



Security in knowledge

Automating the 20 Critical Security Controls

Andrew Wild

Qualys

Wolfgang Kandek

Qualys

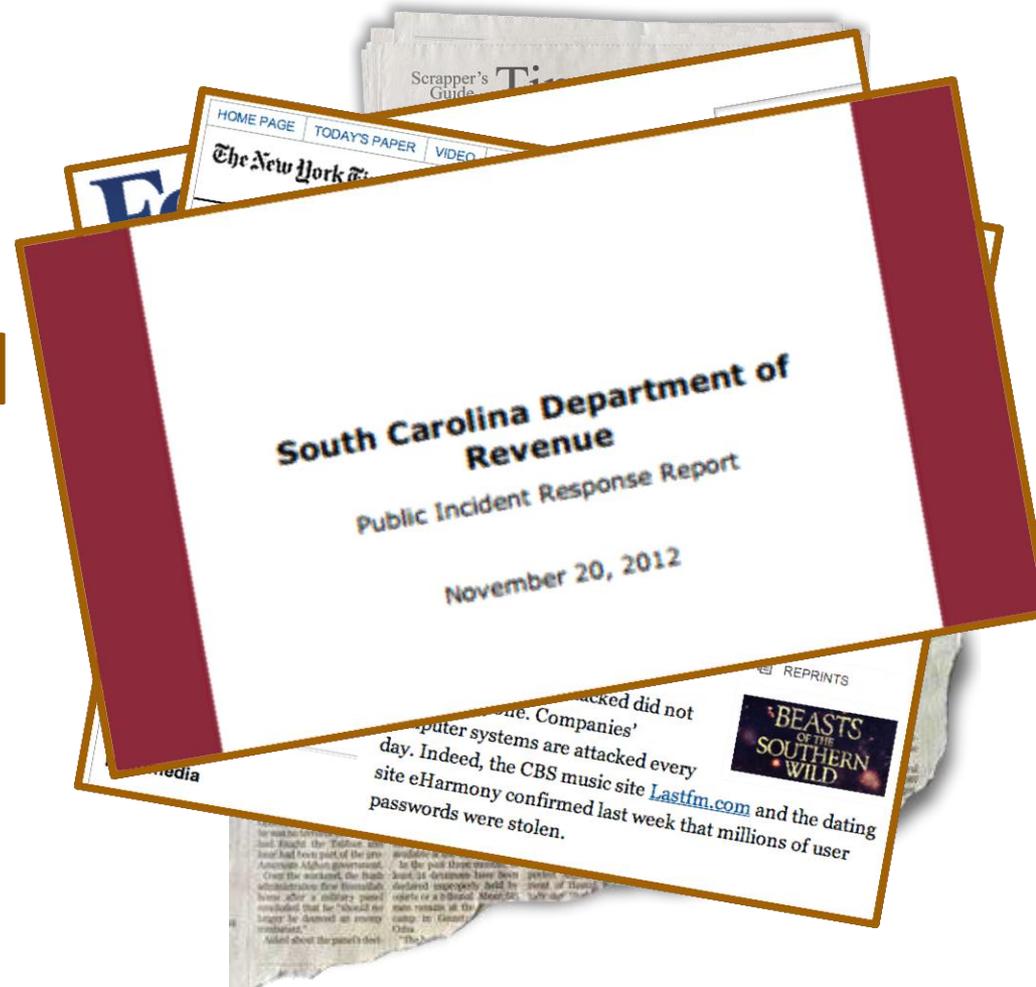
Session ID: SPO1-T19

Session Classification: Intermediate

2011 – the Year of Data Breaches



2012 – proceeded almost the same



2013 – started in a similar Way



Background

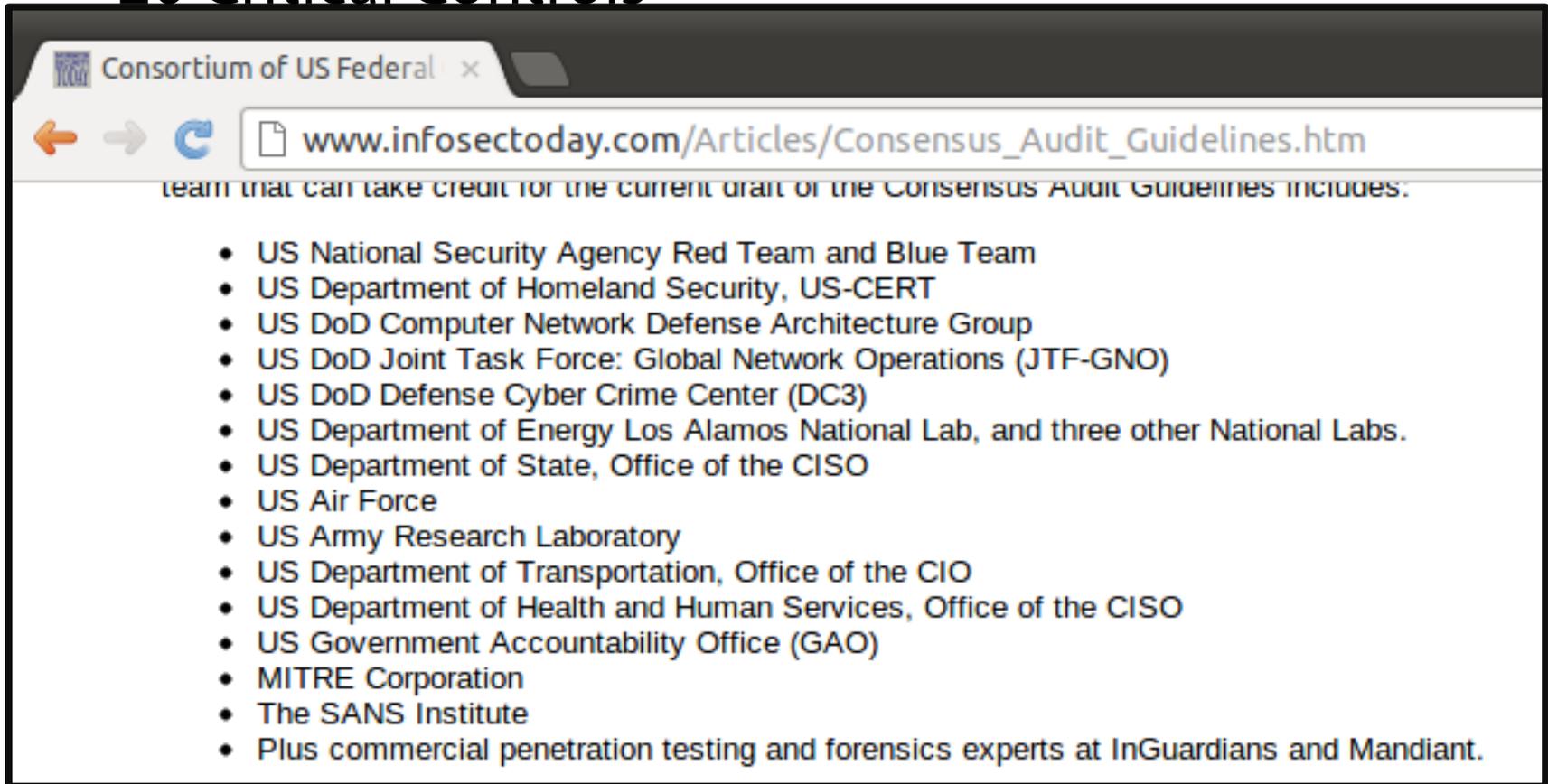
- Open System Administration Channels
 - Default and Weak Passwords
 - End-user has Administrator Privileges
 - Outdated Software Versions
 - Non-hardened Configurations
- ▶ Flaws in System Administration

Solution

- 20 Critical Controls
- Owned by SANS
 - with widespread industry expert input

Solution

- 20 Critical Controls



The screenshot shows a web browser window with the address bar containing the URL www.infosectoday.com/Articles/Consensus_Audit_Guidelines.htm. The page content includes a list of 20 critical controls that can take credit for the current draft of the Consensus Audit Guidelines. The list is as follows:

- US National Security Agency Red Team and Blue Team
- US Department of Homeland Security, US-CERT
- US DoD Computer Network Defense Architecture Group
- US DoD Joint Task Force: Global Network Operations (JTF-GNO)
- US DoD Defense Cyber Crime Center (DC3)
- US Department of Energy Los Alamos National Lab, and three other National Labs.
- US Department of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Department of Transportation, Office of the CIO
- US Department of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE Corporation
- The SANS Institute
- Plus commercial penetration testing and forensics experts at InGuardians and Mandiant.

Solution

- 20 Critical Controls
- Owned by SANS
 - with widespread industry expert input
 - International participation

Solution

The screenshot shows a web browser window with the address bar displaying www.cpni.gov.uk/advice/cyber/Critical-controls/. The page header includes the CPNI logo and the text "Centre for the Protection of National Infrastructure". A navigation menu contains links for "Home", "About CPNI", "Threats", and "Security advice". Below the menu, a breadcrumb trail reads "Home | Security advice | Cyber security | Critical controls". A banner image features the word "email" repeated in a digital font. The main content area is titled "Cyber security" and includes a list of sub-topics: "Critical controls" (with sub-items "Getting started" and "In depth"), "Protecting business systems", and "Understanding electronic attack". There are also checkboxes for "Personnel security" and "Physical security". The article title is "Top 20 critical security controls for cyber defence", followed by a share button showing "222" shares and icons for YouTube and a printer. The article text begins: "The top 20 critical security controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence. CPNI is participating in an international government-industry effort to promote the top 20 critical controls for computer and network security. The development of these controls is being coordinated by the SANS Institute."

Solution

Strategies to Mitigate Targeted Cyber Intrusions: DSD Defence Signals Directorate - Google Chrome

www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.	Excellent	Low	High	High	Prevent	Yes	No	No
2	Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.	Excellent	Low	Medium	Medium	Prevent	Yes	Possible	Possible

Physical security

Solution

- 20 Critical Controls
- Owned by SANS
 - with widespread industry input
 - International participation
- Prioritized

Solution

Critical Control	Effect on Attack Mitigation
1. Inventory of Authorized and Unauthorized Devices	Very High
2. Inventory of Authorized and Unauthorized Software	Very High
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4. Continuous Vulnerability Assessment and Remediation	Very High
5. Malware Defenses	High
6. Application Software Security	High
7. Wireless Device Control	High
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
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12. Controlled Use of Administrative Privileges	Moderate to Moderately High
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

Solution

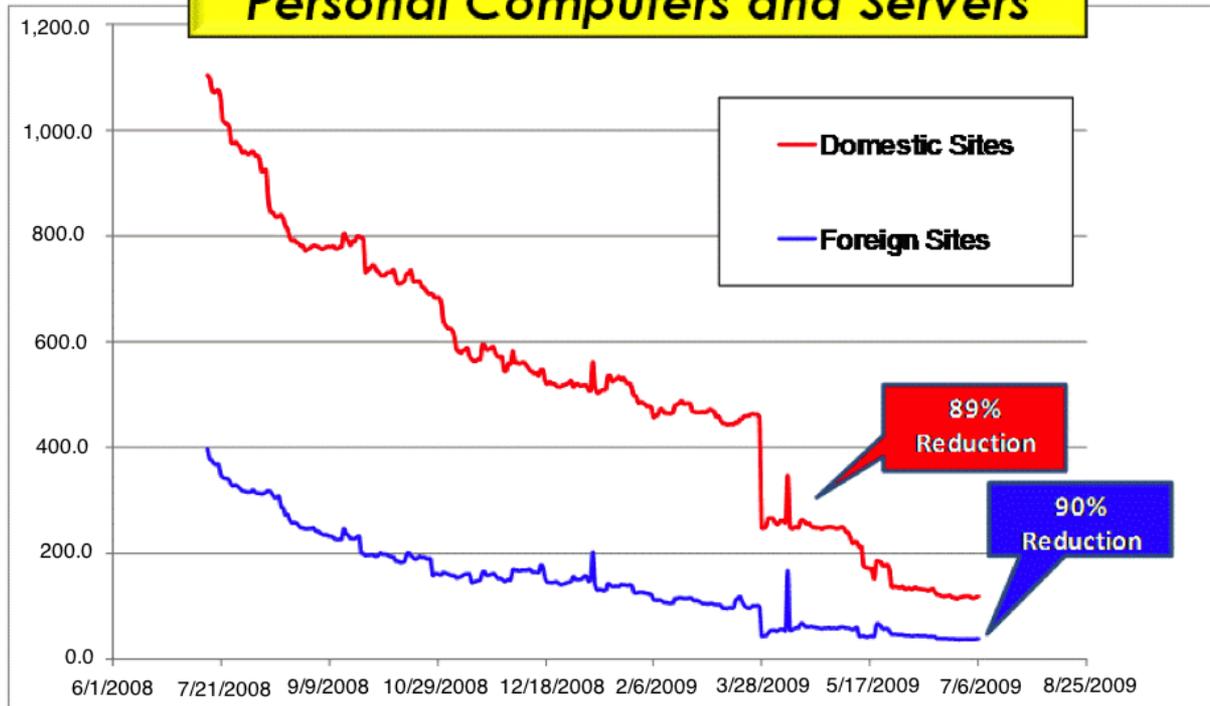
- 20 Critical Controls
- Owned by SANS
 - With widespread industry expert input
 - International participation
- Prioritized
- Automation is critical to success

Solution



Results First 12 Months

Personal Computers and Servers



Solution

- 20 Critical Controls
- Owned by SANS
 - with widespread industry input
 - International participation
- Prioritized
- Automation is critical to success
 - 90 % Risk Reduction at US DoS
 - 85 % Incident Reduction at DSD Australia

Solution

Critical Control	Effect on Attack Mitigation
1. Inventory of Authorized and Unauthorized Devices	Very High
2. Inventory of Authorized and Unauthorized Software	Very High
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4. Continuous Vulnerability Assessment and Remediation	Very High

Qualys

- QualysGuard
 - Vulnerability Management
 - Policy Compliance
 - Web Application Scanning
 - PCI
 - Malware Detection
- SaaS Solution
 - Browser-based, Multi-tenant
 - Public and Private Cloud
 - Scanning, Reporting, Ticketing
 - Extensive API

CC1: Hardware Inventory

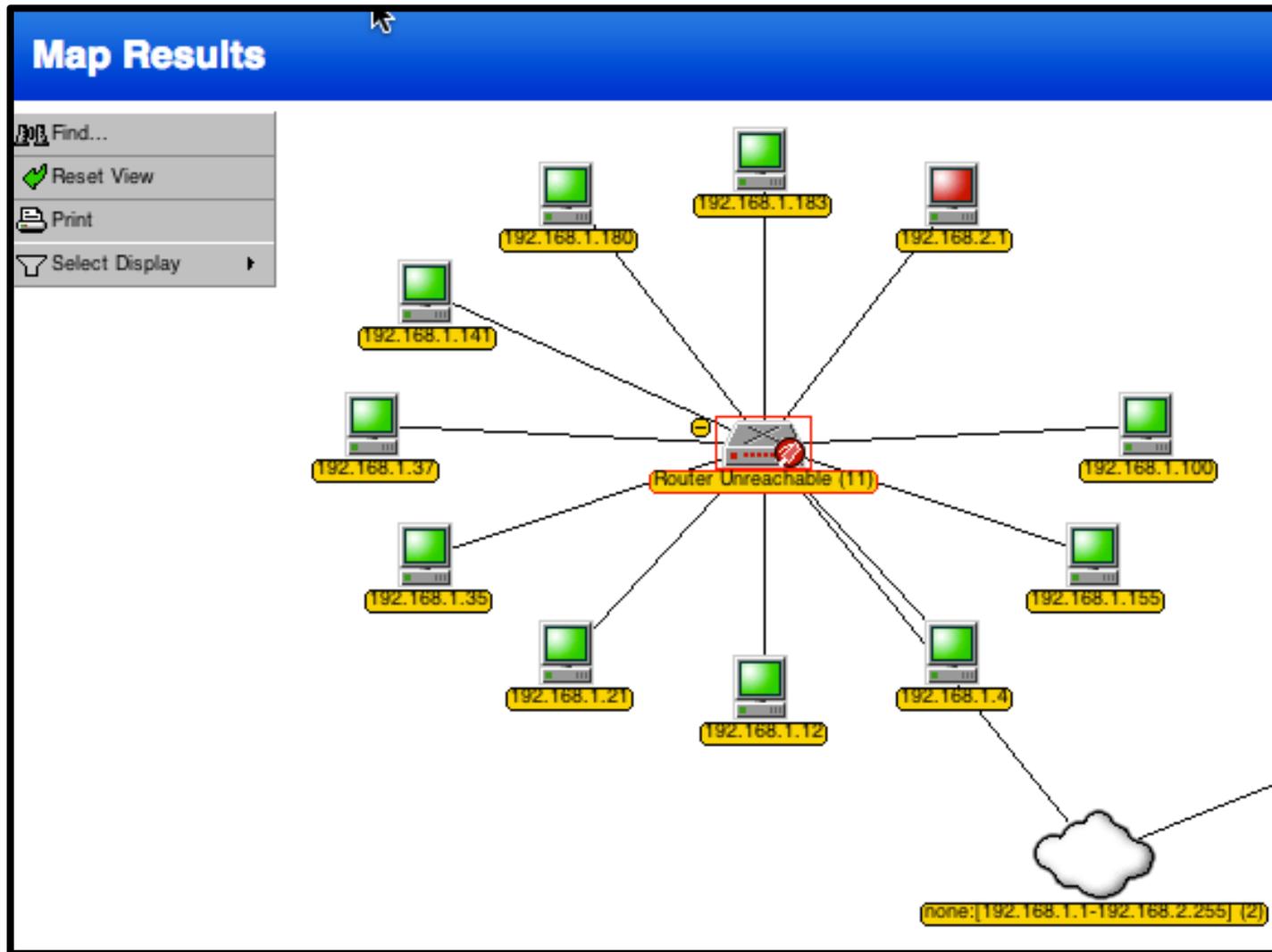
- Asset Visibility
 - Size of Network
 - Machine Types
 - Location

CC1: Hardware Inventory

The screenshot displays the Qualys Guard Enterprise Suite interface. At the top, the logo and name 'QUALYS GUARD ENTERPRISE SUITE' are visible. Below the logo, there is a navigation bar with tabs for 'Dashboard', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase', and 'Users'. The 'Assets' tab is currently selected. Underneath, there are sub-tabs for 'Assets', 'Asset Groups', 'Host Assets', 'Asset Search', 'Virtual Hosts', 'Domains', 'Applications', and 'Ports/Ser'. A search bar and a 'Filters' dropdown are present. The main content area shows a table of host assets with columns for IP address, host name, and operating system. The last row is highlighted in blue.

IP	Host Name	OS
67.188.157.40	c-67-188-157-40.hsd1.ca.comcast.net	
67.202.41.187	ec2-67-202-41-187.compute-1.amazonaws.com	Oracle Enterprise Linux 5.2
68.123.47.151	adsl-68-123-47-151.dsl.pltn13.pacbell.net	Linux 2.4-2.6
68.124.23.73	adsl-68-124-23-73.dsl.pltn13.pacbell.net	Linux 2.4-2.6
69.181.165.102		
70.1.238.61	70-1-238-61.pools.spcsdns.net	Windows 2003/XP
70.96.188.21	box21.bluehost.com	
71.198.187.95	c-71-198-187-95.hsd1.ca.comcast.net	
75.101.203.111	ec2-75-101-203-111.compute-	Linux 2.4-2.6 / by_di.pl

CC1: Hardware Inventory



CC1: Hardware Inventory

- Asset Visibility
 - Size of Network
 - Machine Types
 - Location
- New Equipment Detection
 - Authorized
 - Unauthorized

CC1: Hardware Inventory



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	Netblock	Status
192.168.100.55		WKANDEK-XPTTEST3		Windows XP Service Pack 2-3		S	L	N	Added
192.168.100.57				Ubuntu / Linux 2.6.x		S	L	N	Added

CC1: Hardware Inventory

- Automation
 - Scans are scheduled
 - Delta Reports are scheduled
 - Reports can be e-mailed
 - Alerting on newly discovered hosts
 - Via API
 - Integration into Asset Management Systems
 - Via API
 - Coming: ticket generation on newly discovered hosts

CC2: Software Inventory

- Asset Visibility
 - Operating Systems
 - Applications
 - Versions
 - Patch Levels
- Blacklisting

CC2: Software Inventory

(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

CC2: Software Inventory

- Asset Visibility
 - Operating Systems
 - Applications
 - Versions
 - Patch Levels
- Blacklisting
- Whitelisting

CC2: Software Inventory

- Asset Visibility

(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 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

contains regular expression list

Microsoft Office

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

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

CC2: Software Inventory

- Asset Visibility
 - Operating Systems
 - Applications
 - Versions
 - Patch Levels
- Blacklisting
- Whitelisting
- Interactive Search

CC2: Software Inventory

The screenshot shows the Qualys software inventory interface. At the top, there is a navigation bar with tabs for Assets, Asset Groups, Host Assets, Asset Search, Virtual Hosts, Domains, and Applications. Below the navigation bar, there are search filters for Application, Asset Group, and IP Address or Net Block. The IP Address or Net Block field contains the value 192.168.100.51. There are Search and Download CSV buttons. Below the search filters, there is a table with two columns: IP / DNS Hostname and Version. The table lists several applications installed on the host 192.168.100.51 (wkandek-xptest):

IP / DNS Hostname	Version
123 Write All Stored Passwords (1 Host)	
192.168.100.51 wkandek-xptest	
Adobe Flash Player 10 ActiveX (1 Host)	
192.168.100.51 wkandek-xptest	10.2.152.32
Adobe Reader 9.3 (1 Host)	
192.168.100.51 wkandek-xptest	9.3.0
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595) (1 Host)	
192.168.100.51 wkandek-xptest	1
Hotfix for Windows XP (KB954550-v5) (1 Host)	
192.168.100.51 wkandek-xptest	5
Look@LAN 2.50 Build 35 (1 Host)	
192.168.100.51 wkandek-xptest	

CC2: Software Inventory

The screenshot displays the QualysGuard Enterprise Suite interface. At the top, there is a navigation bar with tabs for Assets, Asset Groups, Host Assets, Asset Search, Virtual Hosts, Domains, and Applications. Below this is a search bar with the text "Search for Application: and Asset Group: and IP Address or Net Block:". The main header area includes the QualysGuard logo and the text "QUALYS GUARD ENTERPRISE SUITE". Below the header, there is a secondary navigation bar with tabs for Dashboard, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. A third navigation bar is visible, with tabs for Assets, Asset Groups, Host Assets, Asset Search, Virtual Hosts, Domains, Applications, and Ports/Services. The search bar is populated with "mirc" in the "Application" field. Below the search bar, there is a table with the following data:

IP / DNS Hostname	Version
mIRC (4 Hosts)	
192.168.100.51 wkandek-xptest	7.19
192.168.100.55 wkandek-xptest3	7.19
192.168.100.56 wkandek-xptest4	7.19
192.168.100.54 wkandek-xptest2	7.19

CC2: Software Inventory

- Automation
 - Scans are scheduled
 - Reports are scheduled
 - Reports can be emailed
 - Alerting on Exceptions
 - Via API
 - Integration into Asset Management Systems
 - Via API
 - Coming: Ticket generation on Exceptions

CC3: Secure Base Configurations

- Configuration Validation
 - SCAP/FDCC

CC3: Secure Base Configurations

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 Owner: -
DNS Name: wkandek-xptest2 Location:
NetBIOS Name: WKANDEK-XPTTEST2 Function:
OS: Windows XP AssetTag:
Last Scan Date: 09/10/2012 at 11:30:05 (GMT-0700)

CCE	CCE4	Rule ID	Rule Title	Posture
CCE-2928-0	CCE-980	account_lockout_duration	Account Lockout Duration	Failed
CCE-2986-8	CCE-658	account_lockout_threshold	Account Lockout Threshold	Failed
CCE-3040-3	CCE-332	GuestAccountStatus	Accounts: Guest account status	Passed
CCE-2344-0	CCE-533	LimitBlankPassword	Accounts: Limit local account use of blank passwords to console logon only	Passed
CCE-3135-1	CCE-438	RenameAdministrator	Accounts: Rename administrator account	Failed
CCE-3025-4	CCE-834	RenameGuest	Accounts: Rename guest account	Failed
CCE-2864-7	CCE-842	DebugPrograms_Administrators	Administrators Have Right To Debug Programs	Passed
CCE-3034-6	CCE-487	AlerterService	Alerter Service Disabled	Passed
CCE-3100-5	CCE-231	Always-Use-Classic-Logon	Always Use Classic Logon	Failed
CCE-2052-9	CCE-600	arp.exePermissions	arp.exe Permissions	Failed
CCE-2184-0	CCE-393	at.exePermissions	at.exe Permissions	Failed
CCE-2312-7	CCE-166	attrib.exePermissions	attrib.exe Permissions	Failed
CCE-3162-5	CCE-2	AuditAccessToGlobalObjects	Audit: Audit the access of global system objects	Passed

231 of 231 Items Shown, 0 selected

CC3: Secure Base Configurations

- Configuration Validation
 - SCAP/FDCC
 - Cyberscope Reporting
 - CIS

CC3: Secure Base Configurations

- Configuration Validation

Compliance Policy Library

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

- Weekly/Daily Scheduled Vulnerability Scanning

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning

New Scheduled Vulnerability Scan

Launch Help  

- Task Title** >
- Target Hosts >
- Scheduling >
- Notifications >
- Schedule Status >

Task Title

Title: *

Task Owner: *

Option Profile: [* Select](#)

Scanner Appliance: [View](#)

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning

New Scheduled Vulnerability Scan Launch Help

Task Title

Target Hosts

Scheduling

Notifications

Schedule Status

Target Hosts

Select at least one asset group or IP to scan.

Asset Groups [+ Select](#)

IPs/Ranges [+ Select](#)
Example:192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [+ Select](#)
Example:192.168.0.87-192.168.0.92, 192.168.0.200

Select at least one Asset Tag to scan.

Asset Tags

No tags have been selected

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning

The screenshot displays the 'New Scheduled Vulnerability Scan' dialog box with the 'Scheduling' tab selected. The dialog has a blue header with the title and 'Launch Help' link. On the left is a sidebar with navigation options: Task Title, Target Hosts, Scheduling (selected), Notifications, and Schedule Status. The main area is titled 'Scheduling' and contains the following fields:

- Start:** A date field set to 'Sep 10, 2012', a calendar icon showing '31', and a time field set to '00:00'.
- Time Zone:** A dropdown menu set to 'Select' and a checkbox for 'DST'.
- Duration:** A checkbox for 'Pause' followed by a dropdown set to 'after 01 hours'.
- Resume Days:** A dropdown menu set to 'Manually'.
- Occurs:** A dropdown menu set to 'Daily' and a text field set to '1 days'.
- Ends after:** A checkbox for 'Ends after' followed by an empty text field and the word 'occurrences'.

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning

CC4: Continuous Vulnerability Assessment/Remediation

The screenshot displays the Qualys Guard Enterprise Suite web interface. At the top, the logo and name "QUALYS GUARD ENTERPRISE SUITE" are visible. Below the logo is a navigation bar with a "VM" dropdown and a main menu containing "Dashboard", "Scans", "Reports", "Remediation", "Assets", "KnowledgeBase", and "Users". The "Scans" section is active, indicated by a blue bar with sub-tabs for "Scans", "Maps", "Schedules", "Appliances", "Option Profiles", and "Authentication".

Below the navigation bar, there are several controls: "Actions" (dropdown), "New" (dropdown), "Search", "Filters" (dropdown), and a "Windows Records" button. A dropdown menu is open under the "New" button, listing the following options:

- Windows Record...
- Unix Record...
- Oracle Record...
- Oracle Listener Record...
- SNMP Record...
- MS SQL Record...
- Cisco IOS Record...
- IBM DB2 Record...
- VMware Record...
- Authentication Vaults
- Download...

The background of the interface shows a table with columns for "Type" and "Name". The "Type" column contains several "Windows" entries, each with a checkbox. The "Name" column contains various system names, including "Palo Alto Auth".

CC4: Continuous Vulnerability Assessment/Remediation

The image shows a screenshot of the QualysGuard Enterprise web interface. On the left, a sidebar menu is open, showing a 'Scans' section with a 'Type' dropdown menu. The dropdown menu lists various record types: Windows Record..., Unix Record..., Oracle Record..., Oracle Listener Record..., SNMP Record..., MS SQL Record..., Cisco IOS Record..., IBM DB2 Record..., VMware Record..., Authentication Vaults, and Download... The main content area is titled 'New Unix Record' and is divided into two main sections: 'Login Credentials' and 'Policy Compliance'.

Login Credentials

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Basic authentication Authentication Vault

Basic authentication (user name and password) is supported for SSH1 and SSH2. Key authentication (RSA and/or DSA) is supported for SSH2 only.

User Name: *

Password: Clear Text Password

Confirm Password:

Root Delegation:

RSA Private Key:

Paste the RSA private key into the space provided (SSH2 only). See [Help](#) for proper formatting.

DSA Private Key:

Paste the DSA private key into the space provided (SSH2 only). See [Help](#) for proper formatting.

Policy Compliance

If services (SSH, telnet, rlogin) are not running on well known ports (22, 23, 513 respectively) enter the ports in the custom field below.

Ports: Well Known Ports (22,23,513) Custom Ports:

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
- Verify Patching

CC4: Continuous Vulnerability Assessment/Remediation

Fixed Vulnerabilities - Google Chrome
Qualys, Inc. [US] https://qualysguard.qualys.com/fo/report/view_report.php?id=4346382

Fixed Vulnerabilities

File View Help

▼ 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	+

CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
- Verify Patching
- Report on Unauthorized Services

CC4: Continuous Vulnerability Assessment/Remediation

The screenshot displays the 'Edit Scan Template' window with a blue header bar containing 'Edit Scan Template' and 'Launch Help'. On the left is a sidebar with navigation options: 'Report Title', 'Scan Results Section', 'Display', 'Filter', 'Services and Ports' (highlighted), and 'User Access'. The main area is titled 'Services' and is divided into three columns: 'Required Services', 'Available Services', and 'Unauthorized Services'. The 'Available Services' column contains a list of services including vnetd, voip sip, Volume Manager Storage Administration, VXWORKS WDBRPC UDP, watchguard admin, webshield, win remote desktop, winmx, WINS Replication, Wonderware InTouch, wmsserver, and WSUS_SERVER. Below this list is a 'View...' button. Between the columns are buttons for '<< Add', 'Add All', 'Remove >>', and 'Remove All'. The 'Unauthorized Services' column contains 'vnc'. Below the service lists is a 'Service Info' text area. The 'Ports' section below has a 'Required Ports:' label and an empty input field. At the bottom of the window are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

CC4: Continuous Vulnerability Assessment/Remediation

Edit Scan Template [Launch Help] [Close]

List Unauthorized Mgmt Services

File View Help

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	2	0	0	2
Total	2	0	0	2

5 Unauthorized Service Detected (2)

QID: 38175
Category: General remote services **CVSS Base:** 0 [1]
CVE ID: - **CVSS Temporal:** 0
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/12/2009
User Modified: -
Edited: No
PCI Vuln: Yes

- ▶ 192.168.100.54 (wkandek-xptest2, WKANDEK-XPTEST2) Windows XP Service Pack 3 CVSS: 0 **New**
- ▶ 192.168.100.55 (wkandek-xptest3, WKANDEK-XPTEST3) Windows XP Service Pack 3 CVSS: 0 **New**

Required Ports:

Cancel [Test] [Save As...] [Save]

CC4: Continuous Vulnerability Assessment/Remediation

The screenshot displays the Qualys Guard Enterprise Suite interface within an "Edit Scan Template" window. The main window title is "List Unauthorized Mgmt Services". The interface includes a navigation menu with "Assets" selected, and a sub-menu with "Ports/Services" selected. The search criteria are set to "VNC" for the port/service, "Sandbox" for the asset group, and an empty field for IP address or net block. The search results table shows two hosts with VNC services running on port 5900 via TCP.

QUALYS GUARD ENTERPRISE SUITE

VM

Dashboard Scans Reports Remediation **Assets** KnowledgeBase Users

Assets Asset Groups Host Assets Asset Search Virtual Hosts Domains Applications Ports/Services

Search for **Port or Service:** and **Asset Group:** and **IP Address or Net Block:**

VNC Sandbox **Search** **Download CSV**

IP / DNS Hostname	Protocol	Port	Default Service
vnc (2 Hosts)			
192.168.100.54 wkandek-xptest2	TCP	5900	vnc
192.168.100.55 wkandek-xptest3	TCP	5900	vnc

Cancel **Test** **Save As...** **Save**

CC4: Continuous Vulnerability Assessment/Remediation

- Automation
 - Scans are scheduled
 - Reports are scheduled
 - Reports are emailed
 - Alerting on Vulnerabilities
 - Tickets for Vulnerabilities, Remediation SLA and Confirmation
 - Integration into Asset Management Systems
 - Via API

Other Critical Controls

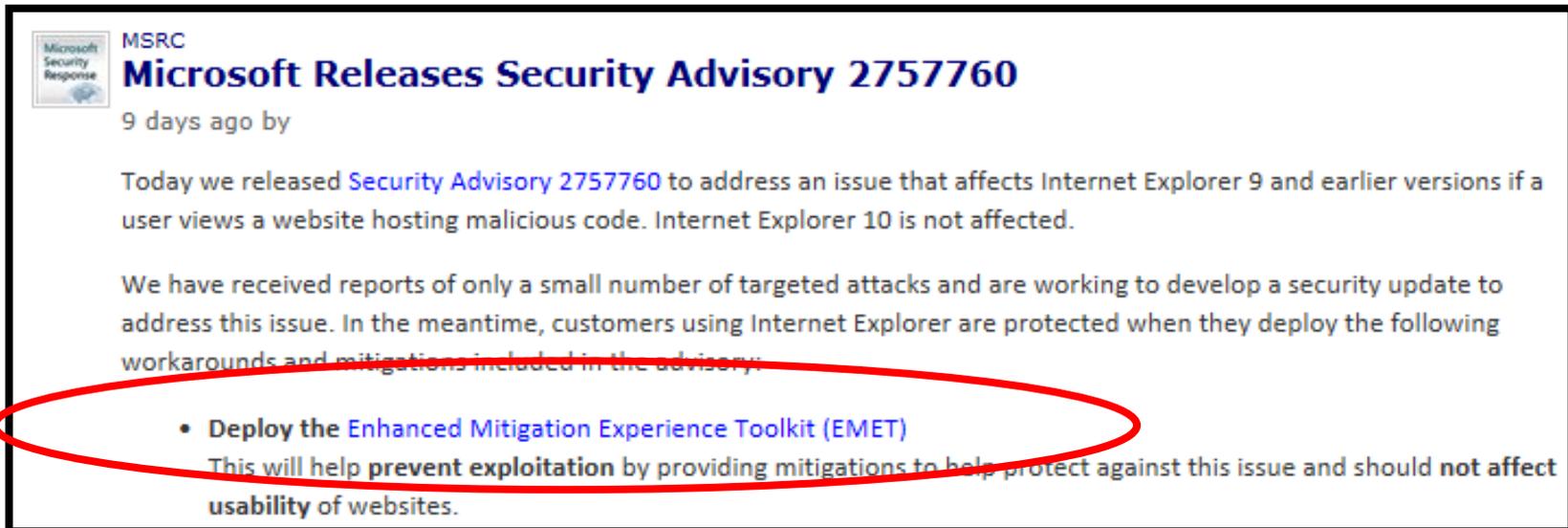
- CC6: Application Software Security
 - Automated Web Application Scans
- CC7: Wireless Device Controls
 - Wireside Detection
- CC11: Control of Network Ports
 - Scans and Reports for authorized and unauthorized Ports and Services
- CC16: Account Monitoring
 - Controls for Admin accounts, password policies, account lockout settings

Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
- Mitigated by use of EMET

Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)



The screenshot shows a Microsoft Security Response advisory. The title is 'Microsoft Releases Security Advisory 2757760'. The advisory is dated '9 days ago by'. The text states: 'Today we released Security Advisory 2757760 to address an issue that affects Internet Explorer 9 and earlier versions if a user views a website hosting malicious code. Internet Explorer 10 is not affected.' It then says: 'We have received reports of only a small number of targeted attacks and are working to develop a security update to address this issue. In the meantime, customers using Internet Explorer are protected when they deploy the following workarounds and mitigations included in the advisory:'. A red oval highlights the following bullet point: '• Deploy the Enhanced Mitigation Experience Toolkit (EMET)'. Below this, it says: 'This will help prevent exploitation by providing mitigations to help protect against this issue and should not affect usability of websites.'

MSRC
Microsoft Releases Security Advisory 2757760
9 days ago by

Today we released [Security Advisory 2757760](#) to address an issue that affects Internet Explorer 9 and earlier versions if a user views a website hosting malicious code. Internet Explorer 10 is not affected.

We have received reports of only a small number of targeted attacks and are working to develop a security update to address this issue. In the meantime, customers using Internet Explorer are protected when they deploy the following workarounds and mitigations included in the advisory:

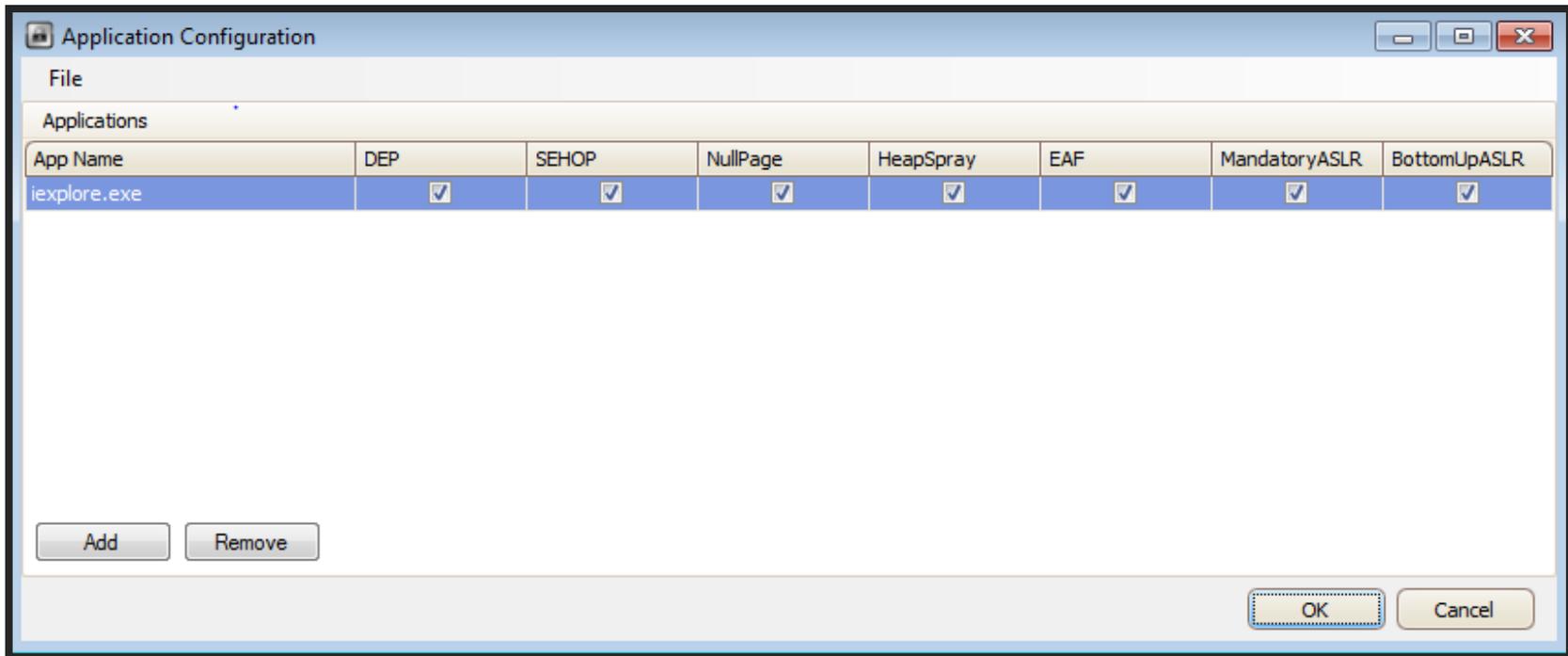
- **Deploy the Enhanced Mitigation Experience Toolkit (EMET)**
This will help prevent exploitation by providing mitigations to help protect against this issue and should not affect usability of websites.

Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
- Mitigated by use of EMET

Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)



Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
- Mitigated by use of EMET
- Audit the Deployment

Policy Dynamics

Edit Control: 100000 - Google Chrome

Qualys, Inc. [US] https://qualysguard.qualys.com/fo/controls/edit_control.php?id=100000&refresh_parent=1

Edit Control

This control type checks for the existence of a user-specified Windows registry key.

General Information

Statement: *

Category: *

Sub-Category: *

Comments:

Ignore Errors

By ignoring errors, the service marks control instances as Passed in cases where an error occurs during control evaluation.

Ignore errors and mark status as Passed

Scan Parameters*

The scan parameters, or data point, indicate what location, file, or setting for the scan to check.

Registry Hive: HKEY_LOCAL_MACHINE (HKLM)

Registry Key: SOFTWARE\Microsoft\EMET\iexplore.exe

Data Type: Boolean

ilities

Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities
CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
- Mitigated by use of EMET
- Audit the Deployment
 - User Defined Registry Check

Summary

- Functionality to assess Controls exist
- Automation available, but frequently API integrations is needed
- Offerings are improving with better workflow coming

Thank You

Andrew Wild – awild@qualys.com

Wolfgang Kandek – wkandek@qualys.com

<http://laws.qualys.com>



Security in knowledge