.conf2015

I See What You're Doing Up There

How to leverage SaaS apps from Splunk to gain total visibility into your user activity in the cloud

splunk>

Jason Conger
Practice Manager, Splunk

Elias Haddad
Product Lifecycle Engineer, Splunk

Wissam Ali-Ahmad
Sr. Sales Engineer, Splunk

splunk>

Disclaimer

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 the 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.

You need visibility into your SaaS applications for better business insight.

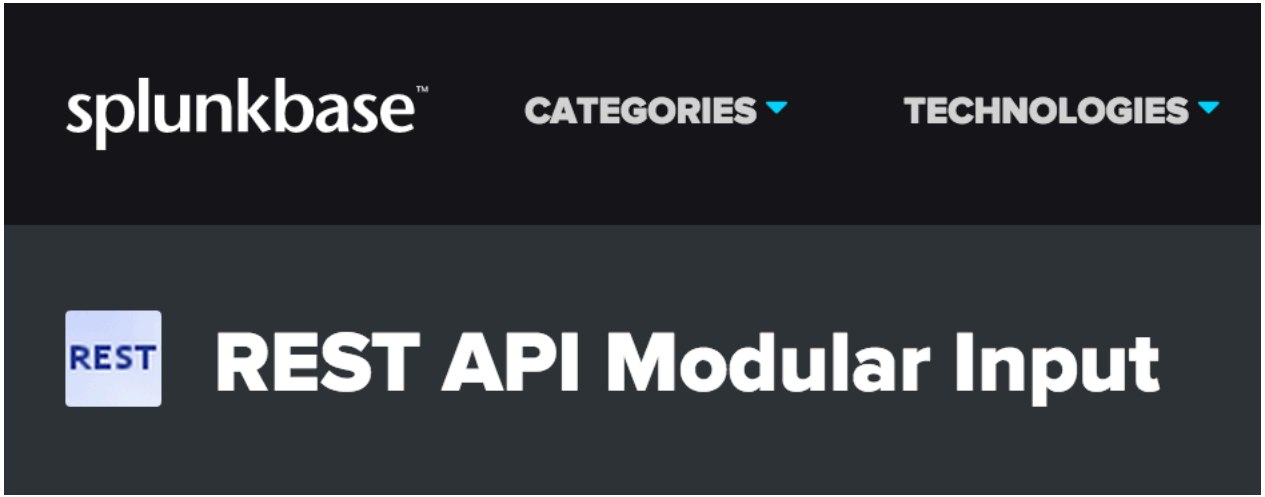

ura Poitras/Praxis Films

How To Splunk The Saas Data

splunk>

splunk>


splunk>
REST



https://splunkbase.splunk.com/app/1546/

How Do You Know What To Query?

ID	Time	Data
1	2015-09-24 11:00:00	Text
2	2015-09-24 11:00:00	Text
3	2015-09-24 11:00:00	Text
4	2015-09-24 11:00:00	Text
5	2015-09-24 11:00:00	Text

my_app.conf
1st run: position = 0
2nd run: position = 300
3rd run: position = 630
Nth run: position = *x*

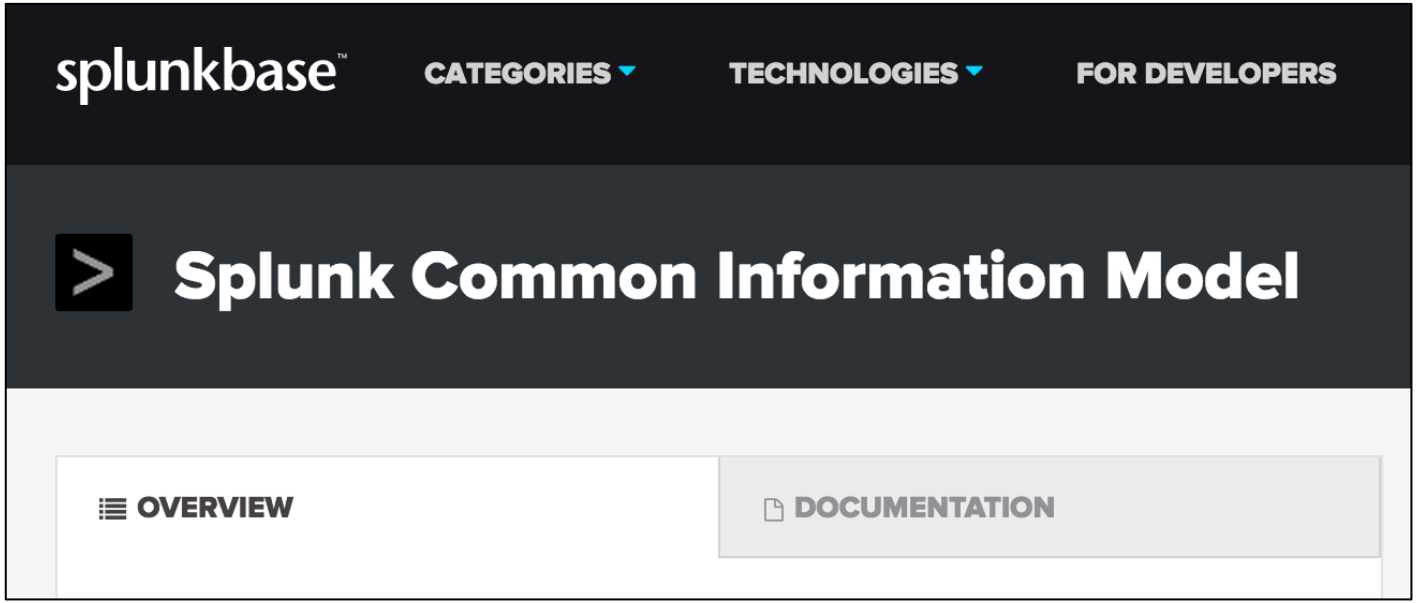
3rd Party Data
1st run: returned 0 – 300
2nd run: returned 301 – 630
3rd run: returned 630 - *x*

Pick Up Where You Left Off In Scripted And Modular Inputs

http://blogs.splunk.com/2014/09/22/pick-up-where-you-left-off-in-scripted-and-modular-inputs/

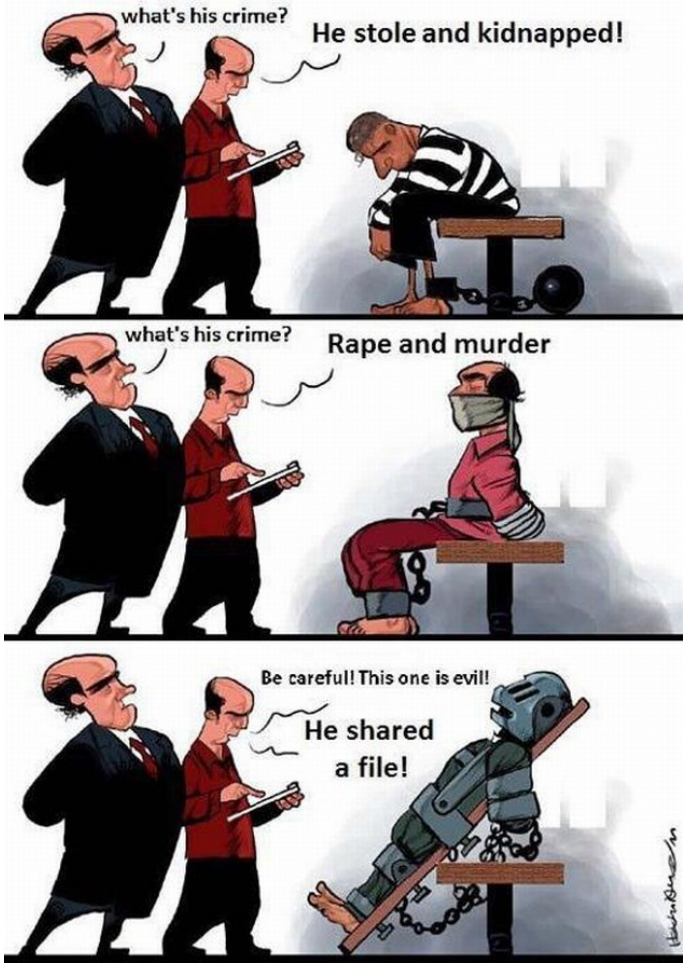
Report, Sync, Splunk

HTTP://

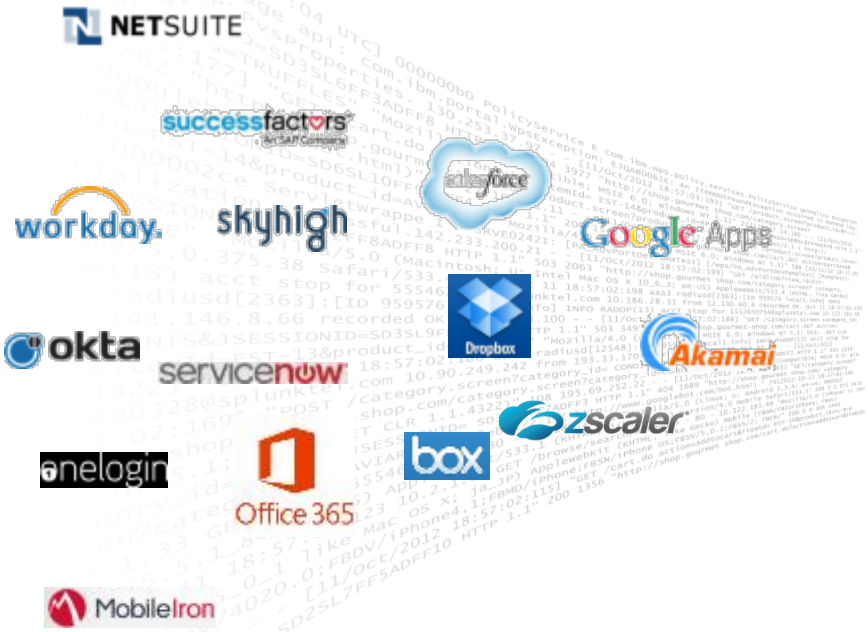

splunkbase
CATEGORIES
TECHNOLOGIES
FOR DEVELOPERS
Splunk Common Information Model
OVERVIEW
DOCUMENTATION

Visibility Of User Activities Across Saas Apps

splunk>


what's his crime?
He stole and kidnapped!
what's his crime?
Rape and murder
Be careful! This one is evil!
He shared a file!

Cloud Visibility with Splunk



Unified Cloud Visibility & Alerting

Splunk App for SalesForce

Splunk App for Dropbox

Splunk App for Okta

...

splunk>enterprise

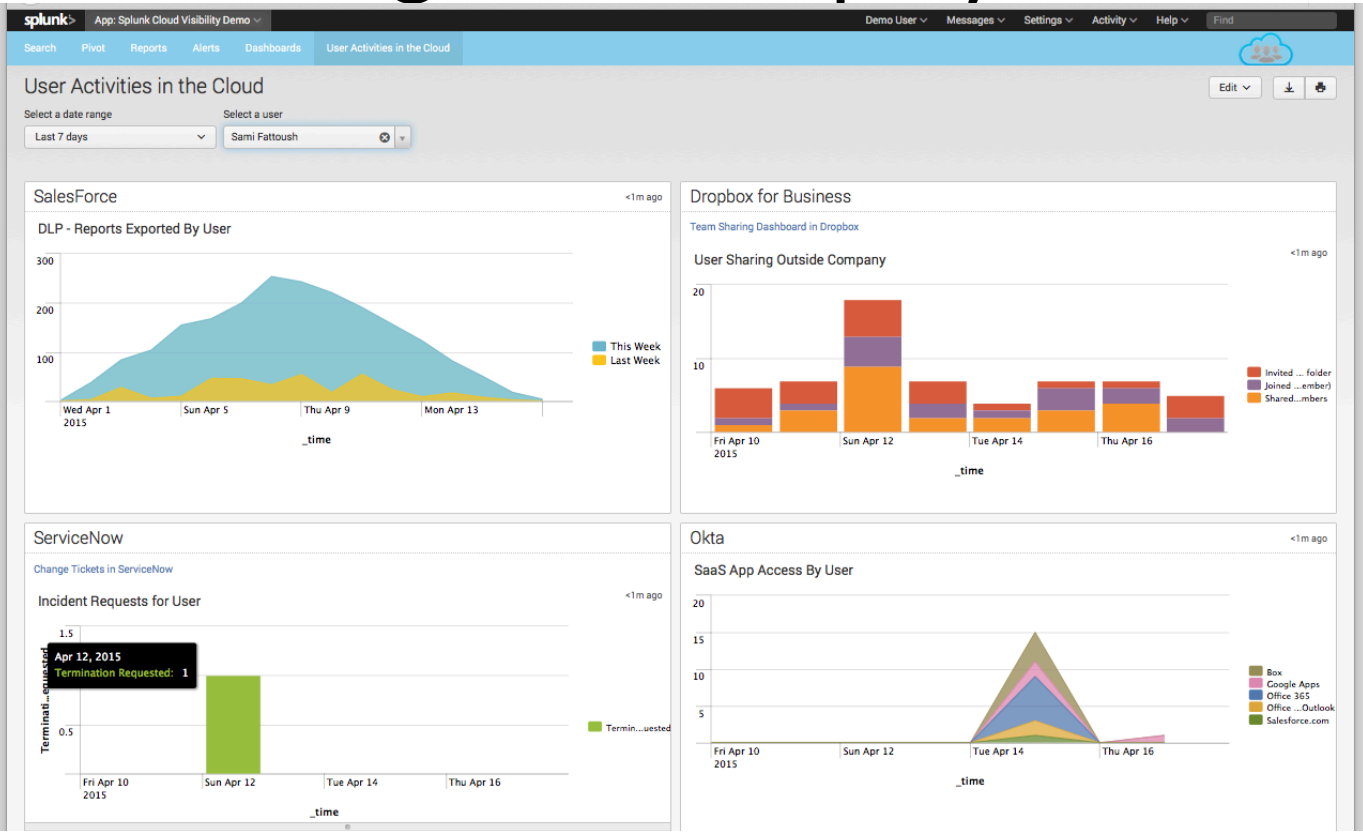
Monitor & Analyze User Behavior in SaaS Apps

- Login Analytics
  - Superman & Bruteforce scenarios (across multiple apps)
  - Predictive analytics of login activities (corp vs non-corp)
  - Audit for compliance: auto-lockout, multi-factor auth
- In-App Activity
  - App access (user, device, method and location)
  - Data upload and download trends (type, size)
  - In-app searches, keywords used
  - Collaboration: following what, who, how often
  - Third party apps authorized by user (rogue apps)

Data Loss Prevention

- Content Access Analytics
  - Export activities
    - Sudden burst of export activities within short period of time
  - Download trends
    - Large downloads of sensitive content
    - Folder events: too many shares to non-corporate users
- Collaboration membership events
  - Content sharing with non-team members (exfiltration)
- Rogue/Unknown Apps
  - Users authorizing unknown/unmanaged apps to access sensitive content

Disgruntle Employee



Demo

splunk>

THANK YOU

splunk>