Your Systems Are Talking to You

Presenter:
George Sconyers
Senior Solutions Architect
Omega ATC
Agenda

• Housekeeping
• Presenters
• About Conexxus
• Presentation
• Q & A
Housekeeping

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

- YouTube (youtube.com/conexxusonline)
- Website Link (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
# Presenters

**Conexxus Host**
- Allie Russell
- Conexxus
  - arussell@conexxus.org

**Moderator**
- Kara Gunderson
- Chair, Data Security Committee
- POS Manager, CITGO Petroleum
  - 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
<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 24, 2018</td>
<td>QIR in the World of Retail Petroleum</td>
<td>Chris Bucolo Todd Rosen</td>
<td>ControlScan</td>
</tr>
<tr>
<td>June 21, 2018</td>
<td>How can we leverage data science to more effectively detect security threats?</td>
<td>Thomas Duncan Ashwin Swamy</td>
<td>Omega ATC</td>
</tr>
<tr>
<td>July 26, 2018</td>
<td>Roadmap to a Vulnerability Disclosure Program</td>
<td>Joe Basirico</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>August 23, 2018</td>
<td>Moving Toward Outdoor EMV</td>
<td>Linda Toth</td>
<td>Conexxus</td>
</tr>
<tr>
<td>September 20, 2018</td>
<td>Your Systems Are Talking to You!</td>
<td>George Sconyers</td>
<td>Omega ATC</td>
</tr>
<tr>
<td>November 2018</td>
<td>Building a Scalable Security Engineering Team</td>
<td>Joe Basirico</td>
<td>Security Innovation</td>
</tr>
</tbody>
</table>
NACS Show
October 7-10, 2018
Las Vegas, NV

Conexxus thanks our 2018 Annual Diamond Sponsors!

mSHIFT
Relevant. Mobile. Solutions.

Stuzo

DIEBOLD NIXDORF

GILBARCO VEEDER-ROOT

Cybera
Simplify Security and Networks
Your Systems Are Talking to You

Bringing Operational Intelligence to Convenience Retail
# Good Information – What is it exactly?

## FEATURES OF GOOD INFORMATION

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate</td>
<td>Should be true and correct</td>
</tr>
<tr>
<td>Complete</td>
<td>No key facts missing</td>
</tr>
<tr>
<td>Timely</td>
<td>Delivered on time and up-to-date</td>
</tr>
<tr>
<td>Relevant</td>
<td>Meets the need of the audience</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost should be no more than the benefit</td>
</tr>
<tr>
<td>Effective</td>
<td></td>
</tr>
<tr>
<td>Meaningful</td>
<td>Is it easy to understand</td>
</tr>
</tbody>
</table>

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
**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 to add after saving your connection string. Data is compiled as a JSON body and sent via HTTP POST.

<table>
<thead>
<tr>
<th>Base URL</th>
<th>https://&lt;redacted&gt;.com:8088/services/collector/raw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send gateway message</td>
<td>Only with sensor mos</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
</tbody>
</table>

**Headers**

- **Key**: X-Splunk-Request-Channel
  - **Value**: 847D-77B33BD77132
- **Key**: Authorization
  - **Value**: 45F9-a23f-01caf8f9c4de

Save | Delete | Add
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. 3rd Party Skills

Source SAP Blogs
What does Alexa look like to users?

Dot

Echo (Several Variations)

Show

Spot

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

$11.99
Only 3 left!
Free shipping
Arrives by Tuesday, Sep 25
Or get it by Wed, Sep 19 with faster shipping Options

Source: Walmart
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

Source Amazon Alexa Training
Voice Assistant Behind the Scenes – the Skills

Source Amazon Alexa Training
Help train speech recognition to understand what the user wants by providing sample utterances. Keep in mind all ages, genders, cultural backgrounds.
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
Q & A
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Profile: Conexxus.org
• Follow us on Twitter: @Conexxxusonline
• Speaker:
  George Sconyers, Senior Solutions Architect, Omega ATC
  george.sconyers@omegaatc.com