Microsoft Defender

- Linux Configuation

Linux Configuation

The following guide describes how to manually install Defender for Linux

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/linux-install-manually?view=o365-worldwide

Linux commands for Microsoft Defender can be located at:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/linux-resources?view=o365-worldwide

After installing Defender a configuration file called mdatp_managed.json can be used to set the Defender settings This file should be saved in /etc/opt/microsoft/mdatp/managed.

Behaviour monitoring:

sudo mdatp config behavior-monitoring --value enabled

Enable Potentially Unwanted Applications

sudo mdatp threat policy set --type potentially_unwanted_application --action block

Next, cron jobs should be created for scheduled scans. This can been done via:

sudo crontab -e

Copy and paste the below into the editor to define the scans

Microsoft Defender quick scan Monday to Saturday
00 2 * * 1-6 /usr/bin/mdatp scan quick > /var/log/mdatp_cron_job.log
Microsoft Defender full scan on Sunday
00 2 * * 0 /usr/bin/mdatp scan full > /var/log/mdatp_cron_job.log

Exit the editor saving your changes.

If you need to restart the service use

sudo service mdatp restart

Check the health of Microsoft Defender by running

mdatp health