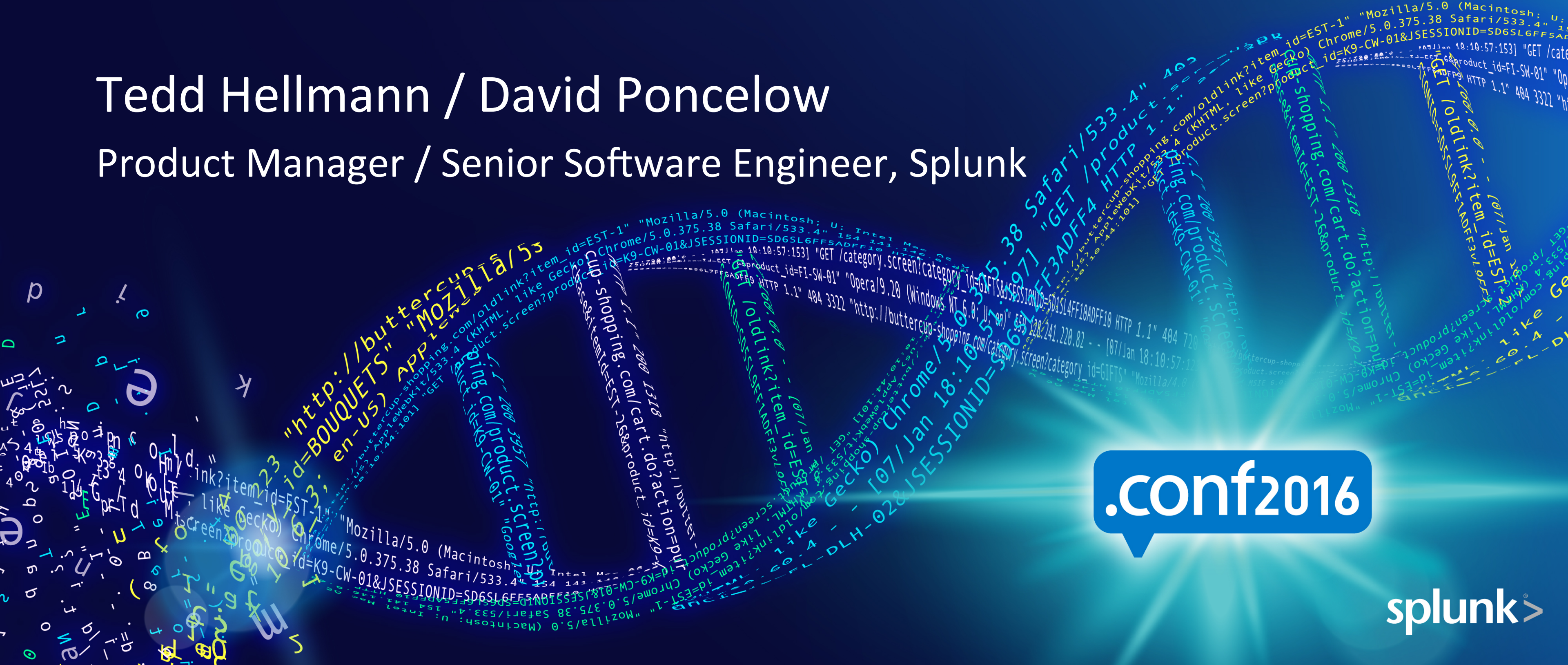
STEP Up Your App Development Game

Tedd Hellmann / David Poncelow

Product Manager / Senior Software Engineer, Splunk



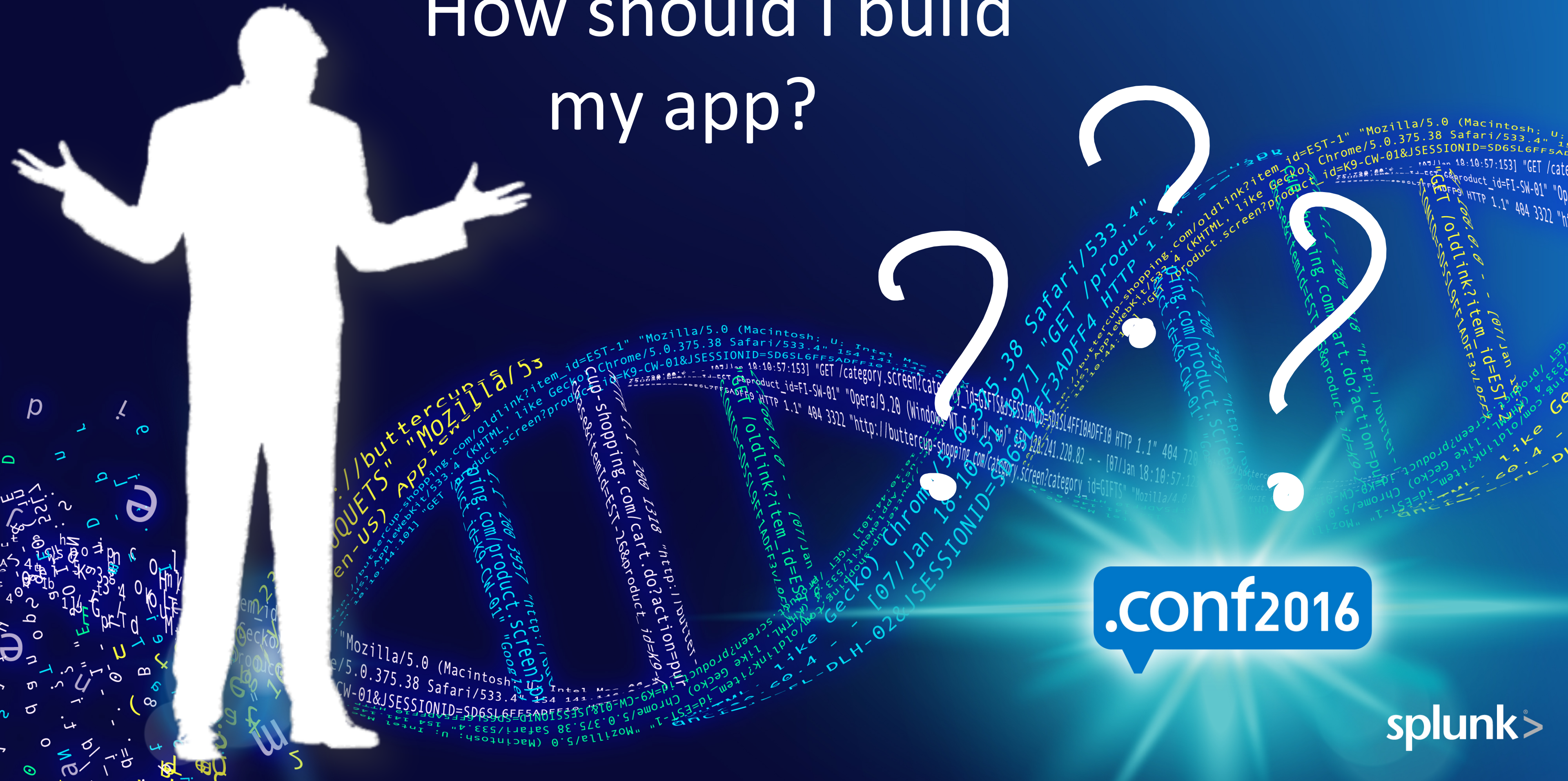
.conf2016

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.

How should I build my app?



.conf2016

splunk>

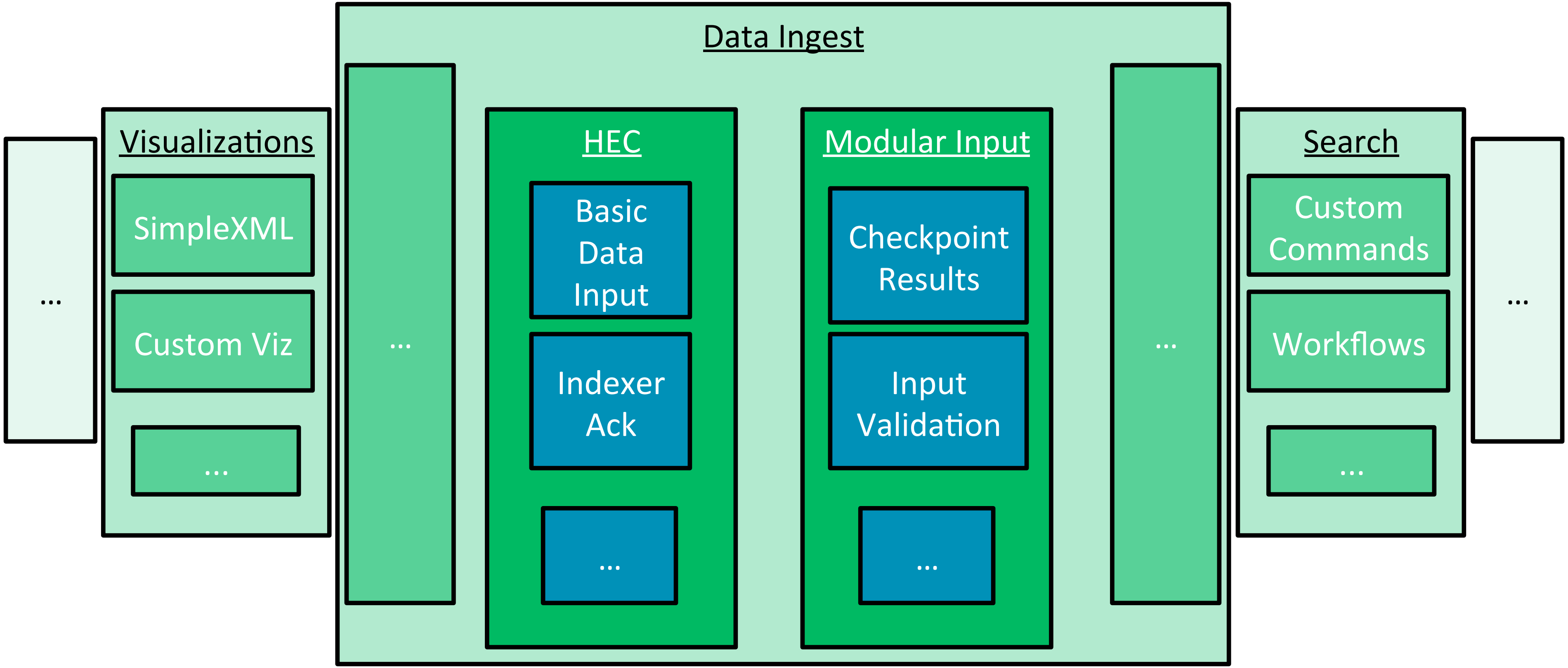
Splunk Developer Guidance

EVERYTHING YOU NEED TO BUILD

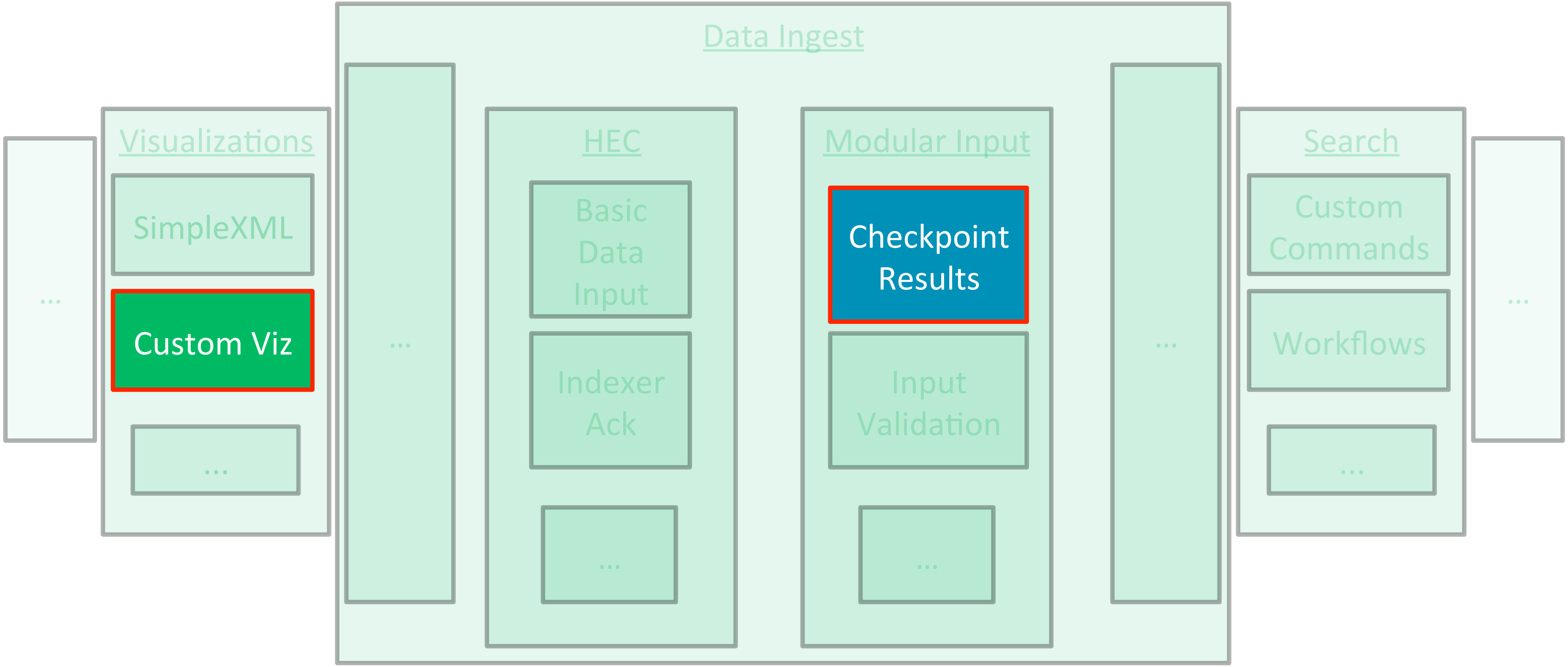
STEP up your game

- STEP - interactive learning environment
- Explore topics through Techniques and Recipes
- Technique: explore the details of features you can use in apps (modular inputs, custom visualizations, custom alert actions, …)
- Recipe: dive into the details of bringing several techniques together to address a business goal

STEP up your game



STEP up your game



STEP up your game

STEP Preview

2 Techniques

1 Recipe

T

STEP into real-world examples

.conf2016

splunk>

Planning a journey

Platform and **tools**:
a kitbag for our journey

UI and **visualizations**:
what the apps look like

Working with data: where it comes from & how we manage it

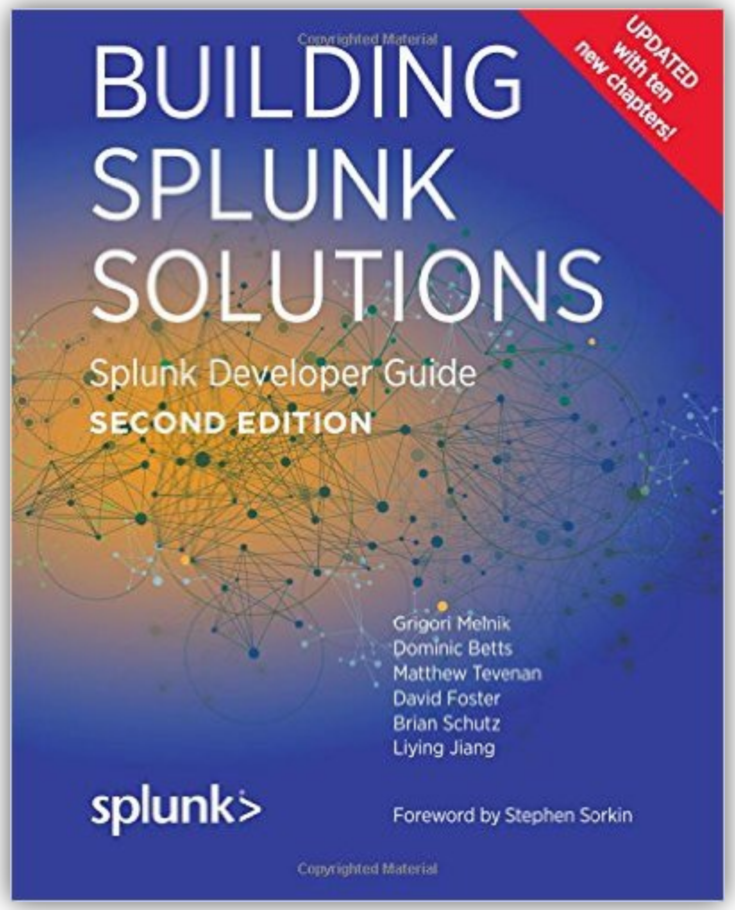
Adding code: using JavaScript and Search Processing Language

Packaging and **deployment**: reaching our first destination

Dealing with **OAuth**

Alerting

Building in telemetry with
high-performance data collection



Copyrighted Material

BUILDING SPLUNK SOLUTIONS

Splunk Developer Guide

SECOND EDITION

UPDATED with ten new chapters!

Grigori Melnik
Dominic Betts
Matthew Tevenan
David Foster
Brian Schutz
Liying Jiang

splunk>

Foreword by Stephen Sorkin

Copyrighted Material

splk.it/devguide

1. Start with a Questions Backlog

- Architecture
  - What does a typical Splunk application reference architecture look like?
  - What common paradigms are applicable to Splunk app development?
  - What are the typical deployment topologies? Why should I choose a specific one? What are the confounding factors on the choice of my topology?
  - How do I partition my Splunk solutions?
  - What are the tradeoffs of various types of inputs?
  - How do I architect my Splunk solution and deployment for a very large scale?
  - How do I architect my Splunk solution for the cloud? What are specific considerations for deploying to AWS or Azure?
  - What's the landscape of Splunk extension points?
  - How do I integrate data from Splunk into existing applications and systems?

- Why should I not use transactions?
- When should I use pivot vs tstats?
- Why should I use data models?
- When my data source touches on many data models, should I assume complete separation or heavy inheritance?
- How do I extend an existing data model?
- What does CIM offer and why should I build CIM-compliant apps?
- In the context of CIM, what are the tradeoffs of using my props.conf and transforms.conf and rewriting them on indexing, completely discarding the vendor supplied field names? How do I reconcile the advantages of a clean interface & normalisation, but at the cost of losing alignment with published vendor documentation, and a learning curve for existing users?
- How do I manage my solution declarative configuration? How do I detect/troubleshoot bad config?

How do I package an app? deal with app versioning and updates?

- Development
  - How should I set up my development environment to be productive with Splunk?
  - What are different ways of how I develop my Splunk app ? Pros and cons of using specific SDK vs REST APIs? Pros and cons of using SimpleXML vs Advanced XML vs Web Framework …
  - How do I analyze a data source for a TA?
  - What are the different ways of enriching the data in Splunk? What are their tradeoffs?
  - When should I use event types and transactions for data classification?
  - How do I extend Splunk to define a custom input capability?
  - When should I use modular inputs vs scripted inputs vs..?
  - What are streaming vs non-streaming outputs considerations?
  - How do I deal with long-running scripts? Handling shutdown/restart of Splunk? Concurrency? State persistence etc.

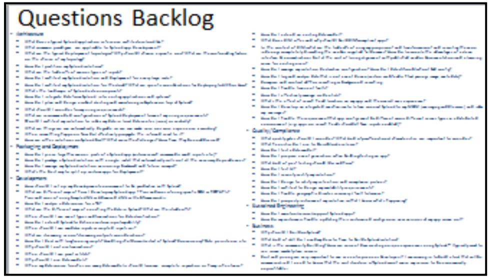
- How do I prepare event generation when building/testing an app?
- What kind of perf testing should I do and how?
- How do I test UI?
- How do I security certify my solution?
- How do I design to satisfy my retention and compliance policies?
- How do I architect to design my availability requirements?
- How do I handle geographic disaster recovery / fault tolerance?
- How do I properly instrument my solution so that I know what's happening?

- Sustained Engineering
  - How do I maintain/service/support Splunk apps?
  - How do my customers handle updating their customized configs once new versions of my app come out?
- Business

2. Identify Extensibility Surface Area

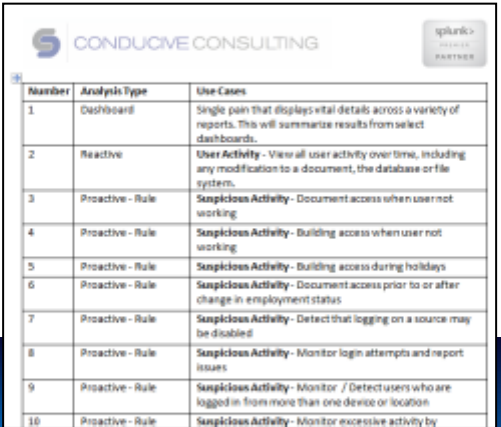
- **Data ingestion & indexing**
  - **Input**
    - Modular inputs
    - Custom (trained) source types
    - Custom sources
    - HTTP Event Collection
  - **Data ingestion pipeline**
    - Field extractions
    - Field transformations
  - **Indexing**
    - Custom indexes
- **Searching**
  - **Search authoring**
    - Custom search commands
    - Macros (basic, parametrized)
    - Saved searches
  - **Data classification**
    - Event types
    - Transactions
  - **Data enrichment**
    - Lookups
    - KV store collections
    - Workflow actions
  - **Data normalization**
    - Tags
    - Aliases
  - **Data mining**
    - `cluster` & `dedup`
    - `anomalousvalue`
    - `kmeans`
    - `predict` commands …
- **Processing & reporting**
  - **Search-time mapping**
    - Data models
  - **CIM extensions**
  - **Custom Visualizations**
  - **Custom UI**
  - Pages, views & dashboards
    - JS, CSS Extensions
    - Custom setup screens
  - **Scheduled processing**
    - Scheduled reports
  - **Alerting**
    - Scripted alerts
    - Custom alert actions
  - **Branding & navigation**
    - Custom app navigation
    - App branding
  - **Manageability**
    - Custom splunkweb controllers
    - Custom splunkd endpoints

3. Mine business requirements
4. Formulate learning objectives
5. Design around 3 and 4



Questions Backlog

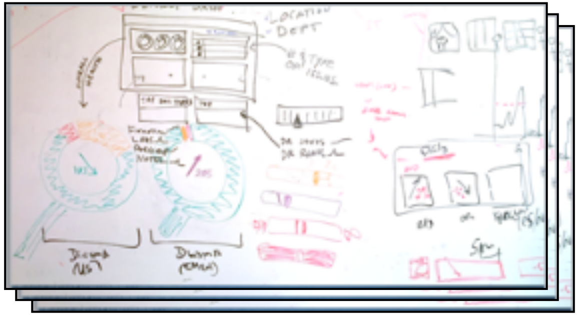
- Architecture
- Packaging and Deployment
- Development
- Quality/Compliance
- Sustained Engineering
- Business

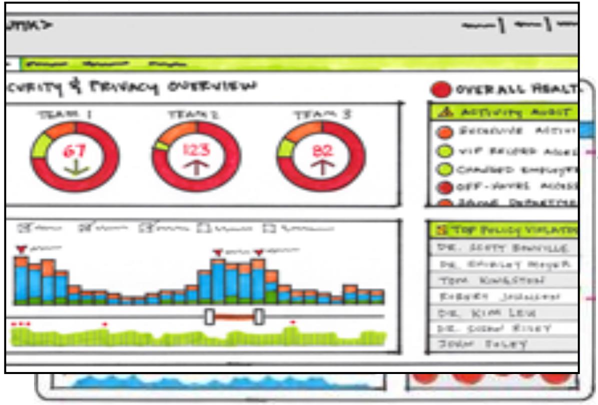


CONDUCIVE CONSULTING

splunk> PREMIER PARTNER

Number	Analysis Type	Use Cases
1	Dashboard	Single pain that displays vital details across a variety of reports. This will summarize results from select dashboards.
2	Reactive	**User Activity** - View all user activity over time, including any modification to a document, the database or file system.
3	Proactive - Rule	**Suspicious Activity** - Document access when user not working
4	Proactive - Rule	**Suspicious Activity** - Building access when user not working
5	Proactive - Rule	**Suspicious Activity** - Building access during holidays
6	Proactive - Rule	**Suspicious Activity** - Document access prior to or after change in employment status
7	Proactive - Rule	**Suspicious Activity** - Detect that logging on a source may be disabled
8	Proactive - Rule	**Suspicious Activity** - Monitor login attempts and report issues
9	Proactive - Rule	**Suspicious Activity** - Monitor / Detect users who are logged in from more than one device or location
10	Proactive - Rule	**Suspicious Activity** - Monitor excessive activity by



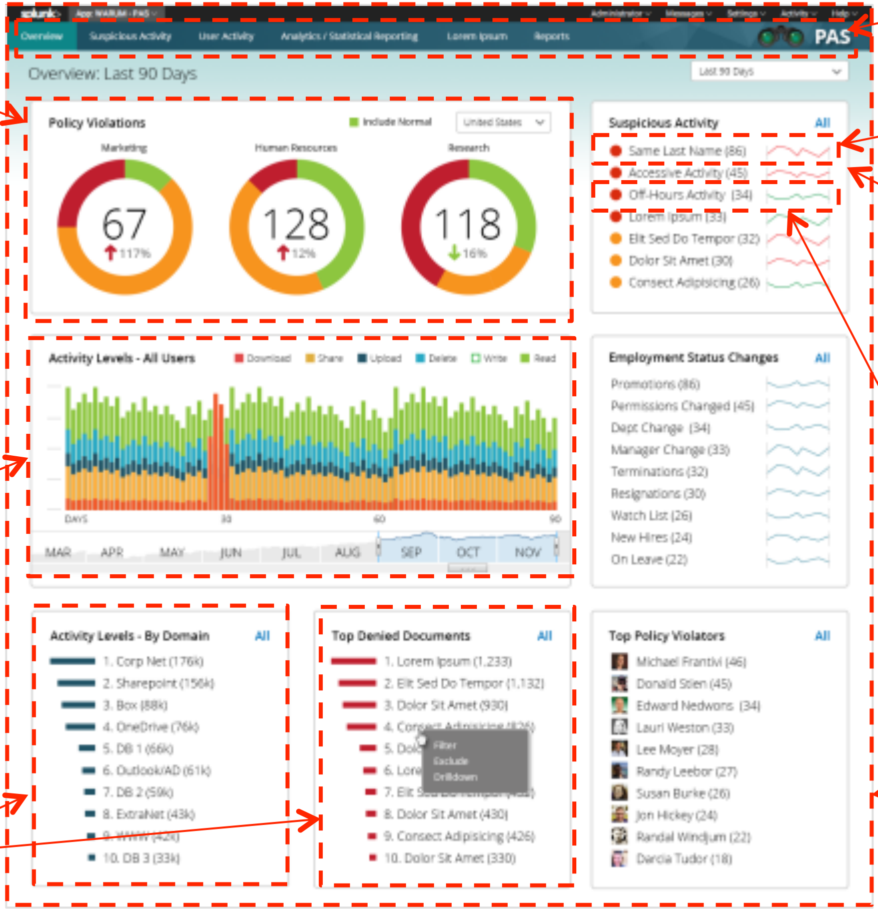


...

- Data
  - Search language
  - Aggregating siloed metrics into meaningful KPIs
  - Data manipulation
  - Data normalization
  - Sub-searches
  - Config-driven
  - Persistence with KV store
  - Macros
- Viz:
  - Dynamic scaling
  - Customizing in-the box viz controls

- General search patterns
- Search optimizations
- Ux Prototyping
- Adapting 3rd party viz library
- Composite charts with interactions
- Dealing with high-volume data sets
- Troubleshooting perf issues
- Post-process or not-post-process – deployment implications
- Automated UI testing (w.Selenium)

  - Post-processing
  - Integrating with 3rd party component
  - Unit testing (w.Mocha)
  - Persisting state (per user)



Overview: Last 90 Days

Suspicious Activity All
- Same Last Name (86)
- Accessive Activity (45)
- Off-Hours Activity (34)
- Lorem Ipsum (33)
- Elit Sed Do Tempor (32)
- Dolor Sit Amet (30)
- Consect Adipisicing (26)

Employment Status Changes All
- Promotions (86)
- Permissions Changed (45)
- Dept Change (34)
- Manager Change (33)
- Terminations (32)
- Resignations (30)
- Watch List (26)
- New Hires (24)
- On Leave (22)

Activity Levels - By Domain All
1. Corp Net (176k)
2. Sharepoint (156k)
3. Box (88k)
4. OneDrive (76k)
5. DB 1 (66k)
6. Outlook/AD (61k)
7. DB 2 (59k)
8. ExtraNet (43k)
9. WWW (42k)
10. DB 3 (33k)

Top Denied Documents All
1. Lorem Ipsum (1,233)
2. Elit Sed Do Tempor (1,132)
3. Dolor Sit Amet (930)
4. Consect Adipisicing (826)
5. Dolo
6. Lore
7. Elit Sed Do Tempor (482)
8. Dolor Sit Amet (430)
9. Consect Adipisicing (426)
10. Dolor Sit Amet (330)

Top Policy Violators All
- Michael Frantivi (46)
- Donald Stien (45)
- Edward Nedworns (34)
- Lauri Weston (33)
- Lee Moyer (28)
- Randy Leebor (27)
- Susan Burke (26)
- Jon Hickey (24)
- Randal Windjum (22)
- Darcia Tudor (18)

- Custom nav
- Ux activities permeating all dev

- Using sub-searches to correlate data
- Troubleshooting searches

- Data mining:
  - Exploration
  - Preparation: filtering/deduping/ bucketing
  - Using advanced statistics functions
  - Threshold-based anomaly detection
  - Evaluating goodness /accuracy

- Data modeling
- Using lookups
- Building a baseline lookup table
- Windows of time/Custom time ranges
- Overlaying time data

- Setting the stage
- Overall Splunk app structure
- UI technology selection: Simple XML vs SplunkJS
- Modularity
- Dev & test env
- Dev workflow
- Modularity
- Data onboarding
- CIM compliance
- Tools

Plus non-functional topics:
- App versioning
- Packaging Installation
- Security review
- Deployment
- Publishing to splunkbase
- App certification

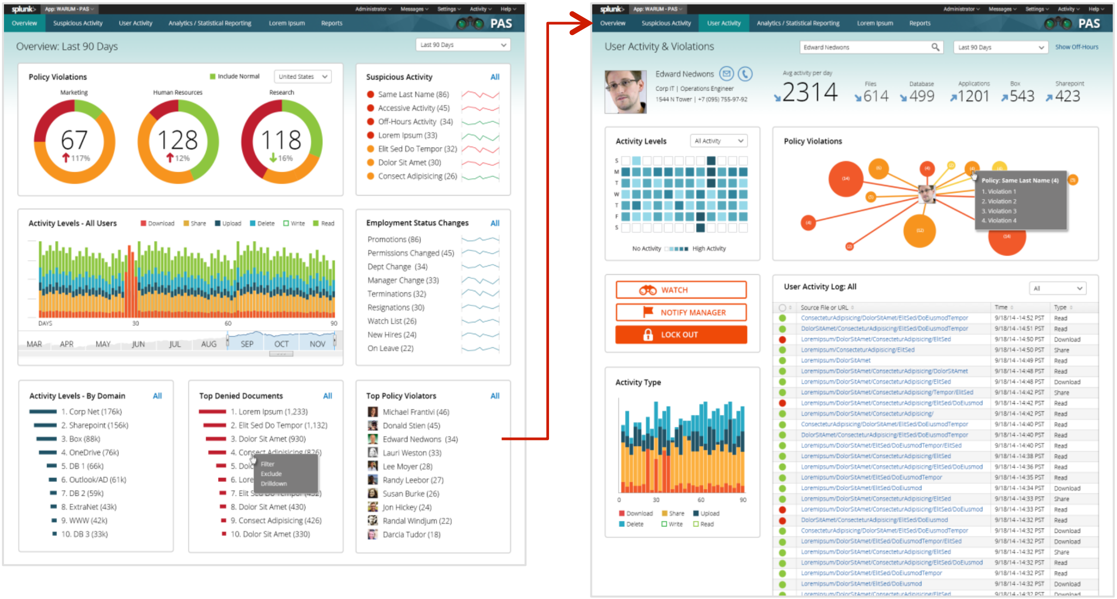
Building Solutions on the Splunk Platform

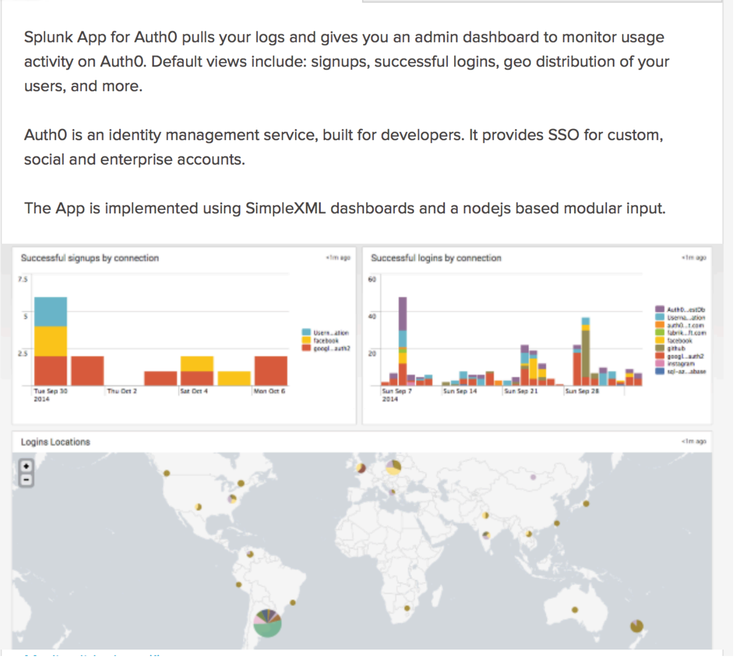
1. **Splunk Reference Apps**

   Complete, working real-world Splunk solutions built together with partners (Conducive, Auth0)

2. **Splunk Developer Guide**

> This is **unbelievable**, it covers most everything I learned the hard way…
>
> – *Bernie Macias, Technical Architect, **Zillow***





Splunk App for Auth0 pulls your logs and gives you an admin dashboard to monitor usage activity on Auth0. Default views include: signups, successful logins, geo distribution of your users, and more.

Auth0 is an identity management service, built for developers. It provides SSO for custom, social and enterprise accounts.

The App is implemented using SimpleXML dashboards and a nodejs based modular input.

Successful signups by connection
Successful logins by connection
Logins Locations

dev.splunk.com/goto/devguide

Splunk Reference App Demo

Splunk Reference App – Pluggable Audit System

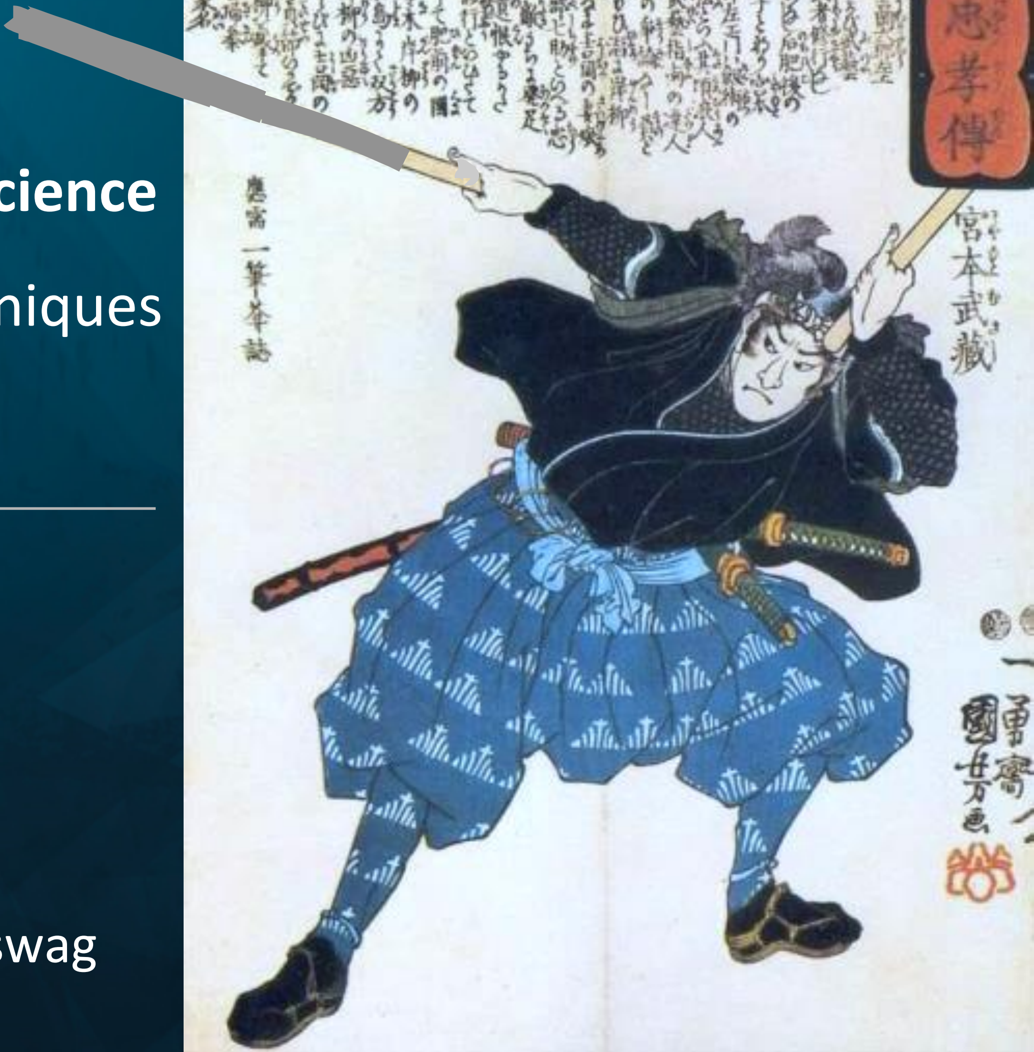
splunkbase.splunk.com/app/1934/

OR search name from Splunk Web UI

Takeaways

- App development **!= rocket science**
- STEP up your game with techniques and recipes

- Get in touch with us
  - STEP@.splunk.com
  - Leave feedback for STEP
  - Come by our booth, get some swag



Resources

dev.splunk.com

Related breakout sessions & activities

Faster Splunk App Certification with Splunk AppInspect

(Grigori Melnik/Andy Nortrup)

Best Practices for Working with Splunk Cloud
(Dennis Bourg/Eric Six)

HTTP Event Collector in Splunk 6.4 - More Super Powers!

(Glenn Block/Itay Neeman)

Building Splunk Visualizations with the New Custom Visualization API

(Marshall Agnew)

Dashboard Wizardry

(Nicholas Filippi/Siegfried Puchbauer)

Best Practices for Developing Splunk Apps and Add-ons

(Jason Conger)

How to Build a Solution from Scratch: A Case Study of Partner Engagement and Co-Development

(Vladimir Melnik/Igal Vanier)

Onboard Your Data Faster Using the Splunk Add-on Builder

(Elias Haddad/Guodong Wang)

THANK YOU

.conf2016

splunk>