VRDA

Vulnerability Response Decision Assistance

Art Manion
CERT/CC

Yurie Ito
JPCERT/CC

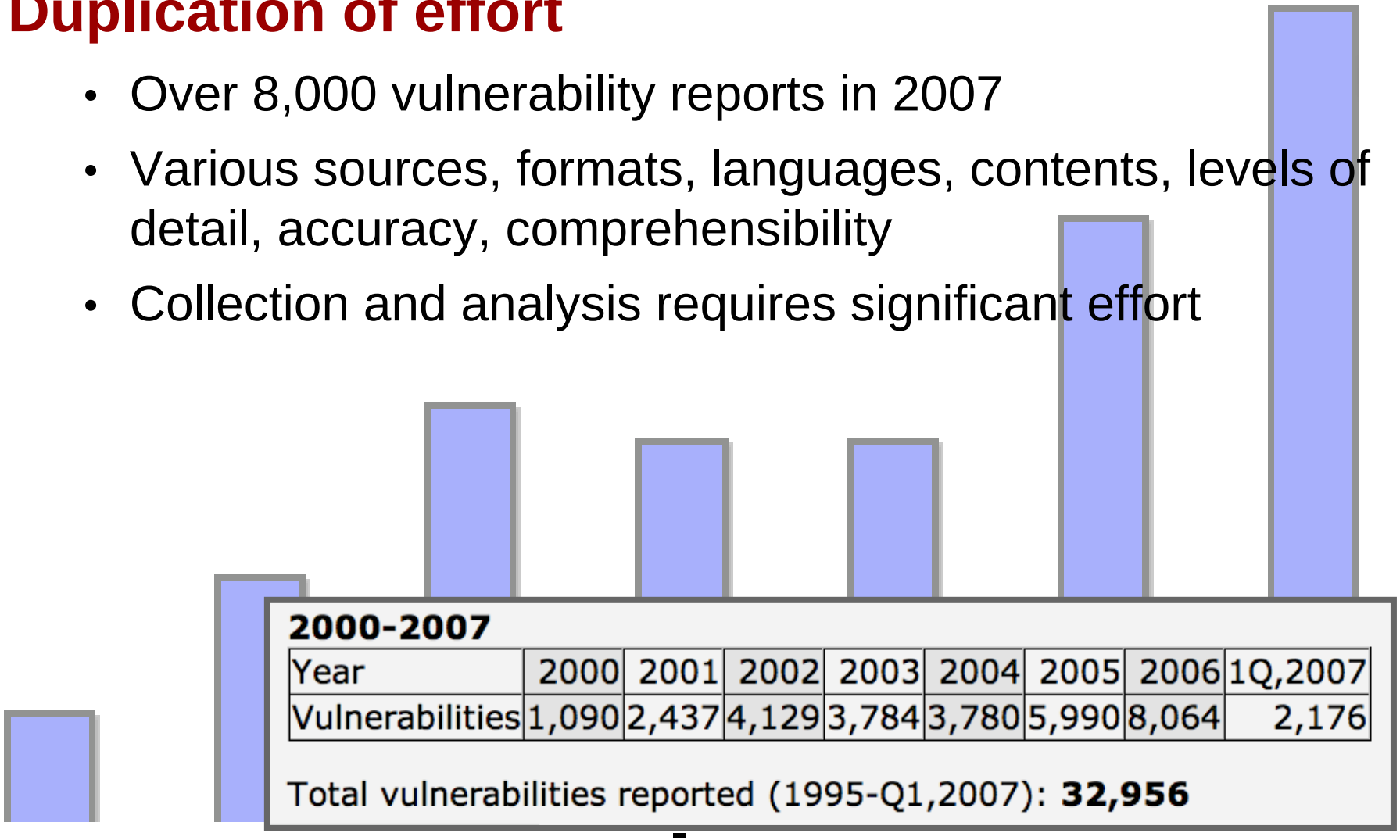
EC2ND 2007

VRDA Rationale and Design

Problems

Duplication of effort

- Over 8,000 vulnerability reports in 2007
- Various sources, formats, languages, contents, levels of detail, accuracy, comprehensibility
- Collection and analysis requires significant effort



2000-2007

Year	2000	2001	2002	2003	2004	2005	2006	1Q,2007
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064	2,176

Total vulnerabilities reported (1995-Q1,2007): **32,956**

Problems (2)

Inconsistent response decisions

- Analysts may disagree
- Analysts apply personal prejudices
- Decisions may not represent organizational values

Problems (3)

Existing metrics insufficient

- Most metrics output global severity values
  - "One size does not fit all."
- Common Vulnerability Scoring System (CVSS)
  - Contains environmental metrics
  - Focus on base score
- Values vary by organization
  - May respond differently to the same vulnerability
  - Use different software
  - Use the same software in different ways
  - Value information assets differently

Solution

VRDA proposes to answer the question:

How do I best respond to a given vulnerability report?

Goals

- Record vulnerability data in structured format
- Support individualized response decision
- Transition organizational knowledge from human analysts to VRDA
- Improve response accuracy and consistency
- Reduce duplication of effort

Audience

System administrators

- Operational responsibility for fixing systems

CSIRTs

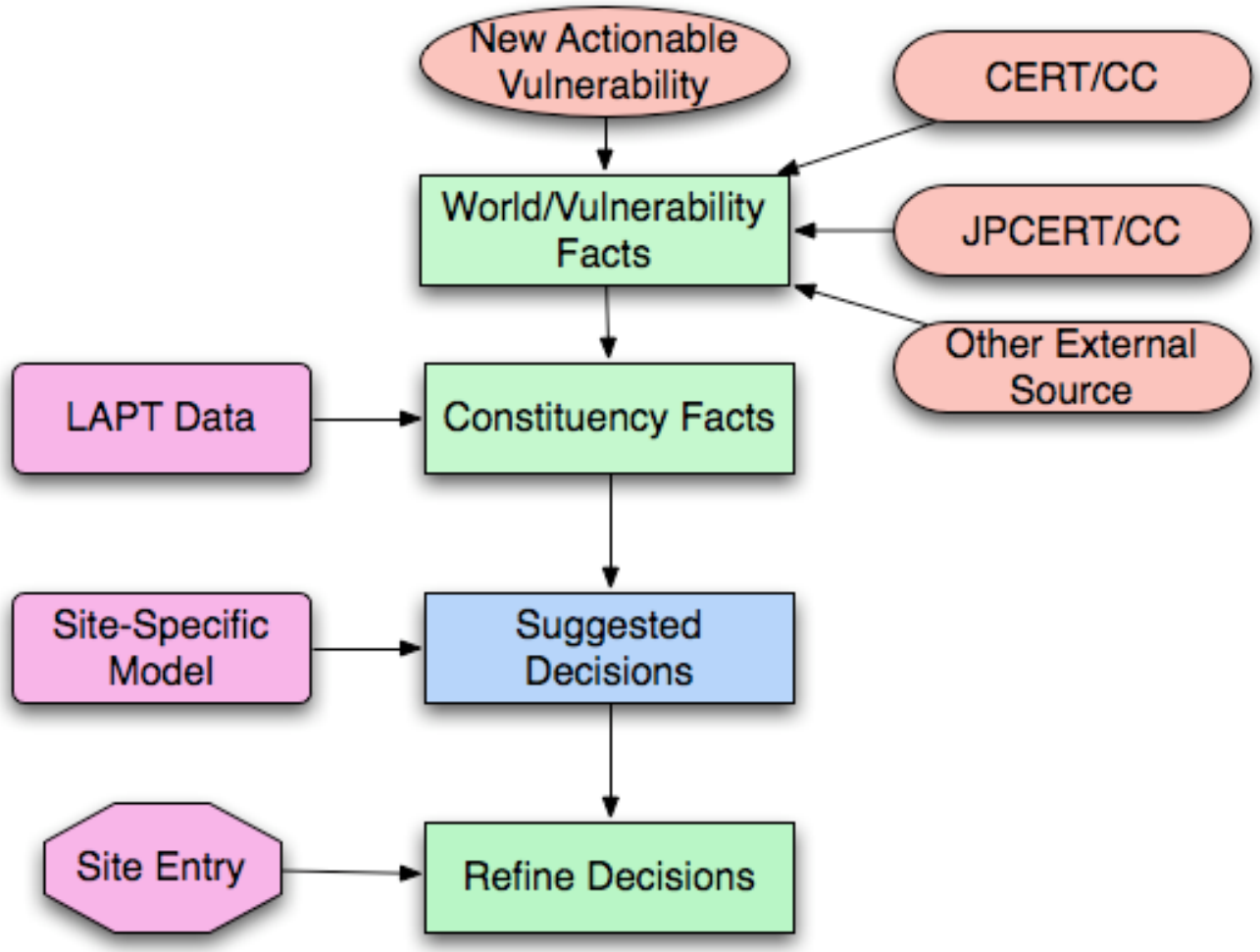
- Provided advice to system administrators, users

Vendors

- Product security response teams

Anybody regularly responding to vulnerability reports

Operational Concept



Components

Decisions to make: Tasks

Vulnerability representation: Facts

Product usage: LAPTs

Encoding decision-making: Decision Model

Tasks

Decisions an organization must make

Specific to each VRDA user

Example tasks

- Publish an advisory
- Initiate patch process
- Implement workaround
- Ignore (don’t expend effort on low priority vulnerabilities)

Facts

Properties of vulnerabilities and their environment

Assertions based on available information

- Vulnerability Facts–inherent technical attributes
- World Facts–about environment
- Constituency Facts–specific to VRDA user organization

Balance accuracy, completeness, granularity, cost

LAPTs

Lightweight Affected Product Tags

Problem: Constituency facts cannot be given to you

LAPTs identify products affected by vulnerability

Facilitates lookup of constituency facts

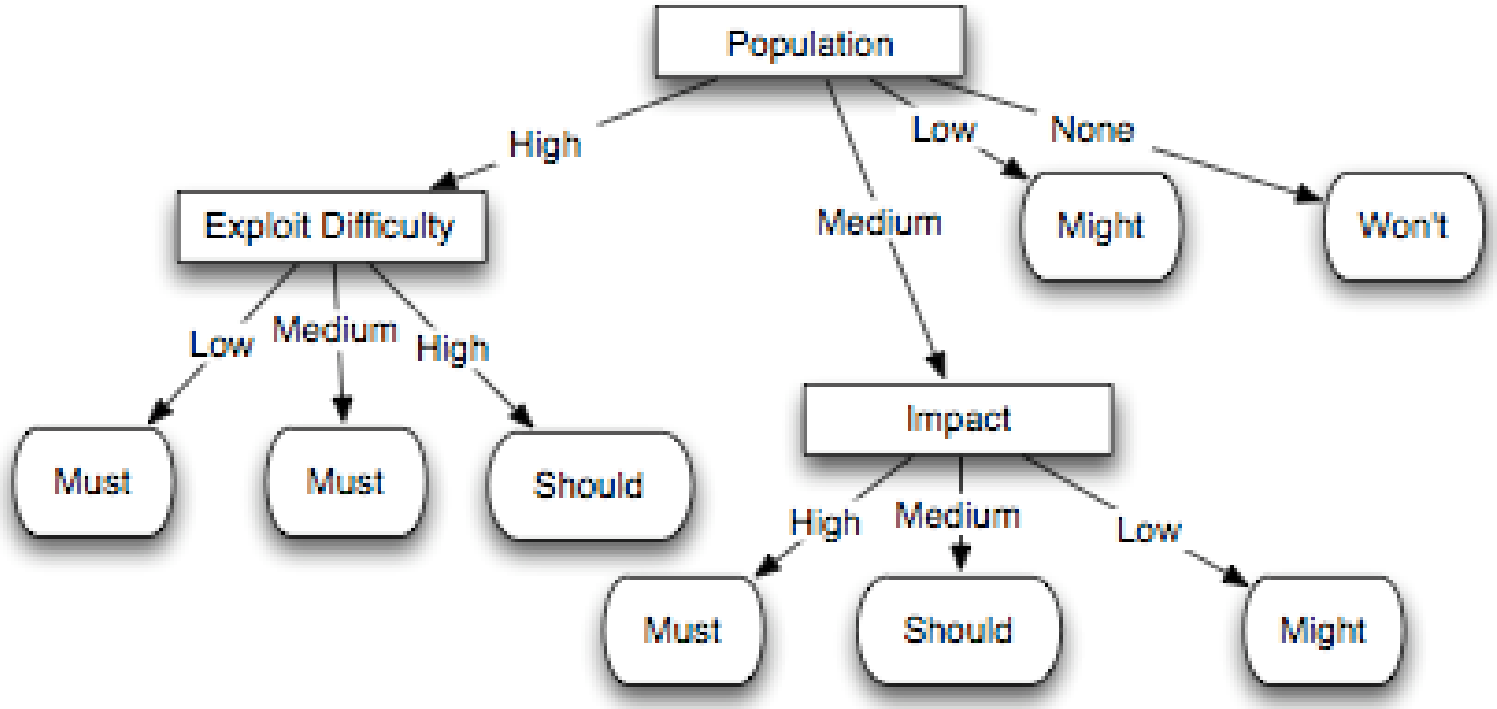
- External feed provides LAPTs for each vulnerability
- Cross-reference with your database

Decision Model

Represents individualized decision-making behavior

Expert system encoding organizational values

Decision trees



Decision Model (2)

Why decision trees?

- Observable, understandable
- Can be created and refined by hand

Model creation

- Design initial model from experience
- Create empirical model based on recorded data

Related Work

Structured vulnerability descriptions

- Common Vulnerability Scoring System (CVSS)
- Open Source Vulnerability Database (OSVDB)
- Open Vulnerability and Assessment Language (OVAL)

Advisory exchange formats

- Common Announcement Interchange Format (CAIF)
- EISPP Common Advisory Format Description
- Deutsches Advisory Format (DAF)
- VULnerability Data publication and Exchange Format (VULDEF)

System information

- Common Model of System Information (CMSI)
- Common Product Enumeration (CPE)

Related Work (2)

Severity metrics

- Common Vulnerability Scoring System (CVSS)

Security Content Automation Protocol (SCAP)

- National (US) Institute of Standards and Technology (NIST), MITRE
- Set of vulnerability management and compliance standards (CVE, CCE, CPE, CVSS, XCCDF, OVAL)

VRDA Usage with KENGINE

KENGINE

VRDA implementation developed by JPCERT/CC

- Intend to open-source

KENGINE provides consistent analysis and reasoning action

Other KENGINE functions

- Task management
- LAPT management
- Decision tree management
- Reporting

KENGINE

Minimum resources to handle the maximum number of vulnerabilities

Deployment

Interview user organization

- Determine all possible tasks
  - Identify task dependencies
  - Mandatory/conditional actions do not involve choice, not tasks
- Determine facts
  - Select only facts necessary to make decisions about tasks

Develop decision model

- Teach/train the system using sample VRDA data and choosing appropriate tasks
- Create or modify decision trees manually

Usage

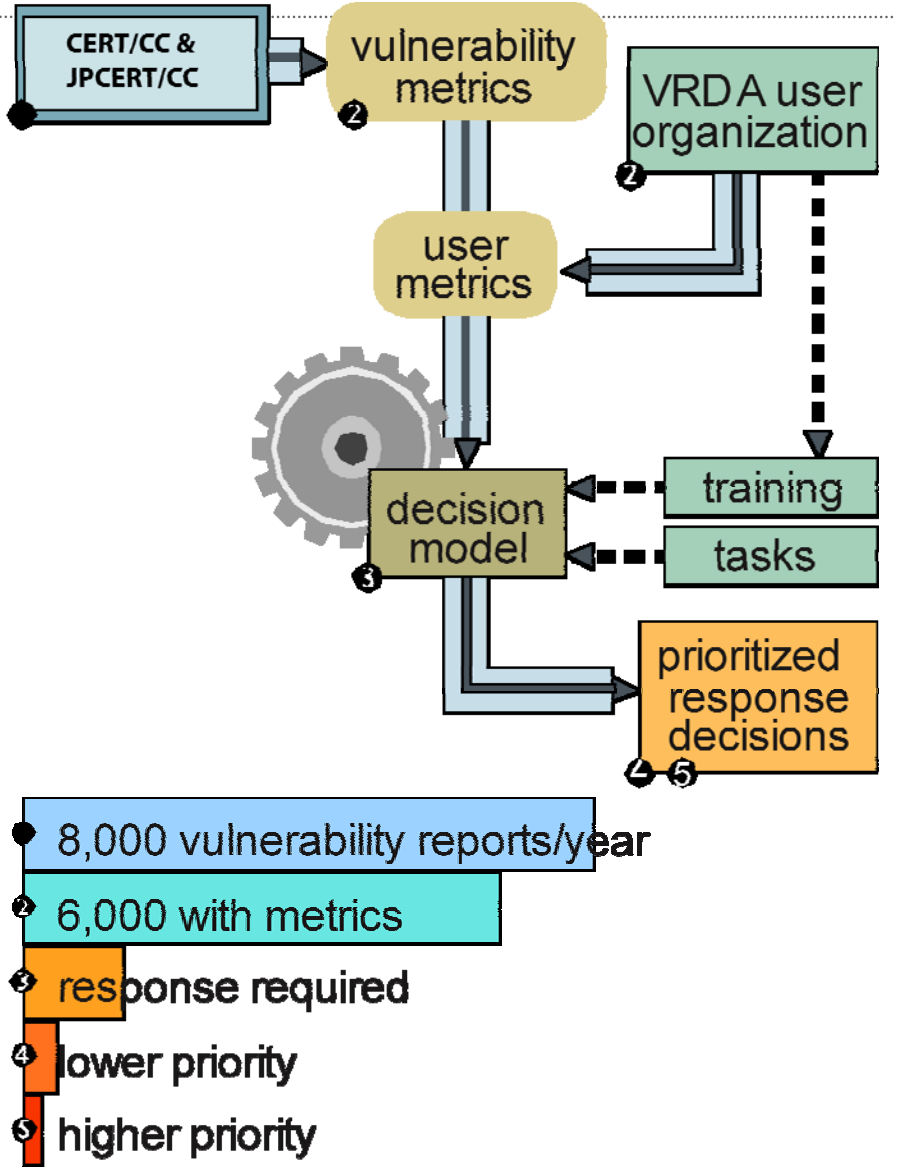
CERT/CC, JPCERT/CC publish vulnerability facts (metrics)

User determines tasks, creates decision model, provides user-specific facts (metrics)

KENGINE gives prioritized response decision

Compare VRDA decisions with actual response, adjust decision model as necessary

Graphic on all three slides with parts highlighted



Usage

Get or create VRDA data

- CERT/CC and JPCERT/CC publish fact feeds

Score organization-specific facts

Process vulnerability reports

- Use the decision model
- Record actual decisions

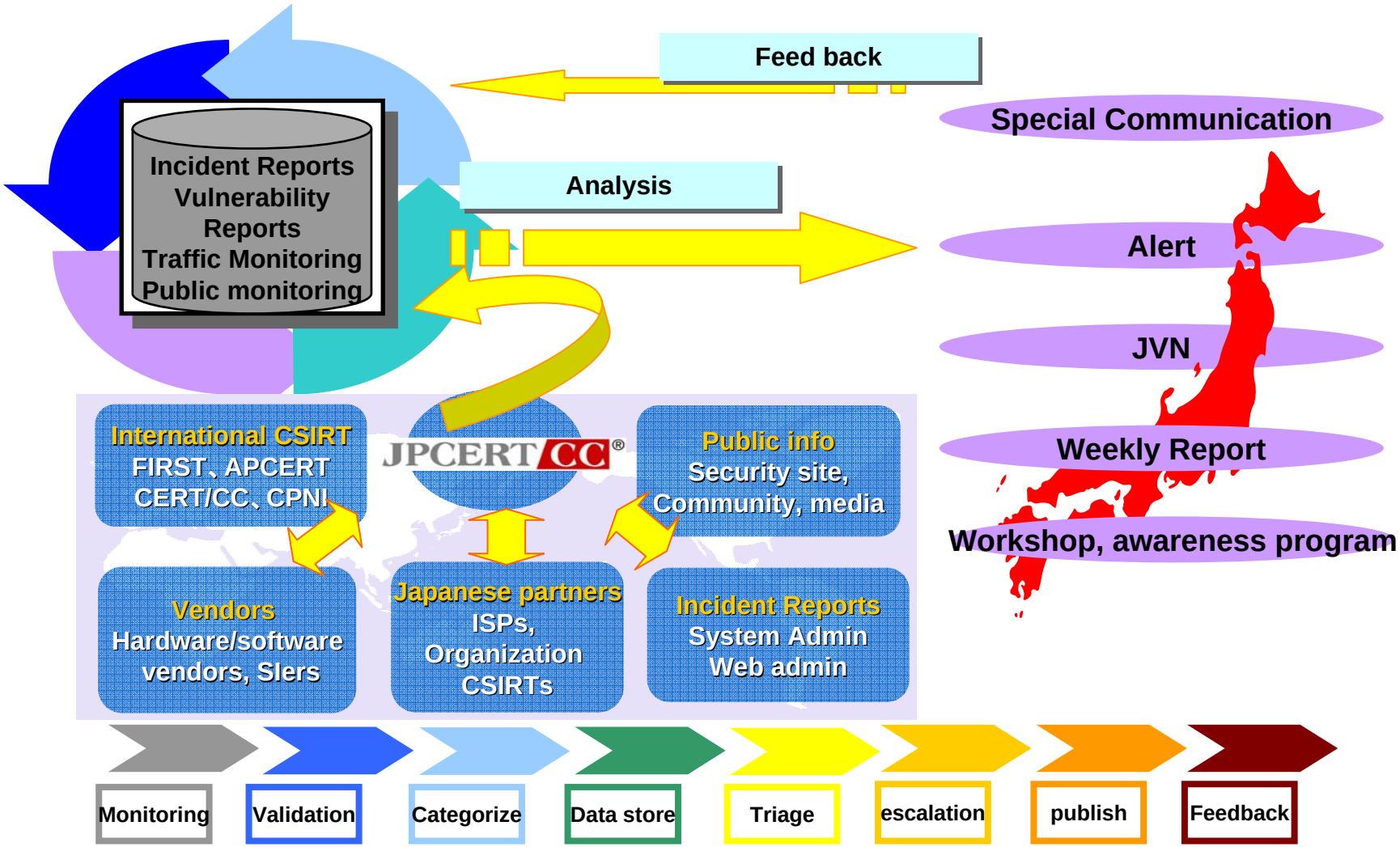
Feedback

Compare recommendations with actual decisions

Refine decision making process

- Update decision model
- Facts may be missing or inaccurate
- Tasks may be missing

JPCERT/CC Operation

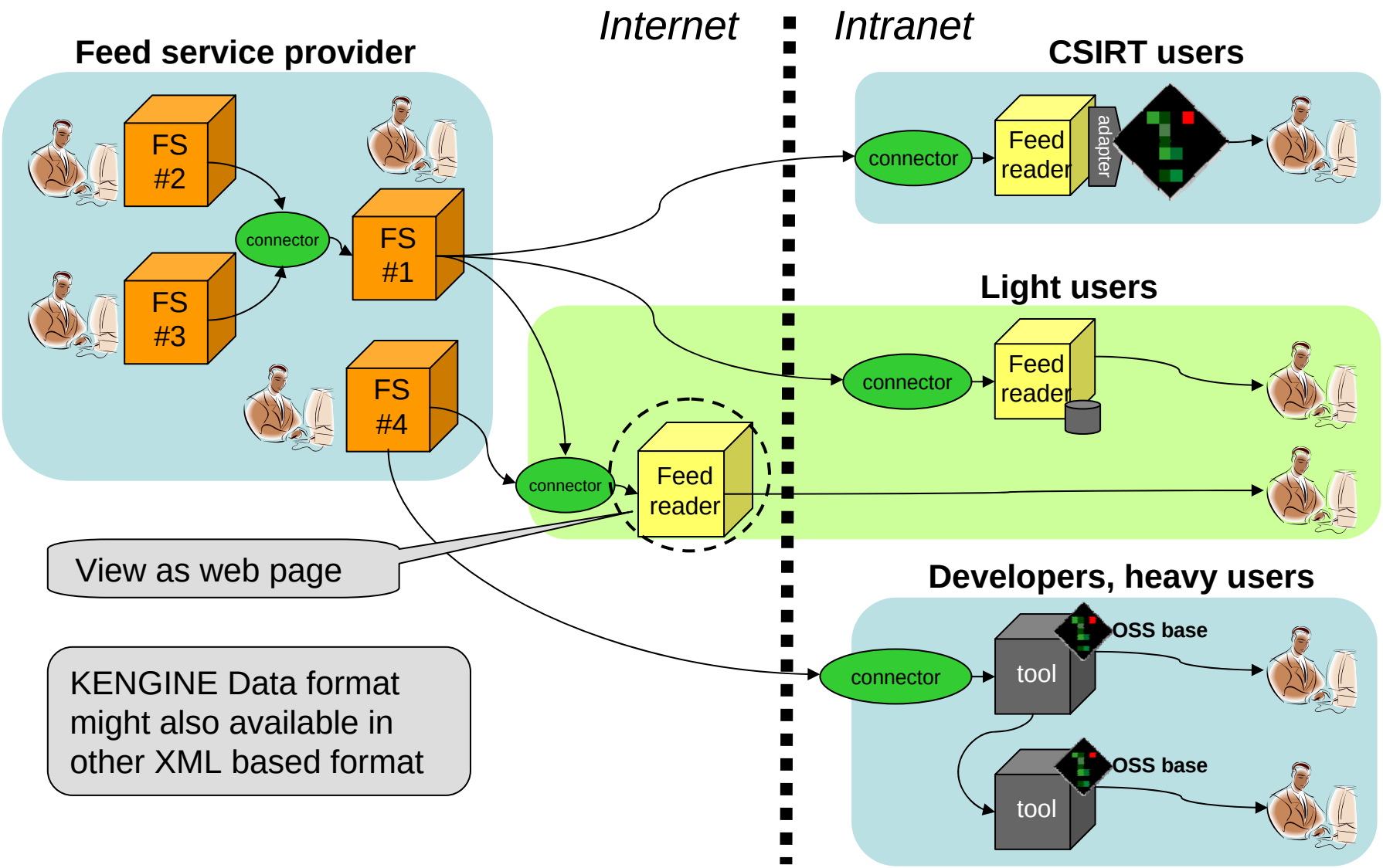


JPCERT/CC Facts

1. Impact
2. System Importance in Japan
3. System Population in Japan
4. Usage by critical infrastructure
5. Impact to internet infrastructure
6. Access requirement
7. How complicated is the attack?
8. Incident/attack activity
9. Information accessibility (public or private report)
10. Confidence in the information source
11. Availability of remediation (patch/countermeasures)
12. Usage by JPCERT

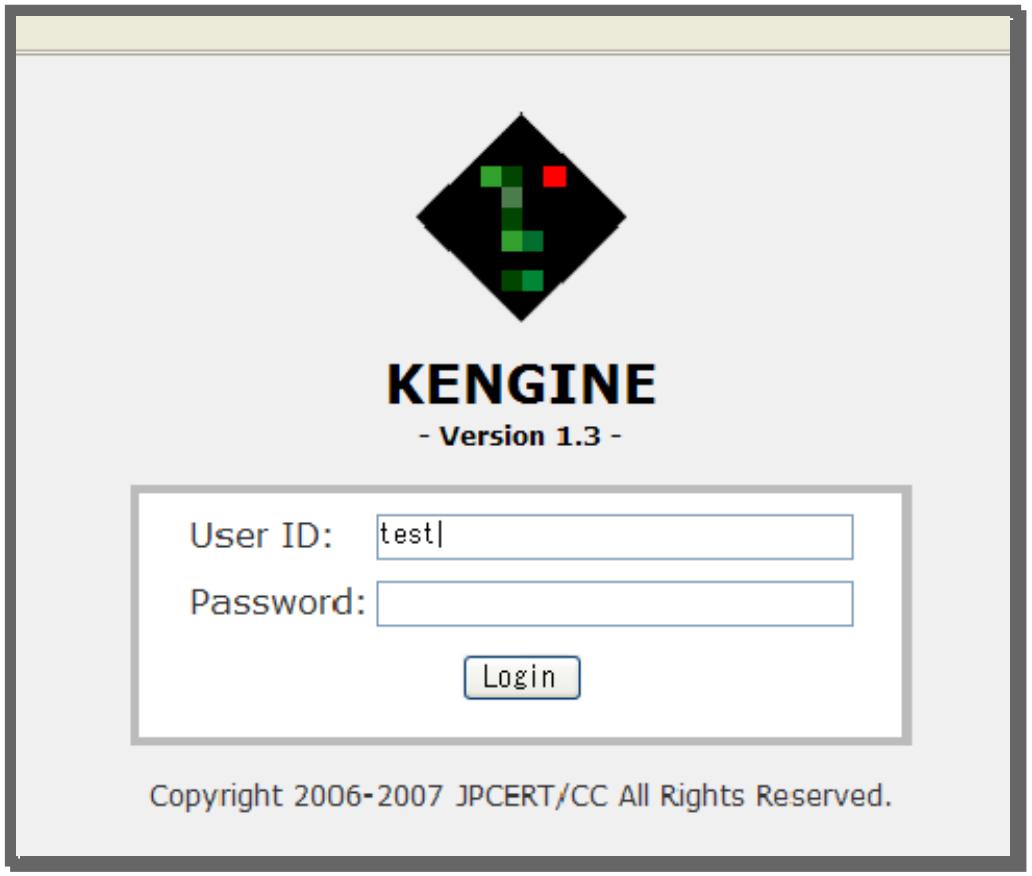
Constituency Facts
Vulnerability Facts
World Facts

Feed Operation



KENGINE Data format might also available in other XML based format

KENGINE


KENGINE
- Version 1.3 -
User ID:
test
Password:
Login
Copyright 2006-2007 JPCERT/CC All Rights Reserved.

Vulnerability Reports

Report ID	Title	Priority [8]	Status	Assign	Task			Created Updated
					Analyze	Security_Alert	Sharing	
JVN#00000023	MS Updates for Multiple Vuls	1	Pending Close (D2)	admin admin	Yes Final	Notify Final	Yes Final	'07/08/14 '07/08/14
JVN#00000029	MS Updates for Multiple Vuls	1	Proposal Req'd (Detailed)	admin admin	Yes Computed	Notify Computed	No Computed	'07/08/14 '07/08/14
JVN#00000013	Sourcefire Snort DCE/RPC Preproce...	1	Pending Close (D2)	admin admin	Yes Final	Refer Final	No Final	'07/06/14 '07/08/14
JVN#00000028	MS SQL Vulnerability	1	Proposal Req'd (Surface)	admin None	Yes Computed	Alert Computed	No Data Computed	'07/08/14 '07/08/14
JVN#00000021	Abobe Acrobat reader	1	Decision Req'd (Surface)	None None	Yes Computed	Refer Proposed	No Data Computed	'07/07/14 '07/08/14
JVN#00000025	GnuPG Vulnerability	1	Detailed Analysis Req'd	admin admin	Yes Computed	Notify Computed	No Data Computed	'07/08/14 '07/08/14

Vulnerability Report Detail

** General Information ** Edit

Report ID	: JVN#00000023		
Title	: MS Updates for Multiple Vuls		
Memo	:		
Status	: Pending Close (D2)		
Created	: 2007/08/14 23:11	**Last Updated**	: 2007/08/14 23:28
Created By	: admin		
Tri Handler	: admin	**Vul Handler**	: admin
Surface Completed	: 2007/08/14 23:12		
Detailed Completed	: 2007/08/14 23:28		
Decision Finalized	: 2007/08/14 23:28		
Report Closed	:		

Hide ** Analysis Information **

- LAPT - Edit

Selected LAPTs

[Microsoft-Excel][Microsoft-InternetExplorer][Microsoft-Windows-Vista][Microsoft-Windows-XP][Microsoft-Word]

- FACT - Edit

Impact)

The impct of the vulnerability is:

None Low ✔ Medium High Unknown

Access_Required)

The type of network and/or physical access required to exploit this vulnerability is:

Routed ✔ Non-routed Local Physical Unknown

Authentication_Required)

What level of authentication does exploiting this vulnerability require?

None Limited ✔ Standard Privileged Unknown

LAPT Management

Search | Reset

Items per page: 50

Name	Related Reports	FACT		Last Checked	Action	
		Organization_Used	Importance			
Adobe-Acrobat	0	Yes	Low	61days	Edit	Delete
Adobe-Acrobat-Reader	1	Yes	Medium	61days	Edit	Delete
Apache	1	Yes	High	61days	Edit	Delete
Apple-MacOS-X	2	Yes	Low	61days	Edit	Delete
Apple-QuickTime	2	No	None	61days	Edit	Delete
Apple-Safari	1	Yes	Low	61days	Edit	Delete
Bind	1	Yes	High	61days	Edit	Delete
Cisco-IOS-10	1	Yes	High	61days	Edit	Delete
Debian	1	No	None	61days	Edit	Delete

Task Workflow

Report ID	Task	Decision	Priority [8]	Task Status Not Started | In Progress | Completed	Update	Memo	Details	Last Updated Report Closed	Action
JVN#00000005	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000003	Analyze	Yes Final	1	○ ○ ◉					Details Memo
JVN#00000010	Analyze	Yes Final	1	○ ○ ◉					Details Memo
JVN#00000023	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000020	Analyze	Yes Computed	1	◉ ○ ○					Details Memo
JVN#00000002	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000012	Analyze	Yes Final	1	○ ○ ◉					Details Memo

Decision Tree

Name:

Security_Alert

Back

Master :

Tree Tag Name : MASTER-Generated

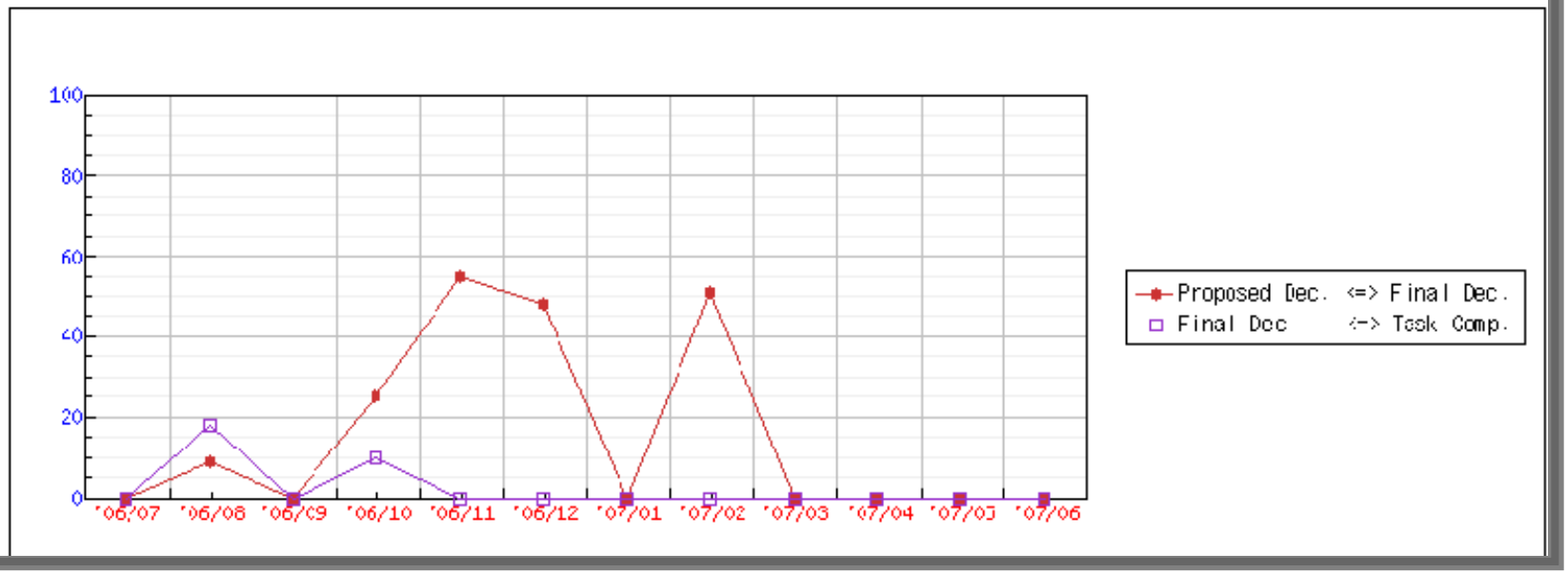
Comment :

- Consider field "Importance"
  - Unknown -> Consider field "Impact"
    - Unknown -> Consider field "Required_Actions"
      - Unknown -> Consider field "Authentication_Required"
        - Unknown -> "No_Act"
        - Privileged -> "No_Act"
        - Standard -> "No_Act"
        - Limited -> "Refer"
        - None -> "Notify"
      - Complex -> "No_Act"
      - Simple -> "Notify"
    - High -> "Alert"
    - Medium -> "Notify"
    - Low -> "Refer"
    - None -> "No_Act"
  - High -> Consider field "Impact"
    - Unknown -> Consider field "Activity"
      - Uknown -> "No_Act"
      - Our incident -> "Alert"

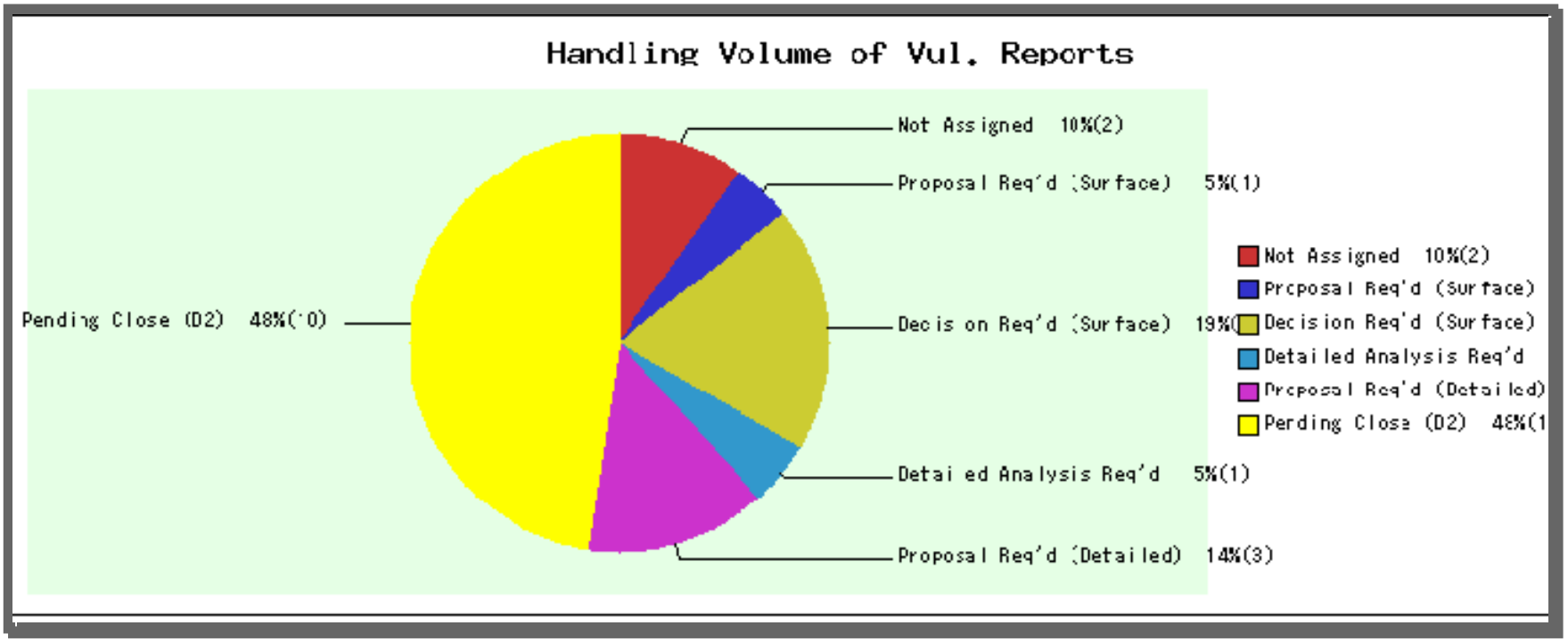
Task Deviation Report

Task:Analyze Review Decision

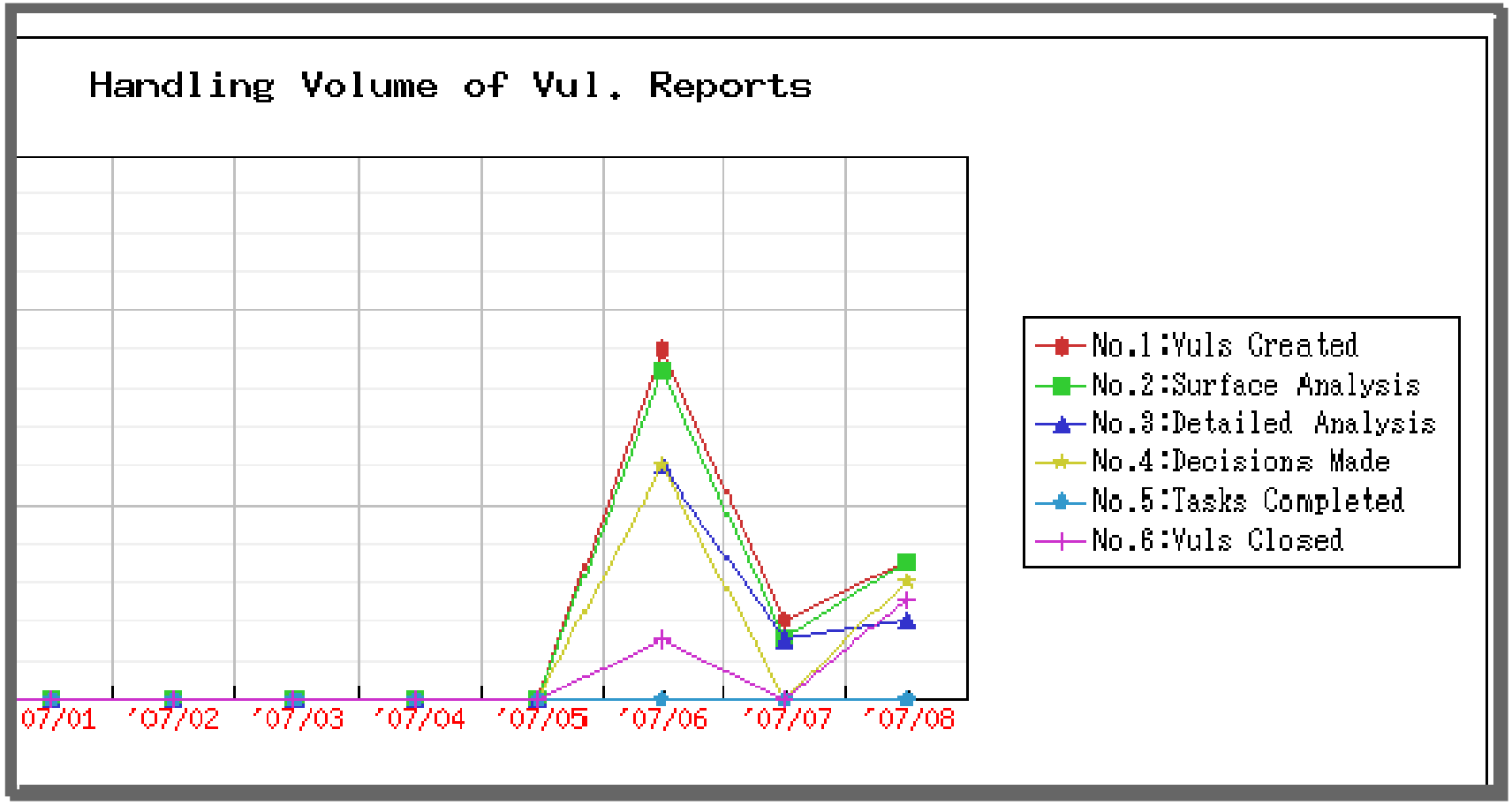
	'06/07	06/08	'06/09	'06/10	'06/11	'06/12	'07/01	'07/02	'07/03	'07/04	'07/05	'07/06	Average
Proposed Dec. <=> Final Dec.	0%	9%	0%	25%	55%	48%	0%	51%	0%	0%	0%	0%	4<%
Fina Dec. <-> Task Comp.	0%	10%	0%	10%	0%	0%	0%	0%	0%	0%	0%	0%	2%



Progress Report



Handling Volume Report



Future

KENGINE availability

- JPCERT/CC intends to provide open-source
- Documented in Japanese and English

JPCERT/CC

- VRDA data feeds with vulnerability and world facts
- Pilot program in progress
- Deployment consulting

CERT/CC

- Developing pilot program
- Considering integration into workflow and products

More Information

Art Manion <amanion@cert.org>

Yurie Ito <yito@jpcert.or.jp>