

Don't worry, everything is FINE

Bart Bosma, Technical Account Manager – Benelux & Nordics

6 October 2011



Agenda

- In the news
- We're FINE
- Detect Vulnerabilities
- Detect Web App Vulnerabilities
- Measure Compliance
- Automation
- Integration
- Hardening
- Conclusion



1



“Leaktober”



“We expose a privacy leak every workday in October”

1. DigiD fraude easy.
2. 7 municipalities vulnerable for DigiD fraude problem.
3. Site NVVP (Netherlands Association for Psychologists and Psychotherapists) leaks privacy data.
4. Hospital site leaks data.

DigiD
Je eigen inlogcode voor de hele overheid

NVVP

tergooziekenhuizen

<http://webwereld.nl/nieuws/108052/lektober--iedere-dag-een-privacylek-op-webwereld.html>



2



We're FINE



Sony PSN hack

Diginotar fiasco



17-year old member of Anonymous arrested for VVG-KLPD hack



3



FINE – What does it mean?

- Create awareness
 - Do you need to comply?

- Measure exposure and determine what you need to mitigate
 - Are you proactive or reactive?

- Efficient use of limited resources
 - What is your budget?

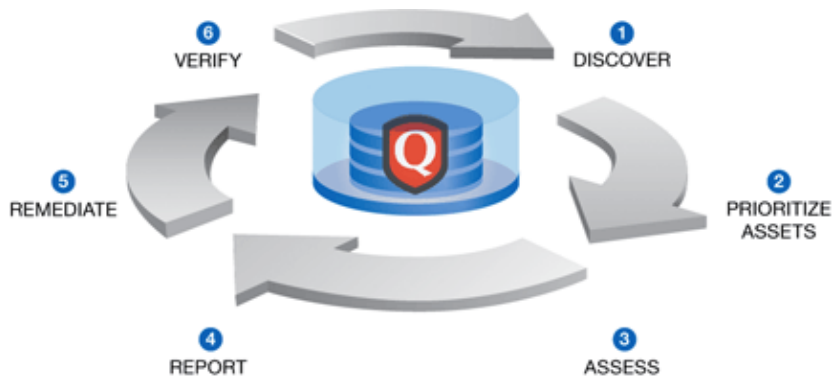


4



Detect Vulnerabilities

Vulnerability Management:



5



Measure and Mitigate Vulnerabilities

(Critical) Patch Report

Report Summary

Company: Qualys
 Created by: Bart Bosma
 Created on: 10/05/2011
 Includes hosts scanned since 09/05/2011.
[View Report Targets...](#)

Total Patches	Hosts Requiring Patches	Vulnerabilities Addressed
18	17	49

PATCHES				HOSTS requiring Microsoft Windows Server Service Could Allow Remote Code Execution					
Vendor ID	Severity	Title	Published	Hosts	IP	DNS Name	NetBIOS	OS	Vulns
CPUOCT2010	5	Oracle Database October 2010 Secur...	358 days ago	1	10.10.26.121	2ksp4-26-121.2ksp...	2KSP4-26...	Windows 2000	1
KB824721	5	Microsoft Windows Server 2003 Servic...	6 years ago	1	10.10.26.185	2k3sp2-26-185	2K3SP2-26...	Windows 2003 Service Pac...	1
KB891861	5	Windows 2000 Service Pack 4 Update ...	6 years ago	1	10.10.30.183	symim-30-183	SYMM-30...	Windows 2003 R2 Service ...	1
MS05-047	5	Microsoft Plug and Play Remote Code ...	5 years ago	1	10.10.31.234	bug112996-216	BUG11299...	Windows 2003 Service Pac...	1
MS08-067	5	Microsoft Windows Server Service Coul...	2 years ago	4					
KB936929	5	Microsoft Windows XP Service Pack 3 ...	3 years ago	1					
PMASA-201...	4	PhpMyAdmin Multiple Vulnerabilities (...)	74 days ago	1					

Detect WebApp Vulnerabilities

Web Application Scanning:



Find your Web Applications

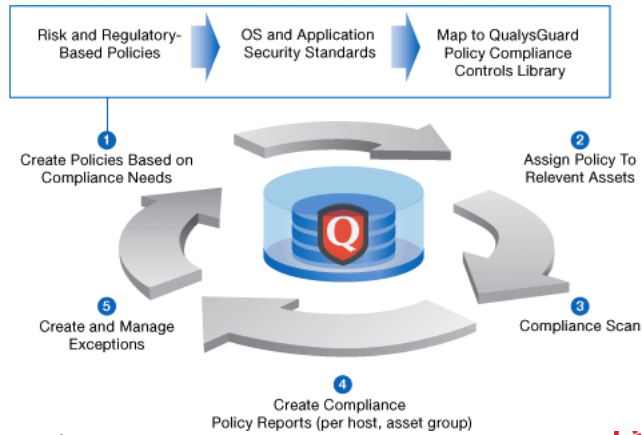
Web Application Catalog:

IP Address	FQDN	Port	NetBIOS	Status	Created
10.10.29.121		8080	PAT-UBU1010-U-3	Approved	13 Sep 2011
10.10.29.121		80	PAT-UBU1010-U-3	New	13 Sep 2011
10.10.30.5	hp-30-5.vuln.qa.qualys.com	2381		Rogue	13 Sep 2011
10.10.31.109		80		New	06 Sep 2011
10.10.31.109		8889		New	06 Sep 2011
10.10.32.149	win-32-149	80	WIN-32-149	New	06 Sep 2011
10.20.30.56	ora9208-win-30-56	443	ORAG208-WIN-30-	New	06 Sep 2011
10.20.30.56	ora9208-win-30-56	80	ORAG208-WIN-30-	New	06 Sep 2011
10.10.32.148	win-32-148	8080	WIN-32-148	New	06 Sep 2011
10.10.32.148	win-32-148	80	WIN-32-148	New	06 Sep 2011
10.10.32.139		80		New	06 Sep 2011
10.10.32.145	owaspbwa.localdomain	8080	OWASPBWA	New	06 Sep 2011



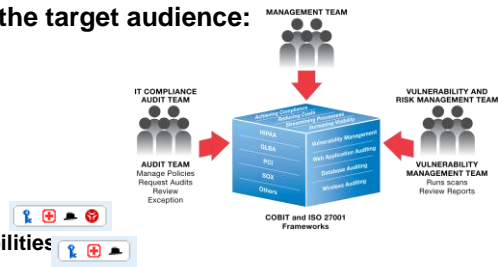
Measure Compliance

Policy Compliance:



Automation is key

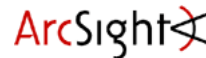
- easy deployment / agent-less
- collect data automatically so you can be proactive
- set up schedules for Network Discovery Scanning, Vulnerability Scanning, Web App Scanning and Policy Compliance Scanning
- run the right report for the target audience:
 - trending
 - technical
 - top xx
- prioritize mitigation
 - business value/impact
 - CVSS
 - exploitability of vulnerabilities
 - (virtual) patch available



10



Integration



11



Hardening

To make the hardening process efficient, create hardening guidelines and measure their effectiveness.

Create a baseline system, derive the policy from it and measure against the baseline (Golden image)

- or -

Import CIS benchmark and measure against it.

- or -

Do detail checks, e.g on Windows systems:

- determine if AV is installed and up-to-date,
- determine which applications are installed,
- check file integrity,
- audit passwords,
- enumerate shares,
- audit security settings.



Conclusion

- Efficient use of resources requires automation.
- Provide the right information to the right person.
- Make it possible to have all security information in one place.
- Use Policy compliance to determine the hardening status of systems.





Thank You

bbosma@qualys.com

