OSS Security
“What you need to know”

Callum Barclay

CTO and Founder

Computer Security Products Inc.

About CSP

- Based in Toronto, Canada with Partners, Agents and Distributors worldwide
- NonStop® Alliance One Partner since 1987.
- Develop, Support and Distribute Security, Compliance and Audit Solutions for the HP NonStop® Market.

- Large number of Customers and over 1000+ licenses World Wide
- Customers include:
  - Largest Banks
  - Major Stock Exchanges
  - Defense and Healthcare organizations
  - Telecommunications
  - Manufacturers

Integrity Ready Partner
hp invent

Business Partner
hp invent

CSP
Computer Security Products Inc.

Agenda

- Current applications in OSS
- What people told us about OSS security
- OSS Specific Security Settings
- Procedures and tools
- CSP – How we can help OSS users

Applications in OSS

- NonStop Web services related:
  - SOAP
  - iTP Web server
  - JSP, JBOSS, Spring, Apache C
  - SQL/MX

Applications in OSS

- 3rd Party:
  - Base24 EPS (TSS)
  - Lusis Tango
  - ReD Fraud
  - IBM MQ
  - GGS
  - AJB
  - LIG
  - Others....

ORACLE
GOLDEN GATE

AJB software

IBM WEBSPHERE MQ

ReDi

OSS Security Survey Results:

- Survey sent to 369 Users, -> 73 competed surveys.
- 82% using or planning to use OSS
- Most popular are SQLMX and IBMMQ
- 90% though it important or critical to have a secure OSS environment
- A plethora of security strategies!!

OSS Security Survey Results (cont'd)

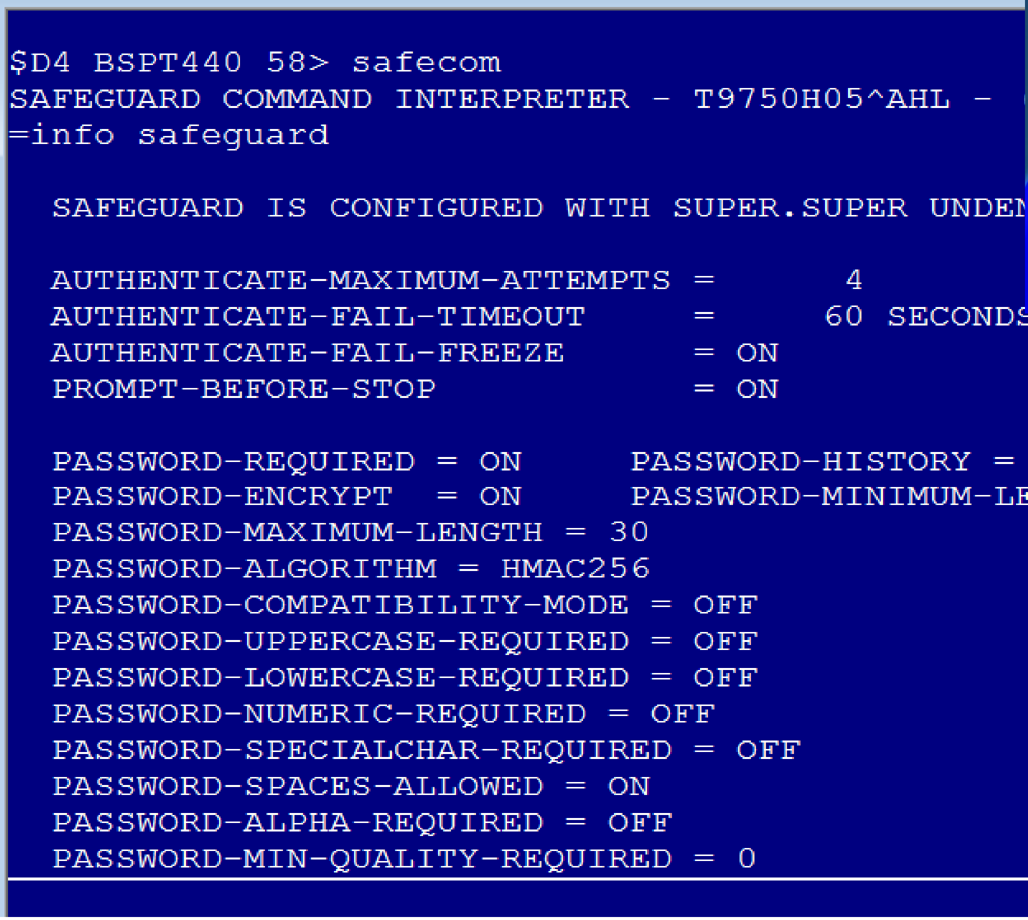
- Over 43% said it would be difficult or very difficult
- Yet over 80% want better granularity and visibility of OSS security settings!
- Primary concerns: Lack of knowledge or difficulty of integration with existing schemes.
- Room for Improvement:
  - Visability
  - Command Control and auto-elevation of privilege
- NonStop-X??

NonStop system security context

- Safeguard Globals
- OSS specifics:
  - Filesets
  - User and admin access
  - Default shell and file permissions
  - Audit setup

Safeguard

Safeguard
COMMANDER SAFEGUARD
Safeguard MISSION: CLEAN SWEEP
© Copyrights 2005. Procter & Gamble Pakistan, All Rights Reserved
www.commandersafeguard.com



```
$D4 BSPT440 58> safecom
SAFEGUARD COMMAND INTERPRETER - T9750H05^AHL -
=info safeguard

  SAFEGUARD IS CONFIGURED WITH SUPER.SUPER UNDE

  AUTHENTICATE-MAXIMUM-ATTEMPTS =       4
  AUTHENTICATE-FAIL-TIMEOUT     =      60 SECONDS
  AUTHENTICATE-FAIL-FREEZE      = ON
  PROMPT-BEFORE-STOP            = ON

  PASSWORD-REQUIRED = ON      PASSWORD-HISTORY =   3
  PASSWORD-ENCRYPT  = ON      PASSWORD-MINIMUM-LENGTH =   4
  PASSWORD-MAXIMUM-LENGTH = 30
  PASSWORD-ALGORITHM = HMAC256
  PASSWORD-COMPATIBILITY-MODE = OFF
  PASSWORD-UPPERCASE-REQUIRED = OFF
  PASSWORD-LOWERCASE-REQUIRED = OFF
  PASSWORD-NUMERIC-REQUIRED = OFF
  PASSWORD-SPECIALCHAR-REQUIRED = OFF
  PASSWORD-SPACES-ALLOWED = ON
  PASSWORD-ALPHA-REQUIRED = OFF
  PASSWORD-MIN-QUALITY-REQUIRED = 0
                                                                   CONV
```

OSS Filesets

- OSS filesets – analogous to the Unix “mount” operation, with NonStop OSS specifics.
- Managed through SCF:
  - Audit set ON if needed.
  - Access options:
    - Lock-out SUPER.SUPER.
    - Make read-only.

Audit in OSS

- Set by fileset
- Set ON for Security-OSS-Administrator.
- Turn on the OSS Client audit in Safeguard
- Warning: injudicious audit settings may overwhelm your audit pool...

Access Rights for OSS files

- Not subject to Safeguard rules.
- Secured using Unix like permission strings:

Owner	Group	World
r w x	r w x	r w x

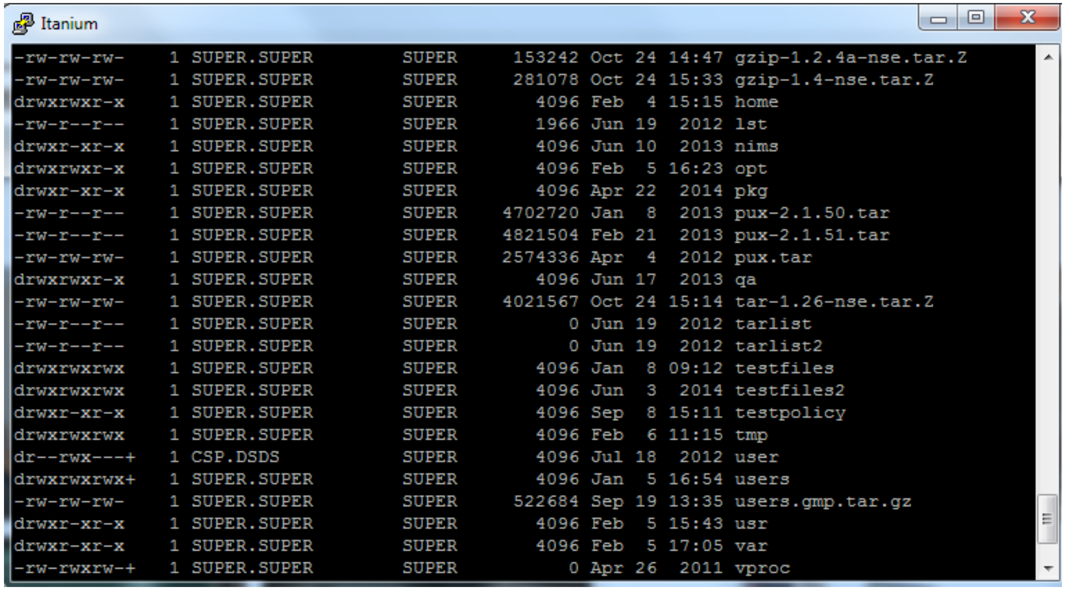
- Options for setuid, setgid etc.
- Managed with chmod, chown, chrgrp commands.

OSS Basic Permissions

- OSS uses the Unix format (owner/group/world)
- Don’t rely on the defaults!
- Common issues (just like Guardian):
  - Orphan Files
  - Excessive Privileges
  - Files Accessible to all users
- How are you checking yours?

OSS Basic Permissions – Issues

- Visibility and reportability
- The three categories (owner/group/world) are sometimes not granular enough.
- Managed from the command line and/or scripts

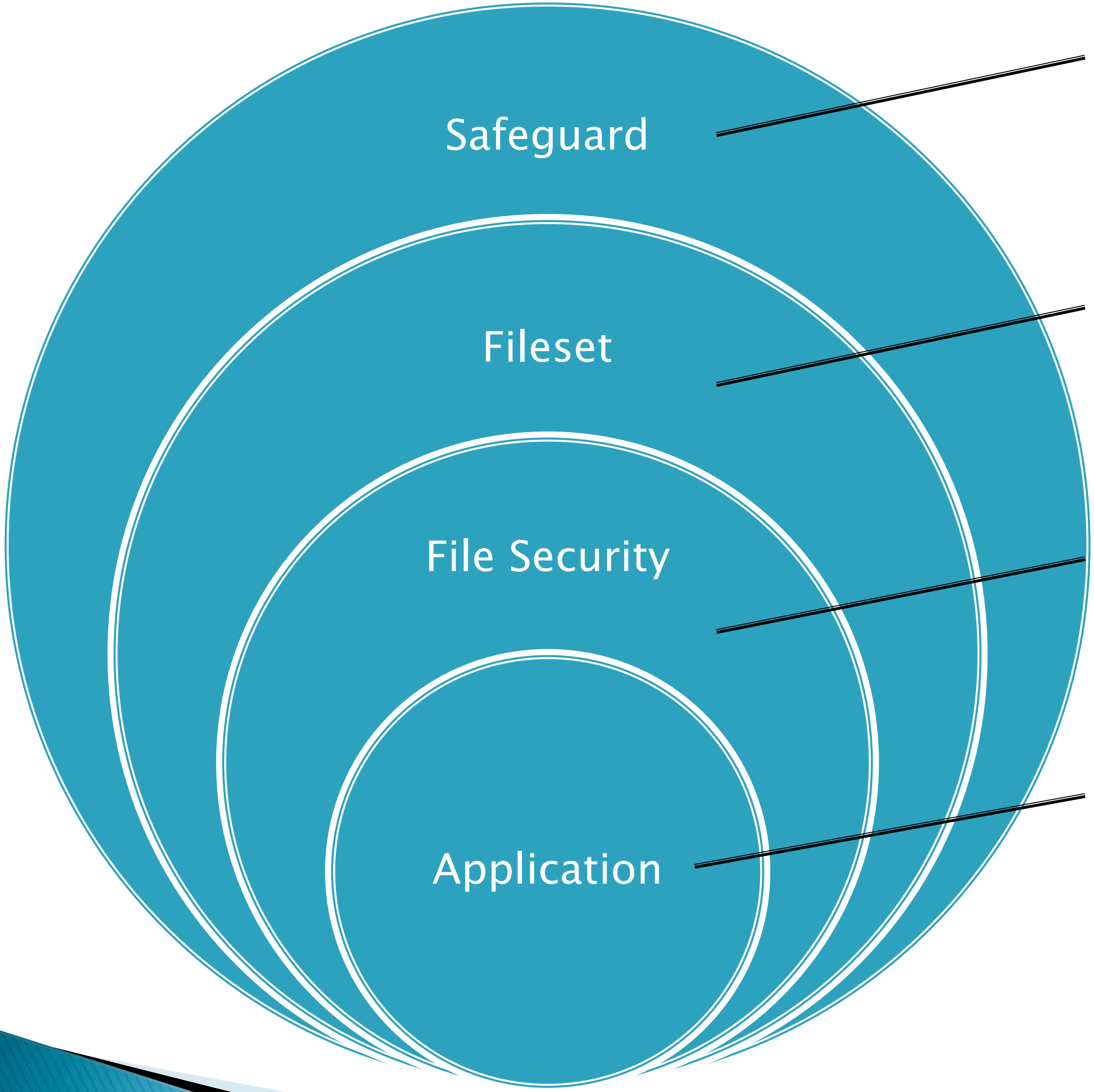


```
-rw-rw-rw-    1 SUPER.SUPER        SUPER     153242 Oct 24 14:47 gzip-1.2.4a-nse.tar.Z
-rw-rw-rw-    1 SUPER.SUPER        SUPER     281078 Oct 24 15:33 gzip-1.4-nse.tar.Z
drwxrwxr-x    1 SUPER.SUPER        SUPER       4096 Feb  4 15:15 home
-rw-r--r--    1 SUPER.SUPER        SUPER       1966 Jun 19  2012 lst
drwxr-xr-x    1 SUPER.SUPER        SUPER       4096 Jun 10  2013 nims
drwxrwxr-x    1 SUPER.SUPER        SUPER       4096 Feb  5 16:23 opt
drwxr-xr-x    1 SUPER.SUPER        SUPER       4096 Apr 22  2014 pkg
-rw-r--r--    1 SUPER.SUPER        SUPER    4702720 Jan  8  2013 pux-2.1.50.tar
-rw-r--r--    1 SUPER.SUPER        SUPER    4821504 Feb 21  2013 pux-2.1.51.tar
-rw-rw-rw-    1 SUPER.SUPER        SUPER    2574336 Apr  4  2012 pux.tar
drwxrwxr-x    1 SUPER.SUPER        SUPER       4096 Jun 17  2013 qa
-rw-rw-rw-    1 SUPER.SUPER        SUPER    4021567 Oct 24 15:14 tar-1.26-nse.tar.Z
-rw-r--r--    1 SUPER.SUPER        SUPER          0 Jun 19  2012 tarlist
-rw-r--r--    1 SUPER.SUPER        SUPER          0 Jun 19  2012 tarlist2
drwxrwxrwx    1 SUPER.SUPER        SUPER       4096 Jan  8 09:12 testfiles
drwxrwxrwx    1 SUPER.SUPER        SUPER       4096 Jun  3  2014 testfiles2
drwxr-xr-x    1 SUPER.SUPER        SUPER       4096 Sep  8 15:11 testpolicy
drwxrwxrwx    1 SUPER.SUPER        SUPER       4096 Feb  6 11:15 tmp
dr--rwx---+   1 CSP.DSDS           SUPER       4096 Jul 18  2012 user
drwxrwxrwx+   1 SUPER.SUPER        SUPER       4096 Jan  5 16:54 users
-rw-rw-rw-    1 SUPER.SUPER        SUPER     522684 Sep 19 13:35 users.gmp.tar.gz
drwxr-xr-x    1 SUPER.SUPER        SUPER       4096 Feb  5 15:43 usr
drwxr-xr-x    1 SUPER.SUPER        SUPER       4096 Feb  5 17:05 var
-rw-rwxrw-+   1 SUPER.SUPER        SUPER          0 Apr 26  2011 vproc
```

Computer Security Products Inc.

OSS Extended ACLs

- Recommended by HP to provide improved granularity.
- Based on the HP-UX implementation.
- Allow for:
  - specific permissions for users/groups on files/directories.
  - default ACLs on directories
- Managed with setacl, and viewed through getacl.
- Awkward to set and to read.
- Just like Safeguard ACLs, these can get messy very quickly…



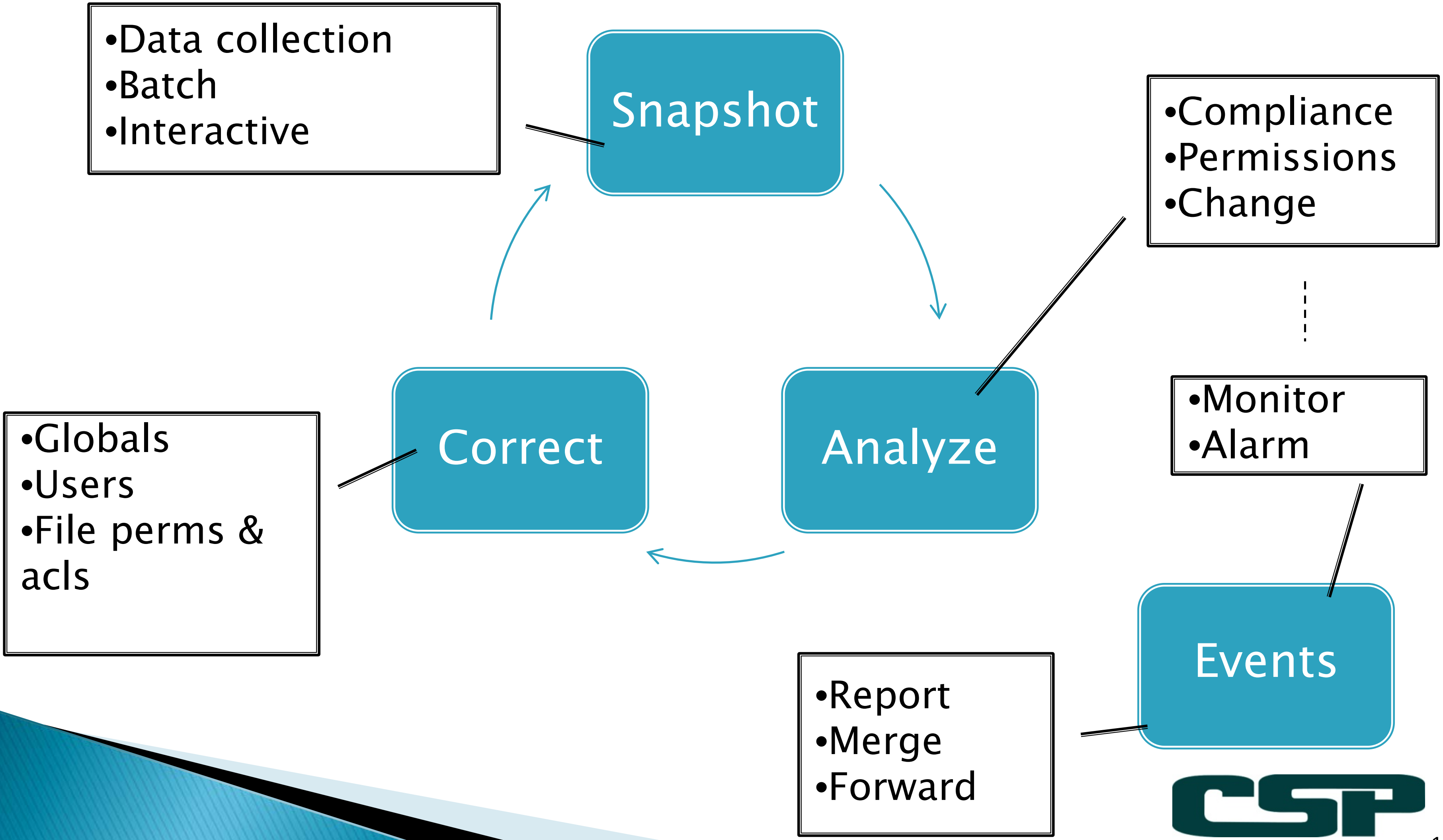
- •Globals
- •Users
- •Security Groups
- •Audit management

- •Restrict access
- •Audit enable

- •Basic permissions
- •Extended ACLs
- •Setuid/setgid

- •Application access rules
- •Log management

Ongoing OSS Compliance



Snapshot

- Data collection
- Batch
- Interactive

Analyze

- Compliance
- Permissions
- Change

Correct

- Globals
- Users
- File perms & acls

Events

- Monitor
- Alarm

- Report
- Merge
- Forward

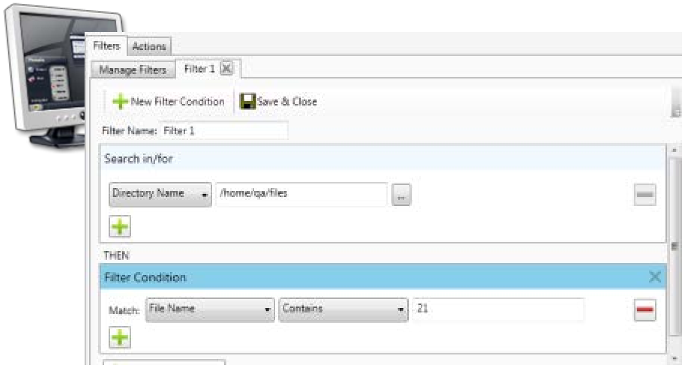
CSP Tools for the task:

- Initial Snapshot:
  - **Protect-UX** – Capture and visualize file permissions
  - **File Integrity Checker** (FIC): Monitor Files for changes.
  - Set up monitoring and event streams with **Alert-Plus** and **Auditview** for merged Audit.

- Ongoing:
  - Snapshot the directory tree and check contents for changes (log files OK)
  - Review for erroneous or excessive privilege, Orphan files, etc.

Protect-UX – a closer look:

Protect-UX Master Node is used to store policies files, credentials etc.



Filters | Actions

Manage Filters | Filter 1 ☒

New Filter Condition | Save & Close

Filter Name: Filter 1

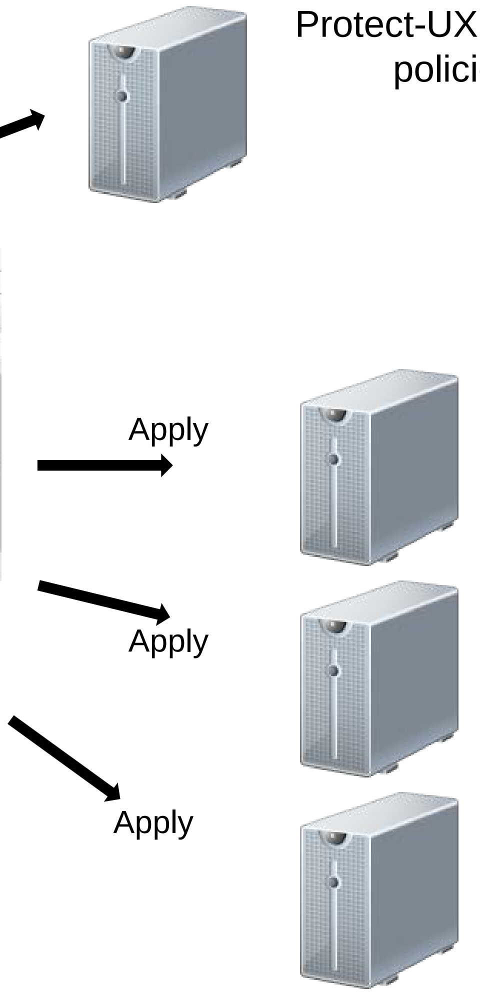
Search in/for

Directory Name: /home/qa/files

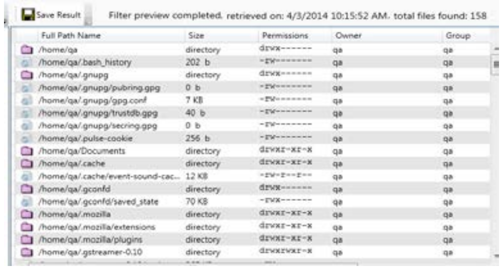
THEN

Filter Condition

Match: File Name | Contains | 21



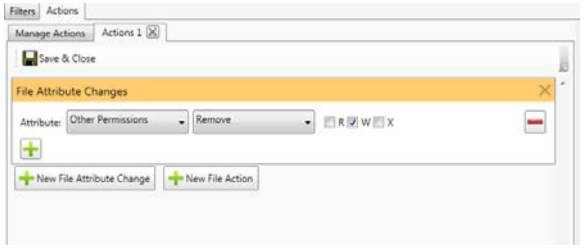
List matching files



Save Result | Filter preview completed. retrieved on: 4/3/2014 10:15:52 AM. total files found: 158

Full Path Name	Size	Permissions	Owner	Group
/home/qa	directory	drwx------	qa	qa
/home/qa/.bash_history	202 b	-rw-------	qa	qa
/home/qa/.gnupg	directory	drwx------	qa	qa
/home/qa/.gnupg/pubring.gpg	0 b	-rw-------	qa	qa
/home/qa/.gnupg/gpg.conf	7 KB	-rw-------	qa	qa
/home/qa/.gnupg/trustdb.gpg	40 b	-rw-------	qa	qa
/home/qa/.gnupg/secring.gpg	0 b	-rw-------	qa	qa
/home/qa/.pulse-cookie	256 b	-rw-------	qa	qa
/home/qa/Documents	directory	drwxr-xr-x	qa	qa
/home/qa/.cache	directory	drwxr-xr-x	qa	qa
/home/qa/.cache/event-sound-cac...	12 KB	-rw-r--r--	qa	qa
/home/qa/.gconfd	directory	drwx------	qa	qa
/home/qa/.gconfd/saved_state	70 KB	-rwx------	qa	qa
/home/qa/.mozilla	directory	drwxr-xr-x	qa	qa
/home/qa/.mozilla/extensions	directory	drwxr-xr-x	qa	qa
/home/qa/.mozilla/plugins	directory	drwxr-xr-x	qa	qa
/home/qa/.gstreamer-0.10	directory	drwxrwxr-x	qa	qa

...and/or apply changes .



Filters | Actions

Manage Actions | Actions 1 ☒

Save & Close

File Attribute Changes

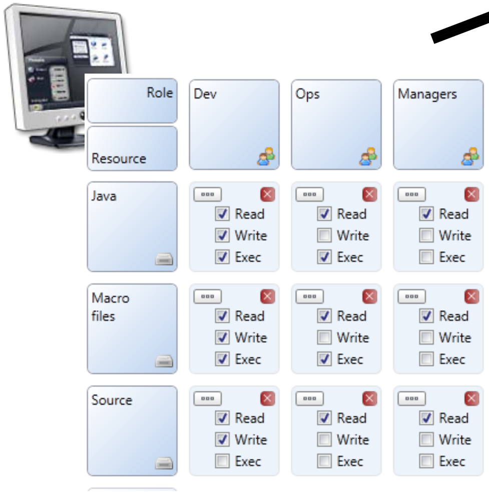
Attribute: Other Permissions | Remove | □ R ☑ W □ X

New File Attribute Change | New File Action

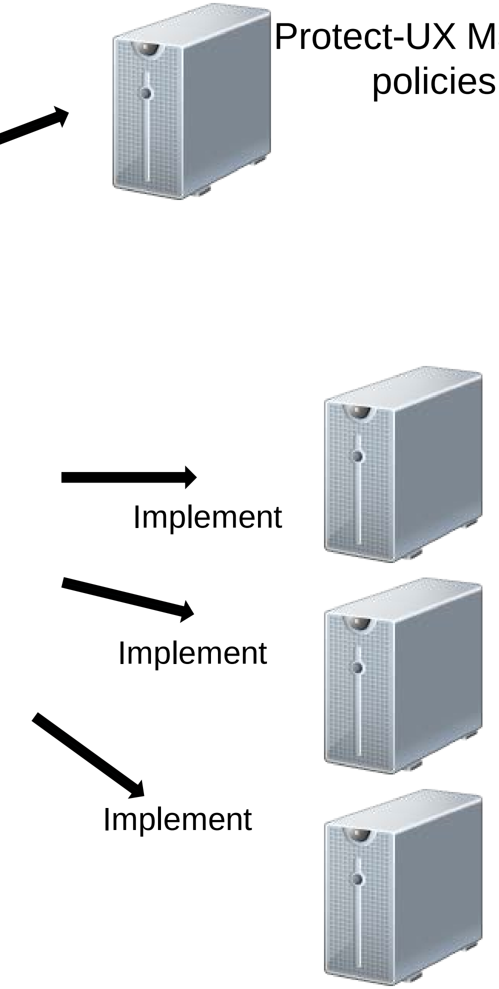
Protect-UX Fileset Macros (user- defined or templates) automates file management tasks based on attribute or name, to:

- discover current state
- apply settings or actions.

Protect-UX Policy Access Matrix



Role / Resource	Dev	Ops	Managers
Java	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Macro files	☑ Read ☑ Write ☑ Exec	☑ Read ☐ Write ☑ Exec	☑ Read ☐ Write ☐ Exec
Source	☑ Read ☑ Write ☐ Exec	☑ Read ☐ Write ☐ Exec	☑ Read ☐ Write ☐ Exec



Protect-UX Master Node is used to store policies files, credentials etc.

Protect-UX Policy is used to manage files for an application deployed on multiple systems with:

- Automated implementation
- Review and analysis tools

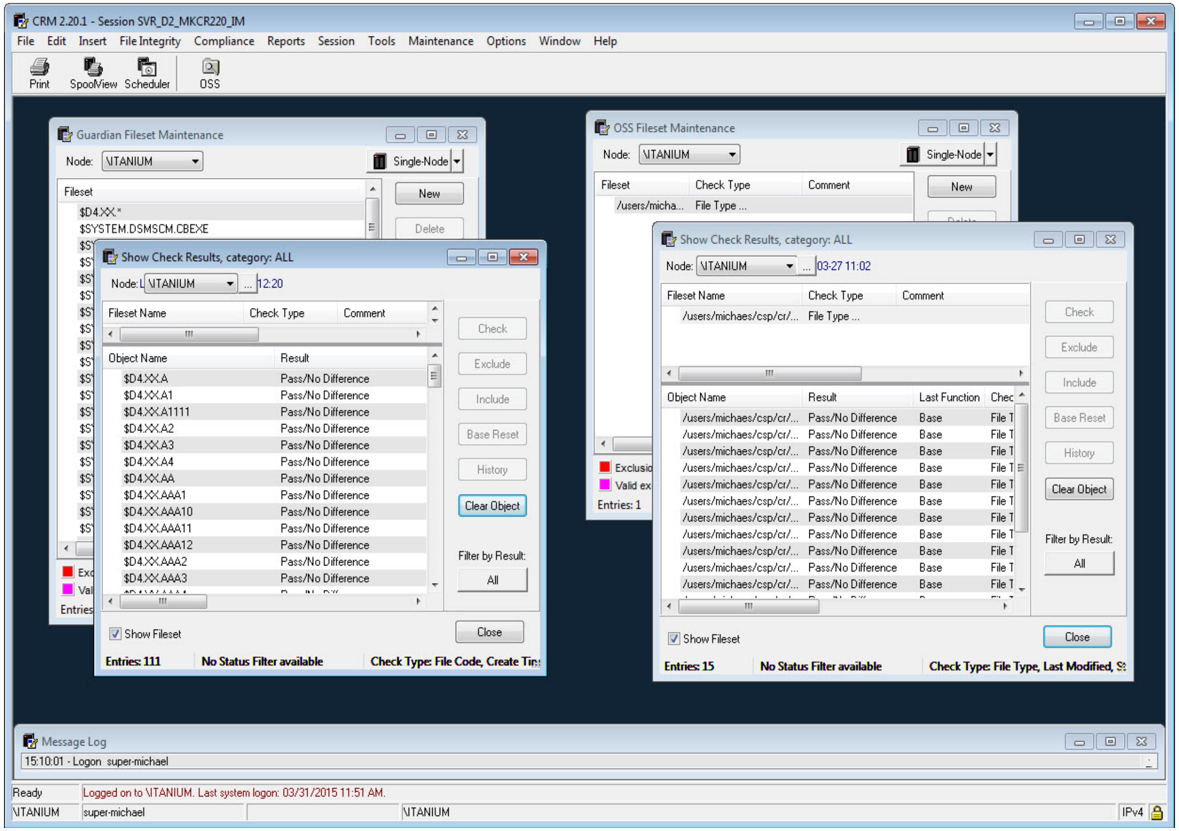
Computer Security Products Inc.

FIC – Check Your Files!

File integrity monitoring is a crucial requirement of PCI

Includes checking of:

- MD5/MD5-Inc
- File Type
- Last Modified
- Status Changed
- Owner
- Security Type
- Safeguard
- Security Mask
- Group
- Set UId
- Set GId
- EOF (also EOF Incremental)



Guardian Fileset Maintenance — Node: \ITANIUM

Fileset
$D4.XX.*
$SYSTEM.DSMSCM.CBEXE

Entries

Show Check Results, category: ALL — Node: \ITANIUM 12:20

Fileset Name	Check Type	Comment

Object Name	Result
$D4.XX.A	Pass/No Difference
$D4.XX.A1	Pass/No Difference
$D4.XX.A1111	Pass/No Difference
$D4.XX.A2	Pass/No Difference
$D4.XX.A3	Pass/No Difference
$D4.XX.A4	Pass/No Difference
$D4.XX.AA	Pass/No Difference
$D4.XX.AAA1	Pass/No Difference
$D4.XX.AAA10	Pass/No Difference
$D4.XX.AAA11	Pass/No Difference
$D4.XX.AAA12	Pass/No Difference
$D4.XX.AAA2	Pass/No Difference
$D4.XX.AAA3	Pass/No Difference

☑ Show Fileset

Entries: 111 | No Status Filter available | Check Type: File Code, Create Tir

OSS Fileset Maintenance — Node: \ITANIUM

Fileset	Check Type	Comment
/users/micha...	File Type ...	

🟥 Exclusio

🟪 Valid ex

Entries: 1

Show Check Results, category: ALL — Node: \ITANIUM 03-27 11:02

Fileset Name	Check Type	Comment
/users/michaes/csp/cr/...	File Type ...	

Object Name	Result	Last Function	Chec
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T
/users/michaes/csp/cr/...	Pass/No Difference	Base	File T

☑ Show Fileset

Entries: 15 | No Status Filter available | Check Type: File Type, Last Modified, S

15:10:01 - Logon super-michael

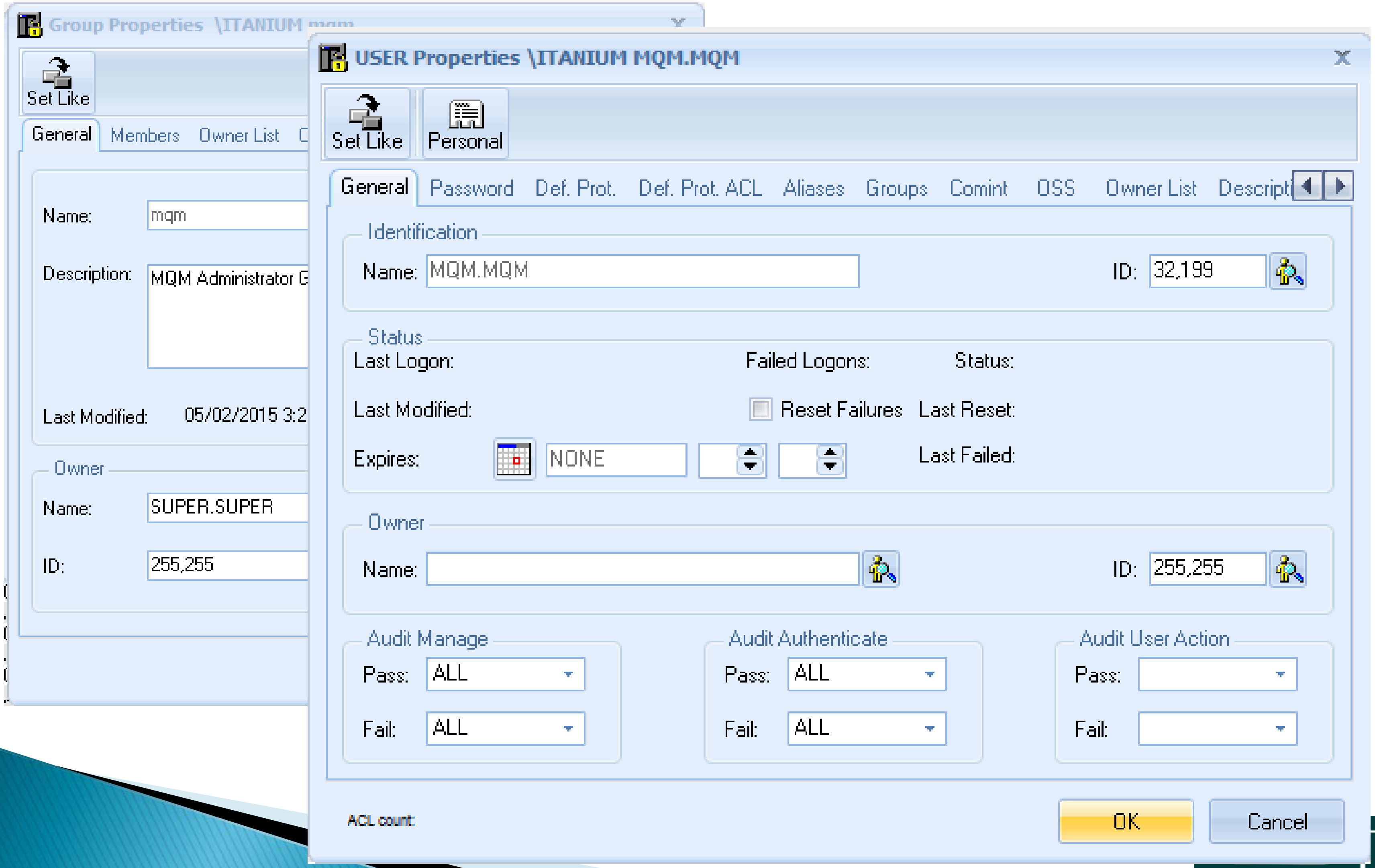
Ready | Logged on to \ITANIUM. Last system logon: 03/31/2015 11:51 AM.

\ITANIUM | super-michael | \ITANIUM | IPv4

Let's look a specific example: IBM MQ

- Pre-installation:
  - Adding the user and group mqm.mqm
  - Ensure the initial location permissions are open
  - Create a fileset (if necessary) to contain files.
- Post-installation:
  - Snapshot the directory tree and contents
  - Review for erroneous or excessive privilege
  - Set up monitoring and event streams

CSP Protect XP:
Add the user and group



Group Properties \ITANIUM mqm

Name: mqm

Description: MQM Administrator G

Last Modified: 05/02/2015 3:2

Owner

Name: SUPER.SUPER

ID: 255,255

USER Properties \ITANIUM MQM.MQM

Identification

Name: MQM.MQM

ID: 32,199

Status

Last Logon:

Failed Logons:

Status:

Last Modified:

□ Reset Failures

Last Reset:

Expires: NONE

Last Failed:

Owner

Name:

ID: 255,255

Audit Manage

Pass: ALL

Fail: ALL

Audit Authenticate

Pass: ALL

Fail: ALL

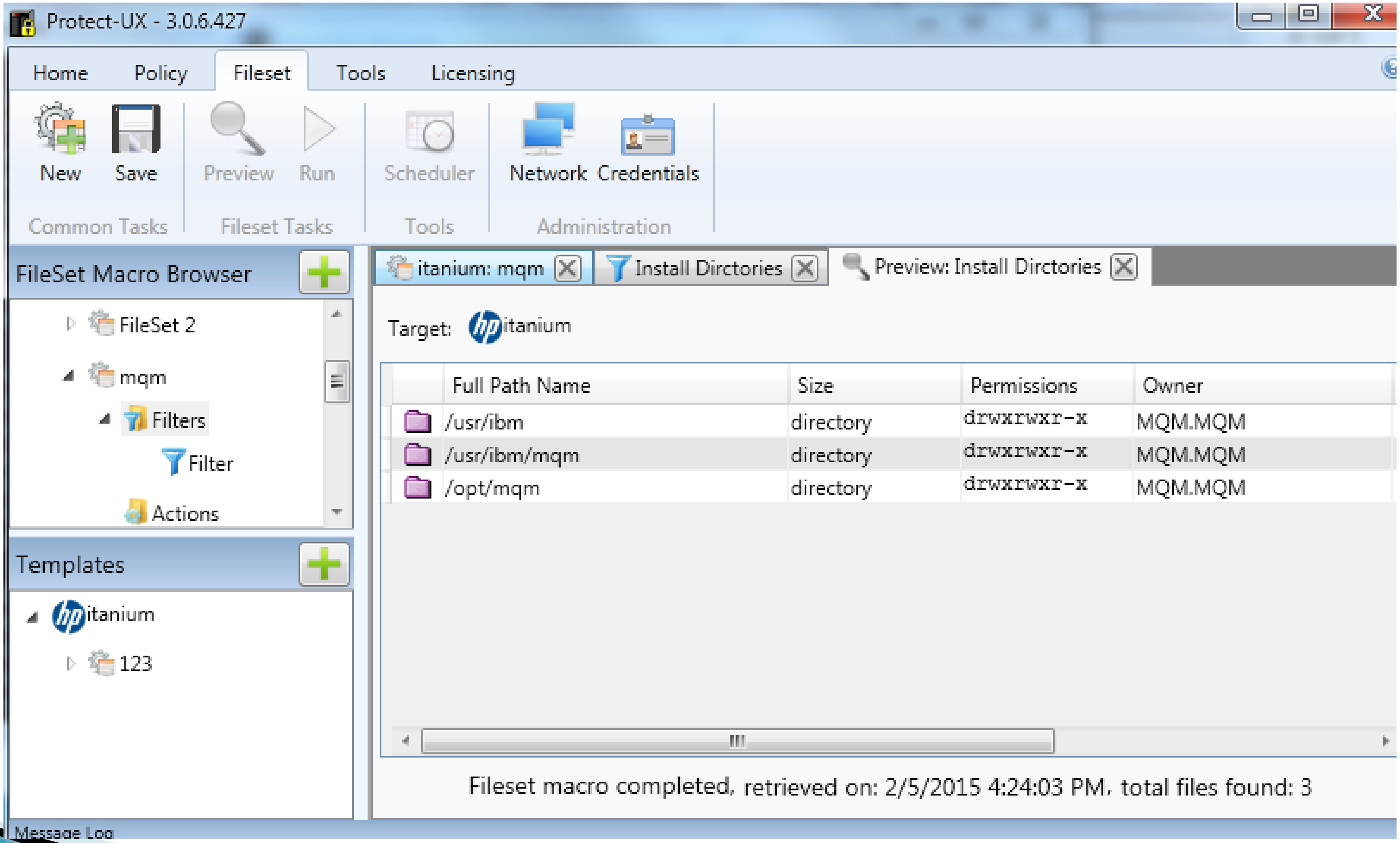
Audit User Action

Pass:

Fail:

ACL count:

Check permissions – Protect-UX



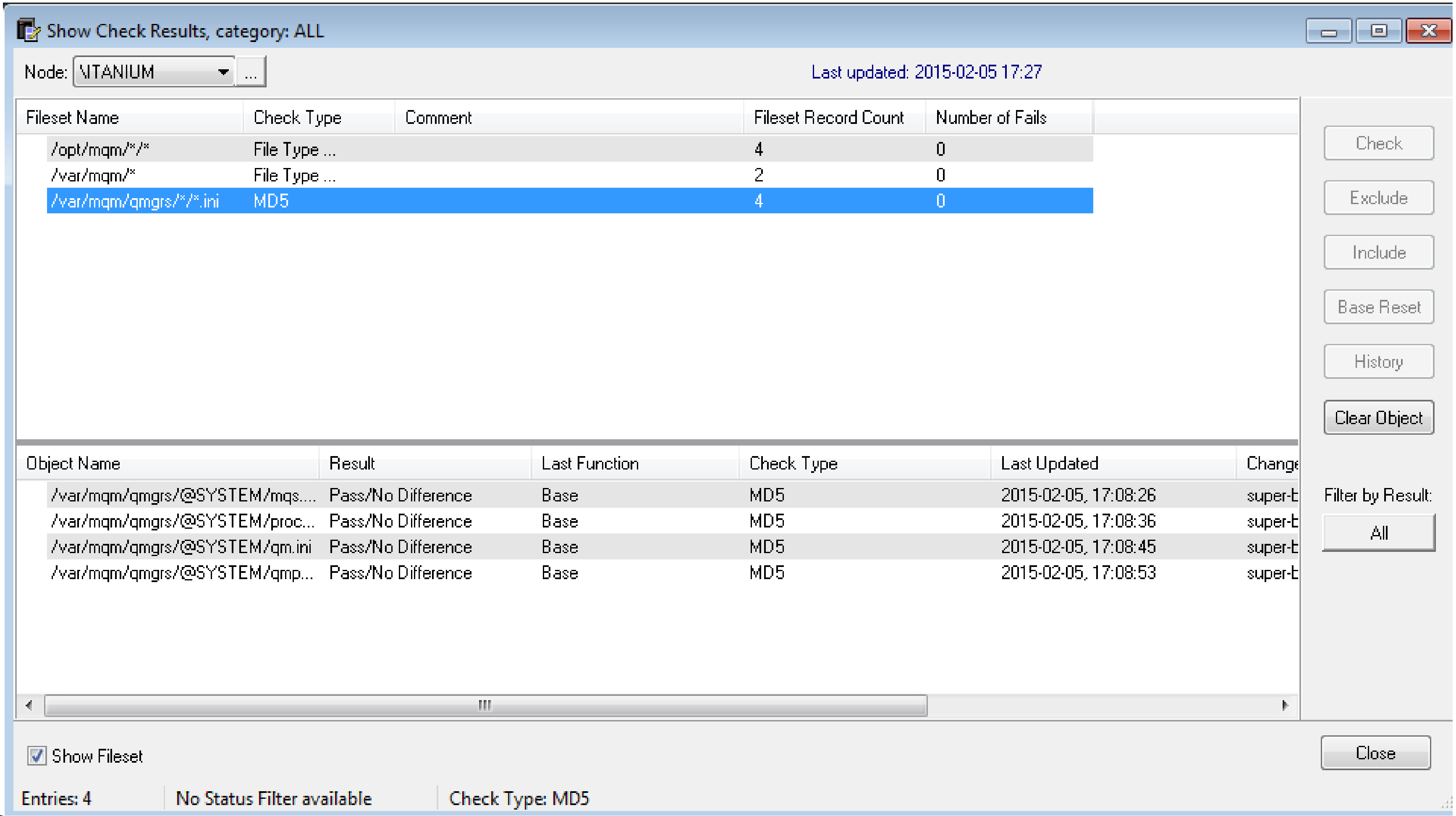
Target: itanium

Full Path Name	Size	Permissions	Owner
/usr/ibm	directory	drwxrwxr-x	MQM.MQM
/usr/ibm/mqm	directory	drwxrwxr-x	MQM.MQM
/opt/mqm	directory	drwxrwxr-x	MQM.MQM

Fileset macro completed, retrieved on: 2/5/2015 4:24:03 PM, total files found: 3

Computer Security Products Inc.

FIC – Create Snapshot



Show Check Results, category: ALL

Node: \ITANIUM

Last updated: 2015-02-05 17:27

Fileset Name	Check Type	Comment	Fileset Record Count	Number of Fails
/opt/mqm/*/*	File Type ...		4	0
/var/mqm/*	File Type ...		2	0
/var/mqm/qmgrs/*/*.ini	MD5		4	0

Object Name	Result	Last Function	Check Type	Last Updated	Change
/var/mqm/qmgrs/@SYSTEM/mqs....	Pass/No Difference	Base	MD5	2015-02-05, 17:08:26	super-b
/var/mqm/qmgrs/@SYSTEM/proc...	Pass/No Difference	Base	MD5	2015-02-05, 17:08:36	super-b
/var/mqm/qmgrs/@SYSTEM/qm.ini	Pass/No Difference	Base	MD5	2015-02-05, 17:08:45	super-b
/var/mqm/qmgrs/@SYSTEM/qmp...	Pass/No Difference	Base	MD5	2015-02-05, 17:08:53	super-b

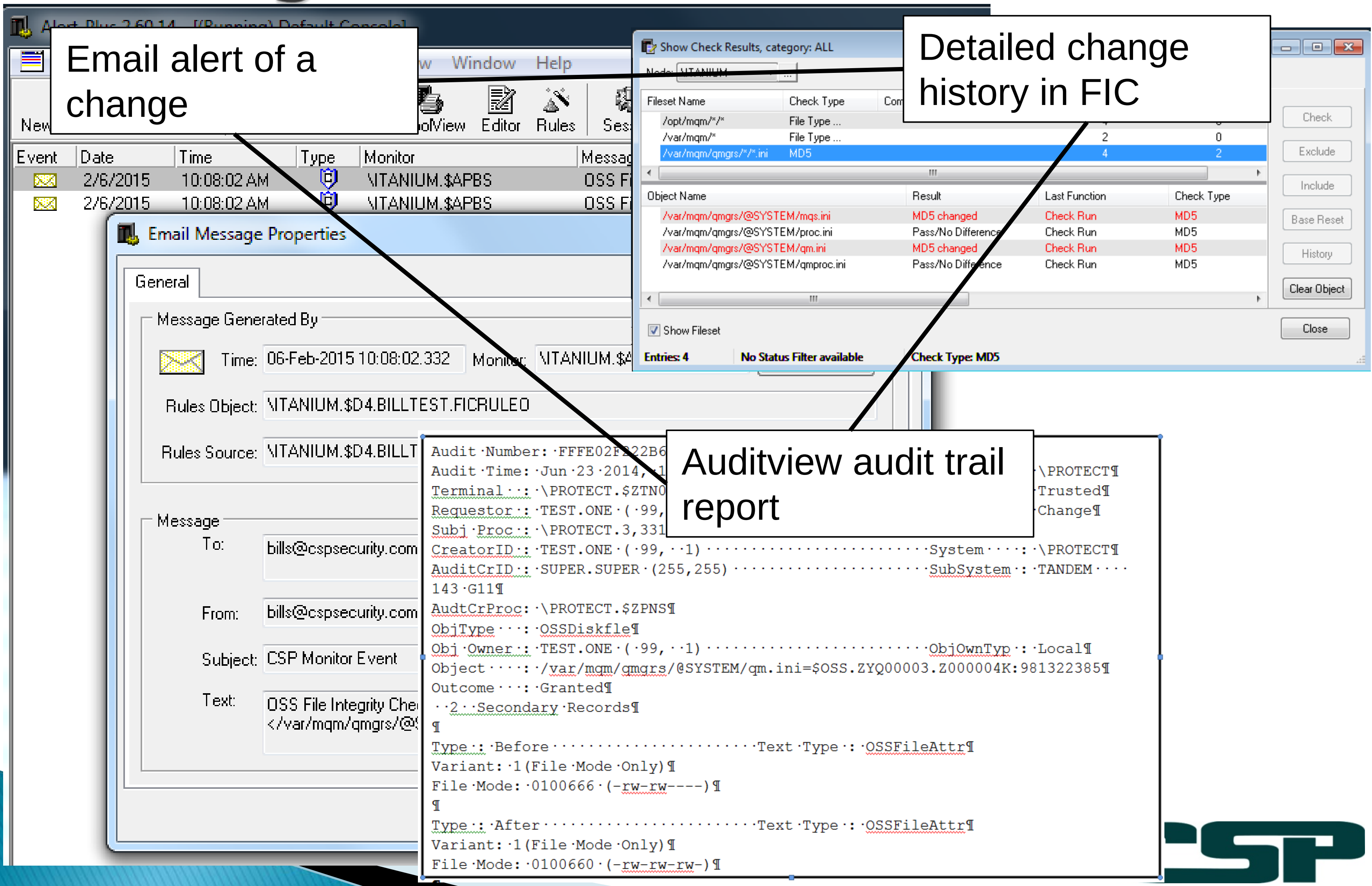
☑ Show Fileset

Filter by Result: All

Entries: 4 | No Status Filter available | Check Type: MD5

Computer Security Products Inc.

Change detection



Email alert of a change

Detailed change history in FIC

Auditview audit trail report

Event	Date	Time	Type	Monitor	Messag
✉	2/6/2015	10:08:02 AM	C	\ITANIUM.$APBS	OSS Fi
✉	2/6/2015	10:08:02 AM	C	\ITANIUM.$APBS	OSS Fi

Message Generated By

Time: 06-Feb-2015 10:08:02.332 Monitor: \ITANIUM.$A

Rules Object: \ITANIUM.$D4.BILLTEST.FICRULE0

Rules Source: \ITANIUM.$D4.BILLT

Message

To: bills@cspsecurity.com

From: bills@cspsecurity.com

Subject: CSP Monitor Event

Text: OSS File Integrity Che
</var/mqm/qmgrs/@S

Fileset Name	Check Type	Com		
/opt/mqm/*/*	File Type ...			
/var/mqm/*	File Type ...		2	0
/var/mqm/qmgrs/*/*.ini	MD5		4	2

Object Name	Result	Last Function	Check Type
/var/mqm/qmgrs/@SYSTEM/mqs.ini	MD5 changed	Check Run	MD5
/var/mqm/qmgrs/@SYSTEM/proc.ini	Pass/No Difference	Check Run	MD5
/var/mqm/qmgrs/@SYSTEM/qm.ini	MD5 changed	Check Run	MD5
/var/mqm/qmgrs/@SYSTEM/qmproc.ini	Pass/No Difference	Check Run	MD5

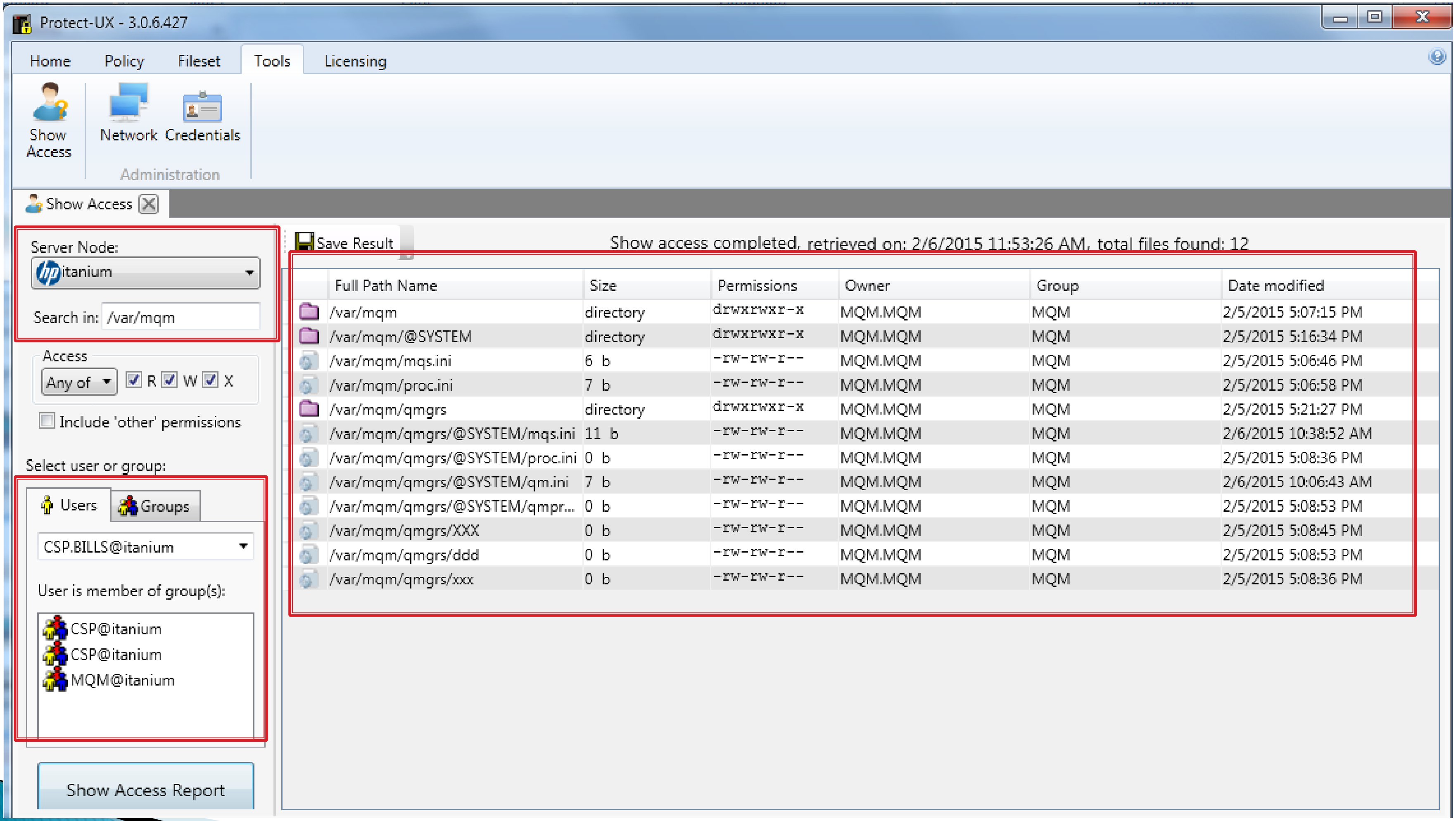
☑ Show Fileset

Entries: 4 **No Status Filter available** **Check Type: MD5**

```
Audit·Number:·FFFE02F222B6
Audit·Time:·Jun·23·2014,·1                                    \PROTECT¶
Terminal··:·\PROTECT.$ZTN0                                    Trusted¶
Requestor·:·TEST.ONE·(·99,                                    Change¶
Subj·Proc·:·\PROTECT.3,331
CreatorID·:·TEST.ONE·(·99,··1)·······················System····:·\PROTECT¶
AuditCrID·:·SUPER.SUPER·(255,255)····················SubSystem·:·TANDEM····
143·G11¶
AudtCrProc:·\PROTECT.$ZPNS¶
ObjType···:·OSSDiskfle¶
Obj·Owner·:·TEST.ONE·(·99,··1)·······················ObjOwnTyp·:·Local¶
Object····:·/var/mqm/qmgrs/@SYSTEM/qm.ini=$OSS.ZYQ00003.Z000004K:981322385¶
Outcome···:·Granted¶
··2··Secondary·Records¶
¶
Type·:·Before·······················Text·Type·:·OSSFileAttr¶
Variant:·1(File·Mode·Only)¶
File·Mode:·0100666·(-rw-rw----)¶
¶
Type·:·After························Text·Type·:·OSSFileAttr¶
Variant:·1(File·Mode·Only)¶
File·Mode:·0100660·(-rw-rw-rw-)¶
```

Computer Security Products Inc.

Verifying the permissions



Server Node: itanium

Search in: /var/mqm

Access: Any of ☑ R ☑ W ☑ X

□ Include 'other' permissions

Select user or group:

CSP.BILLS@itanium

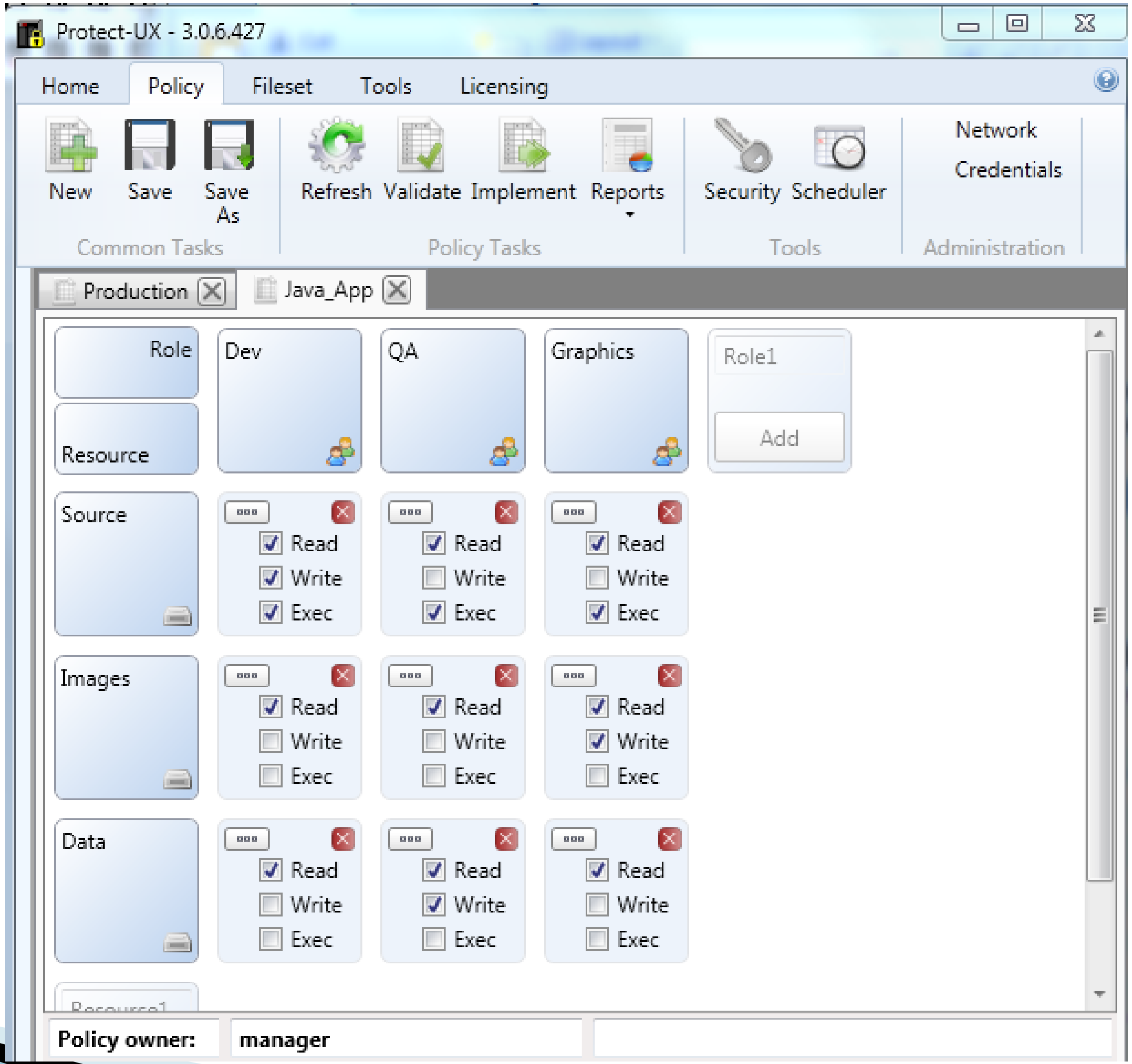
User is member of group(s):

CSP@itanium
CSP@itanium
MQM@itanium

Show access completed, retrieved on: 2/6/2015 11:53:26 AM, total files found: 12

Full Path Name	Size	Permissions	Owner	Group	Date modified
/var/mqm	directory	drwxrwxr-x	MQM.MQM	MQM	2/5/2015 5:07:15 PM
/var/mqm/@SYSTEM	directory	drwxrwxr-x	MQM.MQM	MQM	2/5/2015 5:16:34 PM
/var/mqm/mqs.ini	6 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:06:46 PM
/var/mqm/proc.ini	7 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:06:58 PM
/var/mqm/qmgrs	directory	drwxrwxr-x	MQM.MQM	MQM	2/5/2015 5:21:27 PM
/var/mqm/qmgrs/@SYSTEM/mqs.ini	11 b	-rw-rw-r--	MQM.MQM	MQM	2/6/2015 10:38:52 AM
/var/mqm/qmgrs/@SYSTEM/proc.ini	0 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:08:36 PM
/var/mqm/qmgrs/@SYSTEM/qm.ini	7 b	-rw-rw-r--	MQM.MQM	MQM	2/6/2015 10:06:43 AM
/var/mqm/qmgrs/@SYSTEM/qmpr...	0 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:08:53 PM
/var/mqm/qmgrs/XXX	0 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:08:45 PM
/var/mqm/qmgrs/ddd	0 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:08:53 PM
/var/mqm/qmgrs/xxx	0 b	-rw-rw-r--	MQM.MQM	MQM	2/5/2015 5:08:36 PM

Apply ACLs as needed



Role / Resource	Dev	QA	Graphics	Role1
Source	☑ Read ☑ Write ☑ Exec	☑ Read □ Write ☑ Exec	☑ Read □ Write ☑ Exec	
Images	☑ Read □ Write □ Exec	☑ Read □ Write □ Exec	☑ Read ☑ Write □ Exec	
Data	☑ Read □ Write □ Exec	☑ Read ☑ Write □ Exec	☑ Read □ Write □ Exec	
Resource1				

Policy owner: **manager**

Summary

- OSS application security requires a combination of:
  - System settings (Safeguard, fileset etc.)
  - File permission validation and control
  - Change detection and management
  - Event and audit review
  - Application specifics (e.g. for MQM the internal authorization settings etc.)
- You can do it all with native tools, but...

CSP Solutions deliver:

- Manage and review Safeguard settings easily.
- Apply permission templates from a GUI console.
- Establish baseline and snapshot views of your OSS environment with regular checks.
- Review and verify settings and file attributes as needed.
- Alerts, reports and correlation of OSS events.

2015 enhancements to Protect-UX

- Improved Product Work Flows.
- OSS Command Control.
- Implement an HTML5 based web interface.
- Optional Authorization Streams.

Thank you!

Questions?

Computer Security Products Inc.