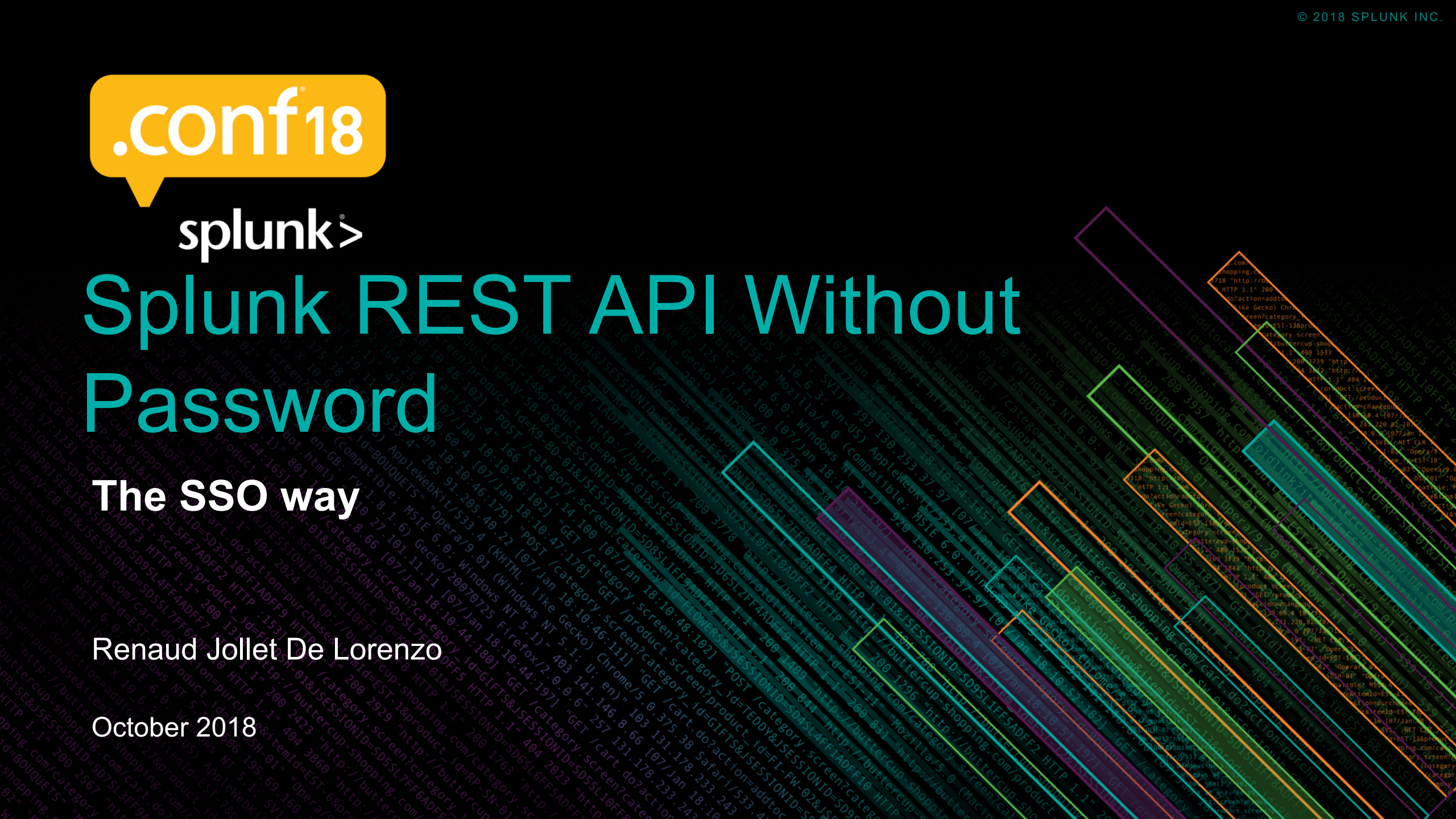
© 2018 SPLUNK INC.



Splunk REST API Without Password

The SSO way

Renaud Jollet De Lorenzo

October 2018

© 2018 SPLUNK INC.

Forward-Looking Statements

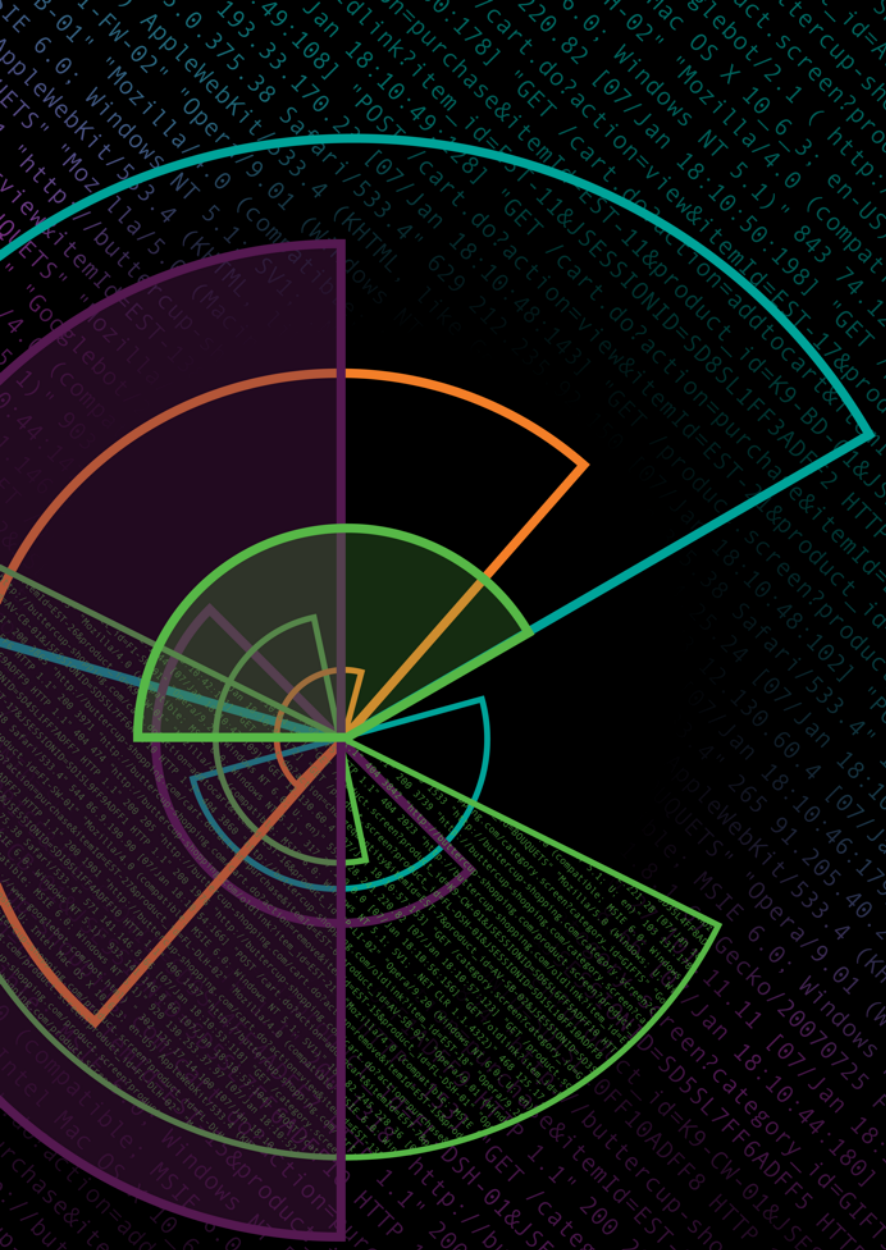
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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. © 2018 Splunk Inc. All rights reserved.

splunk> .conf18

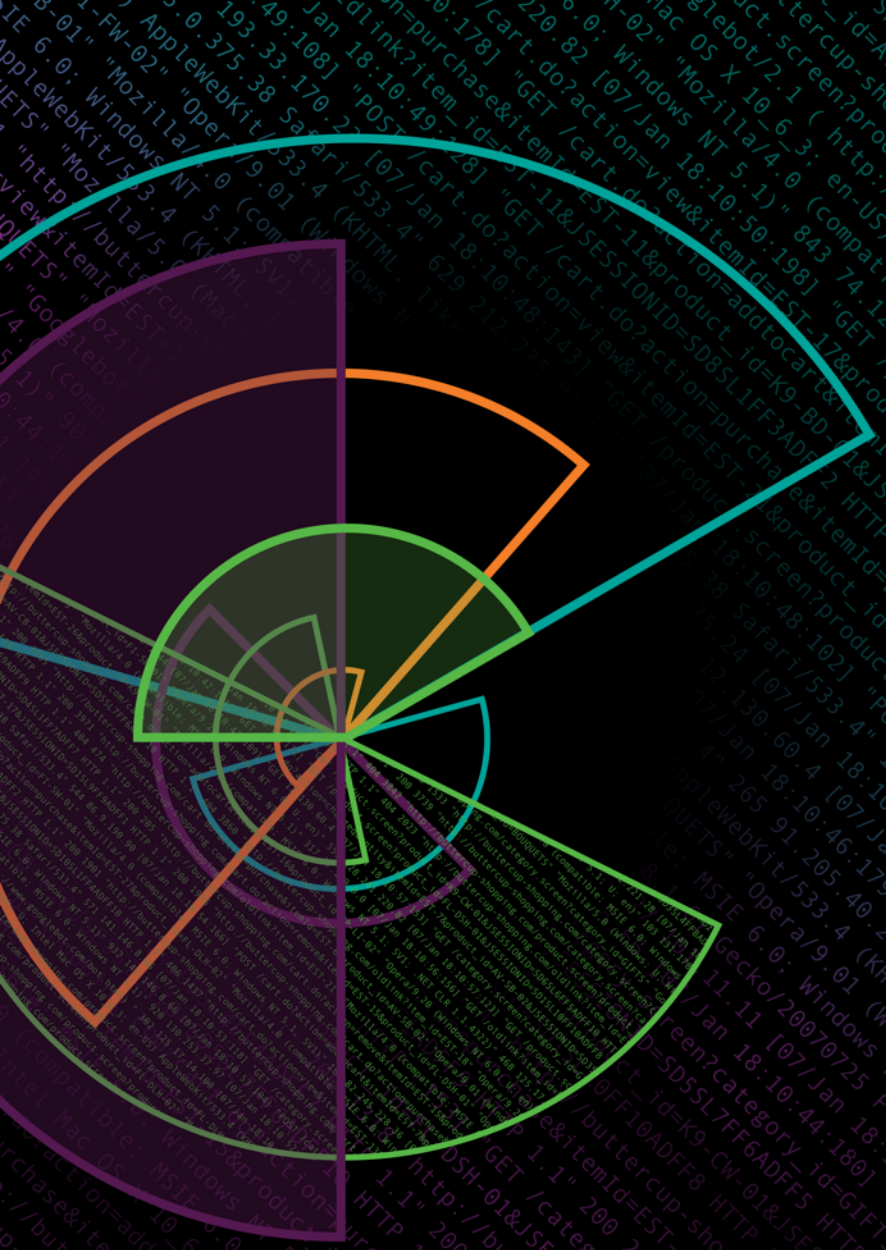
© 2018 SPLUNK INC.



One Does Not Simply

Have a REST API

© 2018 SPLUNK INC.



An Open REST API

© 2018 SPLUNK INC.

Secure DevOps Testing

Is your logs correctly collected by Splunk ?

Does the user with its roles will have access to this logs ?

Is there any error or warning generated by the host during the test ?

1. Run the test
   - Install the app
   - Run your test scenario
2. Get the logs
   - Get the application and OS logs from the REST API
3. Assert if successful
   - Check if you get the expected logs
   - Be notified if any unexpected error occurs in at the app or OS level during the test

© 2018 SPLUNK INC.

Open but Secure

© 2018 SPLUNK INC.

User Manual

First reflex Splunk docs

- -k
  - Verify the server
- admin
  - Be a limited User
- admin:pass
  - Prefer token over password

© 2018 SPLUNK INC.

Proposed Solution

First thought

- Reverse Proxy to the management port
  - Possible mismatch of the user with the client certificate
  - We don’t want to manage password
- Having a shared REST API user
  - No user differentiation in the audit logs
  - Managing User Authorization will be tough

© 2018 SPLUNK INC.

““After a successful login, a session cookie is created and the user can seamlessly access Splunk Web.”,

About Proxy SSO, Splunk docs

© 2018 SPLUNK INC.

SSO

Single-Sign-On

Compatible with your company authentication and authorization service.

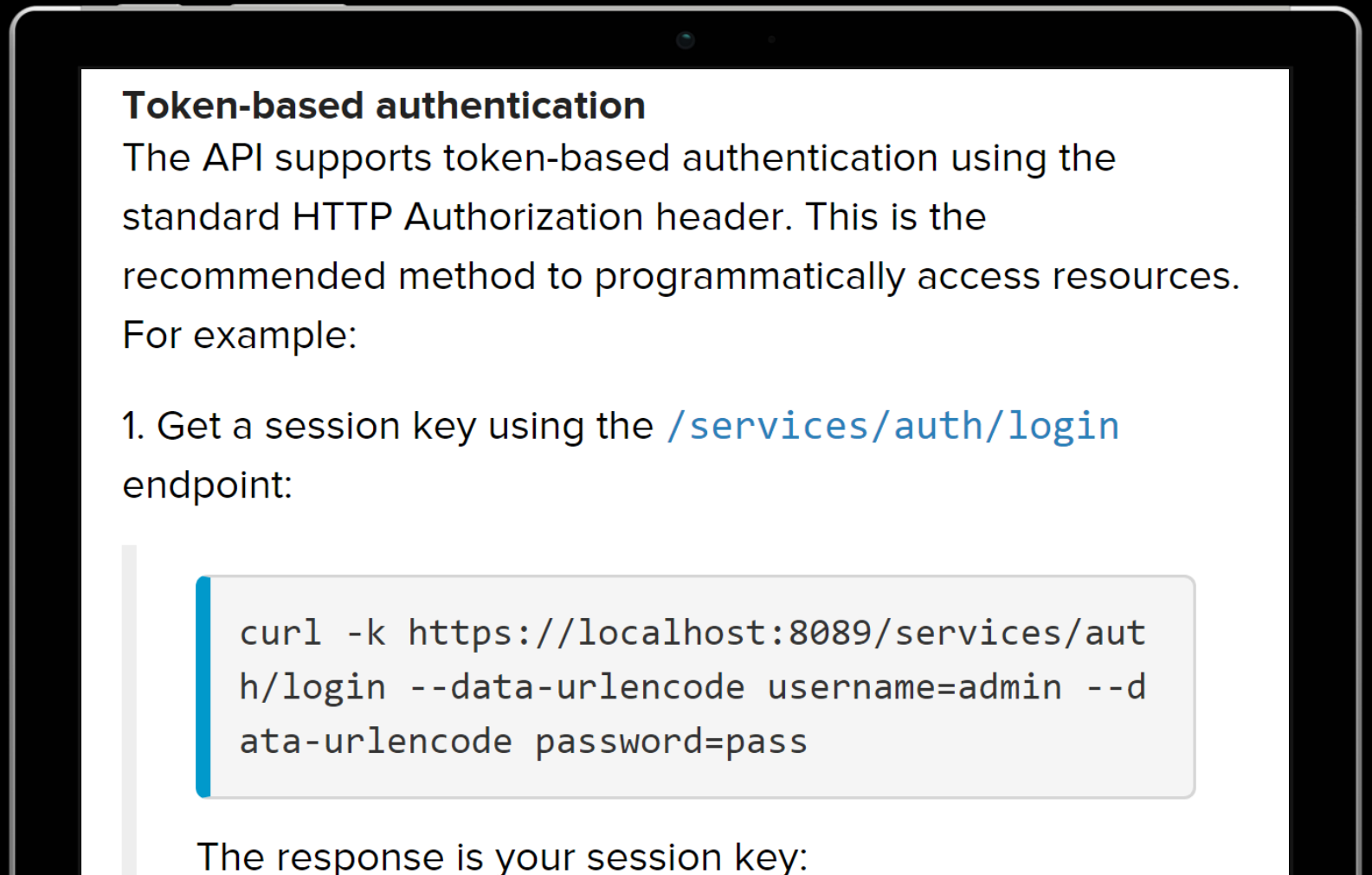
Seamless Splunk Web access but not to the REST API.

splunk> .conf18

© 2018 SPLUNK INC.

Token Based Authentication

Going deeper in Splunk docs



Token-based authentication

The API supports token-based authentication using the standard HTTP Authorization header. This is the recommended method to programmatically access resources. For example:

1. Get a session key using the `/services/auth/login` endpoint:

```
curl -k https://localhost:8089/services/auth/login --data-urlencode username=admin --data-urlencode password=pass
```

The response is your session key:

- Splunk REST API Support token
- But to get a token you have to use password

© 2018 SPLUNK INC.

Proposed Token Solution

- Advantage
  - Token have limited lifetime
  - Potential mismatch between token and certificate
- Drawback
  - Potential mismatch between token and certificate

1. Get token
   - Splunk Web (SSO)
   - Get token endpoint (using a basic Splunk app)
2. REST API
   - Client Certificate Proxy
   - Bearer token in the header

© 2018 SPLUNK INC.

““After a successful login, a session cookie is created and the user can seamlessly access Splunk Web.”,

About Proxy SSO, Splunk docs

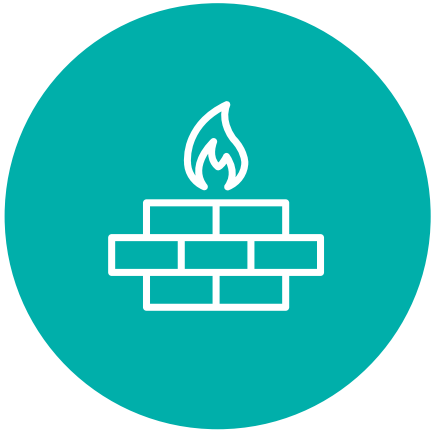
© 2018 SPLUNK INC.

Getting Closer

Connecting the dot

Management port support token

Splunk Web support SSO



Splunkd token in the cookie

splunk> .conf18

© 2018 SPLUNK INC.

Workaround

Our final solution

1. SSO
   - Authenticate the user using certificate
   - Set REMOTE_USER
2. Splunk Web
   - Call Splunk web
   - Collect splunkd token in the cookie
3. REST API
   - Add bearer token in the header
   - Make the query the management port

© 2018 SPLUNK INC.

Conclusion

1. You can apply the same Authentication for the REST API as for Splunk Web
2. API is User Experience
3. Open API need to be as secure as the web client

© 2018 SPLUNK INC.

Q&A

Renaud Jollet De Lorenzo

© 2018 SPLUNK INC.

Thank You

Don't forget to rate this session in the .conf18 mobile app