symantec™

How security intelligence can be used for incident management

Volker Rath, Techn. Lead Consulting Services

Safety and protection matters

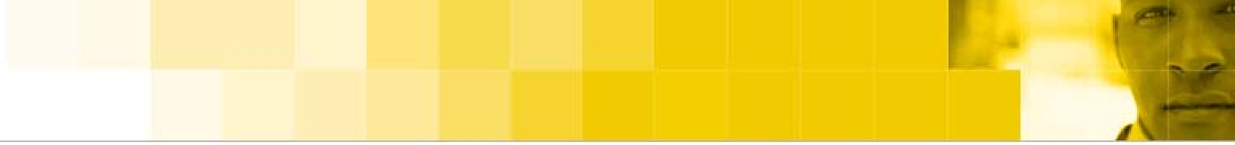
- Lots of news about threats and diseases.
- Which immunizations?
- Spreading new viruses.
- Pu

unknown quality (web, rumors)

- Unable to prioritize infos

Being paranoid is no the solution!

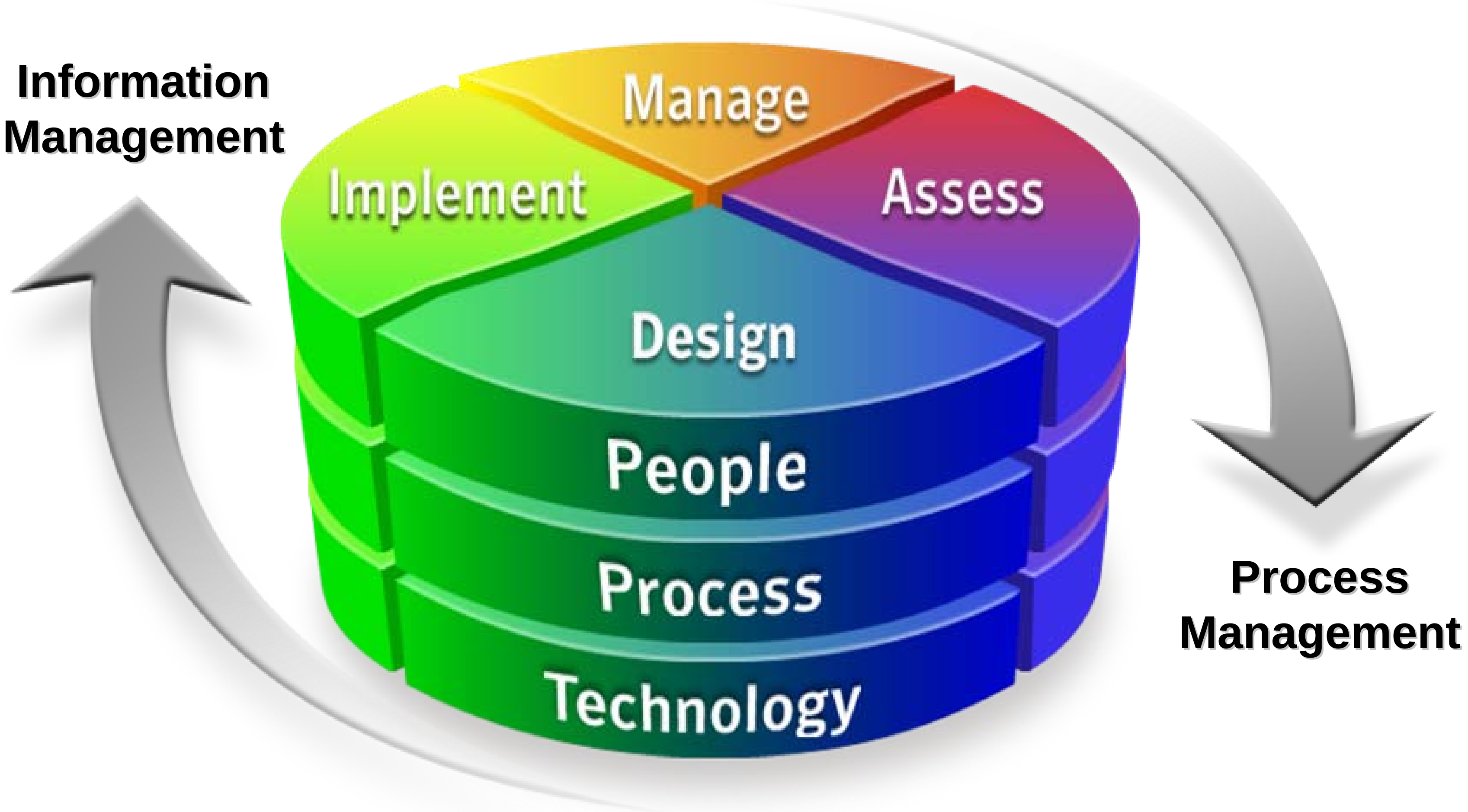
Information is there and available but I'm not able to filter, prioritize them to define the right actions!



How to deal with (IT) risks

- I need to know the risks
- Identify the risk factors
  (Likelihood, potential damage, potential targets etc.)
- Define risk estimation
- Define countermeasures
- Define action plan

Symantec Threat and Vulnerability Service Model



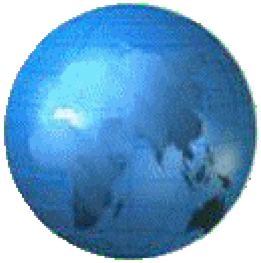
How to get risk related information?

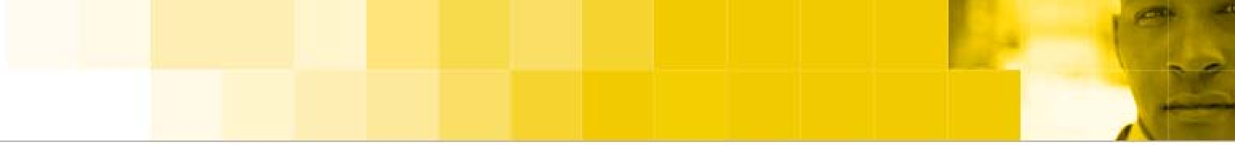
Security Intelligence Services provide information on risks:

- Threats
- Vulnerabilities
- Suspect internet behavior
- Current attacks and Virus outbreaks

- Semiannual Internet Security Threat Report

- What is DeepSight Threat Management System?



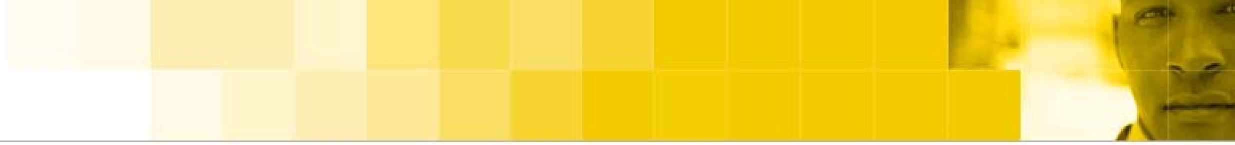


Why Security Intelligence helps Incident Management

- Provides background information for incident management and forensics
  (how an attack, virus etc. works)

- Helps to find a proper individual risk rating to threats and incidents to prioritize actions
  (we do not have unlimited resources)

- Reactive to proactive approach in security area to minimize risk (→ incidents)



Threat & Vulnerability Mgmnt. vs. Incident Management

TVM

- *Proactive*, tries to fix problems before they become an incident

IM

- *Reactive*, manages mitigation of threats and incidents

Both deal with…

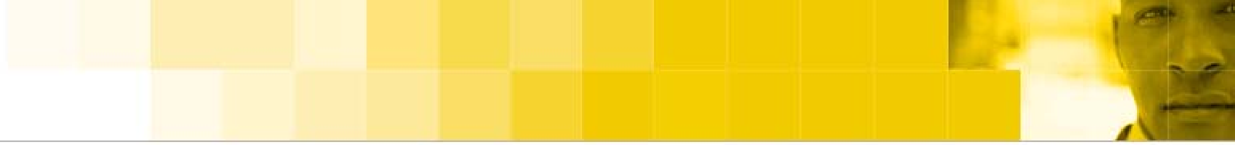
- Technology
- Assets
- People
- Process

Treat and Vulnerability Management today

- Surf the web to get information
- Subscribe Intelligence Services (e.g. Symantec DeepSight ™)
- Analysis of unstructured information (mainly mail notifications)
- Correlate information
  → new postings + all following updates
  → find relations (vulnerabilities used in malicious codes)
  → Vulnerabilities and Malicious codes used in attacks
- Define countermeasures
  → what to do? (e.g. patch)
  → where (technical)? (e.g. affected HW/SW)
  → where (geographical)?
  → who? (e.g. local admins)

Manage
Implement
Assess
Design
People
Process
Technology

- Tracking activities (what has been done till when)
- Reporting



Challenges in the TVM area

Information is available (mail, web), but not manageable, because…

…information is unstructured (e.g. email text)

…to many data sources

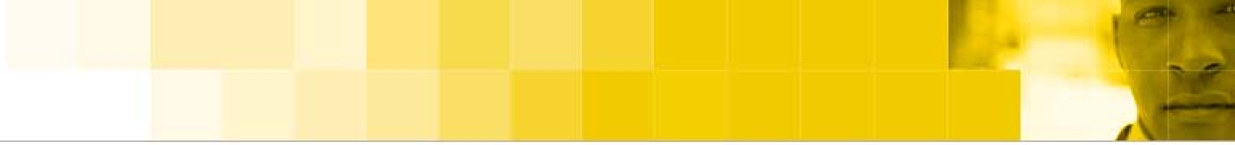
…no complex queries possible on information sources

…individual ratings, comments etc. can not be added

…”rating mathematics” cannot be changed

…no individual reports available
(e.g. get all vulnerabilities, that use port 80
get all patches for product X and version Y)

…information cannot be used automatically in other security solutions
(“Integration into Policy Compliance, SW-Rollout, Messaging etc.”)



Challenges in management?

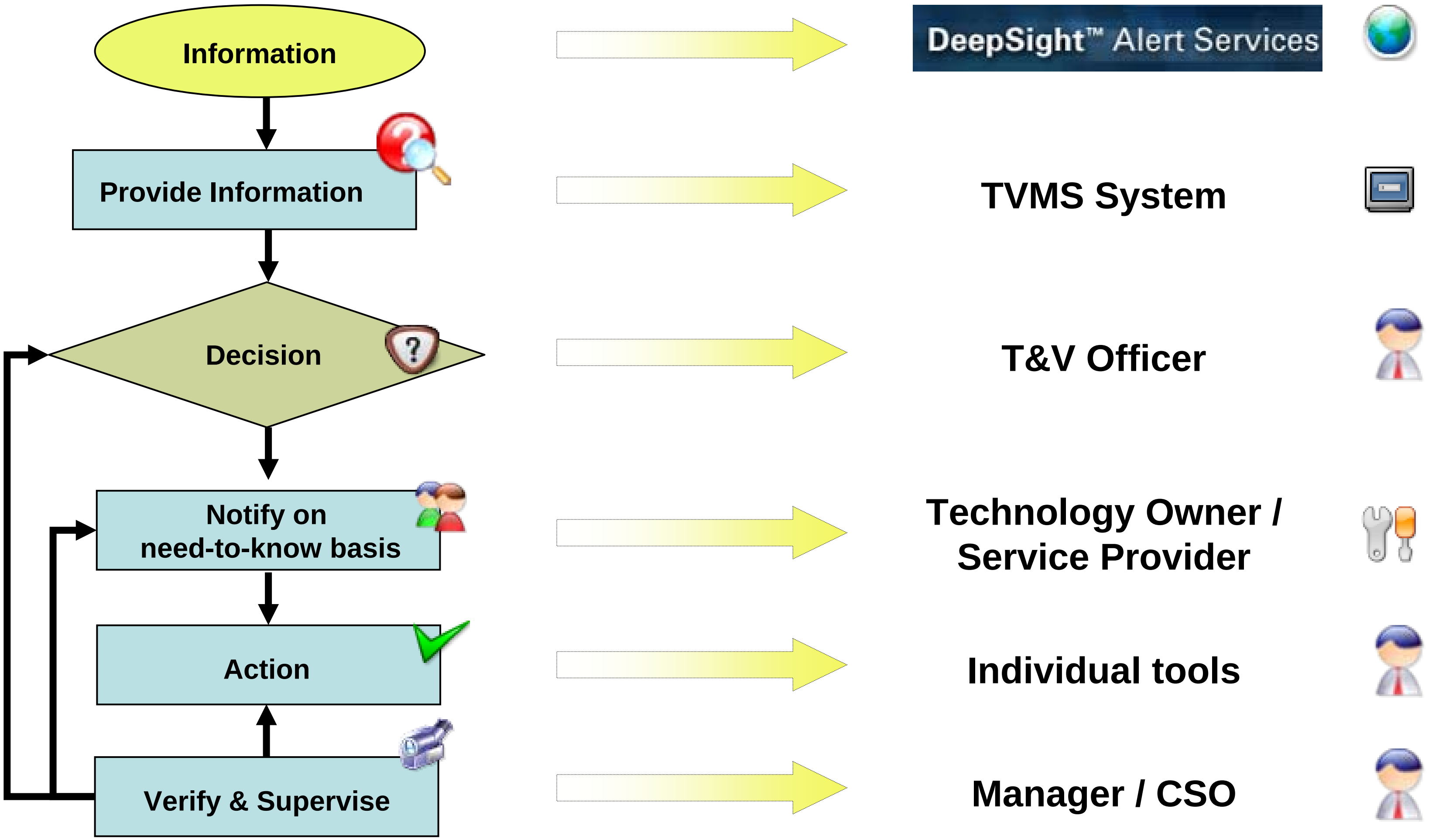
- People who are responsible for availability are also responsible for security. That does not work!
  (Risk management is not an admin's job! Example: SQL Slammer)

- Information coming via email does not give customers Knowledge-Base features on vulnerabilities and threats.
  (New postings + x updates = information that is needed)

- Information is flooding people that are under time pressure

- Information is not provided on a need-to-know basis
  (Useless information is annoying people who will start to ignore it)

TVM Process



Information

Provide Information

Decision

Notify on need-to-know basis

Action

Verify & Supervise

DeepSight™ Alert Services

TVMS System

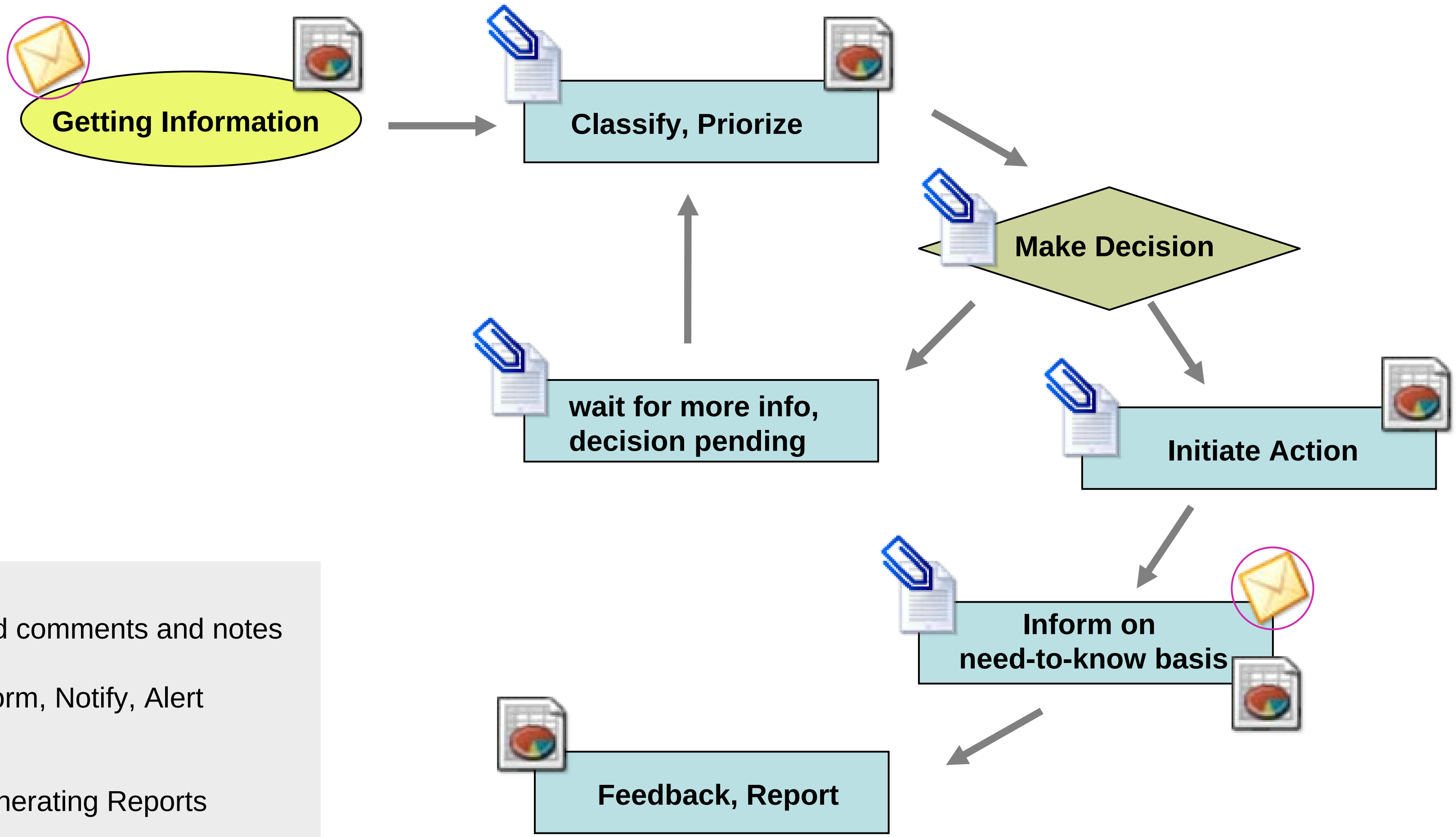
T&V Officer

Technology Owner / Service Provider

Individual tools

Manager / CSO

What a basic TVM System has to cover



Getting Information

Classify, Priorize

Make Decision

wait for more info, decision pending

Initiate Action

Inform on need-to-know basis

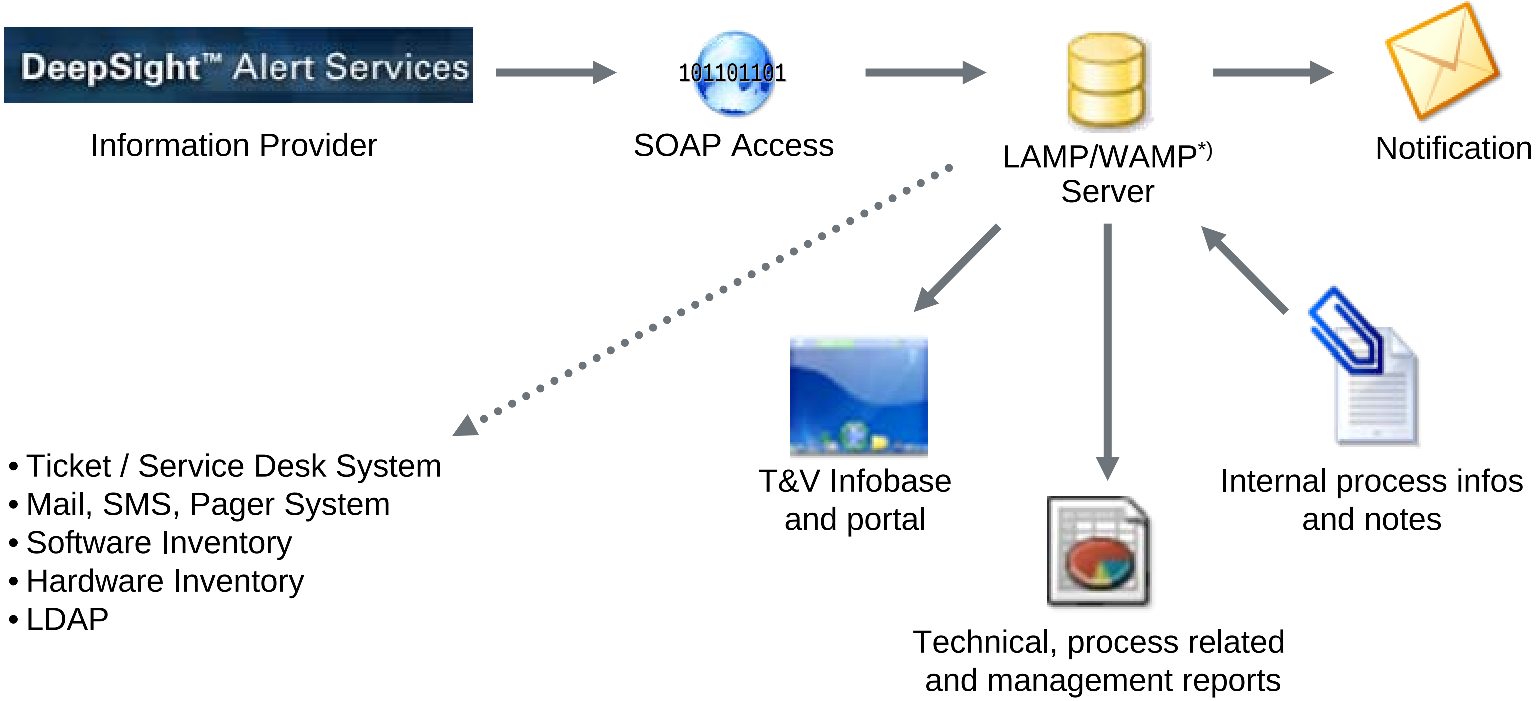
Feedback, Report

Add comments and notes

Inform, Notify, Alert

Generating Reports

Symantec’s approach for a TVM System



Information Provider

SOAP Access

LAMP/WAMP*) Server

Notification

- Ticket / Service Desk System
- Mail, SMS, Pager System
- Software Inventory
- Hardware Inventory
- LDAP

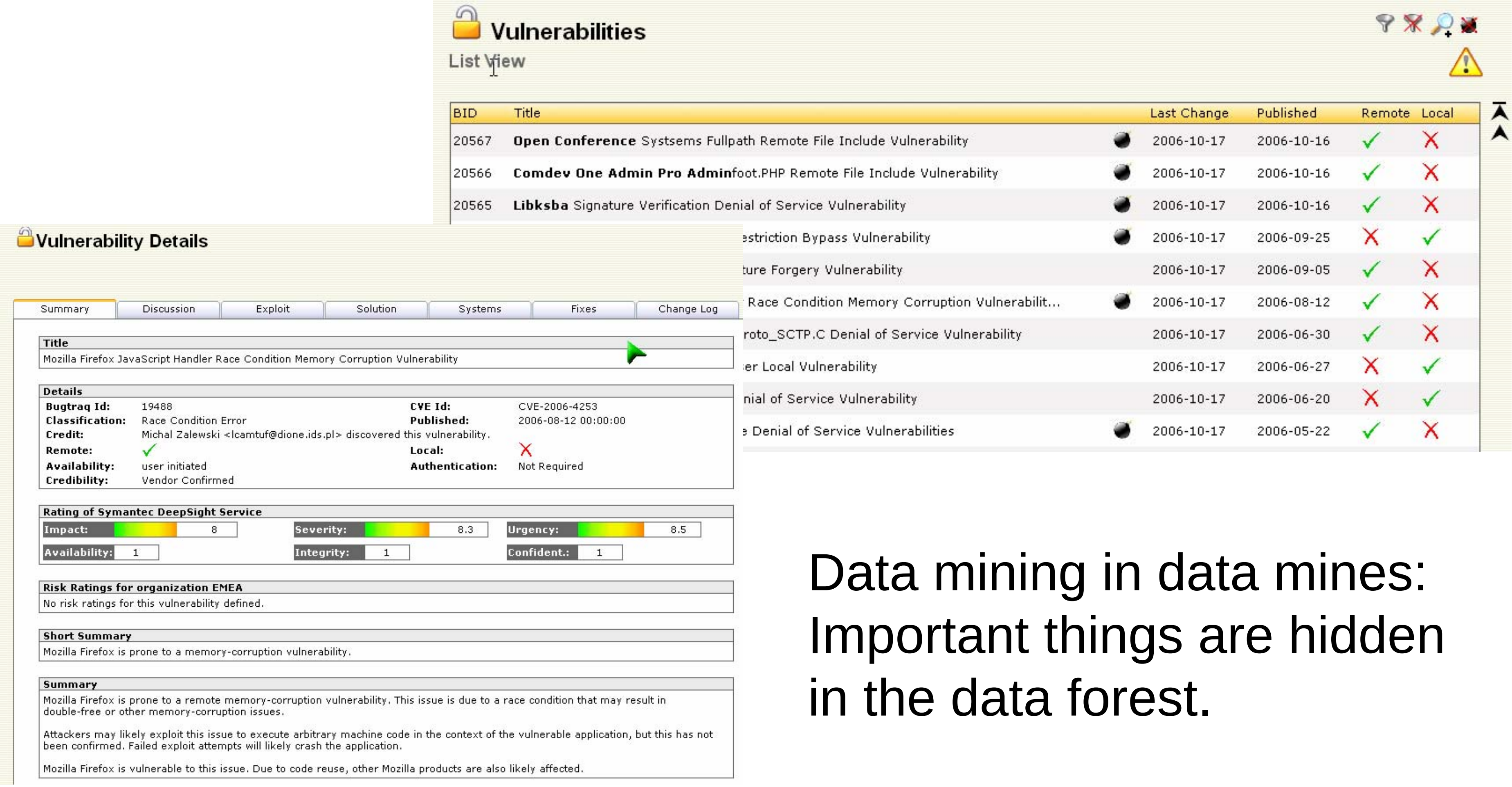
T&V Infobase and portal

Internal process infos and notes

Technical, process related and management reports

*) Linux/Windows, Apache, MySQL, PHP

Get an impression…



Vulnerabilities

List View

BID	Title		Last Change	Published	Remote	Local
20567	**Open Conference** Systsems Fullpath Remote File Include Vulnerability	●	2006-10-17	2006-10-16	✓	✗
20566	**Comdev One Admin Pro Admin**foot.PHP Remote File Include Vulnerability	●	2006-10-17	2006-10-16	✓	✗
20565	**Libksba** Signature Verification Denial of Service Vulnerability	●	2006-10-17	2006-10-16	✓	✗
	estriction Bypass Vulnerability	●	2006-10-17	2006-09-25	✗	✓
	ture Forgery Vulnerability		2006-10-17	2006-09-05	✓	✗
	Race Condition Memory Corruption Vulnerabilit...	●	2006-10-17	2006-08-12	✓	✗
	roto_SCTP.C Denial of Service Vulnerability		2006-10-17	2006-06-30	✓	✗
	er Local Vulnerability		2006-10-17	2006-06-27	✗	✓
	nial of Service Vulnerability		2006-10-17	2006-06-20	✗	✓
	e Denial of Service Vulnerabilities	●	2006-10-17	2006-05-22	✓	✗

Vulnerability Details

Title

Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability

Details

Bugtraq Id:	19488	**CVE Id:**	CVE-2006-4253
Classification:	Race Condition Error	**Published:**	2006-08-12 00:00:00
Credit:	Michal Zalewski <lcamtuf@dione.ids.pl> discovered this vulnerability.		
Remote:	✓	**Local:**	✗
Availability:	user initiated	**Authentication:**	Not Required
Credibility:	Vendor Confirmed		

Rating of Symantec DeepSight Service

Impact:	8	**Severity:**	8.3	**Urgency:**	8.5
Availability:	1	**Integrity:**	1	**Confident.:**	1

Risk Ratings for organization EMEA

No risk ratings for this vulnerability defined.

Short Summary

Mozilla Firefox is prone to a memory-corruption vulnerability.

Summary

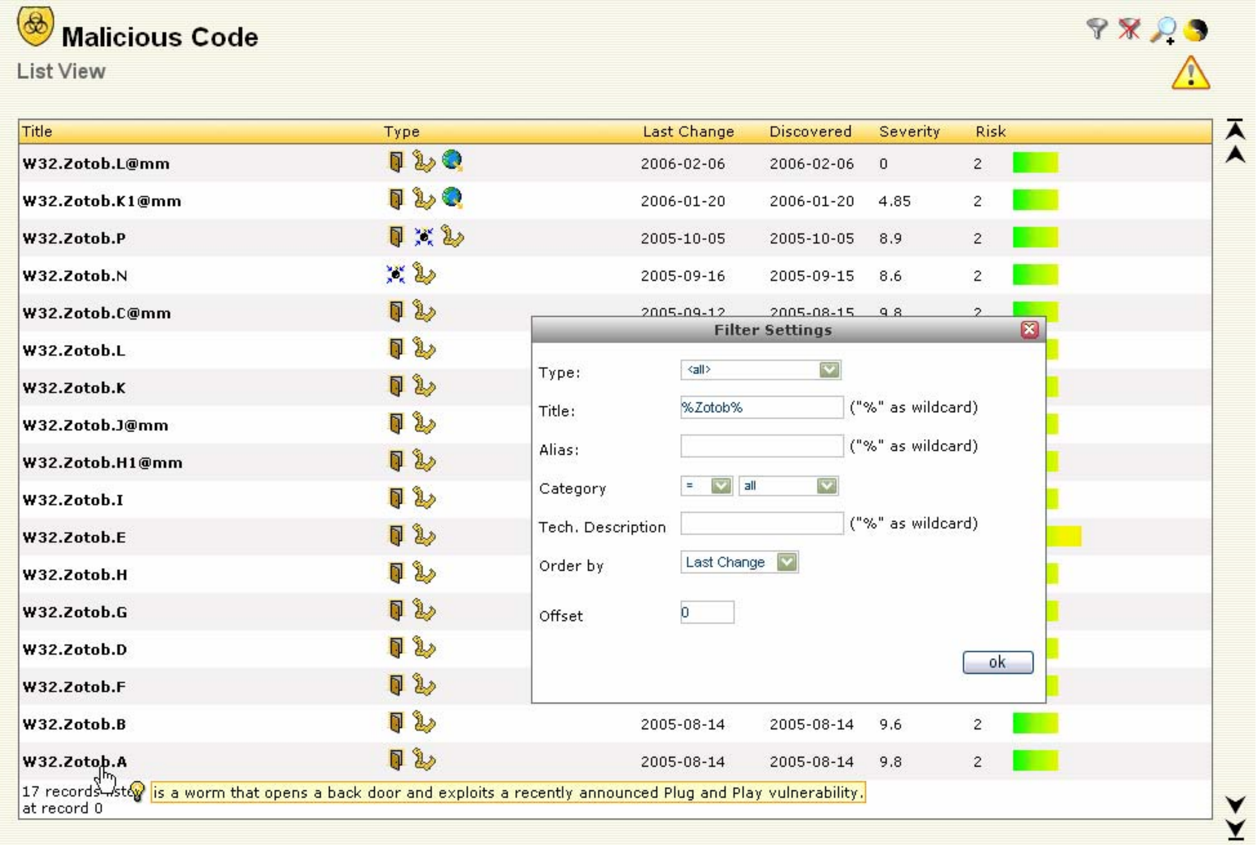
Mozilla Firefox is prone to a remote memory-corruption vulnerability. This issue is due to a race condition that may result in double-free or other memory-corruption issues.

Attackers may likely exploit this issue to execute arbitrary machine code in the context of the vulnerable application, but this has not been confirmed. Failed exploit attempts will likely crash the application.

Mozilla Firefox is vulnerable to this issue. Due to code reuse, other Mozilla products are also likely affected.

Data mining in data mines: Important things are hidden in the data forest.

Get an impression



Malicious Code

List View

Title	Type	Last Change	Discovered	Severity	Risk
W32.Zotob.L@mm		2006-02-06	2006-02-06	0	2
W32.Zotob.K1@mm		2006-01-20	2006-01-20	4.85	2
W32.Zotob.P		2005-10-05	2005-10-05	8.9	2
W32.Zotob.N		2005-09-16	2005-09-15	8.6	2
W32.Zotob.C@mm		2005-09-12	2005-08-15	9.8	2
W32.Zotob.L					
W32.Zotob.K					
W32.Zotob.J@mm					
W32.Zotob.H1@mm					
W32.Zotob.I					
W32.Zotob.E					
W32.Zotob.H					
W32.Zotob.G					
W32.Zotob.D					
W32.Zotob.F					
W32.Zotob.B		2005-08-14	2005-08-14	9.6	2
W32.Zotob.A		2005-08-14	2005-08-14	9.8	2

17 records liste[illegible]

at record 0

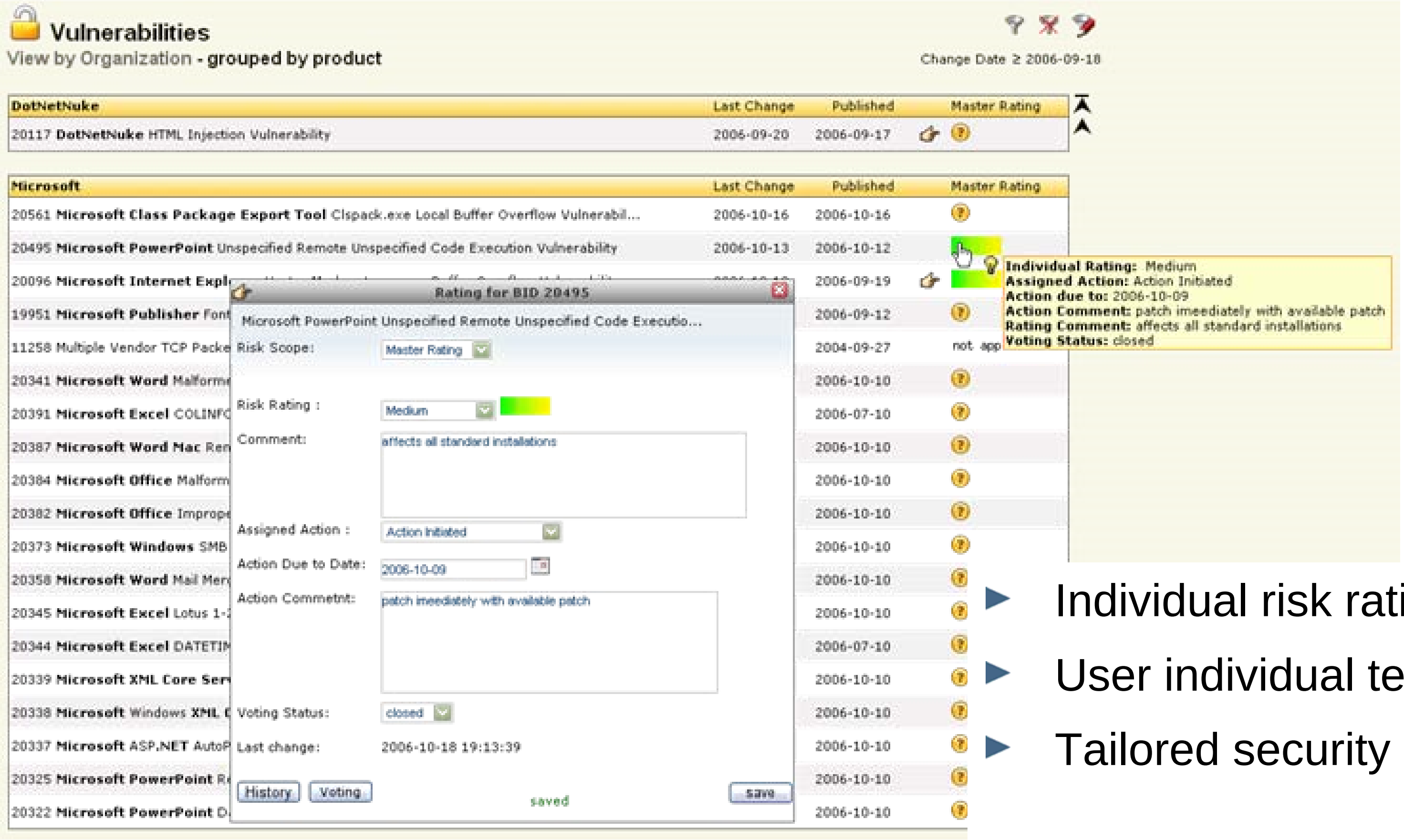
is a worm that opens a back door and exploits a recently announced Plug and Play vulnerability.

Filter Settings

Type:	<all>	
Title:	%Zotob%	("%" as wildcard)
Alias:		("%" as wildcard)
Category	= all	
Tech. Description		("%" as wildcard)
Order by	Last Change	
Offset	0	

Same name, different technology, different risks, different mitigation.

Information on need-to-know basis



Vulnerabilities

View by Organization - grouped by product

Change Date ≥ 2006-09-18

DotNetNuke	Last Change	Published		Master Rating
20117 **DotNetNuke** HTML Injection Vulnerability	2006-09-20	2006-09-17	☞	?

Microsoft	Last Change	Published		Master Rating
20561 **Microsoft Class Package Export Tool** Clspack.exe Local Buffer Overflow Vulnerabil...	2006-10-16	2006-10-16		?
20495 **Microsoft PowerPoint** Unspecified Remote Unspecified Code Execution Vulnerability	2006-10-13	2006-10-12		🟩
20096 **Microsoft Internet Expl**		2006-09-19	☞	🟩
19951 **Microsoft Publisher** Font		2006-09-12		?
11258 Multiple Vendor TCP Packe		2004-09-27		not app
20341 **Microsoft Word** Malforme		2006-10-10		?
20391 **Microsoft Excel** COLINFC		2006-07-10		?
20387 **Microsoft Word Mac** Ren		2006-10-10		?
20384 **Microsoft Office** Malform		2006-10-10		?
20382 **Microsoft Office** Imprope		2006-10-10		?
20373 **Microsoft Windows** SMB		2006-10-10		?
20358 **Microsoft Word** Mail Merg		2006-10-10		?
20345 **Microsoft Excel** Lotus 1-2		2006-10-10		?
20344 **Microsoft Excel** DATETIM		2006-07-10		?
20339 **Microsoft XML Core Serv**		2006-10-10		?
20338 **Microsoft** Windows **XML C**		2006-10-10		?
20337 **Microsoft ASP.NET** AutoP		2006-10-10		?
20325 **Microsoft PowerPoint** R		2006-10-10		?
20322 **Microsoft PowerPoint** D		2006-10-10		?

Individual Rating: Medium
Assigned Action: Action Initiated
Action due to: 2006-10-09
Action Comment: patch imeediately with available patch
Rating Comment: affects all standard installations
Voting Status: closed

Rating for BID 20495

Microsoft PowerPoint Unspecified Remote Unspecified Code Executio...

Risk Scope: Master Rating

Risk Rating : Medium

Comment: affects all standard installations

Assigned Action : Action Initiated

Action Due to Date: 2006-10-09

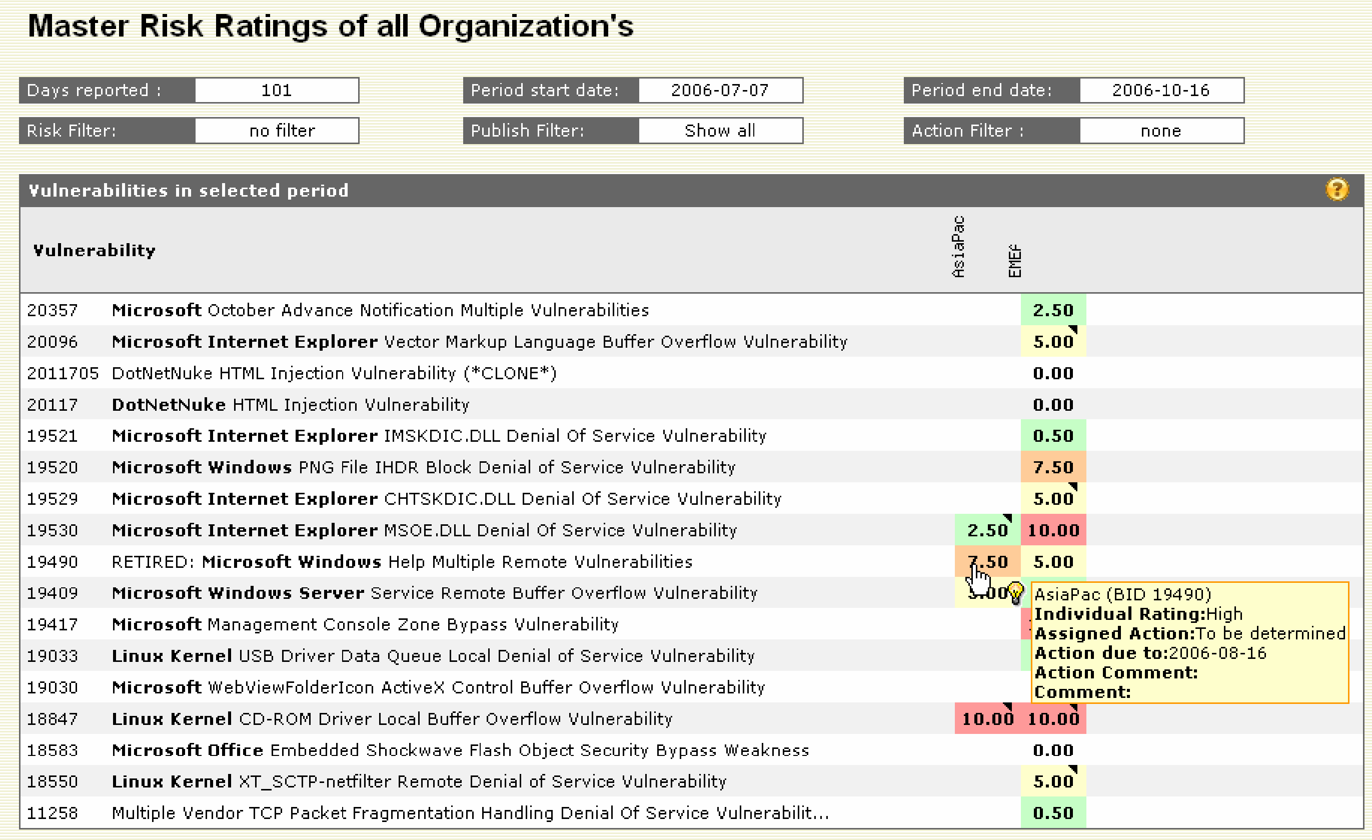
Action Commetnt: patch imeediately with available patch

Voting Status: closed

Last change: 2006-10-18 19:13:39

- Individual risk ratings by CERT
- User individual technology filters
- Tailored security advisories

Get an impression



Master Risk Ratings of all Organization's

Days reported :	101	Period start date:	2006-07-07	Period end date:	2006-10-16
Risk Filter:	no filter	Publish Filter:	Show all	Action Filter :	none

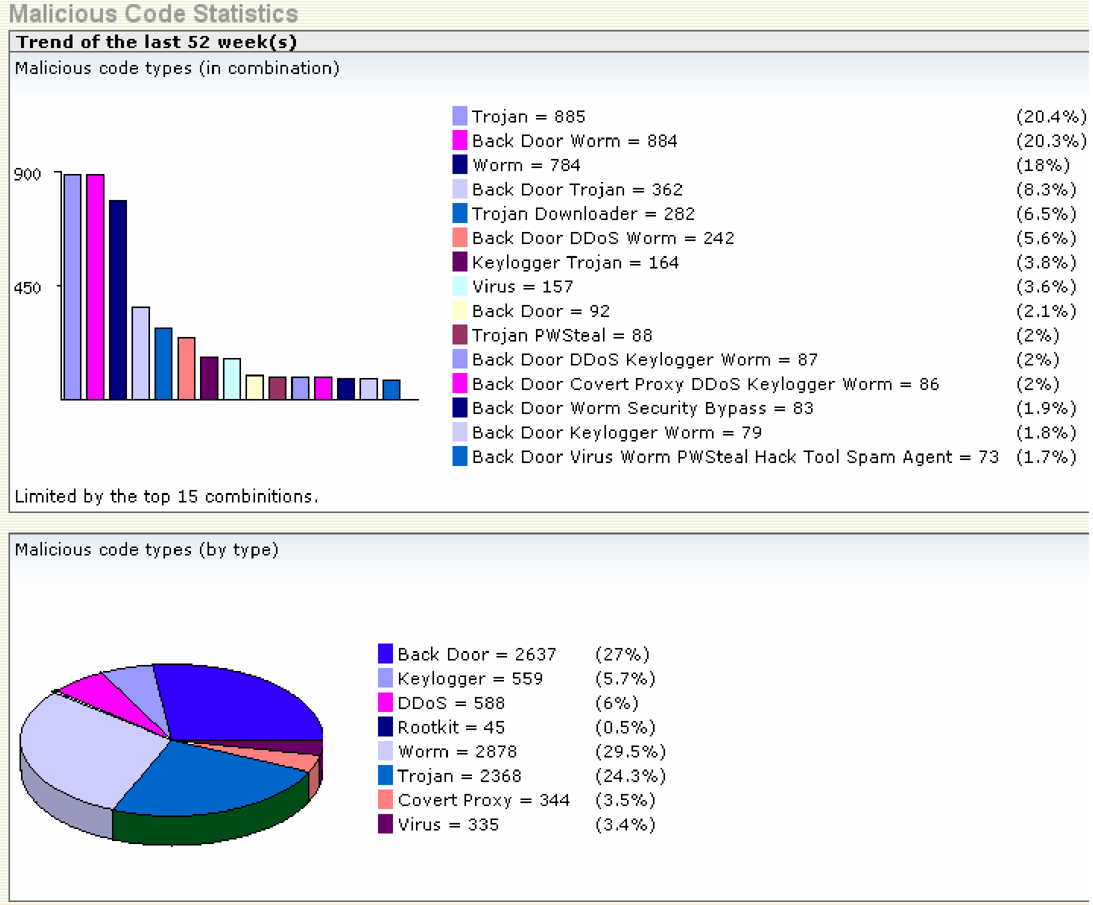
Vulnerabilities in selected period

Vulnerability		AsiaPac	EMEA
20357	**Microsoft** October Advance Notification Multiple Vulnerabilities		2.50
20096	**Microsoft Internet Explorer** Vector Markup Language Buffer Overflow Vulnerability		5.00
2011705	DotNetNuke HTML Injection Vulnerability (*CLONE*)		0.00
20117	**DotNetNuke** HTML Injection Vulnerability		0.00
19521	**Microsoft Internet Explorer** IMSKDIC.DLL Denial Of Service Vulnerability		0.50
19520	**Microsoft Windows** PNG File IHDR Block Denial of Service Vulnerability		7.50
19529	**Microsoft Internet Explorer** CHTSKDIC.DLL Denial Of Service Vulnerability		5.00
19530	**Microsoft Internet Explorer** MSOE.DLL Denial Of Service Vulnerability	2.50	10.00
19490	RETIRED: **Microsoft Windows** Help Multiple Remote Vulnerabilities	7.50	5.00
19409	**Microsoft Windows Server** Service Remote Buffer Overflow Vulnerability	5.00	[illegible]
19417	**Microsoft** Management Console Zone Bypass Vulnerability		[illegible]
19033	**Linux Kernel** USB Driver Data Queue Local Denial of Service Vulnerability		[illegible]
19030	**Microsoft** WebViewFolderIcon ActiveX Control Buffer Overflow Vulnerability		[illegible]
18847	**Linux Kernel** CD-ROM Driver Local Buffer Overflow Vulnerability	10.00	10.00
18583	**Microsoft Office** Embedded Shockwave Flash Object Security Bypass Weakness		0.00
18550	**Linux Kernel** XT_SCTP-netfilter Remote Denial of Service Vulnerability		5.00
11258	Multiple Vendor TCP Packet Fragmentation Handling Denial Of Service Vulnerabilit...		0.50

AsiaPac (BID 19490)
Individual Rating: High
Assigned Action: To be determined
Action due to:2006-08-16
Action Comment:
Comment:

Need of well coordinated actions in a connected world.

New threat scenario



Malicious Code Statistics

Trend of the last 52 week(s)

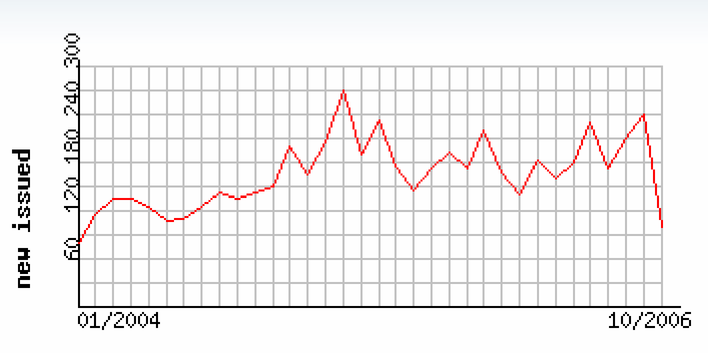
Malicious code types (in combination)

Trojan = 885	(20.4%)
Back Door Worm = 884	(20.3%)
Worm = 784	(18%)
Back Door Trojan = 362	(8.3%)
Trojan Downloader = 282	(6.5%)
Back Door DDoS Worm = 242	(5.6%)
Keylogger Trojan = 164	(3.8%)
Virus = 157	(3.6%)
Back Door = 92	(2.1%)
Trojan PWSteal = 88	(2%)
Back Door DDoS Keylogger Worm = 87	(2%)
Back Door Covert Proxy DDoS Keylogger Worm = 86	(2%)
Back Door Worm Security Bypass = 83	(1.9%)
Back Door Keylogger Worm = 79	(1.8%)
Back Door Virus Worm PWSteal Hack Tool Spam Agent = 73	(1.7%)

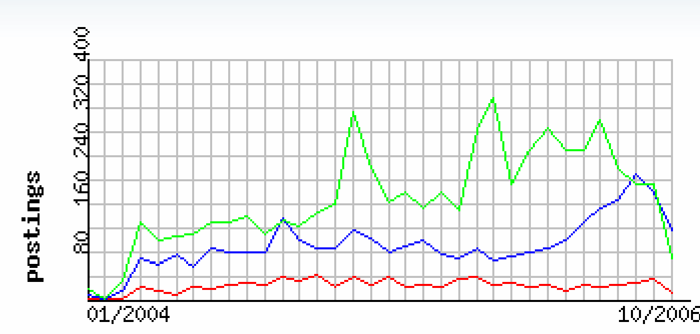
Limited by the top 15 combinitions.

Malicious code types (by type)

Back Door = 2637	(27%)
Keylogger = 559	(5.7%)
DDoS = 588	(6%)
Rootkit = 45	(0.5%)
Worm = 2878	(29.5%)
Trojan = 2368	(24.3%)
Covert Proxy = 344	(3.5%)
Virus = 335	(3.4%)



Malicious Codes

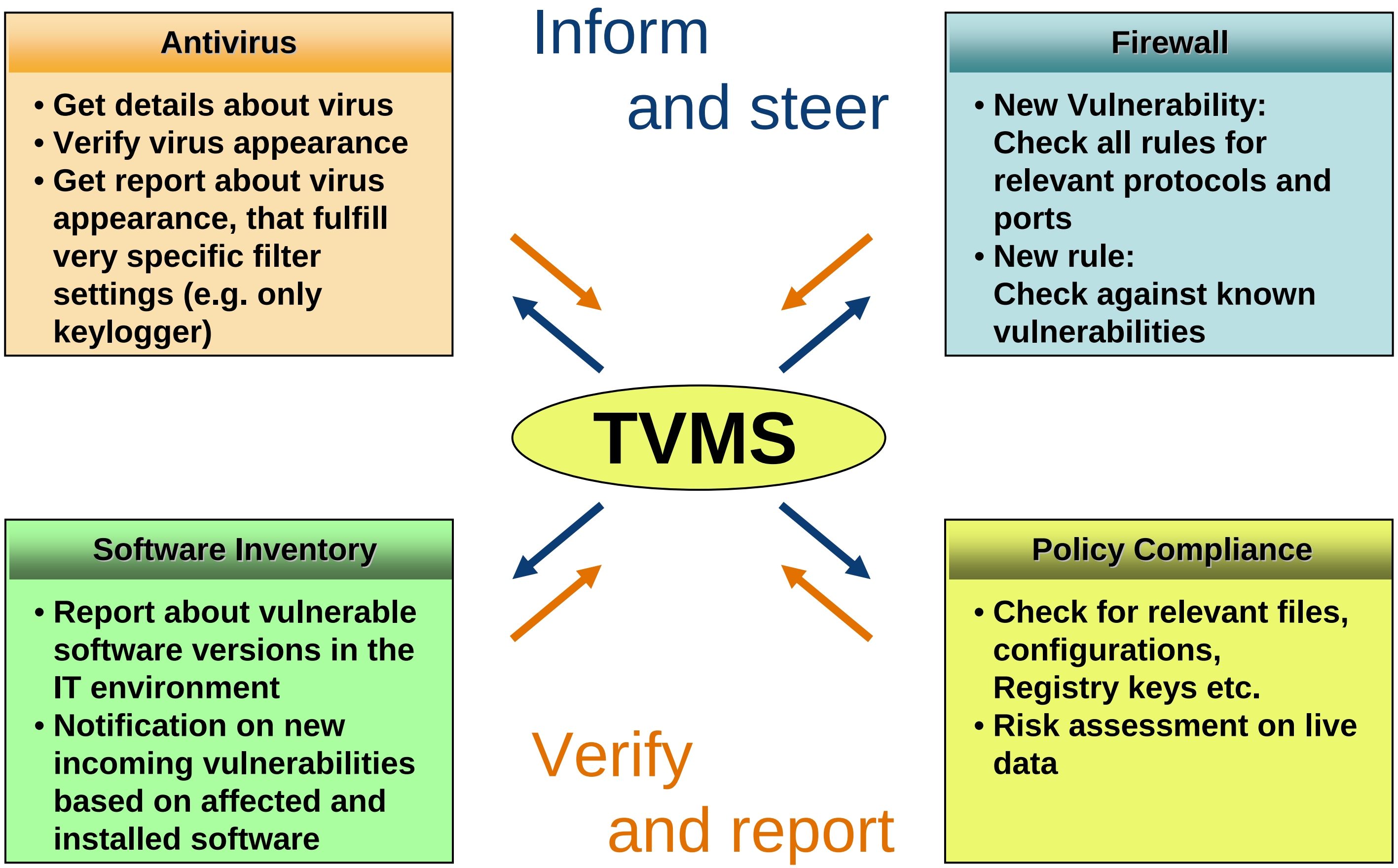


New Vuln. by Impact

Legend:

RED: High Risk [9 ≤ Impact/Severity ≤ 10]
BLUE: Medium Risk [6 ≤ Impact/Severity < 9]
GREEN: Low Risk [Impact/Severity < 6]

Vision



Antivirus

- Get details about virus
- Verify virus appearance
- Get report about virus appearance, that fulfill very specific filter settings (e.g. only keylogger)

Inform

and steer

Firewall

- New Vulnerability: Check all rules for relevant protocols and ports
- New rule: Check against known vulnerabilities

TVMS

Software Inventory

- Report about vulnerable software versions in the IT environment
- Notification on new incoming vulnerabilities based on affected and installed software

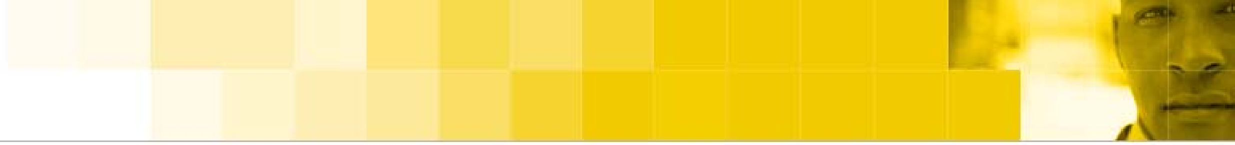
Verify

and report

Policy Compliance

- Check for relevant files, configurations, Registry keys etc.
- Risk assessment on live data

…Intrusion Detection, Log Analysis, etc.

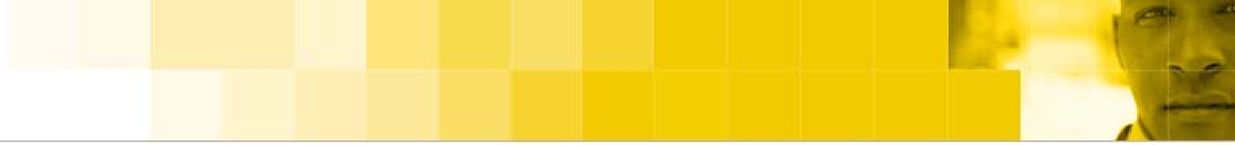


How Incident Management profits from this

- Good TVM → minimized risk → less incidents

- In case of an incident, useful information is available immediately:
  → technical background information
  → fine-tuning of security policies and compliance tools
  → who is potentially affected?
  → who are the people that need to involved in the mitigation?
  → who is protected and who isn't?
  → what is the situation outside of our organization?
  → etc.

- Combined managent systems data (Policy Compliance, TVM, IM, Risk Management, SD, AV, FW etc.) allows to generate high level risk reports to the management
  → Key Performance Indicators, Key Risk Indicators



Success factors

What are the key success factors to build successful processes?

Some tips…

Realize risk in a connected world

Built processes and solutions that are mature.

Processes needs to be understandable, accepted and proven.

Realize that security is a speed game.

Proactive and reactive processes are worthless if they are too slow!

Build effective processes that people understand

Build the right teams - find the right partners.

Thank you very much