STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Highly Restricted

Title:	**TRE Event Log Management**
Effective Date:	**07 Jun 2019**
Reference Number:	**SOP-09-04**
Version Number:	**1.4**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**07 Jun 2021**

Table of Contents

1. Purpose 3

2. Scope 3

3. Responsibilities 3

4. Procedure 3

4.1. Virtual Workstations 3

4.2. Monitoring and Auditing Event Logs 3

4.3. Secure storage of Log Files 4

5. Cross-referenced ISMS Documents 4

6. Appendices 4

1. Purpose

This document describes the procedure for configuring, enabling, monitoring, storing and retrieving log files containing important event information corresponding to TRE infrastructure assets.

2. Scope

Events logged on virtual machines used by TRE users for data access.

Events that are logged on TRE user end-points, and TRE infrastructure that is not connected to the internal TRE network is out of scope.

3. Responsibilities

The TRE System Administrator is responsible for:

- Ensuring logging is enabled
- Ensuring log files are duplicated at a remote location
- Reviewing log files
- Informing the Information Security Manager of log content that may require further actions or changes

4. Procedure

4.1. Virtual Workstations

Local event logging on VM instances is performed by the Systemd-Journald service. Each VM instance has the journal logging parameter set to persistent and system events (including service status, logins, sshd connections, kernel message, cron executions) get logged to the journal directory.

A SIEM agent is also installed on each virtual machine. These agents send log files to the TRE SIEM appliance in real-time. The logs are transferred in an encrypted form to prevent tampering. The logging is configured to be conformant to the PCI-DSS SCAP profile. This is checked by generating a SCAP report when each virtual machine is provisioned. These SCAP reports are reviewed by a System Administrator before access is provided.

4.2. Monitoring and Auditing Event Logs

The TRE System Administrator, at least every month, reviews local event logs to check for activity related to the following:

- SSH logins
- User Account additions/ modifications
- System file changes
- Updates
- Service changes (e.g. a restart of sshd.service)

journalctl is used to search and interrogate the journal, with specific FIELD=VALUE type, or the full log can be displayed:

```
$ journalctl
$ journalctl _SYSTEMD_UNIT=sshd.service
$ journalctl -t service sshd
```

auditd is installed on each VM instance to monitor target files. The example below shows part of an auditd configuration. In this example, if a user is added to the system, the subsequent changes to group, passwd and shadow files are logged using auditd.

/etc/audit/rules.conf (log any change/ modification to the listed files)

```
-a exit,always -S unlink -S rmdir
-a exit,always -S stime.*
-a exit,always -S setrlimit.*
-w /var/www -p wa
-w /etc/group -p wa
-w /etc/passwd -p wa
-w /etc/shadow -p wa
-w /etc/sudoers -p wa
```

The logs are reviewed using the SIEM appliance twice weekly and tickets are created for events that require follow up action. Any log activity that might indicate a security incident must be reported to the Information Security Manager immediately.

4.3. Secure storage of Log Files

Journal and audit logs are recorded locally to <host>/var/log and <host>/var/log/journal. The logs are also transferred for storage and management to a remote SIEM appliance. These logs will be retained for the current year + 1 year in accordance with the UoM Records Retention Schedule.

5. Cross-referenced ISMS Documents

NumberNumber	TypeType	TitleTitle
<NO DATA>	<NO DATA>	<NO DATA>

6. Appendices

None