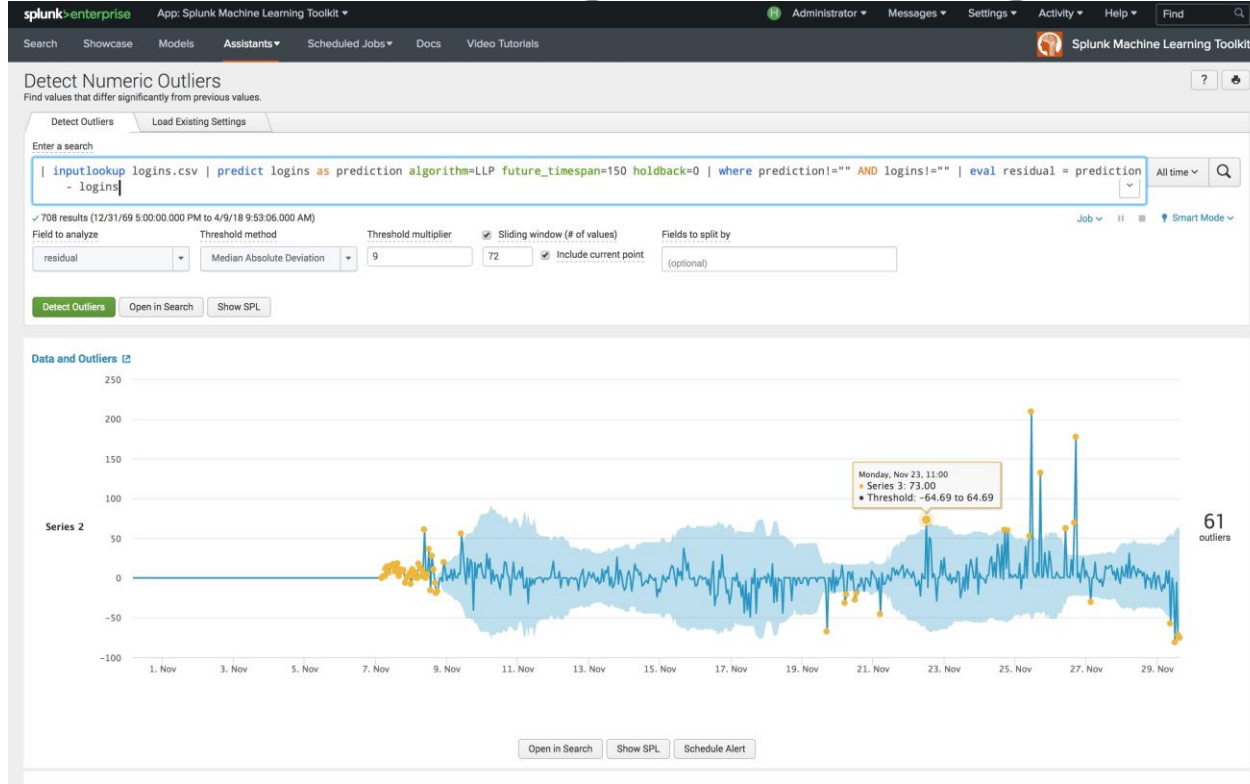
Slot for storenumber in a user request and the slot location identified.

← Slot is a number

# Store Traffic Example

- Door open / close sensors and motion sensors
- SIEM retains door and motion data AND runs analysis
- Alexa retrieves the door and motion data from the SIEM for a requested time frame
- Alexa runs a pre-defined analysis for store traffic using the SIEM and voices all results
- Some Operational Intelligence for Marketing

# SIEM Machine Learning – Detecting Outliers



Source: Business Wire  
Splunk Article

# Operational Intelligence Approach Summary

- Use a SIEM and consolidate both security AND operations data into it
- Use the SIEM to develop operational intelligence for all employees who need it
- Couple a voice assistant like Alexa to the SIEM to share operational intelligence
- Don't be afraid to get help from an MSSP with SIEM and voice assistant experience





- Website: [www.conexxus.org](http://www.conexxus.org)
- Email: [info@conexxus.org](mailto:info@conexxus.org)
- LinkedIn Profile: [Conexxus.org](https://www.linkedin.com/company/conexxus.org)
- Follow us on Twitter: [@Conexxusonline](https://twitter.com/Conexxusonline)
- Speaker:  
George Sconyers, Senior Solutions Architect,  
Omega ATC  
[george.sconyers@omegaatc.com](mailto:george.sconyers@omegaatc.com)