tripwire®

CONFIDENCE: SECURED

Monitoring and Maintaining Compliance

What Defines SCM?

Import and Assess

Know the Configuration State

- Absorb many policies
- Assess many platforms
- Tailor and customize policies
- Report discrepancies
- Manage exceptions & waivers
- Put checks in checkboxes
- Make reports for auditors

Detect and Detail

Know What Happened & Why

- When is a policy violated?
- When do I find out about it?
- How do I find about about it?
- Who violated it and why?
- Is this an operational issue…
- Or a security issue…
- Or a compliance issue?

Remediate and Integrate

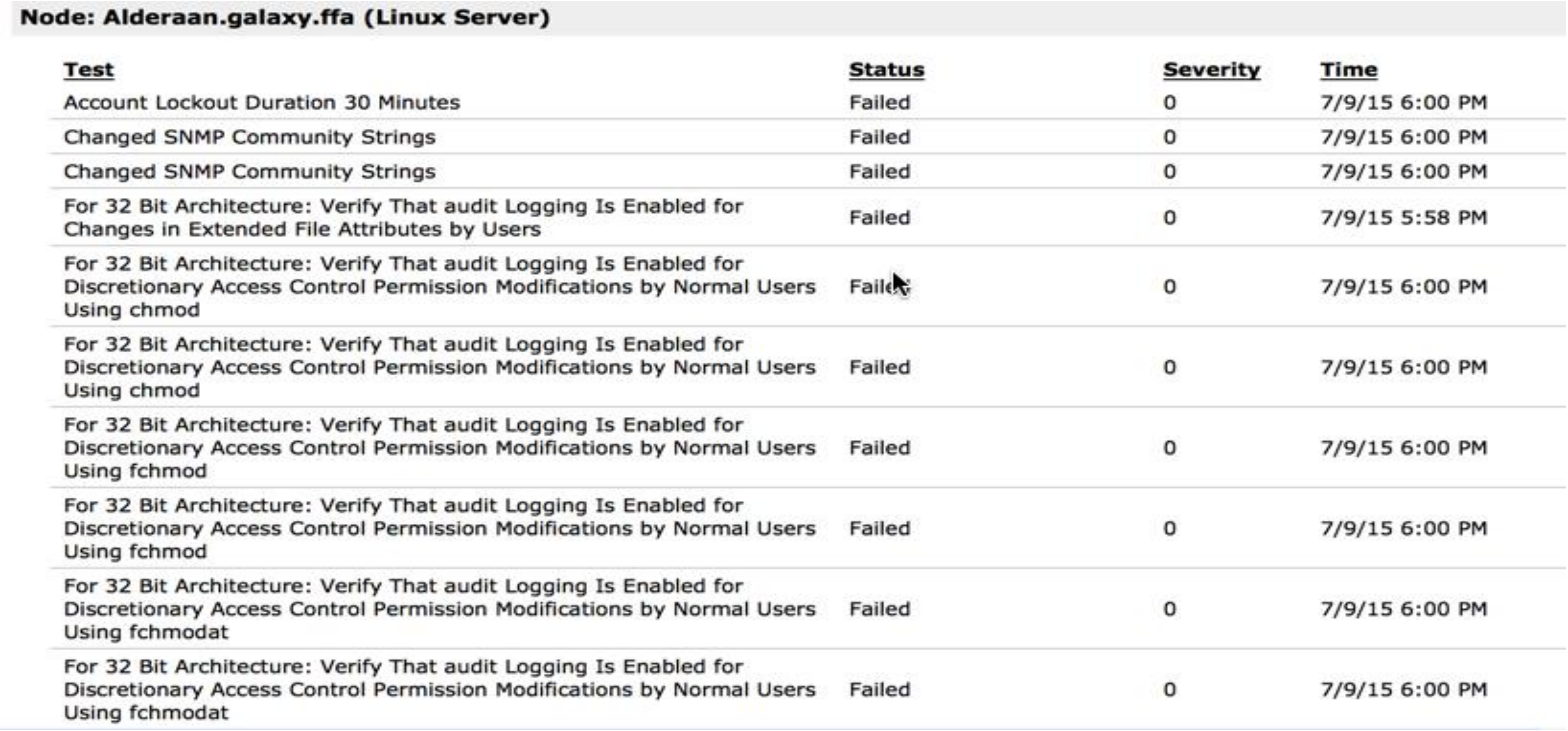
What Do I Do About It?

- Can I show ops how to fix this?
- Can I fix it myself?
- Can I feed change systems?
- Can I be fed by them?
- Can I inform security systems?
- Do I absorb business context?
- Can I be a “leading indicator”?

Creating your standard

- Should have the standards pre-built
- Should make it easy to create your own standard
- Should allow a customer to copy tests to your own standard
- Should allow a customer to edit tests so that it conforms to your company standard
- Should have a way of detecting in a reasonable timeframe the changes to a system that will make it pass or fail a test

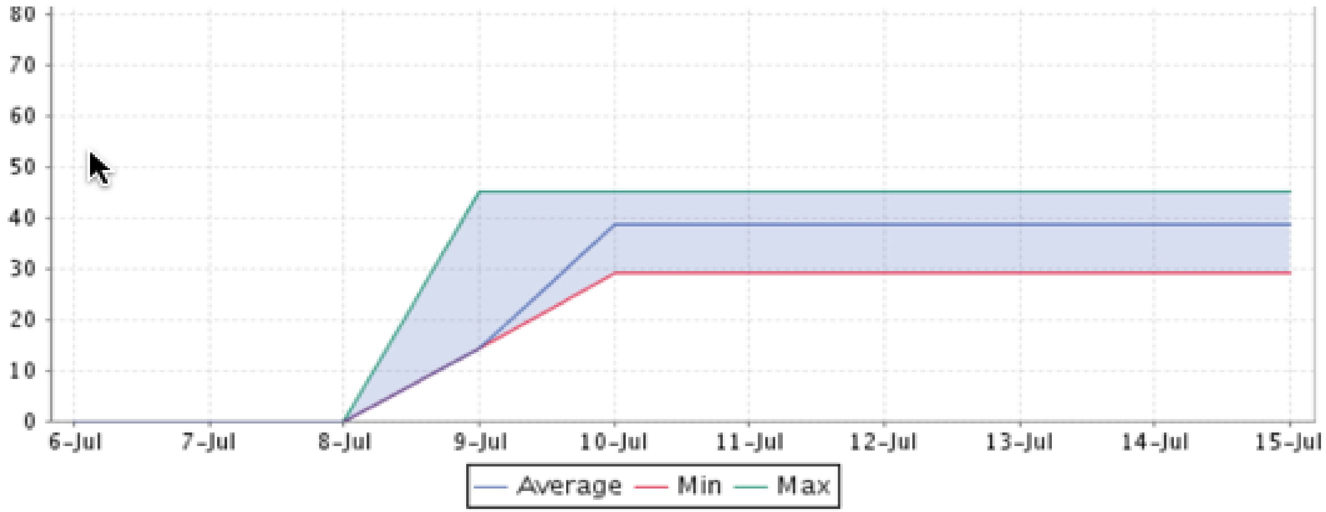
Test Summary Reporting



Node: Alderaan.galaxy.ffa (Linux Server)

Test	Status	Severity	Time
Account Lockout Duration 30 Minutes	Failed	0	7/9/15 6:00 PM
Changed SNMP Community Strings	Failed	0	7/9/15 6:00 PM
Changed SNMP Community Strings	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Changes in Extended File Attributes by Users	Failed	0	7/9/15 5:58 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using chmod	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using chmod	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using fchmod	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using fchmod	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using fchmodat	Failed	0	7/9/15 6:00 PM
For 32 Bit Architecture: Verify That audit Logging Is Enabled for Discretionary Access Control Permission Modifications by Normal Users Using fchmodat	Failed	0	7/9/15 6:00 PM

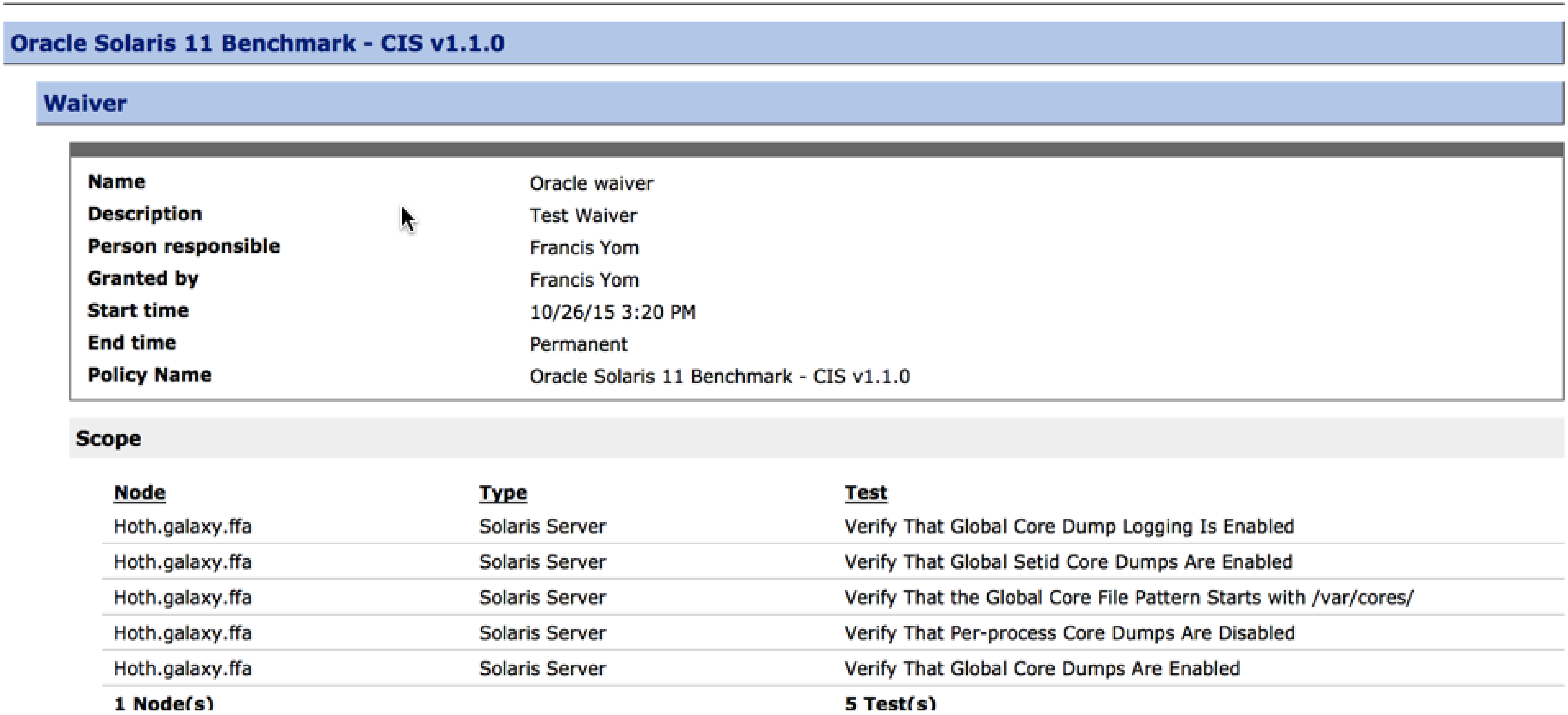
Result Trending Report



Details

Interval	Average	Min	Max
7/6/15	0.00	0.00	0.00
7/7/15	0.00	0.00	0.00
7/8/15	0.00	0.00	0.00
7/9/15	14.19	14.19	45.06
7/10/15	38.68	28.93	45.06
7/11/15	38.68	28.93	45.06
7/12/15	38.68	28.93	45.06
7/13/15	38.68	28.93	45.06
7/14/15	38.68	28.93	45.06
7/15/15	38.68	28.93	45.06
Totals:	**23.53**	**14.19**	**45.06**

Exception Reporting



Oracle Solaris 11 Benchmark - CIS v1.1.0

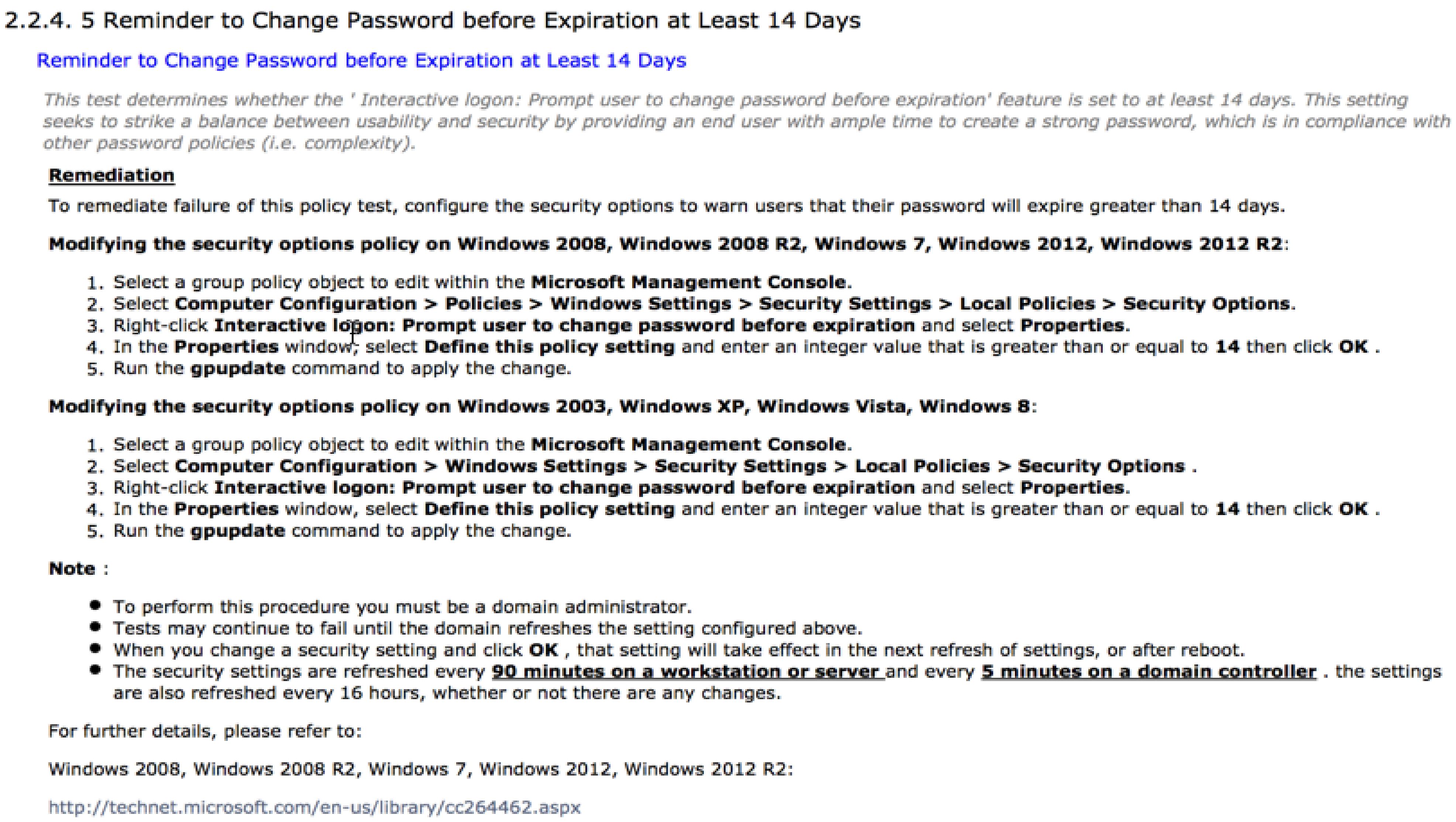
Waiver

Name	Oracle waiver
Description	Test Waiver
Person responsible	Francis Yom
Granted by	Francis Yom
Start time	10/26/15 3:20 PM
End time	Permanent
Policy Name	Oracle Solaris 11 Benchmark - CIS v1.1.0

Scope

Node	Type	Test
Hoth.galaxy.ffa	Solaris Server	Verify That Global Core Dump Logging Is Enabled
Hoth.galaxy.ffa	Solaris Server	Verify That Global Setid Core Dumps Are Enabled
Hoth.galaxy.ffa	Solaris Server	Verify That the Global Core File Pattern Starts with /var/cores/
Hoth.galaxy.ffa	Solaris Server	Verify That Per-process Core Dumps Are Disabled
Hoth.galaxy.ffa	Solaris Server	Verify That Global Core Dumps Are Enabled
1 Node(s)		**5 Test(s)**

Remediation Assistance



2.2.4. 5 Reminder to Change Password before Expiration at Least 14 Days

Reminder to Change Password before Expiration at Least 14 Days

This test determines whether the ' Interactive logon: Prompt user to change password before expiration' feature is set to at least 14 days. This setting seeks to strike a balance between usability and security by providing an end user with ample time to create a strong password, which is in compliance with other password policies (i.e. complexity).

Remediation

To remediate failure of this policy test, configure the security options to warn users that their password will expire greater than 14 days.

Modifying the security options policy on Windows 2008, Windows 2008 R2, Windows 7, Windows 2012, Windows 2012 R2:

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: Prompt user to change password before expiration** and select **Properties.**
4. In the **Properties** window, select **Define this policy setting** and enter an integer value that is greater than or equal to **14** then click **OK** .
5. Run the **gpupdate** command to apply the change.

Modifying the security options policy on Windows 2003, Windows XP, Windows Vista, Windows 8:

1. Select a group policy object to edit within the **Microsoft Management Console.**
2. Select **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** .
3. Right-click **Interactive logon: Prompt user to change password before expiration** and select **Properties.**
4. In the **Properties** window, select **Define this policy setting** and enter an integer value that is greater than or equal to **14** 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:

Windows 2008, Windows 2008 R2, Windows 7, Windows 2012, Windows 2012 R2:

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

tripwire®
CONFIDENCE: SECURED

Thank you

tripwire.com | @TripwireInc