© 2017 SPLUNK INC.

"Can We See Everything That We Need To In The Cloud? – That's A Question We Just Can't Answer Yet"

Private University



© 2017 SPLUNK INC.

"Our SaaS Providers Handle The Security Of The Cloud Service But We Are Worried About Cloud Being Used As An Attack Vector"

Large State School





"Hahahahahaahhahaaha"

- 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

spiunk

Forward-Looking Statements

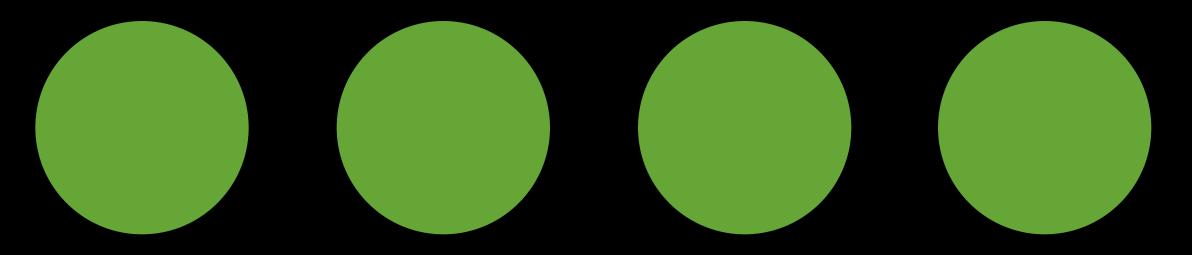
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.

.screen?product_id=FL-DSH-01&JSE

Objectives



Common challenges associated with cloud transition

> /oduct.screen?product_id=FL-DSH-01&JESSIONID=SD55L7FF6AD /oldlink?item id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1

Enterprise Security as the cloud-ready SIEM

URPRISE&JSES

Cloud Terminology

Georgetownspecific solutions



About Us Craig Vincent

Sales Engineer & Regional Security Subject Matter Expert



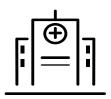
Splunk Mandiant





Universities & Colleges

State & Local Governments



Medical Centers



1 "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/catt.doraction=purchase6itemId=EST-6&product_id=F1-5W. 40:56:116 "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/catt.doraction=purchase6itemId=EST-3@Aproduct_id=F1-5W. 40:56:116 "GET /product.screen?product_id=FL-DSM-01&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/catt_doraction=purchase6itemId=EST-3@Aproduct_id=F1-5W. 40:56:116 "GET /product.screen?product_id=FL-DSM-01&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/catt_doraction=purchase6itemId=EST-3@Aproduct_id=F1-6W. 450 "450 "GET /pld1ink?item_id=EST-2@AJSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup.screen?category.id=EST-6&Product_id=F1-6&Product_id=F

About Us

David Naylor

Security Analyst at Georgetown University

.v.screen?category_id=GIFT5&i5ESSIONID=S015L4FF18ADFF10 HTTP 1. /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L9F1ADFF3 T /oldlink?item_id=EST-26&JESSIONID=SD55L9F1ADFF3 HTTP 1.1" 7 14 .com

200 13:





Challenges of Moving to the Cloud



Challenges of Moving to the Cloud

Lack of Visibility



© 2017 SPLUNK INC.

61% of survey respondents say its 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

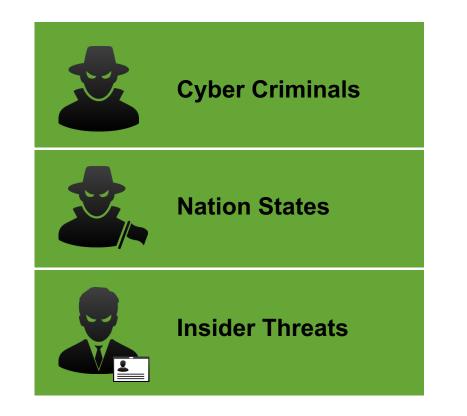
- Not your systems
- Unclear where the line of security responsibility lies
- Difficult to understand the cloud terminology and systems



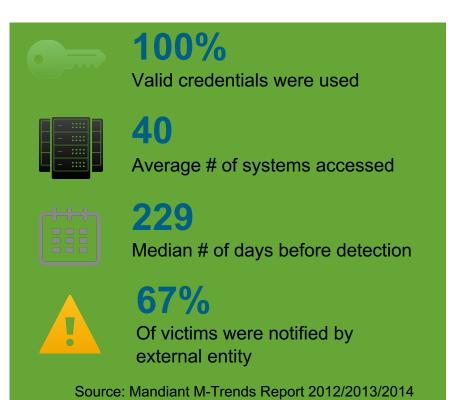




Advanced Threats are Hard to Find



product.screen?product_id=FL-DSH-01&JSESSIONID=SD5





New Approach to Security is needed



Attack Approach

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

Security Approach

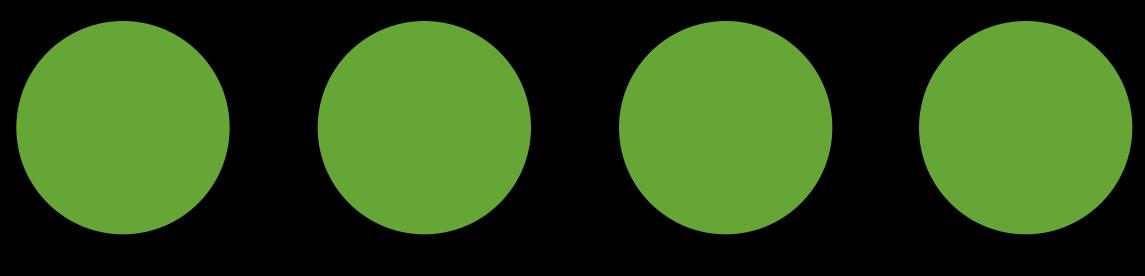
- Fusion of <u>people</u>, <u>process</u>, & <u>technology</u>
- Contextual and behavioral
- Rapid learning and response
- Share info & collaborate
- Analyze all data for relevance
- Leverage IOC & Threat Intel



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





Prevent

Detect

Wfoduct.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1 // toomage/id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1 URPRISE&JSESSI

200 1318

Investigate

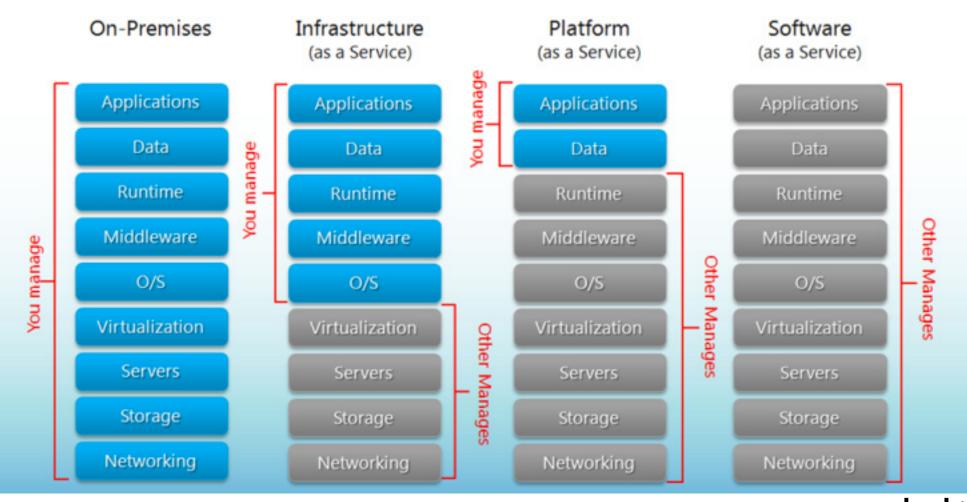
Respond



Uncovering the Cloud



Comparison of Cloud Services



splunk'> .conf2017

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

laaS

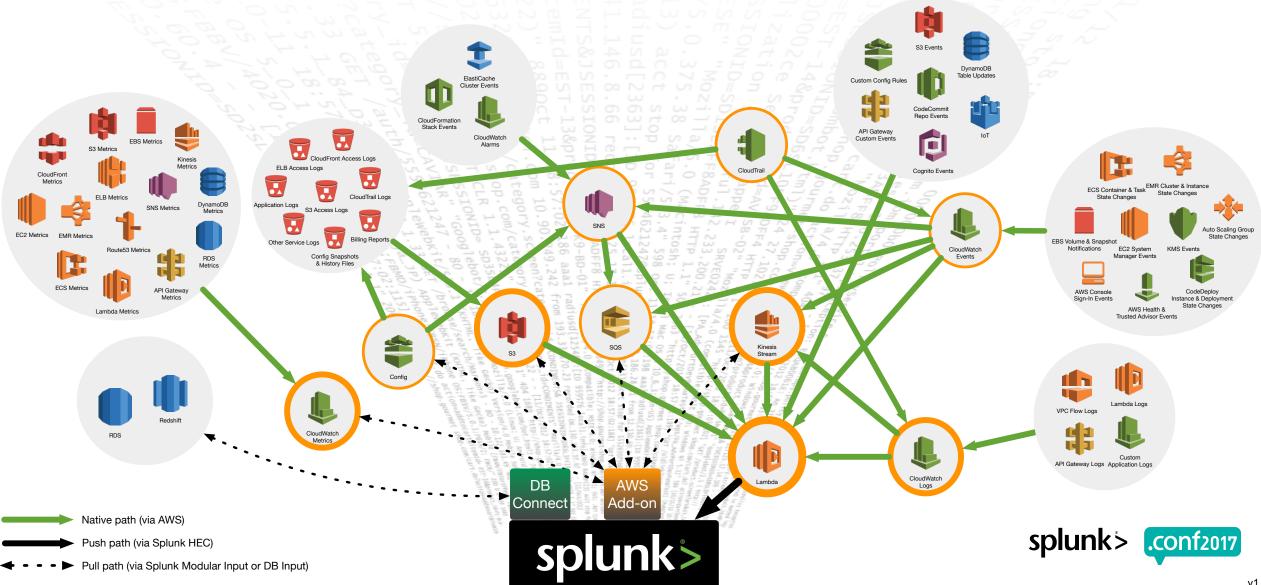
Networking Configuration

Infrastructure as a Service

• Responsible for all security except for infrastructure security



End-to-End Visibility with AWS and Splunk



v1.1

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



splunk

CONf2017

State of the Union @ Georgetown

Current Successes and Limitations

- 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







© 2017 SPLUNK INC

Georgetown & ES

Policy Enforcement Correlation Search

v Correlation S to Content Management	Search	
Correlation Search		
Search Name *	Policy- Insecure AWS Security Group	
Application Context *	Enterprise Security ~	
UI Dispatch Context *	Enterprise Security ~	
	Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.	
Description	Detects security groups that are set to allow all traffic	
	Describes what kind of issues this search is intended to detect.	

- 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

splunk>

.conf2017

Georgetown & ES Cloud Data Enrichment

۲	•						
splunk> App: Search & Reporting ~ Messages ~ Settings ~ Activity ~ Find							
Search Datasets Reports Alerts Dashboards							
Q New Search							
<pre>(index="main" sourcetype="aws:description" aws_account_id="*" region="*" sou eventstats latest(_time) as latest_time eval latest_time=relative_time(latest_time,"-55m") where ('_time' > latest_time) dedup id sortbytime dedup private_ip_address eval ip=if(ip_address!="null",private_ip_address." ".ip_address,private_ipp eval dns=if(dns_name!="",private_dns_name." ".dns_name,private_dns_name) rename "tags.App Manager" as tagsappmanager eval owner=if(isnull(tagsappmanager),"",tagsappmanager) eval priority="medium" eval platform=if(platform=="null",""," ".platform) eval category=placement." ".instance_type." ".state.platform rename vm_name as nt_host table ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,catego</pre>	p_address)		,should_ti	mesync,s	should_update,requires_av		
\sim 44 events (8/18/17 5:00:00.000 PM to 8/19/17 5:07:05.000 PM) No Event Sampling \sim							
Events Patterns Statistics (44) Visualization							
100 Per Page ∽							
ip ≎ / mac ≎ nt_host ≎ dns ≎ / owner ≎ pri	riority 🌣 🛛 lat 🜣	long \diamond city \diamond	country 0	bunit 0	category 0		

 Gather cloud context by updating ES asset table using AWS Description logs



Georgetown & ES Cloud Data Enrichment

Edit Lookup File

simple_asset_lookup

1	ір	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	cate
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul	TR	арас	
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas	
4				CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton	USA	americas	pcilc
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167	Dallas	USA	americas	рсі
6	2.0.0/8					low	50.84436	-0.98451	Havant	UK	emea	pci s
7	192.168.15.8-192.168.15.10					medium	38.959405	-77.04	Washington D.C.	USA	americas	pcilt
8	192.168.0.0/16					high	37.694452	-121.894461	Pleasanton	USA	americas	iso2
9	5.6.7.8	00:12:cf:30:27:b5	millenium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerc
10	192.168.15.9-192.168.15.9		acmefileserver			low	50.84436	-0.98451	Havant	UK	emea	рсі
11	192.168.15.9-192.169.15.27					medium	38.959405	-77.04	Washington D.C.	USA	americas	
12	9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	ema
13		00:25:bc:42:f4:60-00:25:bc:42:f4:6F				critical	32.931277	-96.818167	Dallas	USA	americas	virtu
14		00:25:bc:42:f4:60-00:25:bc:42:f4:60				low	50.84436	-0.98451	Havant	UK	emea	рсі
15		00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas	
16				PA-dC02		high	37.694452	-121.894461	Pleasanton	USA	americas	pcilc
17				ACMEaPP		critical	32.931277	-96.818167	Dallas	USA	americas	pci c

/buttercup

Set /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10AOFF10 HTTP 1.1" 404 720 "http://butterCub.m/cart.do?ac S6:156] "GET /product.screen?product_id=FL-DSH=01&JSESSIONID=SD55L7F6ADFF9 HTTP 1.1" 404 3322 "http://butterCub.mo/cart.do?ac "468 125.17 id ink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://butterCub.mo/cart.do?ac "65 125.17 id ink?item_id=EST-26&JSESSIONID=SD5SL9F1ADFF3 HTTP 1.1" 200 1318 "cart.do?acGET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9F1ADFF3 HTTP 1.1" 200 1318 "cart.do?acGET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9F1ADF73 HTTP 1.1" 200 1318 "cart.do?acGET /oldlink?item_id=ES



Georgetown & ES

Cloud Data Enrichment

P 1.1" 200 1318 "http://www.sesSSIONID=SD95L4FF4APF7/http://www.sec.ave.sov

- a dest 1
- a dest_asset_id 1
- a dest_asset_tag 4
- a dest_bunit 1
- a dest_category 1
- a dest_city 1
- a dest_country 1
- a dest_is_expected 1
- # dest_lat 1
- # dest_long 1
- a dest_nt_host 1
- a dest_owner 1
- a dest_pci_domain 2
- a dest_priority 1

'Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 728 "http://butterCub_om/c '56:156] "GET /product.screen?product_id=FL-DSH=01&JSESSIONID=SDSSJ7F6ADFF9 HTTP 1.1" 404 3322 "http://butter " 468 125.17 id.tem.id=EST-26&JSESSIONID=SDSSL9FF1ADFF3 HTTP 1.1" 200 1318 "http://butter.do?acff7.org/catef7.o

468 125 17 1

- a dest_requires_av 1
- a dest_should_timesync 1
- a dest_should_update 1

neports Top values Events with this field

Values

ACME-001

	11.25.57.000 AIM	hos
>	9/25/17	Mon
	11:25:50.000 AM	hos
>	9/25/17	Mon
	11:25:35.000 AM	hos
>	9/25/17	Mon
	11:25:19.000 AM	hos
>	9/25/17	Mon
	11:25:14.000 AM	hos
>	9/25/17	Mon



Georgetown & ES

Using Lambda to find bad configurations

		•		
aws Servic	ces 🗸 Resource Groups 🗸 🛧		۵. Virginia	▪ Support ▪
AWS Config Dashboard	Rules			Status 😧
Rules Resources Settings	Rules represent your desired configuration so	settings. AWS Config evaluates whether your resource configurations comply w	with relevant rules and summarizes the results in the following tab	c c
What's new	Rule name	Compliance	✓ Edit rule	
	encrypted-volumes	noncompliant resource(s)	Å	
Learn More	s3-bucket-public-write-prohibited	Compliant	di ^a	
Documentation 🗗 Partners 🗗	s3-bucket-public-read-prohibited	Compliant	ø	
Partners 🛃	cloudtrail-enabled	Compliant	Ø	
FAQs 🗗	eip-attached	Compliant	dit	
🗨 Feedback 🔇 Engli	ish (US)	© 2008 - 2017, Å	Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy P	Policy Terms of Us

AWS config rules use a lambda instance to affordably ensure configuration compliance



Areas For Future Work

Adaptive Response

Disabling AWS instances from within Splunk

T'S NY 5'10'83' 'Jan 18:10:57:153] 'tent's 5'1' 60' (10'/Jan 18:10:57:153] 'GET / Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFFI0ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cattom=purchase&Itentid=EST-6&product Or actor (Jos Participation) (10'/Jan 18:10:57:123) "GET / Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFFI0ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cattom=purchase&Itentid=EST-6&product Or actor (Jos Participation) (10'/Jan 18:10:55:123) "GET / Category.screen?category_id=GIFTS&JSESSIONID=SDISLAFFI0ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cattom=purchase&Itentid=EST-6&product Or actor (Jos Participation) (10'/Jan 18:10:56:136] "GET / roduct.screen?product_id=FL-DSH-01&JSESSIONID=SDISL7FF6ADFF10 HTTP 1.1" 200 7J318 "http://buttercup-shopping.com/cattom=purchase&Itentid=EST-6&product 'Jos Com/category.id=Com/category.id=CIFTS&JSESSIONID=SDISL7FF6ADFF10 HTTP 1.1" 200 7J318 "http://buttercup-remove&Itentid=EST-6&product.id=AV-cEremPirche

Takeaways

- 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



splunk> .conf2017

Public Sector & Education Industry Day at .conf2017 Wednesday, September 27th, 2017 11:00am-7:00pm | Room 202A

400+ Attendees

Sessions

Customer Speakers

Birds of

Feather

Sessions

15

splunk> conf2017 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

