Why So Cirrus?

Rick Correa
Sr. SecOps Manager
Why so Cirrus?

Rick Correa
Sr. SecOps Global Manager
Gets Headaches
Reverse Engineer turned Manager

Mike Sconzo
Head of Threat Intel
Gives Rick Headaches
PM turned Threat Intel

Input content from various folks at Box including Ben Walter, Kyle Bailey, Cameron Hoelscher
IaaS vs. PaaS vs. SaaS – Log all the Things!

We’ll focus on SaaS but happy to talk about other as-a-Services over 🍾….approaches are similar

Infrastructure

• AWS, Azure

Platform

• Heroku, Google App Engine

SaaS

• Box, Concur, Gmail, Slack, o365

Traditional Security Stack vs. Cloud-Based Security Stack

”…when I got into the field, we had Microsoft or Linux (….or Novell)”

Now, mix of on-prem and cloud services....

The modern cloud IT Stack - shout out to Jody Forness

https://www.youtube.com/watch?v=S6-oRhoyHiA
Case Study

OAuth 2 Introduction

Industry standard authentication method to authenticate to web services without having to create an account by brokering access to existing providers.

It’s also cool that OAuth2 integrations keep your data in less places (for example Slack\Email can store data as well but you can force data back to your online file storage solution and just transparently pass links which make managing a lot easier! – less copies of data – only references).

Oauth can give shady apps access to your data....
Basic OAuth Interactions
1. User requests to delegate access to their account
1. User requests to delegate access to their account
2. Client sends a request for scopes to the authorization server (AS)
1. User requests to delegate access to their account
2. Client sends a request for scopes to the authorization server (AS)
3. AS requests consent from the user to grant permissions to the client

Do want to grant access to Rogue App?
4. User Accepts, an authorization code is redirected to the client
4. User accepts, an authorization code is redirected to the client

5. Client presents the authorization code to the AS for confirmation
4. User Accepts, an authorization code is redirected to the client
5. Client presents the authorization code to the AS for confirmation
6. If the code is correct, a bearer token is issued to the client
4. User Accepts, an authorization code is redirected to the client
5. Client presents the authorization code to the AS for confirmation
6. If the code is correct, a bearer token is issued to the client
7. Client can now initiate API calls to interact with the users account
The risk is real...

Russian hackers use OAuth, fake Google apps to phish users

The phishing schemes can work, in spite of Google’s 2-step verification, Trend Micro said.

Scopes

Important to note the scope of an application

• SaaS Providers build & define the available scopes
• Developers are responsible for setting the scope of their app
  • Some platforms require verification to use broadly scoped permissions
• Token Life is generally defined by the provider or there are “options”

Examples of Dangerous Scopes

• Read/compose email & calendar entries
• Read & write to all files & folders
• “Full” Access
• Refresh access indefinitely?
Scopes (cont.)

Scopes are defined by the 3rd party application developers

<table>
<thead>
<tr>
<th>Application Scopes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the scopes shown on the OAuth consent screen when users or admins authorize your app. Learn more.</td>
<td></td>
</tr>
<tr>
<td>✓ Read all files and folders stored in Box</td>
<td></td>
</tr>
<tr>
<td>✓ Read and write all files and folders stored in Box</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage users</td>
</tr>
<tr>
<td></td>
<td>Manage groups</td>
</tr>
<tr>
<td></td>
<td>Manage webhooks</td>
</tr>
<tr>
<td></td>
<td>Manage enterprise properties</td>
</tr>
<tr>
<td></td>
<td>Manage retention policies</td>
</tr>
<tr>
<td></td>
<td>Enable integrations</td>
</tr>
</tbody>
</table>
Events

Events can vary from provider to provider

Scopes are what they have access to, Events are what actions they perform with those accesses.

These are the scopes that are noteworthy for Box but it’s not an exhaustive list. Each SaaS is unique but there are some commonalities and the approaches to securing are similar.

ACCESS_GRANTED and ADD_LOGIN_ACTIVITY_DEVICE are particularly interesting for access.
Why so Cirrus?

Used by several providers as integrations
Oauth vs. SAML

Open Authorization (OAuth) = **Authorization**
  - Addon’s, Apps & Integrations

Security Assertion Markup Language (SAML) = **Authentication**
  - Enterprise Single Sign On
  - Central Identity Provider
  - Web portal applications
First Principals

Can’t stress this enough in our team.....

Set-up a test case, validate it.

Better yet.....tabletop it with the team!
Realistic threat – real data - real team – your real logs.

Even better – involve IT and legal for remediation and input guidance. Establish escalation paths\SLAs with IT and AC priv communications paths
Case Study
Insider Threat

So what happens when someone asks you to find out **WHO** did **WHAT, WHEN** and **WHERE** ....and while starting to think on **WHY** and **HOW**?
Tools
Most providers call them either Events or Activities.

- **Box** - For these sets of examples, I’m using Box’s Splunk App. Box also has an admin console. [https://developer.box.com/reference#events](https://developer.box.com/reference#events)

- **Google Apps** - I’m also using the Google Investigate tool for Gdrive activities: [https://developers.google.com/admin-sdk/reports/v1/guides/manage-audit-drive](https://developers.google.com/admin-sdk/reports/v1/guides/manage-audit-drive)


- **Slack** [https://api.slack.com/events/api](https://api.slack.com/events/api)
Pro-Tip!

Check that you have the appropriate plans and support to get access to discovery\activities features. Some services don’t offer access detailed logs in their individual or small office offerings.

First principals! Validate before you need it!

Depending on org. culture, IT may own the access and may require time\approvals to get access.
Why so Cirrus?

Who
Can we tell the difference between an actual user, integration or rogue app install?

Can we identify the parties involved and who owns the impacted asset?

Generally – User activity will come from the User’s IP. App Integrations will come either from an external IP (e.g. AWS) or if it’s a local app, could come from the user’s machine.
Who – I’ll use Box, but other SaaS providers will be similar...

Notice the 1.1.1.1 and 254.254.254.254 IP addresses....

<table>
<thead>
<tr>
<th><em>time</em></th>
<th><em>additional_details_service_name</em></th>
<th><em>additional_details_file_path</em></th>
<th><em>event_type</em></th>
<th><em>created_by_login</em></th>
<th><em>ip_address</em></th>
<th><em>source_item_name</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-04-28 04:20:49</td>
<td>Box Elements (used in Box Web App)</td>
<td>/target/img/path</td>
<td>DELETE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:20:32</td>
<td>Box Elements (used in Box Web App)</td>
<td>/target/img/path</td>
<td>PREVIEW</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:20:24</td>
<td>Box Elements (used in Box Web App)</td>
<td>/target/img/path</td>
<td>ITEM_SHARED_UPDATE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:19:50</td>
<td>Box Elements (used in Box Web App)</td>
<td>/target/img/path</td>
<td>SHARE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:19:47</td>
<td>Box Elements (used in Box Web App)</td>
<td>/target/img/path</td>
<td>METADATA_INSTANCE_CREATE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:19:28</td>
<td>Multiput Uploads</td>
<td>/target/img/path</td>
<td>UPLOAD</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>LK5gCciyDiTlnxK3xuxnXtpw.jpg</td>
</tr>
<tr>
<td>2019-04-28 04:14:27</td>
<td></td>
<td>/target/img/path</td>
<td>WATERMARK_LABEL_CREATE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28 04:14:07</td>
<td></td>
<td>/target/img/path</td>
<td>UNLOCK</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28 04:14:00</td>
<td></td>
<td>/target/img/path</td>
<td>LOCK</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28 04:13:49</td>
<td></td>
<td>/target/img/path</td>
<td>UNFAVORITE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28 04:13:46</td>
<td></td>
<td>/target/img/path</td>
<td>FAVORITE</td>
<td>rickcorreallbox.com</td>
<td>1.1.1.1</td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
</tbody>
</table>
Why so Cirrus?

What

Can we tell what the actor accessed, modified and downloaded?

<table>
<thead>
<tr>
<th>time</th>
<th>additional_details_service_name</th>
<th>event_type</th>
<th>created_by_login</th>
<th>source_item_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-04-28</td>
<td>04:16:12</td>
<td>DELETE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:15:40</td>
<td>DOWNLOAD</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:15:38</td>
<td>ITEM_SHARED_UPDATE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:14:47</td>
<td>SHARE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:14:27</td>
<td>WATERMARK_LABEL_CREATE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:14:07</td>
<td>UNLOCK</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:14:00</td>
<td>LOCK</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:49</td>
<td>UNFAVORITE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:46</td>
<td>FAVORITE</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:38</td>
<td>PREVIEW</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:24</td>
<td>PREVIEW</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:11</td>
<td>PREVIEW</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:13:02</td>
<td>PREVIEW</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:12:55</td>
<td>PREVIEW</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:08:02</td>
<td>DOWNLOAD</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:08:02</td>
<td>DOWNLOAD</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
<tr>
<td>2019-04-28</td>
<td>04:08:02</td>
<td>DOWNLOAD</td>
<td><a href="mailto:rickcorrea@Box.com">rickcorrea@Box.com</a></td>
<td>Screen Shot 2019-01-05 at 10.06.56 AM.png</td>
</tr>
</tbody>
</table>

Sometimes getting the entire picture involves several look-ups or correlations involving user, endpoint, service, oauth, SSO logs.
When

Can we tell when the activity occurred?

- Potential Gotchas - Are we logging timestamps? Are our timestamps set on a standard timezone (ideally GMT +0) and NTP’d enable correlation?

- Splunk Transactions are awesome way to correlate cloud + device

- Do we know what the delay is from when the activity occurs to when it’s logged?
Why so Cirrus?

Where
Are they behind a proxy or VPN? Coming from inside or outside the network?

Determine the outer most edge…..look for all application activity going back to when the Oauth bearer toke was granted

Going back to 1st principles – are there microservices or proxies brokering requests to the edge?

Perform some recon on the IPs via tools like OpenDNS, PassiveTotal, DomainTools, Tor and known VPN proxy lists
Why so Cirrus?

How

Look at the target, the content, the MO, the current “pulse.”

Do the logs provide a complete picture of what the target did? Was it an actual user? Did the user initiate the action or was it the rogue application? How did the user get the application installed? Do other users have it installed as well?

Main takeaway – validation of processes or process improvements including increased control or logging. If a feature is missing, reach out to vendor and get a feature request in.
Why
Personally, I think these are the hardest steps. Look at the target, the content, the MO, the current “pulse.” Not always obvious.

Easy
• Financial fraud
• Insider threat – trade secrets/IP theft

Still kinda easy
• Commodity Malware – cryptomining, credential stealing
• Information

Harder
• Shady apps – plausible deniability
Case Study Outcomes

Take control of your Cloud Services

Control Access - Whitelist\Blacklist OAuth, Proper content sharing settings

Revoke shady apps and apps with aggressive scopes

Empower end-users by exposing which applications they have access to and do formal risk acceptance with management if they wish to retain access

Require application review to add to whitelist
Shadow IT
…more than managed services

We’ve talked a lot about logging and have made major assumptions that you have administrative ownership over things....

What if you don’t?

The misfortune of others becomes your misfortune....esp. with GDPR and CCPA

Misconfigured cloud resources and 3rd party breaches are a real thing.

....just this weekend, news broke of a container image hosting service get compromised.

* Image Source: https://www.pexels.com/photo/adorable-animal-cat-close-up-320014/
Mythical Single Pane of Glass

……or Mythical Single Glass of Pain

CASB vs. Centralized Logging vs. Admin Panels

**CASBs will show visibility into both known and some shadow IT service visibility**

Focus on getting centralized logs, if budget allows CASBs are awesome!

CASBs can also make it easy to manage rogue apps and revoke access.

* CASB logs are fun in a SIEM

* Image Source: https://commons.wikimedia.org/wiki/File:T-Pain,_2012.jpg
Continuous Auditing

...could dashboard it out too

- Having Logs for OAuth app activity in our SIEM has been critical
- Discover all users who authorized the app
  
  event_type = "ADD_LOGIN_ACTIVITY_DEVICE"  ip_address = <IP of redirect domain>

- Track exactly what the malicious app was doing
  
  additional_details_service_name = <App_Name>

- Establish baselines and look for deviations
- Can also be done in our Admin Console or CASB
Check Oauth Grants
Check yourself before you wreck yourself!

Applications Linked to your Account
Here is a list of all the web or desktop applications from partners that are linked to your Box account. You can remove any of these to reset the association that was made between the application and your account. (e.g. removing an association will allow you to use another account to sign in with that particular application and Box)
Take Away
Demand smarter architectures and better products

We have a really hard time accepting solutions that don’t have a robust APIs and provide centralized logs....

If you can’t manage it, block it!

- Oauth Grants\Apps\Integrations
- Browser Extensions
- DNS Category Blocks or “less” trusted TLDs
- Log\validate all the things to SIEM\CASB

* https://commons.wikimedia.org/w/index.php?curid=10791499
Questions?

Thank you!
If you’re ever in Austin
join our DFIR community
https://www.austindfir.com

Also have a few cool stickers to share.