



Threat Response - Doing the right thing first time

Greg Day

Principal security analyst EMEA

AVERT Member

July 28, 2009



How many of you are watching this

McAfee

CNN INTERNATIONAL
com/technology

POWERED BY Google

HOME ASIA EUROPE U.S. WORLD WORLD BUSINESS **TECHNOLOGY** ENTERTAINMENT WORLD SPORT TRAVEL

ON TV VIDEO

Hot Topics » [Style and Design](#) » [Planet In Peril](#) » [Eco Solutions](#) » [iPhone](#) » [Digital Biz](#) » more topics »

Weather Forecast Edi

MIX SHARE EMAIL SAVE PRINT


Jackson dies, almost takes Internet with him

June 26, 2009 – Updated 1902 GMT (0302 HKT)

READ VIDEO INTERACTIVE TIMELINE

By Linnie Rawlinson and Nick Hunt
CNN

LONDON, England (CNN) -- How many people does it take to break the Internet? On June 25, we found out it's just one -- if that one is Michael Jackson.



The biggest showbiz story of the year saw the troubled star take a good slice of the Internet with him, as the ripples caused by the news of his death swept around the globe.

"Between approximately 2:40 p.m. PDT and 3:15 p.m. PDT today, some Google News users experienced difficulty accessing search results for queries related to Michael Jackson," a Google spokesman told CNET, which also reported that Google News users complained that the service was inaccessible for a time. At its peak, Google

OLED LIGHTING: A LAYER OF LIGHT
**NEW LIGHT,
NEW LIFE.**
TOP DESIGNERS IMAGINE FUTURE
USES FOR OLED LIGHTING
[CLICK HERE](#)

- When does it become an incident?

By The End of 2008



	1997	End of 2007	End of 2008
Vulnerabilities	440	38,500	34,100
Password Steal (Main variants)	4,000	100,000	380,000
Potentially Unwanted Programs	10,000	24,000	26,000
Malware (family) (DAT related)	17,000	358,000	484,000
Malware (main variants)	18,000 (?)	586,000	2,700,000
Malware Zoo (Collection)	30,000 (?)	5,800,000	16,300,000

5791 per day!

We can no longer afford to clean up after the incident...

McAfee

The screenshot shows the BBC News website interface. At the top left is the BBC logo with 'Low graphics' and 'Help' links. A search bar is on the top right. The main header features the word 'NEWS' and a 'Watch ONE-MINUTE WORLD NEWS' button. Below the header, a navigation menu on the left lists various news categories: News Front Page, Africa, Americas, Asia-Pacific, Europe, Middle East, South Asia, UK, Business (highlighted), Market Data, Economy, Companies, Health, Science & Environment, Technology, and Entertainment. The main content area shows a news article titled 'Pension details of 109,000 stolen'. The article text states that a laptop with pension details for 109,000 members of six schemes was stolen from offices in Marlow, Buckinghamshire, on March 23. The data was protected by a password but not encrypted. An image shows a person's hands holding a laptop. The article also mentions that the theft has been reported to the police and is part of a long line of similar cases.

How many of you were monitoring – Nirbot.worm?



Exploits

- Microsoft Windows Server Service Buffer Overflow (MS06-040)
- Symantec Client Security and Symantec Antivirus Elevation of privilege vulnerability (SYM06-010)

Can:

- Gather system information (CPU, RAM, OS Version, IP address, UserName, Uptime)
- Scan network for machines to infect.
- Launch a TFTP, HTTP server and SOCKS4 proxy.
- Download and Execute files.
- Update bot.
- Uninstall bot.

```
mIRC - [##OC [2]: .scan.stats]
File View Favorites Tools Commands Window Help
@Avert
[2K|USA|P|00|UbaKfh20]
* Now talking in ##OC
<Avert> Me logged in as channel operator
and waiting for the bot to connect.
* [2K|USA|P|00|UbaKfh20] has joined ##OC
* Retrieving ##OC modes...
<Avert> The bot has joined in. I'm gonna
pass some sample commands
* Avert changes topic to '.sysinfo'
<[2K|USA|P|00|UbaKfh20]> System: [OS:
Microsoft Windows 2K Service Pack 4
(5.0 build 2195)] [CPU: 1 x Intel(R)
Xeon(TM) CPU 2.40GHz @ 2392Mhz] [RAM:
83MB/255MB] [Country: United States]
[IP: 192.168.1.59] [User: Administrator
] [System Dir: C:\WINNT\system32]
[Uptime: 0d 1h 19m]
* Avert changes topic to '.netinfo'
* [2K|USA|P|00|UbaKfh20] was kicked by
<[2K|USA|P|00|UbaKfh20]> Net: IP:
192.168.1.59 Host: VinooUM2000
* Avert changes topic to '.scan.stats'
<[2K|USA|P|00|UbaKfh20]> Statistics:
Exploits: N: 0 M: 0 S: 0; Daemons:
TFTP: 0 HTTP: 0
```

How many of you were monitoring Conficker.worm?



The screenshot shows a web browser window with a news article. The article title is "French airforce surrenders to German virus". Below the title is a social media sharing bar with icons for various platforms and a "0 tweet" button. The main image shows two Rafale fighter jets in flight. The text of the article describes how the Conficker worm caused the French air force to ground its aircraft in January. It mentions that the aircraft were unable to download flight plans because their databases were infected by a Windows virus. The article also notes that the Conficker worm spread worldwide last year, and that Microsoft warned of the risks, but that an adequate defense against the virus with a patch followed standard French military procedure, which either didn't happen or wasn't done properly. The article concludes by stating that the worst hit were the Villacoublay air base and the 8th Transmissions Regiment, along with the French Navy's entire fleet of Rafale aircraft.

French airforce surrenders to German virus

0 tweet



French fighter planes were grounded in January due to a computer virus.

According to an unnamed Intelligence Magazine quoted by the Telegraph, the aircraft were unable to download their flight plans after databases were infected by a Windows virus. Apparently it was worse for Naval staff, who were instructed to surrender using their computers in case the virus spread.

The Conficker worm started to spread world wide last year, and Microsoft warned of the risks, but apparently mounting an adequate defense against the virus with a patch followed standard French military procedure, and either didn't happen, or just wasn't done properly.

Worst hit were the Villacoublay air base and in the 8th Transmissions Regiment, along with the French Navy's entire fleet of Rafale aircraft.

Internet 100%

Threat Incident response



- When is the right time to engage?
 - On industry/vendor advisory?
 - On business incident?
 - On technology alerts?
 - Real time events
 - Log analytics
- Reactive or proactive
 - On vulnerability?
 - On Exploit?
 - On threat?
 - On data breach?



You receive alerts/advisories like these...



(MS08-067) Microsoft Windows Server Service Vulnerability	
Threat Identifier(s)	CVE-2008-4250;MS08-067
Threat Type	Vulnerability
Risk Assessment	Critical
Main Threat Vectors	LAN; WAN; Web
User Interaction Required	No
Description	A vulnerability exists in Microsoft Windows Server Service that allows for remote code execution through the handling of specially-crafted requests. In a successful attack scenario, an attacker could gain control of a target system. This vulnerability is currently being exploited by malware.
Importance	High. Critical. On October 23, 2008, Microsoft released the issue.
McAfee Product Coverage *	
DAT files	The scan engine does not scan the vulnerable component. Coverage is provided as Spy-Agent.da in the 5444 DAT files, released November 24, 2008.
VSE BOP	Generic Buffer Overflow Protection is expected to cover code-execution exploits.
Host IPS	Buffer overflow protection is expected to cover code-execution exploits. An updated signature specifically address the MS08-067 vulnerability.
IntruShield	Existing signature 0x4760 can detect some of the known exploits. Starting 23rd Oct 2008, (0x40709d) Remote Code Execution Vulnerability can detect possible future variants of this exploit.
Foundstone	The FSL package of October 23, 2008, assess if your systems are vulnerable.
MNAC	The MNAC package of October 23, 2008, assess if your systems are vulnerable.
V-Flash	The V-Flash of October 24, 2008, assess if your systems are vulnerable.
Additional Information	McAfee Threat Center: [MS08-067] Microsoft Windows Server Service Vulnerability [95864]

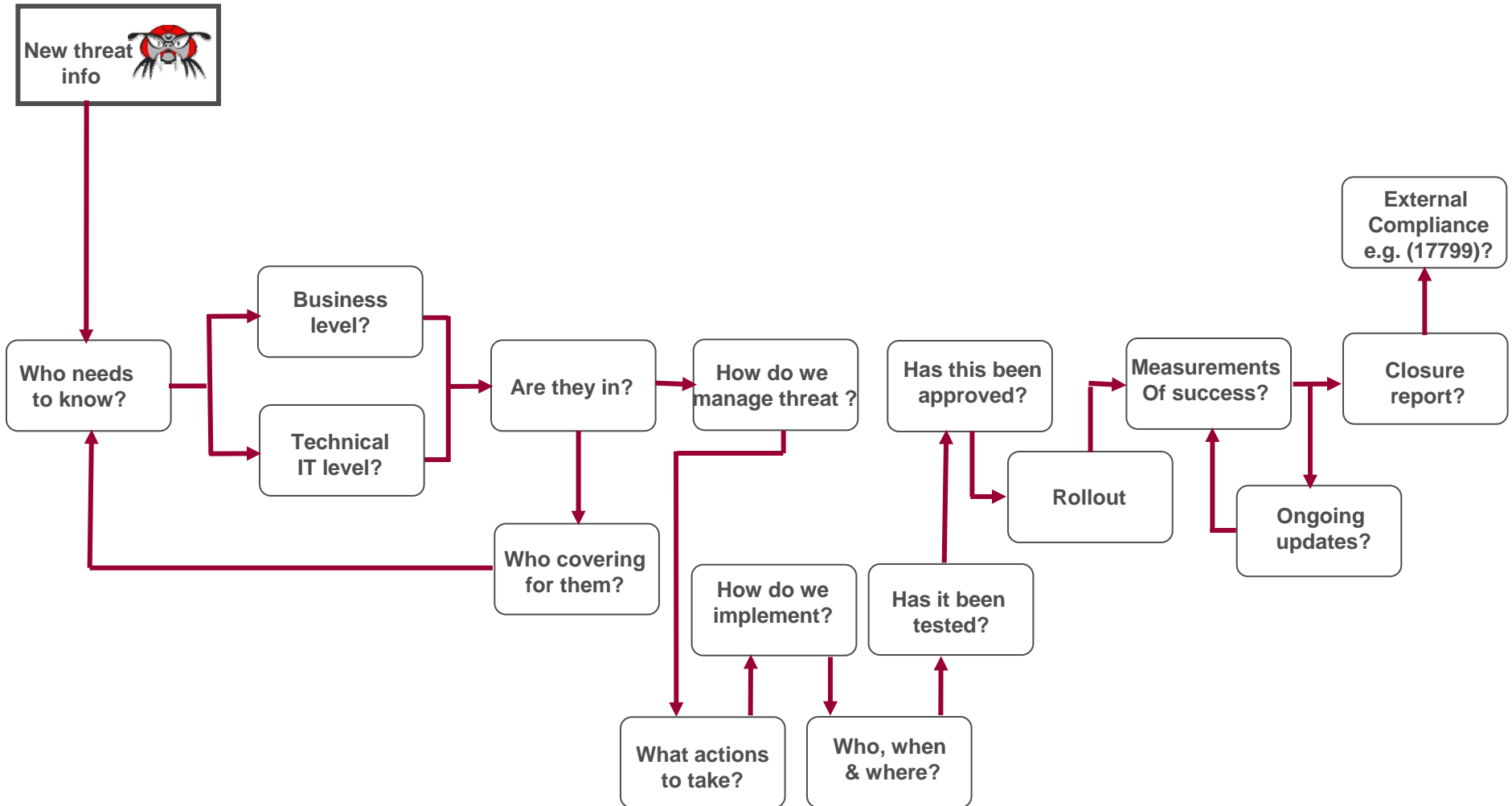
W32/Conficker.worm		[MTIS09-003-A]
Threat Identifier(s)	W32/Conficker.worm	
Threat Type	Malware	
Risk Assessment	Low	
Main Threat Vectors	LAN; WAN; Web	
User Interaction Required	Yes	
Description	The W32/Conficker worm exploits the MS08-067 vulnerability, in Microsoft Windows Server Service. Machines should be patched and rebooted to protect against this worm's reinfecting the system after cleaning, which may require more than one reboot. Scheduled tasks and autorun.inf files have been seen to reactivate the worm.	
Importance	Low. W32/Conficker.worm exploits the MS08-067 vulnerability.	
McAfee Product Coverage *		
DAT files	Coverage was provided in the 5444 DAT files, released November 24, 2008 . Detection and repair was updated in the 5488 DAT files, released January 7 . (Users infected by W32/Conficker.worm should perform an On Demand Scan to remove remnants of the worm in memory using the latest DATs. After detection of W32/Conficker!mem and rebooting, the W32/Conficker.worm malware components will be removed.)	
VSE BOP	Buffer overflow protection is expected to cover code-execution exploits.	
Host IPS	Generic Buffer Overflow is expected to cover code-execution exploits. "Windows Server Service Buffer Overflow Vulnerability (Tighter Security)," Signature 3768, can provide partial coverage. Signature 3961, released October 28, 2008, will block denial-of-service and code-execution exploits associated with MS08-067.	
IntruShield	The sigset release of October 23, 2008, includes the signature "NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability," which provides coverage.	
Foundstone	Coverage not warranted at this time	
MNAC	Coverage not warranted at this time	
V-Flash	Out of scope	
Additional Information	McAfee VIL: W32/Conficker.worm McAfee VIL: MS08-067 - Microsoft Windows Server Service Vulnerability - 958644	

Which should lead to questions like these...

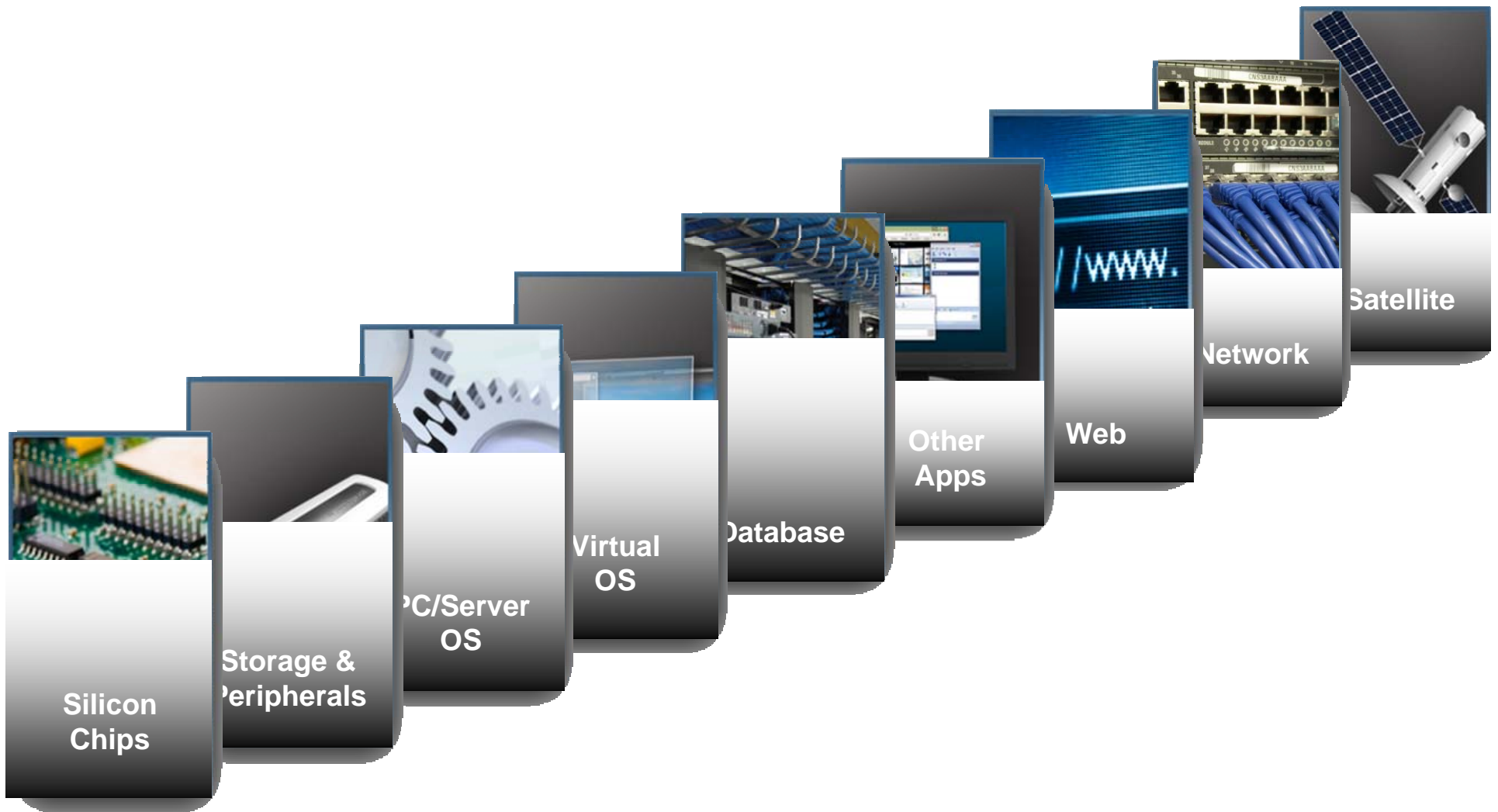


- What is the threat?
- Is it real or theoretical?
- What could the threat do?
- What would it actually do to my business?
- How would that impact my business?
- How likely is it to happen?
- What countermeasures do I have in place?
- Which countermeasures should I enable?
- What order should I enable them in?
- What impact will these have on my business?

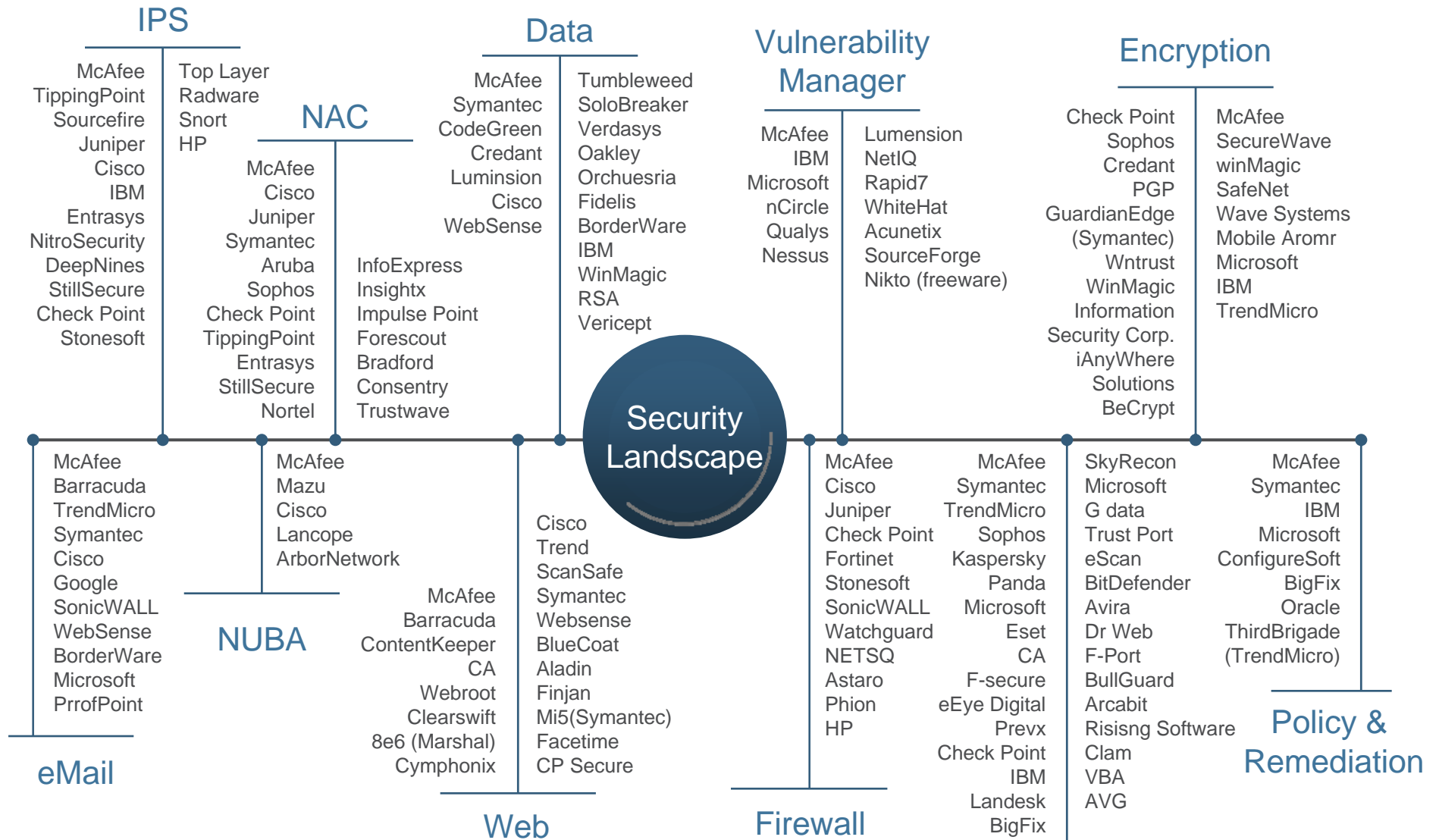
Which instigate something level of incident response like this...



To answer we have to correlate Multi-Layered Intelligence: from Silicon to Satellite



Utilising some of these vendors



Which makes Coordinating the response?

McAfee



To summarise the issues



When does a threat become an incident?

- No single point of threat/risk measurement
- Lack of correlation to the business risk
- Lack of correlation between risk and mitigation tools
 - Have I already solved the problem?

How do I decide when to act?

- Often many - if not all security solutions can have some involvement
 - What is the right solution to apply?
- Should I apply the same solution across the business?
- How do I validate the problem is solved?
 - Too many security consoles
- Have I already solved the problem

So what the problem???

McAfee



We need Smarter Intelligence!

Time to change our approach! Multi-Correlated: Centralized Intelligence

McAfee



How – An “Optimized” Security Architecture?



Security Maturity Model

Reactive	Compliant	Proactive	Optimized
<ul style="list-style-type: none">/ Event driven/ Reactive protection/ Basic security	<ul style="list-style-type: none">/ Policy development/ Some standardization/ External compliance met	<ul style="list-style-type: none">/ Proactive security/ Centralized view/ Security enables compliance/ Audit once, report many/ More integration	<ul style="list-style-type: none">/ Multi-layered, Multi-correlated/ Global threat intelligence/ Automated compliance/ Opex efficiencies

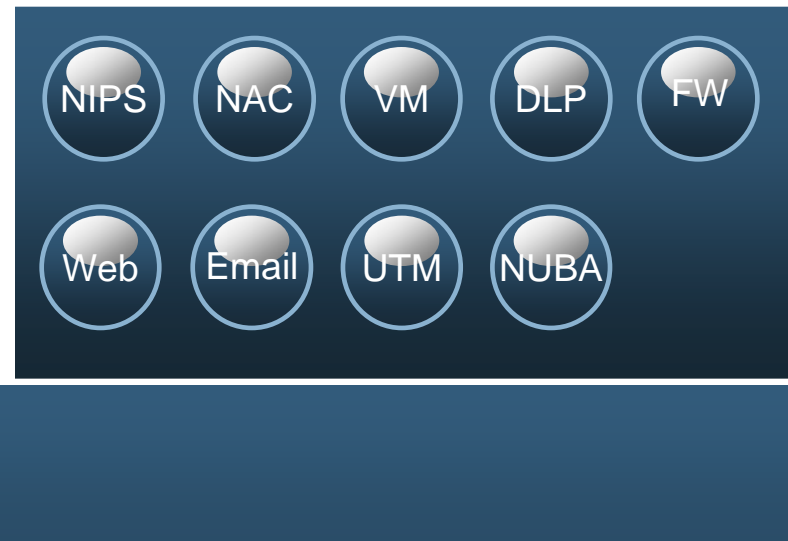
Integrate and correlate our Multi-layered Defense



System



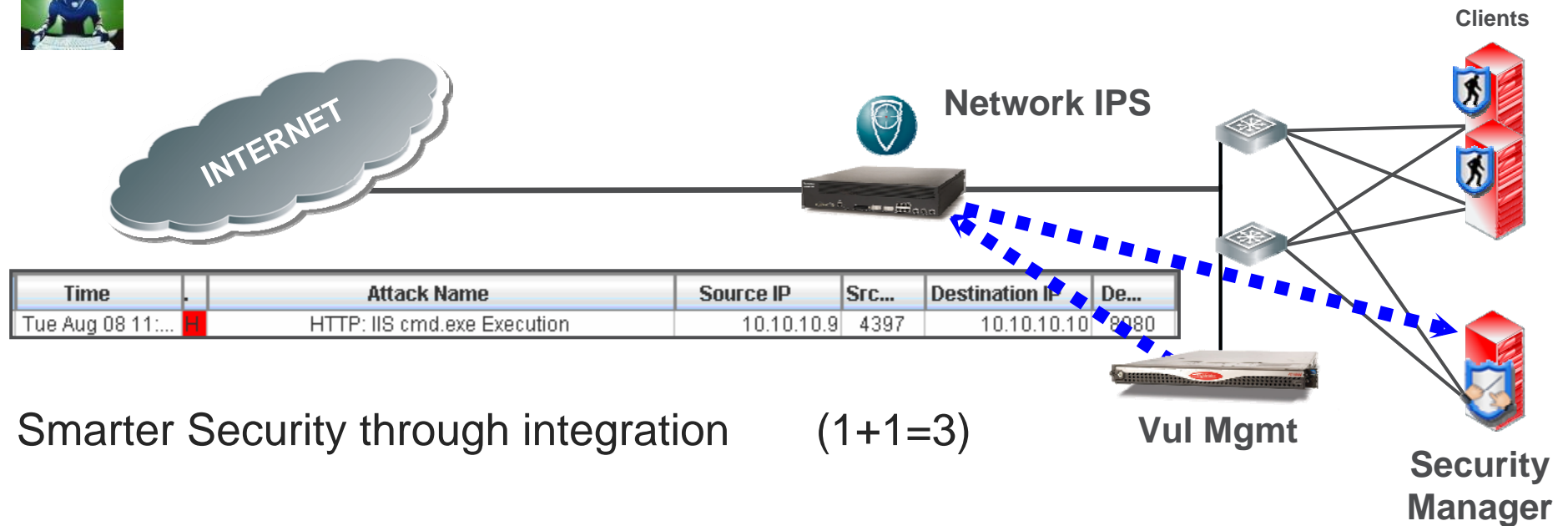
Network



Gathering all the facts



Q: Traffic from the **INTERNET** going to **YOUR WEBSERVER** contains a **RELEVANT Web ATTACK**, but the **SERVER HAS LOCAL PROTECTION TO STOP IT**,
 Q: Traffic from **X** going to **Y** contains a potential Web server threat?
 What should I do?
 I don't need to do anything!



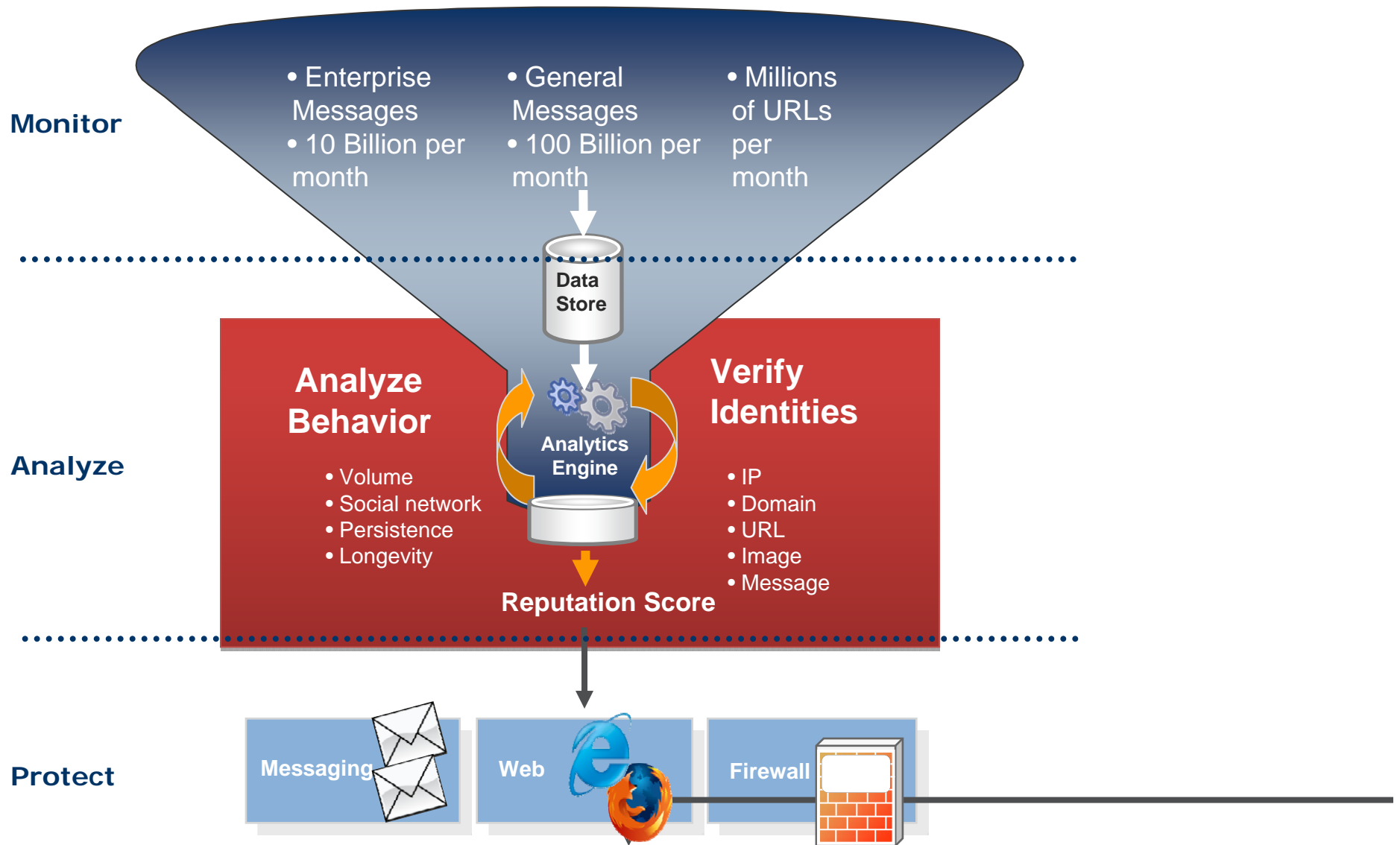
Collaborative Real time intelligence



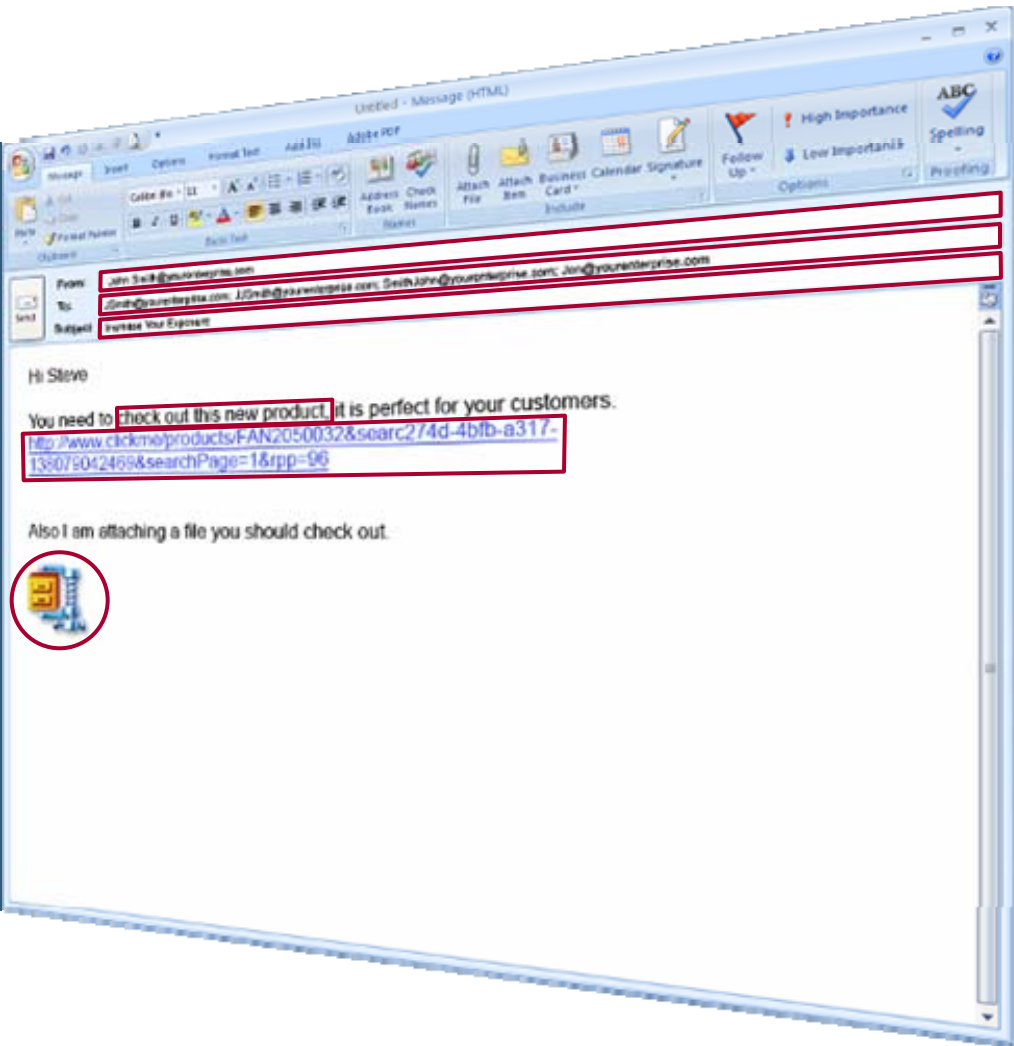
Shared view of the problem – Cloud based intelligence



Is it from a Trusted Source?

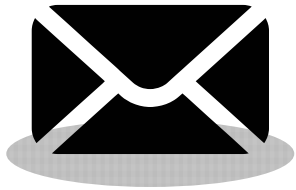


- Sender
- Recipient
- Subject
- Keyword
- Hyperlink
- Attached File



Content-Based

**SUSPICIOUS
MESSAGE**



Content-Based



209.85.171.100

IP Monitoring



Domain Registry



Multiple Queries

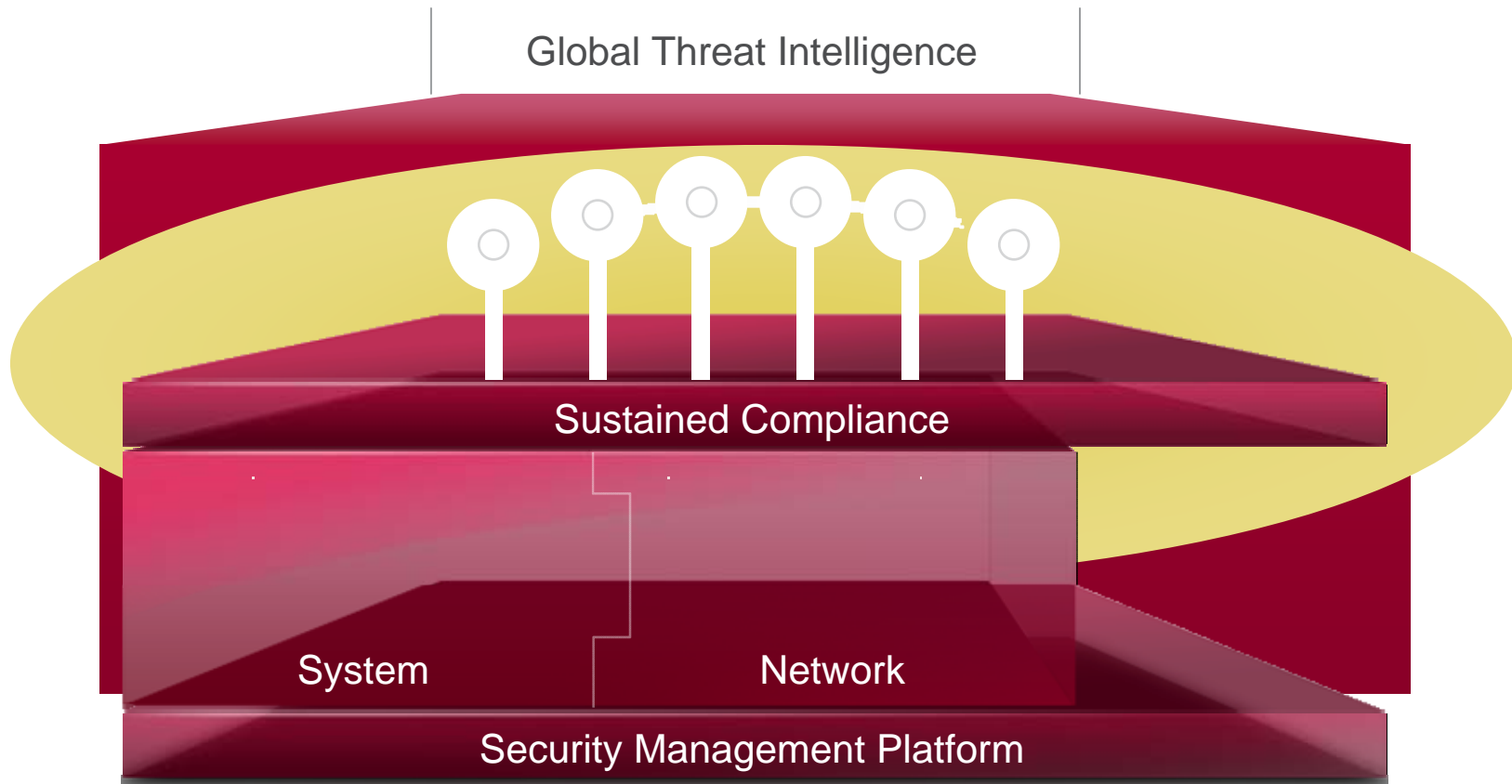
Single point of visibility



An Optimized Security Architecture

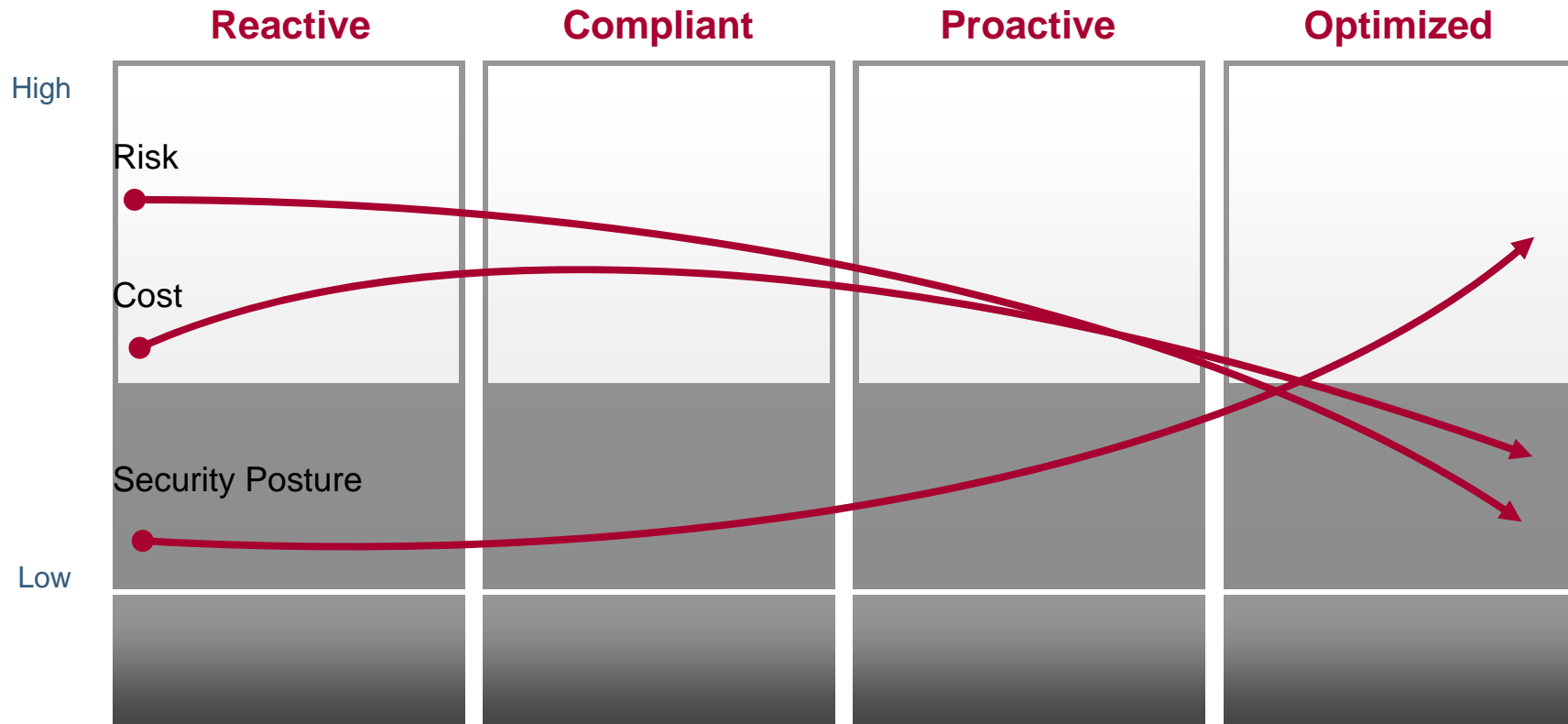


An Optimized Security Architecture – Must scale beyond individual vendors





Maturity Model of Enterprise Security



The next level: Optimized Security Architecture leads to CARMA



McAfee Avert® Labs
Security Threat Advisory

October 25, 2008

Executive Summary
Since the last McAfee® Avert® Labs Security Advisory (October 28), the following noteworthy event has taken place:

- McAfee product coverage has been updated for a critical Microsoft Windows vulnerability.

McAfee product coverage for this event:

McAfee Product Coverage Updates *									
Threat	Advisory	Importance	DAT	BOF	Host IPS	Intrusion Shield	Foundstone	HNAC	V-Flash
HTS08-182-A	Previous	High	N/A	Exp	Pend	Yes	Yes	Yes	Yes
MS08-067 sv	Current	High	N/A	Exp	Yes	Yes	Yes	Yes	Yes
(MS08-067) Microsoft Windows Server Service Vulnerability (998644) [HTS08-182-A]									

Threat Identifier(s): CVE-2008-4250;MS08-067

Vulnerability: Vulnerability

Risk Assessment: Critical

Main Threat Vectors: LAN; WAN; Web

User Interaction Required: No

Description: A vulnerability in Microsoft Windows Server Service could allow for remote code execution. The flaw lies in the improper handling of maliciously crafted RPC requests. Exploitation could allow an attacker to take full control of a target system. This threat is currently being exploited by malware.

Importance: High. On October 23, Microsoft released a patch that fixes the issue.

McAfee Product Coverage *

DAT files: The scan engine does not reside between the attack vector and the vulnerable component. Coverage for observed payloads is provided as SpyAgent.da in the 5414 DAT files, released October 23.

VSE BOF: Generic buffer overflow protection is expected to cover future code-execution exploits.

Host IPS: Generic buffer overflow protection is expected to cover future code-execution exploits. Signature 3768, "Windows Server Service Buffer Overflow Vulnerability (Tighter Security)," provides coverage for known code-execution exploits. Signature 3961, released on October 26, blocks denial-of-service and code-execution exploits associated with MS08-067.

IntrusionShield: Signature "0x47602b00 DCERPC: SRV/SVC Buffer Overflow" can detect some of the known attacks. Signature "0x40708600 NETBIOS-S:" Microsoft Server Service Remote Code Execution Vulnerability," released

Server: mcafee-ssharma | Time: 5/5/08 4:44 PM PST | User: ga

McAfee Orion Platform

Countermeasure Aware Information

Threat Details

Threat Information

Name: (MS08-001) Microsoft Data Stream Handling Memory Corruption Vulnerability (947664)

Description: A vulnerability is present in Microsoft Internet Explorer that may allow for arbitrary code execution.

Countermeasures: VIL, HIP, VSE, .S, Foundstone

Reported Date: 4/8/08 6:03:44 PM

Attack Vector: Website with malicious content

Level: 0

Severity: Critical

Vendor Ratings: Critical

Ports

Countermeasures

Product

VIL (Vendor: mcafee, Engine Version: 5.1)

HIP (Vendor: mcafee, Product Version: 7.0, Engine Version: 2.0 or higher, Build: 99 or higher, Content Version: 428 or higher, Product Version: 8.0, Engine Version: 3.0 or higher, Build: 131 or higher, Content Version: 428 or higher)

VSE (Vendor: mcafee, Product Version: 8.0 or higher, Build: 131 or higher)

VSE 8.5 (Vendor: mcafee, Product Version: 8.5 or higher, Build: 354 or higher)

Foundstone (Vendor: mcafee, Content Version: 5807 or higher)

Applications

Microsoft Windows 2000 Sp4 - Microsoft Internet Explorer 5.01 Sp4

Microsoft Windows 2003 Sp2 - Microsoft Internet Explorer 6 Sp2

Microsoft Windows 2003 Sp2 - Microsoft Internet Explorer 7

Microsoft Windows 2008 - Microsoft Internet Explorer 7

Asset Coverage

1,139 covered | 1,460 uncovered

Answers the question: "Am I at Risk?"

Actions Taken

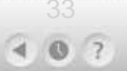
- ““3,000 to 30” – Countermeasure aware risk management correlates MTIS threat feeds with discovered vulnerabilities, assets, and deployed countermeasures (intrusion protection, anti-virus, buffer overflow)
- Leverages AVERT threat advisory information, delivered by MTIS feed
- **Risk = (Threat X Vulnerability X Asset)/Detailed Countermeasure**

- Countermeasure Aware Risk Management Application (“CARMA”)
- An architecture for future business analytics
- Example: Helps the customer user during a Microsoft Patch Tuesday event
 - What is MY exposure to a specific threat?
 - Do I need to stop production and patch now?
 - With my deployed security, WHERE am I still at risk?
 - If I am at risk, HOW am I at risk?
- Current methods are manual
 - E.g. get Threat Feed, go query each management console to show compliance with threat, once translated from problem to appropriate solutions

McAfee's Project CARMA

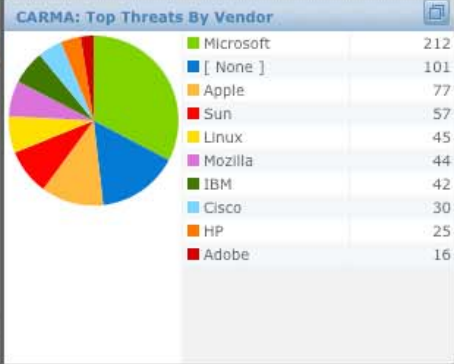
First phase

- At the heart is the MTIS Threat Feed
- Feed includes Countermeasures
 - VirusScan
 - Engine Version
 - DAT Version
 - Product Buffer Overflow Protection Version
 - Host Intrusion Prevention
 - Product Version
 - Content Version with High Level Signature (McAfee Default policy)
- Also includes Detectors
 - Foundstone
 - Specific FSL Check ID



CARMA: Most Recent Threats

	Total
December 10, 2008	2
Linux Kernel sendmsg() Denial-of-Service	1
Linux Kernel svc_listen() Denial-of-Service	1
December 9, 2008	29
(MS08-072) Microsoft Word Memory Cor	2
(MS08-072) Microsoft Word Memory Cor	1
(MS08-072) Microsoft Word RTF Object P	1
(MS08-072) Microsoft Word RTF Object P	1
(MS08-072) Microsoft Word RTF Object P	1
(MS08-072) Microsoft Word RTF Object P	1
(MS08-072) Microsoft Word RTF Object P	1
(MS08-072) Microsoft WordRTF Object P	1
(MS08-072) Microsoft WordRTF Object P	1
(MS08-073) Microsoft Internet Explorer t	1

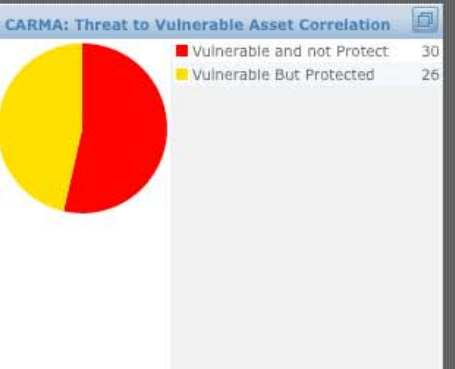
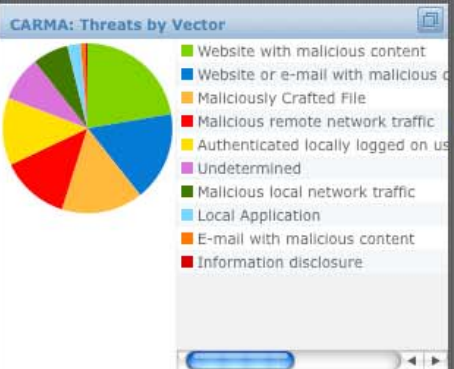
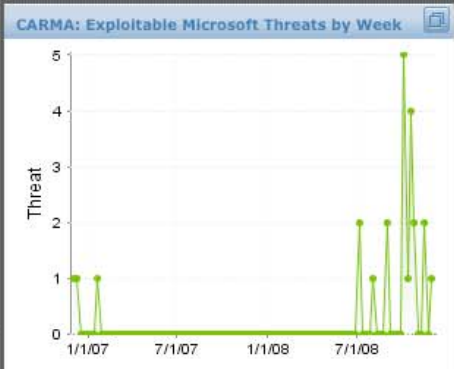
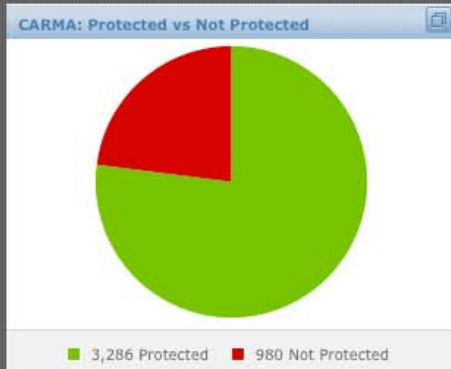
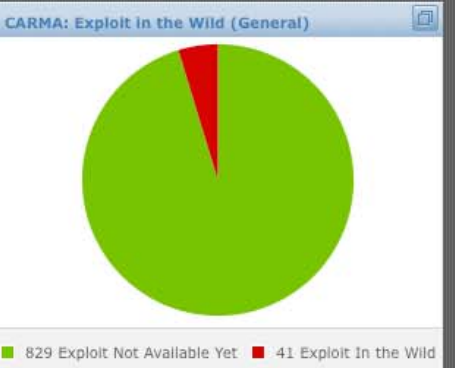
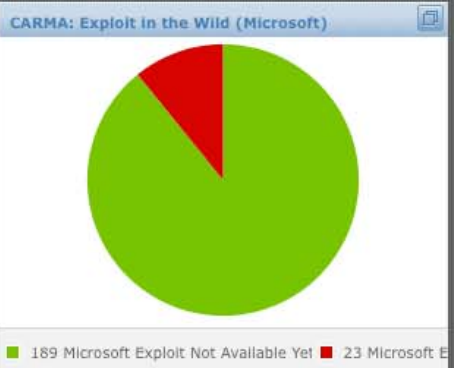
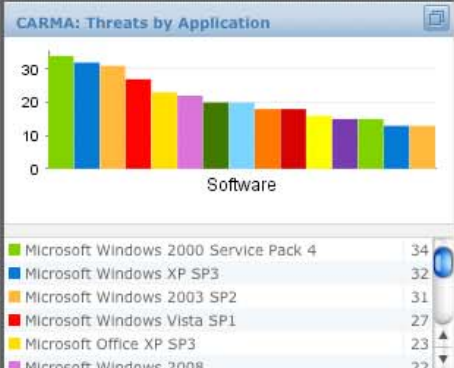
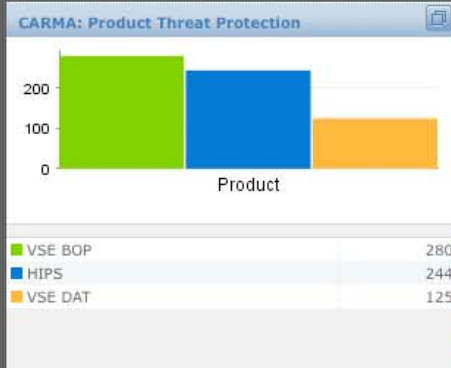


CARMA: Top 10 Least Covered Threats (Pessimist)

Threat Name	Total
(MS07-003) Microsoft Outlook Denial of Service Vulnerability	1
(MS07-008) Microsoft HTML Help ActiveX Control Vulnerability	1
(MS07-010) Microsoft Antivirus Engine Vulnerability	1
(MS07-011) Microsoft OLE Dialog Memory Corruption	1
(MS07-014) Microsoft Word Macro Vulnerability	1
(MS07-017) Microsoft Font Rasterizer Vulnerability	1
(MS07-017) Microsoft GDI Invalid Window Size Elevation	1
(MS07-017) Microsoft GDI Local Elevation of Privileges	1
(MS07-017) Microsoft WMF Denial of Service Vulnerability	1
(MS07-021) Microsoft CSRSS DoS Vulnerability	1
Total	10

CARMA: Top 10 Least Covered Assets (Pessimist)

System Name	Total
FS-TEST	391
EPO-MAC	391
BTRPM-DC1	391
10.101.101.5	362
10.101.101.2	362
10.101.101.1	362
FS67TEST	362
MAC002332C963AA	362
IMAC	273
MCAFEES-16AB991A	273
Total	3,520



Granular validation of implemented configuration



Threat Information	
Name :	(MS08-067) Microsoft Windows Server Service Vulnerability (958644)
Description:	A vulnerability exists, in Microsoft Windows Server Service, which may allow for remote code execution.
Overview:	MS08-067 srv 958644
Observation:	The Microsoft Server Service allows for local resource sharing via RPC. A vulnerability exists, in Microsoft Windows Server Service, which may allow for remote code execution. The flaw lies in the improper handling of specially-crafted (malicious) RPC requests. In a successful attack scenario, an attacker could potentially take full control of a target system via this vulnerability.
Recommendation:	Download and install the patch available from Microsoft(958644): http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
Vendor:	Microsoft
Threat Source:	McAfee
Threat Source Creation Date:	10/22/08 11:13:07 PM
Threat Source Last Modification Date:	11/18/08 11:29:02 AM
Creation Date:	12/5/08 3:07:15 PM
Last Modification Date:	12/10/08 4:16:17 PM
Attack Vector:	Malicious local network traffic
Countermeasures:	HIPS, VSE BOP
Detectors:	Foundstone
Severity:	8
Vendor Rating:	Critical
Basic Threat Score:	9.995
Ports:	

Name	Value
BID	31874
CVE	2008-4250
MSFTBulletin	MS08-067
Secunia	SA33376

W32/Conficker.worm [MTIS09-003-A]

Threat Identifier(s)	W32/Conficker.worm
Threat Type	Malware
Risk Assessment	Low
Main Threat Vectors	LAN; WAN; Web
User Interaction Required	Yes
Description	The W32/Conficker worm exploits the MS08-067 vulnerability, in Microsoft Windows Server Service. Machines should be patched and rebooted to protect against this worm's reinfesting the system after cleaning, which may require more than one reboot. Scheduled tasks and autorun.inf files have been seen to reactivate the worm.
Importance	Low. W32/Conficker.worm exploits the MS08-067 vulnerability.
McAfee Product Coverage *	
DAT files	Coverage was provided in the 5444 DAT files, released November 24, 2008 . Detection and repair was updated in the 5488 DAT files, released January 7 . (Users infected by W32/Conficker.worm should perform an On Demand Scan to remove remnants of the worm in memory using the latest DATs. After detection of W32/Conficker/mem and rebooting, the W32/Conficker.worm malware components will be removed.)
VSE BOP	Buffer overflow protection is expected to cover code-execution exploits.
Host IPS	Generic Buffer Overflow is expected to cover code-execution exploits. "Windows Server Service Buffer Overflow Vulnerability (Tighter Security)," Signature 3768, can provide partial coverage. Signature 3961, released October 28, 2008, will block denial-of-service and code-execution exploits associated with MS08-067.
IntruShield	The sigset release of October 23, 2008, includes the signature "NETBIOS-SS; Microsoft Server Service Remote Code Execution Vulnerability," which provides coverage.
Foundstone	Coverage not warranted at this time
MNAC	Coverage not warranted at this time
V-Flash	Out of scope
Additional Information	McAfee VIL: W32/Conficker.worm McAfee VIL: MS08-067 - Microsoft Windows Server Service Vulnerability - 958644

Risk Summary Risk Details

Where am I at Risk?

4 Not At Risk 30 At Risk

*as of 12/10/08 4:17:15 PM

Cross Reference with other organisations



External References

Name	Value	Confidence	Description	URL
BID	31874	N/A		
CVE	2008-4250	N/A		
MSFTBulletin	MS08-067	N/A		
Secunia	SA32326	N/A		

Name	Confidence	Dependencies
Microsoft Windows 2000 Service Pack 4	10	Microsoft Windows 2000 Service Pack 4 (10)
Microsoft Windows 2003 Itanium Sp2	10	Microsoft Windows 2003 Itanium Sp2 (10)
Microsoft Windows 2003 Sp2	10	Microsoft Windows 2003 Sp2 (10)
Microsoft Windows 2008	10	Microsoft Windows 2008 (10)
Microsoft Windows Vista SP1	10	Microsoft Windows Vista SP1 (10)
Microsoft Windows Vista X64 SP1	10	Microsoft Windows Vista X64 SP1 (10)
Microsoft Windows XP SP3	10	Microsoft Windows XP SP3 (10)
Microsoft Windows Xp X64 Sp2	10	Microsoft Windows Xp X64 Sp2 (10)
Microsoft Windows 2003 x64 SP2	10	Microsoft Windows 2003 x64 SP2 (10)

Countermeasures

Product	Description
HIPS	(Vendor: McAfee, Product Version: 6.0 or higher, Build: 3961 or higher)
VSE BOP	(Vendor: McAfee, Product Version: 8.5 or higher)
VSE BOP	(Vendor: McAfee, Product Version: 8.0 or higher)

Detectors

Product	Description
Foundstone	(Vendor: McAfee, Signature: 6190)
Foundstone	(Vendor: McAfee, Signature: 6191)

Actions Taken

Understand where and why I'm at risk

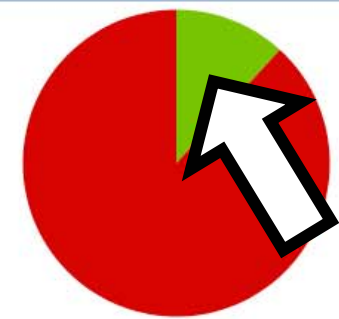


Threat Information

Name :	(MS08-067) Microsoft Windows Server Service Vulnerability (958644)
Description:	A vulnerability exists, in Microsoft Windows Server Service, which may allow for remote code execution.
Overview:	MS08-067 srv 958644
Observation:	The Microsoft Server Service allows for local resource sharing via RPC. A vulnerability exists, in Microsoft Windows Server Service, which may allow for remote code execution. The flaw lies in the improper handling of specially-crafted (malicious) RPC requests. In a successful attack scenario, an attacker could potentially take full control of a target system via this vulnerability.
Recommendation:	Download and install the patch available from Microsoft(958644): http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp
Vendor:	Microsoft
Threat Source:	McAfee
Threat Source Creation Date:	10/22/08 11:13:07 PM
Threat Source Last Modification Date:	11/18/08 11:29:02 AM
Creation Date:	12/5/08 3:07:15 PM
Last Modification Date:	12/10/08 4:16:17 PM
Attack Vector:	Malicious local network traffic
Countermeasures:	HIPS, VSE BOP
Detectors:	Foundstone
Severity:	8
Vendor Rating:	Critical
Basic Threat Score:	9.995
Ports:	

Risk Summary Risk Details

Where am I at Risk?



4 Not At Risk 30 At Risk

*as of 12/10/08 4:17:15 PM

External References

Name	Value	Description	URL
BID	31874	N/A	
CVE	2008-4250	N/A	
MSFTBulletin	MS08-067	N/A	
Secunia	SA33326	N/A	

Actions Taken

--



*as of 12/10/08 4:17:15 PM

- Red – vulnerable, NO protection!!!
- Yellow - vulnerable BUT they have required countermeasure in place.
- Grey- Unknown – No agent or no assessment
- Green NOT vulnerable YET, but they have a countermeasure in place as well

Surely Vulnerability management does this?

McAfee

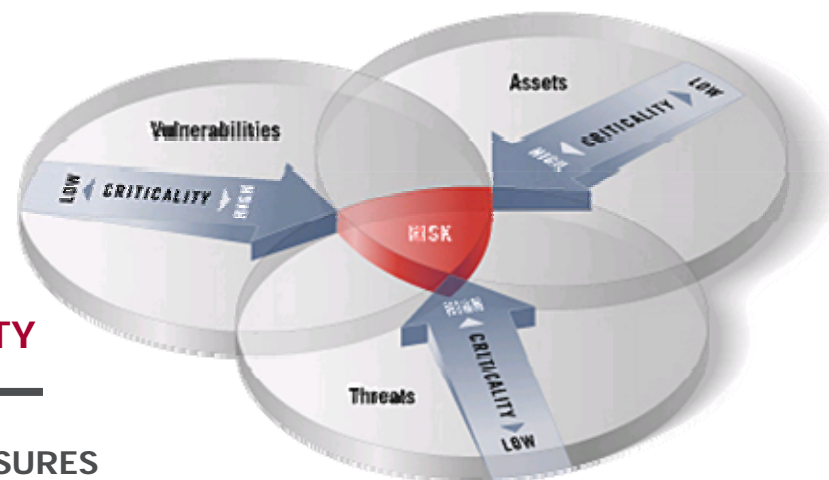
Vulnerability Management

VULNERABILITY
CRITICALITY *

THREAT
CRITICALITY *

ASSET
CRITICALITY

COUNTERMEASURES COUNTERMEASURES COUNTERMEASURES



However, vulnerability/risk mgmt does show the next step!

Response prioritization

- business impact
- risks associated with remediation
- cost of remediation

Impact to the business is not linear— Risk Analysis gives prioritisation to remediation



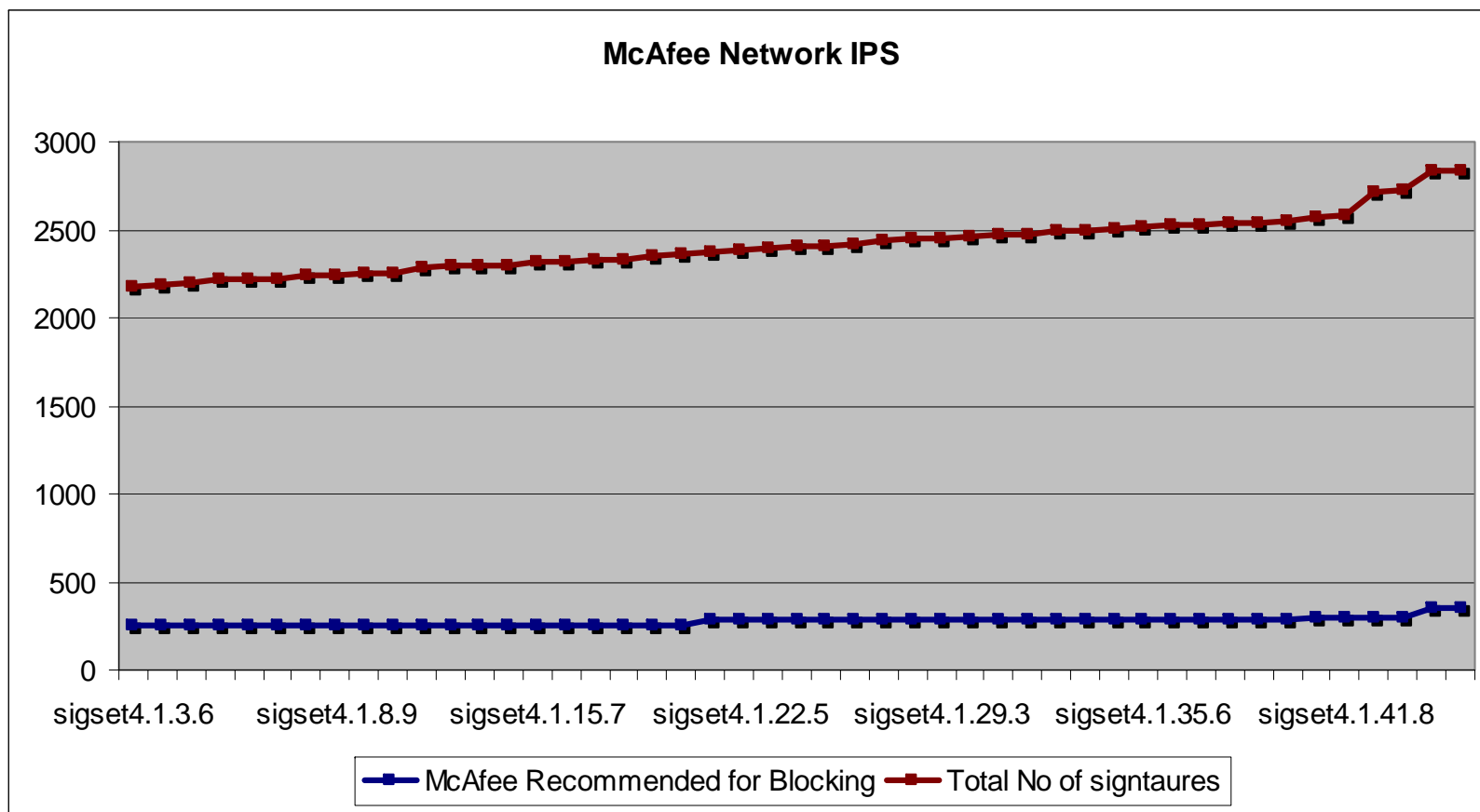
- PC down = the loss of productivity and the cost of fixing the asset.
- A revenue-generating web server = higher cost, as the financial impact would be much greater.

Example costs for a global enterprise:

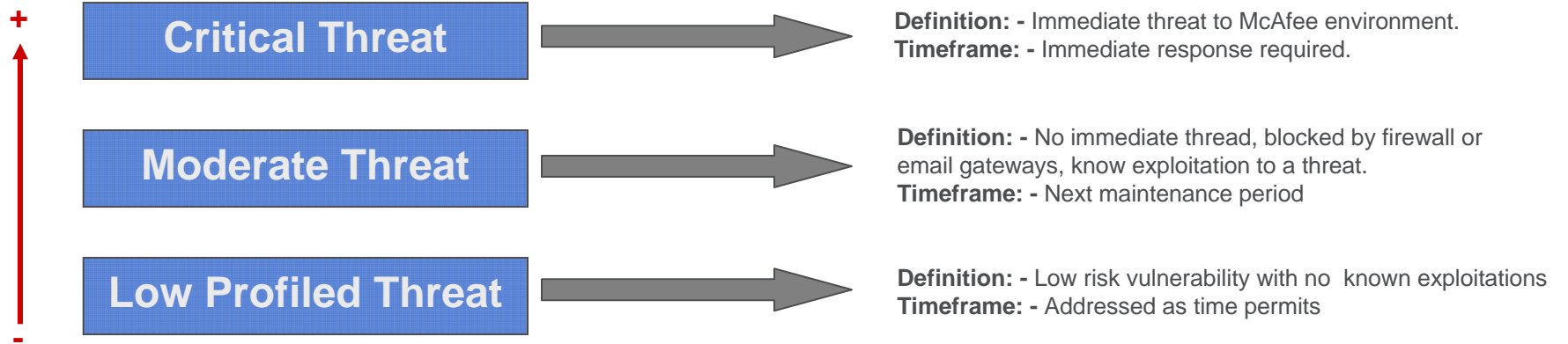
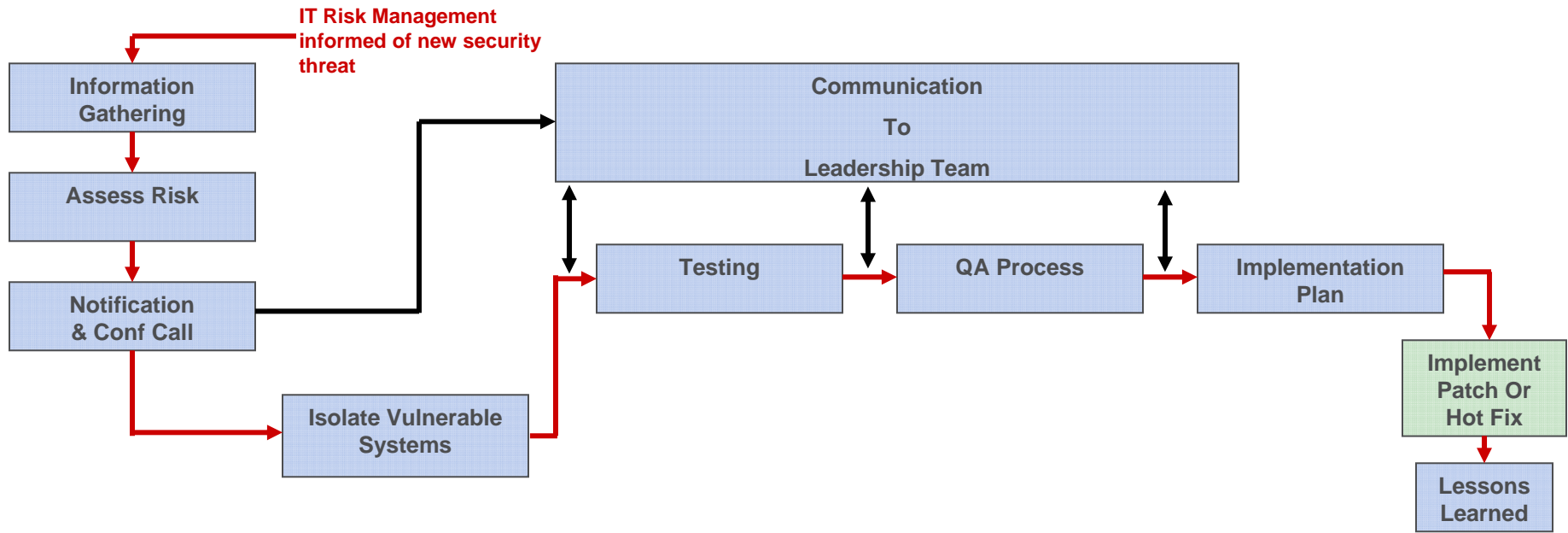
- \$100 per hour, per desktop
- \$1,000 per hour, per server
- \$10,000 per hour, per central application
- \$100,000 per hour per mission-critical application.



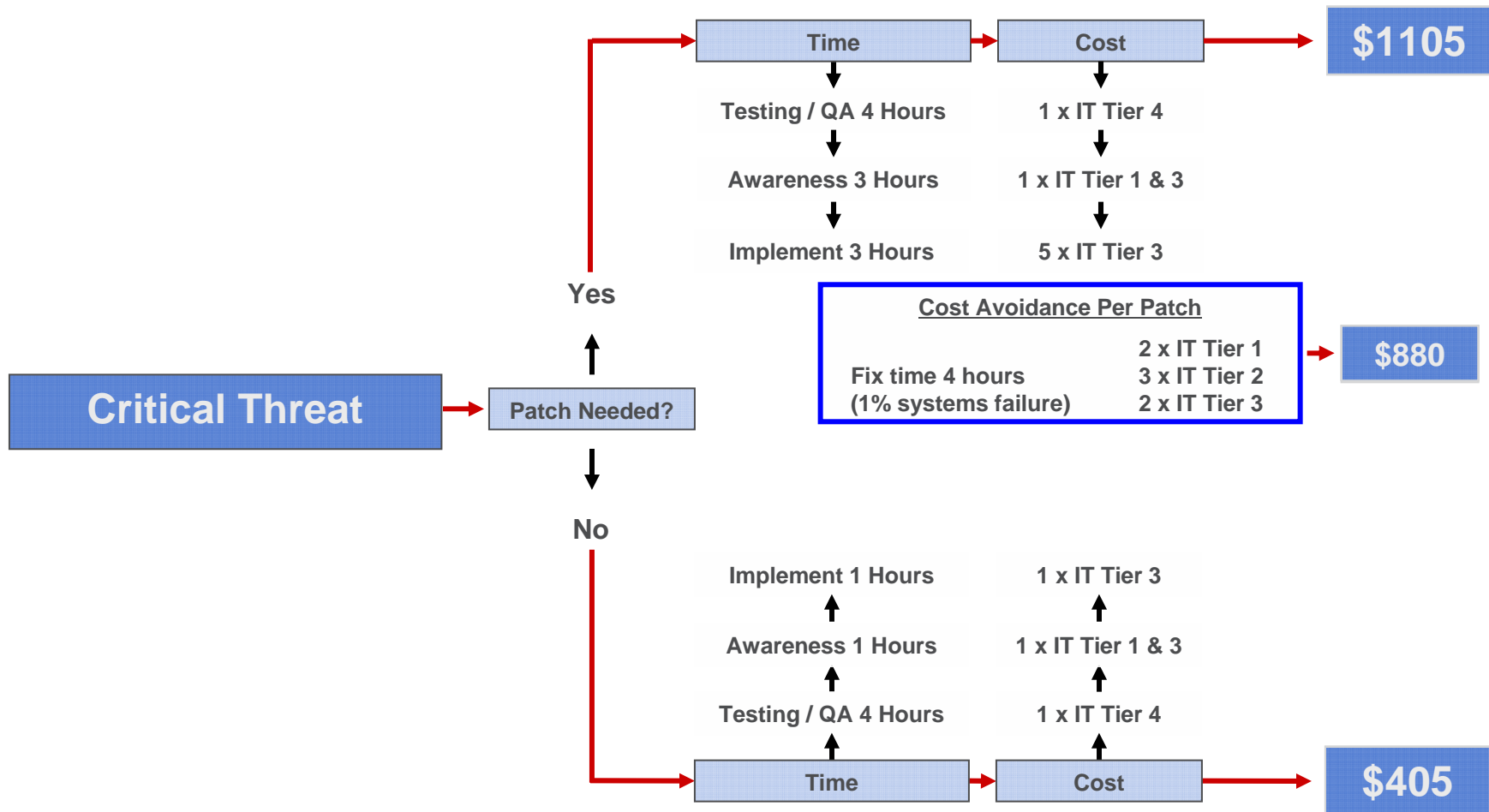
Confidence in the solution



Cost of the solution to the business?



Costs – Emergency Patching Versus Not Patching



Cost Saving = Number of patches not required * ((cost avoidance + Cost per patch) - cost of not patching)

Summary



- The scope of threat and security solutions is only going to increase in complexity (diversity of use and technology)
- 1. When should I engage?
- 2. Integration is required to get the bigger picture (OSA)
 - Common point of visibility
 - Coordination of threat intelligence
- 3. Optimised Security Architectures (OSA) will provide
 - Framework for
 - improving security posture
 - Reducing costs and risk
- 4. Validation of the Risk to your business (ongoing)
 - Collaborative cloud based intelligence
 - Real risk analysis - Mapping countermeasures against threat
- 5. Allows a business risk approach (asset value)
 - Should I respond now or later (risk versus costs)
 - What is the right solution
 - Time to implement
 - Risk factor
- 6. Validation of application of resolution (retesting the risk)

When does this become an incident?

McAfee



McAfee®