splunk> .conf2017

How To Gain Visibility into Office 365, Box using Splunk Enterprise Security

Girish Bhat, Director, Security Product Marketing

Chinmay Kulkarni, Senior Software Engineer, Splunk ES

September 26, 2017 | 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> .conf2017

This image cannot currently be displayed.

Section subtitle goes here

splunk> .conf2017

Agenda

- Outlook - Hybrid World with Clouds
- Splunk Enterprise and Splunk Enterprise Security
- Why Common Information Model (CIM)?
- Mapping to CIM
- Enterprise Security ♥ CIM
- Demo
- Q & A

Who is Girish?

- Security Product Marketing @Splunk
  - Enterprise Security, Security Portfolio
  - Splunk CISO customer advisory board program
  - Security customer use case program
- Prior work involved authentication, IAM, compliance, VPN, DLP, IDS/IPS, mobile, SaaS, IaaS, virtualization and network monitoring solutions
- Used to be a Product manager, Software Engineer and Hardware Engineer

Who is Chinmay?

- Chinmay Kulkarni
  - Engineering @ Splunk
  - @chinmaymk
- I mostly write ~~bugs~~ features.

POLL

splunk> .conf2017

SaaS Adoption Trends

- Office 365, Salesforce.com, Box, AWS are the top **SaaS** apps used by Enterprises (Source: Okta)
- SaaS tools - limited visibility into user activity
- By 2018, the 60% of enterprises that implement cloud visibility and control tools will experience one-third fewer security failures (Source: Gartner)
- By 2018, **40% of Office 365 deployments** will rely on 3rd party tools to fill in gaps in security and compliance (Source: Gartner)

Secure both Cloud and On-Premises Apps

Please choose the statement that best reflects your organization's strategy for cloud computing:

We have moved some enterprise applications to the cloud, with more to come	26%
We are moving our email, calendar, documents and storage to the cloud	13%
We have moved some enterprise applications to the cloud, and have no plans to migrate anything else	13%
We are moving some or all of our data center and/or networking infrastructure to the cloud	12%
We are moving mission-critical enterprise applications to the cloud	11%
We have always been cloud-based	5%
None of the above -- we are not moving to the cloud	21%

On-premises Apps Use

Source: Computer World Tech Forecast 2017

Splunk Enterprise vs Splunk Enterprise Security

	Splunk Enterprise	Splunk Enterprise Security
Monitor and Report	✓	✓
Detect and Alert	✓	✓
Analyze and Investigate	✓	✓
Respond and Collaborate	DIY	✓
Correlation Search	DIY	✓
Asset/Workflow	DIY	✓
Context for all workflow and tasks	DIY	✓
Action/remediation	DIY	✓
Threat Intelligence	DIY	✓

DIY – Do It Yourself

splunk> .conf2017

Splunk ES v4.7: Insight from SaaS Services

Office 365

box

salesforce

amazon web services

okta

- Get context from popular Enterprise SaaS apps, correlate across SaaS and / on-premises sources to improve investigation and incident response
- Determine scope of user activity, network activity, endpoint activity, access activity & abnormal activity from Cloud services
- Discover, Monitor and Report on Cloud service activity within your environment

Mapping to Splunk Enterprise Security

TA	CIM	Correlation Searches	Dashboards
O365	Change Analysis Authentication	Abnormally High Number of Endpoint Changes By User Account Deleted Anomalous Audit Trail Activity Detected Brute Force Access Behavior Detected and Detected Over One Day Concurrent Login Attempts Detected Default Account Activity Detected Excessive Failed Logins Geographically Improbable Access Detected High or Critical Priority Individual Logging into Infected Machine Insecure Or Cleartext Authentication Detected Network Change Detected and Network Device Rebooted Same Error On Many Servers Detected Short-lived Account Detected	access_anomalies access_center access_search access_tracker account_management default_accounts endpoint_changes network_changes user_activity

Mapping to Splunk Enterprise Security

Service	CIM	Correlation Searches	Dashboards
Box	Change Analysis Inventory Authentication	Account Deleted Brute Force Access Behavior: Detected and Detected Over One Day Cleartext Password At Rest Detected Concurrent Login Attempts Detected Default Account: Activity Detected and At Rest Detected Excessive Failed Logins Geographically Improbable Access Detected High or Critical Priority Individual Logging into Infected Machine Insecure Or Cleartext Authentication Detected Short-lived Account Detected Anomalous Audit Trail Activity Detected Abnormally High Number of Endpoint Changes By User Network Device Rebooted and Network Change Detected Same Error On Many Servers Detected	access_anomalies access_center access_search access_tracker account_management default_accounts endpoint_changes network_changes system_center user_activity

Scenario – Meta slide

- Take a hypothetical company – Home Mailbox office
- They want to use SharePoint
- Security Engineer Writes correlation searches for SharePoint data source
- CTO announces they are moving to box
- Security Engineer Rips his heir
- Comes to acceptance with situation
- Segway into data models/CIM
- How enterprise security uses CIM
- Demo for use case with O365

Life in Security

splunk> .conf2017

Life in Security

Life in Security

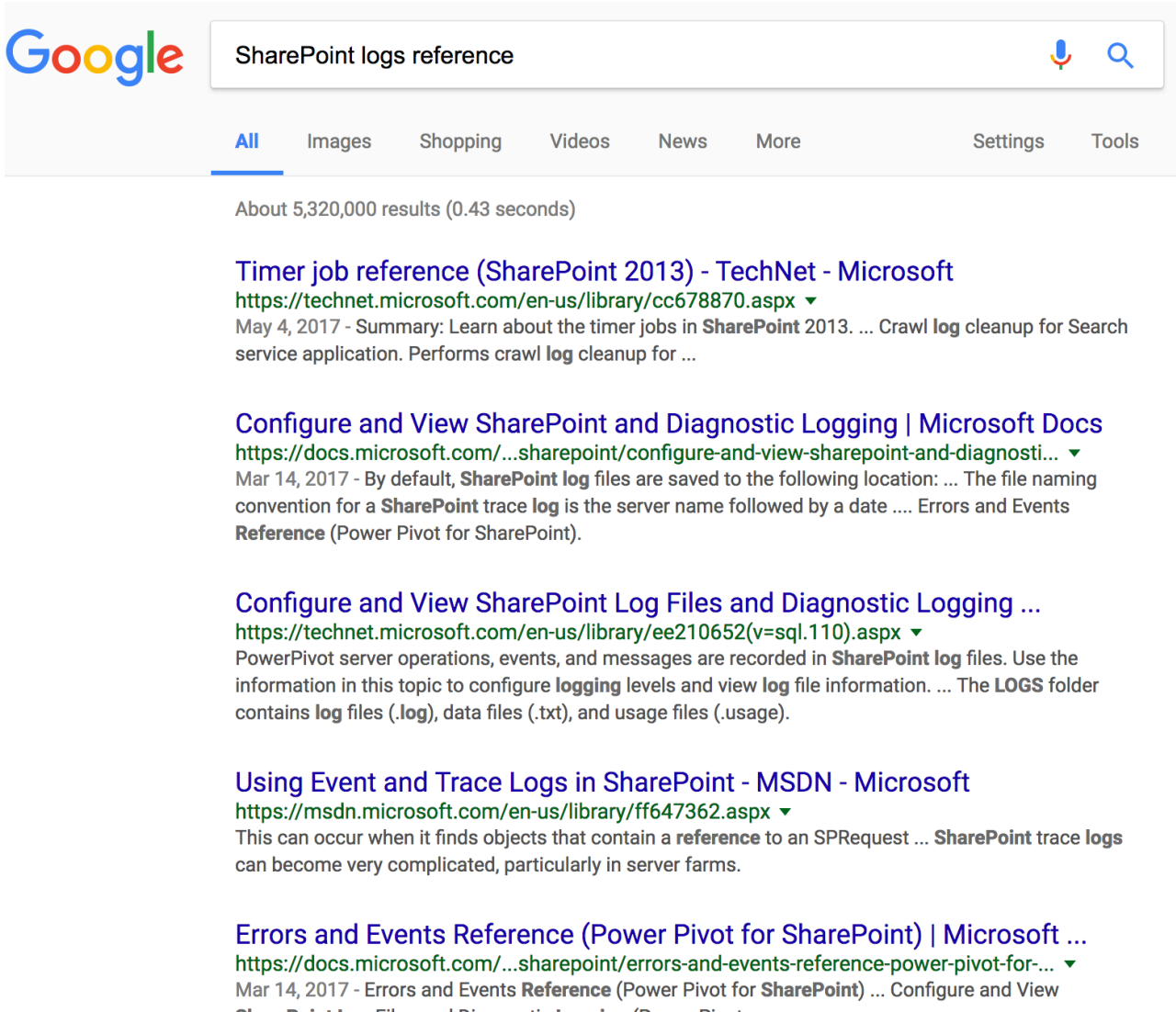
splunk> .conf2017

Home Mailbox Office

Home Mailbox Office

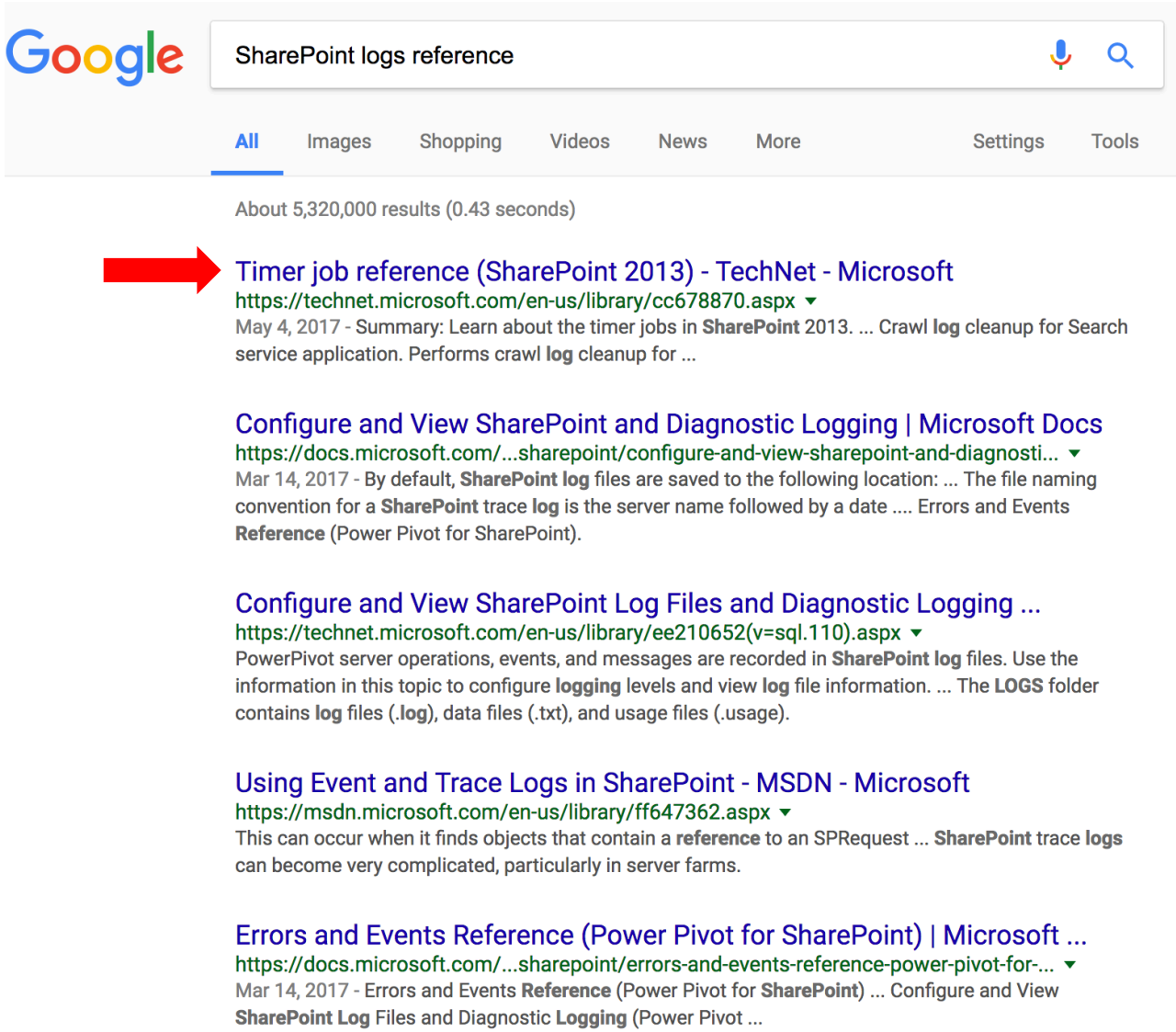
No Problemo

So SharePoint



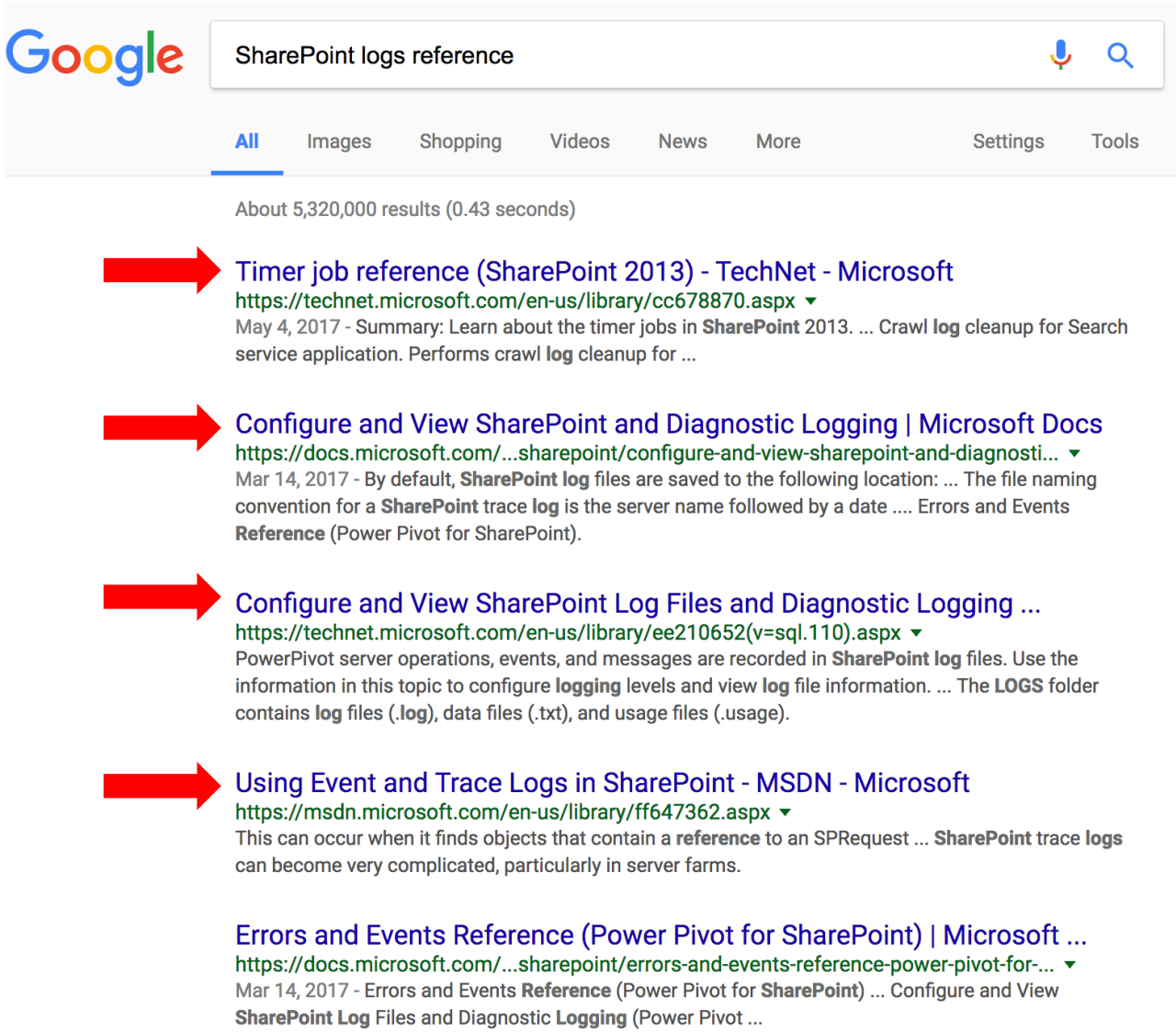
splunk> .conf2017

So SharePoint



splunk> .conf2017

So SharePoint



splunk> .conf2017

Correlation Searches

```
file_size > 100MB
```

Correlation Searches

```
file_size > 100MB

filename = *.mp4 OR filename = *.mov
OR filename = *.avi OR filename = *.wmv
```

Correlation Searches

```
file_size > 100MB

filename = *.mp4 OR filename = *.mov
OR filename = *.avi OR filename = *.wmv

src_location != “United States”

file_name NOT IN (malware)

file_size > normal_upload_size

**disclaimer** not real rules.
```

Life in Security

splunk> .conf2017

Home Mailbox Office

Home Mailbox Office

Acceptance

Acceptance

Abstraction!

Data Models!

What is a data model?

A data model is a hierarchically structured search-time mapping of semantic knowledge about one or more datasets. It encodes the domain knowledge necessary to build a variety of specialized searches of those datasets. These specialized searches are used by Splunk software to generate reports for Pivot users.

splunk> .conf2017

Common Information Model

- Collection of data models
- Normalization layer, speed benefits
- Batteries included:
  - Network
  - Authentication
  - Change
  - Create your own!

How To Map To CIM

- props.conf

```
[fortinet]
FIELDALIAS-bytes_out_sourcetype_fortinet = sent as bytes_out
FIELDALIAS-bytes_in_sourcetype_fortinet = rcvd as bytes_in
FIELDALIAS-dest_ip_sourcetype_fortinet = dst as dest_ip,dst as dest
FIELDALIAS-dest_dns_sourcetype_fortinet = dstname as dest_dns
FIELDALIAS-dest_port_for_fortinet = dst_port as dest_port
```

- tags.conf

```
[eventtype=fortinet]
network  = enabled
firewall = enabled
```

docs.splunk.com/Documentation/CIM/latest/User/Overview

splunk> .conf2017

Enterprise Security ♥ CIM

- Powers all correlation searches
- Dashboards use data model drilldowns
- Batteries included:
  - Network
  - Authentication
  - Change
  - Create your own!

splunk> .conf2017

Data Exfiltration

O365

- User logged in middle of the night
- User logged in outside of US
- Downloaded a file
- Uploaded that file to a personal app

Unauthorized access

Box

- User accessed a file in box outside his department
- It triggered notable events
- We also noticed few other notables triggered
- It seems the account may have been compromised or we have an insider threat (in-house hacker)!

Key Takeaways

This is where the subtitle goes

1. Gain insight from Hybrid, Cloud and On-Premises Services
2. CIM makes your life easier
3. Office 365, Box and other cloud services can be used with ES now

Thank You

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

Join the Pony Poll

ponypoll.com/***