OpenVMS Sicherheit und Monitoring mit System Detective

pointsecure
Security and Auditing for OpenVMS

3G01: Regelbasiertes Monitoring von OpenVMS Alpha und IA64
John R. Covert
DECUS-München 19. April 2007 Nürnberg

Einführung

- $2 Mio Sicherheitsverlüste in den USA pro Jahr wegen Worms, Viren, u.A.
  -*Secure Enterprise Magazine*
- Die Verlüste sind noch größer in den Global 5000 Firmen.
- VMS ist sehr sicher, aber fahrlässiges Benehmen von Benuztern führt trotzdem zu Sicherheitslücken.

pointsecure

Benutzer: a necessary evil

- Vorgänge, die absichtlich oder unabsichtlich zu Störungen führen
- Unbefugtes suchen nach Daten die nicht richtig gesichert sind.
- Einbruch in Systemen wegen mangelhafter Zugangssicherheit
- Social Engineering: Einbruch durch Betrug und Lüge.

pointsecure

System Detective

- Sicherheit und Auditing
- Echtzeitwarnungen bzw. -ausloggen bei Policy-Anstoß
- Logging gemäß Reg-Bestimmungen
- Gleichzeitiges Mitschauen und ggf. Mittippen auf VMS Terminals
- Monitoring von inaktiven Terminals
- Log review

pointsecure

Regel-basiertes Monitoring

- Die Parameter des Monitoring wird für jedes System, bzw. Clusterwide in einer Konfigurations-Datei definiert.
  - [Selector] : Eigenschaften des Processes
  - [Trigger] : Events, die sicherheitswichtig sind
    - Time : Uhrzeit/Tag wann ein Event wichtig ist
    - Qualifier : priority, privilege, port
  - [Action] : Was passiert wenn der Trigger los geht

pointsecure

Regel-basiertes Monitoring

- Process-Entdeckung: Wir bauen für jeden Process eine ProcessRulesTabelle wobei wir aktivieren für diesen Process die Regel, und nur die, deren „SELECT“-Sätze treffenden Objekte haben:
  - [no]username
  - [no]identifier
  - [no]uic_group
  - [no]captive

Die Zeit-Qualifiers an den „Trigger“-Sätzen sind by Process-Entdeckung analysiert. Die ProcessRulesTabelle wird zum richtigen Zeitpunkt wiederaufgebaut.

pointsecure

Triggers

- Die Events, die eine Aktion triggern, sind
  - Image
  - File
  - Login
  - Idle
  - Image_exit
  - Exclude (syntax element, nicht Event. Die „Selected“ Objekte von den folgenden Regeln, bis [End_of_Section], sind ignoriert.

pointsecure

Triggers (2)

- Erklärung kaum erförderlich:
  - Image (Aktivierung)
  - Login (Job)
  - Image_exit

pointsecure

Triggers (3)

- File xyz
  - Objekt ist IDENTIFIER, nicht File Name.
  - Set File /ACL=(ID=xyz,ACC=RWCD)
  - Trigger feuert bei Zugang zur Datei mit einem oder mehreren von den Access Modes
  - Für Performance: Die IDs in einem separaten Nummernfolge von anderen IDs wählen.

pointsecure

Triggers (4)

- Idle minutes
  - Trigger feuert beim Auslauf der angegebenen Anzahl von Minuten. Zehn oder mehr „Gebrauchseinheiten“ in einer Minute setzt die Idlezeit auf null zurück.
  - Gebrauchseinheit:
    - 1/100 Sekunde CPU Zeit
    - 1 Direct I/O
    - 1 Buffered I/O
  - Mehrere Idle Triggers erlaubt; sortiert.

pointsecure

Actions

- Die möglichen Aktionen sind:
  - Delete
  - Forcex
  - Nolog
  - Temp_log
  - Perm_log
  - Ignore
  - Force_event
  - Lock_keyboard
  - Manager_Lock
- Die Sekondären Aktionen sind
  - Opcom
  - Command (batch)
  - Notify
- 0/1 Aktionen, Eventlog database
- 0-3 Sek. Aktionen, Option: Eventlog

pointsecure

Actions (2)

- Einfach:
  - Delete (Forcex+Delete)
  - Forcex
  - Force_Event (Logeintrag zum Event Log)
  - Ignore (keine weitere Interesse)
  - Lock_Keyboard (bei IDLE)
    - ^B + Passwort zu Unlock
    - n.b. Benutzer kann auch selber mit ^B sein eigenes Keyboard locken (^char konfigurierbar)
  - Manager_Lock

pointsecure

Actions (3)

- Terminal logging
  - Temp_Log – Output geht zum Session Log
  - Nolog – Stop
  - Perm_log – Session Log, unstoppbar
- n.b. Advise funktion (mehr später) benutzt auch den Session Log
- künftig: Events sind auch zum Session Log geschrieben

pointsecure

Secondary Actions

- Opcom=(Central,Security) Ludwig hat den Schloß verlassen!
- Notify Sie haben in den letzten 20 Minuten nichts getan. Zurück an die Arbeit!
- Command/user/nolog = reply/user=covert „Diese Datei sollst Du nicht anschauen!“
- Command kann auch eine DCL-Datei aufrufen
  - User/System ... neu: /User=name

pointsecure

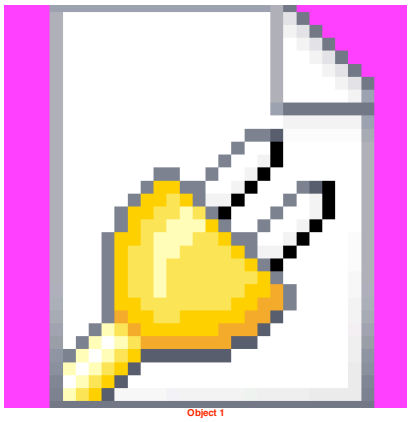
Secondary Action, DCL Datei

- Command = @sendmail „Trouble“ harry,charlie „The cat's out of the bag“

```
$ time = f$getqui("display_entry","submission_time",,"this_job")
$ pipe (write sys$output "Time: "time"" ; -
        write sys$output "Node: "openv$sd_nodename"" ; -
        write sys$output "Username: "openv$sd_username"" ; -
        write sys$output "PID: "openv$sd_epid"" ; -
        write sys$output "Message: "message' "P3"" ) | -  ! P3 is add'l text
 mail /subject=""P1'-"time'-"openv$sd_nodename'-"openv$sd_username"'-
        sys$pipe ""P2"" ! P2 is the mail distribution list
```

pointsecure

Config File



pointsecure

Sysdet Commands

Start / Stop System Detective

Analyse der Event und Session Logs

Advise

Lock

advise
directory
format
initialize
lock/unlock
merge
playback
report
review
show
start
stop
73playback
73report

pointsecure

Advise

- Realtime anschauen auf ein anderes Bildschirm, ggf. auch Eingabe.
- Wer darf was:
  - System Manger vergibt IDs:
    - OPENV$SD_V_xxxx erlaubt View auf p mit xxxx
    - OPENV$SD_I_yyy erlaubt Eingabe zu p mit yyy
  - Benutzer ladet ein (bzw. aus):
    - SYSDET ADVISE/ALLOW=[VIEW|INPUT] xxxx
    - SYSDET ADVISE/ALLOW=[NOVIE|NOIN] xxxx
      - neu: Benutzereinladung konfigurierbar System/ProUser

pointsecure

Advise (2)

- SHOW USER COVERT/FULL

```
Username Process Name    PID     Terminal
COVERT   BATCH_618      00053B33  (Batch)
COVERT   COVERT         000F131D  VTA1372: TNA1373:
                                  (Host: g3.covert.org Port: 62984)
COVERT   John Covert    001C0A56  VTA1368: TNA1369:
                                  (Host: g3.covert.org Port: 58534)
COVERT   Me Too         00000132  VTA2:    TNA1367:
                                  (Host: g3.covert.org Port: 58462)
```

- SYSDET ADVISE 001C0A56
- ^B beendet.

pointsecure

Manager Lock

- Event verursacht Manager Lock
- oder DCL-Command
  - sysdet lock pid
  - sysdet unlock pid
  - sysdet lock 0 ist nur Benutzer lock
- Wer darf was, an wem: Sysmgr vergibt IDs
  - OPENV$SD_L_xxxx erlaubt Lock auf p mit xxxx
  - OPENV$SD_U_yyy erlaubt Unlock auf p mit yyy

pointsecure

Reports

- Report command hat einen Haufen switches für Searchen und Drücken von Reports.
- Review scrollt durch Session Logs, viele Such- und andere Optionen.
- künftig: „Pending“ -- markieren von Session Logs als reviewed oder nicht.

pointsecure

Weitere Infos

- OpenVMS Technical Journal V5, Feb 2005: „Taking OpenVMS Security One Step Further“, Seiten 79-86

  http://h71000.www7.hp.com/openvms/journal/v5/openvms_journal.pdf

- PointSecure Website

  http://www.pointsecure.com/

pointsecure

John R. Covert
2 Flagg Road
Acton, Massachusetts 01720
covert@covert.org
+1 978 263-5433
(030) 8687 0 9350

pointsecure

```
!       OPENV$SD_CONFIG.DAT / OPENV$SD_CONFIG.TEMPLATE
!
! (c) Copyright 2005 BBS Technologies, Inc.
! All Rights Reserved
!
! This is the template configuration file used
! by System Detective.  The template for
! this file will be replaced during upgrades.
! After initial installation copy the template
! to OPENV$SD_CONFIG.DAT.  Modify this DAT file
! for site specific needs.  On upgrades examine
! the new template file to determine if changes
! are required.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
! This section contains System Detective general
! configuration statements.
!
! Set the default log file specification here and then
! set any special log file specifications for indivuduals
! or groups.
!

[log_default] openv$root:[sd.log]username_datetime_epid.sessionlog_nodename

!
! This specifies the user names of users who are allowed
! to shut down System Detective.  If no users are
! listed any privileged user may shut down System Detective.
! To prevent System Detective from being shut down except
! during system shutdown use the single user openv$nouser.
!

[shutdown_users] system,warren,james, john, windy

!
! This specifies a different location for the message file.
! The example below is commented out but it specifies the
! standard message file.
!

![message_file] OPENV$ROOT:[SD]OPENV$SD_MESSAGE.DAT

!
! Session Log files may be encrypted by uncommenting the following:
!

![log_encrypt]

!
```

```
! User invoked session locking may be enabled by commenting out
! the following line.  When enabled, any user may lock his own
! session by entering the session locking attention character
! which, by default, is control-B.  The user then has the option
! of locking his session or repeating the session locking
! attention character to have it sent to the current application.
! If the user locks his session, the lock is similar to the
! session lock imposed by use of the session idle time lock.
! The user may unlock his session by entering the same
! session locking attention character and then, when prompted,
! entering his VMS password.

[SESSION_LOCK] OFF


! The user authorized use of the SYSDET ADVISE command provides
! a powerful tool for the user along with a possibility of misuse.
! The system manager should consider whether the security policy
! is system high.  If all users are cleared for all the
! information in the system, have a need to know, and the
! training to properly use this feature, it may be reenabled
! by commenting out the following two lines.

[NO_USER_ADVISE]
[NO_USER_INPUT]

!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
! This section begins a set of rules that may
! be used as an example.  These rules should be
! reconfigured to meet the site security plan
! in effect at the site.
!
[Start_of_Section]
! All users see this message upon login and whenever System Detective
starts.
! The “~” suppresses the usual System Detective header with time and date
! before this particular message.
[Selector] Username *
        [trigger] Login
        [action] notify = ~System Detective is monitoring activity on this
system.

[End_of_Section]


[Start_of_Section]
! At this site the backup accounts are privileged and carefully restricted.
! Backups are done in batch and over the network and the procedures are
```

```
! carefully protected.  With those protections in place, it was determined
! that there was no need to monitor the backup processes.
! Processes should be ignored with great caution due to the complete
! exemption it grants to the process.  The small overhead incurred in
! monitoring should be carefully balanced against the benefits of
monitoring.

[Selector] Username backup,     ! Backup is automated in batch at this
                backup_rem      ! site and performance is critical so
        [Trigger] login         ! it was decided to ignore this
        [Action] Ignore         ! automated process.

[End_of_Section]

[Start_of_Section]              ! This section has to do with logging.
! This section assumes a generic site security policy on logging
! in which access to sensitive images is logged.

[Selector] Username *           ! Log all users running authorize.
        [Trigger] image *sysexe]authorize.exe
        [Action] opcom=(central,security) He is trying  ! and report him
                to run authorize                        ! to the oper &
CISO.
        [Action] notify = You are being logged.
        [Action] temp_log

[Selector] Username *    ! Turn off logging on exiting authorize.
        [Trigger] image_exit *sysexe]authorize.exe
        [Action] notify = Logging stopped.
        [Action] nolog

[Selector] Username warren, james,john, windy
        [Trigger] Exclude       ! Some users are OK with sysgen & sysman.

[Selector] Username *           ! Log users running sysgen.
        [Trigger] image *sysexe]sysgen.exe
        [Trigger] image *sysexe]sysgen.exe
        [Action] opcom=(central,security) He is trying  ! and report him
                to run sysgen                           ! to the oper &
CISO.
        [Action] notify = You are being logged.
        [Action] temp_log

[Selector] Username *    ! Turn off log on exiting sysgen.
        [Trigger] image_exit *sysexe]sysgen.exe
        [Action] notify = Logging stopped.
        [Action] nolog

[Selector] Username *           ! Log users running sysman.
        [Trigger] image *sysexe]sysman.exe
```

```
        [Action] opcom=(central,security) He is trying  ! and report him
                to run sysman                           ! to the oper &
CISO.
        [Action] notify = You are being logged.
        [Action] temp_log

[Selector] Username *    ! Turn off log on exiting sysman.
        [Trigger] image_exit *sysexe]sysman.exe
        [Action] notify = Logging stopped.
        [Action] nolog

[End_of_Section]


[Start_of_Section]      ! Some example logging rules.
! This section assumes a site security policy where some users
! are logged all the time.  This may be appropriate where users
! log in from outside to do privileged work or to support
! purchased software or work in particularly sensitive areas.

[Selector] Username warren, james,john, windy
        [Trigger] Exclude       ! Not needed in this section at this time
                                ! but we usually exlcude these users at
this sit
e.

[Selector] Username field*,     ! Permanently log all the field service users
                app_support     ! and the offsite applications support user
        [Trigger] Login         ! right from the beginning
        [Action] perm_log       ! and tell them about it.
        [Action] notify = You are being logged.

[Selector] Identifier accounting! Permanently log the accounting people
        [Trigger] Login         ! right from the beginning
        [Action] perm_log       ! but do not tell them about it.

[End_of_Section]


[Start_of_Section]      Examples of rules to control access
! This section assumes that the site security policy restricts certain
! users from accessing certain functions.

[Selector] Username warren, james,john, windy
        [Trigger] Exclude       ! We usually exlcude these users at this
site.

[Selector] Username Sam         ! Do not let Sam get in trouble.
        [Trigger] Image *sysexe]sysgen.exe
        [Qualifier] privilege=(cmkrnl,sysprv)
```

```
        [Action] Forcex
        [Action] Notify = Sam, do not run sysgen with privilege.

[Selector] Username Rod         ! Rod is OK for license
        [Trigger] Exclude       ! so exclude from following rules.

[Selector] Username *           ! Catch users trying to generate license
        [Trigger] file license_generator        ! using file w/ ACE in ACL.
        [Action] opcom=(central,security) Unauthorized user is trying
                to generate a license.
        [Action] delete         ! Delete his process!

! In this case we have a series of rules that apply to one user.
! We could have made a separate section but the exclusions in the
! current section do not exclude him so a separate section is not
! needed.  Sometimes separate sections are advisable so as to
! better document the intent of the series of rules  so we
! will not make mistakes next time we modify the rules.
! This user does critical work which should be logged and he
! works only on weekdays.  Note that he can work late, he just
! can not start working after hours.  Keeping the rules that apply
! to a single user or class of users together sometimes makes sense.

[Selector] Username Mumu        ! Do not let Mumu login after hours.
        [Trigger] Login         ! If he loggs in
        [Time] start=0000 end=0700 ! before 7:00 AM
        [Action] delete         ! delete his process.

[Selector] Username Mumu
        [Trigger] Login         ! If he loggs in
        [Time] start=1730 end=2400 ! after 5:30 PM
        [Action] delete         ! delete his process.

[Selector] Username Mumu
        [Trigger] Login         ! If he loggs in
        [Time] weekend          ! on a weekend
        [Action] delete         ! delete his process.

[Selector] Username Mumu
        [Trigger] Login         ! Anytime he logs in
        [Action] Perm_Log       ! always log him.

[End_of_Section]

[Start_of_Section]
! Start a new section here to make sure no users are excluded by accident.

[Selector] NoIdentifier accounting   ! Keep interlopers out of accounting.
        [trigger] file payroll
        [action] delete
```

```
        [Action] opcom=(central,security) interloper in payroll

[End_of_Section]

[Start_of_Section]
! This section includes some example idle rules.  At this site one
! user needs a short idle time and the remainder need a longer time.
! At this site we do not delete any sessions for idle time.

[selector] username fritz       ! Here we specified a specific user
        [trigger] idle 10       ! for a short idle time.
        [action] notify = Idle for 10 minutes - another 10 min to lock.

[selector] username fritz       ! We lock him quickly but
        [trigger] idle 20       ! we never delete him.
        [action] notify = Idle too long - locking keyboard.
        [action] lock_keyboard

[Selector] Username fritz
        [Trigger] Exclude       ! We already handled Fritz.

[selector] username *
        [trigger] idle 30
        [action] notify = Idle for 30 minutes - another 30 min to lock.

[selector] username *
        [trigger] idle 45
        [action] notify = Idle for 45 minutes - another 15 min to lock.

[selector] username *
        [trigger] idle 60
        [action] notify = Idle too long - locking keyboard.
        [action] lock_keyboard

[End_of_Section]

[End_of_File]
```