TA-DB $CyberTechDocumentation$

Release stable

Jun 19, 2018

Table of Contents

Latest documentation is posted on http://ta-db-cybertech.readthedocs.io

CHAPTER 1

Overview

1.1 About the TA

The DB CyberTech DBN-6300 uses syslog to provide event reporting to a central Security Information and Event Management (SIEM) system and to report general system health information. Syslog output is encoded in the Common Event Format (CEF), which allows easy integration into a number of common security information and event management (SIEM) andlog-analysis tools. DB CyberTech can provide sample integration with popular tools. This manual describes the DBN-6300 syslog messages.

App Author: - Brandon Kirklen – Email - Splunk Answers - Github

1.2 Splunk/DBN Version Compatibility

Splunk Version	App Version	DBN Version
Splunk 6.5.2	1.0.0	2.2.14
Splunk 6.6.1	2.0.0	3.0.0
Splunk 7.0.0	2.0.0	4.2.4

1.3 Install From Github

This TA is avalible on SplunkBase. Or you can clone this github repo into your *$SPLUNK_HOME* folder and then restarting Splunk Enterprise.

Splunkbase::

```
https://splunkbase.splunk.com/app/3587/
```

Clone::

```
git clone https://github.com/DBCyberTech/TA-DB_CyberTech TA-DB_CyberTech
```

CHAPTER 2

Installation and Configuration

2.1 Installation Steps

2.1.1 Step 1: Install the App

Install the DB CyberTech TA by downloading the latest release from DB Cybertech Add-on. Or if you want to test beta code, from Github

2.2 Configure TA-DB_CyberTech

Minimal configuration is needed, simply associate a given input with the TA and you'll see the sourcetypes applied.

CHAPTER 3

User Guide

3.1 DBN TA Source Types

Splits incoming feed into:

1. `system_counters`: This source type is used for various system counter information including
    - `cnt`: An external dump of the internal counter's page, lists stats for incoming feed and engine processing
    - `sys`: Contains system level information including free memory, cache, and system uptime
    - `slowsys`: A more complete set of system level information including airflow readings, disk usage, and wear indicators
    - `dbfwsys`: Information specific to the DBFW process running
2. `sqli_events`: SQL injection events will be associated with this sourcetype. This includes two subevent types
    - `distinct_event`: description of the first sql statement which is deemed a potential sql injection attack
    - `repeat_event`: events which match an injection on a statement already alerted on
3. `discovery_events`: These alerts are triggered in response to new events within the flows being monitored but without rising to the level of an attack.
    - `mds_new_user`: A new user is seen for the first time
    - `mds_new_service`: a new service is seen for the first time
    - `mds_new_host`: a new host is seen for the first time
    - `mds_new_listener`: a new listener is seen for the first time
    - `tally_new_ipseity`: a new context is seen linking client and servicer in dimensions (tally board, user, service, client, server)
4. `health_events`: contains events mainly involving engineering metrics
    - `heart_beat`: used to monitor system up status on a more frequent basis than `dbfwsys`
    - `engine_start`: used to monitor for engine restarts

- `archive`: Indicates status of overnight system archive tool
- `dbfw_gc`: Indicates a system restart due to overload of data
- `dbdu`: postgres database disk usage

5. `insider_threat_events`: events related to table level analysis preformed with the insider threat module
6. `audit`: events exported by native device auditing
7. `upgrade`: raw dump of upgrade messages for external viewing
8. `internal`: catch for bad output of internal messages, trashed

CHAPTER 4

Syslog Messages

4.1 Message Overview

Syslog messages forwarded from the DBN-6300 are formatted to meet the CEF header specification.

Syslog Message Format:

CEF Header Field	DBN-6300 Data
Version	0
Device Vendor	DB Networks
Device Product	DBN
Device Version	Current system version
Signature ID	Numeric ID
Name	String name associated with ID
Severity	Value from 0-7, system specified
cs1Label	system identifier
cs1	System serial number
system_identifier	System serial number
rt	Message creation time in ms from epoch
Message	Varies by event

Here is a genericised cef header as an example of the formatting:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature␣
↪ID|Name|Severity|Extension
```

4.2 Signature ID and Name Values

Note: The default size of the rsyslog is 8K. Logs that exceed this size are truncated automaticaly. If you expect syslog messages greater than 8K, increase the default message size to avoid truncation.

4.3 Syslog Message Detail

4.3.1 Engine Restart Message

The restart message the startup of the DBN-6300. This message indicates that the DBN-6300 has completed its power up sequence after an initial power-up, restart/reset, or fatal error. If this message is detected and no intentional restart was initiated, contact customer service to investigate the cause.

A typical message resembles the following:

```
<133>2018-06-11T12:39:03.984166-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|3|engine_
↪start|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
```

The message is identified by Signature ID= `3` and name= `engine_start`.

4.3.2 Event Report Messages

Event report messages are generated as soon as an event is detected. There are two types of event report messages:

- `distinct_event` messages pertain to new unique SQL statements that are detected as possible threates. Distinct events have a Signature ID= `0` and name= `distinct_event`
- `repeat_event` messages represent repeated executions of previously detected SQL statements. Repeat events have a Signature ID= `1` and name= `repeat_event`

Both messages contain the same information, but are distinguished by the labels above appearing in the name field of the CEF prefix.

A typical `distinct_event` resembles the following. A `repeat_event` has the same structure, but the `cnt` field is greater than 1.

```
<132>2018-06-11T16:28:53.769474-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.
↪4|0|distinct_event|10|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423␣
↪externalId=23179
cnt=1 rt=1528752533769 start=1449230398145 destinationServiceName=accounts␣
↪cn1Label=statement identifier
cn1=22932 statement_identifier=22932 cat=structural dst=10.4.40.7 dpt=1433 src=10.15.
↪32.25 spt=37224
cs2Label=score cs2=1.000 score=1.000 cs3Label=confidence cs3=certain␣
↪confidence=certain
act=exec_dispatch target_sql_id=320
```

The first part of the message contains the elements of the standard CEF format. The remainder is described below.

Field Details:

Field	Description
externalId	Unique event id used to look up the event in the DBN Logs
cnt	Number of occurances of events with given statement identifer
rt	Transmit time of the event
start	epoch time of event (milliseconds)
destinationServiceName	Name of the database associated with the attack
cn1Label	Statement Identifier
cn1	Unique statement id
cat	type of event (structural or parametric)
dst	Destination IP
dpt	Destination Port
src	Source IP
spt	Source Port
cs2Label	Score
cs2	Numerical confidence score (normalized between 01)
cs3Label	Confidence
cs3	String confidence description (certain, overwhelming, likely, suspicious, possible)
act	Type of action involved (Maps to protocol RPC)
target_sql_id	Integer value represented on the system by the target SQL ID

4.3.3 System Health Messages

Health syslog messages are sent every 10 minutes (at minute mod 10 boundaries). These messages are distinguished from event messages by the keywords `cnt`, `sys`, `slowsys`, and `dbfwsys` in the CEF Name field. These messages contain system information useful to DB Networks' Customer Support personnel.

Example `cnt` message:

```
<133>2018-06-11T03:44:44.797928-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|11|cnt|0|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528706684797 xtime_T01=05/31/18 13:41:03 xtime_T02=06/11/18 03:44:44 xtime_T03=1
xtime_T04=10d 14:03:41 xtime_T05=06/01/18 15:48:54 xcap_X13=49460224 xcap_X01=49460224
xcap_X33=49460224 xcap_X03=6 xcap_X26=19 xcap_X27=61040 xcap_X28=61039 xcap_X04=1.00
xcap_X15=6 xcap_X11=1895 xcap_X21=0.01 xpro_X08=1 xpro_X17=1 xpro_X23=0.00 xpro_X24=0.
↪00
xpro_X05=0.00 xpro_X09=0.00 xpro_X18=38287169 xpro_X19=1.00 xpro_X20=0.01 xpro_
↪X35=406348
xpro_X36=8 xpro_X37=61019 xpro_X38=221101 xpro_X39=7046 xeng_X29=92 xeng_X30=19025081
xeng_X31=92 ts=1528706684796
```

As with event messages, the first part of the messages contains the elements defined in the CEF format. Through most of the information in the various health log messages is useful only to DB Networks' support, there are a few fields which can be mapped useful external concepts.

Useful Event Message Counters:

- `xcap_X13` : Total number of packets recieved on the capture port. If this number is not increasing as expected for a given installation, the capture port might not be capturing traffic.
- `xcap_X15` : Total number of packets dropped by the engine. If this number increase rapidly, it might indicate that the span/tap port is configured to send a lot of non-sql traffic. This affects system preformance and should be corrected either by changing the span/tap port configuration or adjusting the network filters on the DBN-6300 to filter out unwanted traffic before it reaches the engine.

The following messages are also sent every 10 minutes. These messages can be useful to DB Networks customer support and development personnel if an issue arises.

sys:

```
<133>2018-06-11T03:49:47.332626-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|12|sys|0|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528706987332 os_uptime=914936 os_loadavg_0=0 os_loadavg_1=0 os_loadavg_2=0 os_
↪freemem=833536000
os_totalmem=8367423488 sys_user=1531705 sys_nice=9690 sys_system=744604 sys_
↪idle=179829889
sys_iowait=30758 sys_irq=276608 sys_softirq=265033 sys_steal=0 sys_guest=0 sys_guest_
↪nice=0
vm_pgpgin=931157 vm_pgpgout=105314097 vm_pswpin=0 vm_pswpout=0 vm_pgfault=542285262
meminfo_MemTotal=8171312 meminfo_MemFree=814000 meminfo_MemAvailable=3852672 meminfo_
↪Buffers=355684
meminfo_Cached=2882872 meminfo_SwapCached=0 meminfo_Active=3055660 meminfo_
↪Inactive=1970804
meminfo_Active(anon)=1816472 meminfo_Inactive(anon)=28444 meminfo_Active(file)=1239188
meminfo_Inactive(file)=1942360 meminfo_Unevictable=0 meminfo_Mlocked=0 meminfo_
↪SwapTotal=976892
meminfo_SwapFree=976892 meminfo_Dirty=496 meminfo_Writeback=0 meminfo_
↪AnonPages=1787968
meminfo_Mapped=2487416 meminfo_Shmem=71208 meminfo_Slab=179368 meminfo_
↪SReclaimable=157068
meminfo_SUnreclaim=22300 meminfo_KernelStack=4256 meminfo_PageTables=31900 meminfo_
↪NFS_Unstable=0
meminfo_Bounce=0 meminfo_WritebackTmp=0 meminfo_CommitLimit=5062548 meminfo_Committed_
↪AS=4248612
meminfo_VmallocTotal=34359738367 meminfo_VmallocUsed=0 meminfo_VmallocChunk=0 meminfo_
↪HardwareCorrupted=0
meminfo_AnonHugePages=0 meminfo_ShmemHugePages=0 meminfo_ShmemPmdMapped=0 meminfo_
↪CmaTotal=0
meminfo_CmaFree=0 meminfo_HugePages_Total=0 meminfo_HugePages_Free=0 meminfo_
↪HugePages_Rsvd=0
meminfo_HugePages_Surp=0 meminfo_Hugepagesize=2048 meminfo_DirectMap4k=157632 meminfo_
↪DirectMap2M=8230912
memsum_usedGb=4 memsum_freeGb=4 disk_sda_readOps=37129 disk_sda_readSectors=1860258
disk_sda_writeOps=11382659 disk_sda_writeSectors=210640331
```

slowsys:

```
<133>2018-06-11T03:49:51.565949-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.
↪4|13|slowsys|0|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528706991565 disk_root_total=47103168 disk_root_avail=36005372 disk_maint_
↪total=2818080
disk_maint_avail=907268 disk_boot_total=194235 disk_boot_avail=79685 disk_sysdata_
↪total=185301
disk_sysdata_avail=162649 vers=0 it_sysdecCommitted=0 it_sysdecProposed=0
```

dbfwsys:

```
<133>2018-06-11T03:49:49.338516-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.
↪4|14|dbfwsys|0|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528706989337 dbfw_pid=1884 dbfw_state=0 dbfw_userCpu=49031 dbfw_sysCpu=20857
dbfw_numThread=19 dbfw_VmSize=2761003008 dbfw_VmRSS=303161344
```

4.3.4 New Discovery Messages

New discovery syslog messages are sent when the DBN-6300 identifies a new user, service, host, listener, or context linking client and server in dimensions (ipseity).

The fields associated with these various messages are shown below with optional values in brackets:

Signature ID	Name	Description
6	mds_new_user	• user_name =<string = non-empty user name> • default_schema =<string = default schema for new user>
7	mds_new_service	• service_name = <string = service_name> • service_name_type =<string =service type (service|SID|global name)> • dialect =<string = database dialect (Oracle|MS Sql)>
8	mds_new_host	• realm =<string = realm name> • addr =<string =IPV4 address>
9	mds_new_listener	• realm = <string = realm name> • addr = <string = IPV4 address> • port = <integer = TCP/IP port>
10	tally_new_ipseity	• tally_board = <string = identifier for tally board, currently main> • [user_name = <string = non-empty user name>] • [service_name = <string = non-empty service name] • client_realm = <string = client realm name> • client_addr = <string = IPV4 addr of client> • server_realm = <string = server listener realm name> • server_addr = <string = IPV4 addr of server listener> • server_port = <int = TCP/IP port of server listener> • client_ipseities = <int = pre-existing ipseities with matching client host – zero implies this is the first> • server_ipseities = <int = pre-existing ipseities with matching server host> • [server_service_ipseities = <int = pre-existing ipseities with matching server host

Example Messages:

mds_new_user

```
<133>2018-06-11T13:50:00.449964-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|6|mds_new_
↪user|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528743000448 user_name=sa default_schema=sa
```

mds_new_service

```
<133>2018-06-11T13:50:00.441856-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|7|mds_new_
↪service|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528743000432 service_name=accounts service_name_type=service dialect=Sql-Server
```

mds_new_host

```
<133>2018-06-11T13:50:00.446950-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|8|mds_new_
↪host|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528743000444 realm=default addr=10.15.33.3
```

mds_new_listener

```
<133>2018-06-11T13:50:00.453014-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|9|mds_new_
↪listener|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528743000433 realm=default addr=10.3.30.14 port=14338
```

tally_new_ipseity

```
<133>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|10|tally_
↪new_ipseity|5|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528743000741 tally_board=main user_name=sa service_name=accounts client_
↪realm=default
client_addr=10.15.33.3 server_realm=default server_addr=10.4.40.7 server_port=1433␣
↪client_ipseities=1
server_ipseities=1 server_service_ipseities=1 server_service_user_ipseities=1
```

4.3.5 Audit Messages

Audit messages are an optional syslog output configured on DBN-6300 under `Settings > Advanced > Audit Log`. The purpose of these messages to to provide a record of selected transactions on the DBN unit. The details of these messages are described below.

audit

```
<133>2018-06-11T16: 53:05 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|20|audit|0|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
rt=1528753985039 category=secOps auditCode=1009 auditMessage="User login succeeded"
userId=admin sessionId=2CTvwhj_iAmVoV7zB8pVCiLSeALej0te src=10.40.7.216 target=
↪"User:admin"
cookies="[{"name":"dbnetworks","cookieDurationSec":3600}]"
```

Audit syslog messages will have a `category`, `auditCode`, `auditMessage`, `userId`, `sessionId` and `target` when applicable. For more information about codes and messages, see *Audit Codes*.

4.3.6 Insider Threat Event Messages

Insider threat messages are sent when the DBN-6300 sees statement executions meeting the criteria of an insider threat rule that has been configured to monitor and syslog. The purpose of these messages is alert customers to policy and stability violations in a monitored network. Insider threat rules are defined in terms of sets or patterns describing data flows. A data flow is the unique combination of a partially or fully qualified table name (for example, `master.sys.databases` specifies database, schema, and relation, but not server) mentioned in a specific network context (i.e., client IP, server IP, server Port, database service, and database user). When a statement is executed, the DBN-6300 analyzes the SQL text semantically, looks up the corresponding data flow (or flows if there are more than one qualified name in the statement), and checks whether that flow meets the criteria of an insider threat rule. If the rule's action is configured to write to syslog when it fires, the details of the data flow and unique identifiers for several aspects of the flow and rule are conveyed in messages described below.

The insider threat event module is made up of five types of events. Below you'll find a description of each event type, an example, and detailed information about the fields in the given event.

IT Clustered Flow

This event is emitted when the autopilot adds a data flow to the incident domain to be clustered with other behavioral incident data flows. Recall, each data flow is composed of a specific session and database object. The database object is one of relation, meta-relation, or user role. Relation and meta-relations are reported with an id, up to three name qualifiers (server, database, and schema) if applicable, a relation name, and mode of access (read or write for relations, create, drop, alter, or truncate for meta-relations). User role database objects are reported with an id, name, type (user or role), mode (create, drop, alter, grant, or revoke), when applicable a session database user ID and name, and when applicable, an optionally qualified relation. In addition to the defining features of the data flow in question, IT Clustered Flow events are characterized by the score information used by the autopilot to determine the data flow should be clustered.

Example:

```
<132>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|18|it_
↪clustered_flow|7|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
it_event_id=1056 cluster_id=74 flow_id=1804 context_id=1800 user_id=300
user_name=BOB client_id=572 client_realm=default client_ip=10.1.41.11 service_id=1030␣
↪dialect=Oracle
service_name=USCYBERCOM.OPSEC service_type=service listener_id=1028 listener_
↪realm=default
listener_ip=11.1.3.32 port=1521 context_earliest=1506003300000 access_id=317 relation_
↪id=317
relation=personcreditcard mode=read access_earliest=1494273900000 flow_
↪earliest=1506003300000
accessScore=0.999996204175 contextScore=0 combinedScore=0.999996204175 importance=1␣
↪risk=0.999996204175
```

Details of the field types:

Field Name	Type	Description
it_event_id	int	Event ID for new clustered data flow
cluster_id	int	Incident internal identifier for linking to DBN web interface
flow_id	int	Data flow internal identifier for linking to DBN web interface
context_id	int	Session internal identifier for linking to DBN web interface
user_id	int	Session database user name internal identifier
user_name	string	Session databse user name, e.g. "BOB"

Continued on next page

Table 1 – continued from previous page

Field Name	Type	Description
client_id	int	Session client internal identifier
client_realm	string	Session client realm, typically "default" unless using VLANs in DBN configuration
client_ip	string	Session client IP address, e.g. "10.1.41.2"
service_id	int	Session database service internal identifier
dialect	string	Session dialect description, e.g. "Oracle"
service_name	string	Session database service name, e.g. "CRM.EU"
service_type	string	Session database service type, either "sid", "global name", or "service"
listener_id	int	Session database listener internal identififer
listener_realm	string	Session database listener realm, typically "default" unless using VLANs in DBN configuration
listener_ip	string	Session database listener IP, e.g. " 10.1.40.32"
port	type	Session database listener port
context_earliest	int	Epoch milliseconds of earliest obvserved time for the data flow's session
access_id	int	Database object internal identifier
relation_id	int	Database object relation internal identifier
meta_relation_id	int	Database object meta-relation internal identifier
server	string	Database object relation server qualifier
database	string	Database object relation database qualifier
schema	string	Database object relation schema qualifier
relation	string	Database object relation name
mode	string	Database object mode of use, e.g. "read" or "alter"
user_role_id	int	Database object user role internal identifier
type	string	Database object user role type, either "user" or "role"
access_earliest	int	Epoch milliseconds of earliest observed time for the data flows's database object
flow_earliest	int	Epoch milliseconds of earliest observed time for the data flow
access_score	float	Internal score for how unexpected the session is in the context of the data flow's database object
context_score	float	Internal score for how unexpected the database object is in the context of the data flow's session
combined_score	float	Internal score combining the access and context score
importance	float	User specified weighting of the combined score
risk	float	Internal score combining combined score and importance

IT New Cluster

This event is emitted each time a new incident is created by the system. This happens when new, unexpectd data flows do not sufficiently match an existing incident. Either a new incident is created with the new data flow, or if the systems' clustering algorithms find a better grouping of unexpected data flows, old incidents are regrouped into new incidents to incorporate the new data flow

Example:

```
<132>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|22|it_new_
↪cluster|7|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
itEventId=1047 cluster_id=127
```

Details of the two field types:

Field Name	Type	Description
it_event_id	int	New incident event ID
cluster_id	int	New incident internal identifier for linking to DBN web interface

IT Obsolete Cluster

When the above mentioned regrouping happens, or the user introduces either learning or policy constraints into the system, incident clusters of data flows can become obsolete. This event is emitted under those circumstances however is disabled by default.

Example:

```
<132>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|23|it_
↪obsolete_cluster|7|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
itEventId=1049 cluster_id=128
```

Field Details:

Field Name	Type	Description
it_event_id	int	Obsolete incident event ID
cluster_id	int	Obsolete incident internal identifier

IT Cluster Activity

This event is emitted when data flows, previously clustered into an incident exhibit activity, i.e. executing sql statement(s). Each event corresponds to a single data flow. The data flow is reported with the same fields defined used by the IT Clustered Flow event except the score specific fields, `access_score`, `context_score`, `combined_score`, `importance`, and `risk`. In addition, the following fields are supplied:

Example:

```
<132>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|24|it_
↪cluster_activity|7|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
itEventId=1044 cluster_id=57 risk_type=high flow_id=1707 context_id=1672 user_id=301␣
↪user_name=system
client_id=298 client_realm=default client_ip=10.1.41.3 service_id=1030 dialect=Oracle
service_name=USCYBERCOM.OPSEC service_type=service listener_id=1028 listener_
↪realm=default
listener_ip=11.1.3.32 port=1521 context_earliest=1504451400000 access_id=480 relation_
↪id=480
relation=customer mode=read access_earliest=1494377400000 flow_earliest=1504464600000
activity_earliest=1505986500000 activity_latest=1506747900000 execs=493
```

Field Details:

Field Name	Type	Description
it_event_id	int	New incident activity event ID
risk_type	string	Incident risk category, either “high” or “low”
activity_earliest	int	Epoch milliseconds of the first observed time of activity for the data flow in this event
activity_latest	int	Epoch milliseconds of the latest observed time of activity for the data flow in this event
execs	int	Number of statement executions by the data flow in this event

IT Auto Learned

This event is emitted when a data flow is learned by the autopilot, using the same fields as the IT Clustered Flow event except `cluster_id`. This event is also disabled by default.

Example:

```
<132>2018-06-11T13:50:00.773763-05:00 dbfw dbn: CEF:0|DB Networks|DBN|4.2.4|18|it_
↪auto_learned|7|
cs1Label=system identifier cs1=FW42-ED-VV-B-0423 system_identifier=FW42-ED-VV-B-0423
itEventId=1056 flow_id=1804 context_id=1800 user_id=300
user_name=BOB client_id=572 client_realm=default client_ip=10.1.41.11 service_id=1030␣
↪dialect=Oracle
service_name=USCYBERCOM.OPSEC service_type=service listener_id=1028 listener_
↪realm=default
listener_ip=11.1.3.32 port=1521 context_earliest=1506003300000 access_id=317 relation_
↪id=317
relation=personcreditcard mode=read access_earliest=1494273900000 flow_
↪earliest=1506003300000
access_score=0.999996204175 context_score=0 combined_score=0.999996204175␣
↪importance=1 risk=0.999996204175
```

For field details see *IT Clustered Flow*.

IT Policy Activity

This event is emitted when data flows matching a committed policy constraint with a syslog category action exhibit activity, i.e. they execute sql statements. This event uses the same fields as the IT Cluster Activity event, substituting `constraint_id`, `category_id`, and `category` for `risk_type`:

Field Details:

Field Name	Type	Description
it_event_id	int	New policy activity event ID
constraint_id	int	Internal identifier or policy constraint that matched the data flow for this event
category_id	int	Internal identifier for the category assigned to the constraint that triggered this event
category	string	Category name for the category assigned to the constraint that triggered this event

IT New Context

This event is emitted once for each new context, also referred to as session, the first time it is observed. A new session event has the following fields:

Field Name	Type	Description
context_id	int	Session internal identifier for linking to DBN web interface.
user_id	int	Session database user name internal identifier.
user_name	string	Session databse user name, e.g. “BOB”
client_id	int	Session client internal identifier.
client_realm	string	Session client realm, typically “default” unless using VLANs in DBN configuration.
client_ip	string	Session client IP address, e.g. “10.1.41.2”
service_id	int	Session database service internal identifier.
dialect	string	Session dialect description, e.g. “Oracle”
service_name	string	Session database service name, e.g. “CRM.EU”
service_type	string	Session database service type, either “sid”, “global name”, or “service”
listener_id	int	Session database listener internal identififer.
listener_realm	string	Session database listener realm, typically “default” unless using VLANs in DBN configuration.
listener_ip	string	Session database listener IP, e.g. “10.1.40.32”
port	type	Session database listener port.
context_earliest	bigint	Epoch milliseconds of earliest obvserved time for the data flow’s session.

IT New Access

This event is emitted once for each new access, also referred to as database object, the first time it is observed. A database object is one of relation, meta-relation, or user role. Relation and meta-relations are reported with an id, up to three name qualifiers (server, database, and schema) if applicable, a relation name, and mode of access (read or write for relations, create, drop, alter, or truncate for meta-relations). User role database objects are reported with an id, name, type (user or role), mode (create, drop, alter, grant, or revoke), when applicable a session database user ID and name, and when applicable, an optionally qualified relation. A new object event has the following fields:

Field Name	Type	Description
access_id	int	Database object internal identifier.
relation_id	int	Database object relation internal identifier.
meta_relation_id	int	Database object meta-relation internal identifier.
server	string	Database object relation server qualifier.
database	string	Database object relation database qualifier.
schema	string	Database object relation schema qualifier.
relation	string	Database object relation name.
mode	string	Database object mode of use, e.g. “read” or “alter”.
user_role_id	int	Database object user role internal identifier.
user_role_name	string	Databse object user role name.
type	string	Database object user role type, either “user” or “role”.
access_earliest	bigint	Epoch milliseconds of earliest observed time for the data flows’s database object.

IT New Flow

This event is emitted once for each new data flow, the first time it is observed. A data flow is the unique combination of a context (also referred to as session) and access (also referred to as object). The fields for a new flow event are those used for a new context, those used for a new access, and also:

Field Name	Type	Description
flow_earliest	bigint	Epoch milliseconds of earliest observed time for the data flow.

4.3.7 CMDB Key-Value Pairs Format

The `tally_new_ipseity` (10), `ITClusteredFlow` (18), `ITClusterActivity` (24), `ITAutoLearned` (25), and `ITPolicyActivity` (26) events can be extended with CMDB data. The current implementation will add CEF pairs for each user extension of user, service, client, and relation (e.g. table) that has the syslog flag (1) set and applies to the event in question. For example, `tally_new_ipseity` events do not have relation attributes to extend, but the IT events do.

Each custom message key is prefixed by an identifier for the scope of attribute being annotated, followed by the name of the annotation. For example, if there exists CMDB data annotating each service with a `risk_score` and a `division`, then the `tally_new_ipseity` custom pairs will look like `mds.services_riskScore=34` and `mds.services_division=HR`.

The tally_new_ipseity events have the following prefixes:

- User annotations will be prefixed by `mds.users_`
- Service annotations will be prefixed by `mds.services_`
- Client host annotations will be prefixec by `mds.hosts_`

The IT events have the following prefixes:

- User annotations will be prefixed by `user_ext_mds.users_`
- Service annotations will be prefixed by `service_ext_mds.services_`
- Client host annotations will be prefixed by `client_ext_mds.hosts_`
- Relation annotations will be prefixed by `relation_ext_parser.relation_`

CHAPTER 5

Release Notes

5.1 Version 2.0.0

5.1.1 New IT Threat Event Types

In this release, IT Threat source types are expanded into `it_clustered_flow`, `it_new_cluster`, `it_obsolete_cluster`, `it_cluster_activity`, `it_auto_learned`, `it_policy_activity`, `it_new_context`, `it_new_access`, and `it_new_flow`. These source types are used by the new IT Threat suite of features in dbn version 3.0.0.

This release also marks the completion of the deprication of custom fields.

5.2 Version 1.0.0

5.2.1 Dealing With Custom Fields

Deprication

Current data from DBN6300 complies with the CEF standard for field values. This includes a construct of mandating a static key set neccesitating a structure for use with custom fields. This structure of `cs1Label=` followed by `cs1=` results in significant message overhead which is not needed in splunk. As such this structure is being phased out of DBN syslog messages. Current releases will continue to support exisiting pairs of key/value pairs formatted in this way but will also be adding a redundant key/value pair. For example current messages contain:

```
cs1Label=system identifier cs1=00:00:00:00:00
```

This will be replaced with:

```
cs1Label=system identifier cs1=00:00:00:00:00 system_identifier=00:00:00:00:00
```

And eventually simplified to:

```
system_identifier=00:00:00:00:00
```

Search Time Replacement

In the mean time, if you would like to use custom field values, you can use a search time extraction like the following:

```
* | rex mode=sed field=cs1Label "s/ /_/g" | eval {cs1Label}=cs1
```

Note: Part of the difficulty when using these custom fields is they have the potential to have spaces in the label. The `rex` part of the above search replaces those spaces before using the label as a field key. This will need to be done for any such custom field before it can be used as a field name.

CHAPTER 6

Audit Codes

6.1 4.2.4

6.1.1 secOps (1xxx)

Code	Message	Target
1000	Create user	User
1001	Update user	User
1002	Delete user	User
1003	Update user's password	User
1004	Lock user	User
1005	Unlock user	User
1006	Clear user's failed login attempts	User
1007	Clear user's old passwords	User
1008	Log out all users	Users
1009	User login succeeded	User
1010	User login failed	User
1011	Log out user	User
1012	Not authorized	User
1013	Not permitted	User
1014	Create role	Role
1015	Update role	Role
1016	Delete role	Role
1017	Update authentication configuration	Authentication
1018	Update tunnel configuration	Tunnel
1019	Update SSL configuration	SSL
1020	Update redaction configuration	Redaction
1021	Clear audit log	AuditLog
1022	Update audit configuration	AuditLog

Continued on next page

Table 1 – continued from previous page

Code	Message	Target
1023	Audit error	
1024	Create session	Session
1025	Delete session	Session
1026	Enable SSH remote access	SSH
1027	Disable SSH remote access	SSH
1028	Create API key	APIKey
1029	Update API key	APIKey
1030	Delete API key	APIKey
1031	Lock API key	APIKey
1032	Unlock API key	APIKey
1033	Update Strict-Transport-Secu rity HTTP header configuration	HSTS
1034	Update user interface port configuration	UIPorts
1035	Update global redaction settings	GlobalRedaction
1036	Update shell password	ShellPassword
1037	Deleted shell password	ShellPassword

6.1.2 sysOps (2xxx)

Code	Message	Target
2000	Update network configuration	Network
2001	Update capture filter	CaptureFilter
2002	Update capture filter mode	CaptureFilter
2003	Create capture VLAN	CaptureVLAN
2004	Update capture VLAN	CaptureVLAN
2005	Delete capture VLAN	CaptureVLAN
2006	Update capture source	CaptureSource
2007	Enable capture source identify	CaptureSource
2008	Disable all capture source identifiers	CaptureSource
2009	Update NTP configuration	Time
2010	Update server time	Time
2011	Update server timezone	Time
2012	Update syslog configuration	Syslog
2013	Restart system	System
2014	Power down system	System
2015	Restart UI server	System
2016	Reset to factory configuration	System
2017	Create system state report	SystemStateReport
2018	Delete system state report	SystemStateReport
2019	Initialize system for file management	FileManagement
2020	Upload backup	Backup
2021	Delete backup	Backup
2022	Download backup	Backup
2023	Set password for backup	Backup
2024	Unlock backup	Backup
2025	Initialize system for restoring a backup	
2026	Restore backup	Backup
2027	Create backup	Backup
2028	Upload upgrade	

Continued on next page

Table 2 – continued from previous page

Code	Message	Target
2029	Delete upgrade	Update
2030	Apply upgrade	Upgrade
2031	Kill watchdog	System
2032	Enable watchdog	System
2033	Disable watchdog	System
2034	Update registry	Registry
2035	Update CMS configuration	CMS
2036	Create a unit within CMS	
2037	Update a unit within CMS	Unit
2038	Delete a unit within CMS	
2039	User accepted the EULA	EULA
2040	EULA covered under seperate agreement	EULA
2041	Clear user data	System
2042	System resource lock debug	[lockName]
2043	Delete job	Job
2044	CMDB data was downloaded	CMDB
2045	CMDB data was merged into the system	CMDB
2046	CMDB configuration data was downloaded	CMDB
2047	CMDB configuration data was loaded	CMDB
2048	User did not accept the EULA	EULA
2049	Create archive drive	System
2050	Expand archive drive	System
2051	Expand primary drive	System
2052	System started	System
2053	File uploaded	File
2054	File downloaded	File
2055	File deleted	File
2056	Update a file	File
2057	Prepare CMS configuration	CMS
2058	Deregister CMS configuration	CMS
2059	Abort job	Job
2060	Force fail job	Job
2061	Detach job	Job

6.1.3 appOps (3xxx)

Code	Message	Target
3000	Map a service to a database	Mapping
3001	Unmap a service from a database	Mapping
3002	Unmanage a service	Mapping
3003	Update time period	TimeLearning
3004	Commit time learning	TimeLearning
3005	Learn statement	statementLearning
3006	Blacklist statement	statementLearning
3007	Update database configuration	Database
3008	Terminal session started	Terminal
3009	Terminal session ended	Terminal
3010	Terminal session not authorized	Terminal
3011	Terminal session not authorized for tail	Terminal

6.1.4 uiCalls (4xxx)

Code	Message
4000	UI route logs

6.1.5 cliCommands (5xxx)

Code	Message
5000	CLI command run
5001	CLI command failed

6.1.6 ldapAuth (6xxx)

Code	Message
6000	Ldap authentication logs

6.1.7 aclOps (7xxx)

Code	Message
7000	Access control list
7001	Access control list debug

6.1.8 certOps (8xxx)

Code	Message
8000	Certificate debug
8001	Certificate being used
8002	Certificate has been verified

6.1.9 distributedOps (10xxx)

Code	Message	Target
10000	Backup remote unit	Node
10001	Create archive drive on remote unit	Node
10002	Expand archive drive on remote unit	Node
10003	Expand primary drive on remote unit	Node
10004	Update network configuration on remote unit	Node
10005	Power down remote unit	Node
10006	Restart remote unit	Node
10007	Restart UI server on remote unit	Node
10008	Restore backup on remote unit	Node
10009	Clear user data on remote unit	Node
10010	Update syslog configuration on remote unit	Node
10011	Update server time on remote unit	Node
10012	Apply upgrade on remote unit	Node

6.2 3.0.0

6.2.1 secOps (1000-1999)

Security Operations (`secOps`):

Code	Message	Target
1000	Create user	User
1001	Update user	User
1002	Delete user	User
1003	Update user's password	User
1004	Lock user	User
1005	Unlock user	User
1006	Clear user's failed login attempts	User
1007	Clear user's old passwords	User
1008	Logout all users	User
1009	User login succeeded	User
1010	User login failed	User
1011	Logout user	User
1012	Not authorized	User
1013	Not permitted	User
1014	Create role	Role
1015	Update role	Role
1016	Delete role	Role
1017	Update authentication configuration	Authentication
1018	Update tunnel configuration	Tunnel
1019	Update SSL configuration	SSL
1020	Update redaction configuration	Redaction
1021	Clear audit log	AuditLog
1022	Update audit configuration	AuditLog
1023	Audit Error	N/A

Continued on next page

Table 3 – continued from previous page

Code	Message	Target
1024	Create session	Session
1025	Delete session	Session
1026	Enable SSH remote access	SSH
1027	Disable SSH remote access	SSH
1028	Create API key	APIKey
1029	Update API key	APIKey
1030	Delete API key	APIKey
1031	Lock API key	APIKey
1032	Unlock API key	APIKey
1033	Update Strict-Transport-Security HTTP header configuration	HSTS
1034	Update user interface port configuration	UIPorts
1035	Update global redaction settings	GlobalRedation
1036	Update shell password	ShellPassword
1037	Deleted shell password	ShellPassword

6.2.2 `sysOps` (2000-2999)

System Operations (`sysOps`):

Code	Message	Target
2000	Update network configuration	Network
2001	Update capture filter	CaptureFilter
2002	Update capture filter mode	CaptureFilter
2003	Create capture VLAN	CaptureVLAN
2004	Update capture VLAN	CaptureVLAN
2005	Delete capture VLAN	CaptureVLAN
2006	Update capture source	CaptureSource
2007	Enable capture source identify	CaptureSource
2008	Disable all capture source identifiers	CaptureSource
2009	Update NTP configuration	Time
2010	Update server time	Time
2011	Update server timezone	Time
2012	Update syslog configuration	Syslog
2013	Restart system	System
2014	Power system down	System
2015	Restart UI server	System
2016	Reset to factory configuration	System
2017	Create system state report	SystemStateReport
2018	Delete system state report	SystemStateReport
2019	Initialize system for file management	FileManagement
2020	Upload backup	Backup
2021	Delete backup	Backup
2022	Download backup	Backup
2023	Set password for backup	Backup
2024	Unlock backup	Backup
2025	Initialize system for restoring a backup	N/A
2026	Restore backup	Backup
2027	Create backup	Backup

Continued on next page

Table 4 – continued from previous page

Code	Message	Target
2028	Upload update	N/A
2029	Delete update	Update
2030	Apply update	Update
2031	Kill watchdog	Watchdog
2032	Enable watchdog	Watchdog
2033	Disable watchdog	Watchdog
2034	Update registry	Registry
2035	Update CMS configuration	CMS
2036	Create a unit within CMS	N/A
2037	Update a unit within CMS	Unit
2038	Delete a unit within CMS	N/A
2039	User accepted the EULA	EULA
2040	EULA covered under seperate agreement	EULA
2041	Clear user data	System
2042	System resource lock debug	[lockName]
2043	Delete job	Job
2044	CMDB data was downloaded	CMDB
2045	CMDB data was merged into the system	CMDB
2046	CMDB configuration data was downloaded	CMDB
2047	CMDB configuration data was loaded	CMDB
2048	User did not accept the EULA	EULA

6.2.3 `appOps` (3000-3999)

Application Operations (`appOps`):

Code	Message	Target
3000	Map a service to a database	Mapping
3001	Unmap a service from a database	Mapping
3002	Unmanage a service	Mapping
3003	Update time period	TimeLearning
3004	Commit time learning	TimeLearning
3005	Learn statement	StatementLearning
3006	Blacklist statement	StatementLearning
3007	Update database configuration	Database
3008	Terminal session started	Terminal
3009	Terminal session ended	Terminal
3010	Terminal session not authorized	Terminal
3011	Terminal session not authorized for tail	Terminal

6.2.4 `uiCalls` (4000-4999)

UI Route Details (`uiCalls`):

Code	Message
4000	UI route logs

6.2.5 cliCommands (5000-5999)

Command Line Interface Command Details (cliCommands):

Code	Message
5000	CLI command run
5001	CLI command failed

6.2.6 ldapAuth (6000-6999)

LDAP Authentication (ldapAuth):

Code	Message
6000	Ldap authentication logs

6.2.7 aclOps (7000-7999)

Access Control List Operations (aclOps):

Code	Message
7000	Access control list
7001	Access control list debug

6.2.8 certOps (8000-8999)

Certificate Operations (certOps):

Code	Message
8000	Certificate debug
8001	Certificate being used
8002	Certificate has been verified

6.3 2.2.14

6.3.1 secOps (1000-1999)

Security Operations (secOps):

Code	Message	Target
1000	Create user	User
1001	Update user	User
1002	Delete user	User
1003	Update user's password	User
1004	Lock user	User
1005	Unlock user	User

Continued on next page

Table 5 – continued from previous page

Code	Message	Target
1006	Clear user's failed login attempts	User
1007	Clear user's old passwords	User
1008	Logout all users	User
1009	User login succeeded	User
1010	User login failed	User
1011	Logout user	User
1012	Not authorized	User
1013	Not permitted	User
1014	Create role	Role
1015	Update role	Role
1016	Delete role	Role
1017	Update authentication configuration	Authentication
1018	Update tunnel configuration	Tunnel
1019	Update SSL configuration	SSL
1020	Update redaction configuration	Redaction
1021	Clear audit log	AuditLog
1022	Update audit configuration	AuditLog
1023	Audit Error	AuditError
1024	Create session	Session
1025	Delete session	Session
1026	Enable SSH remote access	SSH
1027	Disable SSH remote access	SSH
1028	Create API key	APIKey
1029	Update API key	APIKey
1030	Delete API key	APIKey
1031	Lock API key	APIKey
1032	Unlock API key	APIKey
1033	Update Strict-Transport-Security HTTP header configuration	HSTS
1034	Update user interface port configuration	UIPorts

6.3.2 `sysOps` (2000-2999)

System Operations (`sysOps`):

Code	Message	Target
2000	Update network configuration	Network
2001	Update capture filter	CaptureFilter
2002	Update capture filter mode	CaptureFilter
2003	Create capture VLAN	CaptureVLAN
2004	Update capture VLAN	CaptureVLAN
2005	Delete capture VLAN	CaptureVLAN
2006	Update capture source	CaptureSource
2007	Enable capture source identify	CaptureSource
2008	Disable all capture source identifiers	CaptureSource
2009	Update NTP configuration	Time
2010	Update server time	Time
2011	Update server timezone	Time
2012	Update syslog configuration	Syslog

Continued on next page

Table 6 – continued from previous page

Code	Message	Target
2013	Restart system	System
2014	Power system down	System
2015	Restart UI server	System
2016	Reset to factory configuration	System
2017	Create system state report	SystemStateReport
2018	Delete system state report	SystemStateReport
2019	Initialize system for file management	FileManagement
2020	Upload backup	Backup
2021	Delete backup	Backup
2022	Download backup	Backup
2023	Set password for backup	Backup
2024	Unlock backup	Backup
2025	Initialize system for restoring a backup	Backup
2026	Restore backup	Backup
2027	Create backup	Backup
2028	Upload update	Update
2029	Delete update	Update
2030	Apply update	Update
2031	Kill watchdog	Watchdog
2032	Enable watchdog	Watchdog
2033	Disable watchdog	Watchdog
2034	Update registry	Registry

6.3.3 `appOps` (3000-3999)

Application Operations (`appOps`):

3000	Map a service to a database	Mapping
3001	Unmap a service from a database	Mapping
3002	Unmanage a service	Mapping
3003	Update time period	TimeLearning
3004	Commit time learning	TimeLearning
3005	Learn statement	StatementLearning
3006	Blacklist statement	StatementLearning
3007	Update database configuration	Database
3008	Terminal session started	Terminal
3009	Terminal session ended	Terminal
3010	Terminal session not authorized	Terminal
3011	Terminal session not authorized for tail	Terminal

6.3.4 `uiCalls` (4000-4999)

UI Route Details (`uiCalls`):

Code	Message
4000	UI route logs

6.3.5 cliCommands (5000-5999)

Command Line Interface Command Details (cliCommands):

Code	Message
5000	CLI command run
5001	CLI command failed

6.3.6 ldapAuth (6000-6999)

LDAP Authentication (ldapAuth):

Code	Message
6000	Ldap authentication logs

6.3.7 aclOps (7000-7999)

Access Control List Operations (aclOps):

Code	Message
7000	Access control list
7001	Access control list debug

6.3.8 certOps (8000-8999)

Certificate Operations (certOps):

Code	Message
8000	Certificate debug
8001	Certificate being used
8002	Certificate has been verified