Using Splunk to Enhance, and Prove, Your Security Awareness Programs

About Josh

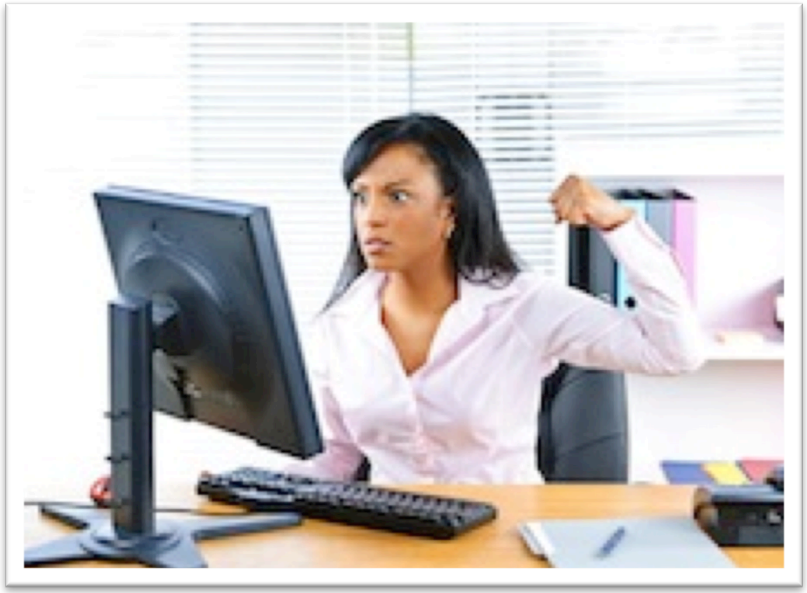
- Canadian
- Managing Partner at Discovered Intelligence
- Using Splunk 6+ years – 5 years as a customer
- Co-Author of "Splunk Operational Intelligence Cookbook"
- IT and Security Ops background

What This Talk Is

- Security Awareness Challenges
- Intersection of Data and Awareness
- Harnessing Data to Build Awareness
- Data-driven Value Measurement

Security Awareness Is Boring

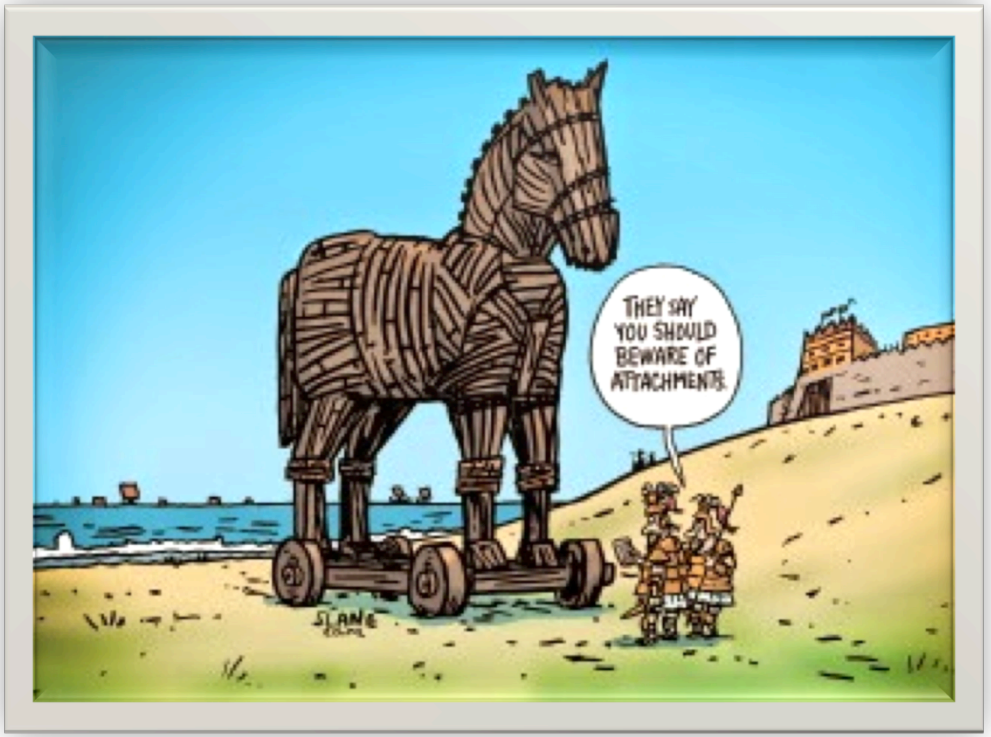
- Dull topics
- Generally dull delivery
- Hard to relate
- Hit & Run



"Really?! More training?!!"

- Everyone

But Security Awareness Is Important…



PREMERA | BLUE CROSS

Mar 17, 2015 – **11.2M** records (names, addresses, DOB, SSNs, bank info & more)

July 19, 2015 – **32M** records (names, addresses & more) + **12.7GB** of corporate emails

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

June 2015 – **21.5M** records (names, addresses, SSNs, fingerprints & more)

BlueCross BlueShield CareFirst

May 20, 2015 - **1.1M** records (names, DOB, emails & subscriber info)

Phishing Statistics

- Phishing cost global organizations $4.5B in 2014
- Globally, attacks rose 162.79% from 2010 to 2014
- Spear phishing attacks rose 40% globally in 2014 alone
- Email fraud has shown to have up to a 45% conversion rate
- Customers are 42% less likely to interact with a brand after being phished

Source: http://blog.returnpath.com/blog/estelle-derouet/13-email-fraud-stats-every-security-professional-should-know

KEEP
CALM
AND
TRAIN
HARD

What We Know About Behavior

- Personal messages are most effective
- People place undue weight on recency
- Are most drawn to relevant material
- People are most influenced by others like them
- (most) Want to do the right thing

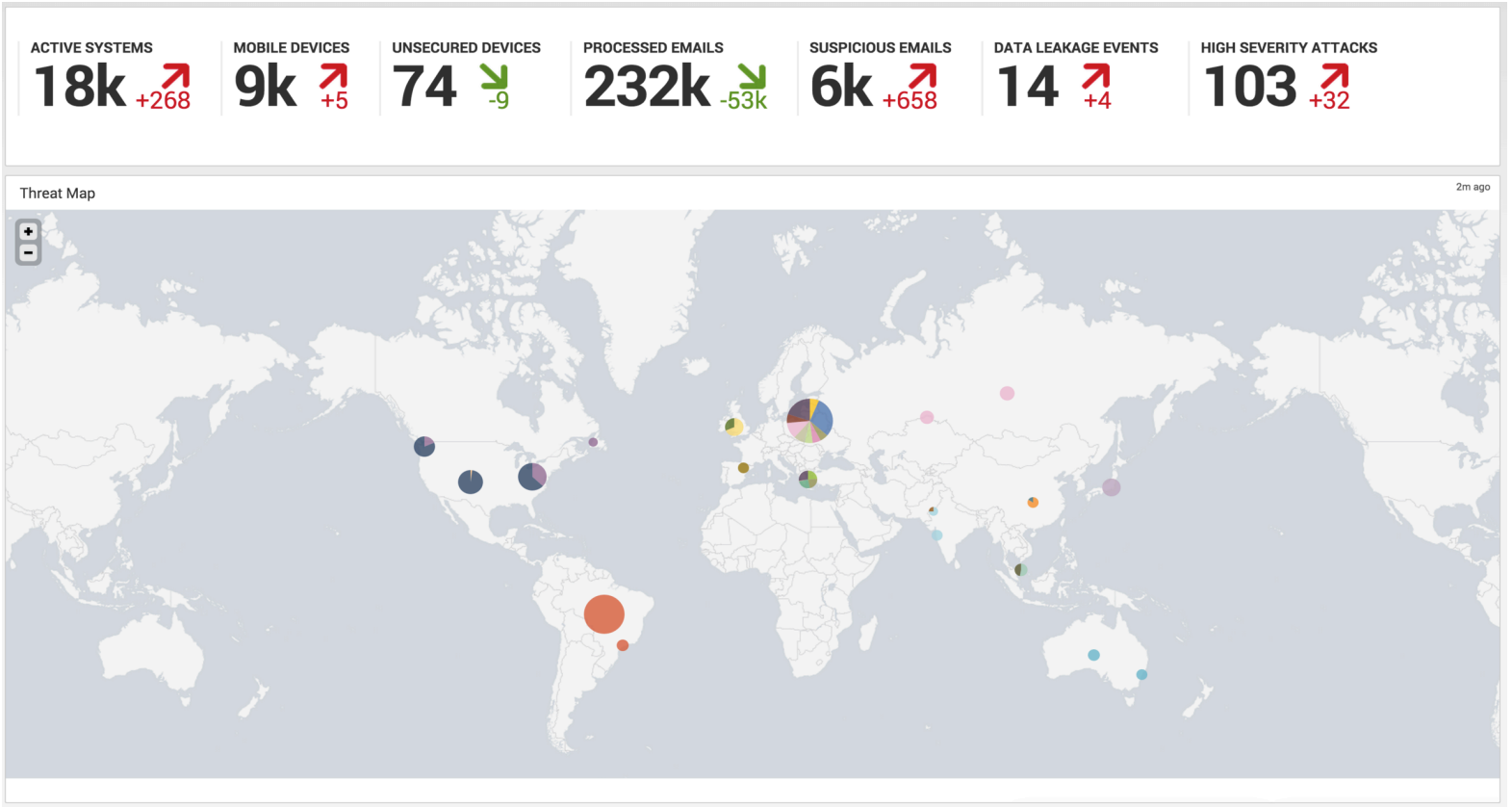
Discovered Intelligence

Do More With Your Big Data™
DiscoveredIntelligence.ca

Incorporate Data Into Awareness Campaigns

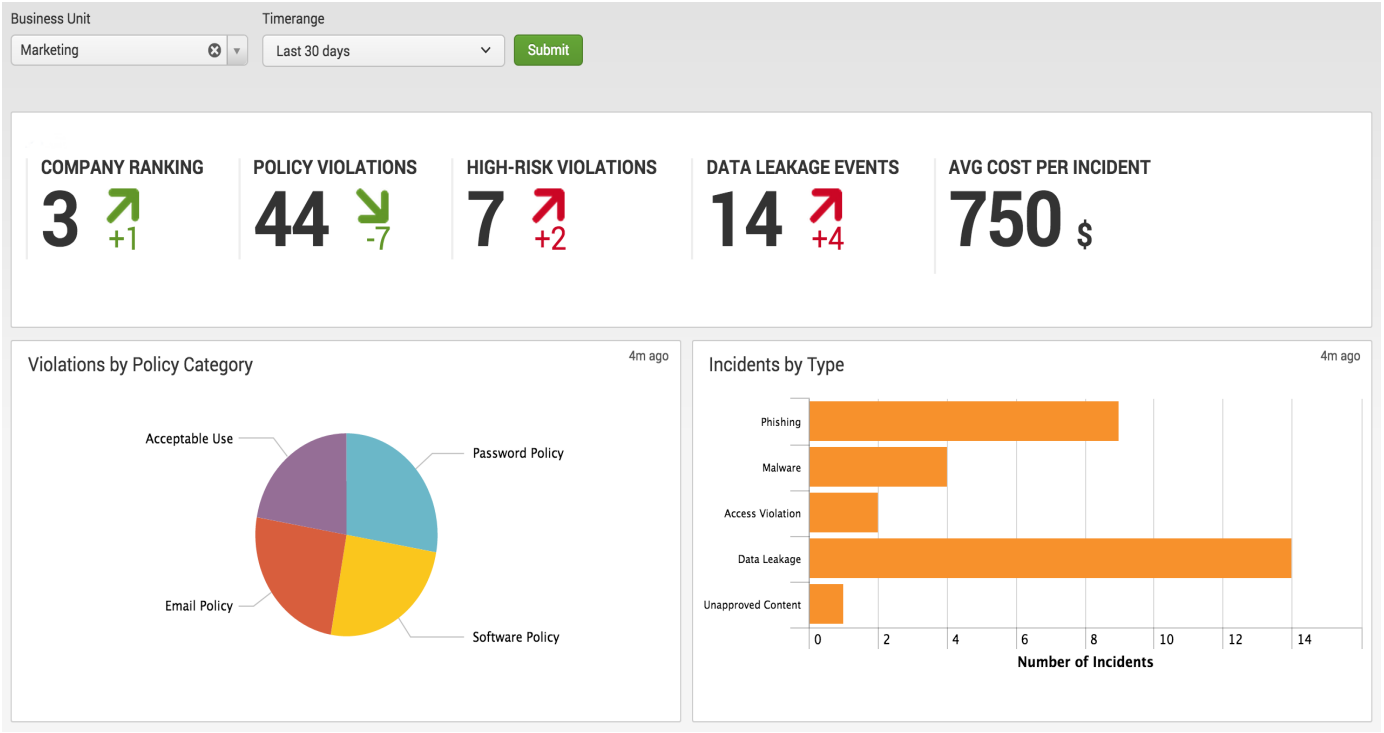
- Ensure materials inclusive of most-recent, relatable, data
- Use public dashboards (think, extranet) that relate current state to awareness topics
- Provide a level of threat intelligence they can relate to and that can become immediately actionable
- Creates a culture of continuous awareness

Illustrate The Risk Landscape



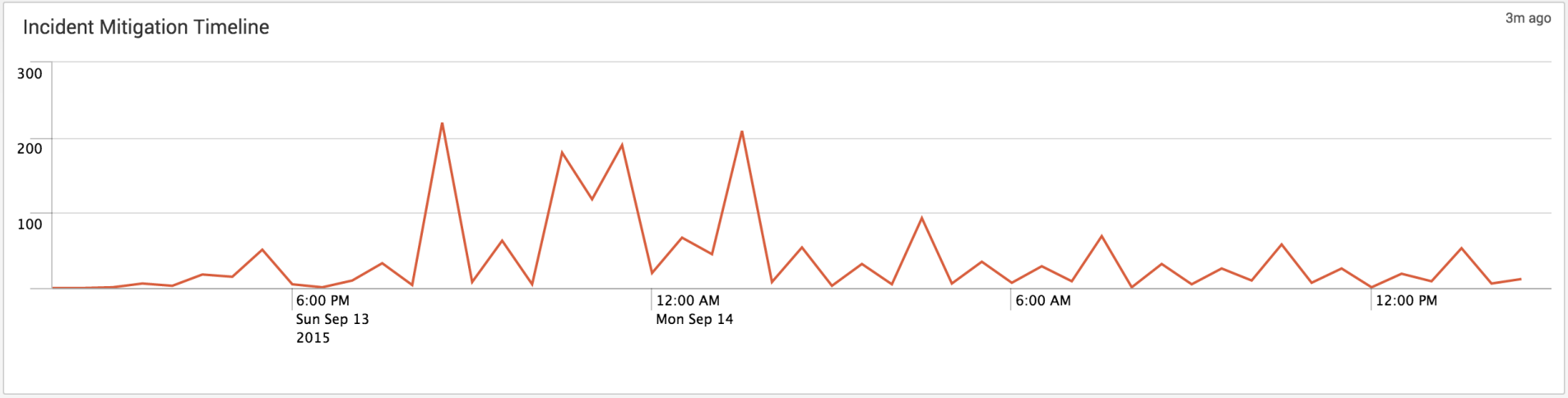
Targeted Training Means Relatable Data

- Focused
- Relatable Metrics
- Drive competitive nature
- Make an impact
- Measure data against dollars



Highlight Employee Contributions

EMAIL SUBMISSIONS	URL CONTRIBUTIONS	SECURED PERSONAL DEVICES	INCIDENTS MITIGATED	INCIDENT SAVINGS
35	16	97 %	516	141k $



Automate “friendly reminders”

- Periodic scheduled searches for high-risk policy violations
- Define acceptable threshold for policy violations in a given window
- When threshold is breached automate a friendly reminder on the policy along with some helpful information
- Splunk command for dynamic email generation to multiple recipients:

  sendresults - https://splunkbase.splunk.com/app/1794/

How Do We Measure…

Traditional Methods for Measuring Effectiveness

- Who completed the training
- Scored based on CBT or quizzes
- Feedback from survey's
- Observing physical behavior

…All of this is good, but what does it provide?

…A Good Measurement of Someone's Mood

Data-driven Measurements of Effectiveness

- Surprise #1… everything we do produces data (wow!)
- Surprise #2… that data is most likely in Splunk!
- Take your policies and map it to the data (Quantifiable metrics!)
- Ability to produce continuous measurements
- Learn about behaviors, not moods!
- When educating, use tools that produce a digital footprint

Policy to Data Examples!

- Users not updating/patching their devices

  tag=update status=installed | stats min(_time) AS install_time by dest, signature_id | stats max(install_time) AS install_time by dest | eval days_ago=round((time()-install_time)/86400,2) | search days_ago>15 | fields – install_time

- Unapproved cloud application usage

  tag=proxy OR tag=dns NOT tag=internal_dest | lookup cloud_domains.csv dest OUTPUT is_permitted | search is_permitted=false | stats count by src,user,dest

- Usage of untrusted/unapproved applications

  tag=process OR tag=service | lookup untrusted_applications.csv process service OUTPUT is_permitted | search is_permitted=false | eval application=if(isnotnull(process),process,service) | stats count by dest,user,application

- Transmission of sensitive materials externally

  tag=email NOT tag=corporate_domain | lookup risky_file_names.csv file_name OUTPUT is_permitted | search is_permitted=false | stats count by file_name,src_user,recipient

- Vulnerabilities are patched within reasonable time

  tag=vulnerability | stats min(_time) AS first_seen max(_time) AS last_seen by dest, signature | where first_seen!=last_seen | eval days_vuln=(last_seen-first_seen)/86400 | stats avg(days_vuln) as avg_days_vuln

- Accessing inappropriate content

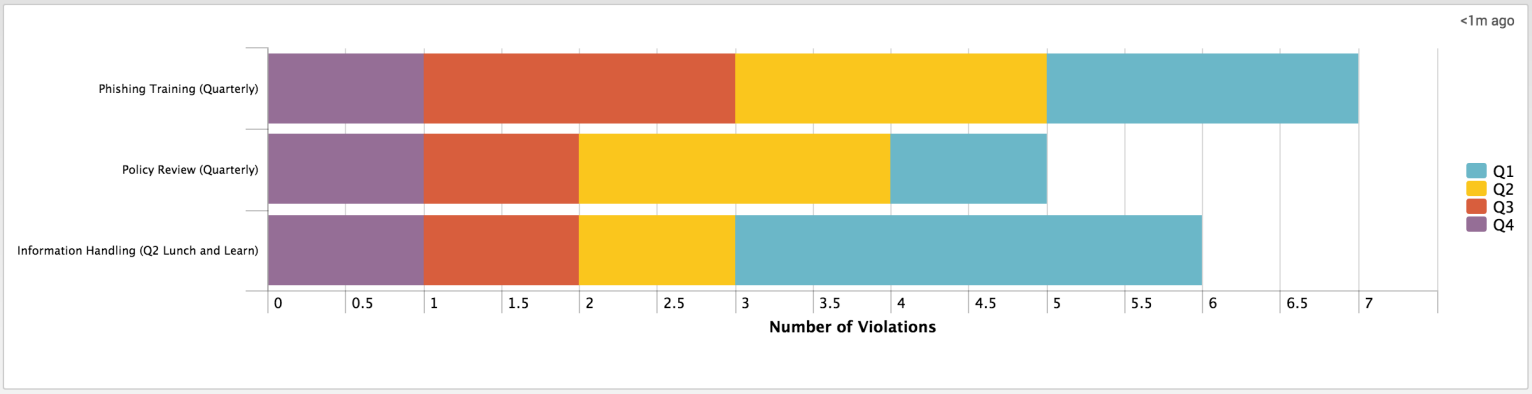
  tag=proxy | lookup proxy_categories.csv category OUTPUT is_permitted | search is_permitted=false | stats count by src,user,category

- Must use badge when entering or exiting office

  tag=badge badge_event="entry" earliest=@d latest=now | append [search tag=badge badge_event="exit" earliest=@d latest=now | stats count AS badge_exits by user] | stats count AS badge_entries, values(badge_exits) AS badge_exits by user | eval comment=case(badge_entries>badge_exits,"Tailgating OUT",badge_exits>badge_entries,"Tailgating IN",1=1,"Perfect! Commend this employee!") | table user, comment

Measure to Prove AND Improve

- Observe and compare before/after awareness campaigns
- Refine the scoring system for policy violations
- Use results to drive focused awareness campaigns
- Construct meaningful KPIs for management



Thank You!