



Maximizing the Business Value of Vulnerability Management

Presented to: San Francisco Bay InfraGard
Fall 2009 Quarterly Meeting, November 19, 2009

By:

Joel Scambray, CEO



Kip Boyle, CISO





Agenda

- Project Overview
- Lesson #1: Cultural change
- Lesson #2: Look beyond tools
- Lesson #3: Metrics
- Q&A



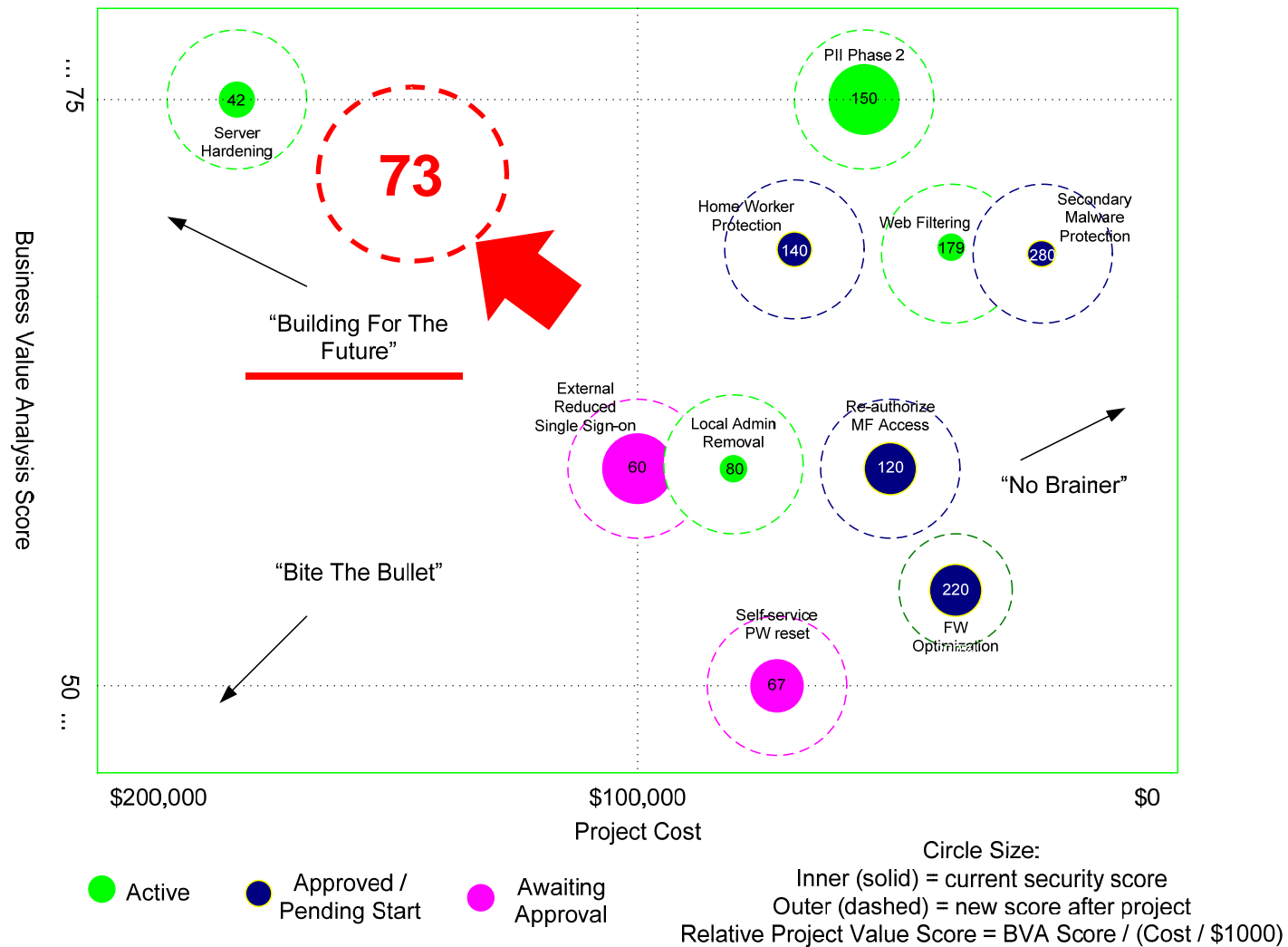
Business Value Proposition 1 of 2

Reliability 08	Improves system availability, security, privacy, by identifying security exposures proactively so that they can be managed to minimize risk.
Return 10	Reduces costs due to productivity loss because of system downtime. Reduces the likelihood of costs associated with data breach notification.
Risk 40	Strengthens confidence in the overall security of systems and/or processes (<i>trustworthiness</i>). Reduces the risk of unauthorized disclosure, and reduces the risk of regulatory action (<i>confidentiality</i>). Ensures better coverage of the risk landscape. Systems will have a higher probability of a reliable controls leading to fewer vulnerabilities.
Indemnity 15	Implements corporate policies (<i>internal compliance requirement</i>). Brings us into closer alignment with industry standards (<i>due care</i>). Reduces the risk of fraud and potential data loss. Reduces the risk of regulatory action if an audit reports a lack of security controls being defined and not in place.
73	Expected Benefits Score (out of a maximum possible score of 100)

Recommended Project Prioritization: A



Business Value Proposition 2 of 2





Project Overview

Phase	Schedule	Cost
Scanner Deployment	Nov 2007 – May 2008	\$200,000
Project 1		
Assessment	June – September 2008	\$85,000
Design & Refinement		
Initial Deployment		
Project 2		
Implementation & Integration	October – March 2009	\$230,000
Metrics & Reporting		
Automation		
Backlog Cleanup	January – March 2009	\$65,000
Total:	~1.5 years	\$580,000

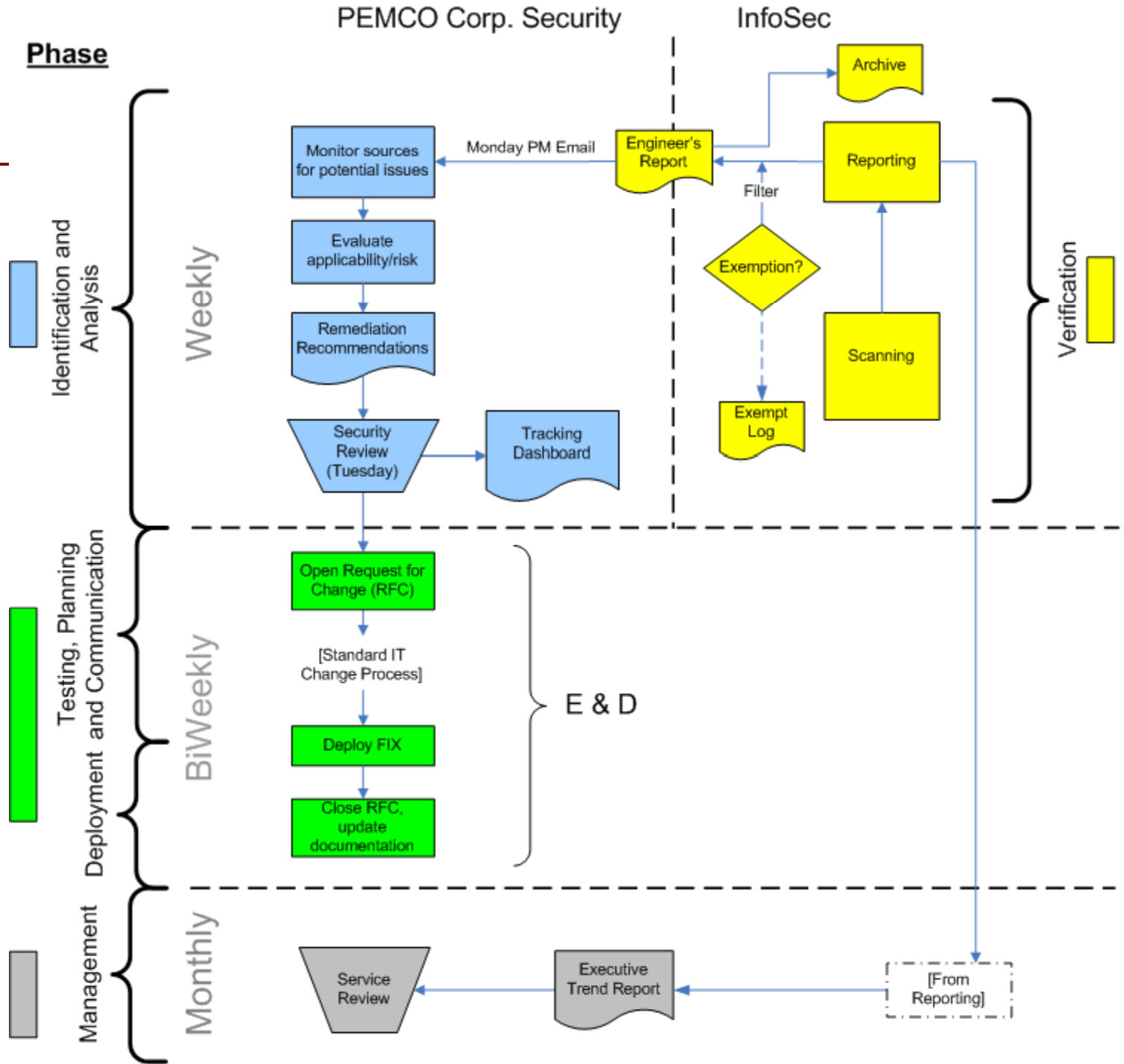


Desired Outcomes

- Holistic process design
- Clarified roles & responsibilities
- Improved tool efficiency
- SOPs and operational readiness for each part of the process
- Reporting automation
- Governance committee and regular meetings
- High-level metrics



Before & After

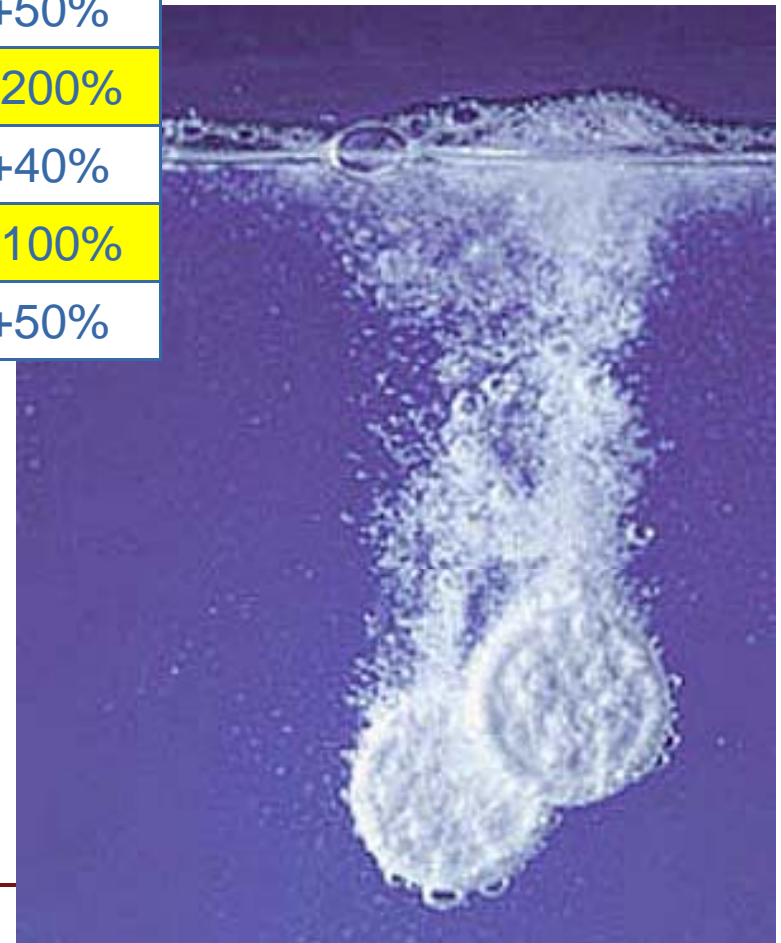




Lesson #1: Cultural change

Interactions	Before	After	Total
Email	2	3	+50%
Documentation	1	3	+200%
Processes	5	7	+40%
Recurring Meetings	1	2	+100%
Decision Points	2	3	+50%

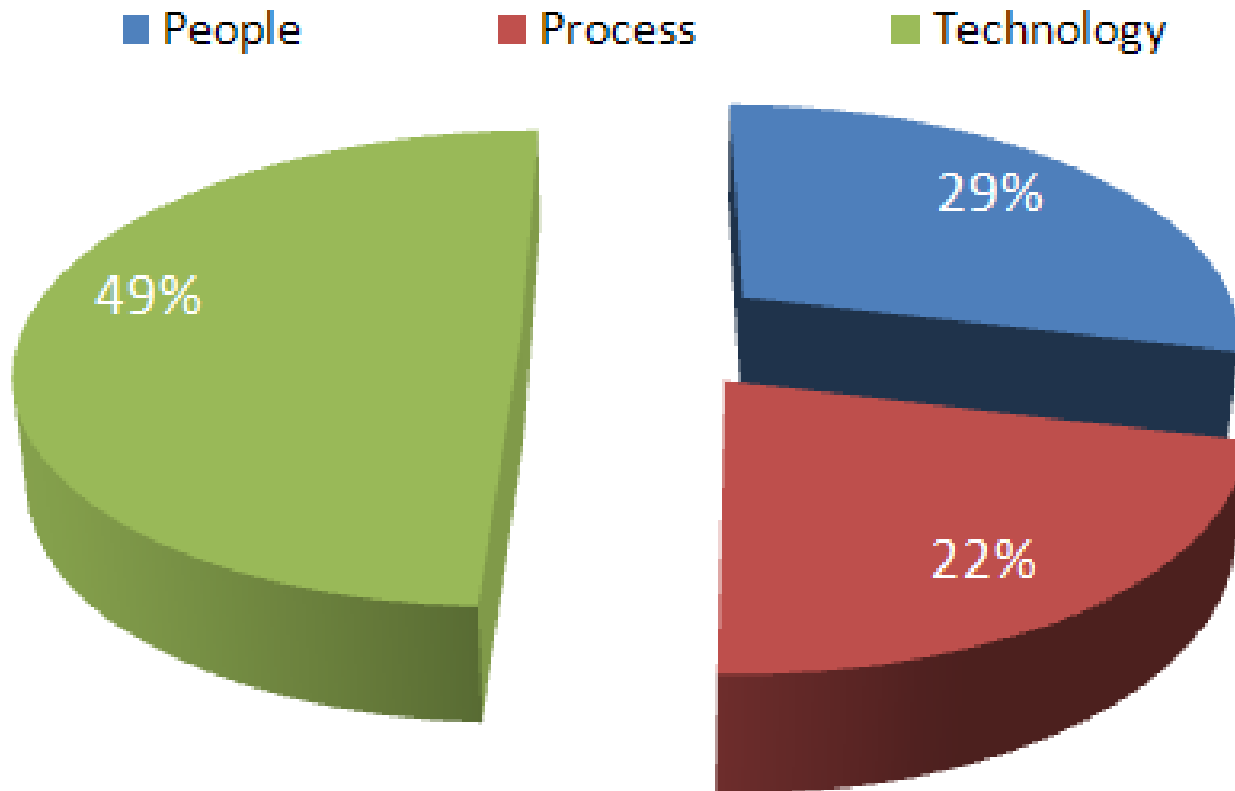
Catalysis





Lesson #2: Look beyond tools

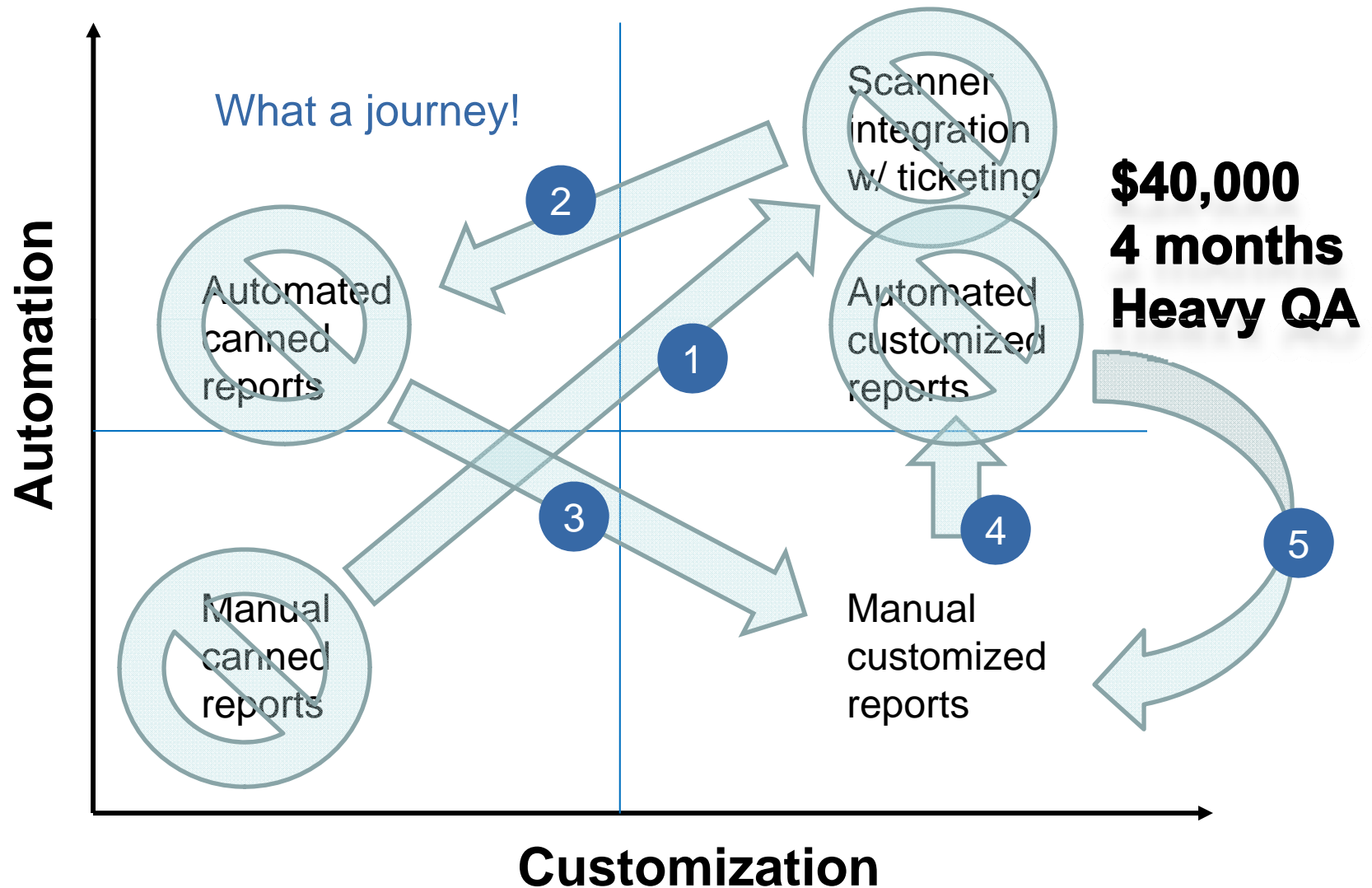
Cost Summary



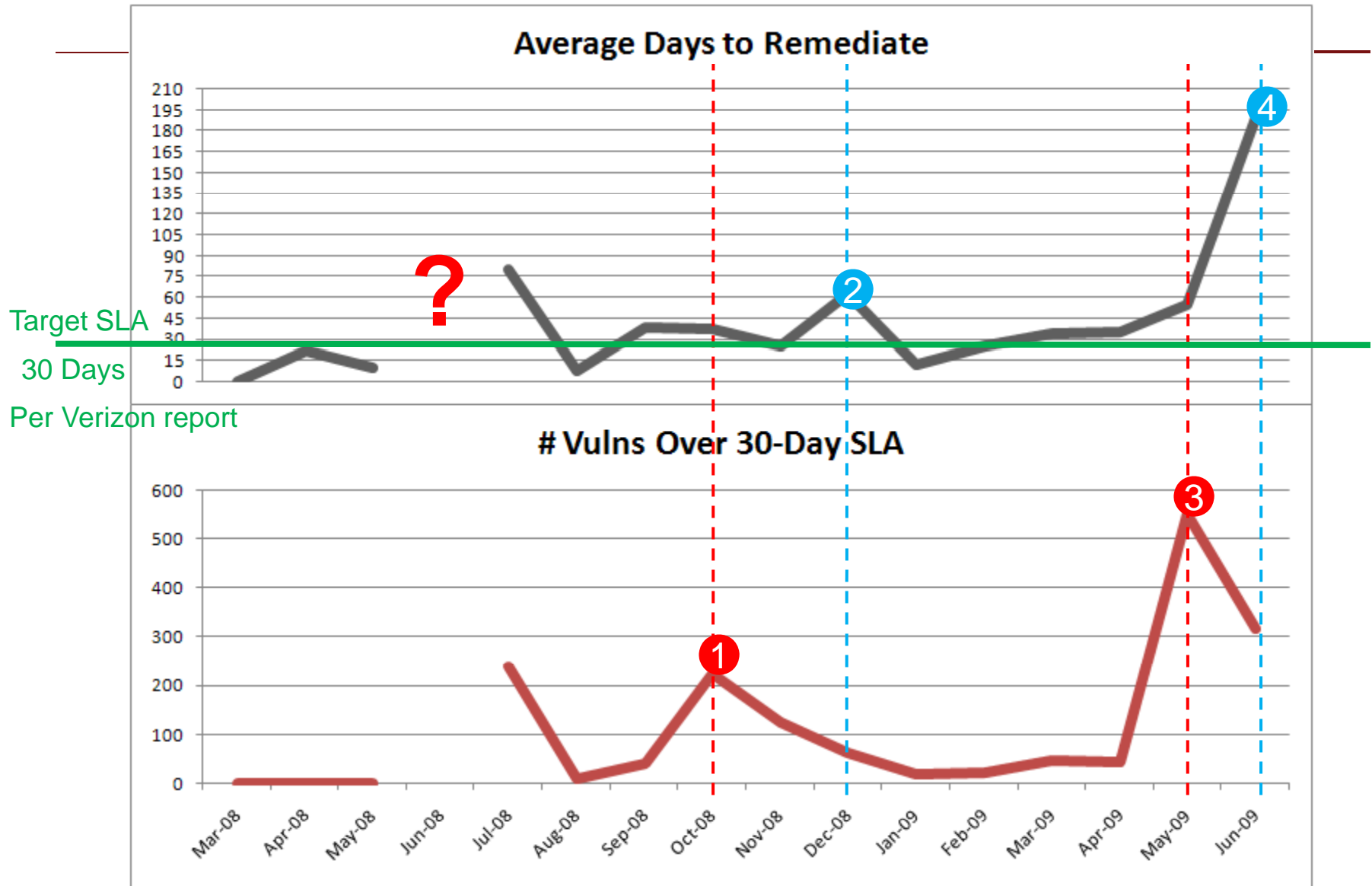
Approx. 1,500 systems (1,300 desktop, 300 server/network),
~ \$580K total



Customized management reporting

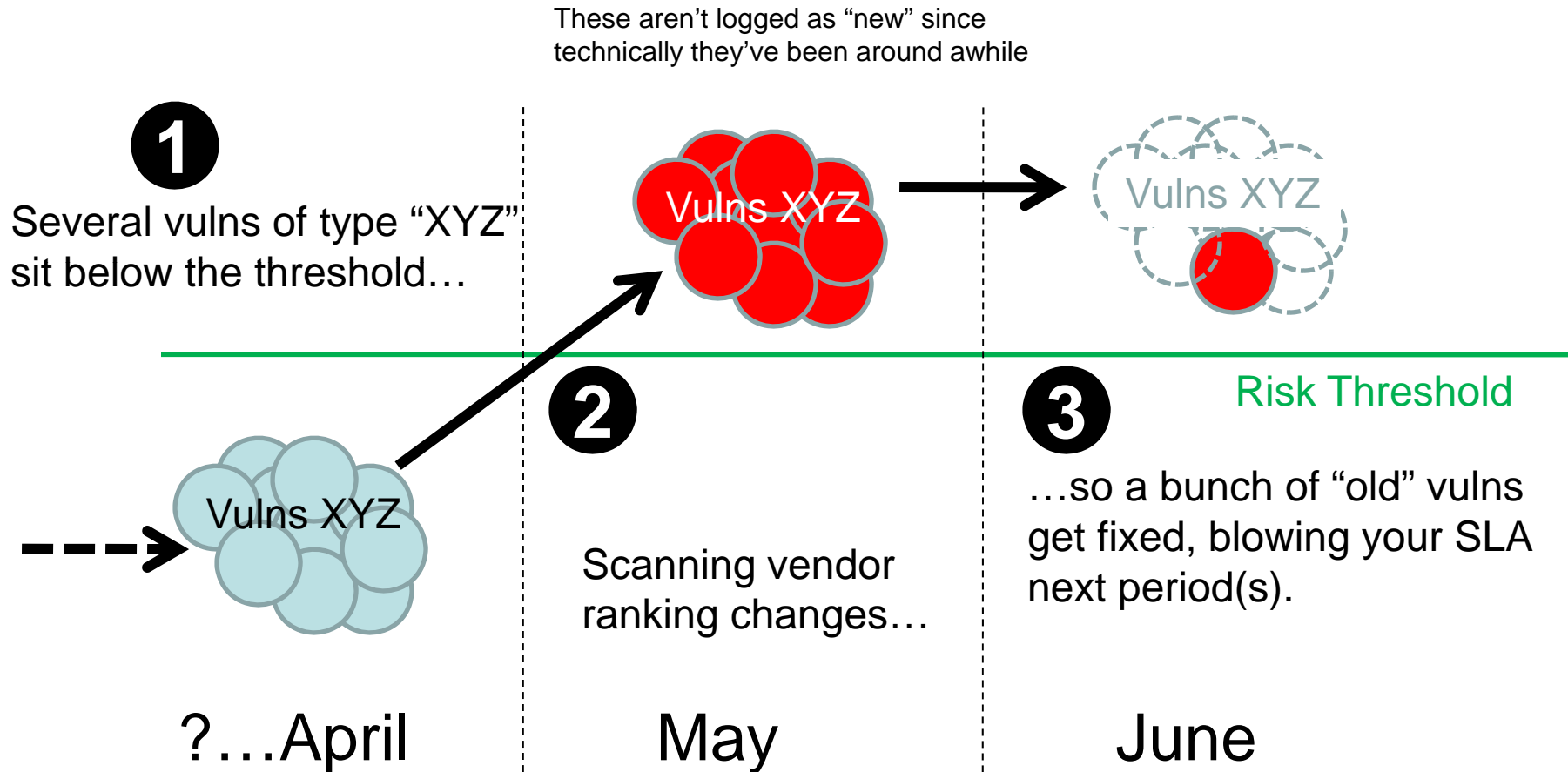


Lesson #3: Metrics





The Vulnerability Submarine





Metrics: A Tough Nut To Crack!

Desired Outcome	Expected	Actual
30-day SLA cultural acceptance	Hard	Easy
Measure & govern to SLA	Easy	Hard
Stakeholders' perception of data reliability	Good	Bad
Richness of scanner reporting	3D pivot	Flat, static
Custom scanner reporting	Hard	Impossible

Wrapping Up

We studied for an algebra test, but somehow sat for a calculus exam...





Questions?

Joel Scambray, CEO



moreinfo_at_consciere.com

Kip Boyle, CISO

