“Can We See Everything That We Need To In The Cloud? – That’s A Question We Just Can’t Answer Yet”
“Our SaaS Providers Handle The Security Of The Cloud Service But We Are Worried About Cloud Being Used As An Attack Vector”
“Hahahahahaahhahahaahhaahhaaahaahaahhaahaahhaaahhaahhahaaaaahhahaahhaahhaahhahhaahhahaaahhahaahhaahaha”

- Customer when asked how the cloud shift was going
Using ES to Secure the Cloud
Relief from the headache in the cloud

David Naylor | Security Analyst, Georgetown University
Craig Vincent | Regional Security SME, Splunk
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.
Objectives

- Common challenges associated with cloud transition
- Enterprise Security as the cloud-ready SIEM
- Cloud Terminology
- Georgetown-specific solutions
About Us
Craig Vincent

- Sales Engineer & Regional Security
- Subject Matter Expert

Universities & Colleges
State & Local Governments
Medical Centers
About Us
David Naylor

- Security Analyst at Georgetown University
Challenges of Moving to the Cloud
Challenges of Moving to the Cloud

Lack of Visibility
61% of survey respondents say it's difficult to get equivalent visibility into cloud-based workloads.

Enterprise Strategy Group 2017
Challenges of Moving to the Cloud

Cloud is ephemeral

- Economics of the cloud are built around change
- Ensuring Security for a constantly changing ecosystem is difficult
Challenges of Moving to the Cloud

Knowledge Gap

- Not your systems
- Unclear where the line of security responsibility lies
- Difficult to understand the cloud terminology and systems
Introduction to Enterprise Security
Introduction to Enterprise Security
Advanced Threats are Hard to Find

Cyber Criminals

Nation States

Insider Threats

100%
Valid credentials were used

40
Average # of systems accessed

229
Median # of days before detection

67%
Of victims were notified by external entity

Introduction to Enterprise Security

New Approach to Security is needed

- Human directed
- Goal-oriented
- Dynamic (adjust to changes)
- Coordinated
- Multiple tools & activities
- New evasion techniques

Fusion of people, process, & technology

- Contextual and behavioral
- Rapid learning and response
- Share info & collaborate
- Analyze all data for relevance
- Leverage IOC & Threat Intel
Introduction to Enterprise Security
Why Enterprise Security

- Native to the Cloud
- Integrates on premise Security with Cloud Security
  - Single Pane of Glass
  - Single Workflow
- Flexibility
  - Able to ask any question
  - Change friendly
Introduction to Enterprise Security

Prevent
Detect
Investigate
Respond
Uncovering the Cloud
Comparison of Cloud Services
Comparison of Cloud Services
Security Responsibility

**Software as a Service**
- Access and Authentication
- Data Transit to the Cloud
- Misuse

- Other security responsibilities tend to lie with the vendor

**Platform as a Service**
- Application Security
- Auditing

- Networking Configuration

**Infrastructure as a Service**
- Responsible for all security except for infrastructure security
End-to-End Visibility with AWS and Splunk

Native path (via AWS)

Push path (via Splunk HEC)

Pull path (via Splunk Modular Input or DB Input)
Important AWS Security Logs
Not all logs are created equal

- **VPC Flow Logs**
  - Provides key network insights, equivalent of FW or NetFlow

- **ELB/CloudFront/S3 Access Logs**
  - Provides History of requests to resources

- **AWS CloudTrail**
  - Provides history of AWS API Calls

- **AWS Config**
  - AWS Resources Inventory, Config History, Config Change Notifications
Georgetown ES
Onboarding data from a variety of cloud service providers
• Splunk has prebuilt collection methods for: AWS, Box, Salesforce
• Custom collection methods for: Google Apps for Education, Acquia, Duo
• Data model mapping was challenging but rewarding
• Moving to Splunk Add-on Builder to simplify the process

Notable Events are useful once tweaked
• Needed to adapt to the realities of Georgetown

Always looking to add more data
Examples
AWS security groups are the firewall policy for the EC2 instance.

At Georgetown, we flag all instances that are set to allow all to push users towards specific firewall rules.
Gather cloud context by updating ES asset table using AWS Description logs.
<table>
<thead>
<tr>
<th></th>
<th>ip</th>
<th>mac</th>
<th>nt_host</th>
<th>dns</th>
<th>owner</th>
<th>priority</th>
<th>lat</th>
<th>long</th>
<th>city</th>
<th>country</th>
<th>bunit</th>
<th>cate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6.0.0.1-9.0.0.0</td>
<td>00:15:70:91:df:6c</td>
<td></td>
<td></td>
<td></td>
<td>low</td>
<td>41.040855</td>
<td>28.986183</td>
<td>Istanbul</td>
<td>TR</td>
<td>apac</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.2.3.4</td>
<td></td>
<td></td>
<td>CОРР1.acmetech.com</td>
<td></td>
<td>medium</td>
<td>38.959405</td>
<td>-77.04</td>
<td>Washington D.C.</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>high</td>
<td>37.694452</td>
<td>-121.894461</td>
<td>Pleasanton</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>5</td>
<td>192.168.12.9-192.168.12.9</td>
<td></td>
<td>storefront</td>
<td></td>
<td></td>
<td>critical</td>
<td>32.931277</td>
<td>-96.818167</td>
<td>Dallas</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>6</td>
<td>2.0.0.0/8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>low</td>
<td>50.84436</td>
<td>-0.98451</td>
<td>Havant</td>
<td>UK</td>
<td>emea</td>
<td>psci</td>
</tr>
<tr>
<td>7</td>
<td>192.168.15.8-192.168.15.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>medium</td>
<td>38.959405</td>
<td>-77.04</td>
<td>Washington D.C.</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>8</td>
<td>192.168.0.0/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>high</td>
<td>37.694452</td>
<td>-121.894461</td>
<td>Pleasanton</td>
<td>USA</td>
<td>americas</td>
<td>iso2</td>
</tr>
<tr>
<td>9</td>
<td>5.6.7.8</td>
<td>00:12:cf:30:27:b5</td>
<td>millenium-falcon</td>
<td></td>
<td></td>
<td>critical</td>
<td>32.931277</td>
<td>-96.818167</td>
<td>Dallas</td>
<td>USA</td>
<td>americas</td>
<td>nerc</td>
</tr>
<tr>
<td>10</td>
<td>192.168.15.9-192.168.15.9</td>
<td></td>
<td></td>
<td>acme\textbackslash{}files\textbackslash{}server</td>
<td>low</td>
<td>medium</td>
<td>38.959405</td>
<td>-77.04</td>
<td>Washington D.C.</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>11</td>
<td>9.10.11.12</td>
<td>00:16:5d:10:08:9c</td>
<td></td>
<td></td>
<td></td>
<td>high</td>
<td>37.694452</td>
<td>-121.894461</td>
<td>Pleasanton</td>
<td>USA</td>
<td>americas</td>
<td>ema</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>00:25:bc:42:fa:60-00:25:bc:42:fa:6f</td>
<td></td>
<td></td>
<td></td>
<td>critical</td>
<td>32.931277</td>
<td>-96.818167</td>
<td>Dallas</td>
<td>USA</td>
<td>americas</td>
<td>virtu</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td>PA\textbackslash{}DC02</td>
<td></td>
<td>high</td>
<td>37.694452</td>
<td>-121.894461</td>
<td>Pleasanton</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td>ACME\textbackslash{}a\textbackslash{}PP</td>
<td></td>
<td>critical</td>
<td>32.931277</td>
<td>-96.818167</td>
<td>Dallas</td>
<td>USA</td>
<td>americas</td>
<td>psci</td>
</tr>
</tbody>
</table>
# Georgetown & ES

## Cloud Data Enrichment

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest</td>
<td>1</td>
</tr>
<tr>
<td>dest_asset_id</td>
<td>1</td>
</tr>
<tr>
<td>dest_asset_tag</td>
<td>4</td>
</tr>
<tr>
<td>dest_bunit</td>
<td>1</td>
</tr>
<tr>
<td>dest_category</td>
<td>1</td>
</tr>
<tr>
<td>dest_city</td>
<td>1</td>
</tr>
<tr>
<td>dest_country</td>
<td>1</td>
</tr>
<tr>
<td>dest_is_expected</td>
<td>1</td>
</tr>
<tr>
<td>dest_lat</td>
<td>1</td>
</tr>
<tr>
<td>dest_long</td>
<td>1</td>
</tr>
<tr>
<td>dest_nt_host</td>
<td>1</td>
</tr>
<tr>
<td>dest_owner</td>
<td>1</td>
</tr>
<tr>
<td>dest_pci_domain</td>
<td>2</td>
</tr>
<tr>
<td>dest_priority</td>
<td>1</td>
</tr>
<tr>
<td>dest_requires_av</td>
<td>1</td>
</tr>
<tr>
<td>dest_should_timesync</td>
<td>1</td>
</tr>
<tr>
<td>dest_should_update</td>
<td>1</td>
</tr>
</tbody>
</table>

### Reports
- Top values
- Events with this field

### Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME-001</td>
<td>11:25:50.000 AM</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>9/25/17</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11:25:35.000 AM</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>9/25/17</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11:25:19.000 AM</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>9/25/17</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11:25:14.000 AM</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>9/25/17</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host</td>
<td></td>
</tr>
</tbody>
</table>
Georgetown & ES
Using Lambda to find bad configurations

AWS config rules use a lambda instance to affordably ensure configuration compliance
Areas For Future Work

- Adaptive Response
  - Disabling AWS instances from within Splunk
1. Understand your level of responsibility
2. IaaS providers provide rich logging for increased visibility
3. ES helps with the entire IR lifecycle
CLOSING REMARKS & CALL TO ACTION
Public Sector & Education Industry Day at .conf2017
Wednesday, September 27th, 2017
11:00am-7:00pm | Room 202A

400+ Attendees
5 Sessions
15 Customer Speakers
10+ Birds of Feather Sessions
Public Sector Birds of a Feather

Meal Room (Lower Level Hall B)

Wednesday, September 27th
1:15pm-2:00pm

Compliance
Security
IT Modernization
Situational Awareness
Mission Analytics

Institutional Intelligence
Learning Analytics
Supply Chain
Smart Communities
Cloud
Public Sector Reception

Walter E. Washington Convention Center
South Pre-Function Space on Level 3

5:30pm-7:00pm

Join Splunk and your peers for hors d'oeuvres and drinks. Unwind, discuss hot topics and share your stories!

*.conf badge required for entry
Thank You

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

splunk> .conf2017