COMMON NONSTOP SECURITY HACKS… AND HOW TO AVOID THEM

Greg Swedosh
Knightcraft Technology

Knightcraft Technology
Information Security Specialists

AGENDA

* Introduction
* Getting The Balance Right
* Compliance vs Security
* Gaining unauthorized privileged access
* Alarming the doors! (what you need to do)
* Recommendations

Knightcraft Technology
Information Security Specialists

INTRODUCTION

* Working on HP NonStop systems since 1985
* Consulting in customer environments for 20 years
  - Australia, New Zealand, UK, Singapore, Japan, India Malaysia and the USA.
  - Banks, retailers, telcos, governments.
* HP NonStop Security Specialist
* System and application roles
* Many of the potential vulnerabilities identified here are not new.
  - But I still see them regularly popping up at customers that I visit.

GETTING THE BALANCE RIGHT

* There needs to be a balance between security and usability.
* Secure the system in a practical way.
  - System/Application Support staff must be able to do their job properly.
  - If the system is secured tightly but inappropriately, support staff will need to use privileged userids regularly to perform even the most basic troubleshooting.

HOW MUCH IS BASED ON TRUST?

* Trust should never be the basis of a security paradigm.
* Security auditors hate the word "trust".
* Security Admin should be split away from Sys Admin.

I'M COMPLIANT BUT… AM I SECURE?

- Many organizations seem to believe that if they are passed by an auditor or QSA as compliant with a standard such as PCI DSS, then they are secure.
- Auditors/QSAs are often not experts in HP NonStop security.
- Compliance audits are typically based on a checklist, documentation and on responses from the customer.

NO BACK DOOR HACK OF NSK SYSTEMS?

* Will this still be true as the number of windows into the system grow?
* Are all entry points locked and monitored?
  - Guardian?
  - OSS?
  - TCP/IP?
  - Client application?
  - Web application?

TWO DIFFERENT TYPES OF AUDIT

Compliance

- Tell the auditor as little as possible so that the company passes the audit.
- Answer only the questions that are asked by the auditor.
- Do not volunteer extra information.
- Do not reveal known security gaps.

Security

- A true in depth analysis of all aspects of system security with a view to truly making the system as secure as possible.
- Ask the difficult questions and actively seek the real answers.

Don’t be confused by the two. They have different results.

VULNERABILITY CAUSES

* According to Ernst & Young's Global Information Security Survey 2014*:
  - 38% of vulnerabilities are caused by careless or unaware employees leaving the company exposed
  - 35% are caused by outdated information security controls or architecture
* Top threats include attacks seeking to:
  - Steal financial data
  - Deface or disrupt their organization
  - Steal intellectual property or data

* http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

DISCLAIMER

* The times are always a changing…
  … what's true today, may not be true tomorrow.

* This is not a finite list…
  … it's a starting point identifying some known areas of vulnerability.

* We all need to be constantly learning.

BECOMING A POWERFUL USER

Some simple yet effective ways to become super.super or other privileged userid…

THE SUPER PATHWAY SERVER

* Finding the perfect Pathway…

```
6> status *,prog $system.system.pathmon
Process              Pri PFR %WT Userid  Program file                Hometerm
$SAPP    B  0,27     100     001  83,6   $SYSTEM.SYSTEM.PATHMON      $VHS
$ZVPT       1,24     100     005 255,255 $SYSTEM.SYSTEM.PATHMON      $ZHOME
$JCAT       0,33     100     001  40,30  $SYSTEM.SYSTEM.PATHMON      $VHS
$SAPP       2,41     100     001  83,6   $SYSTEM.SYSTEM.PATHMON      $VHS
$ZVPT    B  0,31     100     001 255,255 $SYSTEM.SYSTEM.PATHMON      $ZHOME
$JCAT    B  3,11     100     001  40,30  $SYSTEM.SYSTEM.PATHMON      $VHS
```

THE SUPER PATHWAY SERVER

* The perfect Pathway...

```
7> pathcom $zvpt
$Z1AQ: PATHCOM - T0845H09 - (01JUL13)
(C)2008-2013 Hewlett Packard Development Company, L.P.=info pathway
PATHWAY
  MAXASSIGNS 50                 [CURRENTLY 7]
  MAXDEFINES 0                  [CURRENTLY 0]
  MAXEXTERNALTCPS 10            [CURRENTLY 0]
  MAXSERVERPROCESSES 100        [CURRENTLY 47]
  MAXTCPS 5                     [CURRENTLY 1]
  MAXTERMS 70                   [CURRENTLY 1]
  MAXTMFRESTARTS 5
  OWNER \SYSA.255,255
  SECURITY "N"
```

THE SUPER PATHWAY SERVER

* Add a new server with the following properties:
  - Program $system.system.scf (or other program of choice)
  - In/Out set to my paused home term
  - Numstatic set to 1
* Start the server
* If the Pathway is owned by powerful userid…
  - The server can do all that that user can do.
* If the Pathway is owned by super.super…
  - The server can probably do anything.

THE SUPER PATHWAY SERVER

* SET PATHWAY SECURITY "O" in all Pathway configuration files.
* SET PATHWAY OWNER to the appropriate owner (preferably not super.super).
* Appropriately secure configuration and startup files.
* Monitor configuration settings to ensure that they have not changed.
* Monitor configuration and startup files to ensure that they have not changed.

AN NSK TROJAN

* If there is no Safeguard protection for $system.system, anybody can create a file there.
  - e.g. create a TACL macro called $SYSTEM.SYSTEM.STATSU or $SYSTEM.SYSTEM.FIELS (or any other commonly misspelt command)

AN NSK TROJAN

* If the user enters STATSU, they just see this…

```
1> STATSU *,USER
STATSU *,USER
^
*ERROR* Name of variable, builtin, or file needed
2>
```

* It looks normal to the user, but anything could be happening in background.

AN NSK TROJAN

* The STATSU macro
  - Provides expected output displayed to the user.
  - Has whatever the user chooses running in the background.
  - Can check userid of executor to ensure that it runs only as super.super or other specified userid.
  - If the command is invoked by super.super, the command can likely do pretty much anything.

AN NSK TROJAN

* Make sure that all subvolumes in the pmsearchlist are Safeguard protected against unauthorized file creation.
* To find all relevant subvols…

```
8> #pmsearchlist

#pmsearchlist expanded to:

#DEFAULTS $APP1.UTIL $SYSTEM.SYSTEM $OPS.TOOLS $OPS.UTIL
```

* While you're at it…
  - Check your TACLLOCL file. Who can modify it?

NSK VIRUS ATTACK

* If a user has write access to object code…
  - Bind in a library file.
  - Perform check of initiator and security first.
  - Perform whatever malicious activity they choose.
  - Bind to another object to replicate.

* Ensure that all object code subvolumes are appropriately Safeguard protected.
* Ensure system and application objects are monitored for any changes.

A ROGUE NAMED CMON

* If there is no $CMON process…
  - A user can start their own.
  - It can intercept commands from TACL and do whatever the user wants it to do.
  - Code available freely in the TUGLIB as a starter.

A ROGUE NAMED CMON

* If you don't run a CMON, protect the process name $CMON with a Safeguard process record.
* Ensure that Safeguards CMON parameters are appropriately configured.
* If you are running CMON, make sure that the CMON code is appropriately secured.

THE EASIEST DENIAL OF SERVICE

* Authenticate-Fail-Freeze set to ON
  - If a user attempts to logon to super.super incorrectly <max-failed-attempts> times, super.super is frozen.
  - If a user does likewise for super.super's owner (security.admin, security.manager…), super.super is perhaps now unattainable.
  - The system disk will need to be rebuilt with a new userid file to regain super.super.

THE EASIEST DENIAL OF SERVICE

* Check Safeguard global configuration…

```
9> safecom
SAFEGUARD COMMAND INTERPRETER - T9750H05 - (22JAN2014) SYSTEM \SYS
=info safeguard

  AUTHENTICATE-MAXIMUM-ATTEMPTS =      3
  AUTHENTICATE-FAIL-TIMEOUT     =     30 MINUTES
  AUTHENTICATE-FAIL-FREEZE      =     ON
```

* Alter safeguard, authenticate-fail-freeze OFF

THIRD PARTY SECURITY SOFTWARE

* Many organizations use third party security software (comForte, XYGATE, CSP, Greenhouse etc.)
* Privileged functionality related to:
  - Authentication
  - Authorization
  - Access

THIRD PARTY SECURITY SOFTWARE

* Third party security software owner userids MUST be treated with the same regard as super.super, because they are the same!
* Control and audit the owner userid for all use.
* Monitor configuration files for any changes.

XYGATE ACCESS CONTROL (XAC)

- Many organizations use XAC to provide command line security and controlled elevated privileges.
- If not secured and configured appropriately, XAC can provide easy access to becoming a privileged userid.
  - OPENSBYOBJECT *.*.*
  - XAC_RUN_MACRO
    - Break key?
    - Does it exit the macro properly under all conditions?

SAFEGUARD OBJECTTYPES

* Safeguard objecttype records specify which userids can add (create) records for the various Safeguard objecttypes.
* If there is no objecttype record, any user can add a Safeguard record for that entity.
  - Add subvol $data.test
  - Add diskfile-pattern

SAFEGUARD OBJECTTYPES

- Protect objecttypes.
- Ensure that only authorized userids (security administrator, super.super [maybe]) can create Safeguard records.
- While you're at it…
  - Make sure that you have also set up all appropriate Safeguard Security Administrative Groups
  - Make sure that your Safeguard records are owned by the appropriate userid.

NETBATCH

* Netbatch typically runs jobs as super.super and the core application userid.
* If Netbatch “in files” are not secured appropriately, a user could modify to do whatever they want.

NETBATCH

* Ensure that there is a consistent use of infile locations for Netbatch jobs.
* Ensure that all infiles are secured so that they can only be modified by authorized users.
* Make sure that the authorized users can only update as part of an authorized activity.
* Question who is actually authorized and why.

KERNEL MANAGED PROCESSES

* Processes that are configured in SCF to run under the control of the $ZZKRN process.
* Started by the system.
* Often using config files (e.g. SSL config)
  * Are the config files appropriately secured?
  * If not, a user could swap/modify the config file that is run (often as super.super) on system startup.

PROTECTING YOUR NSK SYSTEM WITH MICROSOFT SOFTWARE

* The system console is the most powerful entry point into an NSK system.
* Do you use shared userids to access the console?
  - If a user does not logoff from a console TACL session, the session may stay there indefinitely, until the next user comes along.
  - Being the console, the logged on user will probably be a SUPER user.

PROTECTING YOUR NSK SYSTEM WITH MICROSOFT SOFTWARE

* The console oftens falls outside the standard Windows machine management.
  - Are they regularly patched with Windows updates, antimalware updates etc.
  - Are they physically secure?
  - See the HP Console Security guide
  - With the new consoles, if the Halted System Services files are not present, the system will not boot. How well protected are these files?

WE HAVE A FAILURE TO COMMUNICATE

* Default services for TCP/IP are ftp, echo and finger.
  - What can I find out about your system via the network?
  - Can I deny real service by using these services excessively?
  - Can I "pull down" information I shouldn't?

WE HAVE A FAILURE TO COMMUNICATE

* Do you want other network users to know this information?

```
C:> finger @20.3.12.11

[20.3.12.11]
Checking Processors..
  Grp    User        Program              TTY              Process   Pid
APPL.JOE          $SYSTEM.SYS04.TACL    $X1LX.#IN          $X1LY  2,193
SECURITY.BILL     $SYSTEM.SYS04.TACL    $Z9TN.#IN          $Z9TP  2, 63
USER.FRED         $SYSTEM.SYS04.TACL    $Y6ZM.#IN          $Y6ZN  0, 63
PATHWAY.ADMIN     $SYSTEM.SYS04.TACL    $Z0ZX.#IN          $Z0ZY  2,154
SUPER.SUPER       $SYSTEM.SYS04.TACL    $ZTNP0.#PT9UFMA    $X1M6  0,125
SUPER.SUPER       $SYSTEM.SYS04.TACL    $X1LL.#IN          $X1LM  2,196

C:>
```

WE HAVE A FAILURE TO COMMUNICATE

* Check the PORTCONF file…

```
13> fup copy $system.ztcpip.portconf
#
# This file tells the listner program which ports to
# listen to, and what programs to run
# To run the listner use:
#       $system.ztcpip.listner / name.../ [config-file-name]
#  where config-file-name is this file.
#
ftp     $system.ztcpip.ftpserv
finger  $system.ztcpip.fingserv
7    $system.ztcpip.echoserv
phiwsock     $DSMSCM.ZDSMSCM.PDPEXE
```

* Delete the entries that you don’t need.

SNIFFING OUT PASSWORDS

* If sessions aren't encrypted?
  - I can see everything you enter with a LAN sniffer.
  - Aaah! That's what your password is.
  - SCF TRACE will do the same job.

SNIFFING OUT PASSWORDS

* Use end to end session encryption to protect passwords and data traveling around your network.
* SSL, SSH and SFTP all come for free with the operating system. Use them.

AUDIT REPORTING
THE NEEDLE IN THE HAYSTACK

* Are there too many reports to digest?
* Do you get the information that you need?
* Do the reporting tools do the job properly?
  - Logon, changeuser, verifyuser, privlogon?
  - Are audit pool changes detected?
* By the time you get the reports, is it too late?

AUDIT REPORTING
THE NEEDLE IN THE HAYSTACK

* Use exception reporting i.e. reports should contain no entries if everything is normal.
* Run reports regularly.
* Real time alerting is more proactive.
* Where possible use a SIEM device for centralized logging.

AUDIT REPORTING
THE NEEDLE IN THE HAYSTACK

* The bare minimum of Safeguard reports:
  - Safeguard configuration modifications.
  - Super.* user logon attempts.
  - Security administrator logon attempts.
  - Application owner logon attempts.
  - Failed logon attempts.
  - Safeguard ACL modifications/additions.
  - Safeguard Audit Pool modifications.
  - Userid configuration changes.
* Make sure that appropriate audit parameters are set

MAKE EACH INDIVIDUAL ACCOUNTABLE

* Each userid should be owned by one individual.
* Shared userids should only be accessible after logging on first to an individual userid.
* Don’t use aliases for shared underlying userids.
* Procedures should be in place to minimize and control the use of shared userids.
* Use of privileged userids should be fully audited and reports should be analyzed.

IT'S ONLY A DEVELOPMENT MACHINE!

* Looser grip on passwords?
* Wider use of super.super?
* Less change control?
* No audit reporting?
* Remote access to live systems?
* Same passwords on live as dev?

IT'S ONLY A DEVELOPMENT MACHINE!

* Your Dev systems can provide the key to the back door of your Live systems.
  - Keep them under control.
  - Monitor what's going on.
    - If a user turns encryption OFF on the userid file, is there a mechanism to catch them?
    - Do you have the same password on the Live system as you do on Dev?
* Do not automatically provide remote passwords for all userids. Question all remotes. Are they really needed?

THE TROUBLE WITH ALIASES

* The file system knows nothing about them.
* All users to the system should have their own default subvol (cstm files – tacl, scf, fup, ftp etc.)
* However, any user with an alias with the same underlying userid will (typically) be able to modify any of these user specific files.
* Commands could then potentially be set up to be invoked by somebody else when they logon as their super.super alias.

PROGID PROGRAMS

* It seems obvious that you don't have a ProgID version of a utility such as SCF or FUP or SQLCI on the system without appropriate access control.
* But it happens.
* Regularly review ProgID programs and their security.

GUARDIAN IS NOT A VERY GOOD GUARDIAN

* While a system can be secured with Guardian, it is limited in its capabilities
* Many organizations have a mix of Guardian and Safeguard.
* Without Safeguard protection there is no auditing.

* Use Safeguard for everything.
  - Set volume ACLs denying access to all but super.super and have CHECK-VOLUME set ON.
  - Ensure that you know what is really going on on the system.

SESSION ENCRYPTION

* It's all very well to use session encryption but make sure that you use strong cipher suites.
* SSL 3.0 is now vulnerable. Use TLS.
* Stay abreast of the latest developments in encryption. Vulnerabilities are periodically detected.
* Todays strong "unbreakable" encryption will likely be breakable soon.
* Know all spots where encryption is required in the organization:
  - User sessions (TACL, OSH etc.)
  - File transfer (SFTP, FTPS,XCOM)
  - Application (ATMs, POS devices, iTP webserver etc .)
  - System Console
  - Expand

THE PROBLEM WITH SESSION TRACKING SOFTWARE

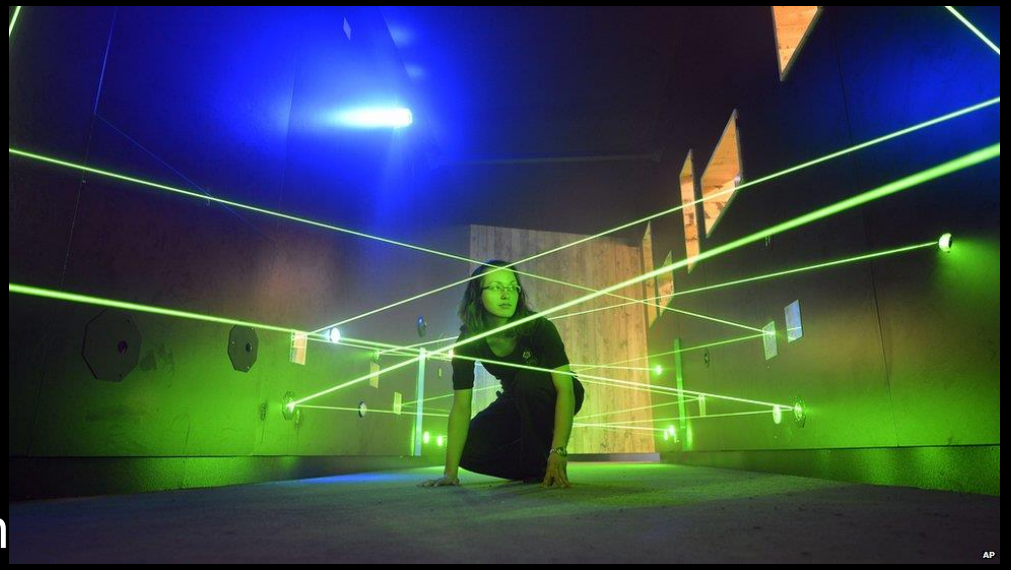
* Various products are available for tracking user sessions (i.e. keystroke auditing) on the NonStop, available from HP and various security partners.
  - Do they track everything a user does?
  - ALL SESSION TRACKING SOFTWARE ON THE NONSTOP CAN BE CIRCUMVENTED FROM TACL!!!
* Even so… you should have session capture.
  - Is it on all user sessions (all except $YMIOP.#CLCI)?
  - Most users will not circumvent with this method so it will capture most stuff.
  - Critical component of multi-layered monitoring approach.

SETTING THE ALARMS

* Perform File Integrity Monitoring (change detection) continuously.
  - Weekly is not enough.
  - Real time monitoring is the optimum.
* Use a multilayered auditing approach. Don’t just rely on one method.
  - Use all software you have to its capacity.
  - And make sure you have everything you need.
  - Don’t cut corners.

SETTING THE ALARMS

* Use a multilayered monitoring approach
  - Safeguard auditing
  - Process Monitoring
  - Session tracking
  - Regular reporting
  - SIEM based monitoring & alerting
  - Data Discovery Tools
  - Real time change detection on files and configuration

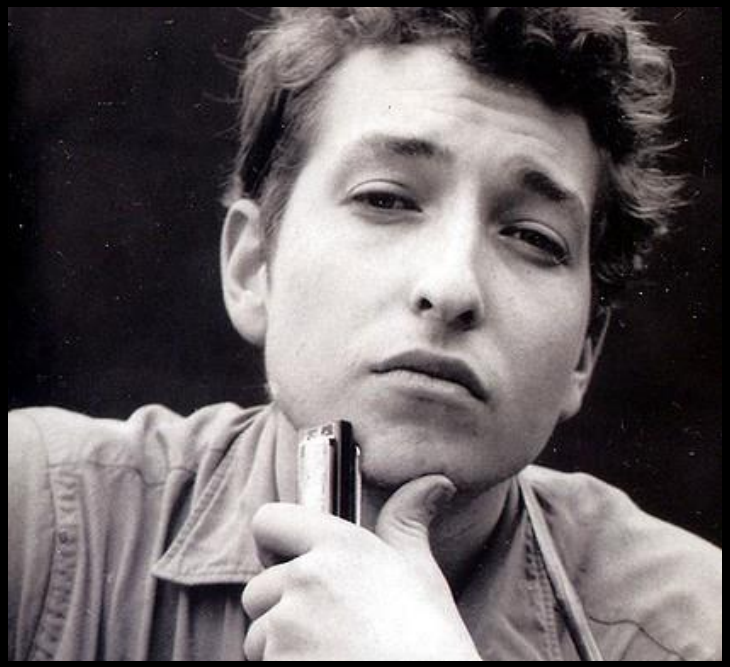


SETTING THE ALARMS

* Use file integrity monitoring (FIM) and auditing for all critical files/subvols and key configuration items
  - Operating system files ($system.system, $system.sysnn)
  - Safeguard configuration
  - Any other security related configuration
  - System and subsystem Startup/Shutdown files
  - Privileged userid CSTM files
  - Files on pmsearchlists
  - Application related files (objects, config, startup)
  - Pathway server configuration
  - TCP/IP process listens
  - SCF configuration (comms, kernel managed processes)
  - Spooler configuration
  - Netbatch related files

THE TIMES THEY ARE A CHANGIN’

* Things change over time.
  - New applications
  - New procedures
  - New requirements
* Documentation doesn’t get done.
* People leave.
* Knowledge of why or how something is done gets lost.



THE TIMES THEY ARE A CHANGIN'

* Review your security setup regularly.
* Review your security procedures regularly.
* Keep abreast of product changes and technological updates.
* Perform regular system security audits.
* Think about how YOU would hack in.
* Bring in a fresh set of eyes to assist.

THE TIMES THEY ARE A CHANGIN’

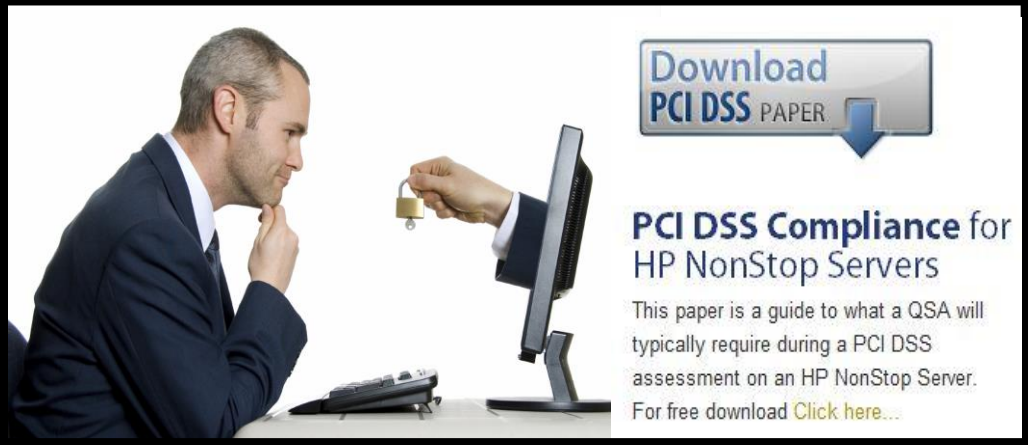
Just because we were secure yesterday…

doesn’t mean that we are secure today.

Let alone tomorrow.

RESOURCES

* NonStop Security Hardening Guide White Paper (HP NonStop Technical Library)
* *PCI DSS Compliance for HP NonStop Servers* – Technical white paper available for free download from ww.knightcraft.com



STEPS TO SECURITY AND COMPLIANCE

Knightcraft Technology
Information Security Specialists

Security Review Service

* A thorough investigation of all security aspects of your NonStop system.

PCI DSS Consultancy

* Help to achieve and maintain compliance in a fast, reliable and cost-effective manner as well as ensuring that your systems are truly secure.

Security Implementation Service

* Configuration of HP NonStop security subsystems in line with best practices.
  - Experts in Safeguard, OSS, XYGATE, SSH, other third party software.

Knightcraft services performed in partnership with com.forte

Email: greg.swedosh@knightcraft.com Website: www.knightcraft.com

Talk to your com.forte representative

STEPS TO SECURITY AND COMPLIANCE

Integrity Detective

* Real time monitoring of changes to files
  - File Integrity Monitoring of Guardian and OSS files.
* Real time monitoring of subsystem configurations
  - Safeguard, Netbatch, Pathway, SCF processes etc.
* Ensures that what you think is running on your system is what is actually running.
* Ensures that what you think is configured on your system is what is actually configured.
* Fully audited, comprehensive reporting.
* Events sent "off box" to corporate SIEM.

* www.4techSoftware.com for details

Knightcraft Technology

Information Security Specialists

QUESTIONS???