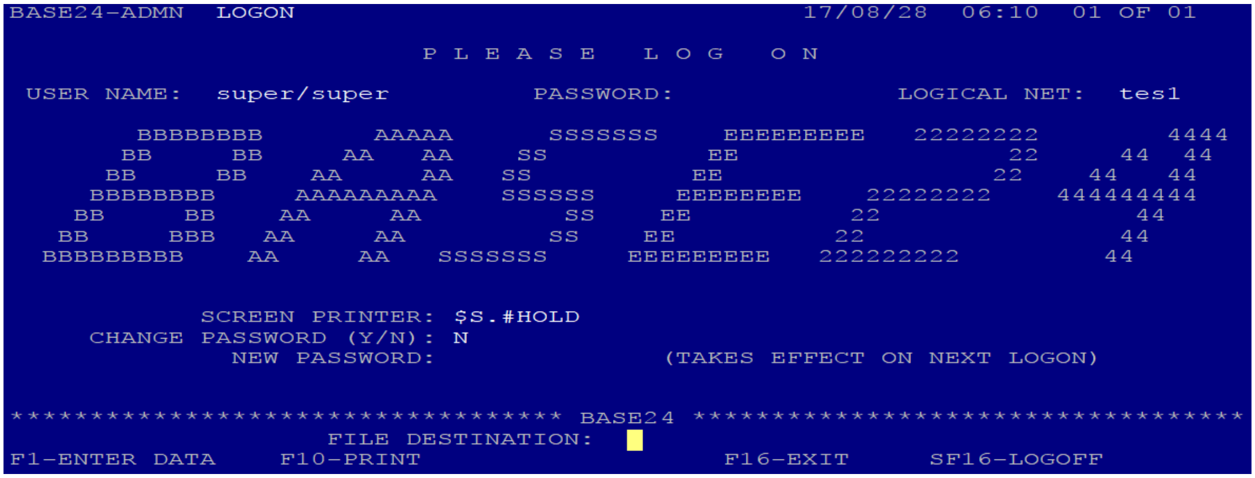
Using the XYGATE Merged Audit (XMA) BASE24 Mover to Collect and Alert OMF Security Audit Events

Dave Teal – XYPRO

BASE24 OMF

The BASE24 Online Maintenance File (OMF) contains audit information about users who have logged on and logged off the BASE24 Pathway system as well as information about users who have accessed or attempted to access (i.e. read, add, delete, update) records in BASE24 files accessed through the BASE24 Pathway system.



```
BASE24-ADMN  LOGON                                17/08/28  06:10  01 OF 01

                          P L E A S E   L O G   O N

 USER NAME:  super/super         PASSWORD:              LOGICAL NET:  tes1

        BBBBBBBB       AAAAA      SSSSSSS    EEEEEEEEE   22222222        4444
       BB     BB     AA   AA    SS          EE                 22   44    44
      BB     BB    AA     AA   SS          EE                 22    44   44
     BBBBBBBB     AAAAAAAAA    SSSSSS     EEEEEEEE    22222222    444444444
    BB     BB    AA     AA         SS    EE          22                44
   BB     BBB   AA     AA         SS    EE          22                44
  BBBBBBBBB    AA     AA   SSSSSSS     EEEEEEEEE   222222222         44


            SCREEN PRINTER: $S.#HOLD
     CHANGE PASSWORD (Y/N): N
              NEW PASSWORD:              (TAKES EFFECT ON NEXT LOGON)


*********************************** BASE24 ***********************************
                    FILE DESTINATION:
F1-ENTER DATA    F10-PRINT                   F16-EXIT     SF16-LOGOFF
```

For reads, a record is only written to the OMF if the record contains cardholder data, such as a Primary Account Number (PAN). In addition, OMF records are written when users attempt to read a record from the file or when a security violation occurs, for example:

- The user does not have security access for the institution (FIID) to which the record belongs.
- The user does not have security access to the file or authority for the function attempted.
- The user does not have authority for the function attempted based on configuration settings in the CRT Authorization Security (CSEC) File.

An OMF record is not written if a user attempts a Read or a Read Next function and the record is not retrieved successfully.

BASE24 provides the means to generate two OMF audit reports:

1. Logon/Logoff Access Report (OMF03)
2. File Access Report (OMF04)

The OMF audit reports include the information from a single day’s OMF file(s), displayed in chronological order.

The OMF-AUDIT parameter in the Logical Network Configuration File (LCONF) affects OMF audit reporting. This parameter controls the amount of information that is written to the OMF and is, therefore, available for reporting.

The OMF-AUDIT parameter has three settings:

- 2 – An OMF record is created when a user adds, updates, or deletes a record in a BASE24 file accessed through Pathway, logs on to Pathway, or logs off Pathway using the SF16 key from the Logon screen. The OMF record that is created when a user adds, updates, or deletes a record includes the following information: application code (file ID), record type, user number, user group, logical network identifier, FIID, region, branch, terminal ID, date, and time. The OMF record that is created when a user logs on, attempts to log on, or logs off includes the following information: user number, user group, logical network identifier, terminal ID, date, and time. The information written to the OMF when the OMF-AUDIT parameter is set to 2 is considered summary information. Therefore, if the OMF-AUDIT parameter is set to 2, only the summary versions of the OMF audit reports can be generated.

- 1 – An OMF record is created the same as when the OMF-AUDIT setting is 2, but in addition to the data listed above, images of the record are added. In the case of an updated record, a before and after image of the updated record is added to the OMF. In the case of a failed logon attempt, information on the reason for the failure is also included. The information written to the OMF when the OMF-AUDIT parameter is set to 1 is considered detail information. Therefore, if the OMF-AUDIT parameter is set to 1, either the summary or detail versions of the OMF audit reports can be generated. In the detail version of the report, the summary information for each record is followed by the image of each record.

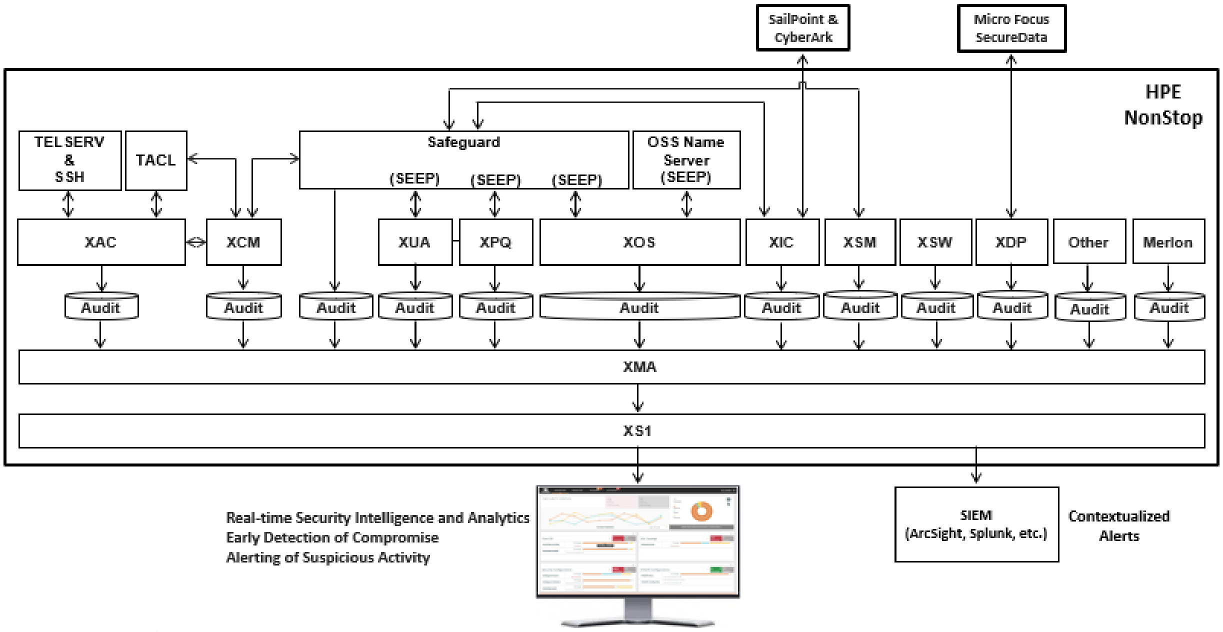
- 0 – No information is written to the OMF. No information is available for reporting.

The OMF is created daily on the first attempt to write a record after midnight. An additional OMF is created when the current OMF becomes full. The standard OMF naming convention is AYYMMDDn.

XYGATE BASE24 Mover

XYPRO developed the BASE24 Mover so that BASE24 Pathway security audit data can be collected, normalized, alerted, and added to the XYGATE Merged Audit (XMA) database, similar to all other security audit data that XMA collects on the NonStop.

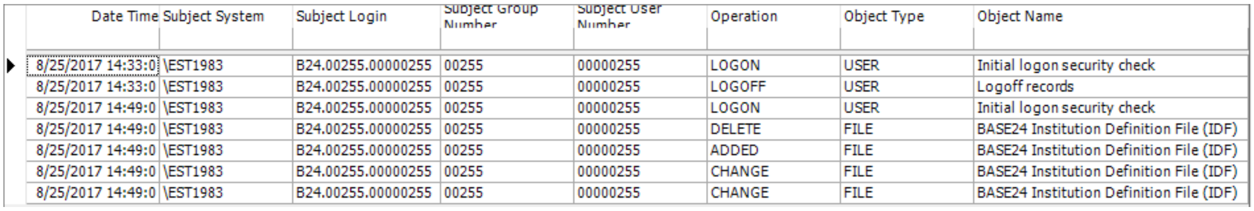
Figure 1 shows XMA collecting from a variety of security audit data sources on the NonStop, including BASE24.



(Figure 1)

At a minimum, BASE24 security audit data stored in the XMA database can be queried and reported for a single day or for multiple days, depending on the data retention period of the XMA database.

Figure 2 shows a sample XMA database query using the XYGATE Report Manager (XRM) GUI.

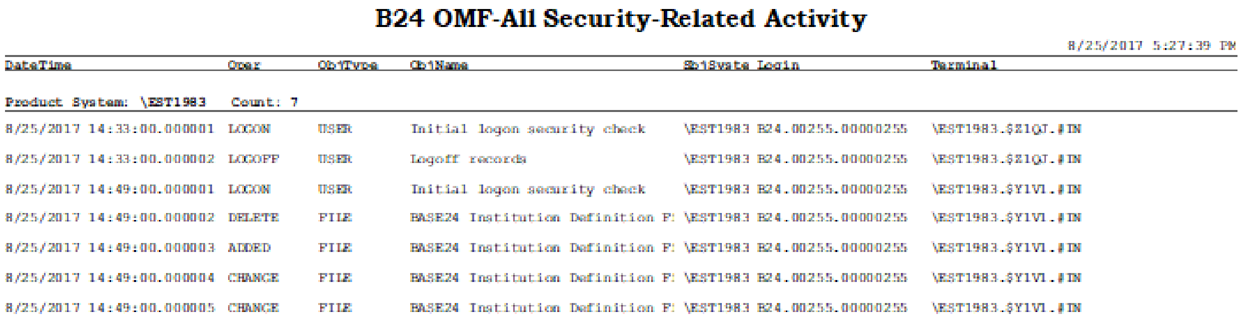


Date Time	Subject System	Subject Login	Subject Group Number	Subject User Number	Operation	Object Type	Object Name
8/25/2017 14:33:0	\EST1983	B24.00255.00000255	00255	00000255	LOGON	USER	Initial logon security check
8/25/2017 14:33:0	\EST1983	B24.00255.00000255	00255	00000255	LOGOFF	USER	Logoff records
8/25/2017 14:49:0	\EST1983	B24.00255.00000255	00255	00000255	LOGON	USER	Initial logon security check
8/25/2017 14:49:0	\EST1983	B24.00255.00000255	00255	00000255	DELETE	FILE	BASE24 Institution Definition File (IDF)
8/25/2017 14:49:0	\EST1983	B24.00255.00000255	00255	00000255	ADDED	FILE	BASE24 Institution Definition File (IDF)
8/25/2017 14:49:0	\EST1983	B24.00255.00000255	00255	00000255	CHANGE	FILE	BASE24 Institution Definition File (IDF)
8/25/2017 14:49:0	\EST1983	B24.00255.00000255	00255	00000255	CHANGE	FILE	BASE24 Institution Definition File (IDF)

(Figure 2)

Using the same GUI, a report can be easily produced.

Figure 3 shows a sample report.



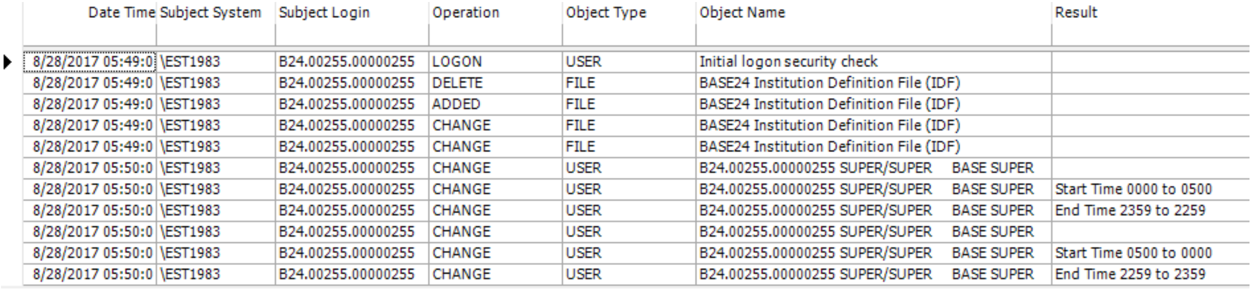
B24 OMF-All Security-Related Activity

```
                                                                                                   8/25/2017 5:27:39 PM
DateTime                     Oper      ObjType   ObjName                            SbjSysts Login               Terminal

Product System: \EST1983   Count: 7
8/25/2017 14:33:00.000001  LOGON     USER      Initial logon security check       \EST1983 B24.00255.00000255  \EST1983.$Z1QT.#IN
8/25/2017 14:33:00.000002  LOGOFF    USER      Logoff records                     \EST1983 B24.00255.00000255  \EST1983.$Z1QT.#IN
8/25/2017 14:49:00.000001  LOGON     USER      Initial logon security check       \EST1983 B24.00255.00000255  \EST1983.$Y1V1.#IN
8/25/2017 14:49:00.000002  DELETE    FILE      BASE24 Institution Definition F:   \EST1983 B24.00255.00000255  \EST1983.$Y1V1.#IN
8/25/2017 14:49:00.000003  ADDED     FILE      BASE24 Institution Definition F:   \EST1983 B24.00255.00000255  \EST1983.$Y1V1.#IN
8/25/2017 14:49:00.000004  CHANGE    FILE      BASE24 Institution Definition F:   \EST1983 B24.00255.00000255  \EST1983.$Y1V1.#IN
8/25/2017 14:49:00.000005  CHANGE    FILE      BASE24 Institution Definition F:   \EST1983 B24.00255.00000255  \EST1983.$Y1V1.#IN
```

(Figure 3)

With one exception, the BASE24 Mover collects all necessary OMF data except record images. The exception is the Security (SEC) file. The BASE24 Mover collects SEC record images and, in the case of an update, contrasts the two record images and resolves the differences. This results in identifying the fields that have changed because of an update. Figure 4 shows an example query where the Start and End Time fields in the BASE24 Security (SEC) file were modified. The BASE24 Mover contrasts the before and after record images to resolve the change and capture it in the XMA database. The RESULT column shows that the values were changed from 00:00 to 05:00 and 23:59 to 12:59 and then returned to their original values.



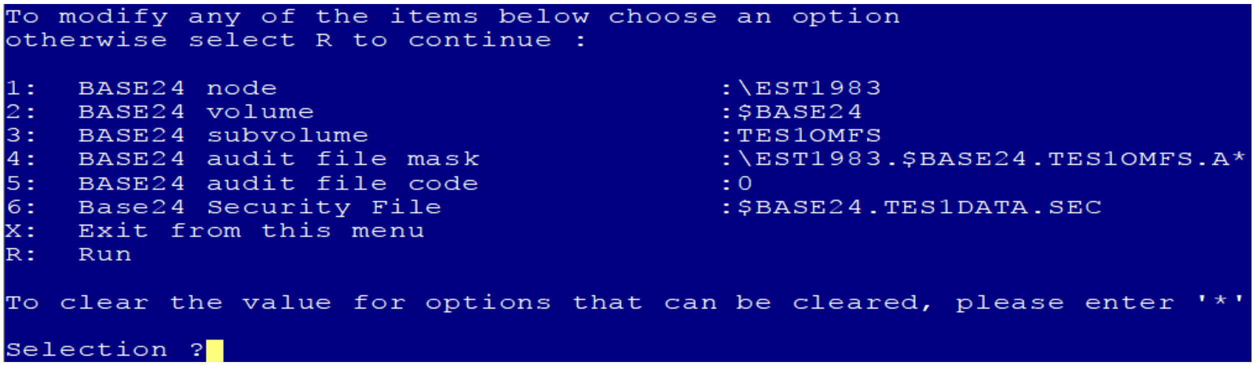
Date Time	Subject System	Subject Login	Operation	Object Type	Object Name	Result
8/28/2017 05:49:0	\EST1983	B24.00255.00000255	LOGON	USER	Initial logon security check	
8/28/2017 05:49:0	\EST1983	B24.00255.00000255	DELETE	FILE	BASE24 Institution Definition File (IDF)	
8/28/2017 05:49:0	\EST1983	B24.00255.00000255	ADDED	FILE	BASE24 Institution Definition File (IDF)	
8/28/2017 05:49:0	\EST1983	B24.00255.00000255	CHANGE	FILE	BASE24 Institution Definition File (IDF)	
8/28/2017 05:49:0	\EST1983	B24.00255.00000255	CHANGE	FILE	BASE24 Institution Definition File (IDF)	
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	Start Time 0000 to 0500
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	End Time 2359 to 2259
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	Start Time 0500 to 0000
8/28/2017 05:50:0	\EST1983	B24.00255.00000255	CHANGE	USER	B24.00255.00000255 SUPER/SUPER BASE SUPER	End Time 2259 to 2359

(Figure 4)

Optionally, BASE24 security audit data can be alerted to a Security Information and Event Management (SIEM) appliance or to XYPRO's XYGATE SecurityOne (XS1) real time Security Intelligence and Analytics solution.

The BASE24 Mover can easily be added using XMA_MANAGER.

Figure 5 shows the use of the XMA_MANAGER macro to set the parameters for adding the BASE24 Mover.



```
To modify any of the items below choose an option
otherwise select R to continue :

1:   BASE24 node                       :\EST1983
2:   BASE24 volume                     :$BASE24
3:   BASE24 subvolume                  :TES1OMFS
4:   BASE24 audit file mask            :\EST1983.$BASE24.TES1OMFS.A*
5:   BASE24 audit file code            :0
6:   Base24 Security File              :$BASE24.TES1DATA.SEC
X:   Exit from this menu
R:   Run

To clear the value for options that can be cleared, please enter '*'

Selection ?
```

(Figure 5)

The XMA BASE24 Mover collects all user activity audit records from the BASE24 OMF file. Security-related EMS event generated by Pathway and NCPCOM are captured by the XMA EMS Mover. These combined sources enable logging for all BASE24 security activity into the XMA NonStop SQL database for reporting and alerting as well as seamless and secure integration within your enterprise SIEM, without custom programming or time-consuming data manipulation.

For more information on how to license the BASE24 Mover for XYGATE Merged Audit, please contact your account executive or visit www.XYPRO.com.