Even Giants Start Small

Metricon 7 – David F. Severski

Security Metrics by Dante

Paradiso

Purgatorio

Inferno

Something for Everyone

- Addressing a very common problem
- See what we did wrong
- Calling out tools used
- Workflows used

Beginners

- Sage head nodding
- Application of principles

Advanced

Agenda in Three Acts

- Problem Identification
- Descriptive Analysis
- Implementing Change

Mandatory Background and Disclaimer Slide

1. We cure sick children.
2. Don’t sue me.

Act I: Problem Identification

- Framing the question

My Team’s Responsibilities

- Security strategy
- Incident management
- Audit, assessment, and compliance
- Risk management and monitoring
- Other duties as assigned…

Existing Risk Management Process

- Board focused
  - Qualitative rankings based on expert opinion
- Threat/Impact/Capability based
- Benchmarks leadership risk tolerances, current funding levels
- Used to identify and prioritize projects

Meta-Problem

- Risk management process provides strategic management
- Managing the tactical side (my responsibility) raises tough questions
    - How good are our capabilities?
    - What is the evidence?
    - What *are* our capabilities anyways?
- Working in our favor
    - Evidence-based medicine
    - Deep organizational commitment to Lean

Initial Steps

- Defined our controls
- Defined our threat scenarios
- Started exploring our data sources
  - Goal: Understand what data we have and how it can be used

Existing Vulnerability Management Process

- Patch management focused
- Death by spreadsheet
- Lots of data, little management knowledge/information
- Things *look* bad, but hard to be certain

Measurement Problem Formulation

- “How well is our patch management program performing?”
- Not explicitly stated or well defined

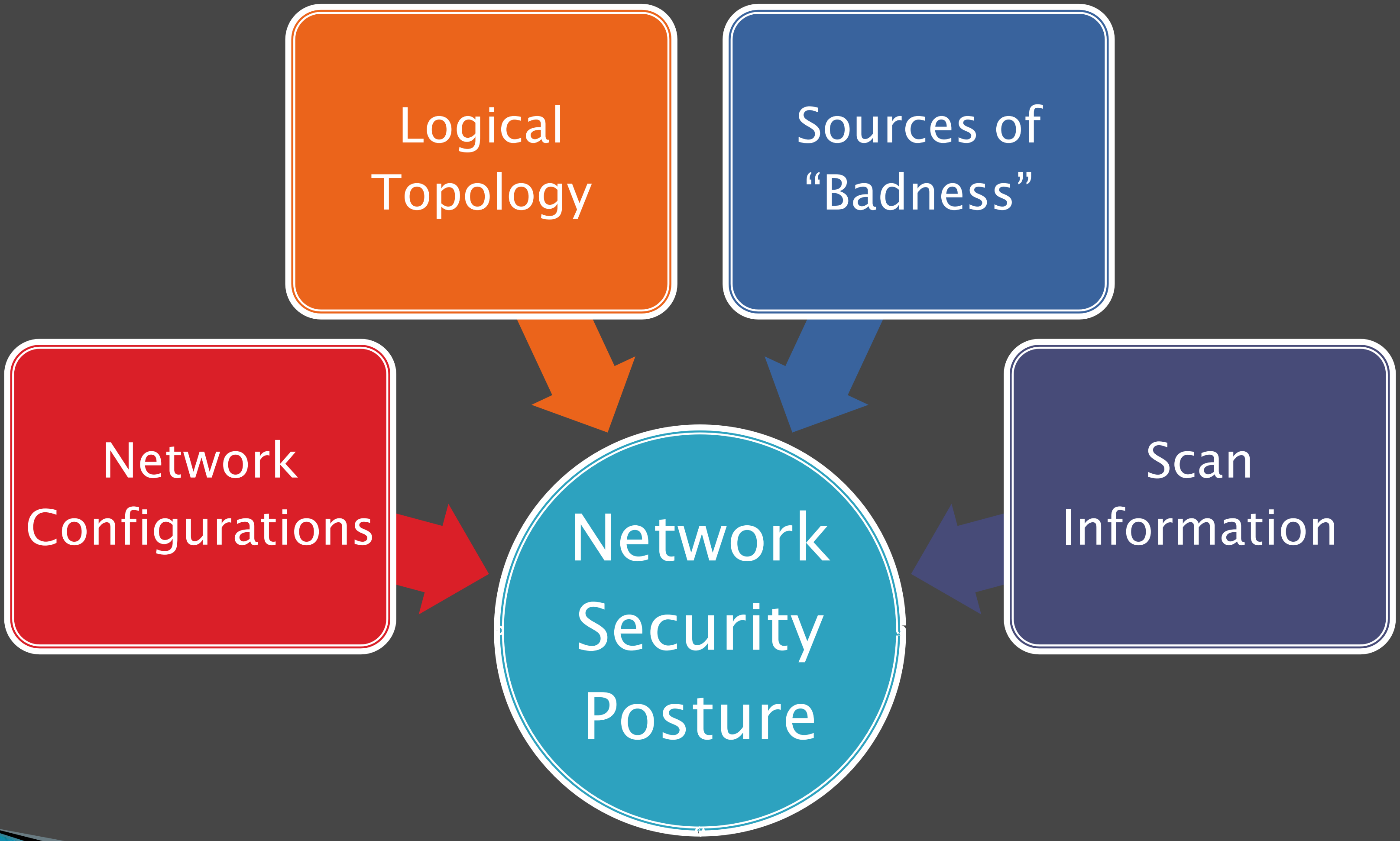
Act II: Descriptive Analysis

- Answering the question (maybe)

Gathering the Ingredients

- Data
  - Nessus scan data
  - Network configuration files
  - Network topology
- Tools
  - Network security posture analysis
  - Scripting
  - Visualization platform

RedSeal



Logical Topology

Sources of "Badness"

Network Configurations

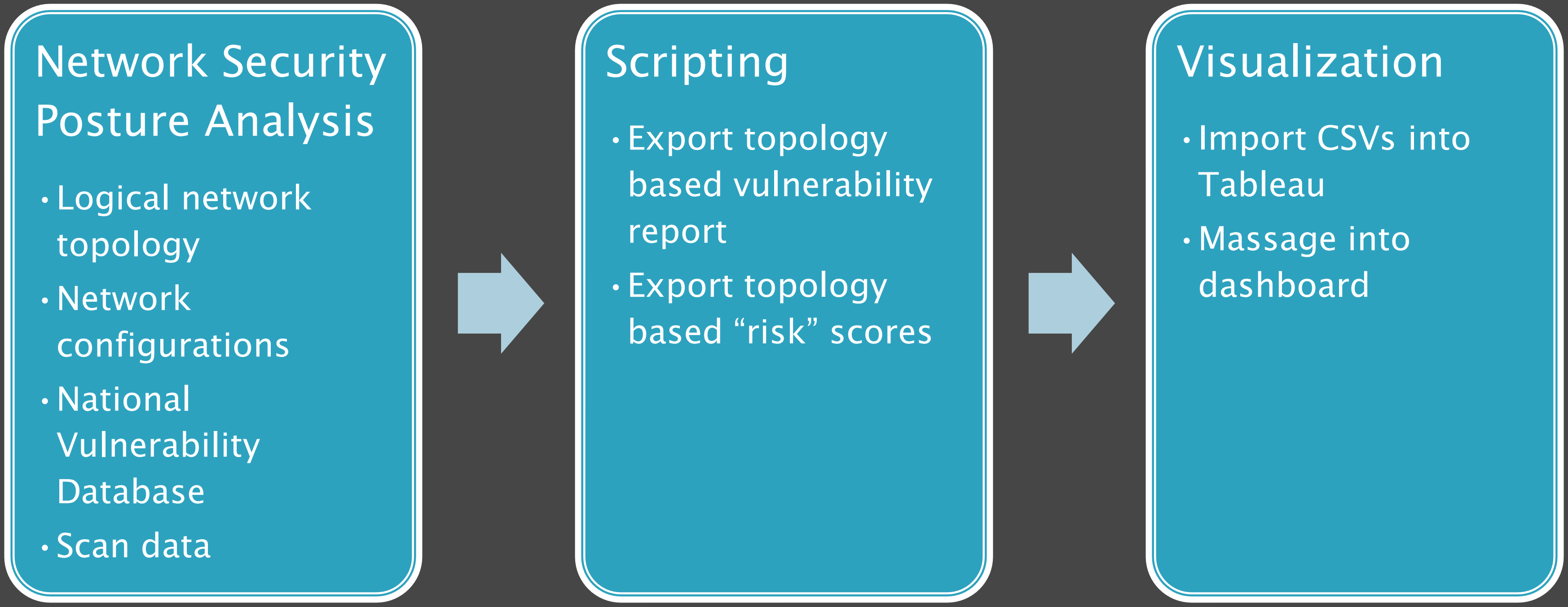
Scan Information

Network Security Posture

Visualization

- Tableau
  - Organization-wide standard visualization tool
  - A fun tool for visualization
    - Perhaps a little too fun

Our Data Flow



Network Security Posture Analysis

- Logical network topology
- Network configurations
- National Vulnerability Database
- Scan data

Scripting

- Export topology based vulnerability report
- Export topology based “risk” scores

Visualization

- Import CSVs into Tableau
- Massage into dashboard

Demo Time

- Let us beseech the demo gods

Alternative Tools

Vulnerability Management

- Risk I/O by HoneyApps
- Scan vendor of choice

Scripting

- Perl
- Python
- Ruby

Visualization

- Excel
- R & Inkscape

Act III: Implementing Change

- Reception and Problem Solving

Work in Progress

- Figuring out what's broken in our process
  - Scan data? Patch management process?
- Key questions so far
  - Is our SLA correct? What *is* our SLA?
    - Prioritized remediation efforts (Have this now)
    - Prioritized assets (Working on this)
  - Who owns the process?
  - Are there feedback loops (operational metrics) in the process?

Looking Back and Looking Forward

“Mistakes Were Made”

- Problem not well formed
- Dashboard is ugly & opaque
  - Edward Tufte is sad
- No historical trending
- Scoring mechanisms not rigorous
  - CVSS base scores, no temporal or environmental
- Labor intensive
  - Currently takes a couple of hours monthly to update
- Fuzzy numbers
  - Risk Index metric
- Data quality problems
  - Gaps in scan data
- Data definitions
  - What is an open vulnerability?

But These Mistakes Haven't Been Fatal

- Problem was not well enough formed
- Dashboard has raised useful questions
- Trending is on the roadmap
- Scoring is consistent over time
- Risk Metric – A consistent index that shows of what's out there today versus yesterday
- It's the data we have at hand
- Push out with v1.0 metrics now
- Iterate over time as we get more traction, time, skills

Current Priorities

- Automate
  - Use PowerShell and REST API
  - Migrate off of CSVs to SQL
- Trending
- Reframe around GQM methodology
  - Formalize and document

Broader Metrics Plan

- Vendor support – pushing our vendors for APIs to data
  - Many vendors tout their analytics
    - Speedometers, traffic lights, 3D pie charts, and more
  - Reference: Symbiotic Security talk from BSidesLV, Josh Sokol and Dan Cornell
  - Building our tactical metrics around our controls
- Leverage our control catalog
    - GQM bottom up approach

Where Do We Spend Our Time?

- Data interchange
- Exchanging security data is tough
  - Though we're trying to do this too
- Focusing on building our metrics/analytics, then sharing the tools/techniques

Takeaways

- Spend time up front to frame your question
  - Drink the GQM Kool-Aid™
    - Top down or bottom up
- Visualization is fun, but is tricky to do well
- Automation and repeatability is key
- Time is always in short supply
  - Find a good enough language for your purposes
- Be prepared for the work to digest your findings
- Maintain focus on your objective

“This could be the start of a beautiful program”

Thank you!

Supporting Slides

Twitter: @DSeverski

Questions We're Asking

- Dashboarding mechanisms are uncertain
- Information overload
- Concentrating our data targets on our LOB applications
- What are the boundaries/interconnections between our apps?
  - Where is the information?