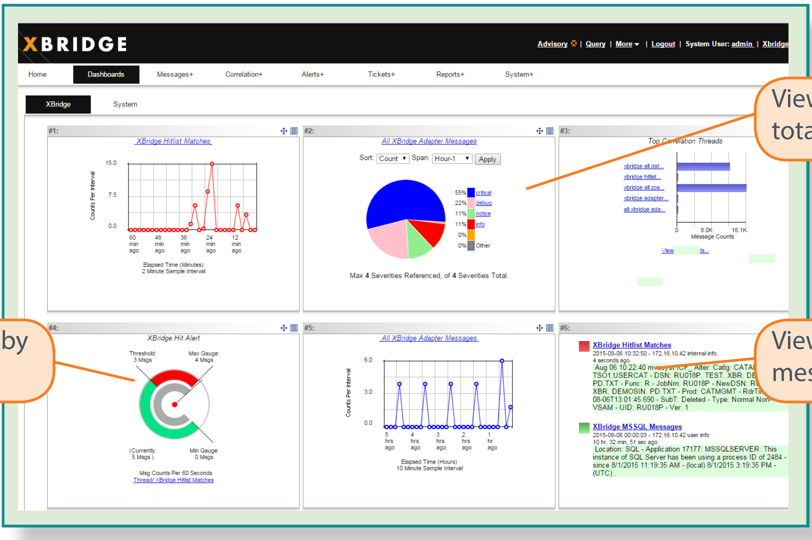
Product Datasheet

Xbridge DataSniff Mainframe Data Loss Prevention, Fortified by CorreLog SIEM Agent for z/OS

Xbridge and CorreLog combine for the industry's only DLP and real-time SIEM system for IBM z/OS.

How do we do it? Xbridge DataSniff identifies files and databases to be monitored for PCI DSS, HIPAA, SOX, or other compliance initiatives. CorreLog SIEM Agent for z/OS digests these files and monitors them for any attempts to manipulate them. SIEM Agent alerts compliance and security personnel in real-time if any "at risk" files are touched or changed. This combination of DLP and SIEM delivers unprecedented real-time security and compliance visibility and notifications for IBM z/OS.



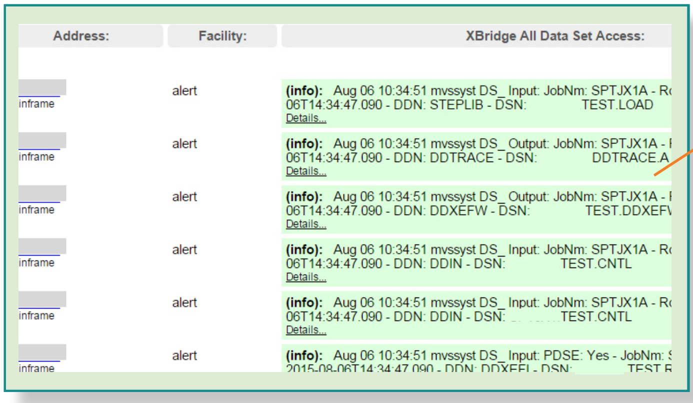
XBridge Hitlist Matches
2015-08-06 10:32:50 - 172.16.10.42 internal info
4 seconds ago
Aug 06 10:22:40 mvssyst ICF_ Alter: Catlg: CATAL
TSO1.USERCAT - DSN: RU018P. TEST. XBR. DE
PD.TXT - Func: R - JobNm: RU018P - NewDSN: R
XBR. DEMOSIN. PD.TXT - Prod: CATMGMT - RdrTi
08-06T13:01:45.690 - SubT: Deleted - Type: Normal Non-
VSAM - UID: RU018P - Ver: 1

XBridge MSSQL Messages
2015-08-06 00:00:03 - 172.16.10.42 user info
10 hr, 32 min, 51 sec ago
Location: SQL - Application 17177: MSSQLSERVER: This instance of SQL Server has been using a process ID of 2484 - since 8/1/2015 11:19:35 AM - (local) 8/1/2015 3:19:35 PM - (UTC) .

View event message total with level of severity.

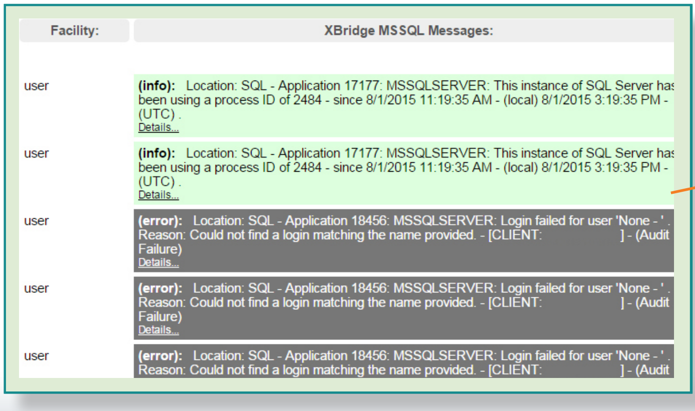
View severe messages by specified intervals.

View recent event messages with details.



Address:	Facility:	XBridge All Data Set Access:
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Input: JobNm: SPTJX1A - Ro 06T14:34:47.090 - DDN: STEPLIB - DSN: TEST.LOAD Details...
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Output: JobNm: SPTJX1A - I 06T14:34:47.090 - DDN: DDTRACE - DSN: DDTRACE.A Details...
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Output: JobNm: SPTJX1A - I 06T14:34:47.090 - DDN: DDXEFW - DSN: TEST.DDXEFV Details...
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Input: JobNm: SPTJX1A - Ro 06T14:34:47.090 - DDN: DDIN - DSN: TEST.CNTL Details...
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Input: JobNm: SPTJX1A - Ro 06T14:34:47.090 - DDN: DDIN - DSN: TEST.CNTL Details...
[redacted] inframe	alert	**(info):** Aug 06 10:34:51 mvssyst DS_ Input: PDSE: Yes - JobNm: S 2015-08-06T14:34:47.090 - DDN: DDXEFI - DSN: TEST.R

There are literally millions of datasets and records accessed by sysprogs or admins, some of it dating back dozens of years. A good percentage of this data isn't even on your radar, but has a huge impact on your compliance. Xbridge's data discovery function provides a means for locating then "watching" this data for any sign of access or tampering. CorreLog SIEM Agent records these accesses (your audit trail), and in real time, notifies security and compliance personnel of any suspicious activity.



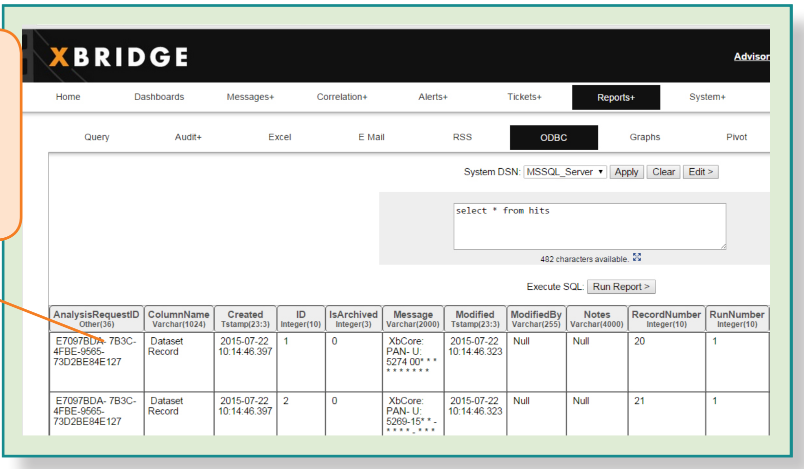
Facility:	XBridge MSSQL Messages:
user	**(info):** Location: SQL - Application 17177: MSSQLSERVER: This instance of SQL Server has been using a process ID of 2484 - since 8/1/2015 11:19:35 AM - (local) 8/1/2015 3:19:35 PM - (UTC) . Details...
user	**(info):** Location: SQL - Application 17177: MSSQLSERVER: This instance of SQL Server has been using a process ID of 2484 - since 8/1/2015 11:19:35 AM - (local) 8/1/2015 3:19:35 PM - (UTC) . Details...
user	**(error):** Location: SQL - Application 18456: MSSQLSERVER: Login failed for user 'None - ' . Reason: Could not find a login matching the name provided. - [CLIENT:] - (Audit Failure) Details...
user	**(error):** Location: SQL - Application 18456: MSSQLSERVER: Login failed for user 'None - ' . Reason: Could not find a login matching the name provided. - [CLIENT:] - (Audit Failure) Details...
user	**(error):** Location: SQL - Application 18456: MSSQLSERVER: Login failed for user 'None - ' . Reason: Could not find a login matching the name provided. - [CLIENT:] - (Audit

If you need to audit user activity to SQL, CorreLog SIEM Agent can deliver event logs to Xbridge including user ID, job number, MVS system, and a multitude of SMF records. Any user (including privileged users) access to these assigned datasets are captured by SIEM Agent and reported in the DataSniff dashboard. Automated alerts in the form of texts, phone calls, helpdesk tickets or email notifications can be sent to the appropriate security and compliance personnel.

Xbridge Data Loss Prevention Fortified by CorreLog SIEM Agent for z/OS

Xbridge and CorreLog combine for the industry's only DLP and real-time SIEM system for IBM z/OS.

Xbridge leverages the deep mainframe security logging capability from CorreLog SIEM Agent for robust reporting. Report queries are easily defined and contain detailed user activity (including privileged users) from RACF, ACF2, Top Secret and DB2 data sources.



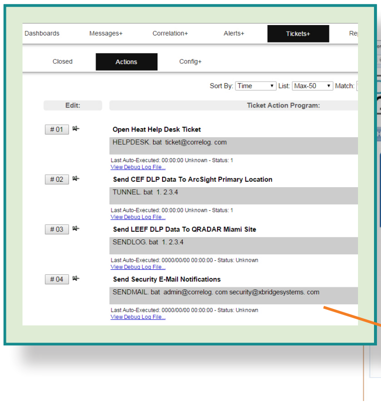
System DSN: MSSQL_Server

```
select * from hits
```

482 characters available.

Execute SQL:

AnalysisRequestID Other(36)	ColumnName Varchar(1024)	Created Tstamp(23:3)	ID Integer(10)	IsArchived Integer(3)	Message Varchar(2000)	Modified Tstamp(23:3)	ModifiedBy Varchar(255)	Notes Varchar(4000)	RecordNumber Integer(10)	RunNumber Integer(10)
E7097BDA- 7B3C-4FBE-9565-73D2BE84E127	Dataset Record	2015-07-22 10:14:46.397	1	0	XbCore: PAN- U: 5274 00* * * * * * * * * *	2015-07-22 10:14:46.323	Null	Null	20	1
E7097BDA- 7B3C-4FBE-9565-73D2BE84E127	Dataset Record	2015-07-22 10:14:46.397	2	0	XbCore: PAN- U: 5269-15* * - * * * * _ * * *	2015-07-22 10:14:46.323	Null	Null	21	1



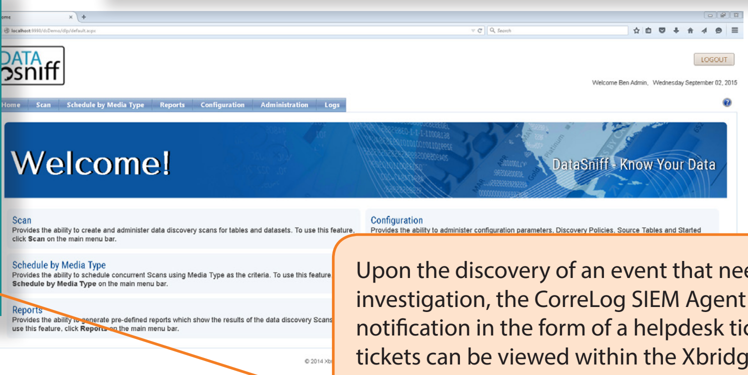
Sort By: Time List: Max-50 Match:

Open Heat Help Desk Ticket
HELPDESK. bat ticket@correlog. com
Last Auto-Executed: 00:00:00 Unknown - Status: 1

Send CEF DLP Data To ArcSight Primary Location
TUNNEL. bat 1. 2.3.4
Last Auto-Executed: 00:00:00 Unknown - Status: 1

Send LEEF DLP Data To QRADAR Miami Site
SENDLOG. bat 1. 2.3.4
Last Auto-Executed: 0000/00/00 00:00:00 - Status: Unknown

Send Security E-Mail Notifications
SENDMAIL. bat admin@correlog. com security@xbridgesystems. com
Last Auto-Executed: 0000/00/00 00:00:00 - Status: Unknown



localhost:9990/dsDemo/dlp/default.aspx

Welcome Ben Admin, Wednesday September 02, 2015

Scan
Provides the ability to create and administer data discovery scans for tables and datasets. To use this feature, click **Scan** on the main menu bar.

Configuration
Provides the ability to administer configuration parameters, Discovery Policies, Source Tables and Started

Schedule by Media Type
Provides the ability to schedule concurrent Scans using Media Type as the criteria. To use this feature **Schedule by Media Type** on the main menu bar.

Reports
Provides the ability to generate pre-defined reports which show the results of the data discovery Scans use this feature, click **Reports** on the main menu bar.

© 2014 Xb

Upon the discovery of an event that needs further investigation, the CorreLog SIEM Agent can issue a notification in the form of a helpdesk ticket. These tickets can be viewed within the Xbridge console. This is critical for not just looking at the tickets and their severity, but also for auditing and compliance.

Xbridge DLP, enhanced by CorreLog SIEM Agent for z/OS, is a powerful mainframe security, auditing and compliance system. The data discovery and resource optimization functions in Xbridge combined with the RACF, ACF2, Top Secret and DB2 access monitoring from CorreLog, provide real-time mainframe security and compliance auditing unmatched in the industry. The system connects to any distributed SIEM including IBM® QRadar Security®, HP ArcSight, RSA Security Analytics, Splunk, LogRhythm, Dell SecureWorks, Solutionary and countless others. IBM, HP and EMC (via RSA) are strategic CorreLog technology partners and the IBM QRadar, HP ArcSight and RSA integrations to CorreLog SIEM Agent are certified.

For more information about the Xbridge DLP and CorreLog SIEM Agent offering, please contact Xbridge or CorreLog today.

Xbridge Systems
4040 Moorpark Ave., Suite 110
San Jose, CA 95117
Phone Number (650) 564-9800
Phone Number (866) 356-1515 (toll free)
Fax (650) 564-9990 (fax)
sales@xbridgesystems.com
www.xbridgesystems.com

CorreLog, Inc.
1004 Collier Center Way, 1st Floor
Naples, Florida 34110
877-267-7356 - Toll-free telephone (US only)
239-514-3331 - Telephone
239-687-3505 - Fax
info@correlog.com
www.correlog.com