tripwire®

CONFIDENCE: SECURED

Tripwire – Foundational Controls

Our Customers Must…

Deliver IT services: enable the “central nervous system” of the enterprise

Secure data & systems: protect sensitive data & remain compliant

Avoid disruptions: provide security while maintaining availability & uptime

Minimize (overall) cost & complexity: drive operational efficiencies & performance

The “Fog of More” – Tony Sager, SVP, Center for Internet Security

Seeking clarity in a busy, crowded, noisy security landscape

Tools
Frameworks
Standards
Public Relations
Analytics
Compliance
Risk Management
Guidelines
Standard of Care
Priorities
Incident Response
Products
Information Sharing
Regulations
Trade
Situation Awareness
Cost Sharing
Governance
Notification
Reporting
Best Practices
Liability
Big Data
Vendors
Services
Law Enforcement
Policies
Oversight
Insurance
System Hardening

Tony Sager presentation at RSA Conference: https://www.youtube.com/watch?v=OZLO-xekp3o

Prioritized Cybersecurity

Center for Internet Security's Top 20 Critical Security Controls

Center for Internet Security

20 Critical Security Controls		Severity	Tripwire Solutions
CSC1	Inventory H/W Assets, Criticality, and Location	Very High	●
CSC2	Inventory S/W Assets, Criticality, and Location	Very High	●
CSC3	Secure Configuration Servers	Very High	●
CSC4	Vulnerability Assessment and Remediation	Very High	●
CSC6	Application Security	High	◔
CSC7	Wireless Device Control	High	◔
CSC5	Malware Protection	High/Medium	◔
CSC10	Secure Config-Network	High/Medium	●
CSC11	Limit and Control Network Ports, Protocols, and Services	High/Medium	●
CSC12	Control Admin Privileges	High/Medium	◔

20 Critical Security Controls		Severity	Tripwire Solutions
CSC13	Boundary Defense	High/Medium	◑
CSC14	Maintain, Monitor, and Analyze Audit Logs	Medium	●
CSC15	"Need-to-Know" Access	Medium	◔
CSC16	Account Monitoring and Control	Medium	◔
CSC18	Incident Response	Medium	◔
CSC8	Data Recovery	Medium	
CSC9	Security Skills Assessment	Medium	
CSC17	Data Loss Prevention	Medium/Low	
CSC19	Secure Network Engineering (Secure Coding)	Low	
CSC20	Penetration Testing and Red Team Exercises	Low	

Mapped to most security and compliance frameworks including NIST, CoBIT, PCI, ISO 27000, FISMA

Tripwire supports the CIS Critical Security Controls

CRITICAL SECURITY CONTROL	TRIPWIRE SUPPORT
CSC1: Inventory of authorized and unauthorized devices	●
CSC2: Inventory of authorized and unauthorized software	●
CSC3: Secure configurations for hardware and software	●
CSC4: Continuous vulnerability assessments and remediation	●
CSC5: Controlled use of administrative privileges	◕
CSC6: Maintenance, monitoring, and analysis of audit logs	●

Plus support of Controls 9, 11, 16 and 18.

"The first six controls provide the most effective security against threats, and improved integration between security and IT operations."

—SANS

Tripwire is focused on three aspects of your business

Protecting your organization

» Foundational security controls

» Automated workflows

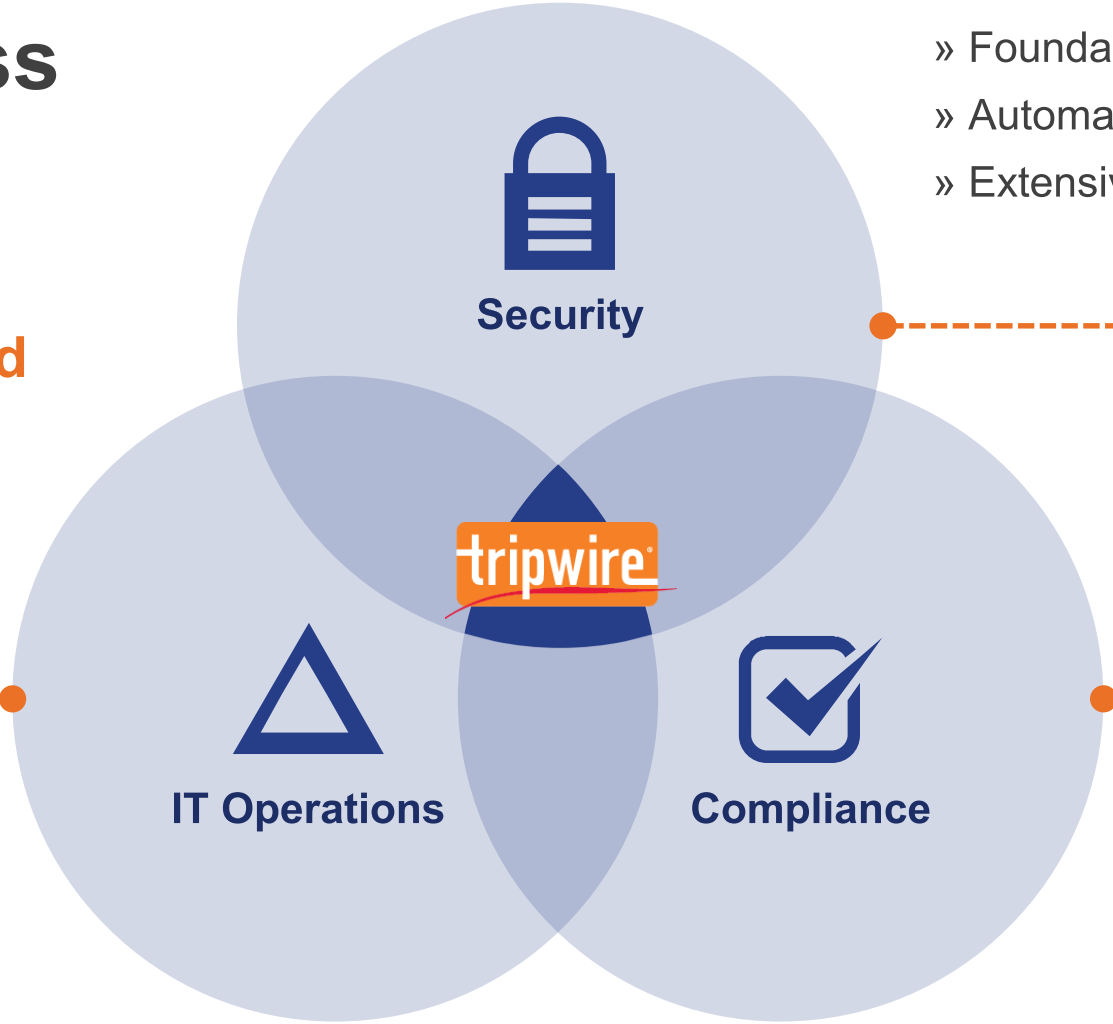
» Extensive integrations

Performing as expected

» Standard configurations

» Change audit and validation

» Improved uptime and MTTR



Proving compliance

» Extensive regulatory coverage

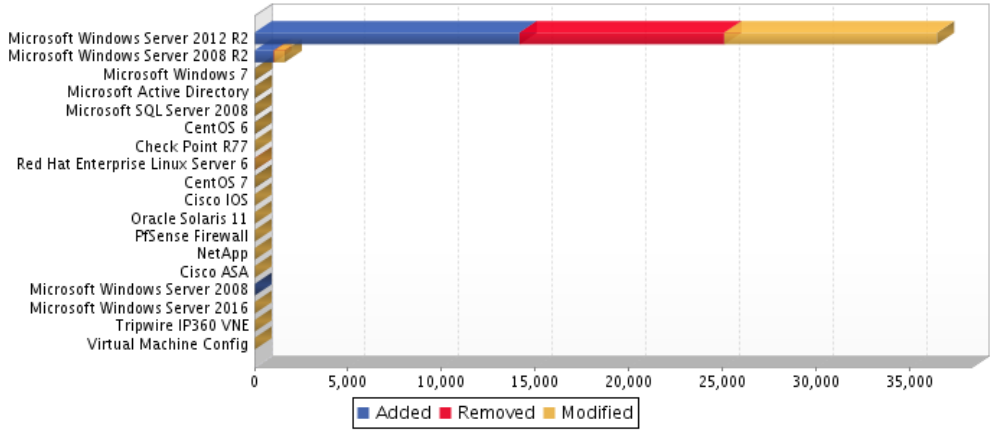
» Continuous monitoring

» Audit evidence and reports

How we enable security

Detect unauthorized changes	Detection and alerts on all changes to established baseline—*what*, *who*, and business context
Assess configurations against security policies	Extensive library of security configuration best-practices to establish and monitor configurations
Identify risks on assets	Discover assets, vulnerabilities and malicious changes, and help automate the workflow and process of remediation
Deal with security data overload	Automate manual processes associated with dealing with change—isolate and escalate changes and events of interest

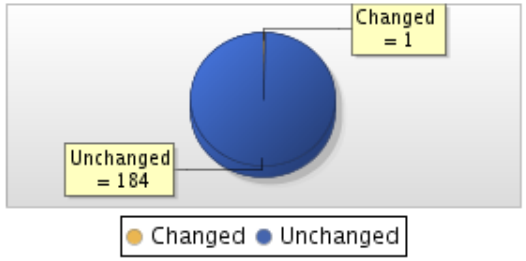
Thousands of changes



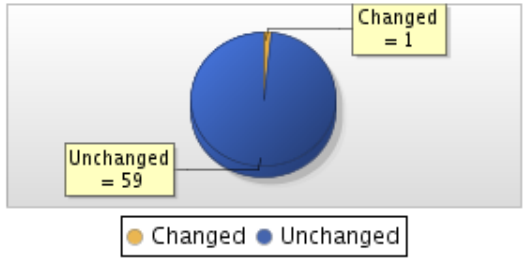
Type	Added	Removed	Modified	Total
Smart Node Group	14,153	10,937	11,355	36,445
Smart Node Group	1,034	14	571	1,619
Smart Node Group	23	0	3	26
Smart Node Group	4	0	11	15
Smart Node Group	4	0	6	10
Smart Node Group	6	0	2	8
Smart Node Group	0	0	8	8
Smart Node Group	0	2	3	5
Smart Node Group	2	0	1	3

Security Dashboard

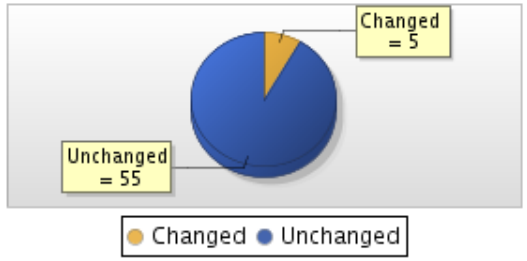
DNS Servers



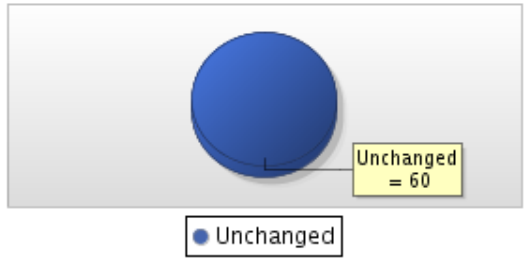
Installed Software



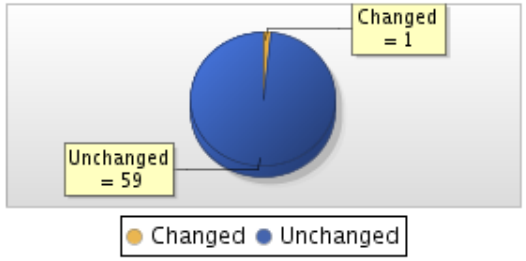
New Executables



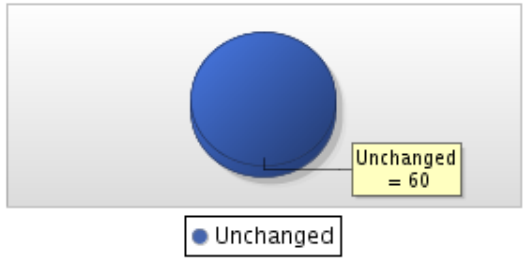
Network Shares



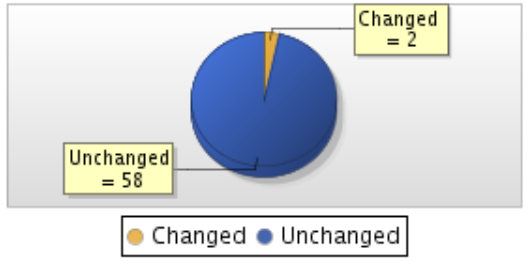
Scheduled Tasks



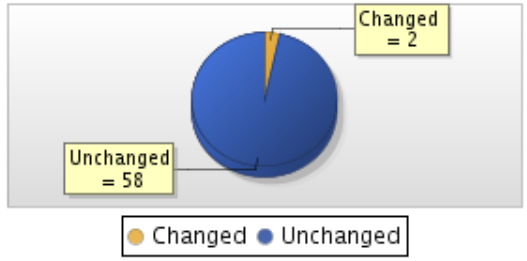
Start Up Tasks



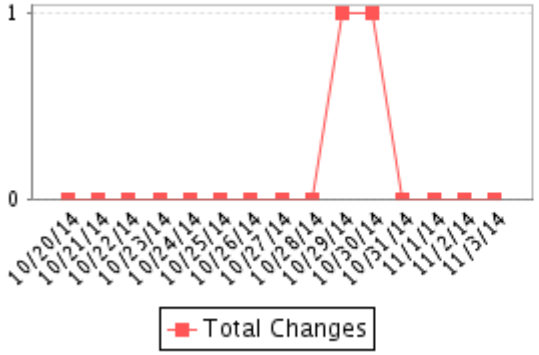
Local Groups



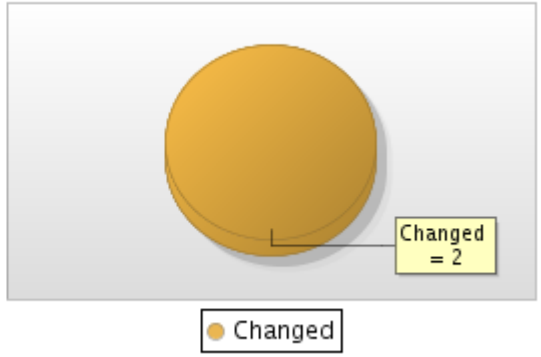
Local Users



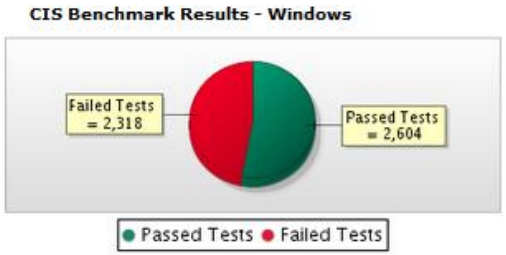
Malware Incidence Over Time

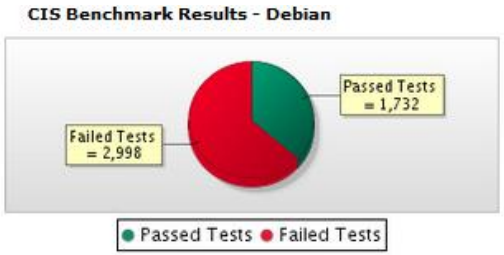


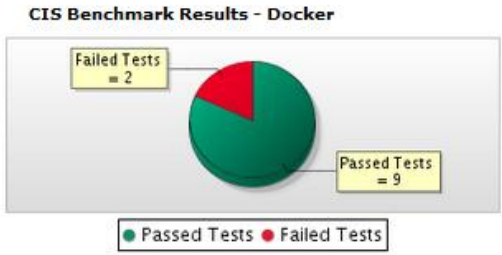
Infected Assets with Changes

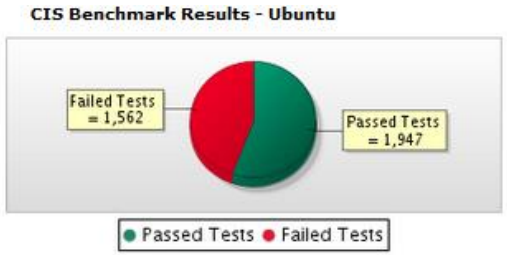


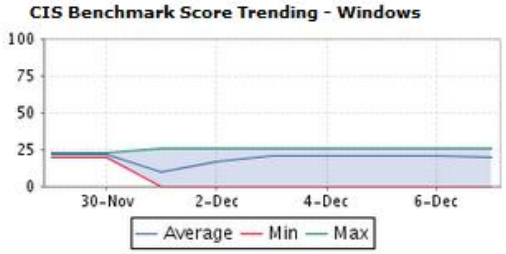
NIST/CIS

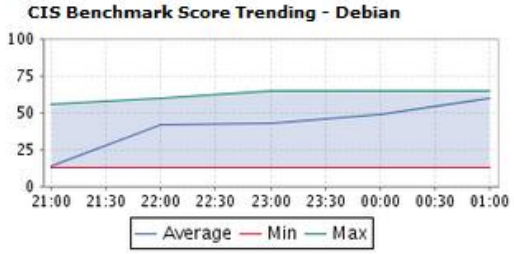

CIS Benchmark Results - Windows
Failed Tests = 2,318
Passed Tests = 2,604
Passed Tests
Failed Tests

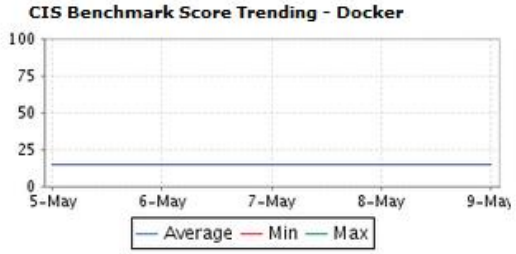

CIS Benchmark Results - Debian
Passed Tests = 1,732
Failed Tests = 2,998
Passed Tests
Failed Tests

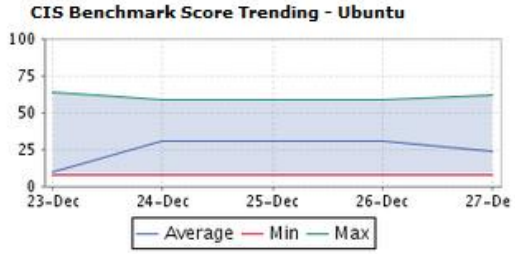

CIS Benchmark Results - Docker
Failed Tests = 2
Passed Tests = 9
Passed Tests
Failed Tests

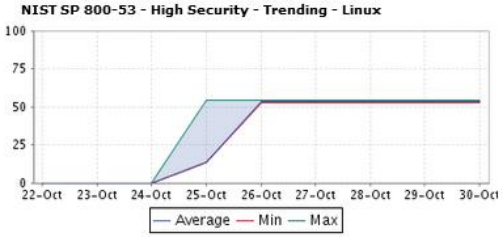

CIS Benchmark Results - Ubuntu
Failed Tests = 1,562
Passed Tests = 1,947
Passed Tests
Failed Tests

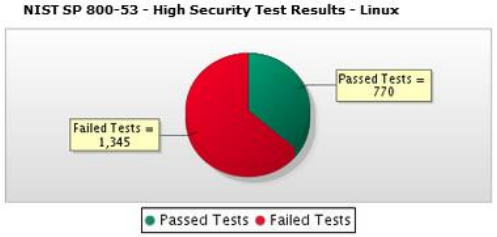

CIS Benchmark Score Trending - Windows
100
75
50
25
0
30-Nov
2-Dec
4-Dec
6-Dec
Average
Min
Max

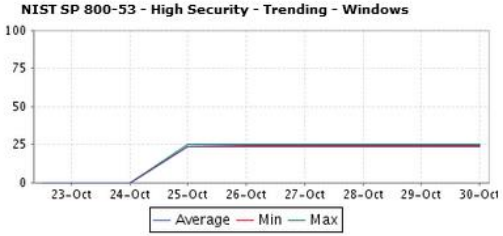

CIS Benchmark Score Trending - Debian
100
75
50
25
0
21:00
21:30
22:00
22:30
23:00
23:30
00:00
00:30
01:00
Average
Min
Max

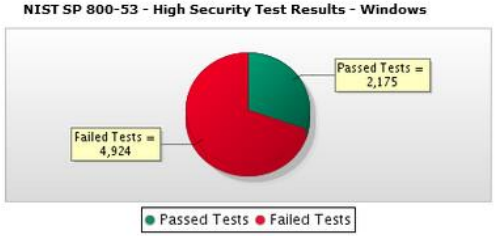

CIS Benchmark Score Trending - Docker
100
75
50
25
0
5-May
6-May
7-May
8-May
9-May
Average
Min
Max


CIS Benchmark Score Trending - Ubuntu
100
75
50
25
0
23-Dec
24-Dec
25-Dec
26-Dec
27-De
Average
Min
Max


NIST SP 800-53 - High Security - Trending - Linux
100
75
50
25
0
22-Oct
23-Oct
24-Oct
25-Oct
26-Oct
27-Oct
28-Oct
29-Oct
30-Oct
Average
Min
Max


NIST SP 800-53 - High Security Test Results - Linux
Passed Tests = 770
Failed Tests = 1,345
Passed Tests
Failed Tests


NIST SP 800-53 - High Security - Trending - Windows
100
75
50
25
0
23-Oct
24-Oct
25-Oct
26-Oct
27-Oct
28-Oct
29-Oct
30-Oct
Average
Min
Max


NIST SP 800-53 - High Security Test Results - Windows
Passed Tests = 2,175
Failed Tests = 4,924
Passed Tests
Failed Tests

Remediation

AC- 2.1 Built-in Guest Account Renamed

Built-in Guest Account Renamed

This test verifies that the 'Accounts: Rename guest account' feature is defined. This setting promotes confidentiality and system integrity by making it somewhat more difficult for a logon vector attack to succeed (this type of attack is easier

Remediation

To remediate failure of this policy test, configure the security options to ensure that the built in Guest account has been renamed.

Modifying the security options policy :

1. Select a group policy object to edit within the **Microsoft Management Console**.
2. Select **Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options**.
3. Right-click **Accounts: Rename guest account** and select **Properties** .
4. In the **Properties** window, select **Define this policy setting** and in the text box, rename the **Guest** account then click **OK** .
5. Run the **gpupdate** command to apply the change.

Note :

- To perform this procedure you must be a domain administrator.
- Tests may continue to fail until the domain refreshes the setting configured above.
- When you change a security setting and click **OK** , that setting will take effect in the next refresh of settings, or after reboot.
- The security settings are refreshed every **90 minutes on a workstation or server** and every **5 minutes on a domain controller** . the settings are also refreshed every 16 hours, whether or not there are any changes.

For further details, please refer to:

http://technet.microsoft.com/en-us/library/cc264462.aspx

Node: Degobah.galaxy.ffa (Windows Server)

Overall result: Failed @ 11/16/16 9:43 AM

Element: Computer

Result

Failed

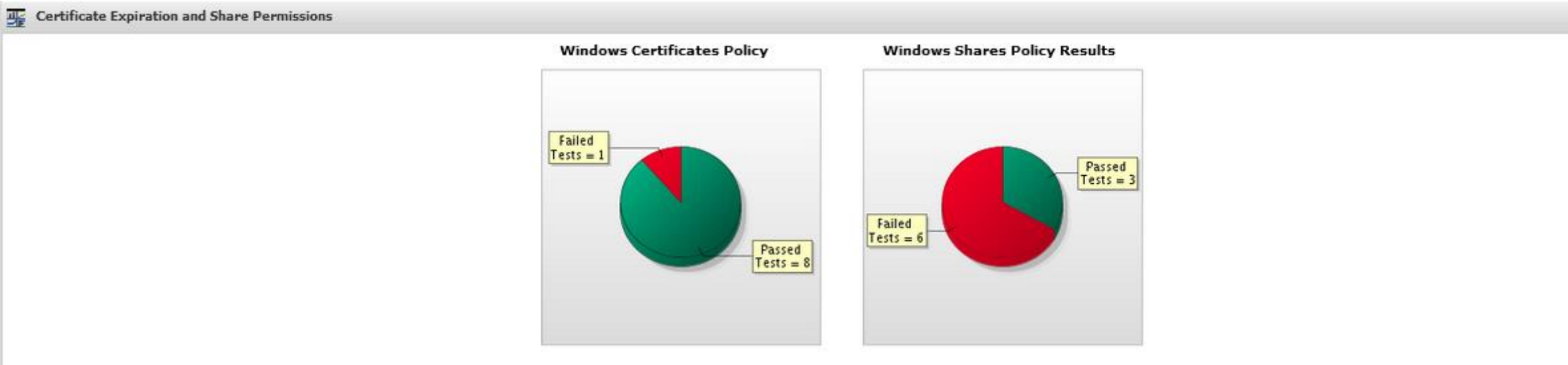
Time

11/16/16 9:43 AM

Actual

NewGuestName="Guest"

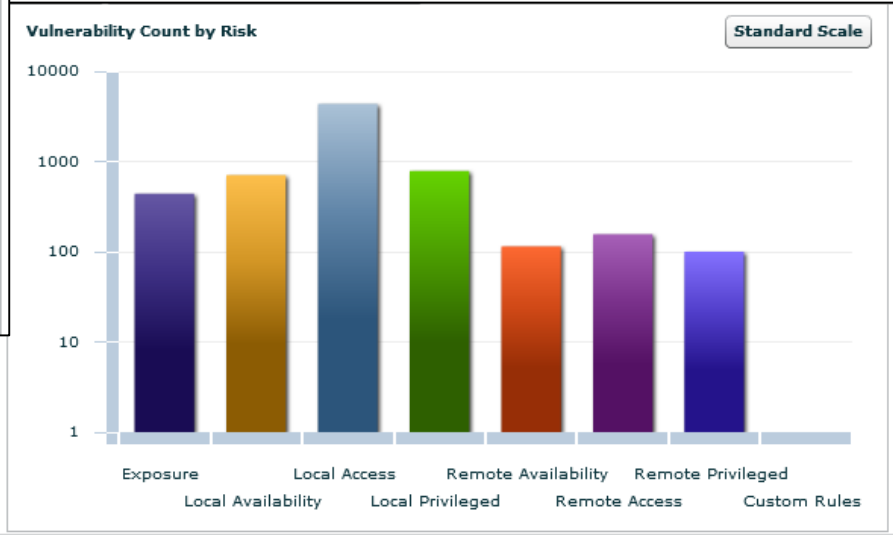
Custom Policies



Vulnerability Heat Map

Risk Matrix

	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged
Automated Exploit		15	174	101	7	16	24
Easy		31	286	72	4	9	8
Moderate		4	8	6		6	1
Difficult		7	48	8	3	11	
Extremely Difficult		229	402	143	27	27	16
No Known Exploit	441	422	3432	455	73	87	51



IP	DNS Name	NetBIOS Domain	NetBIOS Name	Operating System	Host Score	CVSS Base Score	IP360 Asset Value	Has Exceptions?
10.64.0.64	bt2008.scn2.lab.tripwire.com			Windows Server 2008 x64	936622	10.0	0	Yes
192.168.97.136	DNS Timed out	WORKGROUP	ETL	Windows Server 2008 R2	126700	10.0	0	Yes
10.64.0.45	Name not in DNS	WORKGROUP	STNDNSWIN2K8R2B	Windows Server 2008 R2	87398	10.0	0	
10.64.0.30	vista.scn2.lab.tripwire.com	WORKGROUP	VISTA	Windows Vista x86 SP2	78298	10.0	0	
10.64.0.155	exchangeedge.scn2.lab.tripwire.com	EXCHANGEEDGE1	EXCHANGEEDGE	Windows 2003 x64 SP2	76736	10.0	0	

Heat Map Drill Down

Vulnerability Listing For Remote Privileged/Automated Exploit

Display Mode: Show Excepted Findings

ID	Name	Affected Host	Risk	Score	CVSS Base	CVE	Remediation
11121	MS08-021: Microsoft Windows GDI Stack Overfl	1	Remote Privileged	41033	9.3	CVE-2008-1087, CVE-2008-1087	
11234	MS08-052: Microsoft GDI+ WMF Image File Buf	1	Remote Privileged	40049	9.3	CVE-2008-3014, CVE-2008-3014	
11889	MS08-067: Microsoft Windows Server Service RI	1	Remote Privileged	39763	10.0	CVE-2008-4250, CVE-2008-4250, CVE-2008-4250, CVE-2008-4250	
14764	MS09-006: Microsoft Windows Kernel GDI EMF/\	1	Remote Privileged	38853	9.3	CVE-2009-0081, CVE-2009-0081	
21372	MS09-013: Microsoft WinHTTP Integer Underflo	1	Remote Privileged	38619	10.0	CVE-2009-0086, CVE-2009-0086	
21376	MS09-014: Microsoft Windows NTLM Credential	1	Remote Privileged	38619	9.3	CVE-2009-0550, CVE-2009-0550	
21374	MS09-013: Microsoft Windows NTLM Credential	1	Remote Privileged	38619	9.3	CVE-2009-0550, CVE-2009-0550	

Vulnerability CVE/Remediation

ID: 11121 **Name:** MS08-021: Microsoft Windows GDI Stack Overflow Vulnerability

CVE Links:

CVE-2008-1087 CVE-2008-1087

Description:

Stack-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF image file with crafted filename parameters, aka "GDI Stack Overflow Vulnerability."

Remediation:

The vendor has released patches for this vulnerability:

Microsoft Windows 2000 Service Pack 4
http://www.microsoft.com/downloads/details.aspx?familyid=caac000a-22b6-48cb-aa00-1a0bfe886de2

Windows XP Service Pack 2
http://www.microsoft.com/downloads/details.aspx?familyid=c2763dd8-a03e-4a48-aa86-a7ec00250a7a

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
http://www.microsoft.com/downloads/details.aspx?familyid=166f2ab5-913c-47a9-86fe-b814797b751e

Close

Search for any event of interest

Event Time	Event Name	ip	Process
10/25 10:38:14	Login: pam_unix(login:session): session opened for user okenobi by LOGIN(uid=0)	192.168.97.153	login
10/26 08:07:22	Login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost=	192.168.97.151	login
10/26 08:07:35	Login: LOGIN ON tty1 BY mwindu	192.168.97.151	login
10/27 16:11:44	Login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)	192.168.97.151	login
10/23 12:52:48	Login: login on ttyv0 as root	192.168.97.1	login
10/24 10:17:36	<32>Oct 24 10:17:36 php: /index.php: Successful login for user 'admin' from: 172.31.34.40	192.168.97.1	
10/25 10:37:17	Login: FAILED LOGIN 1 FROM (null) FOR mwindu, Authentication failure	192.168.97.153	login
10/25 10:38:06	Login: pam_unix(login:session): session closed for user root	192.168.97.153	login
10/26 08:07:17	Login: pam_unix(login:session): session closed for user root	192.168.97.151	login
10/26 08:07:22	Login: pam_unix(login:auth): check pass; user unknown	192.168.97.151	login
10/26 08:07:35	Login: pam_unix(login:session): session opened for user mwindu by LOGIN(uid=0)	192.168.97.151	login
10/27 16:11:45	Login: ROOT LOGIN ON tty1	192.168.97.151	login
10/27 22:19:12	Login failed for user 'sa'	192.168.97.101	MSSQLS
10/27 22:19:12	Login failed for user 'ncircle'	192.168.97.101	MSSQLS
10/27 22:19:12	Login failed for user 'ncircle'	192.168.97.101	MSSQLS
10/27 22:19:13	The login packet used to open the connection is structurally invalid; the connection has been closed	192.168.97.101	MSSQLS
10/27 22:21:51	Login failed for user 'sa'	192.168.97.101	MSSQLS
10/27 22:21:51	Login failed for user 'sa'	192.168.97.101	MSSQLS
10/27 22:21:51	The login packet used to open the connection is structurally invalid; the connection has been closed	192.168.97.101	MSSQLS
10/27 22:21:52	Login failed for user 'sa'	192.168.97.101	MSSQLS
10/28 08:52:46	SQL Trace ID 2 was started by login "sa"	192.168.97.101	MSSQLS
10/28 08:52:46	SQL Trace ID 1 was started by login "sa"	192.168.97.101	MSSQLS
10/28 15:45:08	SQL Trace ID 1 was started by login "sa"	192.168.97.101	MSSQLS
10/28 15:45:08	SQL Trace ID 2 was started by login "sa"	192.168.97.101	MSSQLS
10/28 15:51:55	Login failed for user 'Administrator'	192.168.97.101	MSSQLS
10/28 15:52:06	Login failed for user 'Administrator'	192.168.97.101	MSSQLS

NIST out of the box reports

- SP 800-53 Rev 4
  - Access Control
    - AC-02
      - Account Management Events by User - Detailed
      - Accounts and Groups Modified by Host - Detailed
      - Accounts Disabled by User - Detailed
      - Accounts Removed or Disabled by User - Detailed
      - Administrator Account Logins by Host - Detailed
      - Database Authentication Activity by Host - Detailed
      - Generic Account Logon Activity by User - Detailed
      - Generic Account Password Change Activity by User - Detailed
      - Privilege Elevation Events by Host - Detailed
      - Privileged Function Events by Host - Detailed
      - Successful After Hours Logon Events by User - Detailed
    - AC-03
    - AC-04
    - AC-05
    - AC-06
    - AC-07
    - AC-10
    - AC-12
    - AC-17
    - AC-20
    - AC-23
  - Audit and Accountability
  - Configuration Management
    - CM-02
      - FIM Baseline Events - Detailed
    - CM-03
      - Configuration and Policy Changes - Detailed
      - FIM Baseline Overwriting Events - Detailed
    - CM-04
    - CM-05

Query name	Account Management Events by User - Detailed
Description	Accounts Created, Deleted or Modified Listed by User
Queried Audit Logger	Audit Logger — Query group
Output	Report — Report Class: Report

Query Filter

Classification Tags	Account|AdminAccount Create|Expire|Lock|Unlock|Re
Terms	
Assets	IP Address
Events Per Query	1000
Date and Time	Newer/Older/Previous
Time Span	Newer than — 1

Processed Filter | Columns | Report Options | Advanced Options

Type	Condition	Value

Start | Save | Clear Form

Vulnerabilities in Logging

Status Overview

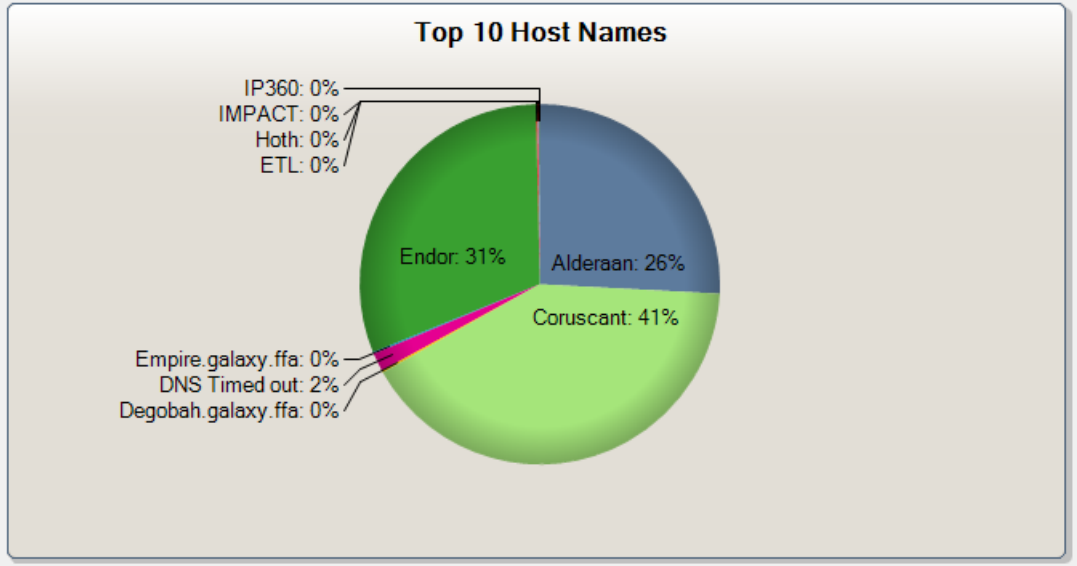
Overall Status

Total Events	382894	Filtered Events	382894
Unique Rules	19	Filtered unique Rules	19
Events last refreshed	05/09 17:26:43	Last Event time	05/09 17:20:37

Top 10 Priorities

Priority	Count
High	2254
Med	2800
Info	334008
Low	43832

Top 10 Vulnerable Hosts



Top 10 Event Sensors

Sensor	Count
TLC.galaxy.ffa	228
Degobah.galaxy.ffa	74174
Empire.galaxy.ffa	259059
Tatooine.galaxy.ffa	642
Coruscant	2243
Naboo	2218
Endor	764
192.168.97.52	43538
kamino.galaxy.ffa	28

Top 10 Src IP Add...

IP Address	Count
127.0.0.1	44029
172.16.97.1	2
172.31.34.5	1
172.31.34.4	2
172.31.34.5	1
172.31.34.1	6
192.168.97.	148108
192.168.97.	2817
192.168.97.	595
192.168.97.	2

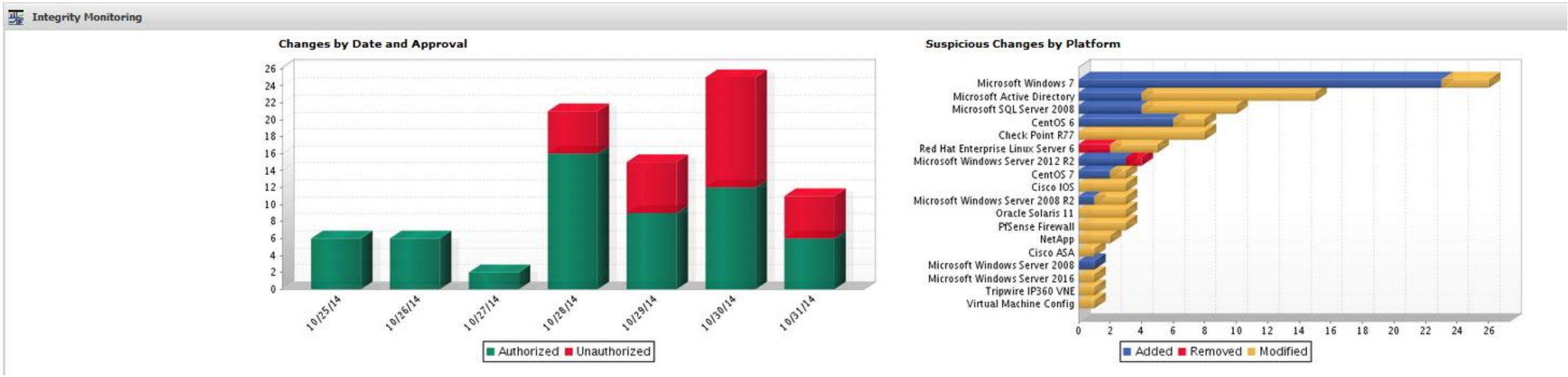
Top 10 Dst IP Addr...

IP Address	Count
10.0.3.48	468
10.248.224.	95
127.0.0.1	3629
172.31.42.1	9
172.31.42.1	32115
192.168.97.	236
192.168.97.	7122
192.168.97.	259103
192.168.97.	74174
192.168.97.	642

How we improve IT operations

Ensure system availability and speed up investigation	Integrity monitoring and change audit to find root cause
Control changes that compromise systems	Real-time change detection— *what*, *who*, *when* and *what it means*
Validate changes and reduce unplanned work	Integration with ITSM to tell authorized from unauthorized changes
Know what's happening in your environment	Discovery, inventory, change and log data for all your critical assets

Authorized/Unauthorized Changes



Changes to specific applications or environments

Lock down permissions

Windows File Share Analysis

Close Empty File Shares

Node	Passed Tests	Failed Tests	Percent Compliant
Degobah.galaxy.ffa	1	0	100%
ETL.galaxy.ffa	0	0	0%
Empire.galaxy.ffa	0	1	0%
Tattoine.galaxy.ffa	1	0	

Close Inactive File Shares (Updates)

Node	Passed Tests	Failed Tests
Degobah.galaxy.ffa	0	1
ETL.galaxy.ffa	0	0
Empire.galaxy.ffa	0	1
Tattoine.galaxy.ffa	0	1

Restrict Access to File Shares

Node	Passed Tests	Failed Tests
Degobah.galaxy.ffa	0	1
ETL.galaxy.ffa	0	0
Empire.galaxy.ffa	0	1
Tattoine.galaxy.ffa	1	0

Close Empty File Shares

This test will fail if an empty file share is detected.

Remediation

Empty, unused file shares present a needless security risk and should be closed.

Closing a file share

The following command will close a local file share:

net share <sharename> /delete

Reference for "net share": http://technet.microsoft.com/en-us/library/bb490712.aspx

Node: Empire.galaxy.ffa (Windows Server)

Overall result: Failed @ 12/24/14 8:09 AM

Element: Local File Shares

Result

Failed

Time

12/24/14 8:09 AM

Actual

Files Present=N
Share=NETLOGON
Description=Logon server share
Path=C:\Windows\SYSVOL\sysvol\Kessel\SCRIPTS

Hardware/Software discovery

IP	DNS Name	NetBIOS Domain	NetBIOS Name	Operating System	Host Score	CVSS Base	Last Scan	Has Exceptions?
10.64.0.64	bt2008.scn2.lab.tripwire.com			Windows Server 2008 x64 SP1	936622	10.0	02/27/2017	Yes
192.168.97.136	DNS Timed out	WORKGROUP	ETL	Windows Server 2008 R2 SP1	126700	10.0	02/21/2017	Yes
10.64.0.45	Name not in DNS	WORKGROUP	STNDNSWIN2K8R2E	Windows Server 2008 R2 SP1	87398	10.0	02/27/2017	
10.64.0.30	vista.scn2.lab.tripwire.com	WORKGROUP	VISTA	Windows Vista x86 SP2	78298	10.0	02/27/2017	
10.64.0.155	exchangeedge.scn2.lab.tripwire.com	EXCHANGEEDGE1	EXCHANGEEDGE	Windows 2003 x64 SP2	76736	10.0	02/27/2017	
10.64.0.105	ubuntu-server10-4.scn2.lab.tripwir...			Ubuntu Linux 10.04	76551	10.0	02/27/2017	
10.64.0.156	ex2k7hubserver.scn2.lab.tripwire.c...	CCMAD	EX2K7HUBSERVER	Windows 2003 x64 SP2	74576	10.0	02/27/2017	
10.64.0.59	win2003mysql5-1.scn2.lab.tripwire...	WORKGROUP	WIN2003MYSQL5-1	Windows 2003 x64 SP2	72776	10.0	02/27/2017	
10.64.0.146	ole6u5-x64-btrfs.scn2.lab.tripwire....			Oracle Enterprise Linux 6.4	38425	10.0	02/27/2017	

Application Listing — **Display Mode:** Show Excepted Findings

ID	Name	Hosts Running	Protocol/Port
8839	Active Directory Application Mode (ADAM)	1	null/0
21118	Adobe AIR 17.0.0.172	1	null/0
13710	Adobe Flash Player 11.3.300.257	1	null/0
24605	Adobe Flash Player 18.0.0.343	1	null/0
9465	Adobe Flash Player for Firefox/Opera	1	null/0
12949	AIX 6.1 TL7 (6100-07) (via SSH)	1	tcp/22
1235	AIX FTP	1	tcp/21
1392	AIX Telnet	1	tcp/23
5925	Apache 2.1.9 - 2.2.0 (via SSH)	1	tcp/22
14967	Apache 2.1.x and 2.2.x HTTP	1	tcp/80
5926	Apache 2.2.0 (via SSH)	3	tcp/22
7749	BIND 8.3.3 (via SSH)	1	tcp/22
1868	Bind 9 tcp DNS	1	tcp/53
10730	BIND 9.7 UDP	1	udp/53
7702	BIND 9.x (via SSH)	1	tcp/22
10489	CACE WinPcap	3	null/0
10518	CACE WinPcap 4.1.2	1	null/0

Web Browsers within the environment

Application Listing **Display Mode:** Show Excepted Findings

ID	Name	Hosts Running	Protocol/Port
1809	Mozilla Application	6	null/0
9339	Microsoft Internet Explorer 8.0 (8.0.6001.18702)	3	null/0
18103	Microsoft Internet Explorer 11	3	null/0
19502	Mozilla Firefox 31.0	2	null/0
9338	Microsoft Internet Explorer 8	2	null/0
9713	Microsoft Silverlight 3.0.40818.0	2	null/0
11150	Microsoft Internet Explorer 9.0 (9.0.8112.16421)	1	null/0
2962	Mozilla Firefox	1	null/0
9273	Microsoft Internet Explorer 7.0 (7.0.6001.18000)	1	null/0
26270	Microsoft Silverlight 5.1.50901.0	1	null/0

VM Remediation

Vulnerability CVE/Remediation

ID: 11121 **Name:** MS08-021: Microsoft Windows GDI Stack Overflow Vulnerability

CVE Links:

CVE-2008-1087 CVE-2008-1087

Description:

Stack-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF image file with crafted filename parameters, aka "GDI Stack Overflow Vulnerability."

Remediation:

The vendor has released patches for this vulnerability:

Microsoft Windows 2000 Service Pack 4
http://www.microsoft.com/downloads/details.aspx?familyid=caac000a-22b6-48cb-aa00-1a0bfe886de2

Windows XP Service Pack 2
http://www.microsoft.com/downloads/details.aspx?familyid=c2763dd8-a03e-4a48-aa86-a7ec00250a7a

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
http://www.microsoft.com/downloads/details.aspx?familyid=166f2ab5-913c-47a9-86fe-b814797b751e

Close

Searching for stopped services

Query Filter

Classification Tags

Query Tips

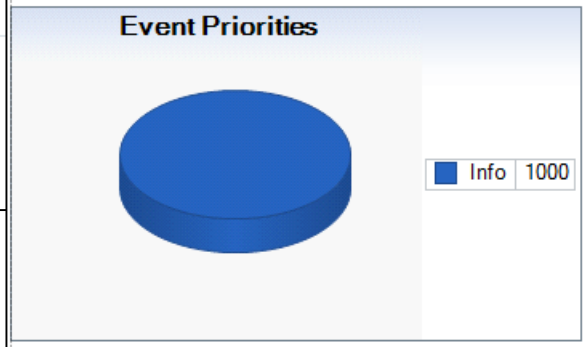
Terms: service sto

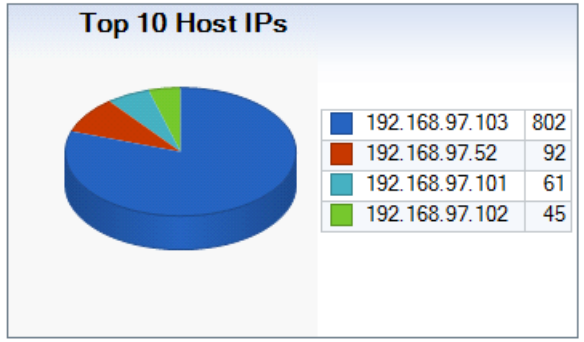
Assets: IP Address

Events Per Query: 1000

Date and Time: All

- stopped (20,351)
- storage (136,421)
- store (2,043,421)
- storedriverdelivery (17,376)
- storedriversubmission (443,518)
- storeec (51)
- storemaintenanceassistant:internalmaintenance (2,062)





Events by Host Report

Timestamp	Process	Priority	Class	User Name
Host IP:	**192.168.97.101**			
10/28/2014 2:17:00 AM	Service Control Manager	Info	Process Audit	*
The WinHTTP Web Proxy Auto-Discovery Service service entered the stop state				
10/28/2014 3:17:26 AM	Service Control Manager	Info	Process Audit	*
The Windows Modules Installer service entered the stop state				

Root/Admin activity

Host : **192.168.97.153**

10/10/2014 6:20:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 6:30:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 6:40:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 6:50:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:00:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:01:01 PM	root	Cron command: (run-parts /etc/cron.hourly)
10/10/2014 7:10:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:20:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:30:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:40:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 7:50:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:00:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:01:01 PM	root	Cron command: (run-parts /etc/cron.hourly)
10/10/2014 8:10:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:20:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:30:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:40:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:50:01 PM	root	Cron command: (/usr/lib64/sa/sa1 -S DISK 1 1)
10/10/2014 8:53:33 PM	root	Successful Logon: root
10/10/2014 8:53:33 PM	root	Successful Logon: root

How we support compliance

Demonstrate compliance with standards	Industry's most comprehensive library of policy tests for all major standards
Reduce the time spent on compliance	Out-of-the-box audit report templates, and automated compliance reporting
Produce data for audits and for forensics	Logging of changes to in-scope assets with details on *who* and *when*
Maintain compliance over time	Continuous monitoring and reporting identifies remediation to stay compliant

FIM required by compliance

Node: Degobah.galaxy.ffa (Windows Server)

Date	Element	Change Type	Attributes	Users
10/30/14 12:40 PM	Listening Ports	Modified	MD5	
10/30/14 12:39 PM	Local Firewall Rules	Modified	MD5	
10/30/14 12:33 PM	C:\How to get a huge raise.pdf.exe	Added		DEGOBAH\Luke

Node: Empire.galaxy.ffa (Active Directory Server)

Date	Element	Change Type	Attributes	Users
10/29/14 10:22 AM	CN=Administrators,CN=Builtin,DC=Kessel	Modified	member	KESSEL\Vader
10/29/14 10:21 AM	CN=R2-D2,CN=Users,DC=Kessel	Added		KESSEL\Vader

eport Viewer - Mozilla Firefox

https://192.168.97.149/console/app.showEditor.cmd?editorName=reportManager.editor.reportViewerDialog&wndName=reportViewer:-1y2p0ij32e7j5:-1y2 90%

ort Viewer Refresh Help

Archive Report | PDF Export | XML Export | CSV Export | Email | Print

ode: Degobah.galaxy.ffa (Windows Server)

Rule: Listening Ports (Command Output Capture Rule)

Element: Listening Ports

Version: 10/30/14 12:40 PM

Node: Degobah.galaxy.ffa
Rule: Listening Ports
Element: Listening Ports
Change Type: Modified
Severity: Highly Vulnerable (903)
Promotion Approval ID:
Comment:
Users:

Attribute	Type	Expected	Observed
MD5	[*]	dc0450a73bfbe3de08145d852a9a2224	3c18bb57572996cdd4f5d6a576eab349

Line	Type	Content
12	[+]	TCP 0.0.0.0:1337 0.0.0.0:0 LISTENING

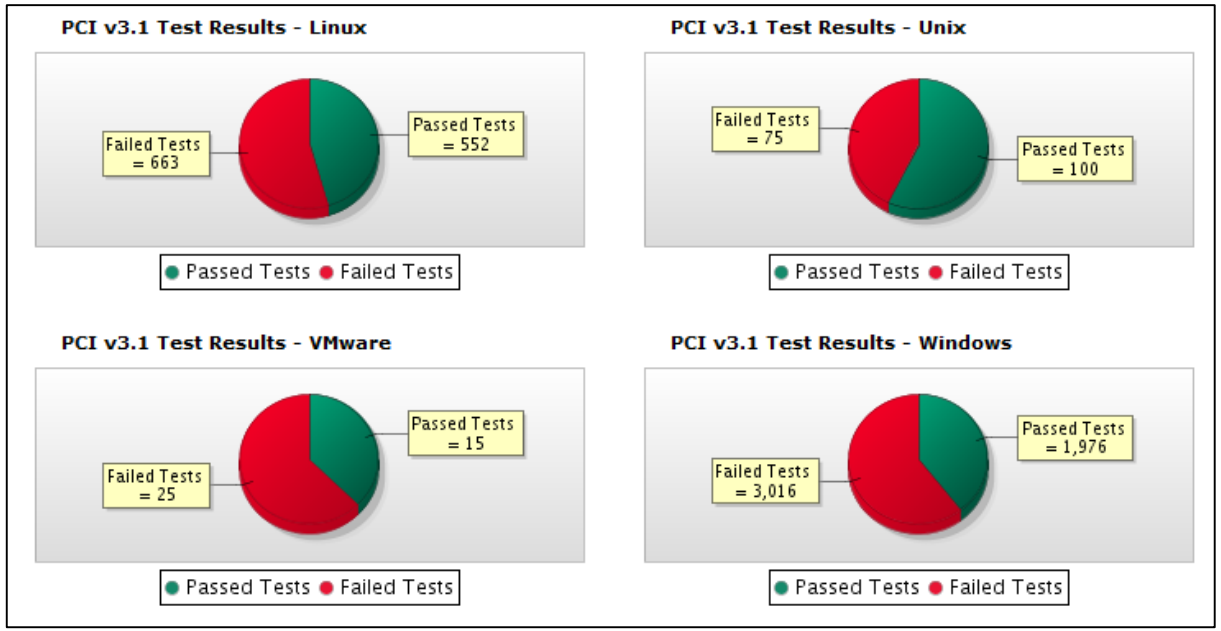
Change Type	Attributes	Users
Added		KESSEL\Vader

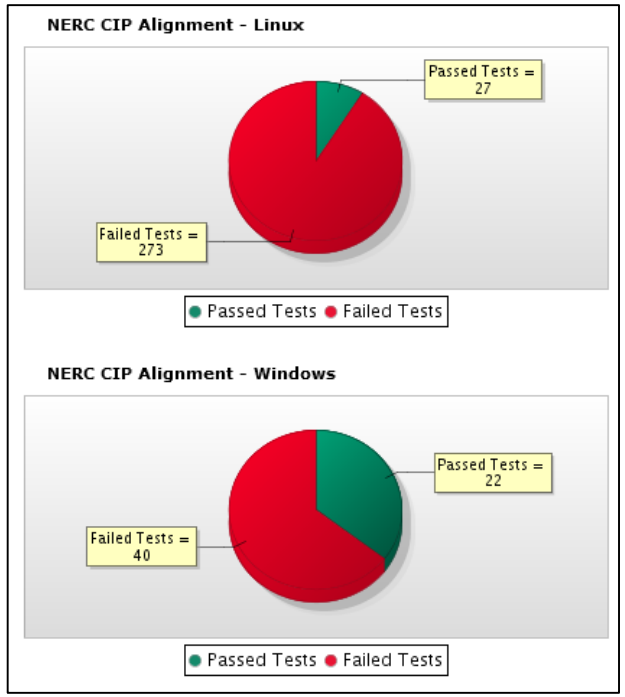
Change Type	Attributes	Users
Modified	SHA-1	
Added		KESSEL\R2-D2
Added		KESSEL\R2-D2

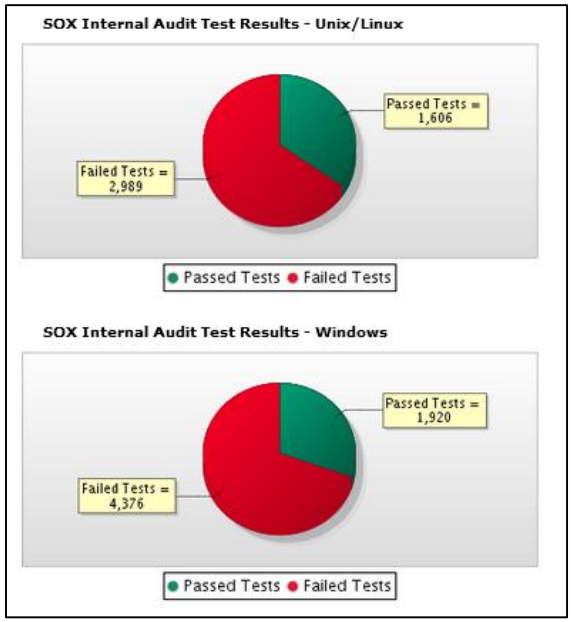
Change Type	Attributes	Users
Modified	MD5	

Change Type	Attributes	Users
Modified	Modify, SHA-1, Size	leia
Modified	Modify, SHA-1, Size	leia
Modified	Modify, SHA-1, Size	leia

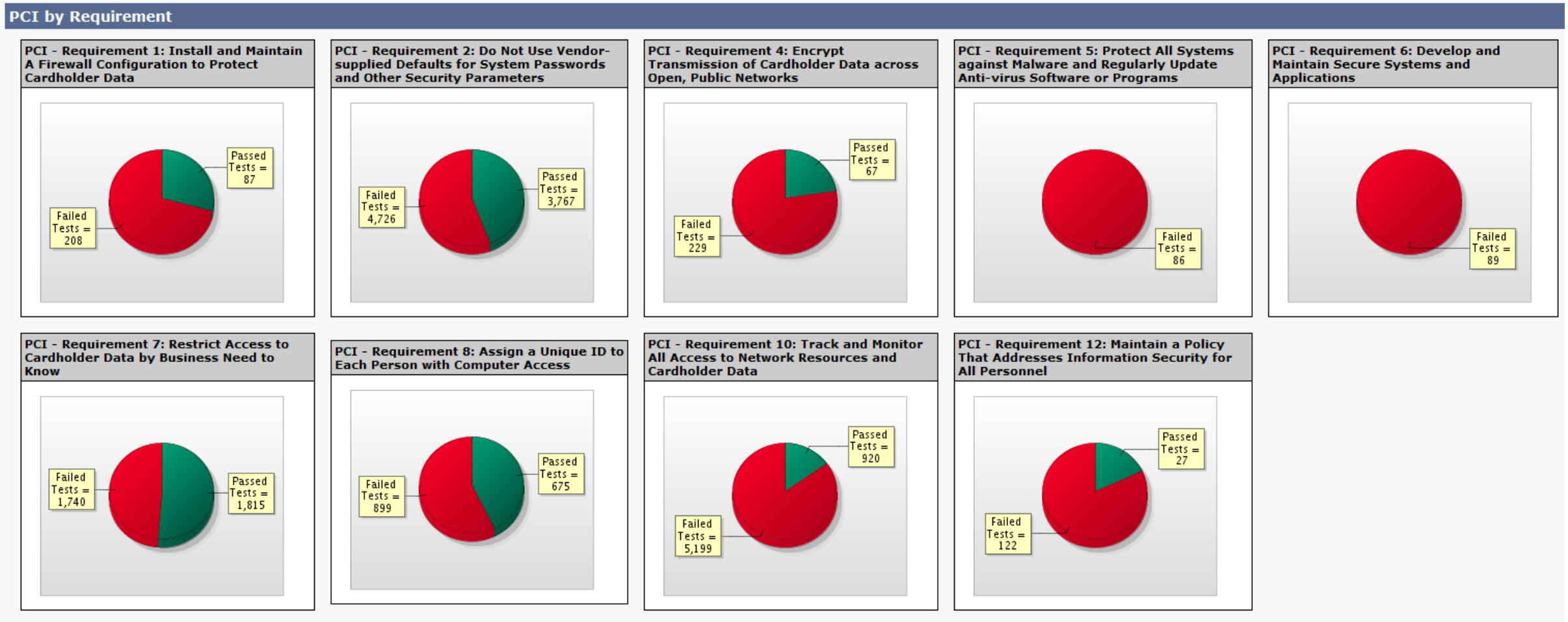
SCM – SOX, PCI, NERC







PCI by requirement



PCI Remediation

12.3.8.3 Machine Inactivity Limit: 900 or Fewer Seconds

Machine Inactivity Limit: 900 or Fewer Seconds

This test verifies that 'Interactive logon: Machine inactivity limit' is set to '900 or fewer seconds'. Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

Remediation

To remediate failure for this policy test, configure the security options to set the inactivity time limit to no more than 900 seconds.

Modifying the security options policy :

1. Select a group policy object to edit within the **Microsoft Management Console**.
2. Select **Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options**.
3. Right-click **Interactive logon: Machine inactivity limit**, select **Properties** .
4. In the **Properties** window, select **Define this policy setting** and in the **Machine will be locked after:** box, enter an integer value that is greater than **0** and less than or equal to **900** , and click **OK** .
5. Run the **gpupdate** command on to apply the change.

Note :

- To perform this procedure you must be a domain administrator.
- Tests may continue to fail until the domain refreshes the setting configured above.
- When you change a security setting and click **OK** , that setting will take effect in the next refresh of settings, or after reboot.
- The security settings are refreshed every **90 minutes on a workstation or server** and every **5 minutes on a domain controller** . The settings are also refreshed every 16 hours, whether or not there are any changes.

For further details, please refer to:

http://technet.microsoft.com/en-us/library/hh831424.aspx

Node: Kamino.galaxy.ffa (Windows Server)

Overall result: Failed @ 11/16/16 9:43 AM

Element: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system|InactivityTimeoutSecs

Result

Failed

Time

11/16/16 9:43 AM

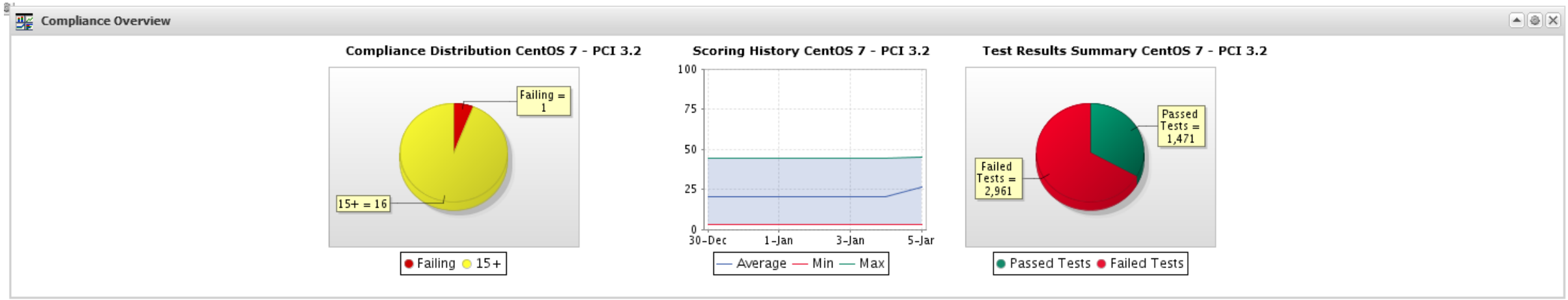
Node: StarDestroyer-13411.galaxy.ffa (Windows Server)

Overall result: Failed @ 12/7/16 1:39 PM

Element: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system|InactivityTimeoutSecs

Result

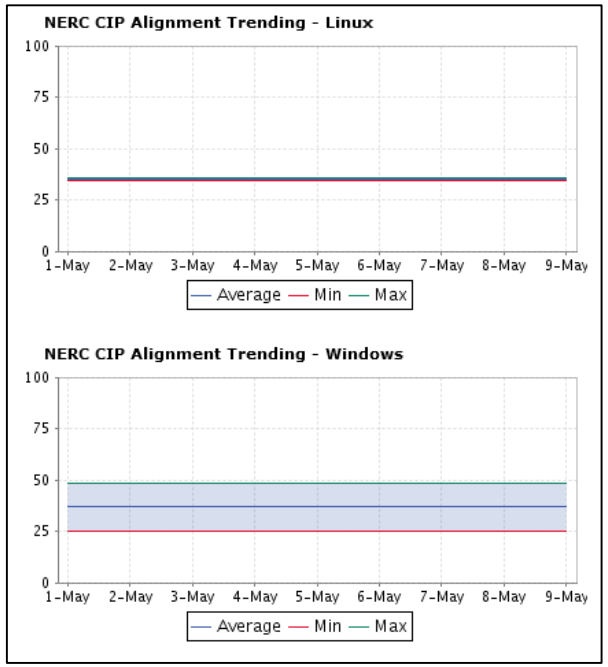
Auditor Dashboard

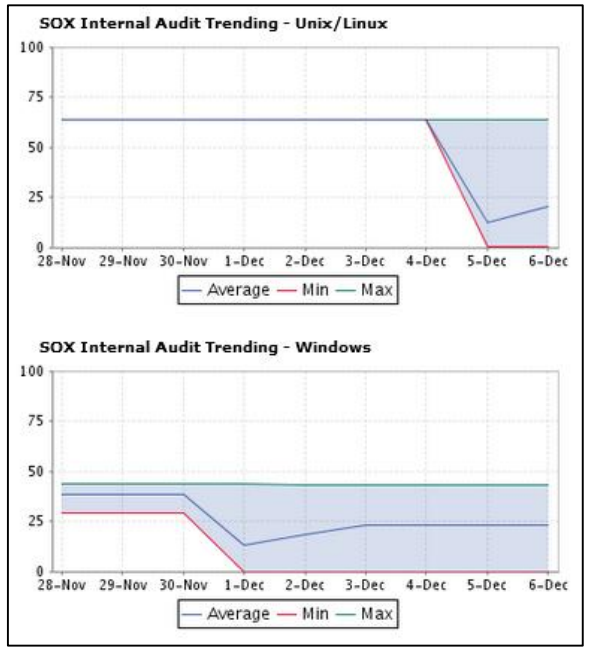


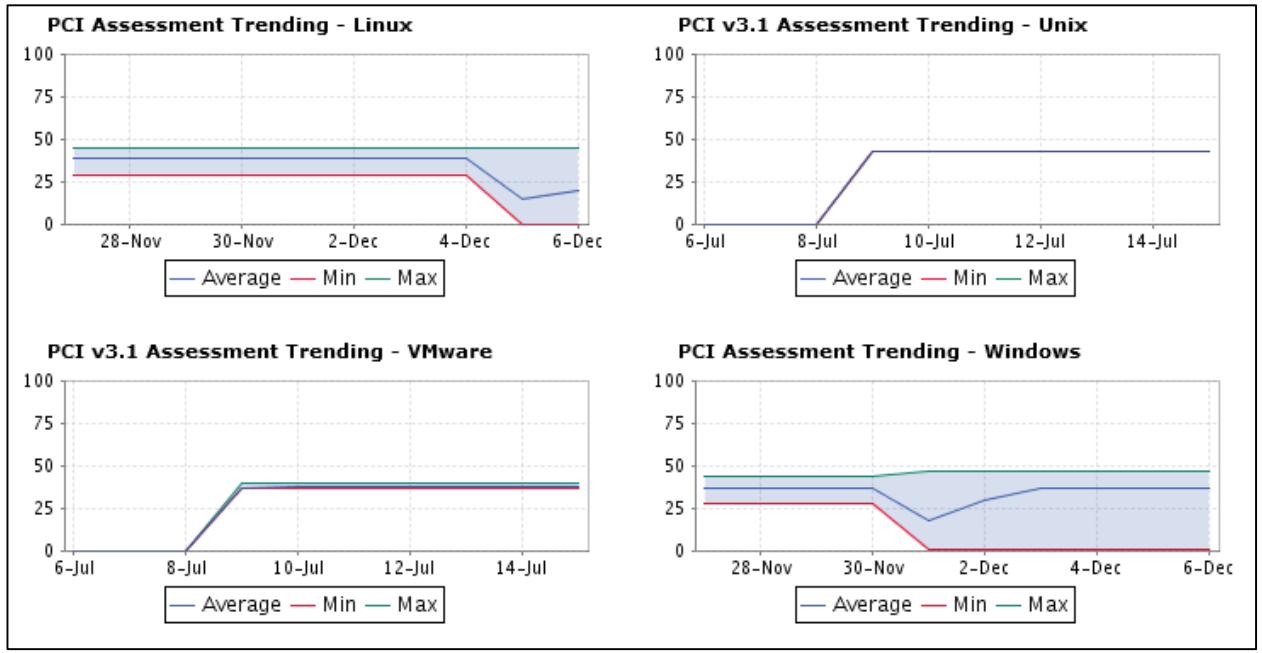
PCI Reports

Name	Run	Browse To
1.PCI Scope Inventory	Run	View
2.PCI FIM Rules Inventory	Run	View
2.PCI Policy Compliance Technical Controls Inventory	Run	View
3.PCI Controls Scheduled Tasks	Run	View
4.PCI Change Process Compliance Last 30 days	Run	View
5.PCI Policy Compliance Technical Controls Detailed Results (ALL)	Run	View
5.PCI Policy Compliance Technical Controls Detailed Results w/ Remediation (Failed)	Run	View
5.PCI Policy Compliance Technical Controls Results Summary (ALL)	Run	View

Historical Information to hit KPIs







Whitelist Automated Evidence Collection

Ensure Installed Software is Authorized and Up To Date [Windows]

Node: Scada-Windows.galaxy.ffa (Windows)

Overall result: Failed @ 3/25/16 3:07 PM

Element: Unauthorized Installed Software

Result

Failed

Time

3/25/16 3:07 PM

Actual

Unauthorized Installed Software=

****
** UNAUTHORIZED SOFTWARE FOUND **
****

Software Name: FileZilla Client 3.7.3
Detected Version: 3.7.3

****
** UNAUTHORIZED SOFTWARE FOUND **
****

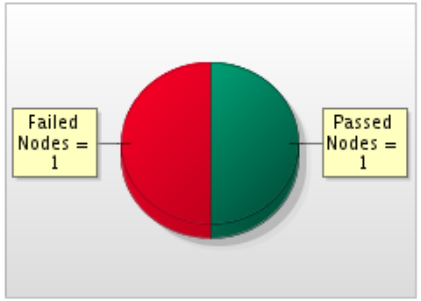
Software Name: Google Chrome
Detected Version: 34.0.1847.116

Close

PORTS | SETTINGS

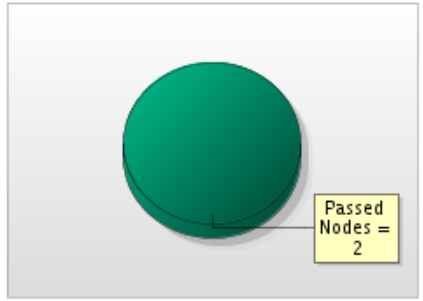
DISA STIG Overview | NERC CIP Overview | **NERC CIP Whitelisting** | NIST 800-53 - High Security | Operations | PCI Overview - v3.1 | SOX Internal Au

CIP 007-R2 - Network Ports



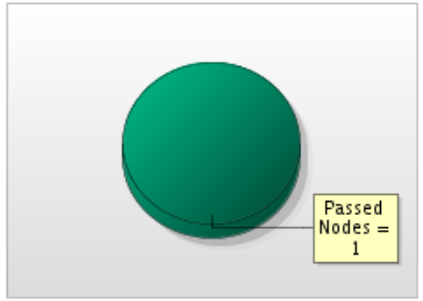
Passed Nodes Failed Nodes

CIP 004-R4 - Local Users Extended



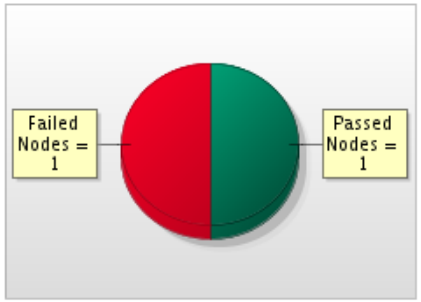
Passed Nodes

CIP 004-R4 - Local Groups



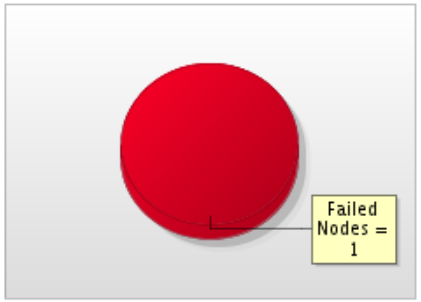
Passed Nodes

CIP 007-R3 - Installed Software



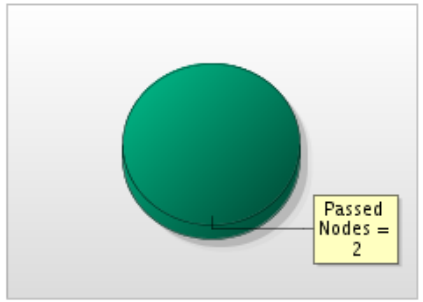
Passed Nodes Failed Nodes

CIP 004-R4 - Local Shares



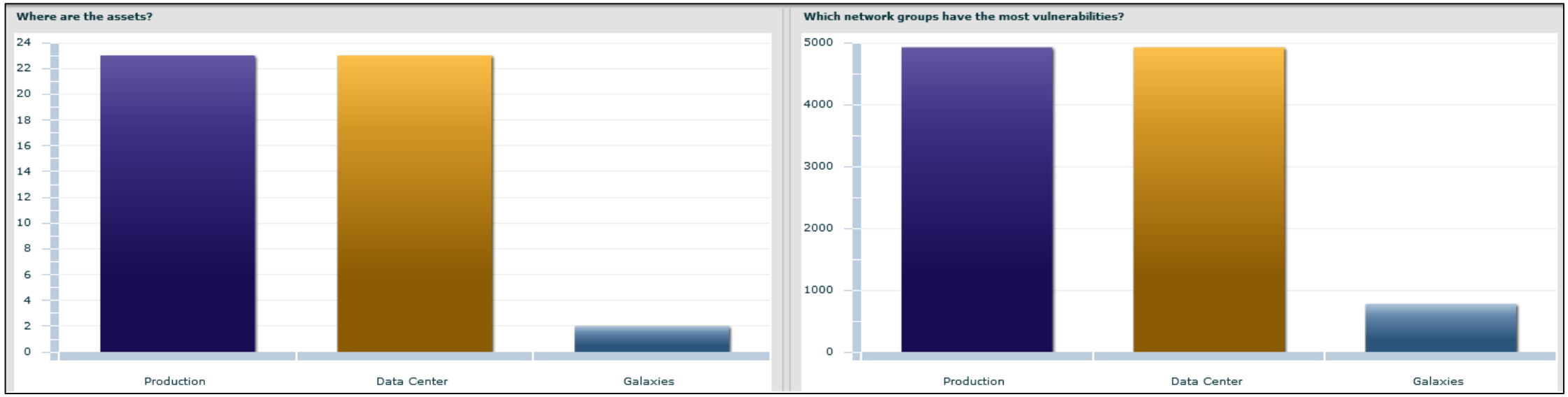
Failed Nodes

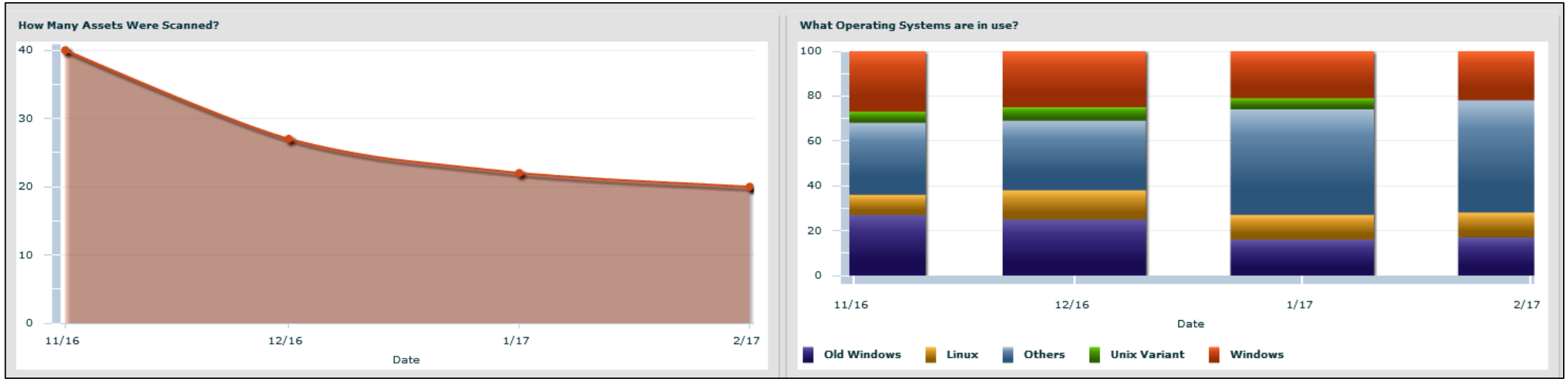
CIP 005-R1 - Persistent Routes



Passed Nodes

Vulnerability Overview for in scope assets





PCI requires CVSS score 8.0 higher vulnerabilities be remediated within 30 days.

IP	Vulnerability	Score	CVSS Base	First Seen	Last Seen	Last Scan	Target	Fix Days	Remediated
10.64.0.17	MS98-004: Microsoft Windows NT IIS MDAC RDS Vul	59350	10.0	02/11/2017 19:09:25	02/26/2017 19:10:28	02/27/2017 19:10:21	03/13/2017 19:09:25	15	Y
10.64.0.17	MS01-033: Microsoft Index Server and Indexing Se	54477	10.0	02/11/2017 19:09:25	02/26/2017 19:10:28	02/27/2017 19:10:21	03/13/2017 19:09:25	15	Y
10.64.0.20	MS03-026: Microsoft Windows DCOM RPC Interface	50753	7.5	02/13/2017 19:07:25	02/26/2017 19:10:28	02/27/2017 19:10:21	03/15/2017 19:07:25	13	Y
10.64.0.17	MS03-026: Microsoft Windows DCOM RPC Interface	50741	7.5	02/16/2017 19:40:31	02/19/2017 19:50:32	02/27/2017 19:10:21	03/18/2017 19:40:31	3	Y
10.64.0.57	MS03-026: Microsoft Windows DCOM RPC Interface	50724	7.5	02/09/2017 19:07:17	02/24/2017 19:08:18	02/27/2017 19:10:21	03/11/2017 19:07:17	15	Y
10.64.0.20	MS03-026: Microsoft Windows DCOM RPC Interface	50717	7.5	02/13/2017 19:07:25	02/13/2017 19:07:25	02/27/2017 19:10:21	03/15/2017 19:07:25	0	Y
10.64.0.57	MS03-026: Microsoft Windows DCOM RPC Interface	50702	7.5	02/10/2017 19:08:52	02/10/2017 19:08:52	02/27/2017 19:10:21	03/12/2017 19:08:52	0	Y
10.64.0.20	MS03-049: Microsoft Windows 2000 / XP Workstatio	50147	7.5	02/13/2017 19:07:25	02/26/2017 19:10:28	02/27/2017 19:10:21	03/15/2017 19:07:25	13	Y
10.64.0.20	MS04-007: Microsoft Windows ASN.1 Library Integer	49664	7.5	02/13/2017 19:07:25	02/23/2017 19:46:37	02/27/2017 19:10:21	03/15/2017 19:07:25	10	Y
10.64.0.20	MS04-007: Microsoft Windows ASN.1 Library Integer	49655	7.5	02/13/2017 19:07:25	02/19/2017 19:50:32	02/27/2017 19:10:21	03/15/2017 19:07:25	6	Y
10.64.0.57	MS04-007: Microsoft Windows ASN.1 Library Integer	49622	7.5	02/10/2017 19:08:52	02/10/2017 19:08:52	02/27/2017 19:10:21	03/12/2017 19:08:52	0	Y
10.64.0.57	MS04-007: Microsoft Windows ASN.1 Library Integer	49622	7.5	02/10/2017 19:08:52	02/10/2017 19:08:52	02/27/2017 19:10:21	03/12/2017 19:08:52	0	Y
10.64.0.20	MS04-011: Microsoft Windows LSASS Buffer Overrun	49334	7.5	02/17/2017 19:58:25	02/19/2017 19:50:32	02/27/2017 19:10:21	03/19/2017 19:58:25	2	Y
10.64.0.20	MS04-011: Microsoft Windows Private Communicatic	49334	7.5	02/17/2017 19:58:25	02/19/2017 19:50:32	02/27/2017 19:10:21	03/19/2017 19:58:25	2	Y
10.64.0.20	MS04-011: Microsoft Windows Private Communicatic	49334	7.5	02/17/2017 19:58:25	02/19/2017 19:50:32	02/27/2017 19:10:21	03/19/2017 19:58:25	2	Y
10.64.0.20	MS04-011: Microsoft Windows LSASS Buffer Overrun	49334	7.5	02/17/2017 19:58:25	02/19/2017 19:50:32	02/27/2017 19:10:21	03/19/2017 19:58:25	2	Y
10.64.0.57	MS04-011: Microsoft Windows LSASS Buffer Overrun	49292	7.5	02/10/2017 19:08:52	02/10/2017 19:08:52	02/27/2017 19:10:21	03/12/2017 19:08:52	0	Y
10.64.0.57	MS04-011: Microsoft Windows LSASS Buffer Overrun	49292	7.5	02/10/2017 19:08:52	02/10/2017 19:08:52	02/27/2017 19:10:21	03/12/2017 19:08:52	0	Y

Out of the box Compliance Reports

Audit Logger | Query Results | Query Results

Overview | Query | Logger Cache | Archive

Query Criteria | Query History

- Requirement 01
  - Section 1.1.1
    - Configuration Changes to Firewalls - Detailed
  - Section 1.1.6
  - Section 1.2.1
  - Section 1.2.3
    - Permitted Inbound Packets by Firewall - Detailed
    - Permitted Outbound Packets by Firewall - Detailed
  - Section 1.3.1
  - Section 1.3.2
  - Section 1.3.3
  - Section 1.3.4
  - Section 1.3.5
- Requirement 02
- Requirement 05
- Requirement 06
  - Section 6.1
  - Section 6.2
  - Section 6.4.5
    - Configuration Changed by Host - Detailed
    - System Updated by Host - Detailed
  - Section 6.6
- Requirement 07
- Requirement 08
- Requirement 09
- Requirement 10
- Requirement 11
- Requirement 12
  - Section 12.3.10
  - Section 12.3.2
    - Successful Logon Events by Host - Detailed
  - Section 12.3.9

PCI DSS 3.0 Requirement 6.4.5 Detailed Report by Host

TRIPWIRE LOG CENTER

From: 10/29/2014 5:09:24 PM **To:** 5/9/2017 5:50:34 PM

The following report provides an overview of the actions undertaken to be compliant with the Payment Card Industry Data Security Standard v3.0 Requirement 6.4.5 during the period of time listed above. This report displays the updating or patching of systems.

Timestamp	User	Event
Host :	**192.168.97.151**	
10/30/2014 4:54:10 PM		NET: updated
10/31/2014 11:02:58 AM		NET: updated
Host :	**192.168.97.153**	
10/29/2014 5:09:24 PM		NET: updated

Summary

tripwire®

CONFIDENCE: SECURED

THANK YOU

tripwire.com | @TripwireInc