SECURITY++

USING SPLUNK FOR SECURITY OPERATIONS

$ whoami

- Marc Silver (@bsdkid).
- Passionate about information security, all round geek.
- Information Security, Discovery Limited.
- Not a sales person, not a Splunk agent, just knowledge sharing.

What we're talking about…

- What problem were we trying to solve?
- What solutions did we consider and why did we choose Splunk?
- What design principles were used to architect it?
- What does our infrastructure look like?
- What/how do we use it?
- Where are we going with it?
- Lessons learned.
- Tips to DIY…
- Questions.

“When you can measure what you are speaking about, and express it in numbers, you know something about it.”

- Lord Kelvin

THE PROBLEM

- We started our journey around four years ago…
- Security is complex.
- Important to understand:
  - what you're trying to protect,
  - What the threats you're protecting against are,
  - How to DETECT them,
  - How you will respond to them.

- Thankfully, many products exist to help us.
- Herein lies some of the complexity and challenge.
- Security products and tools generate lots of data (not all of it useful).
- Tools are needed to help us sift through it all.

- Our objectives:
  - Import data from multiple sources across our network and normalise it.
  - Easily discard information of no value to us.
  - rapidly develop functional logic around the data.
  - alert on specific events we care about.
  - generate valuable reporting.
  - scale and grow as we do.
  - Get ACTIONABLE intelligence from our logs.

THE SOLUTION


HOW DID WE MAKE OUR DECISION?

Source: Gartner (August 2016)

- Lots of research and reading.
- SIEM solutions considered with input from sources such as Gartner, Forrester.
- Lots of discussions with vendors (with additional work to see through the bullshit they try to spin to sell their snake oil).
- Lots of internal discussion and POC's.


The Paradox of Choice


splunk>

BUT ALMOST NOT…

- COST IS A **MAJOR** FACTOR WITH SPLUNK, PARTICULARLY WITH THE WEAK ZAR.

WHY?

- It looks slick as hell. OK, maybe that's not one of the reasons…. :P
- Highly flexible for ingesting data via light, heavy forwarders, syslog.
- Excellent integration into third party data sources like Oracle, MS-SQL etc.
- Support for all the OS's we use (and more).
- We liked the concept of hot, warm, cold data etc.

WHY?

- Flexible data retention.
- Flexible way to assign access at an index level.
- Compression to alleviate storage costs.
- Powerful, flexible query language.

WHY?

- Scalable design.
- Naturally intuitive interface.
- Great reporting capability.

WHY?

- MOST IMPORTANTLY:
  - FITTED OUR CULTURE WELL – DEVELOP INTELLIGENCE WITHIN.

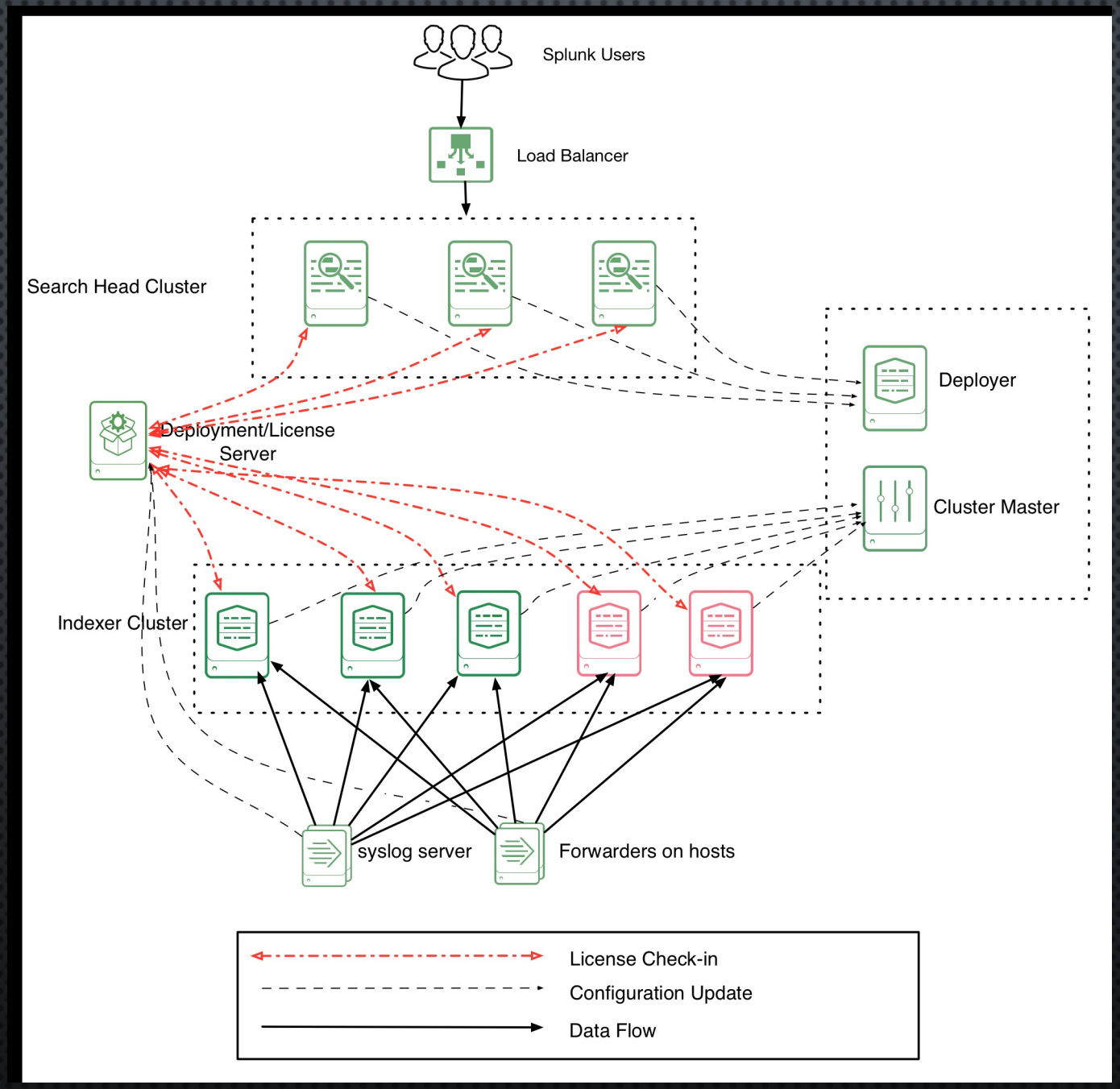
ARCHITECTURE AND IMPLEMENTATION

Design Principles

- Future proof our design as much as possible.
- develop standards for index names and source types up front.
- Index only what's important. Cut out the fat in dev.
- Do it once and never again. Get it right.

SPLUNK COMPONENTS

- INDEXERS
- SEARCH HEADS
- DEPLOYMENT & LICENSE SERVER
- FORWARDERS

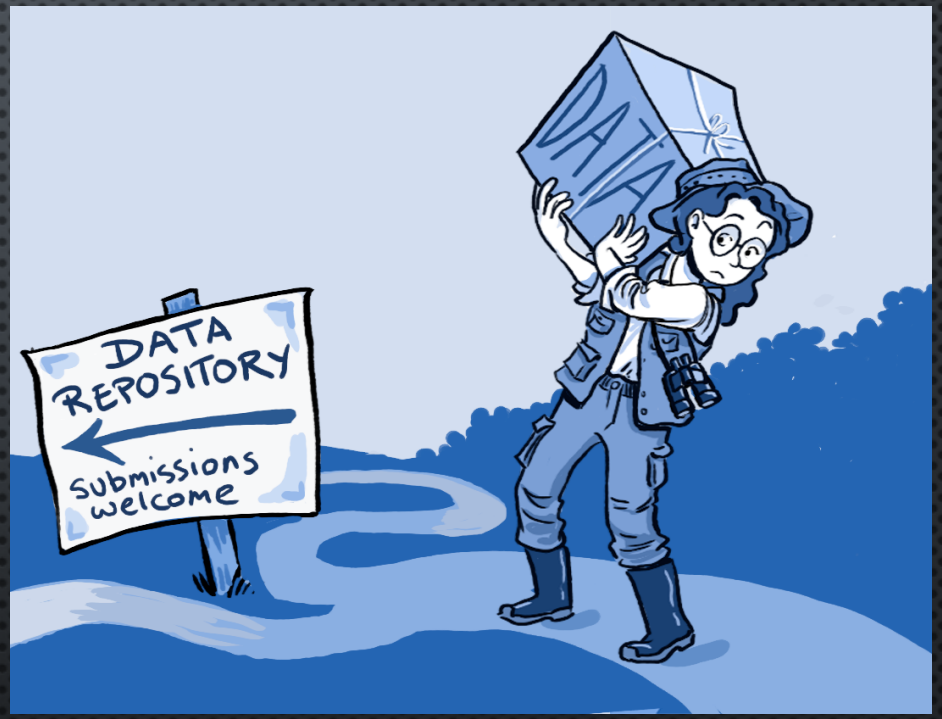

Splunk Users
Load Balancer
Search Head Cluster
Deployer
Deployment/License Server
Cluster Master
Indexer Cluster
syslog server
Forwarders on hosts
License Check-in
Configuration Update
Data Flow

Some Statistics

- 5 Indexers.
- 3 Search Heads.
- 1 Deployment & License server.
- MANY forwarders.
- 205GB data indexed daily.
- More than 140, 000, 000 (140m) events logged per day.
- More than 4, 200, 000, 000 (4.2B) events logged per month.

SOLVE YOUR PROBLEMS, DON'T GET DISTRACTED

- DATA IMPORTED SLOWLY AND OVER TIME.
- ENSURE ALIGNMENT TO YOUR OVERALL OBJECTIVES AND CONTINUALLY EVOLVE OVER TIME TO MAXIMIZE VALUE.
- MINIMIZE NOISE AND ALERT ONLY ON HIGH FIDELITY EVENTS.



HOW ARE WE USING IT?

Logs, logs and more logs.

Needles in Haystacks

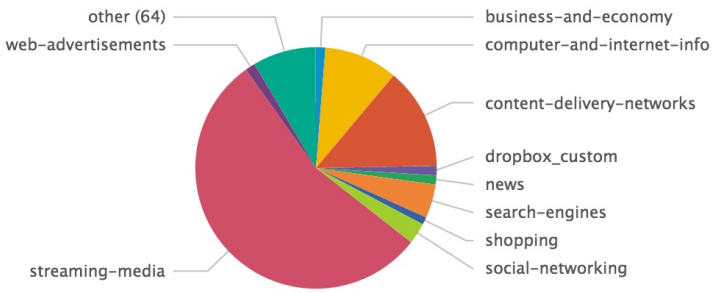
- Real-time detection of phishing attacks against clients.
- Real-time detection of login failure variance.
- Correlation of vulnerability management and patch management systems for accurate views of vulnerabilities across our network.
- Real-time alerting for specific ports of interest. (for example, C2).
- Real-time alerting from *points of interest* on our network.

CATCH ‘EM BEFORE THEY’RE GONE

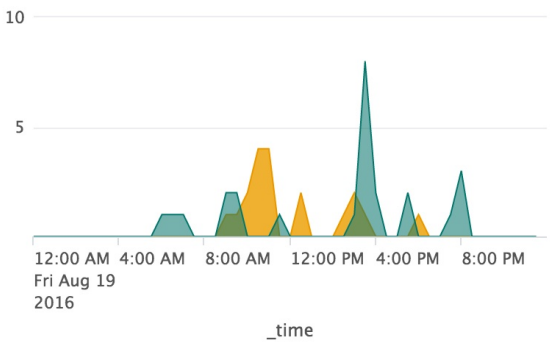
- Visibility and reporting around DLP events.
- Ability to detect geographical anomalies around user connectivity.
- Real-time tracking of sensitive groups.
- Visibility of common intruder attacks such as pass-the-hash etc.
- Alerting for users who download high risk tools.
- After hours alerting through integration with third party messaging services.


INCIDENT

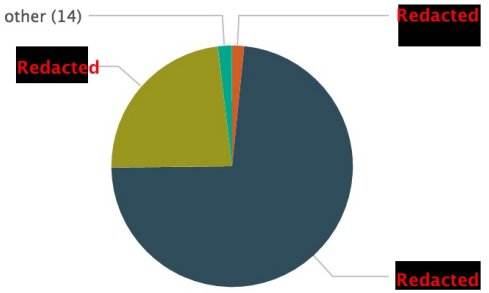
Top Browsing Categories (DSY)



Failed VPN logins over time



Malicious Tools Downloaded by User (DSY)

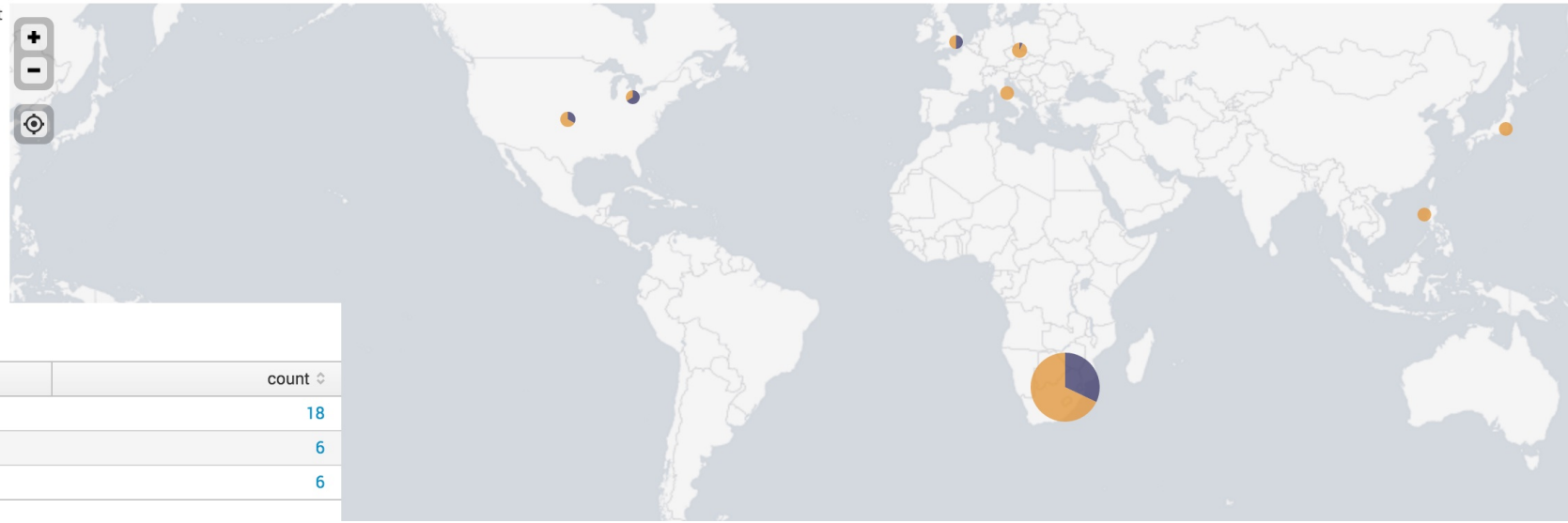


Member Changes to Browsing-Red (DSY)

VPN User Login from Different Country < 24 hours (DSY)

user	_time	dc_country	country
Redacted	2016-07-22 02:00	2	India South Africa
	2016-07-29 02:00	2	India

Dropbox Login Activity by Location (DSY)



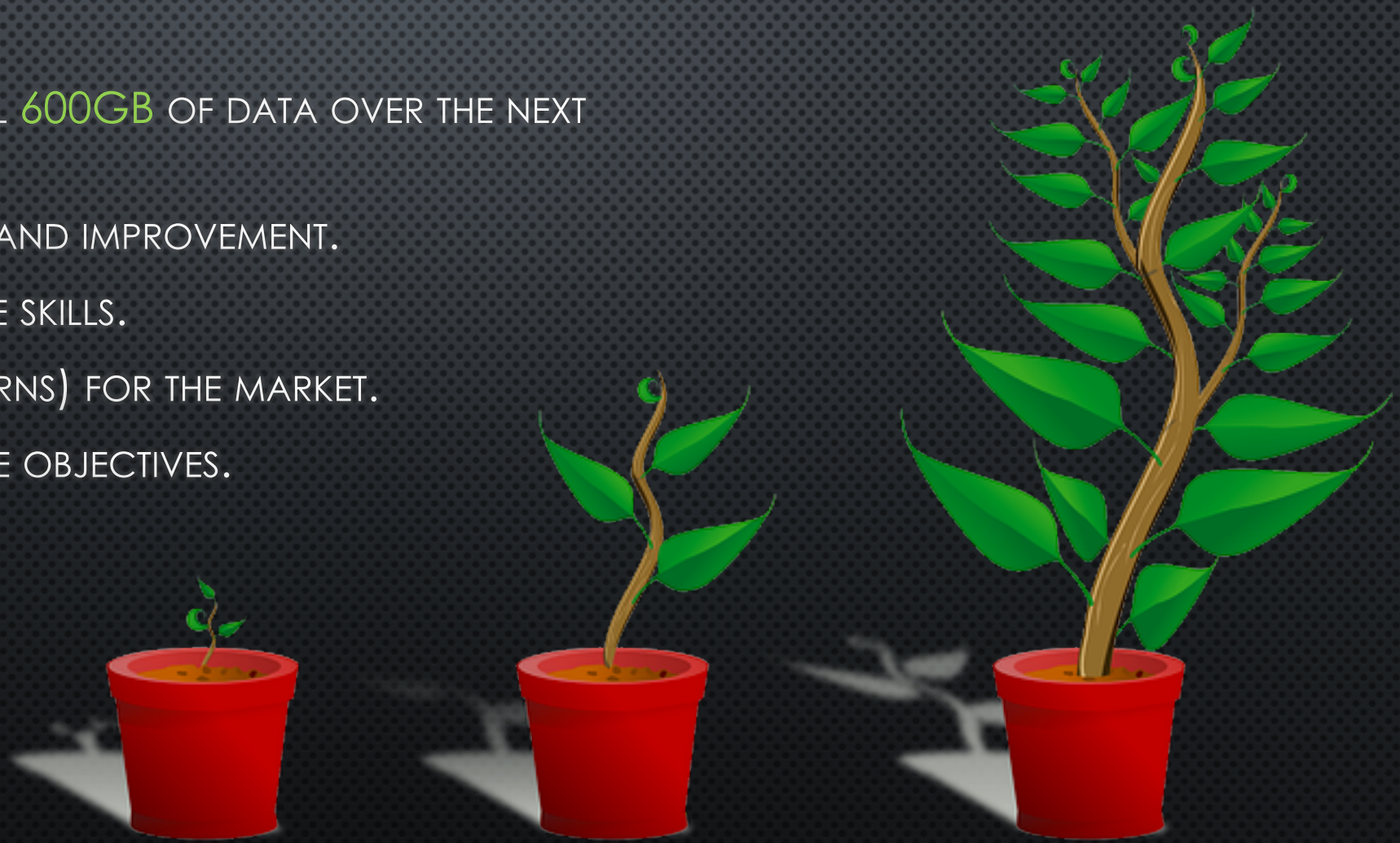
Failed Login Attempts to Routers from Public IP's (Global)

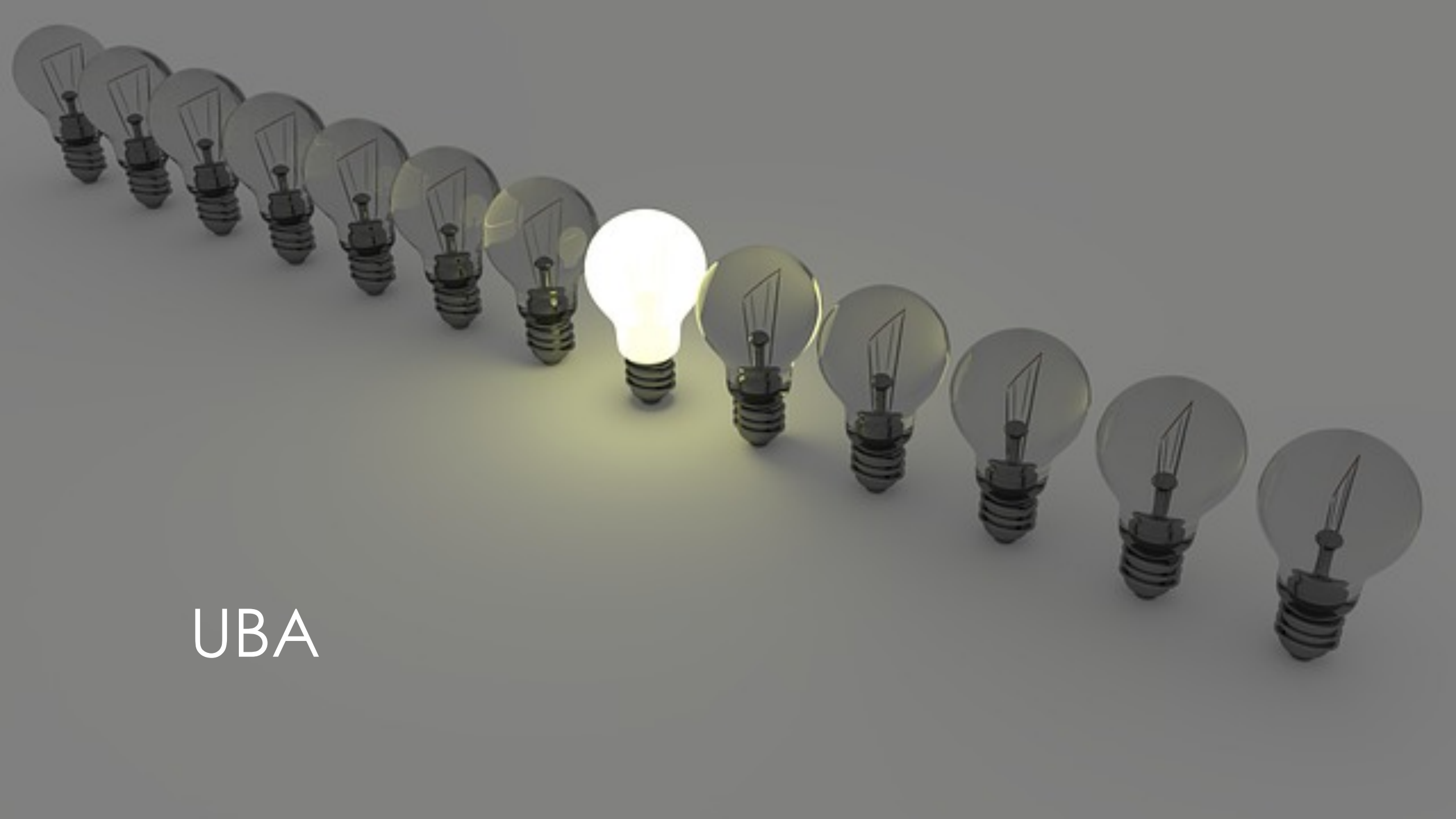
NetworkDeviceName	count
Redacted	18
	6
	6

Sorry, we can’t share more specifics.

WHERE ARE WE GOING?

- Index an additional 600GB of data over the next three years.
- Focus on growth and improvement.
- Grow our in-house skills.
- Develop skills (Interns) for the market.
- Focus on our core objectives.





UBA

LESSONS LEARNED

Things we learned along the way

- Time is absolutely critical. You're not correlating *anything* if your servers aren't using NTP.
- Splunk requires attention and dedication to see results. Don't be in a rush; work slowly and methodically and you'll go far.

Things we learned along the way

- Skills take time to develop; you will unlock more from Splunk as your own skills develop.
- People with some programming knowledge (and especially regex knowledge) are productive in Splunk FASTER than others.
- Invest in solid hardware and storage.
- Don't be scared to make mistakes.

DO IT YOURSELF

What are you waiting for?

- Get started. But plan… and then plan more.
- Start small. Show value, then grow.
- Use tools (regex buddy) to ease your way.
- Invest in people. Tools only take you part of the way and security analytics still requires great people.
- Don't become complacent. Evolve; your attackers are getting better every day and so should you.

THANK YOU FOR LISTENING.
QUESTIONS?