Metricon 3.5

Caroline Wong, CISSP, Global Information Security Chief of Staff

20 April 2009

eBay

eBay Snapshot

Founded in September 1995, eBay is a global online marketplace where practically anyone can trade practically anything.

- Presence in **39 Markets**
- **86.3 million** active members worldwide
- More than **50,000 categories**
- **113 million** concurrent listings
- **1 billion** page views per day
- **$2,000** worth of goods traded every second

eBay: The Green Difference

Used laptop sales on eBay in 2007

A reduction of more than **69,000 tons of greenhouse gases**

Equivalent of saving **467 acres of forest**

On eBay:

A pair of shoes sells every **3 seconds**

A cell phone sells every **7 seconds**

A car sells every **minute**

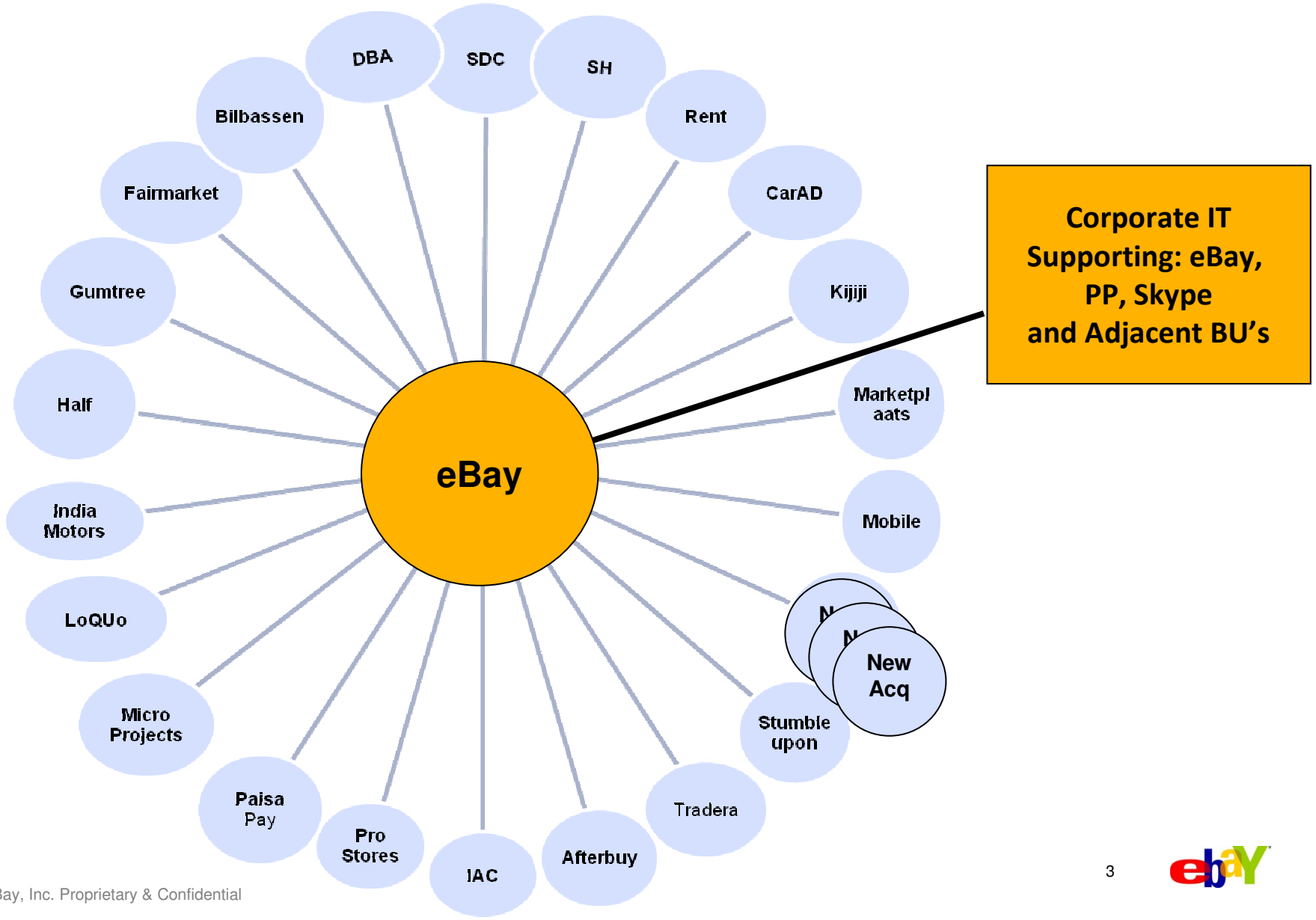
Q4 Auction Highlight

$38,192.12

For limited-edition Presidential Kids Cabbage Patch Dolls

($19,000 for Sarah Palin doll)

Global Information Security – Scope of Responsibility



Agenda

- Review last year's strategy
- Case Study - Web application security vulnerability tracking
- Lessons Learned - Fix process before automation
- Looking ahead - Minimum Security Baselines

Agenda

- Review last year's strategy
- Case Study - Web application security vulnerability tracking
- Lessons Learned - Fix process before automation
- Looking ahead - Minimum Security Baselines

Metrics Vision

Track and assess metrics to ensure that we are effectively meeting the security needs of the corporation, managing risk and assuring ROI.

Program management

- ►Project prioritization & success criteria
- ►Metrics drive roadmap, resourcing, budget
- ►Data informs GIS mgmt for decision-making
- ►Feedback loop for continuous improvement

Drive organizational change

- ►Appropriate ownership & accountability for security issues
- ►VP's receive regular status reports showing KRI's and KPI's that are relevant to their BU
- ►VP's understand reports and know what they must do for remediation

Benchmarking

- ►Compare eBay MP risk levels to external risk levels

Operational / tactical decision making

- ►Support GIS teams for day to day decision-making

How did it go?

- Identified specific security metrics for tracking

  NOTE: This would have been much faster and easier with the CIS Consensus Metrics Definitions!

- Automating data feeds initially displayed “dirty data”
- Worked with functional teams to review processes, identify issues, recommend solutions, implement fixes

CASE STUDY REVIEW: WEB APPLICATION VULNERABILITY TRACKING

- Obtained clean data and defined goals for the year
- Consolidated overall metrics & process review efforts

Agenda

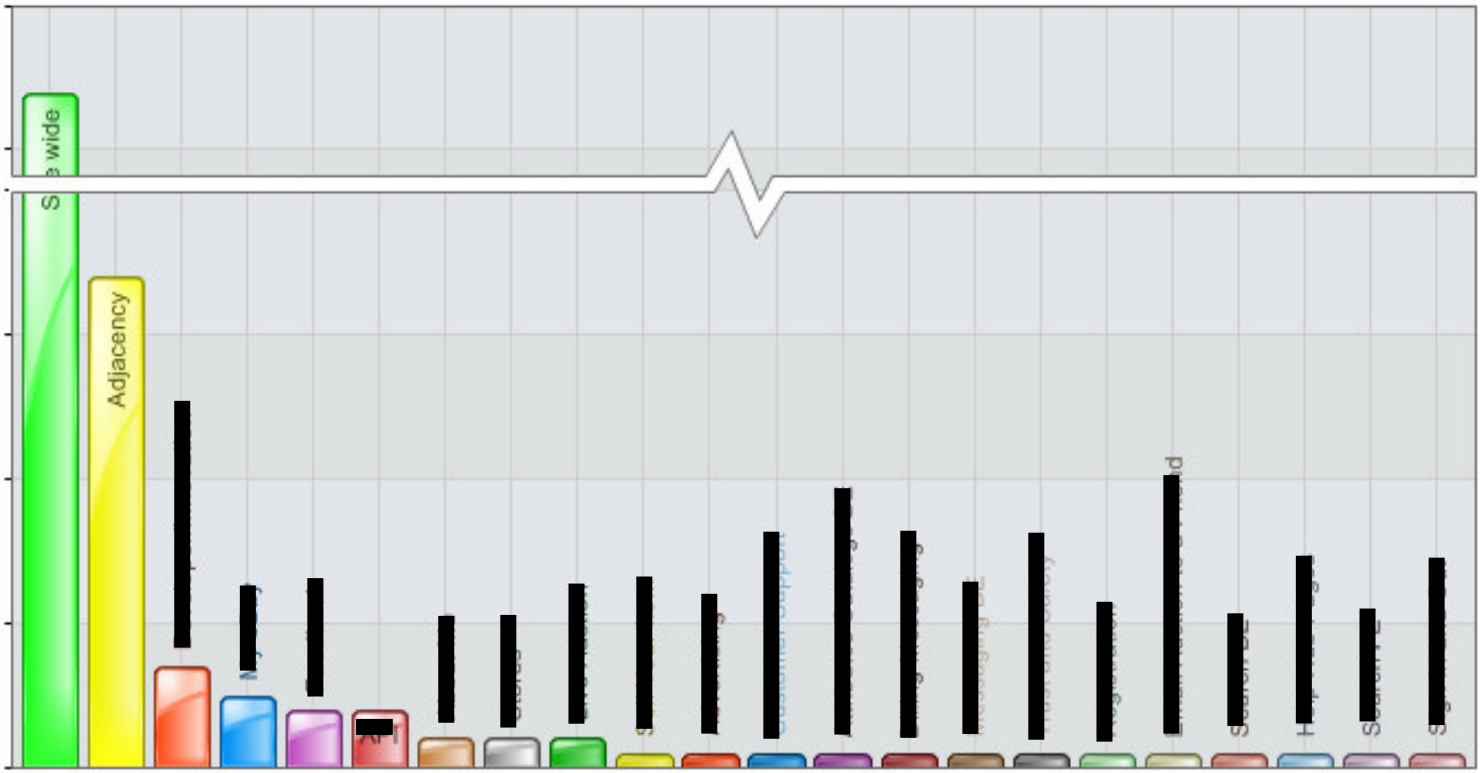
- Review last year's strategy
- Case Study - Web application security vulnerability tracking
- Lessons Learned - Fix process before automation
- Looking ahead - Minimum Security Baselines

Case Study – Web application vulnerability tracking

- Source data - Automated feed from Remedy ticketing system
- Goal - Track & report number of web application vulnerabilities for
  - eBay Functions
  - Individual Business Units

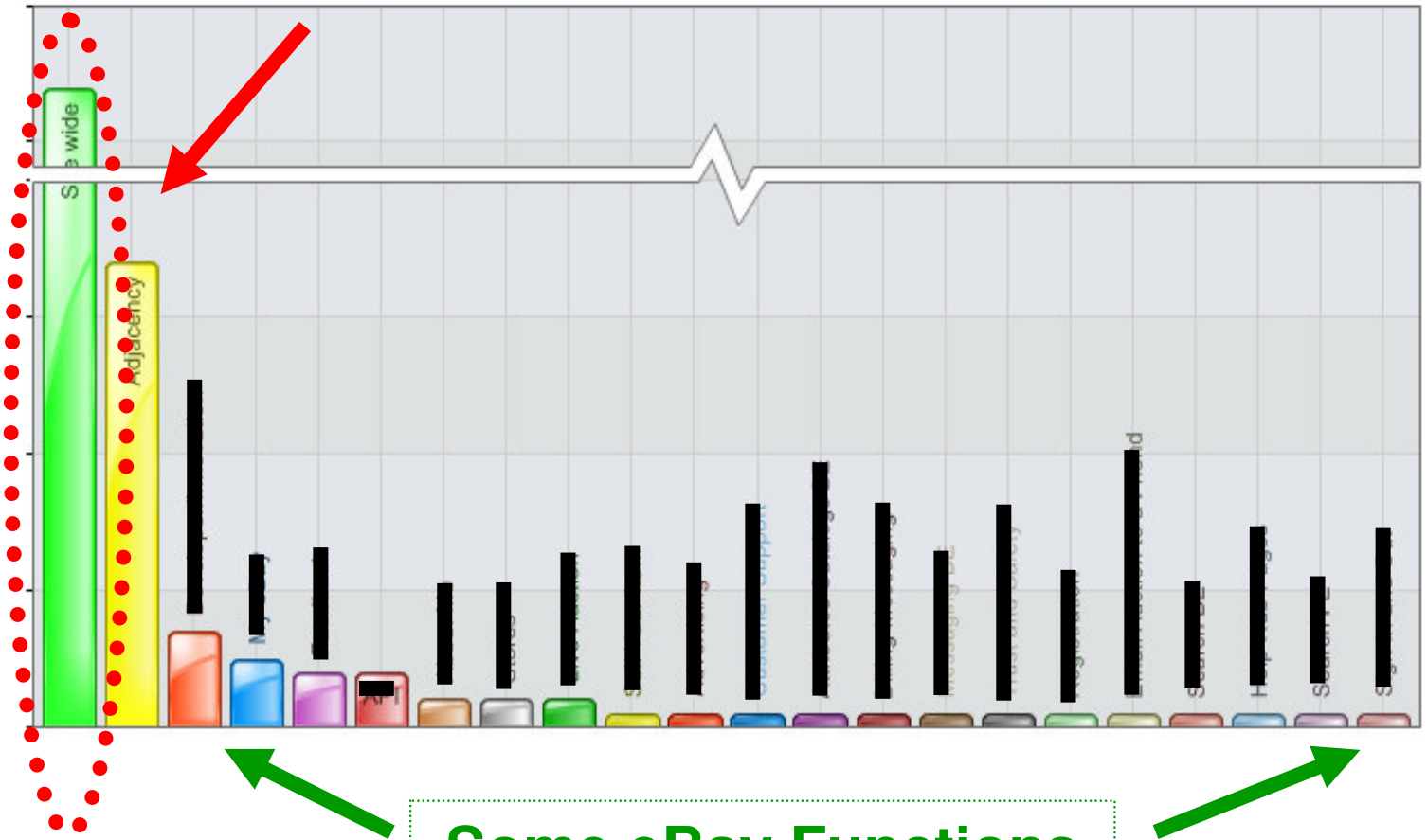
Case Study - Initial reporting with “dirty data”

What’s wrong with this picture?



Case Study - Initial reporting with “dirty data”

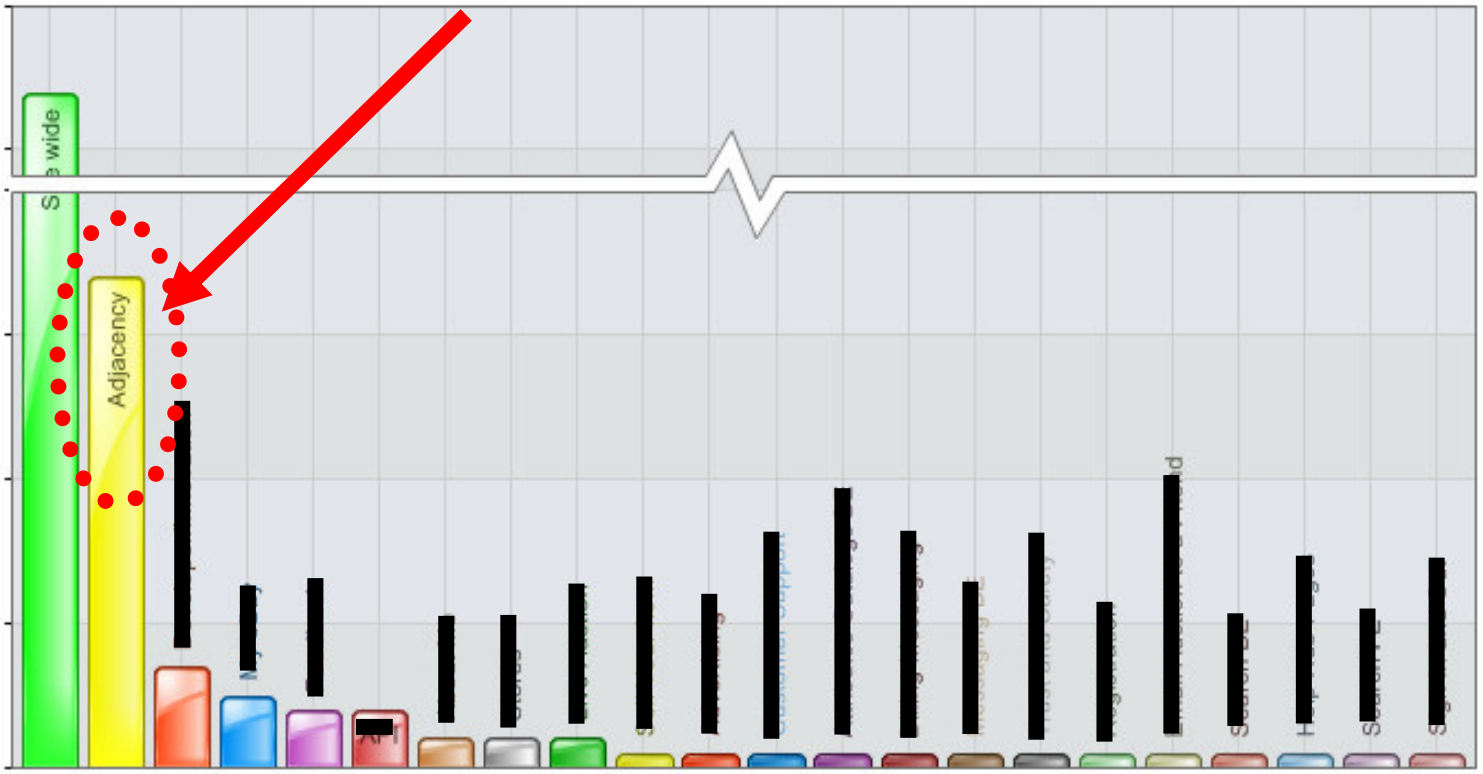
Site wide? Need reporting for each Individual eBay Function



Some eBay Functions

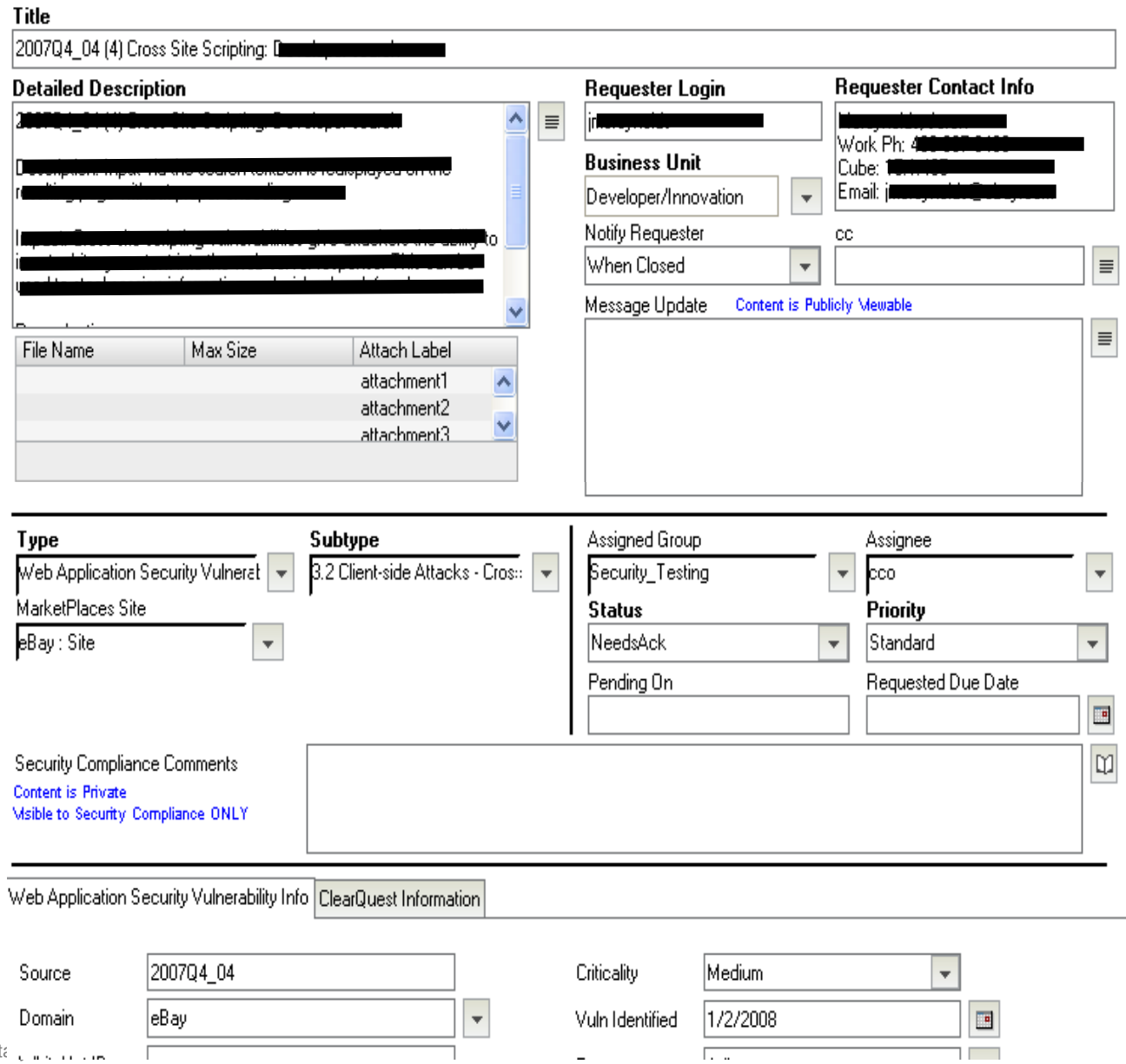
Case Study - Initial reporting with “dirty data”

Adjacency? Need reporting for each Individual BU

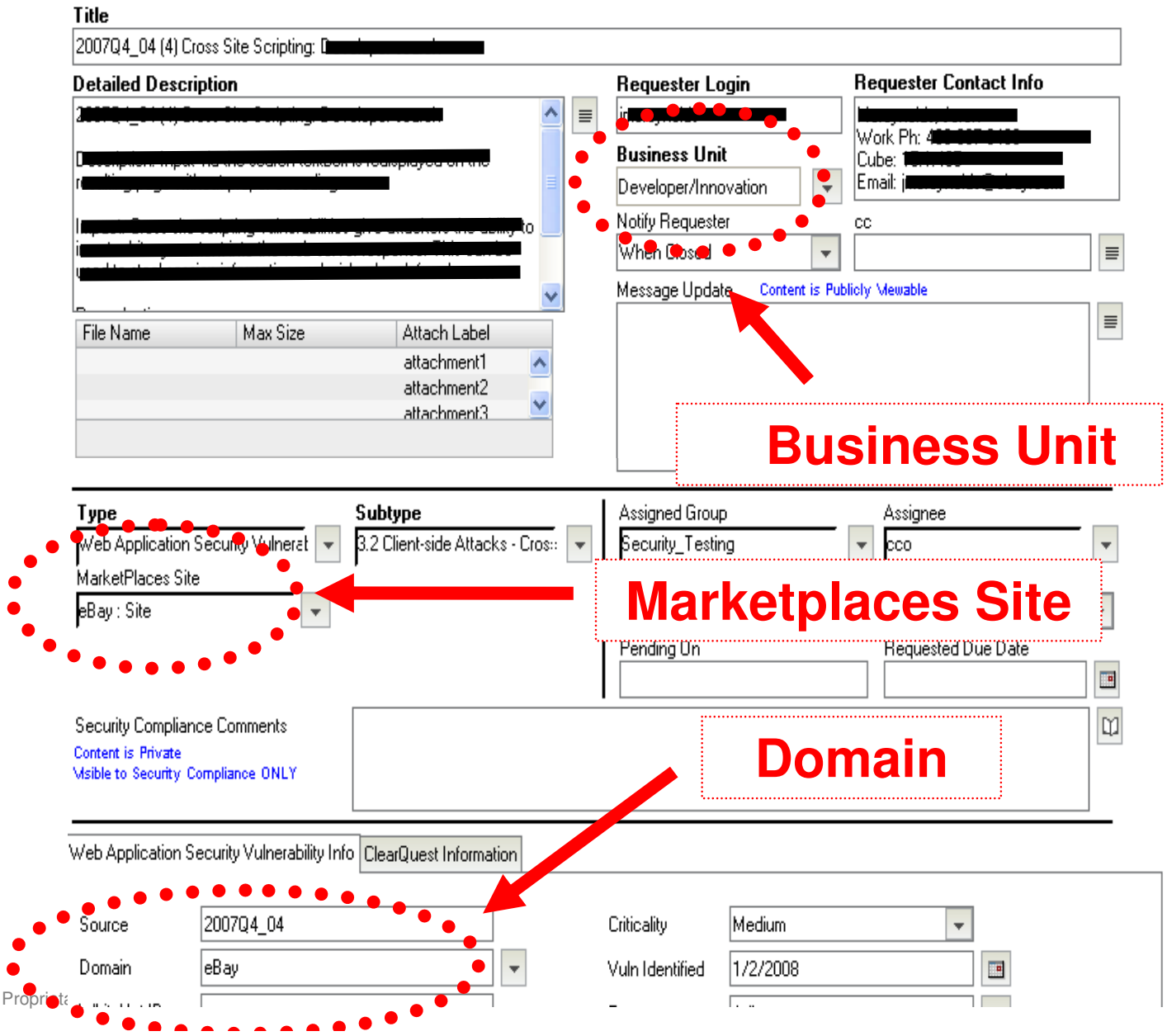


Some eBay Functions

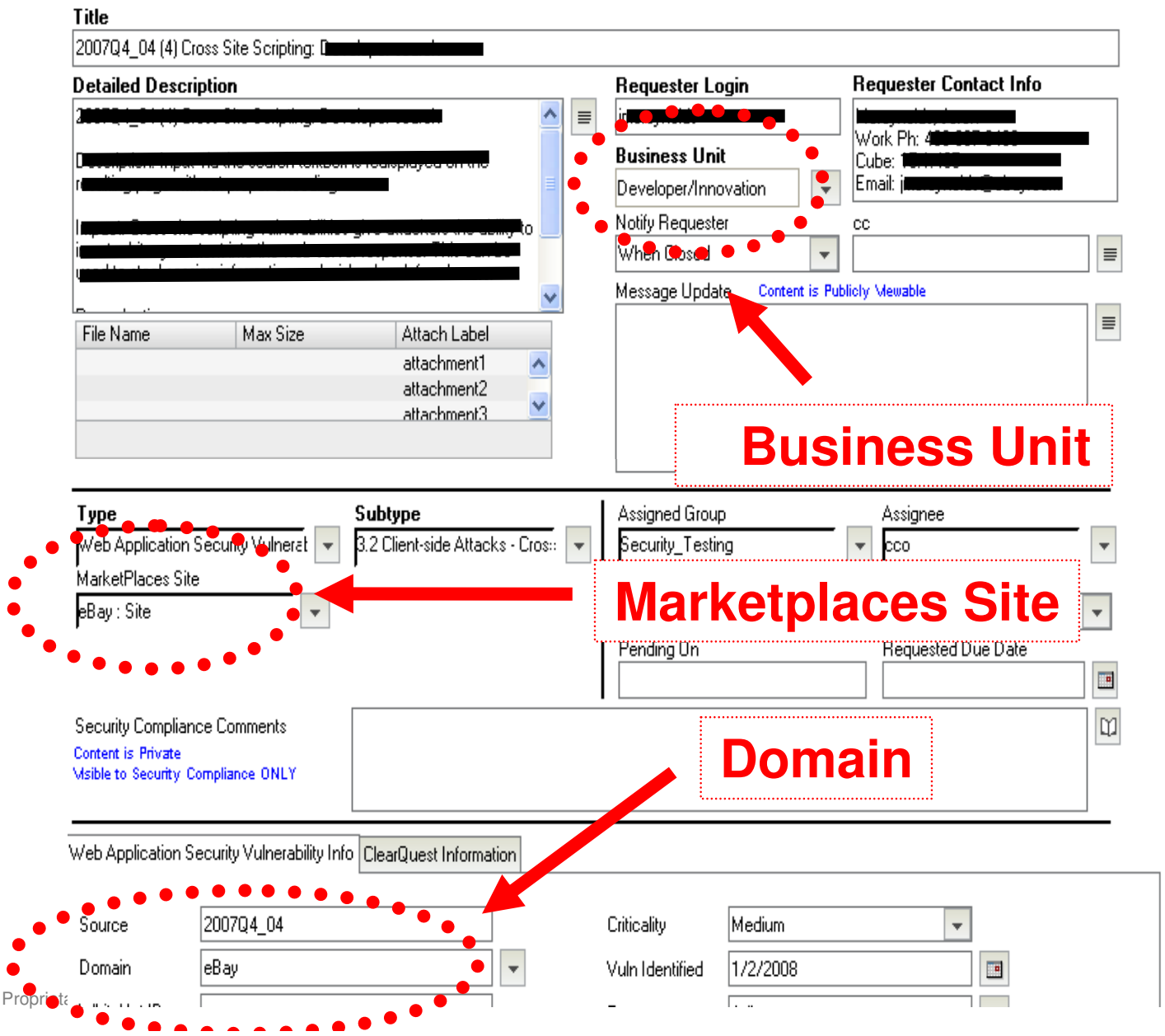
Case Study - Examine data feed source tickets



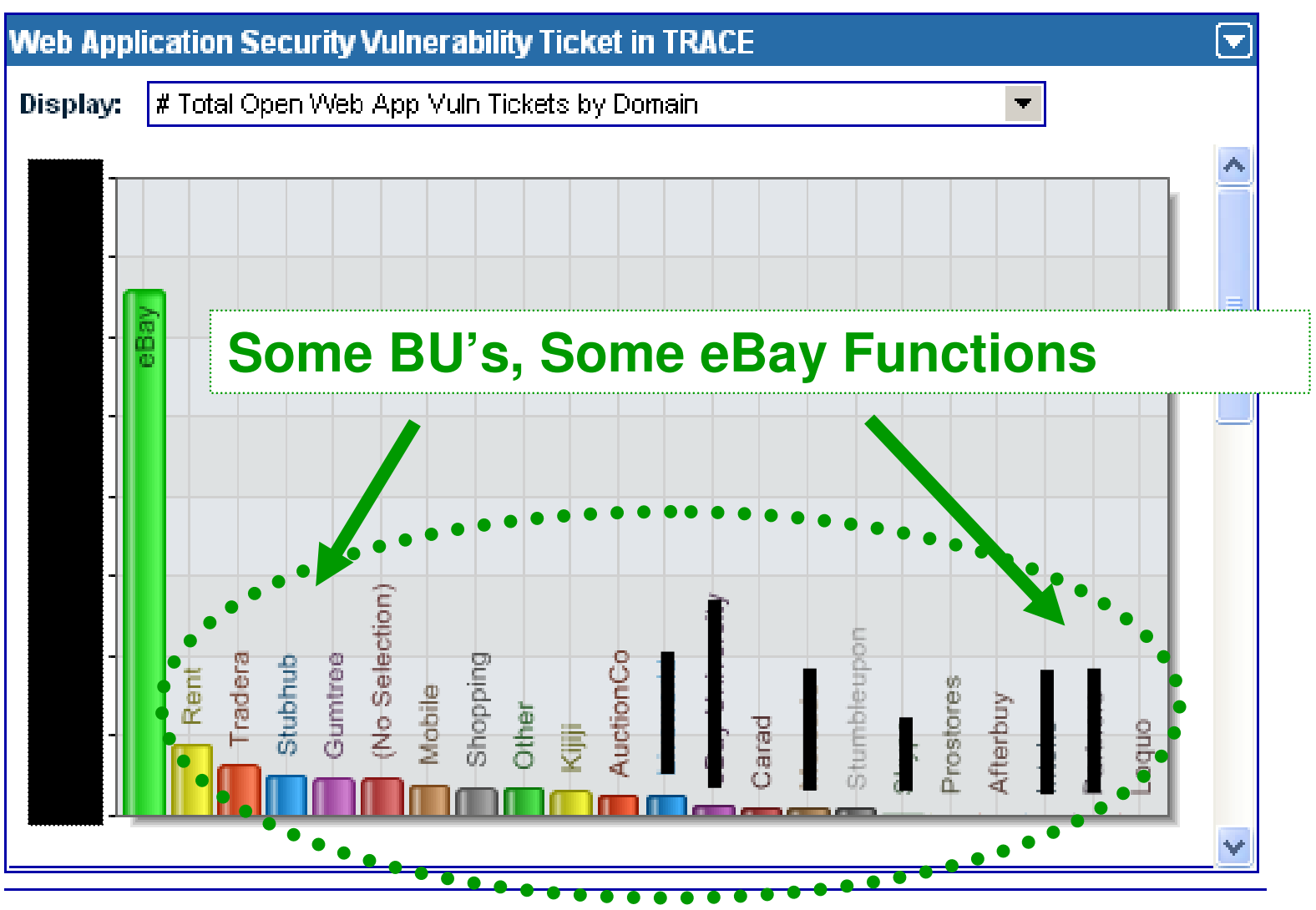
Case Study - Remediation ticket has redundant fields



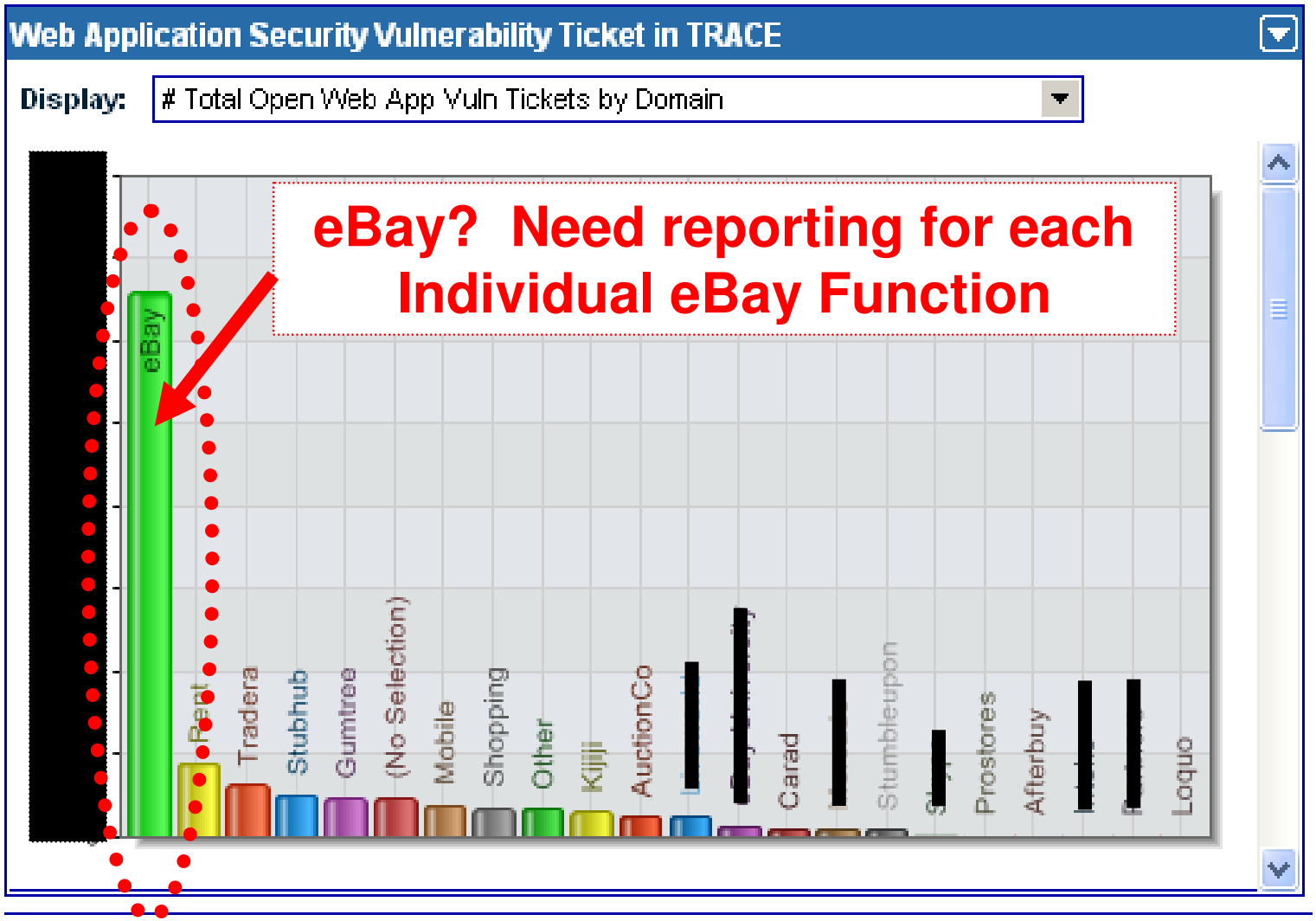
Case Study - What is the right field to report on?



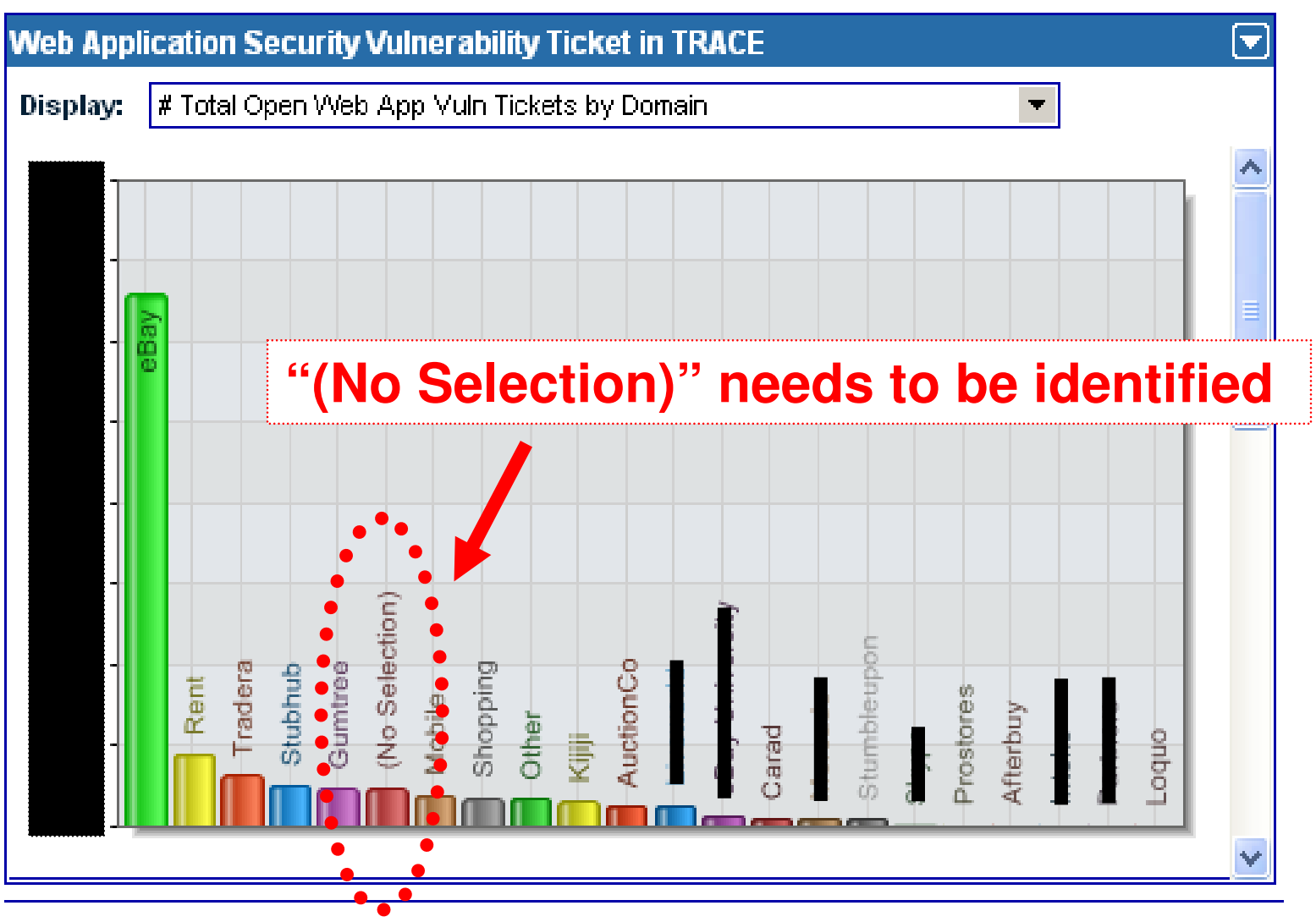
Case Study - Report by Domain?



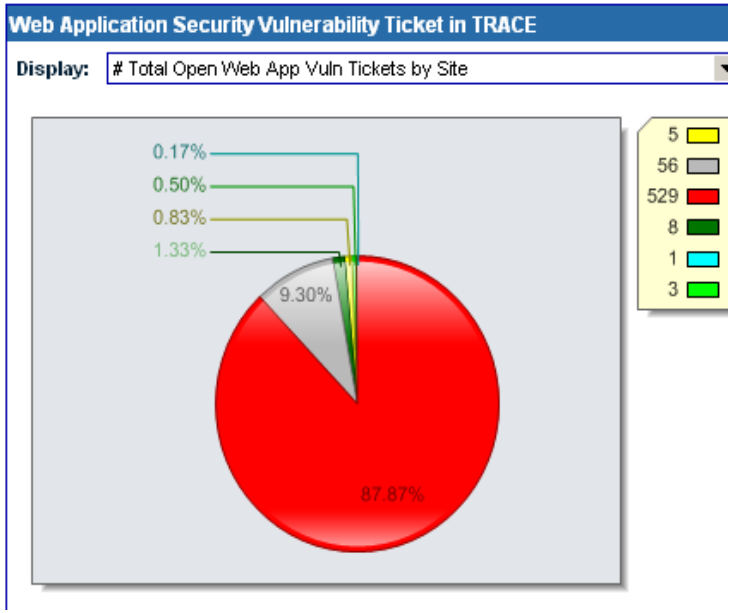
Case Study - Report by Domain? No



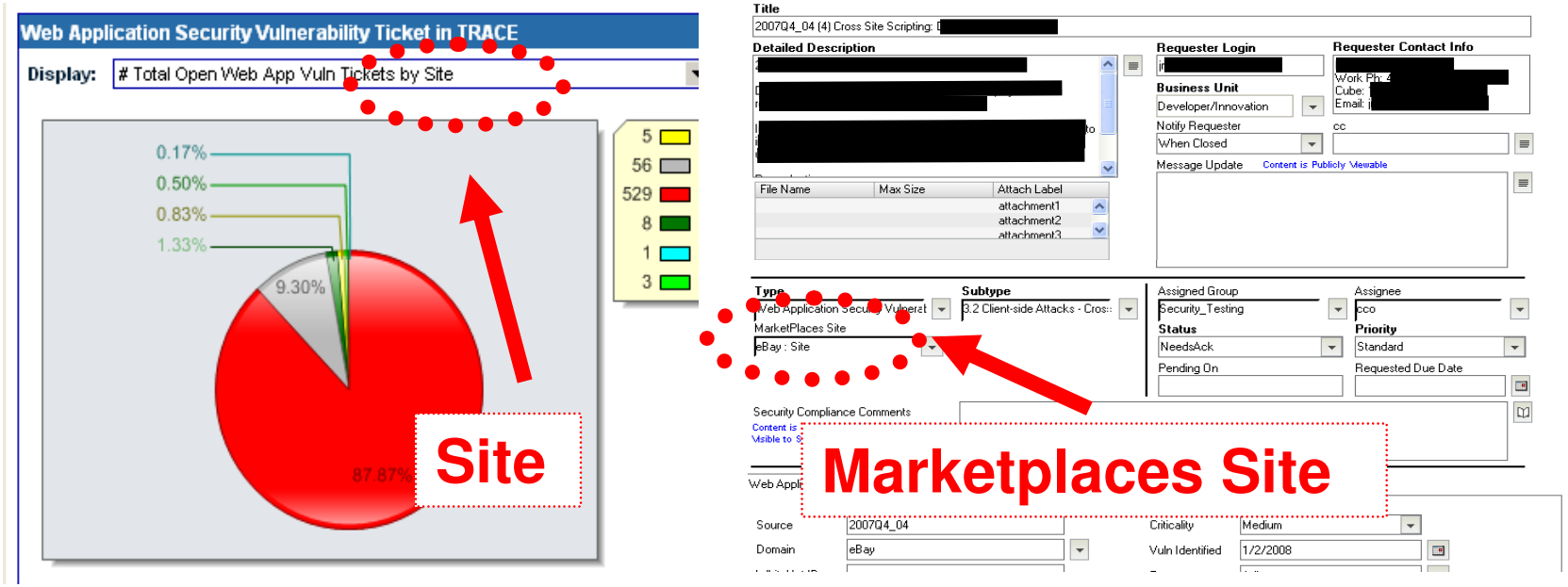
Case Study - Report by Domain? No



Case Study - Report by Site?

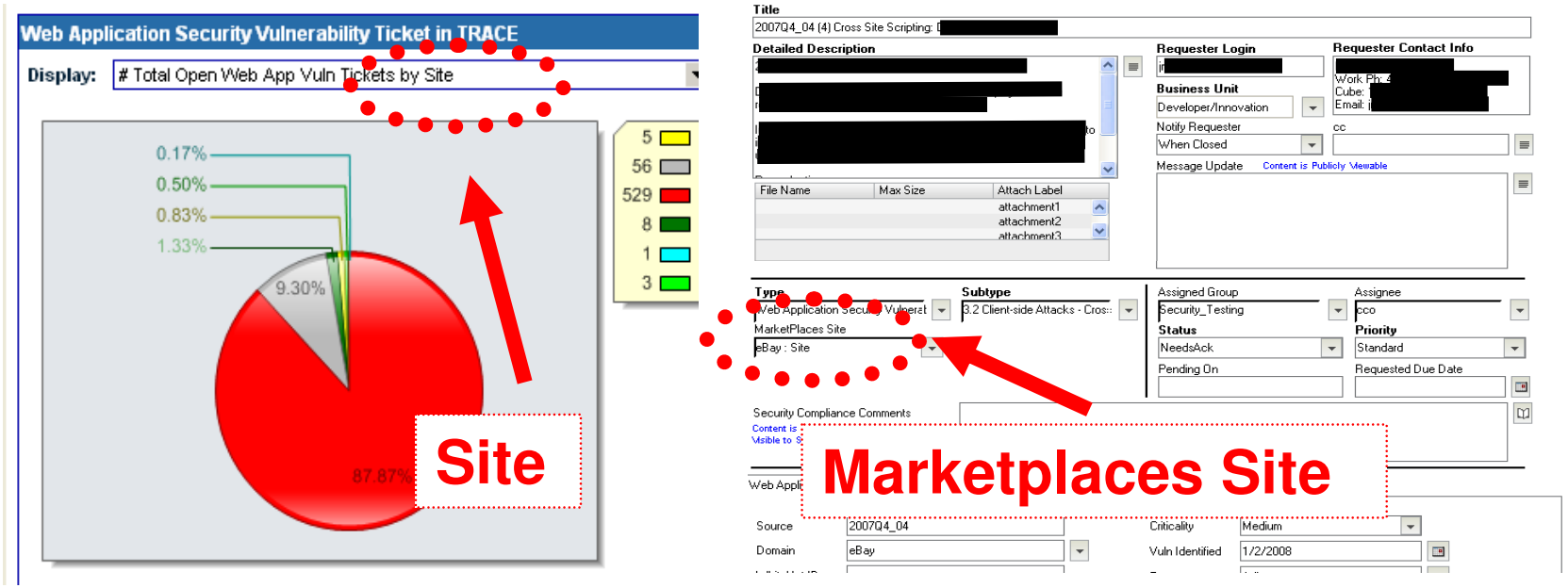


Case Study - Report by Site? No



Compare reporting with source data

Case Study - Report by Site? No

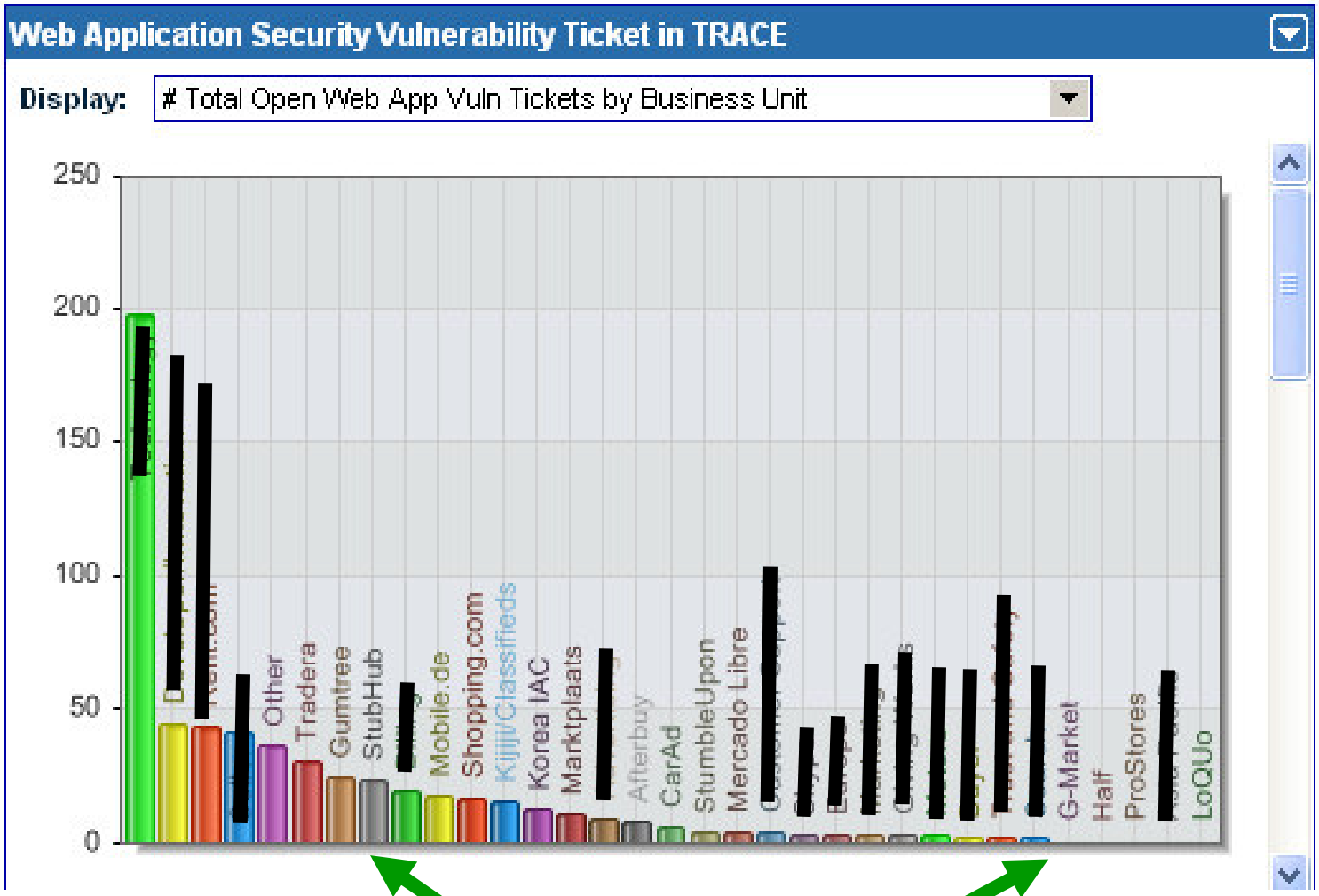


"Site" does not equal "Marketplaces Site"

Reporting reflects an old ticketing structure

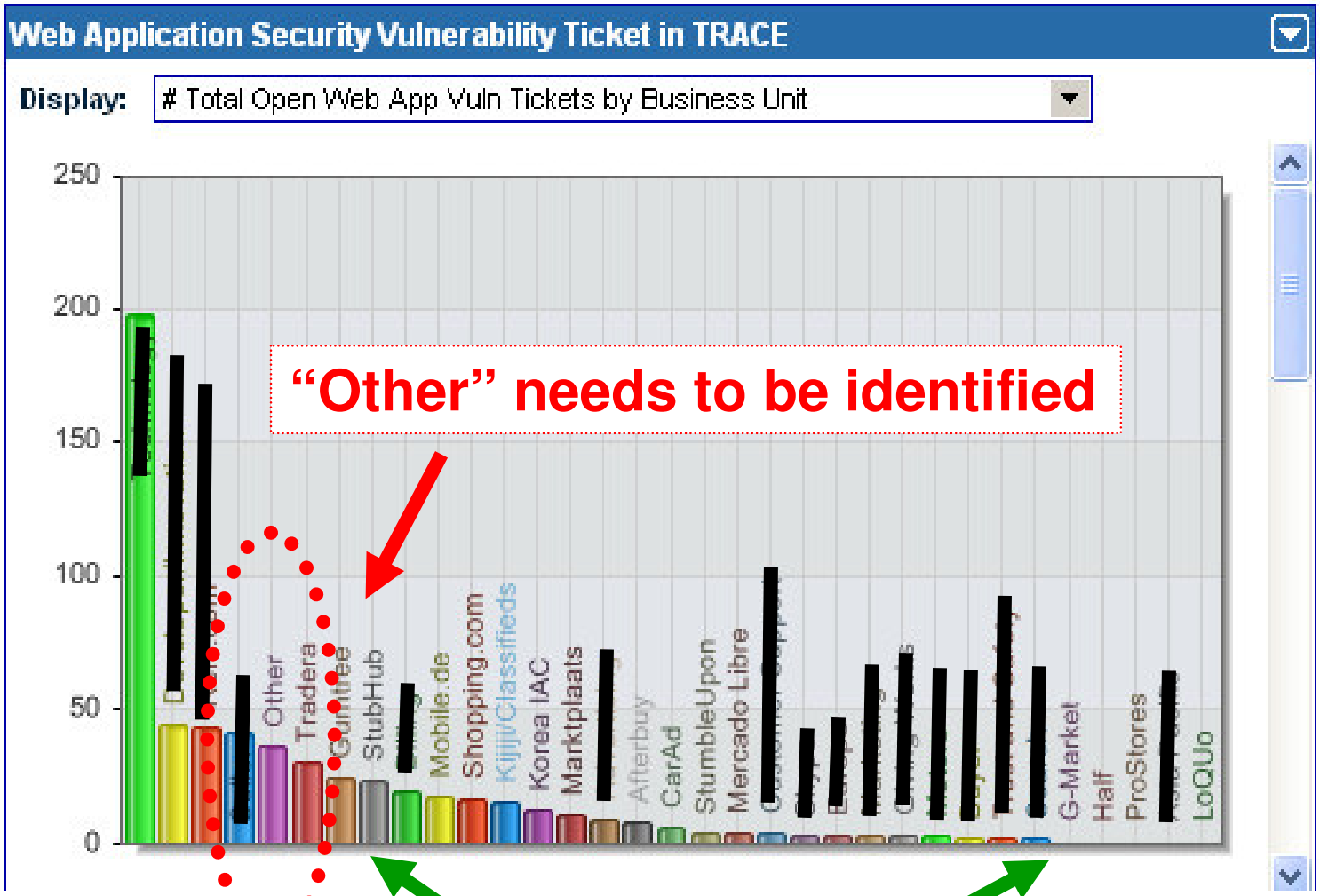
<u>Lesson</u>: When source feed changes, reporting must change also

Case Study - Report by Business Unit?



eBay Functions and BU's

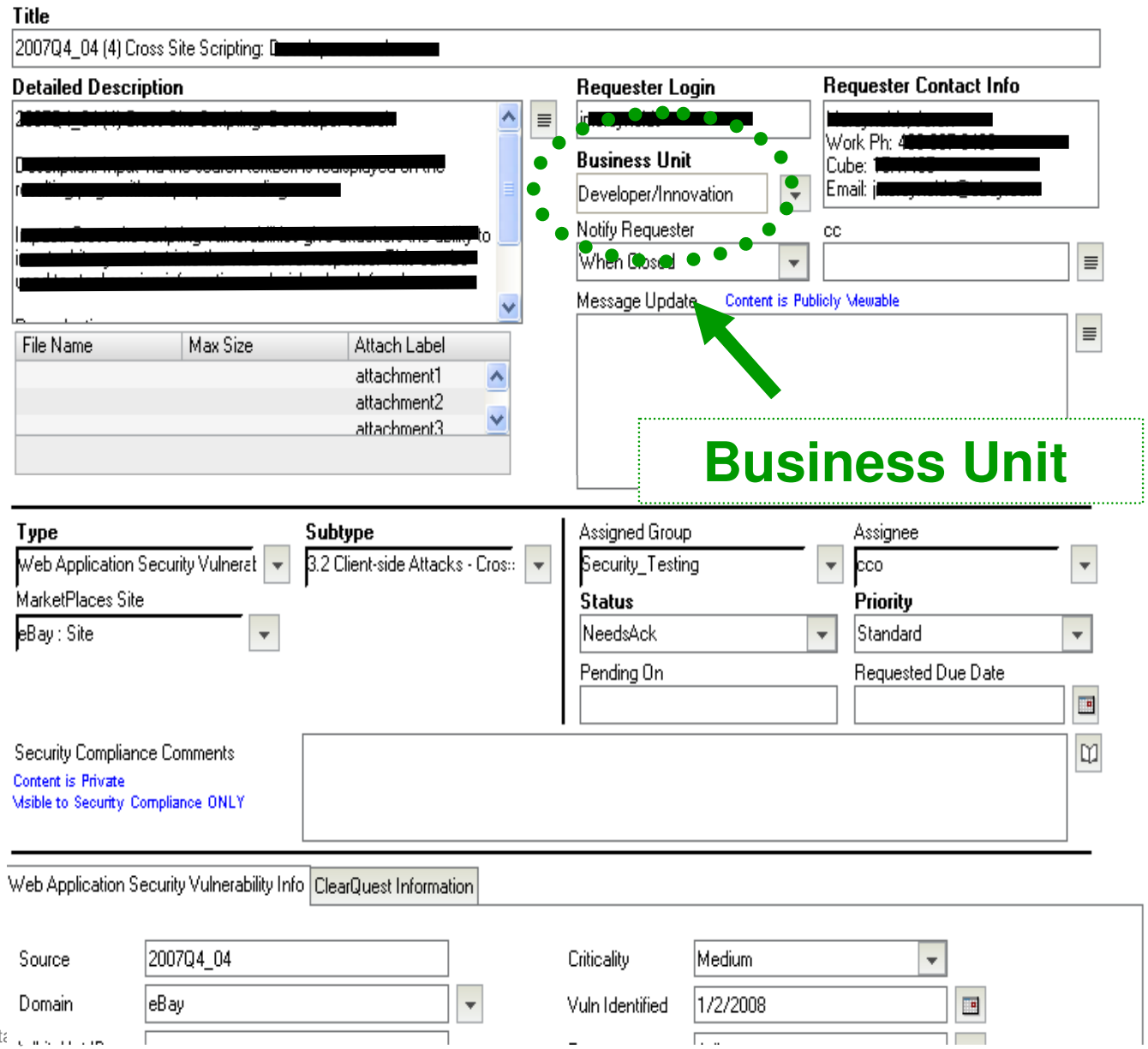
Case Study - Report by Business Unit? Almost!



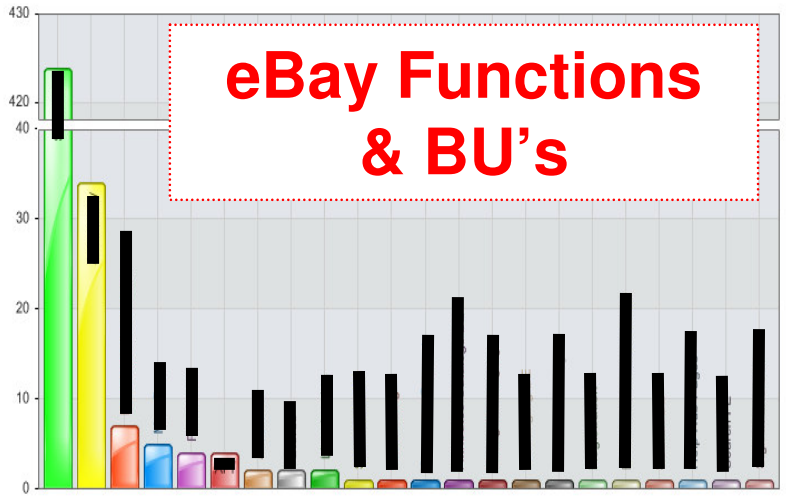
Case Study - Talk to the team who owns the process

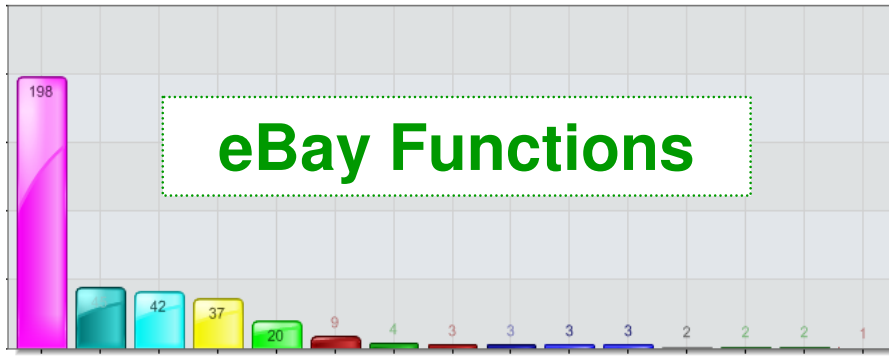
- Explain reporting issues
- Understand the process flow
- Identify process & ticketing issues
- Identify fixes
- Agree to a timeline

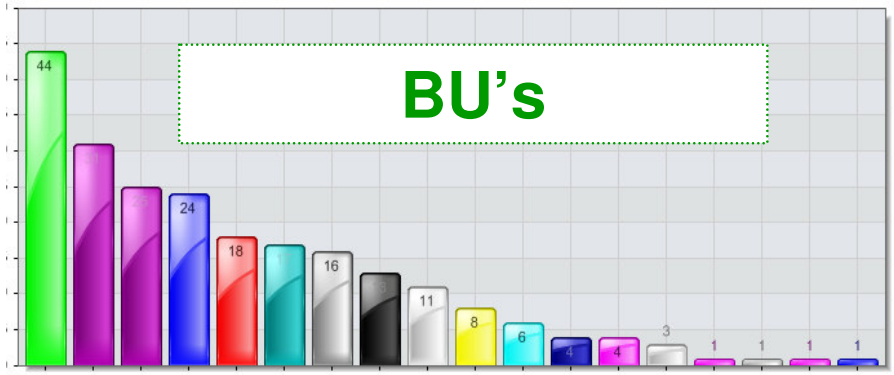
Case Study - Choose ONE field for consistent reporting



Case Study - Implement filters for eBay Functions and BU's

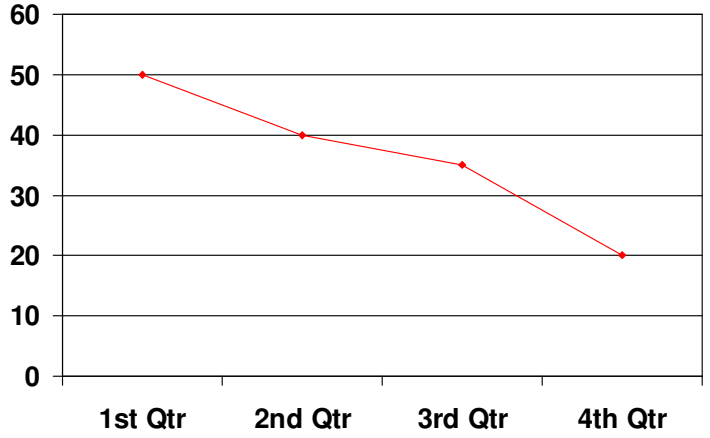






Case Study - Metrics Goals & Timelines

- Key Performance Indicators
- What's the goal for this metric?
- Set timelines for achievement
- Publish monthly reports



	Baseline	Current	Q1	Q2	Q3	Q4
			5% reduc	10% reduc	15% reduc	20% reduc
Vulns	400	450	380	360	340	320
Lines of code (M)	10	10	10	10	10	10
Vulns / MLOC	40	45	38	36	34	32

Note: These numbers do not reflect real data.

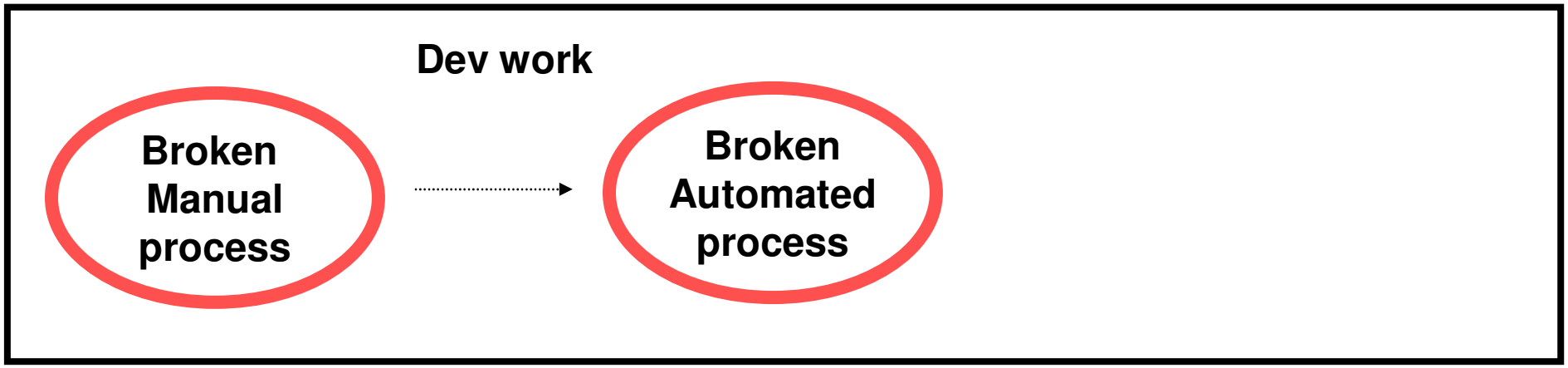
Agenda

- Review last year's strategy
- Case Study - Web application security vulnerability tracking
- Lessons Learned - Fix process before automation
- Looking ahead - Minimum Security Baselines

Lessons Learned: Fix the process first, then automate

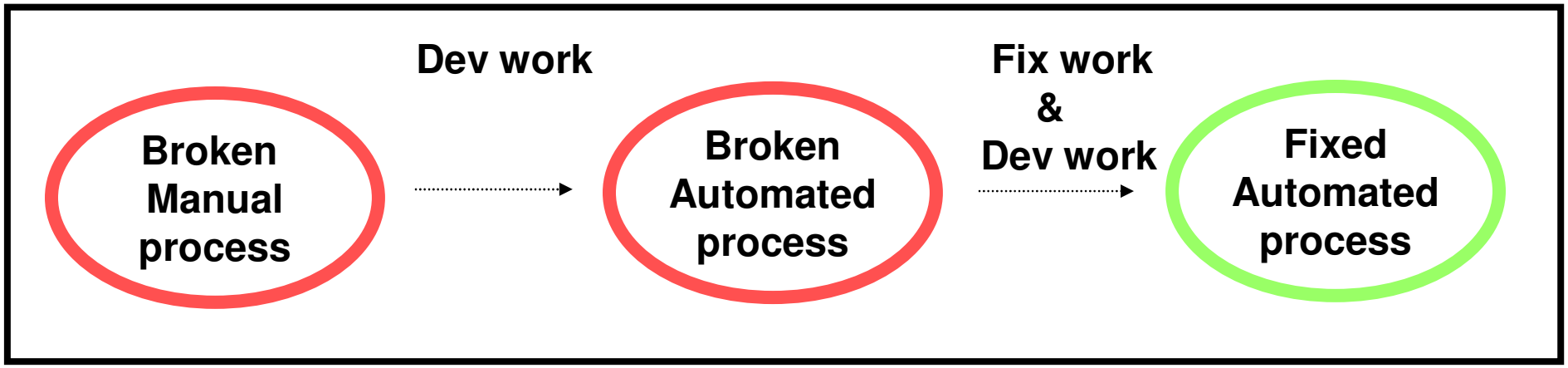
Time

Lessons Learned: Fix the process first, then automate



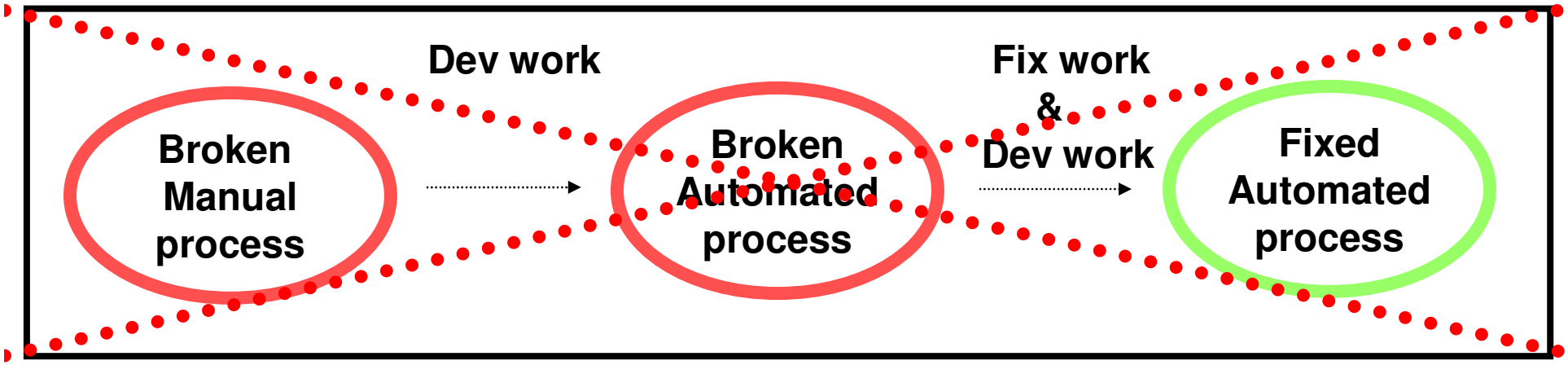
Time

Lessons Learned: Fix the process first, then automate



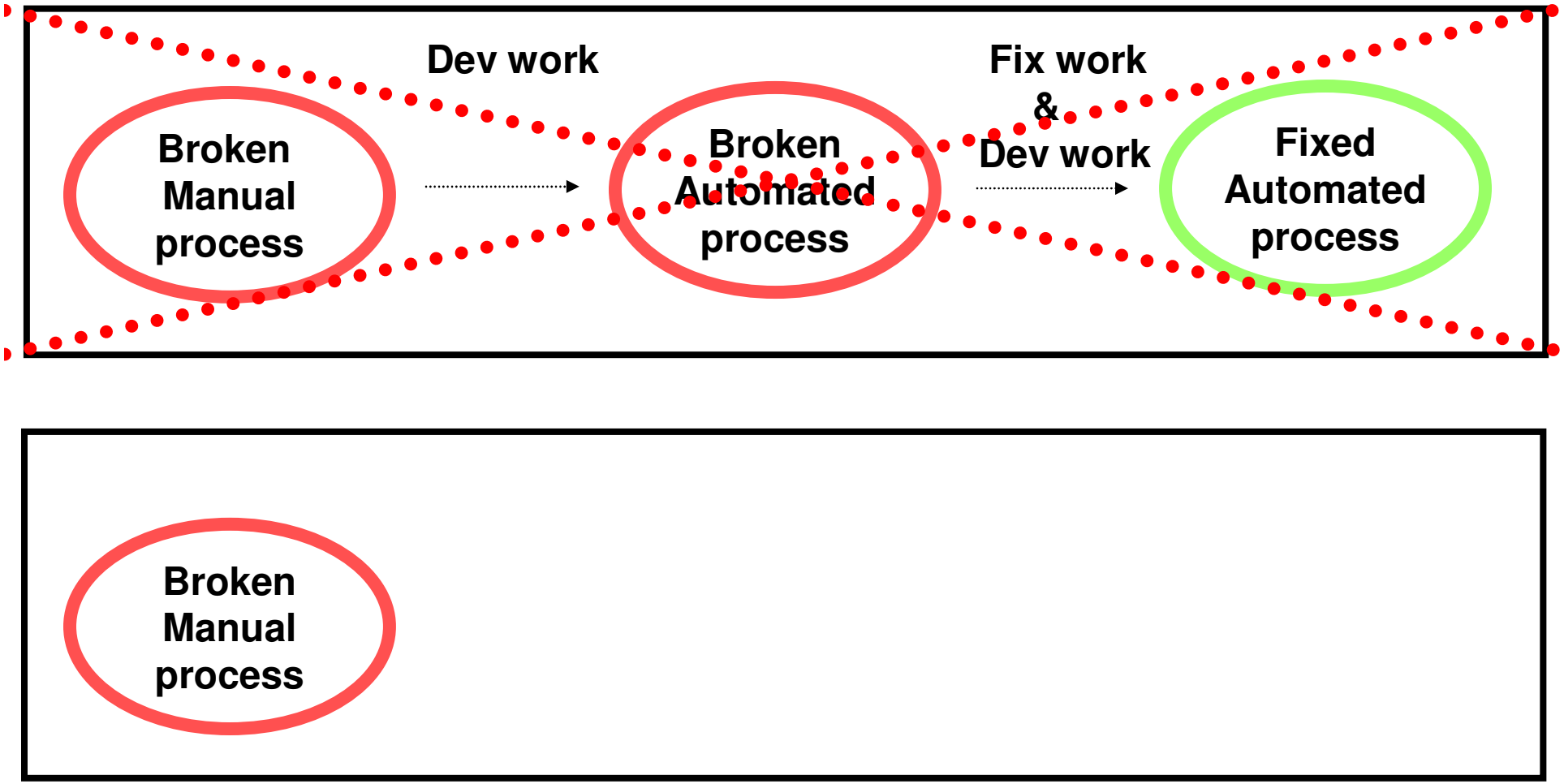
Time

Lessons Learned: Fix the process first, then automate

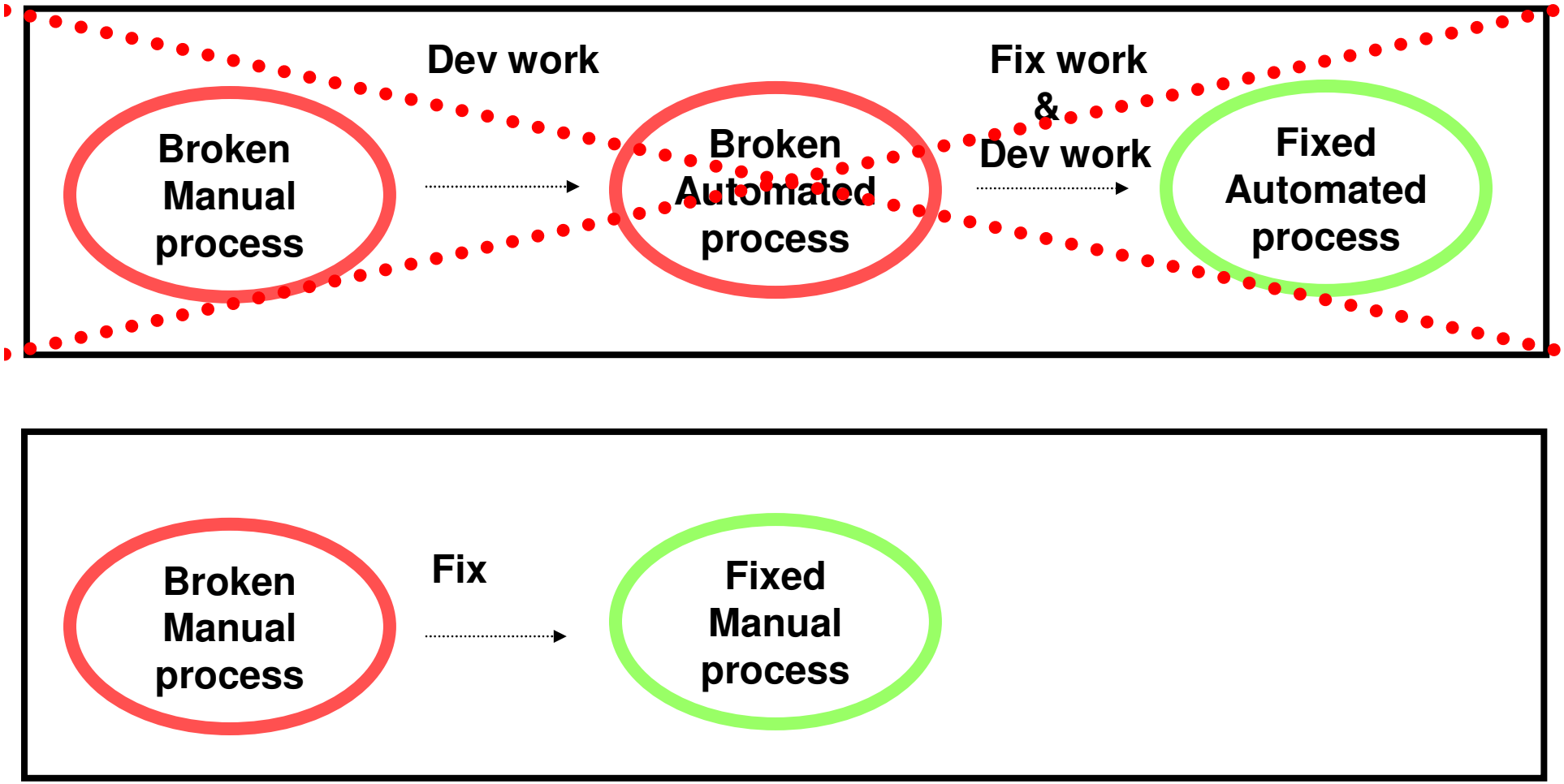


Time

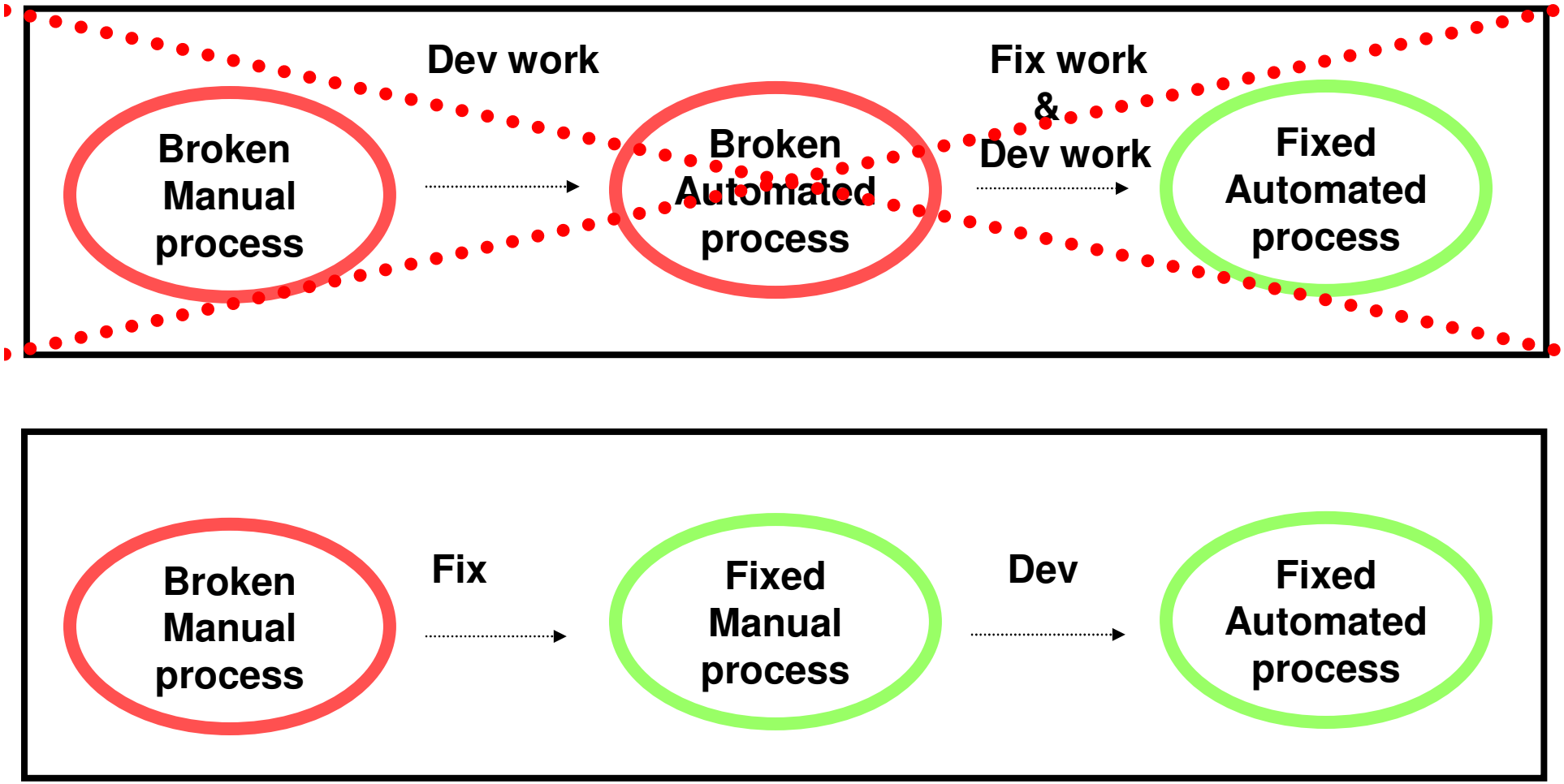
Lessons Learned: Fix the process first, then automate



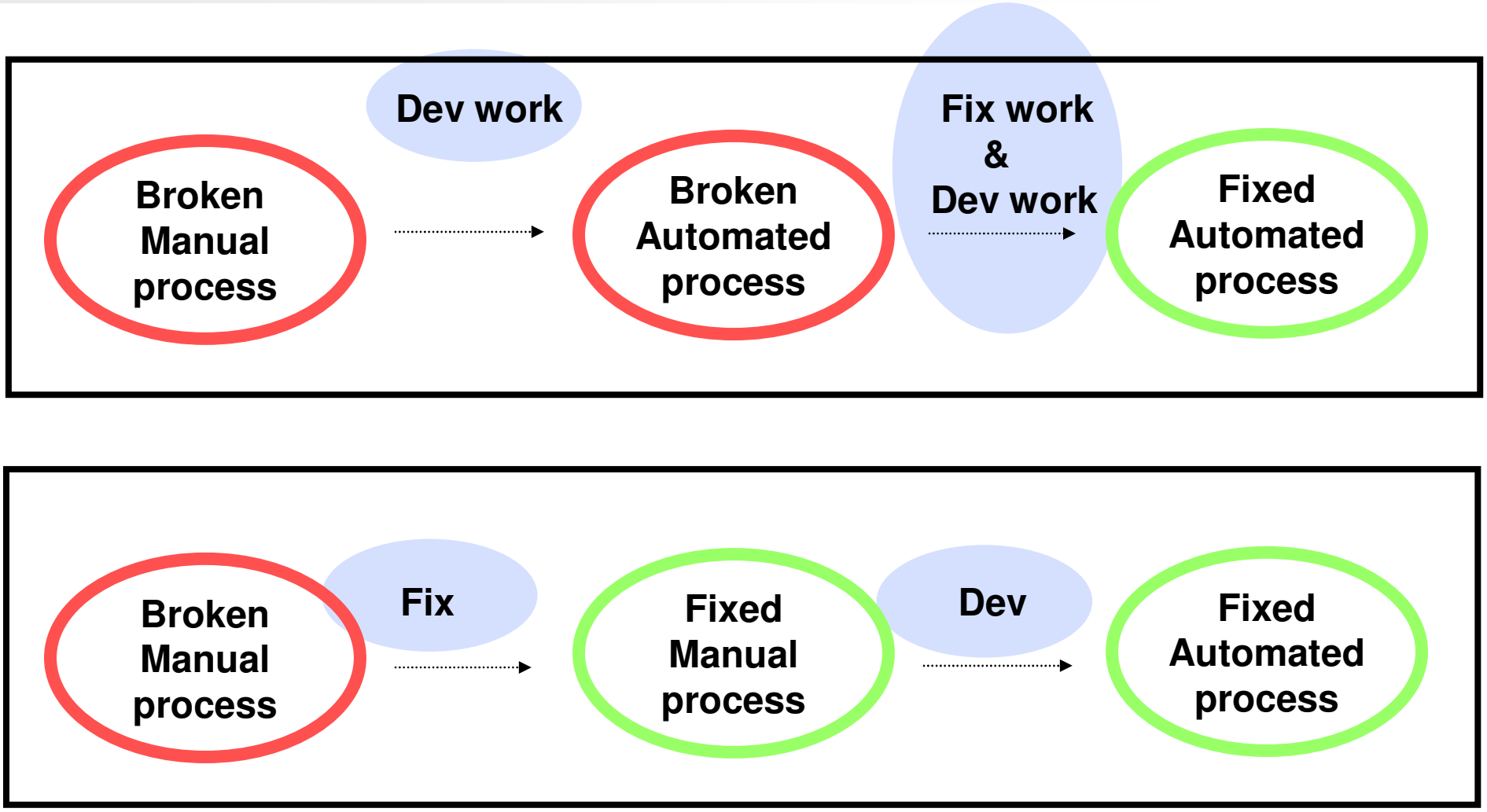
Lessons Learned: Fix the process first, then automate



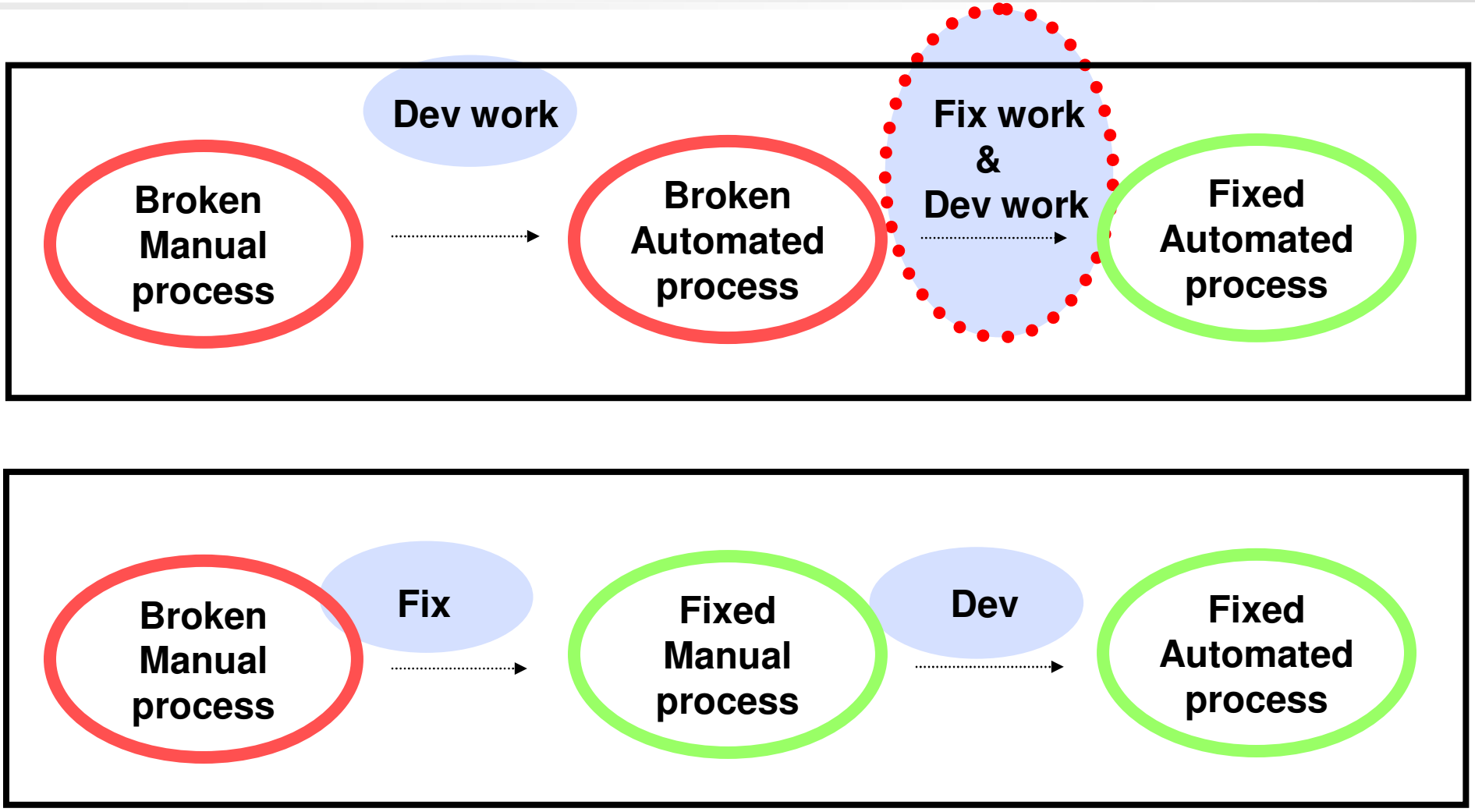
Lessons Learned: Fix the process first, then automate



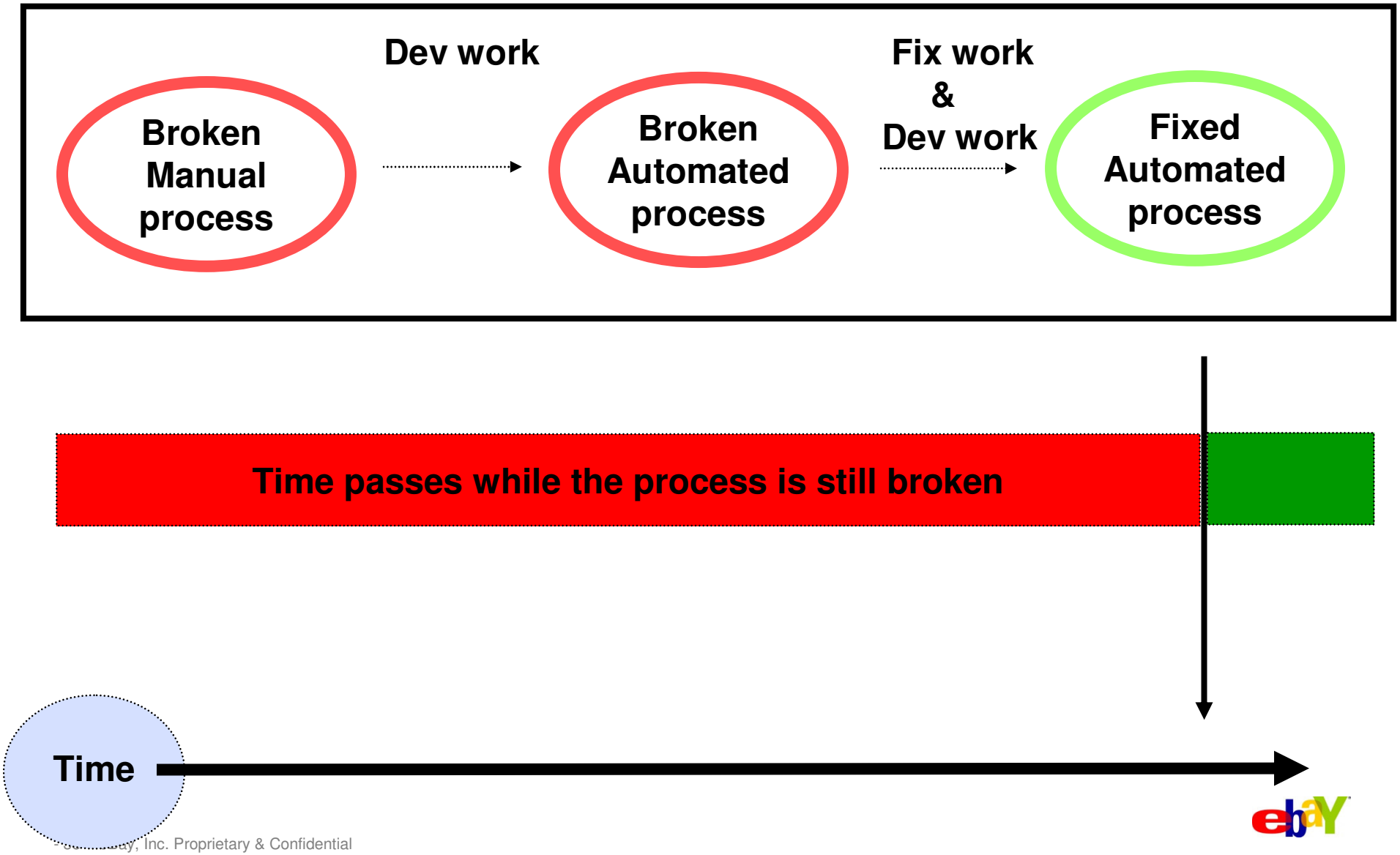
Advantage #1: Less work



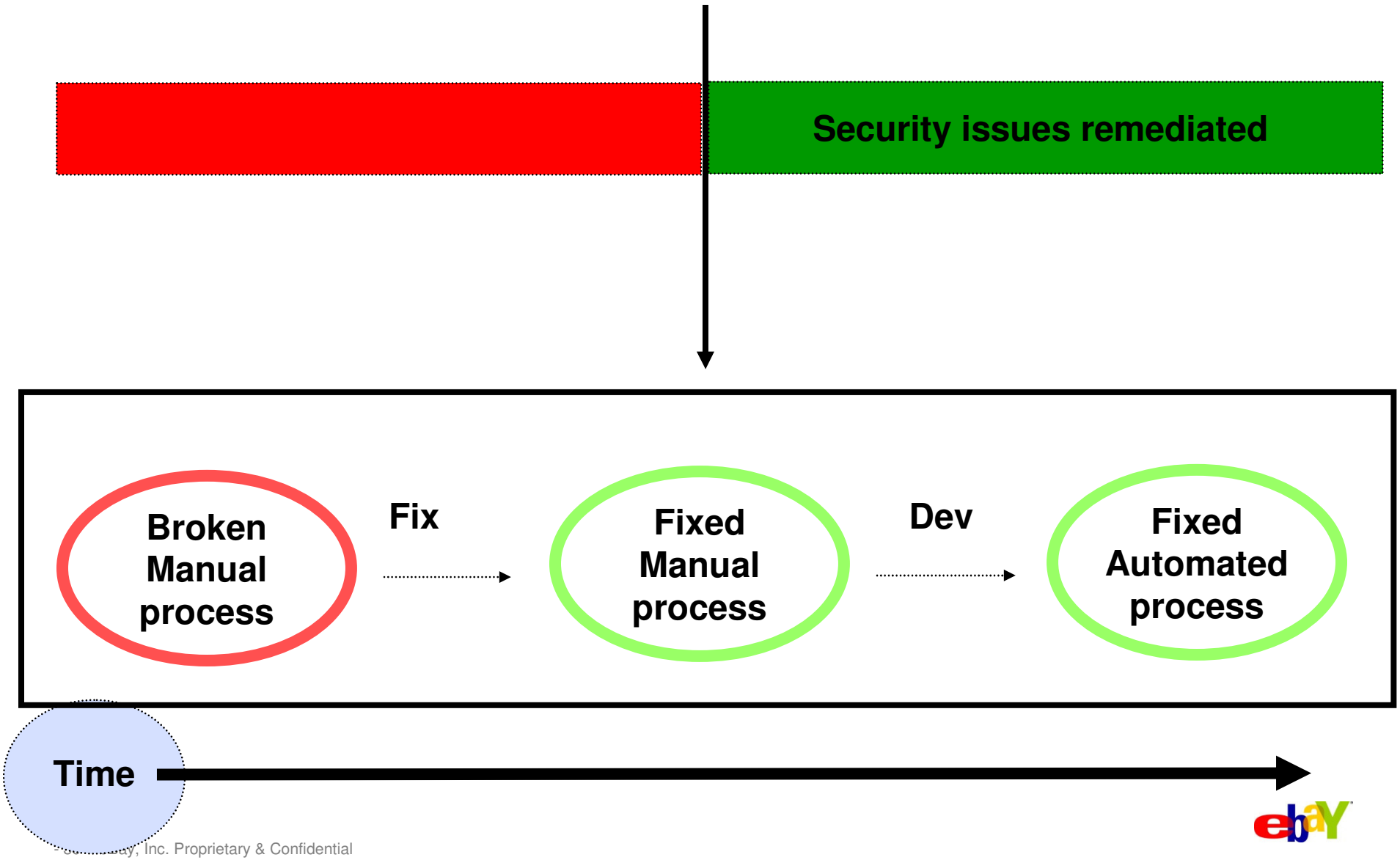
Advantage #1: Less work



Lessons Learned: Better Security



Lessons Learned: Better Security



Agenda

- Review last year's strategy
- Case Study - Web application security vulnerability tracking
- Lessons Learned - Fix process before automation
- Looking ahead - Minimum Security Baselines

Minimum Security Baselines

- **Objective – All eBay Inc. business units adhere to a minimum security baseline**
- **Goal – 70% compliance by the end of the year**

Define Baselines

Category
Antivirus/Anti-malware
BCP
Employee Terminations
Generic Host Hardening
Infosec Incident Response
Password Requirements
Patching
Security Monitoring / SOC
Security Training
Standard Build Process / Secure Config
Vulnerability Remediation Notification/Tracking
Vulnerability Scanning

Minimum Security Baselines

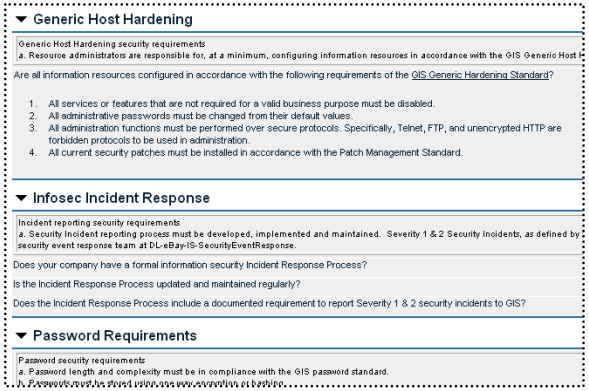
- **Objective – All eBay Inc. business units adhere to a minimum security baseline**
- **Goal – 70% compliance by the end of the year**

Define Baselines

Category
Antivirus/Anti-malware
BCP
Employee Terminations
Generic Host Hardening
Infosec Incident Response
Password Requirements
Patching
Security Monitoring / SOC
Security Training
Standard Build Process / Secure Config
Vulnerability Remediation Notification/Tracking
Vulnerability Scanning

→

Distribute Questionnaires



▼ Generic Host Hardening

Generic Host Hardening security requirements
a. Resource administrators are responsible for, at a minimum, configuring information resources in accordance with the GIS Generic Host

Are all information resources configured in accordance with the following requirements of the GIS Generic Hardening Standard?

1. All services or features that are not required for a valid business purpose must be disabled.
2. All administrative passwords must be changed from their default values.
3. All administration functions must be performed over secure protocols. Specifically, Telnet, FTP, and unencrypted HTTP are forbidden protocols to be used in administration.
4. All current security patches must be installed in accordance with the Patch Management Standard.

▼ Infosec Incident Response

Incident reporting security requirements
a. Security incident reporting process must be developed, implemented and maintained. Severity 1 & 2 Security Incidents, as defined by security event response team at DL-eBay-IS-SecurityEventResponse.

Does your company have a formal information security Incident Response Process?

Is the Incident Response Process updated and maintained regularly?

Does the Incident Response Process include a documented requirement to report Severity 1 & 2 security incidents to GIS?

▼ Password Requirements

Password security requirements
a. Password length and complexity must be in compliance with the GIS password standard.
b. Passwords must be stored using one way encryption or hashing.

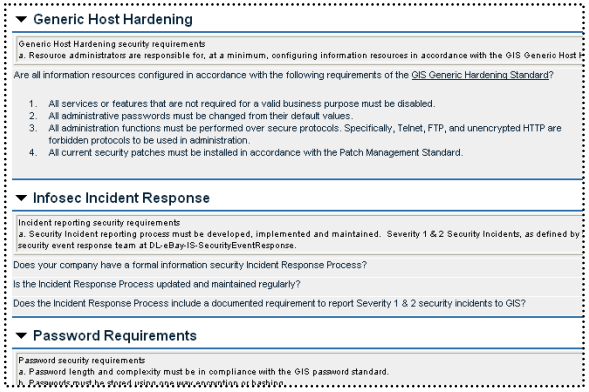
Minimum Security Baselines

- **Objective – All eBay Inc. business units adhere to a minimum security baseline**
- **Goal – 70% compliance by the end of the year**

Define Baselines

Category
Antivirus/Anti-malware
BCP
Employee Terminations
Generic Host Hardening
Infosec Incident Response
Password Requirements
Patching
Security Monitoring / SOC
Security Training
Standard Build Process / Secure Config
Vulnerability Remediation Notification/Tracking
Vulnerability Scanning

Distribute Questionnaires



Report Compliance

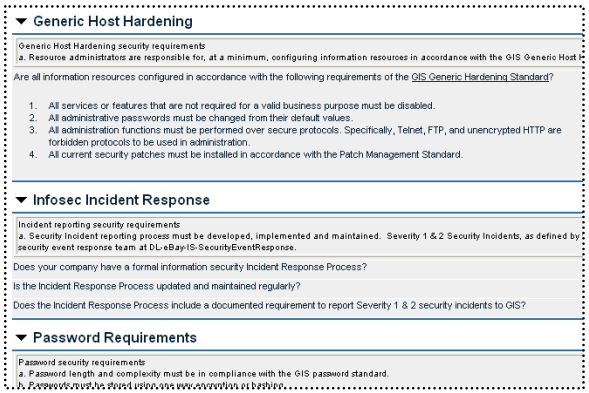
Minimum Security Baselines

- **Objective – All eBay Inc. business units adhere to a minimum security baseline**
- **Goal – 70% compliance by the end of the year**

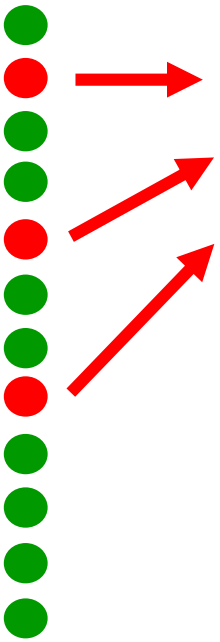
Define Baselines

Category
Antivirus/Anti-malware
BCP
Employee Terminations
Generic Host Hardening
Infosec Incident Response
Password Requirements
Patching
Security Monitoring / SOC
Security Training
Standard Build Process / Secure Config
Vulnerability Remediation Notification/Tracking
Vulnerability Scanning

Distribute Questionnaires



Report Compliance



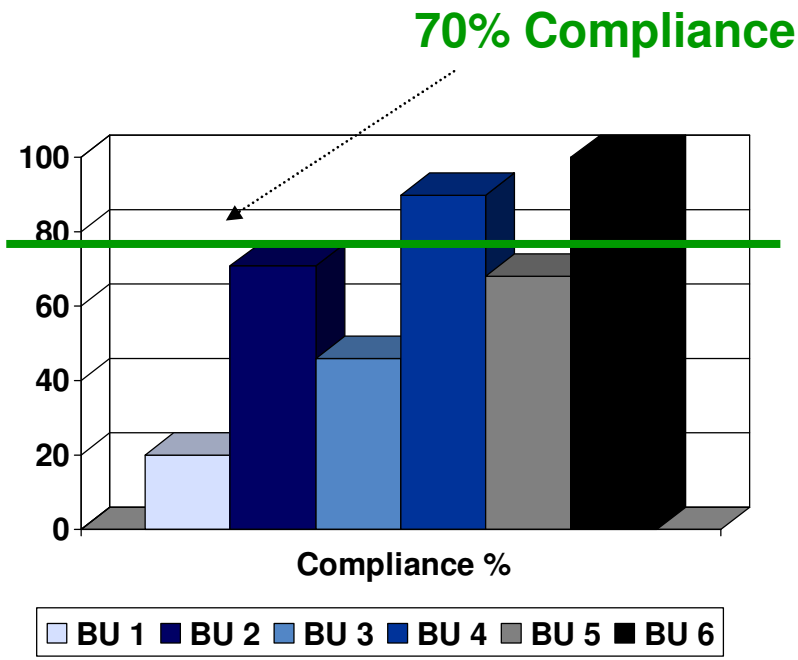
Track & Remediate Findings

Minimum Security Baselines – Periodic Reporting

By individual Business Unit

Category
Antivirus/Anti-malware
BCP
Employee Terminations
Generic Host Hardening
Infosec Incident Response
Password Requirements
Patching
Security Monitoring / SOC
Security Training
Standard Build Process / Secure Config
Vulnerability Remediation Notification/Tracking
Vulnerability Scanning

Overall for governance & oversight



Thank you! Any questions?

- Contact info: carwong@ebay.com