**MySQL Audit Control Policy (NIST AU-2)**

1. MySQL Audit Function Install/Configure (next section) shall be implemented for each identified target system.
2. All events will be audited (logged) for each occurrence of the event.
3. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
4. Auditable events are deemed to be adequate to support after-the-fact investigations of security incidents since each and every event is logged.
5. All events shall be enabled as being audited and logged. Audit logs shall be reviewed once per week by the security operations team. Any event which requires investigation shall kick-off an audit log review by the aforementioned team.

**MySQL Audit Function Install/Configure (NIST AU-2)**

1. Copy audit\_log.so to /usr/lib/mysql/plugin
2. In a connected and logged-in mysql prompt, run the following:

install plugin audit\_log soname ‘audit\_log.so’;

Expected response:

Query OK, 0 rows affected (0.03 sec)

1. In a connected and logged-in mysql prompt, run the following:

Show plugins;

Expected response (near the bottom):

| audit\_log | ACTIVE | AUDIT | audit\_log.so | GPL |

46 rows in set (0.00 sec)

1. Add the below line to /etc/mysql/mysql.conf.d/mysql.cnf and save the file:

audit\_log\_file = /var/log/mysql/audit.log

1. Restart MySQL:

sudo systemctl restart mysql

1. In a connected and logged-in mysql prompt, run the following:

mysql> show global variables like ‘audit%’;

Expected result (or similar):

+---------------------------+-------------------------+

| Variable\_name | Value |

+---------------------------+-------------------------+

| audit\_log\_buffer\_size | 1048576 |

| audit\_log\_file | /var/log/mysql/audit.log |

| audit\_log\_flush | OFF |

| audit\_log\_format | OLD |

| audit\_log\_handler | FILE |

| audit\_log\_policy | ALL |

| audit\_log\_rotate\_on\_size | 0 |

| audit\_log\_rotations | 0 |

| audit\_log\_strategy | ASYNCHRONOUS |

| audit\_log\_syslog\_facility | LOG\_USER |

| audit\_log\_syslog\_ident | percona-audit |

| audit\_log\_syslog\_priority | LOG\_INFO |

+---------------------------+-------------------------+

12 rows in set (0.00 sec)

1. Connect to the database and perform a query to test the audit.log function:

mysql> use GroupProj;

Database changed

mysql>select \* from GroupProj.Angola;

------------------------

7 rows in set (0.00 sec)

1. Check /var/log/mysql/audit.log for capture:

# sudo cat /var/log/mysql/audit.log

Result:

<AUDIT\_RECORD

NAME="Query"

RECORD="69\_2020-11-21T01:59:59"

TIMESTAMP="2020-11-21T02:12:05Z"

COMMAND\_CLASS="select"

CONNECTION\_ID="8"

STATUS="0"

SQLTEXT="select \* from GroupProj.Angola"

USER="root[root] @ localhost []"

HOST="localhost"

OS\_USER=""

IP=""

DB=""

/>