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, 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.
Section subtitle goes here
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.
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:

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

Source: Computer World Tech Forecast 2017
## Splunk Enterprise vs Splunk Enterprise Security

<table>
<thead>
<tr>
<th></th>
<th>Splunk Enterprise</th>
<th>Splunk Enterprise Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor and Report</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Detect and Alert</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Analyze and Investigate</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Respond and Collaborate</td>
<td>DIY</td>
<td>✓</td>
</tr>
<tr>
<td>Correlation Search</td>
<td>DIY</td>
<td>✓</td>
</tr>
<tr>
<td>Asset/Workflow</td>
<td>DIY</td>
<td>✓</td>
</tr>
<tr>
<td>Context for all workflow and tasks</td>
<td>DIY</td>
<td>✓</td>
</tr>
<tr>
<td>Action/remediation</td>
<td>DIY</td>
<td>✓</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>DIY</td>
<td>✓</td>
</tr>
</tbody>
</table>

*DIY – Do It Yourself*
Splunk ES v4.7: Insight from SaaS Services

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

<table>
<thead>
<tr>
<th>TA</th>
<th>CIM</th>
<th>Correlation Searches</th>
<th>Dashboards</th>
</tr>
</thead>
</table>
| 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

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

SharePoint is the future.
No Problemo
So SharePoint log reference:

- Timer job reference (SharePoint 2013) - TechNet - Microsoft
  - May 4, 2017 - Summary: Learn about the timer jobs in SharePoint 2013. Crawl log cleanup for Search service application. Performs crawl log cleanup for...

- Configure and View SharePoint and Diagnostic Logging - Microsoft Docs
  - Mar 14, 2017 - By default, SharePoint log files are saved to the following location:...
  - The file naming convention for a SharePoint trace log is the server name followed by a date. Errors and Events Reference (Power Pivot for SharePoint).

- Configure and View SharePoint Log Files and Diagnostic Logging
  - PowerPivot server operations, events, and messages are recorded in SharePoint log files. Use the information in this topic to configure logging levels and view log file information. The LOGS folder contains log files (.log), data files (.txt), and usage files (.usage).

- Using Event and Trace Logs in SharePoint - MSDN - Microsoft
  - This can occur when it finds objects that contain a reference to an SPORequest... SharePoint trace logs can become very complicated, particularly in server farms.

- Errors and Events Reference (Power Pivot for SharePoint) - Microsoft
  - Mar 14, 2017 - Errors and Events Reference (Power Pivot for SharePoint) Configure and View SharePoint Log Files and Diagnostic Logging (Power Pivot...
So SharePoint

Timer job reference (SharePoint 2013) - TechNet - Microsoft
May 4, 2017 - Summary: Learn about the timer jobs in SharePoint 2013. ... Crawl log cleanup for Search service application. Performs crawl log cleanup for ...

Configure and View SharePoint and Diagnostic Logging | Microsoft Docs
https://docs.microsoft.com/en-us/sharepoint/configure-and-view-sharepoint-and-diagnosti... ▼
Mar 14, 2017 - By default, SharePoint log files are saved to the following location: ... The file naming convention for a SharePoint trace log is the server name followed by a date ... Errors and Events Reference (Power Pivot for SharePoint).

Configure and View SharePoint Log Files and Diagnostic Logging ...
PowerPivot server operations, events, and messages are recorded in SharePoint log files. Use the information in this topic to configure logging levels and view log file information. ... The LOGS folder contains log files (.log), data files (.txt), and usage files (.usage).

Using Event and Trace Logs in SharePoint - MSDN - Microsoft
This can occur when it finds objects that contain a reference to an SPPRequest ... SharePoint trace logs can become very complicated, particularly in server farms.

Errors and Events Reference (Power Pivot for SharePoint) | Microsoft ...
https://docs.microsoft.com/en-us/sharepoint/errors-and-events-reference-power-pivotfor... ▼
Mar 14, 2017 - Errors and Events Reference (Power Pivot for SharePoint) ... Configure and View SharePoint Log Files and Diagnostic Logging (Power Pivot ...)
So SharePoint

Timer job reference (SharePoint 2013) - TechNet - Microsoft
May 4, 2017 - Summary. Learn about the timer jobs in SharePoint 2013. ... Crawl log cleanup for Search service application. Performs crawl log cleanup for ...

Configure and View SharePoint and Diagnostic Logging | Microsoft Docs
https://docs.microsoft.com/en-sharepoint/configure-and-view-sharepoint-and-diagnosti...
Mar 14, 2017 - By default, SharePoint log files are saved to the following location: ... The file naming convention for a SharePoint trace log is the server name followed by a date ... Errors and Events Reference (Power Pivot for SharePoint).

Configure and View SharePoint Log Files and Diagnostic Logging ...
PowerPivot server operations, events, and messages are recorded in SharePoint log files. Use the information in this topic to configure logging levels and view log file information. ... The LOGS folder contains log files (.log), data files (.txt), and usage files (.usage).

Using Event and Trace Logs in SharePoint - MSDN - Microsoft
This can occur when it finds objects that contain a reference to an SPRequest ... SharePoint trace logs can become very complicated, particularly in server farms.

Errors and Events Reference (Power Pivot for SharePoint) | Microsoft ...
https://docs.microsoft.com/en-sharepoint/errors-and-events-reference-power-pivotfor...
Mar 14, 2017 - Errors and Events Reference (Power Pivot for SharePoint) ... Configure and View SharePoint Log Files and Diagnostic Logging (Power Pivot ...
Correlation Searches

file_size > 100MB
Correlation Searches

file_size > 100MB

filename = *.mp4 OR filename = *.mov
OR filename = *.avi OR filename = *.wmv
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
Home Mailbox Office

Yeah.. We're moving to box.
Acceptance

same

but different

but still same
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.
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

```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

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

docs.splunk.com/Documentation/CIM/latest/User/Overview
Enterprise Security ♡ CIM

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

- 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

- 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/***