Leveraging Splunk's Ecosystem for your Own Products

Michael Franke

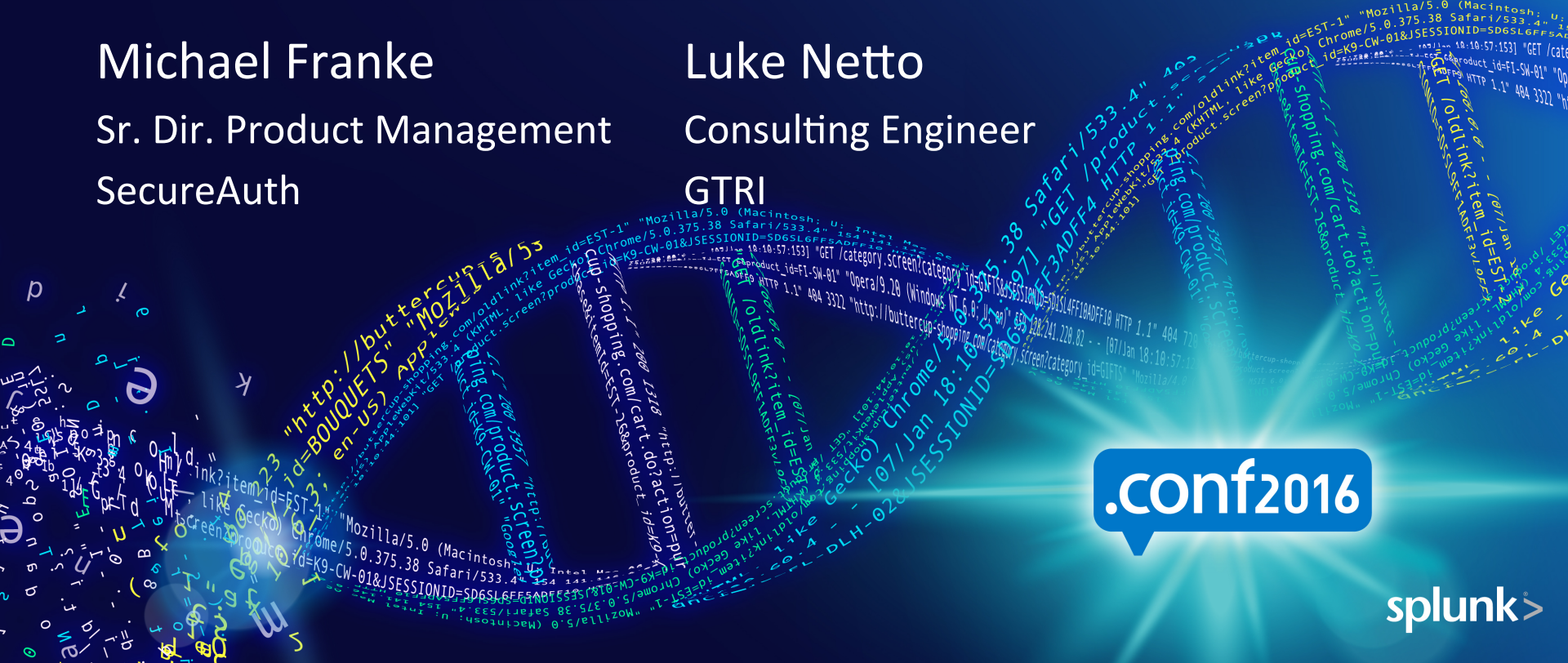
Sr. Dir. Product Management

SecureAuth

Luke Netto

Consulting Engineer

GTRI

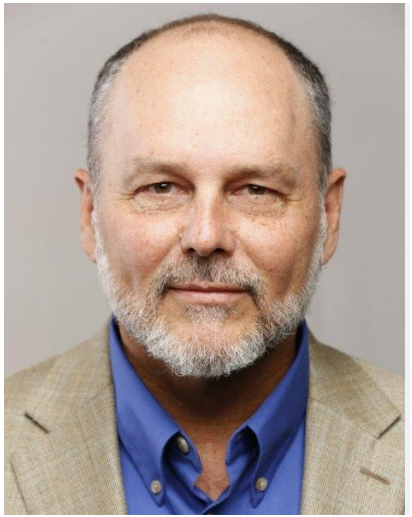


Disclaimer

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.

Michael Franke

- Michael Franke Sr. Director Product Management at SecureAuth
- 20 years of experience with leadership roles in:
  - Product Management
  - Development
  - Security
  - Virtualization
  - Sales Engineering
  - Technical Support
- ~1 year experience with Splunk



SecureAuth

- What is SecureAuth IdP?
  - Security product that protects access to corporate assets such as VPN, web based apps and many other applications through strong multi-factor, adaptive authentication
  - Deployed in enterprise and B2C environments supporting countless number of applications
  - Support diverse security and business workflows
  - Typical user logon workflow:
    - Adaptive check of source IP, machine characteristics…
    - Support 20+ multi-factor methods
    - SSO into protected resource such as VPN or web assets

Luke Netto

- Consulting Engineer at GTRI
- Adjunct Professor at the University of Denver
- 7 years of systems engineering
- 5 years of data analytics
- Systems engineering + data analytics = Splunk
- 3 years using Splunk

- Splunk's 1st Elite Partner and one of just a few Splunk Training Centers in the U.S.
- GTRI provides end-to-end support for Splunk from pre-sales engineering and design services, to post-sales professional services, implementation, training, and optimization
- Six (6) Splunk Partner Awards in the past four (4) years
- Splunk's most credentialed partner in North America:
  - Over 100 Splunk certifications across Sales, Engineer, Architecture and Consulting
  - 7 Certified Splunk Architects
  - 20 Splunk Sales Engineer Certificates (SE-I, SE-II, & SE-III)

Agenda

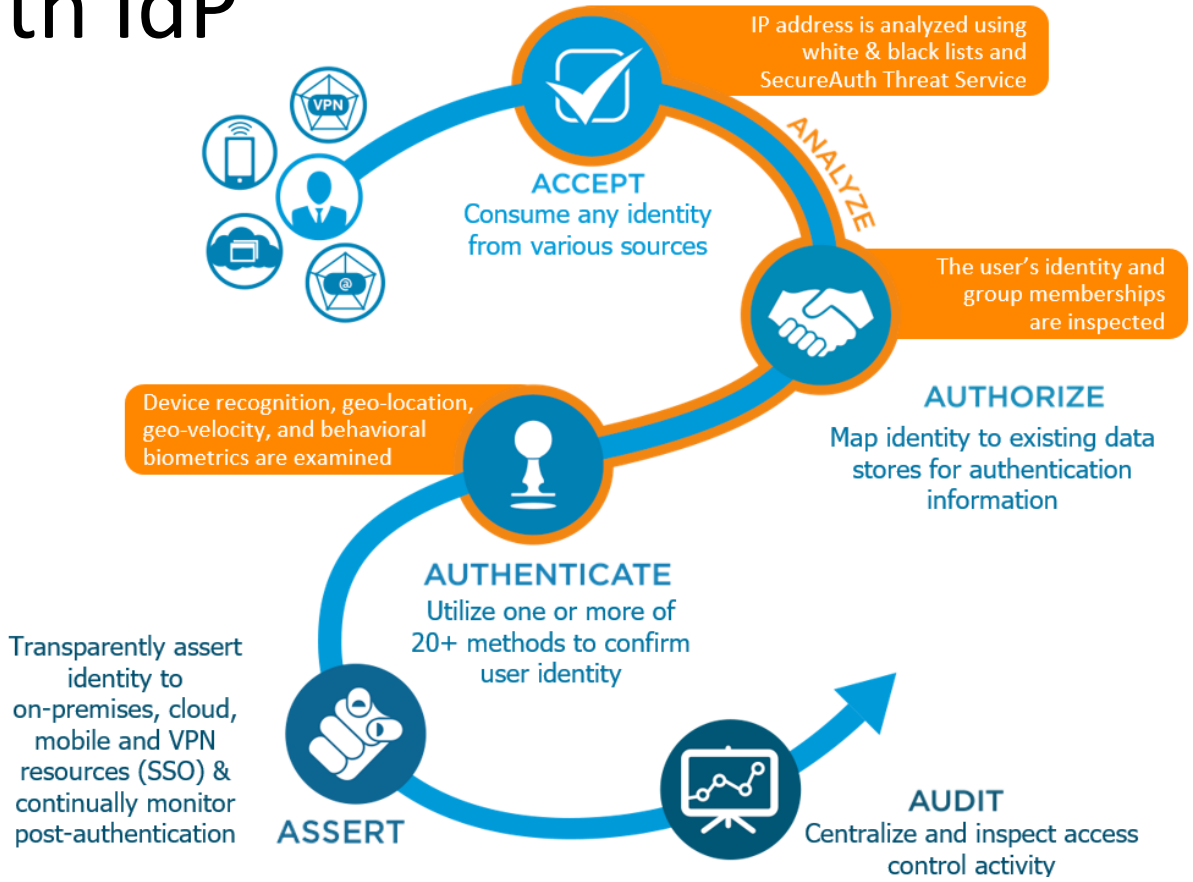
- Introduce the product, SecureAuth IdP
- Explain the need for reporting
- Why Splunk
- Customer responses to SecureAuth's app
- How the app has helped the development team at SecureAuth
- How the app has helped SecureAuth customers
- Demo
- App development and design

The Need

Security Industry Trends

- Large scale data breaches are now weekly news
- Attackers are adapting to countermeasures
- Security requires multifaceted approach – not just a SMS
- Access Control applications provide breach, suspicious activity intel
- Security data digested by standard tools, not proprietary interfaces
- “Passwordless” logon – kill the password
- Various forms of biometric validation being widely adopted

SecureAuth IdP



Customers need visibility

- Security issues
  - Access from suspicious or banned countries, or IP ranges
  - Access attempts from known bad sources based on SecureAuth Threat Intelligence Aggregation Service
  - Detect “unnatural” movement – Logon from NY and CA within the same hour
  - Evaluate machine characteristics – Has this user used this device before?
  - Highlight suspicious activity such as abandoned logon events or high volume of logon attempts
- Utilization
  - Visibility into application utilization and access
- System status
  - System health
  - Dependency systems health (e.g. Active Directory)
- Performance Metrics
  - User response time
  - Dependency response times

Why Splunk?

- Significant customer demand
  - More than 60% of SecureAuth customers use Splunk
- Strength of Splunk's platform and ecosystem
  - Strong support in the market becoming a de facto "standard"
- Short time to market
  - Powerful platform that enabled world-class deliverable within a few months
- Leverage Splunk's brand and market penetration
  - Sales driver by way of SplunkBase
  - Companies looking for strong authentication, adaptive access control system

The Result

Customer Response

- Vast reductions in the time of resolution on issues
  - "Security incident investigations have been reduced from about 2 days to 2 hours"
- Provides clear visibility when investigating security issues
  - Ability to drill down to see every step user took
- Enables customers to monitor and plan for utilization needs
  - Capacity metrics for both IdP and applications
- Helps ensure a positive user experience by surfacing performance issues and system errors
  - IdP and dependency systems performance metrics surfaced
- Overwhelmingly positive customer response

SecureAuth's Response

- Surfaced omissions SecureAuth IdP logging
  - Some logging data was incomplete
- Illuminated valuable data that was not being surfaced in IdP logging
  - Some types of transactions were not producing sufficient log entries
- Worked with early adopter customers refining both data and format
  - Additional visualizations added
  - Details on API utilization
  - More detail data in logging

Customer Success (Pharmaceutical)

- A large pharmaceutical customer reduced security investigations from an average of two days to an average of two hours
  - Clearly visualize the issue
  - Ability to drill down into the logging data and see every step the user performed
  - Source IP, access times, targeted resources, outcome

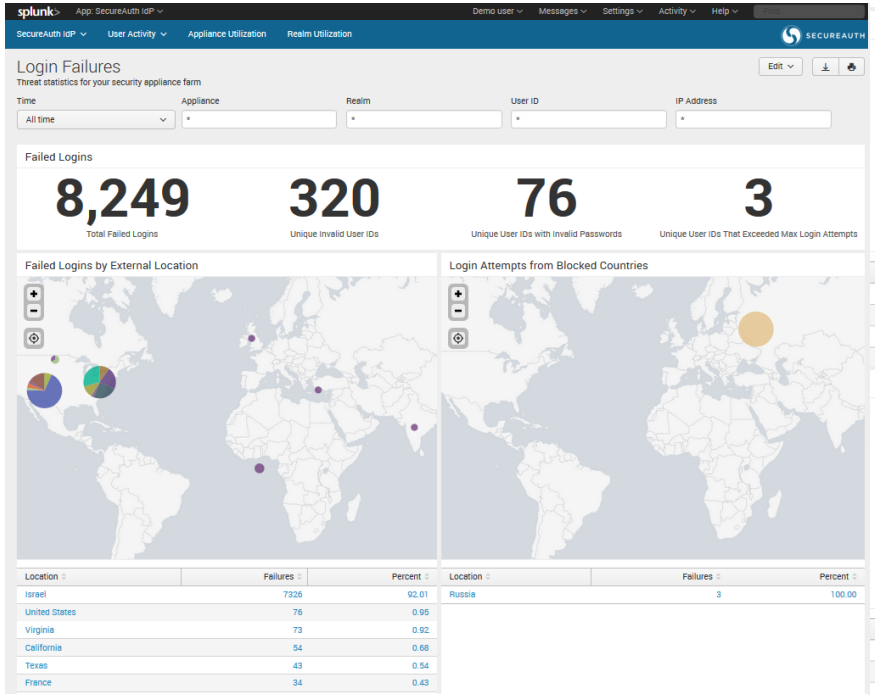
Customer Success (Healthcare)

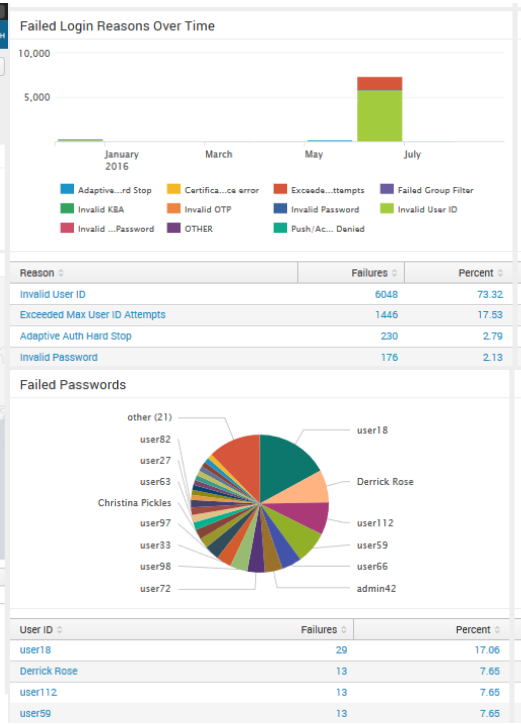
- Enabled a healthcare organization to detect and resolve an evolving attack by foreign hackers
  - Stolen credentials being used to access hospital systems
  - Breach was underway at the time the system was implemented
  - Threat aggregation feed detected malicious IP addresses
  - Geolocation data pinpointed hacker country of origin
  - Strong multi-factor and adaptive authentication thwarted APT breach

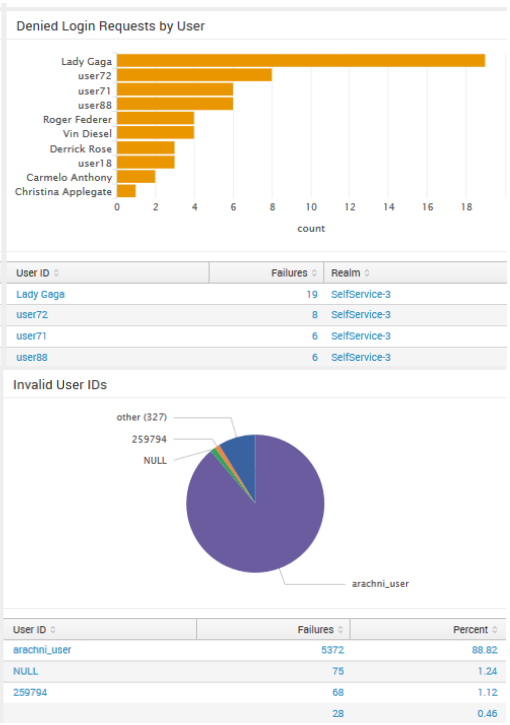
Indirect Revenue Benefits

- Better visibility means increased usage
  - Most customers start with limited use cases such as VPN
  - Vast majority increase utilization to protect all web apps, internal and SAAS
- Existing customers have added more applications and users to our system, on an average of 10% per customer!
  - Some customers have 10x increase in system utilization

Demo







splunk> .conf2016

Application Development

What did SecureAuth learn?

- Our logging was not perfect
  - Splunk was able to bring defects and omissions to light
- We have even more valuabe data to show customers than first anticipated
  - Splunk enabled us to provide amazing visibility into customer logon events and system status
- GTRI – a world class Splunk partner
  - Very professional and enterprise-class dashboard
  - Sped time to market
  - Increased accuracy of reporting

What did GTRI learn?

- Embed external requirements into your app
- Using a platform such as GitHub will prevent email overload
- Giving the customer or end user access to your development environment helps reduce surprises and makes it easier for them to test

Proper Logging

- If you are lucky you can sway the developers' logging format
- Splunk does NOT require logs to be in a special RFC or CEF format, Splunk just wants timestamped data
- Use a timestamp for every event!
- Use unique identiers such as transaction IDs, user IDs, and Event IDs
- Make logs human readable
- http://dev.splunk.com/view/logging-best-practices/SP-CAAADP6

Proper Source Types

- How many of you have asked someone for the type or source of a set of logs and received syslog as the answer?
- Source types tell Splunk what kind of data you have, syslog represents many different kinds of data
- Create a specific source type for your data

Sample Data Is Important

- Sample data is not only used to build your app, but should be included when you publish you app
- This allows other Splunkers to use EventGen and demo your app without having to generate their own data.
- By the way, you can use Splunk to anonymize your data samples! Who said only support can have all the fun?

EventGen Samples

- Put data generated by EventGen into a separate index, don't make kittens sad!

```
props.conf
[source::...secureauth_idp*.sample]
sourcetype = secureauth:idp
TRANSFORMS-secureauth_demo_index =
secureauth_demo_index

transforms.conf
[secureauth_demo_index]
REGEX = .
DEST_KEY = _MetaData:Index
FORMAT = secureauth_demo
```

Macros Are Your Friend

- Use a base macro to specify you index and source type
- This allows the end user to change their index easily and prevents your app from having to search across all indexes!

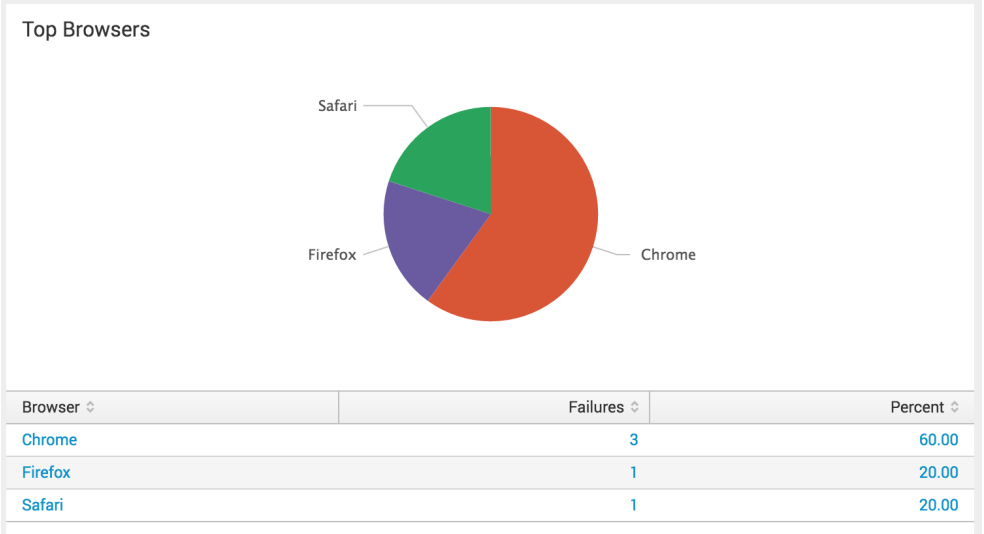
macros.conf

```
[secureauth_base]
definition = (index=secureauth* sourcetype=secureauth:idp NOT Category=DEBUG)
iseval = 0
```

Search Once, Display Twice

Use a post-process search!

```
<panel>
    <title>Top Browsers</title>
    <chart>
      <search base="browsers">
        <query></query>
      </search>
      .
      .
      .
    </chart>
    <table>
      <search base="browsers">
        <query></query>
      </search>
      .
      .
      .
    </table>
  </panel>
```



Lookup at the Right Time

- How many people would do this?
  - sourcetype=mydata| iplocation src | geostats count by Country
- Aggregate your data first!
  - Sourcetype=mydata | stats count by src | iplocation src | geostats sum(count) as count by Country
- Check out my blog on blogs.splunk.com for another lookup trick: "Lookups: Not Just for Enriching Data." http://goo.gl/RLfkMu

We're Not in Kansas Anymore

- "… if we believe the users of your IP are mostly in the US, but aren't certain about the city and State we may leave them blank. In this case the lat/lon will correspond to the center of the US which happens to be in Kansas."

  - MaxMind Support

https://support.maxmind.com/correction-faq/ip-resolution/why-is-the-latlon-for-my-ip-in-kansas/

Internal Addresses

- Remember, iplocation does not work with internal IP addresses
- Use iplocation in combination with a custom lookup

transforms.conf

[internal_ip_lookup]

filename = internal_ip.csv

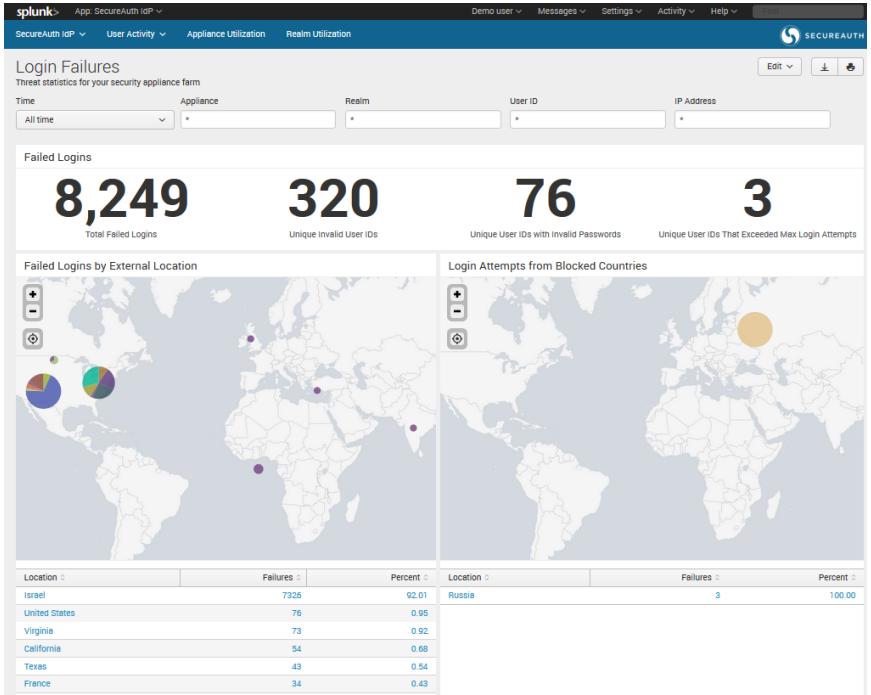
max_matches = 1

min_matches = 1

match_type = CIDR(ip)

Simple and Clean

- A consistent look and feel is key to an eye-catching app
- Stay with Simple XML if possible



The Process

Understand the Data

- Does documentation describing the logs already exist?
- If not, use the product manager ☺
- Understand the system producing the log(s)
- Understand the different unique IDs
- Break the logs into categories such as user vs. system
- Break the categories into sub-categories or transaction types such as a user login vs. a user adding a product to an online shopping cart
- Secureauth gave basic queries to GTRI to help visualize the outcome

Obtain the Data

- Syslog, SQL, CEF, flat files … oh my
- Some systems output more details using one log format versus another, use the one that makes sense, Splunk can ingest them all
- Obtain the data in the most raw form – export SQL tables to flat files, use a tool such as netcat to capture logs being transmitted over a network
- The key is to obtain enough data that represents complete transactions of every transaction type you expect to visualize

Use a Development Instance

- Splunk easily scales from the Desktop to Enterprise
- This means you can use your laptop for development!
- Use multiple installations
  - /opt/splunk/splunk_secureauth
  - /opt/splunk/splunk_abc
  - /opt/splunk/splunk_xyz
- Break things and ask questions!
- Don’t be afraid to start over!

What Now?

- Get the app, use Eventgen, and demo it yourself! The demo data will take some time to generate. http://www.gtri.com/secureauthapp/
- Secure your own environment with SecureAuth IdP! http://www.gtri.com/secureauth/
- Have co-workers that are new to Splunk? Have them attend a FREE hands-on Splunk Bootcamp from GTRI! http://www.gtri.com/splunkbootcamp/

THANK YOU

splunk>