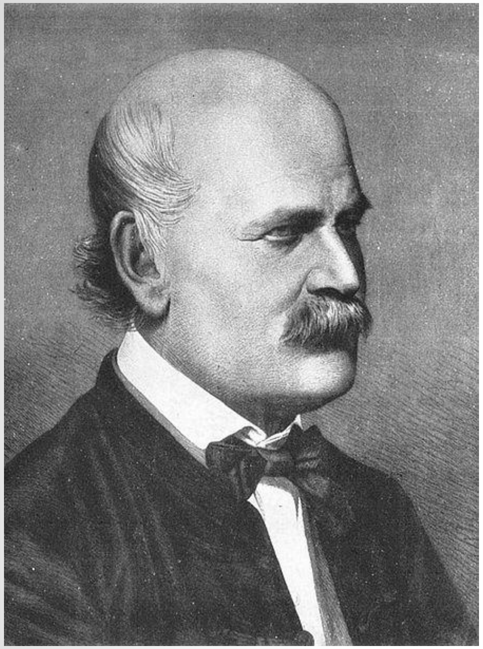
QUALYS®

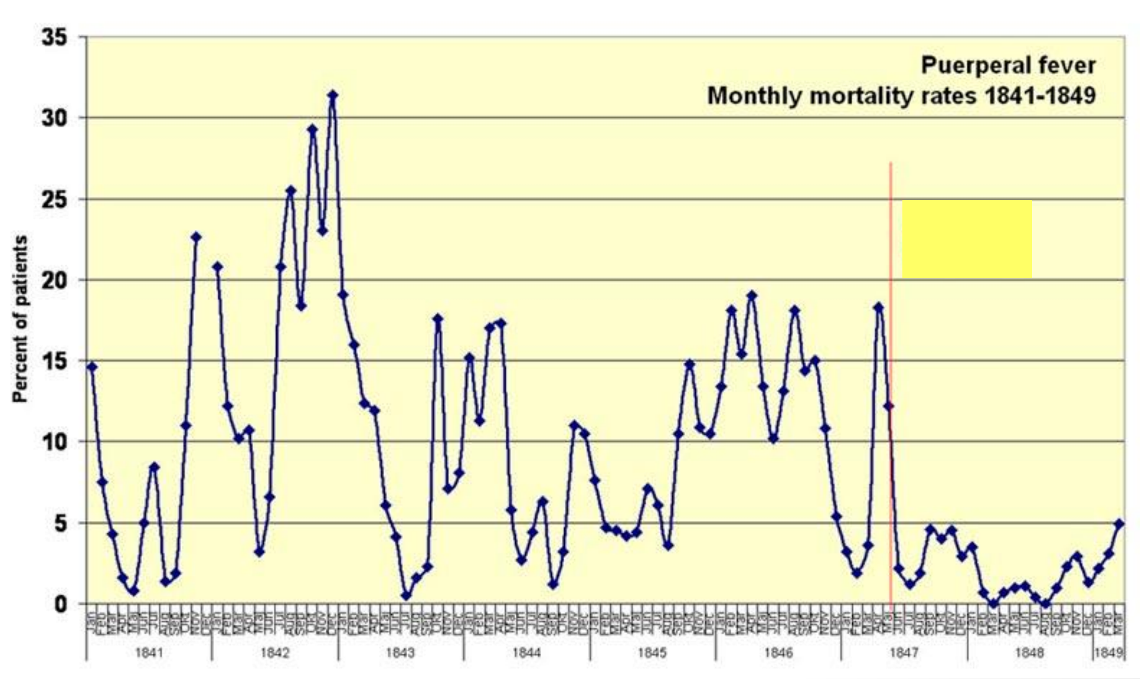
"Advanced Vulnerability Management new approach to solve critical controls”

Andrzej Kleśnicki
Technical Account Manager Central Eastern Europe

Riga, 23/10/2013

Before we start – history lesson





Dr Ignaz Philipp Semmelweis

Born: 1st of June 1818, Buda
Died: 13th of September 1865, Vienna

Lessons learned

- Routine hygiene is important
- Simple measures can be quite effective
- Status quo is not always right approach
- Doing thing is not so importing as doing them right

- Wash your hands ☺

What about security?

- **96% of successful breaches can be avoided if the victim puts in place simple or intermediate control:**
  - According to report: James A. Lewis, Raising the Bar for Cybersecurity. Washington, DC: CSIS, 2013
- **To be more secure we just need to follow IS Security hygiene, that would be:**
  - Continuous
  - Effective
  - Prioritised
  - That really works!
- **Do we already have IS security hygiene guidelines?**

SANS TOP 20 Critical Controls for Effective Cyber Defense

SANS TOP-20 Critical Security Controls

Brief History of TOP-20 CSC

- In 2008, the Office of the Secretary of Defense asked the National Security Agency for help in prioritizing the myriad security controls that were available for cybersecurity with strong emphasis on **"What really Works"**.

- The request went to NSA because NSA best understood how cyber attacks worked and **which attacks were used most frequently.**

- A consortium of U.S. and international cyberdefense agencies quickly grew, and was joined by experts from private industry and around the globe.

- Surprisingly, the clear consensus of the consortium was that there were **only 20 Critical Controls that addressed the most prevalent attacks** found in government and industry. This then became the focus for an initial draft document. The draft of the 20 Critical Controls was circulated in 2009 to several hundred IT and security organizations for further review and comment.
- Over 50 organizations commented on the draft. They endorsed the concept of a focused set of controls and the selection of the 20 Critical Controls.

- **Last release - Version 4.1, March, 2013**

SANS TOP-20 Critical Security Controls

5 critical principles of effective cyber defense system as reflected in the Critical Controls are:

1. **Offense informs defense:** Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

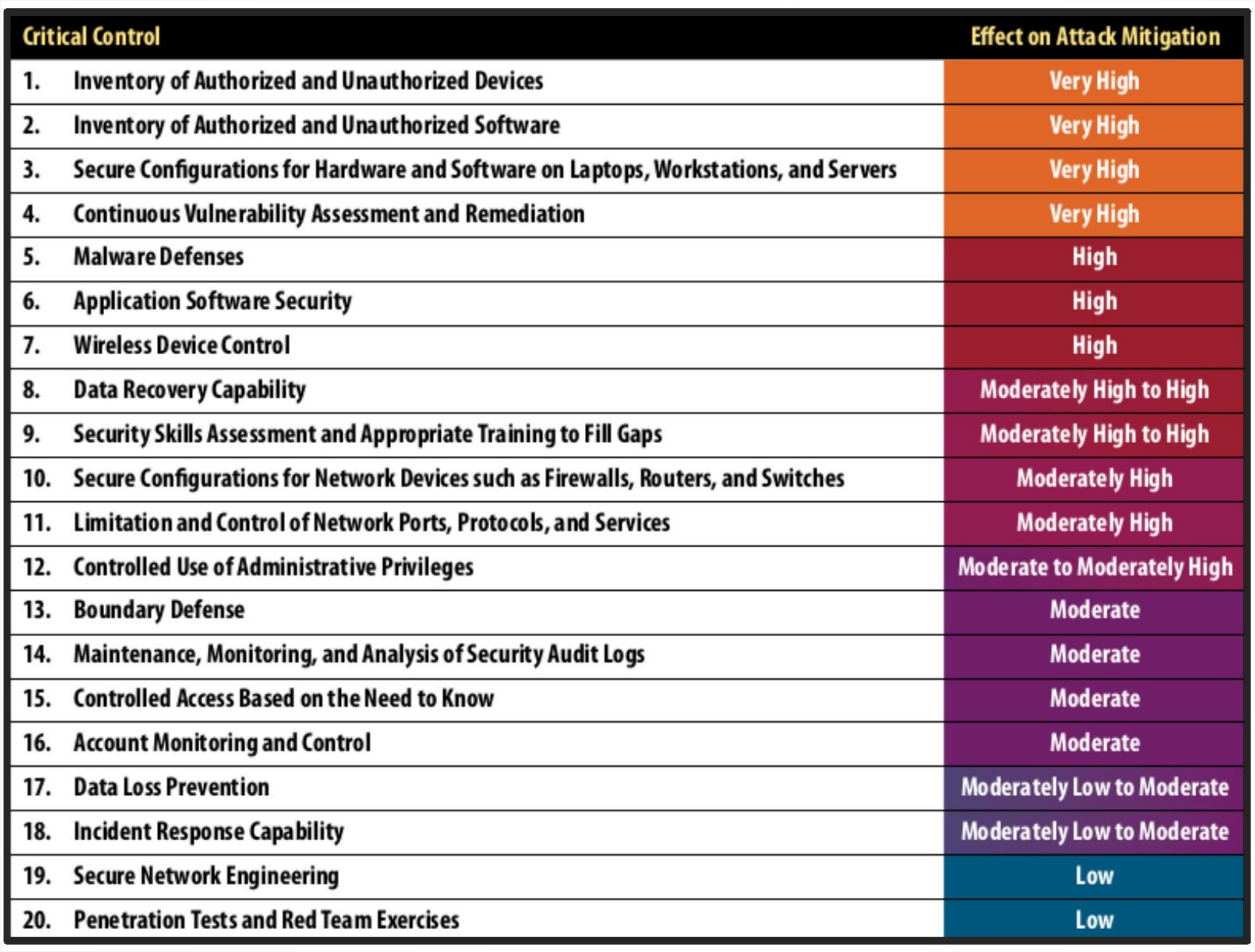
2. **Prioritization:** Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.

3. **Metrics:** Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

4. **Continuous monitoring:** Carry out continuous monitoring to test and validate the effectiveness of current security measures.

5. **Automation:** Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

SANS TOP 20 Critical Controls



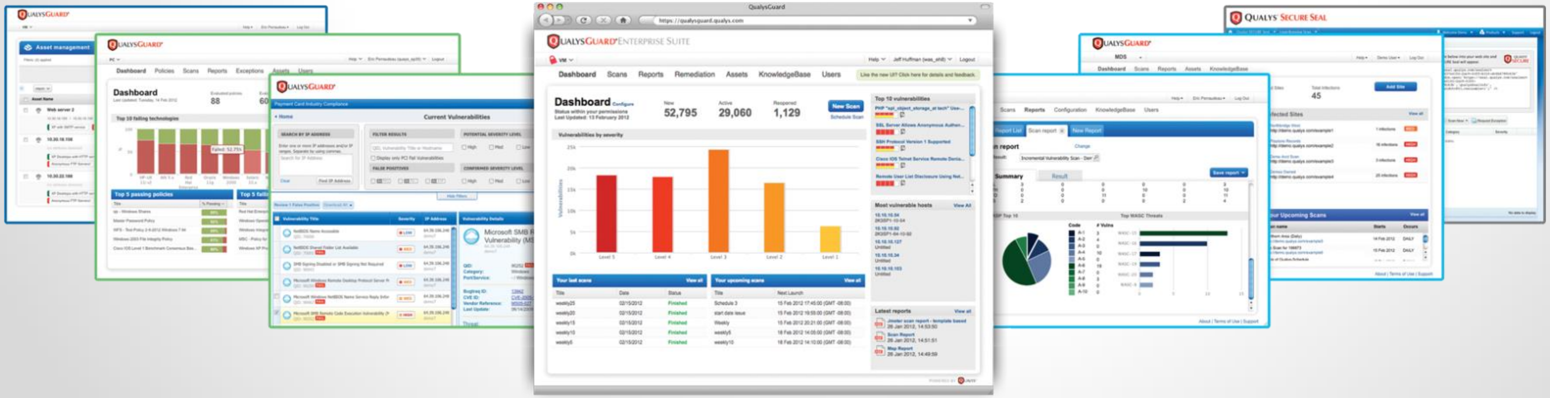
Critical Control	Effect on Attack Mitigation	
1. Inventory of Authorized and Unauthorized Devices	Very High	Q
2. Inventory of Authorized and Unauthorized Software	Very High	Q
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High	Q
4. Continuous Vulnerability Assessment and Remediation	Very High	Q
5. Malware Defenses	High	Q
6. Application Software Security	High	Q
7. Wireless Device Control	High	Q
8. Data Recovery Capability	Moderately High to High	
9. Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High	
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High	Q
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High	Q
12. Controlled Use of Administrative Privileges	Moderate to Moderately High	Q
13. Boundary Defense	Moderate	
14. Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate	
15. Controlled Access Based on the Need to Know	Moderate	
16. Account Monitoring and Control	Moderate	
17. Data Loss Prevention	Moderately Low to Moderate	
18. Incident Response Capability	Moderately Low to Moderate	
19. Secure Network Engineering	Low	
20. Penetration Tests and Red Team Exercises	Low	Q

Qualys solution for Very-High to Mid-High SANS Critical Controls

QUALYS

Critical Control	Effect on Attack Mitigation	
1. Inventory of Authorized and Unauthorized Devices	Very High	VM
2. Inventory of Authorized and Unauthorized Software	Very High	PC VM
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High	PC
4. Continuous Vulnerability Assessment and Remediation	Very High	VM
5. Malware Defenses	High	WAS VM
6. Application Software Security	High	WAS WAF
7. Wireless Device Control	High	VM

10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High	PC
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High	PC VM



QUALYS

CC1: Inventory of Authorized and Unauthorized Devices

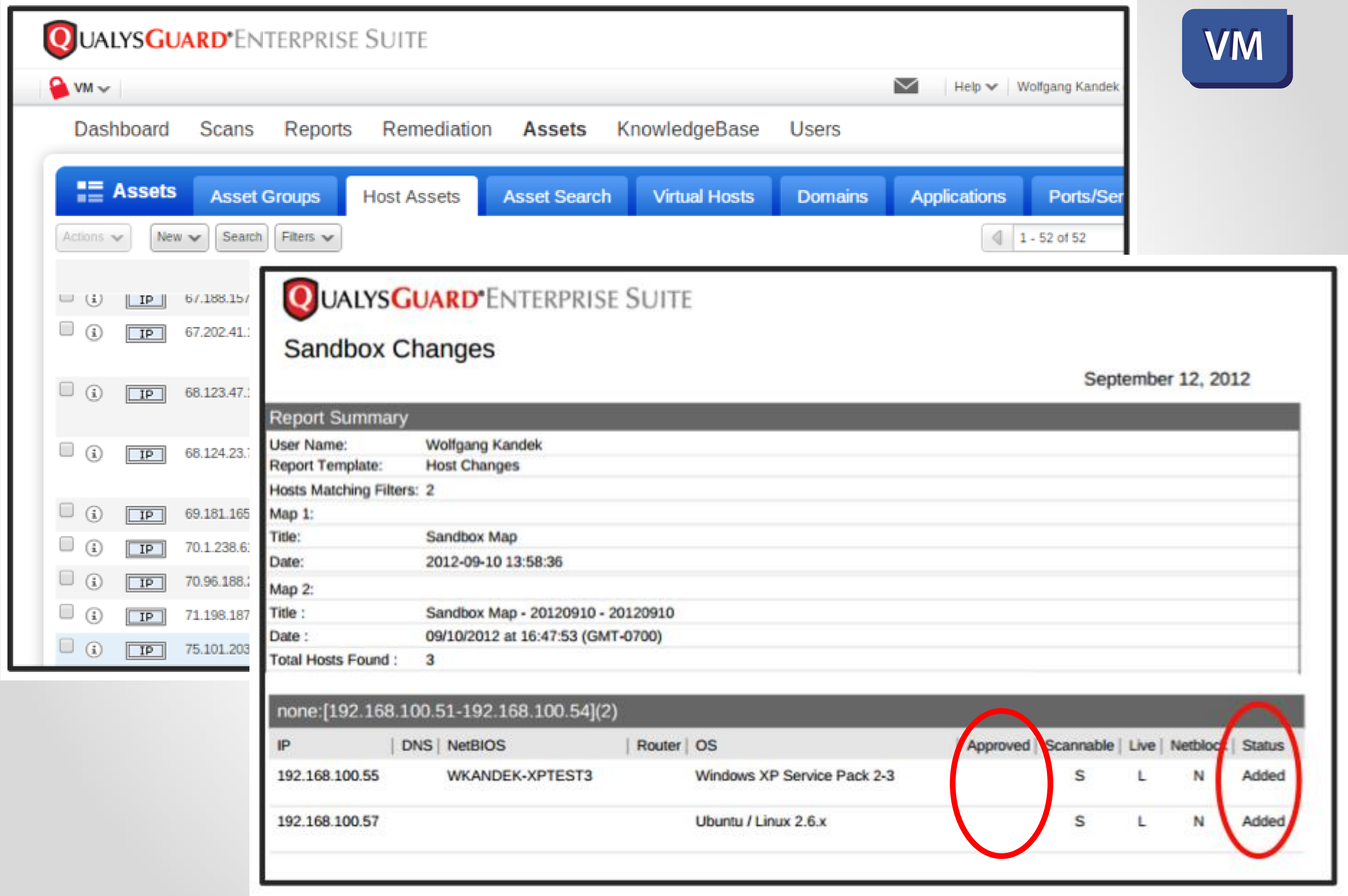
Goal: Effective asset management ensures that assets are discovered, registered, classified, and protected from attackers who exploit vulnerable systems accessible via the Internet.

VM

How QualysGuard supports this:

- VM gives full asset visibility over live devices with network mapping:
  - Size of Network
  - Machine Types
  - Location
- VM detects authorized and unauthorised devices:
  - Authorized
  - Unauthorized
- VM offers full support for automation
  - Scans are scheduled (continuous, daily, weekly etc)
  - Delta reports for changes
  - Alerting, ticketing
  - API for integration for example with Asset management tools

CC1: Inventory of Authorized and Unauthorized Devices



IP	67.188.15
IP	67.202.41.
IP	68.123.47.
IP	68.124.23.
IP	69.181.165
IP	70.1.238.6
IP	70.96.188.
IP	71.198.187
IP	75.101.203

Sandbox Changes

September 12, 2012

Report Summary

User Name:	Wolfgang Kandek
Report Template:	Host Changes
Hosts Matching Filters:	2
Map 1:	
Title:	Sandbox Map
Date:	2012-09-10 13:58:36
Map 2:	
Title :	Sandbox Map - 20120910 - 20120910
Date :	09/10/2012 at 16:47:53 (GMT-0700)
Total Hosts Found :	3

none:[192.168.100.51-192.168.100.54](2)

IP	DNS	NetBIOS	Router	OS	Approved	Scannable	Live	Netbloc	Status
192.168.100.55		WKANDEK-XPTEST3		Windows XP Service Pack 2-3		S	L	N	Added
192.168.100.57				Ubuntu / Linux 2.6.x		S	L	N	Added

CC2: Inventory of Authorized and Unauthorized Software

Goal: Effective software management ensures that software are discovered, registered, classified, and protected from attackers who exploit vulnerable software.

How QualysGuard supports this:

- VM & POL gives full software visibility with scanning:
  - Operating Systems
  - Applications
  - Versions
  - Patch Level
- VM & POL gives Blacklisting of unauthorised software and services
- VM & POL gives Whitelisting of authorised software and services
- VM provides Interactive Search
- VM & POL offers full support for automation
  - Scheduled scans & reports
  - Email reports
  - Alerting on exceptions
  - Ticketing
  - API for Integration with Asset Management tools

VM

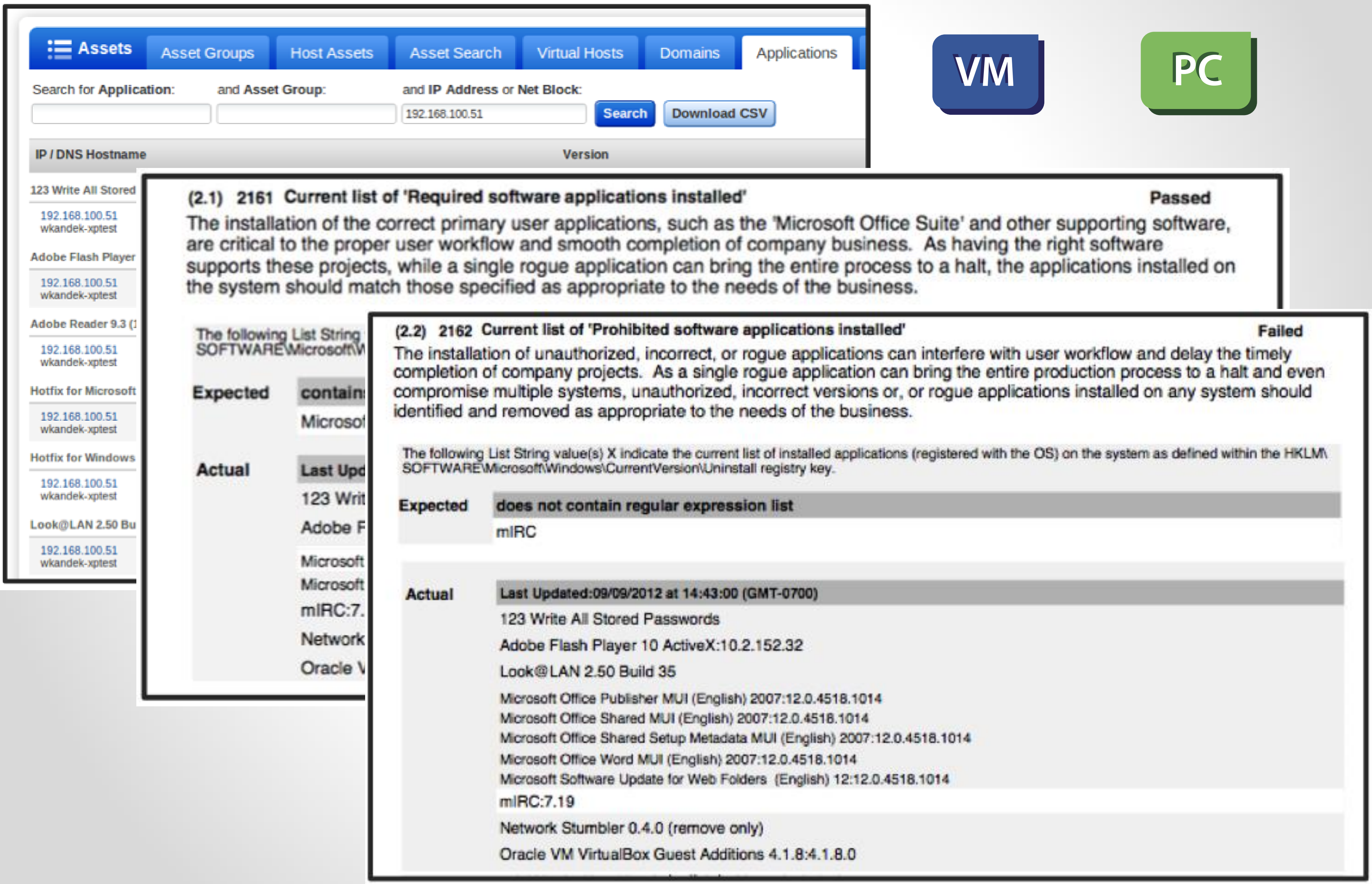
PC

QUALYS®

CC2: Inventory of Authorized and Unauthorized Software

VM

PC



Search for **Application**: and **Asset Group**: and **IP Address** or **Net Block**: 192.168.100.51

IP / DNS Hostname	Version
123 Write All Stored	
192.168.100.51 wkandek-xptest	
Adobe Flash Player	
192.168.100.51 wkandek-xptest	
Adobe Reader 9.3 (1	
192.168.100.51 wkandek-xptest	
Hotfix for Microsoft	
192.168.100.51 wkandek-xptest	
Hotfix for Windows	
192.168.100.51 wkandek-xptest	
Look@LAN 2.50 Bu	
192.168.100.51 wkandek-xptest	

(2.1) 2161 Current list of 'Required software applications installed' **Passed**

The installation of the correct primary user applications, such as the 'Microsoft Office Suite' and other supporting software, are critical to the proper user workflow and smooth completion of company business. As having the right software supports these projects, while a single rogue application can bring the entire process to a halt, the applications installed on the system should match those specified as appropriate to the needs of the business.

The following List String
SOFTWARE\Microsoft\W

Expected **contain**
Microsof

Actual **Last Upd**
123 Writ
Adobe F
Microsof
Microsoft
mIRC:7.
Network
Oracle V

(2.2) 2162 Current list of 'Prohibited software applications installed' **Failed**

The installation of unauthorized, incorrect, or rogue applications can interfere with user workflow and delay the timely completion of company projects. As a single rogue application can bring the entire production process to a halt and even compromise multiple systems, unauthorized, incorrect versions or, or rogue applications installed on any system should identified and removed as appropriate to the needs of the business.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall registry key.

Expected **does not contain regular expression list**
mIRC

Actual **Last Updated:09/09/2012 at 14:43:00 (GMT-0700)**
123 Write All Stored Passwords
Adobe Flash Player 10 ActiveX:10.2.152.32
Look@LAN 2.50 Build 35
Microsoft Office Publisher MUI (English) 2007:12.0.4518.1014
Microsoft Office Shared MUI (English) 2007:12.0.4518.1014
Microsoft Office Shared Setup Metadata MUI (English) 2007:12.0.4518.1014
Microsoft Office Word MUI (English) 2007:12.0.4518.1014
Microsoft Software Update for Web Folders (English) 12:12.0.4518.1014
mIRC:7.19
Network Stumbler 0.4.0 (remove only)
Oracle VM VirtualBox Guest Additions 4.1.8:4.1.8.0

CC3: Secure Base Configuration

Goal: Effective configuration management ensures assets are configured based on industry standards and protected from attackers who find and exploit misconfigured systems**.**

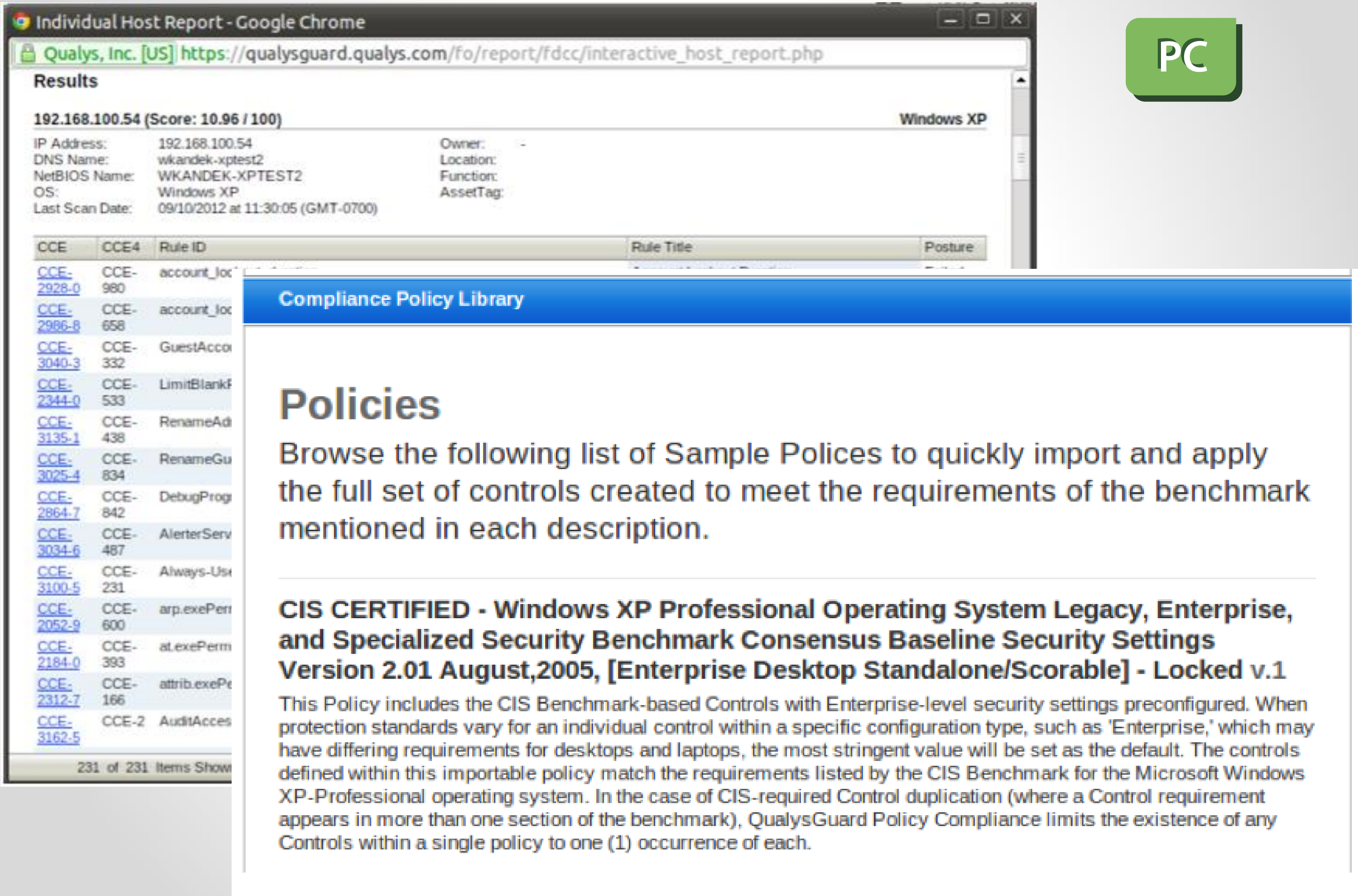
How QualysGuard supports this:

PC

- Configuration validation of each system
- Build in controls catalogue: CIS, SCAP, FDCC
- User Defined Controls
- Golden image policy
- Reporting on deviation from the baseline
- With full support for automation
  - Scheduled scans & reports
  - Email reports
  - Alerting on exceptions
  - Ticketing
  - API for Integration with GRC tools

CC3: Secure Base Configuration

PC



Individual Host Report - Google Chrome
Qualys, Inc. [US] https://qualysguard.qualys.com/fo/report/fdcc/interactive_host_report.php

Results

192.168.100.54 (Score: 10.96 / 100) **Windows XP**

IP Address: 192.168.100.54
DNS Name: wkandek-xptest2
NetBIOS Name: WKANDEK-XPTEST2
OS: Windows XP
Last Scan Date: 09/10/2012 at 11:30:05 (GMT-0700)

Owner: -
Location:
Function:
AssetTag:

CCE	CCE4	Rule ID	Rule Title	Posture
CCE-2928-0	CCE-980	account_loc		
CCE-2986-8	CCE-658	account_loc		
CCE-3040-3	CCE-332	GuestAcco		
CCE-2344-0	CCE-533	LimitBlankP		
CCE-3135-1	CCE-438	RenameAd		
CCE-3025-4	CCE-834	RenameGu		
CCE-2864-7	CCE-842	DebugProg		
CCE-3034-6	CCE-487	AlerterServ		
CCE-3100-5	CCE-231	Always-Use		
CCE-2052-9	CCE-600	arp.exePerr		
CCE-2184-0	CCE-393	at.exePerm		
CCE-2312-7	CCE-166	attrib.exePe		
CCE-3162-5	CCE-2	AuditAcces		

231 of 231 Items Show

Policies

Browse the following list of Sample Polices to quickly import and apply the full set of controls created to meet the requirements of the benchmark mentioned in each description.

CIS CERTIFIED - Windows XP Professional Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings Version 2.01 August,2005, [Enterprise Desktop Standalone/Scorable] - Locked v.1

This Policy includes the CIS Benchmark-based Controls with Enterprise-level security settings preconfigured. When protection standards vary for an individual control within a specific configuration type, such as 'Enterprise,' which may have differing requirements for desktops and laptops, the most stringent value will be set as the default. The controls defined within this importable policy match the requirements listed by the CIS Benchmark for the Microsoft Windows XP-Professional operating system. In the case of CIS-required Control duplication (where a Control requirement appears in more than one section of the benchmark), QualysGuard Policy Compliance limits the existence of any Controls within a single policy to one (1) occurrence of each.

CC4: Continuous Vulnerability Assessment/Remediation

Goal: Effective vulnerability management will ensure that assets are monitored for vulnerabilities and are patched, upgraded or services disabled to protect from exploit code.

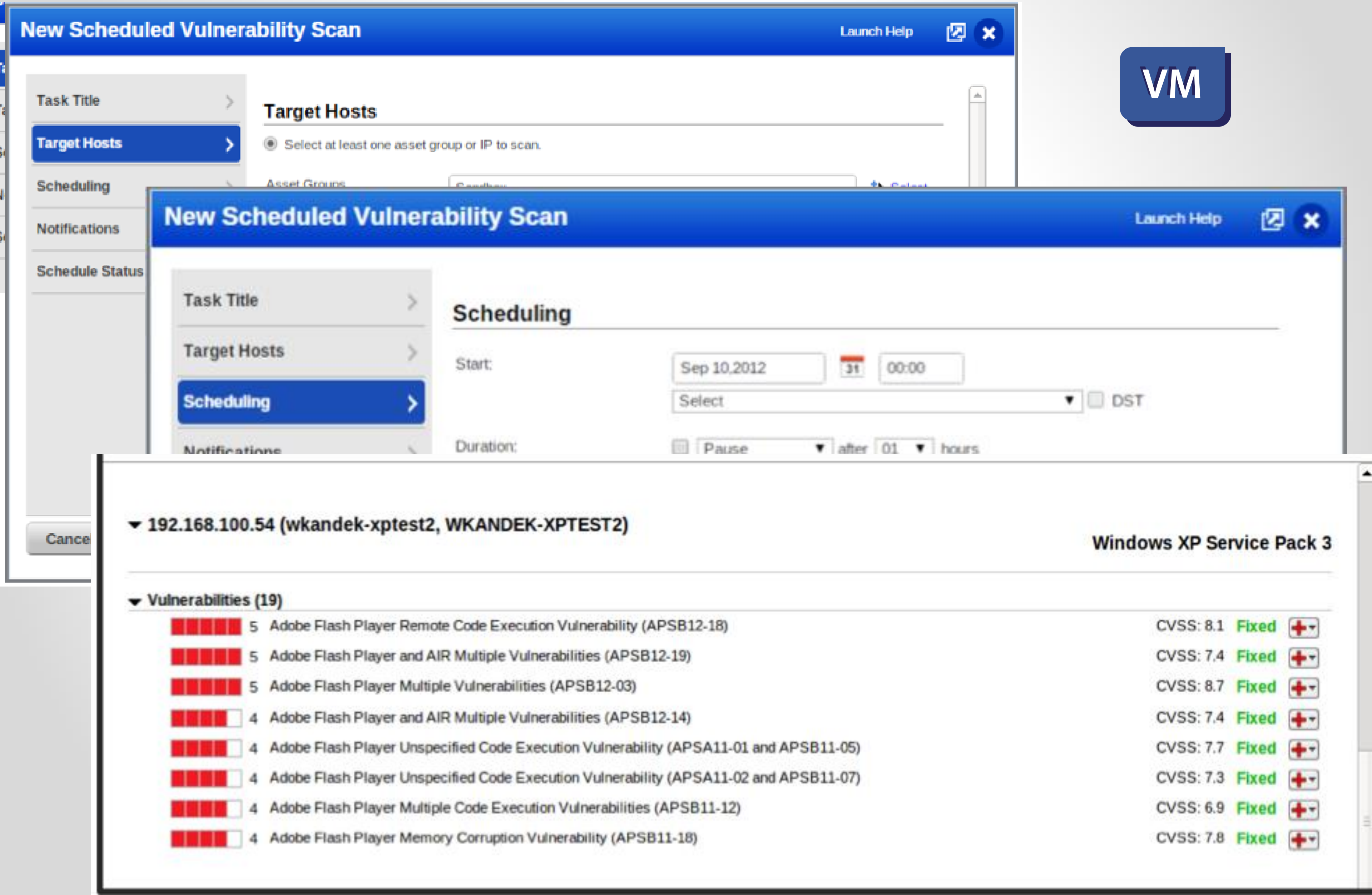
How QualysGuard supports this:

VM

- Scheduled & On demand Vulnerability Scanning
- Continuous Vulnerability Assessment
- Authenticated Scanning
- Patch Verification
- Report on Unauthorized Services
- With full support for automation
  - Scheduled scans & reports
  - Email reports
  - Alerting on exceptions
  - Ticketing with SLA metrics and confirmation
  - API for Integration with IPS, SIEM etc

CC4: Continuous Vulnerability Assessment/Remediation

VM



Target Hosts

● Select at least one asset group or IP to scan.

Asset Groups: Sandbox

Scheduling

Start: Sep 10,2012 00:00

Select ▾ □ DST

Duration: □ Pause ▾ after 01 ▾ hours

▾ 192.168.100.54 (wkandek-xptest2, WKANDEK-XPTEST2)

Windows XP Service Pack 3

▾ Vulnerabilities (19)

🟥🟥🟥🟥🟥	5	Adobe Flash Player Remote Code Execution Vulnerability (APSB12-18)	CVSS: 8.1	Fixed
🟥🟥🟥🟥🟥	5	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB12-19)	CVSS: 7.4	Fixed
🟥🟥🟥🟥🟥	5	Adobe Flash Player Multiple Vulnerabilities (APSB12-03)	CVSS: 8.7	Fixed
🟥🟥🟥🟥	4	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB12-14)	CVSS: 7.4	Fixed
🟥🟥🟥🟥	4	Adobe Flash Player Unspecified Code Execution Vulnerability (APSA11-01 and APSB11-05)	CVSS: 7.7	Fixed
🟥🟥🟥🟥	4	Adobe Flash Player Unspecified Code Execution Vulnerability (APSA11-02 and APSB11-07)	CVSS: 7.3	Fixed
🟥🟥🟥🟥	4	Adobe Flash Player Multiple Code Execution Vulnerabilities (APSB11-12)	CVSS: 6.9	Fixed
🟥🟥🟥🟥	4	Adobe Flash Player Memory Corruption Vulnerability (APSB11-18)	CVSS: 7.8	Fixed

CC5: Malware Defenses

Goal: The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.

How QualysGuard supports this:

VM

- Vulnerability Scan can detect installed Malware by running malicious services
- Authenticated Vulnerability Scan can detect installed Malware in file-system and registries
- Vulnerability Report will report discovered Malware

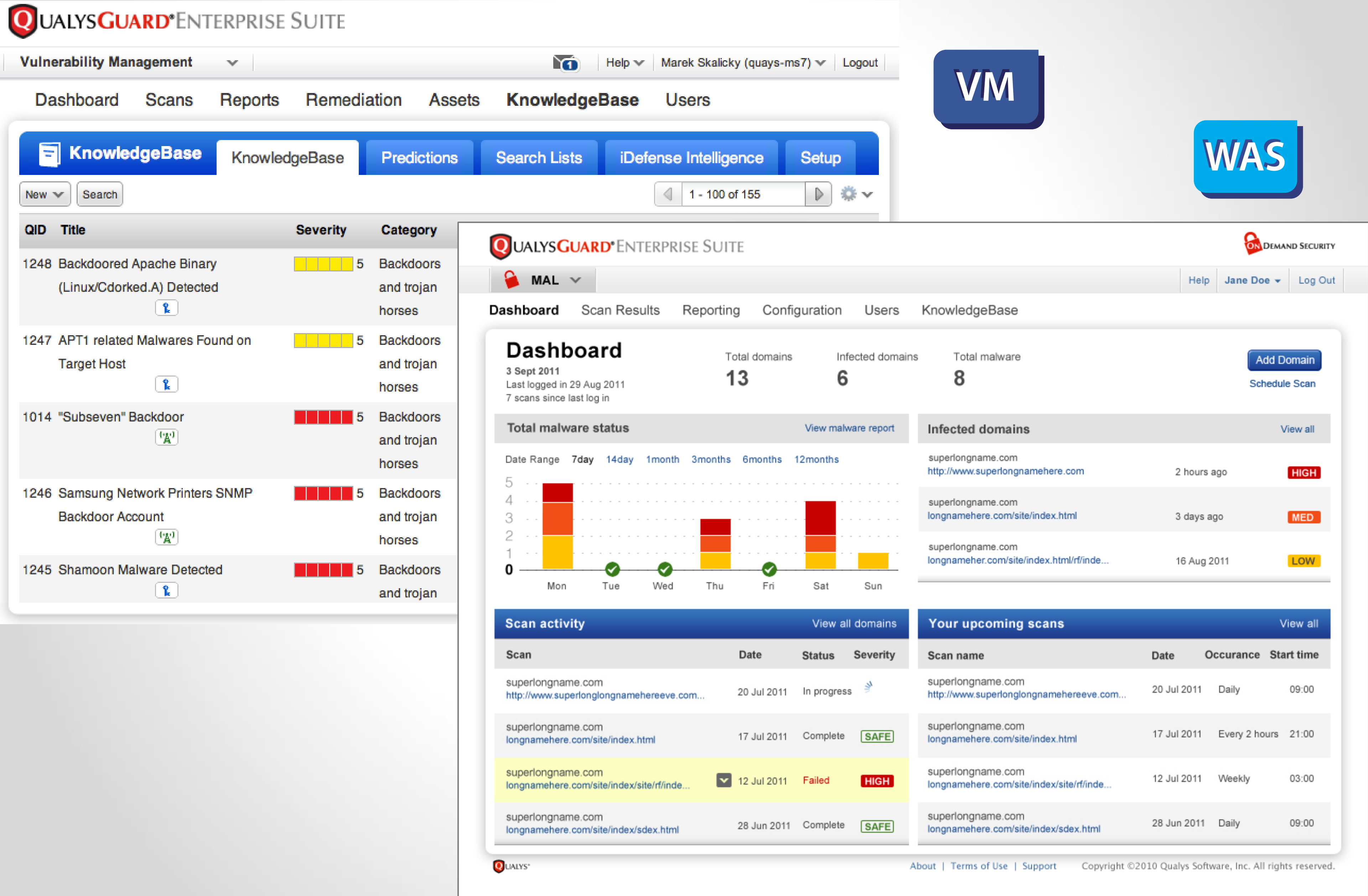
WAS

- Web Application Scan now contains Malware Detection Scan for web applications
- Static signatures and Behavioural Analyses of HTML code
- Malware Scan of web apps prevent clients from being infected by corporate web sites

CC5: Malware Defenses

VM

WAS



QUALYSGUARD® ENTERPRISE SUITE

QID	Title	Severity	Category
1248	Backdoored Apache Binary (Linux/Cdorked.A) Detected	5	Backdoors and trojan horses
1247	APT1 related Malwares Found on Target Host	5	Backdoors and trojan horses
1014	"Subseven" Backdoor	5	Backdoors and trojan horses
1246	Samsung Network Printers SNMP Backdoor Account	5	Backdoors and trojan horses
1245	Shamoon Malware Detected	5	Backdoors and trojan

QUALYSGUARD® ENTERPRISE SUITE

Dashboard

3 Sept 2011
Last logged in 29 Aug 2011
7 scans since last log in

Total domains	Infected domains	Total malware
13	6	8

Total malware status View malware report

Infected domains View all

superlongname.com http://www.superlongnamehere.com	2 hours ago	HIGH
superlongname.com longnamehere.com/site/index.html	3 days ago	MED
superlongname.com longnameher.com/site/index.html/rf/inde...	16 Aug 2011	LOW

Scan activity View all domains

Scan	Date	Status	Severity
superlongname.com http://www.superlonglongnamehereeve.com...	20 Jul 2011	In progress	
superlongname.com longnamehere.com/site/index.html	17 Jul 2011	Complete	SAFE
superlongname.com longnamehere.com/site/index/site/rf/inde...	12 Jul 2011	Failed	HIGH
superlongname.com longnamehere.com/site/index/sdex.html	28 Jun 2011	Complete	SAFE

Your upcoming scans View all

Scan name	Date	Occurance	Start time
superlongname.com http://www.superlonglongnamehereeve.com...	20 Jul 2011	Daily	09:00
superlongname.com longnamehere.com/site/index.html	17 Jul 2011	Every 2 hours	21:00
superlongname.com longnamehere.com/site/index/site/rf/inde...	12 Jul 2011	Weekly	03:00
superlongname.com longnamehere.com/site/index/sdex.html	28 Jun 2011	Daily	09:00

CC6: Application Software Security

Goal: Effective application security ensures that developed and 3rd party delivered applications are protected from attackers who inject specific exploits to gain control over vulnerable machines.

How QualysGuard supports this:

WAS

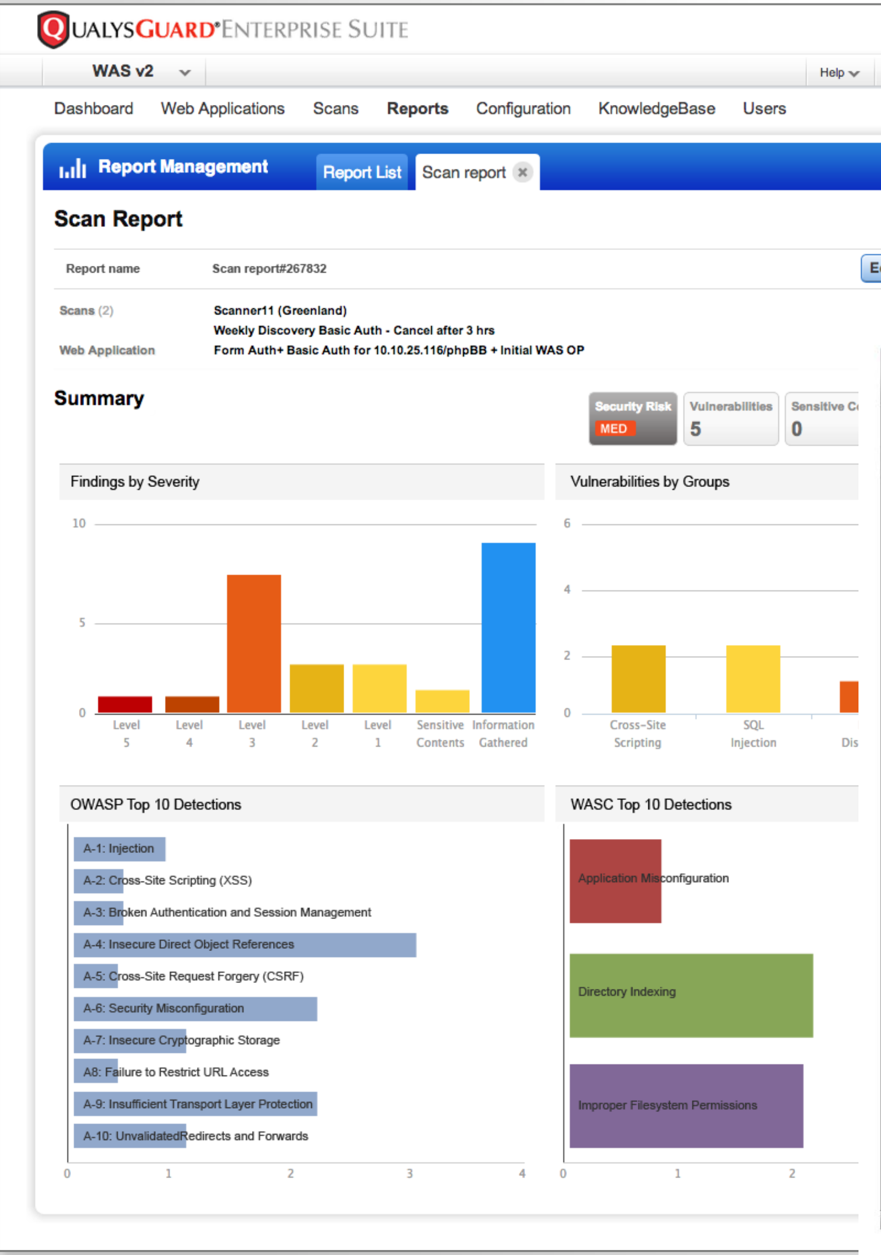
- Scheduled & On demand Web Application Scanning
- OWASP TOP-10 and WASC TOP-10 Vulnerabilities supported
- Web application discovery (web crawling)
- User - Authentication support
- Fully unattended and automated
- Part of development lifecycle
- With full support for automation
  - Scheduled scans & reports
  - Ticketing with SLA metrics and confirmation
  - API for Integration with WAF

WAF provides active protection of corporate data and reputation provided via web application interface

WAF

Prevention with WAS and Protection with WAF available in the same UI and integrated security suite

CC6: Application Software Security



QUALYSGUARD ENTERPRISE SUITE

WAS v2 | Help | Vanessa FOLLYS | Log Out

Dashboard | Web Applications | Scans | Reports | Configuration | KnowledgeBase | Users

Report Management | Report List | Scan report | Edit Report | Download

Scan Report

Report name: Scan report#267832

Scans (2): Scanner11 (Greenland)
Weekly Discovery Basic Auth - Cancel after 3 hrs

Web Application: Form Auth+ Basic Auth for 10.10.25.116/phpBB + Initial WAS OP

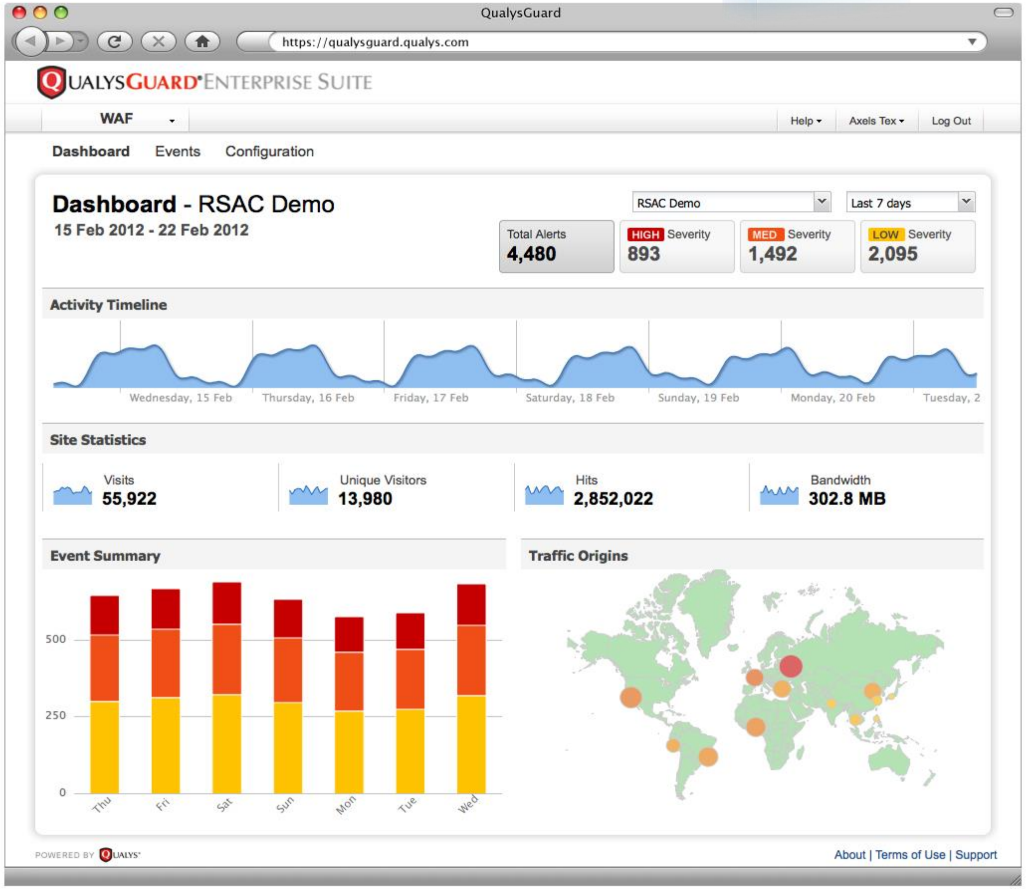
Summary

Security Risk: MED | Vulnerabilities: 5 | Sensitive C: 0

Findings by Severity
10
5
0
Level 5
Level 4
Level 3
Level 2
Level 1
Sensitive Contents
Information Gathered
Vulnerabilities by Groups
6
4
2
0
Cross-Site Scripting
SQL Injection
Dis
OWASP Top 10 Detections
A-1: Injection
A-2: Cross-Site Scripting (XSS)
A-3: Broken Authentication and Session Management
A-4: Insecure Direct Object References
A-5: Cross-Site Request Forgery (CSRF)
A-6: Security Misconfiguration
A-7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A-9: Insufficient Transport Layer Protection
A-10: UnvalidatedRedirects and Forwards
0
1
2
3
4
WASC Top 10 Detections
Application Misconfiguration
Directory Indexing
Improper Filesystem Permissions
0
1
2

WAS

WAF



QualysGuard

https://qualysguard.qualys.com

QUALYSGUARD ENTERPRISE SUITE

WAF | Help | Axels Tex | Log Out

Dashboard | Events | Configuration

Dashboard - RSAC Demo

15 Feb 2012 - 22 Feb 2012

RSAC Demo | Last 7 days

Total Alerts	HIGH Severity	MED Severity	LOW Severity
4,480	893	1,492	2,095

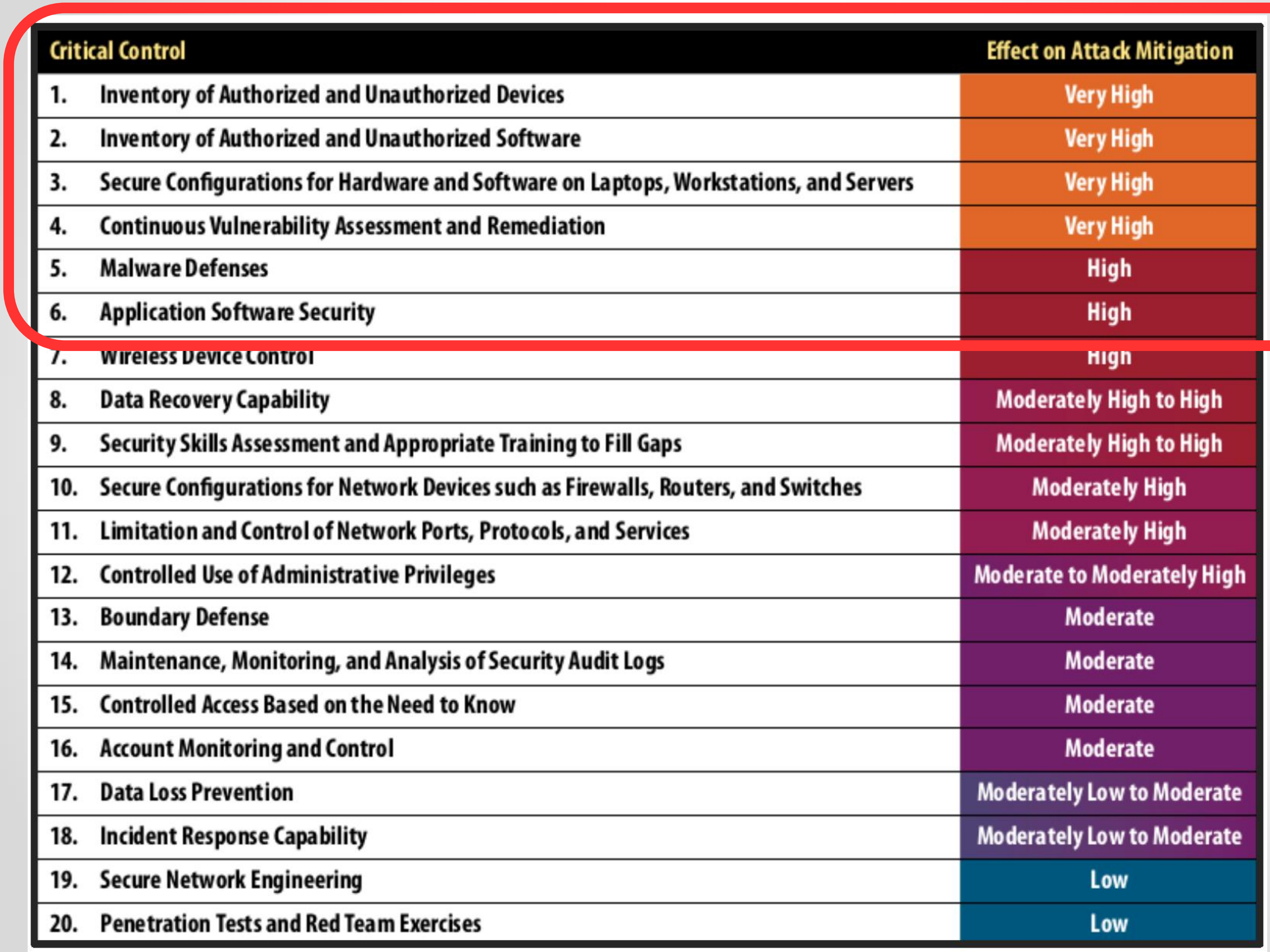
Site Statistics

Visits	Unique Visitors	Hits	Bandwidth
55,922	13,980	2,852,022	302.8 MB

POWERED BY QUALYS

About | Terms of Use | Support

SANS TOP 20 Critical Controls - REMINDER

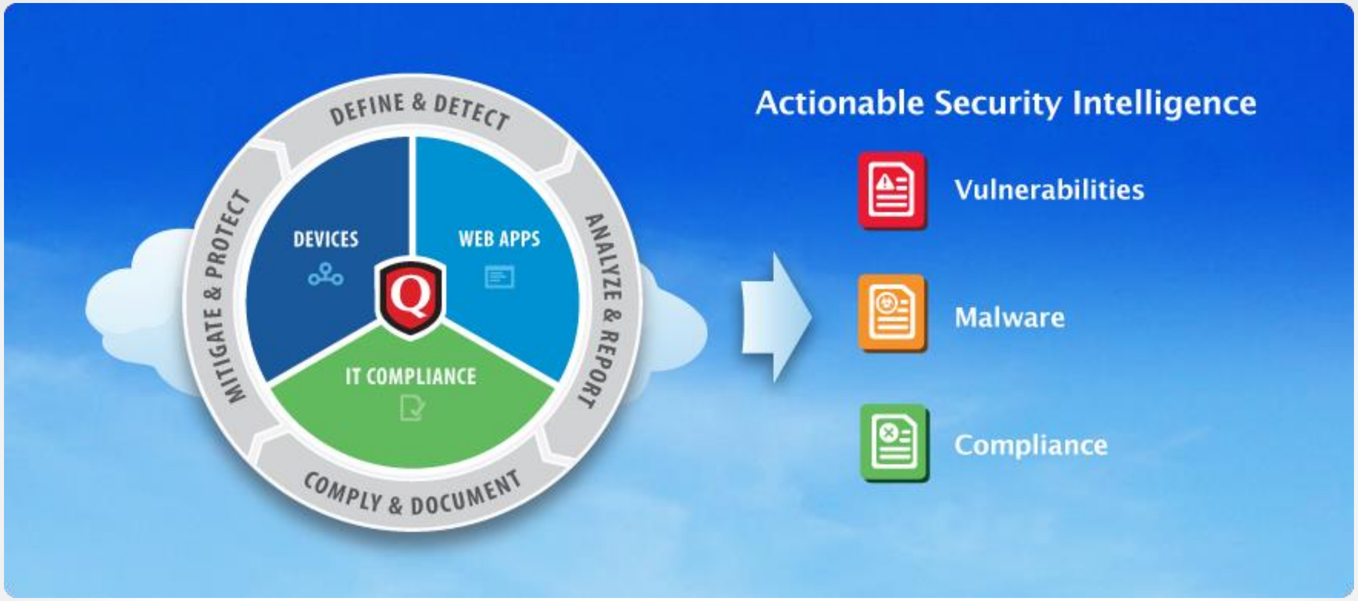


Critical Control		Effect on Attack Mitigation	
1.	Inventory of Authorized and Unauthorized Devices	Very High	Q
2.	Inventory of Authorized and Unauthorized Software	Very High	Q
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High	Q
4.	Continuous Vulnerability Assessment and Remediation	Very High	Q
5.	Malware Defenses	High	Q
6.	Application Software Security	High	Q
7.	Wireless Device Control	High	Q
8.	Data Recovery Capability	Moderately High to High	
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High	
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High	Q
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High	Q
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High	Q
13.	Boundary Defense	Moderate	
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate	
15.	Controlled Access Based on the Need to Know	Moderate	
16.	Account Monitoring and Control	Moderate	
17.	Data Loss Prevention	Moderately Low to Moderate	
18.	Incident Response Capability	Moderately Low to Moderate	
19.	Secure Network Engineering	Low	
20.	Penetration Tests and Red Team Exercises	Low	Q

Advance Vulnerability Management with QualysQuard delivers **Very High and High** effect on Cyber-Attack Mitigation….

Qualys at a Glance

A pioneer and leader in Cloud Security & Compliance



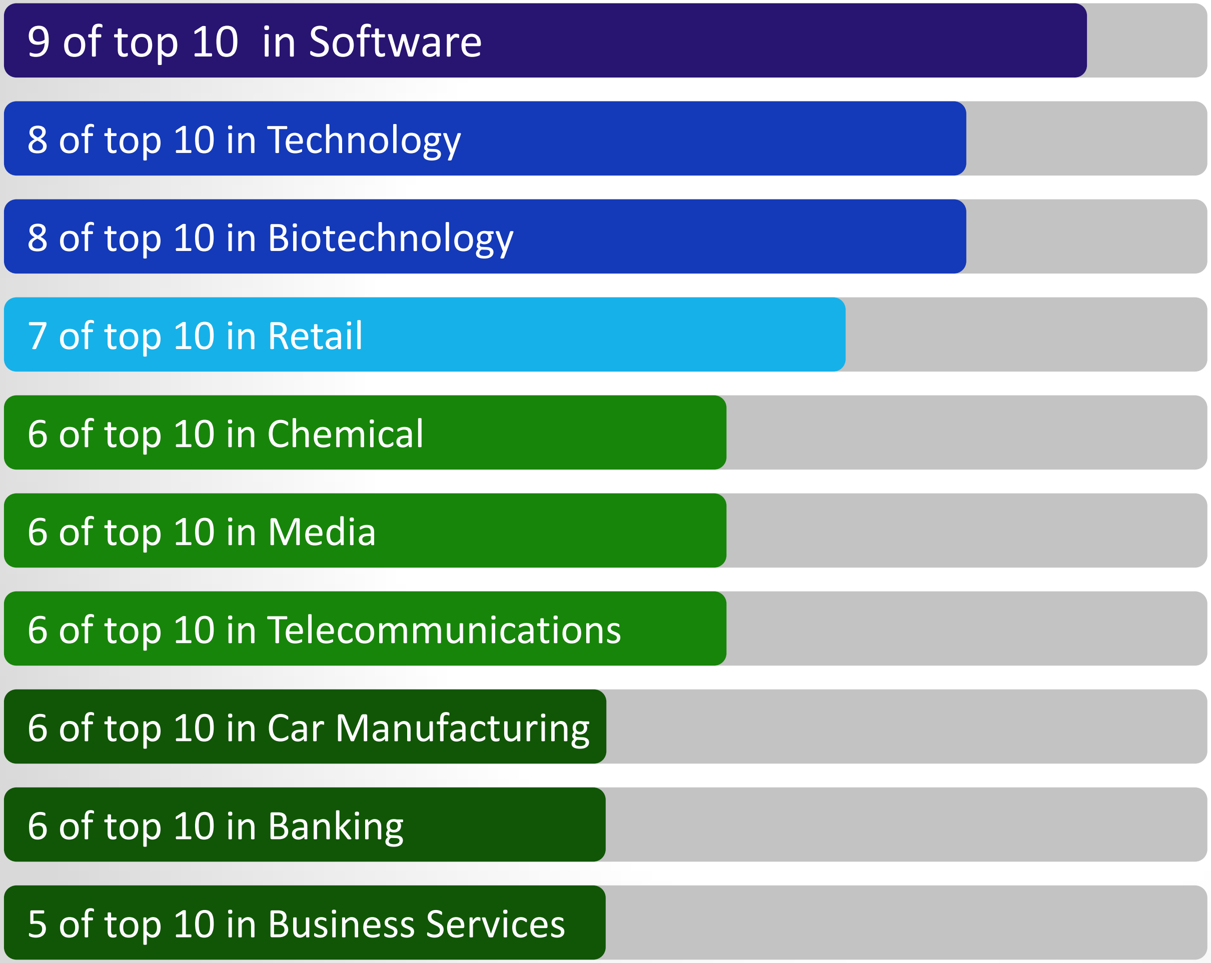
QualysGuard Cloud Platform & Suite of Integrated Solutions

6,000+	Customers	100+	Countries	$95M	LTM Revenues*

The 12 months ended March 31st 2013

Blue Chip Global Customer Base

63% F50 – 55% F100 – 40% F500 – 32% F1000 -22% Forbes Global 2000



9 of top 10 in Software

8 of top 10 in Technology

8 of top 10 in Biotechnology

7 of top 10 in Retail

6 of top 10 in Chemical

6 of top 10 in Media

6 of top 10 in Telecommunications

6 of top 10 in Car Manufacturing

6 of top 10 in Banking

5 of top 10 in Business Services

6,150^{+} Customers

ADP Agilent Technologies ally

accenture Bayer Boston Scientific

bp BASF The Chemical Company Cargill

CATERPILLAR CISCO DAIMLER

DU PONT Deloitte. ERNST & YOUNG

gsk GlaxoSmithKline Goldman Sachs GM THE HOME DEPOT

KPMG Lilly Ogilvy

ORACLE PRICEWATERHOUSECOOPERS Russell Investments

Symantec. STAPLES T-Mobile

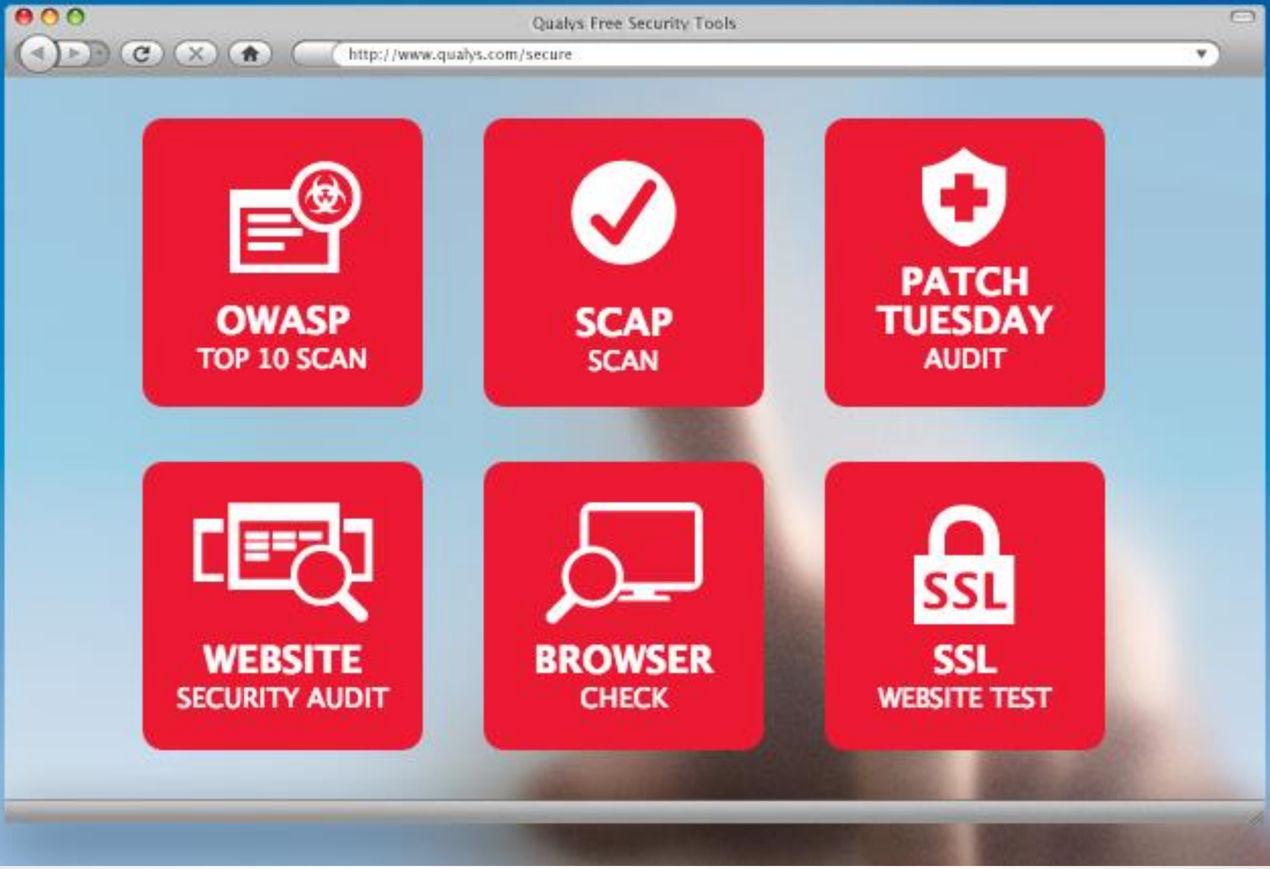
THOMSON VeriSign THE WB TELEVISION NETWORK

Based on Forbes Global 2000 Classification

Security at Your Fingertips - FREE

Make sure your systems are secure and compliant.

Select a free tool below. There's nothing to download!



www.qualys.com/secure

Thank you for

analytica

- Managed Security Services Provider
- Value added Reseller of Qualys Services
- Integration
- Training
- and more …

Request evaluation

WIN A BACKPACK

http://tiny.cc/4abe5w

QUALYS®

CONTINUOUS SECURITY

Thank You