How do schools use HFL Broadband systems when they received an extremist alert

Summary

All HFL Broadband schools should configure to receive extremist filtering alerts. If an alarm gets generated, schools will need to know what to do. This document is a guide for schools to help them carry out steps when an alert is triggered.

It is important to note that the alert triggered may be a ‘false positive’. However, schools will naturally wish to carry out investigation work.

Potential challenges

A challenge may be that schools will not have user-based filtering (UBF) deployed, which means internal systems have not been synced with the SafetyNet filtering platform. If this is the case, you will only see the device IP address that triggered the alert. IP addresses are often dynamically assigned to devices and change frequently. If UBF is not set up, identifying the person who triggered the alert will require immediate action, and even then, this may not be possible. Schools are advised to speak to their IT Support to assist with marrying up the IP address in question, to the school user ID/or failing that, a specific device.

If systems have been synced, school user IDs will hopefully be visible.

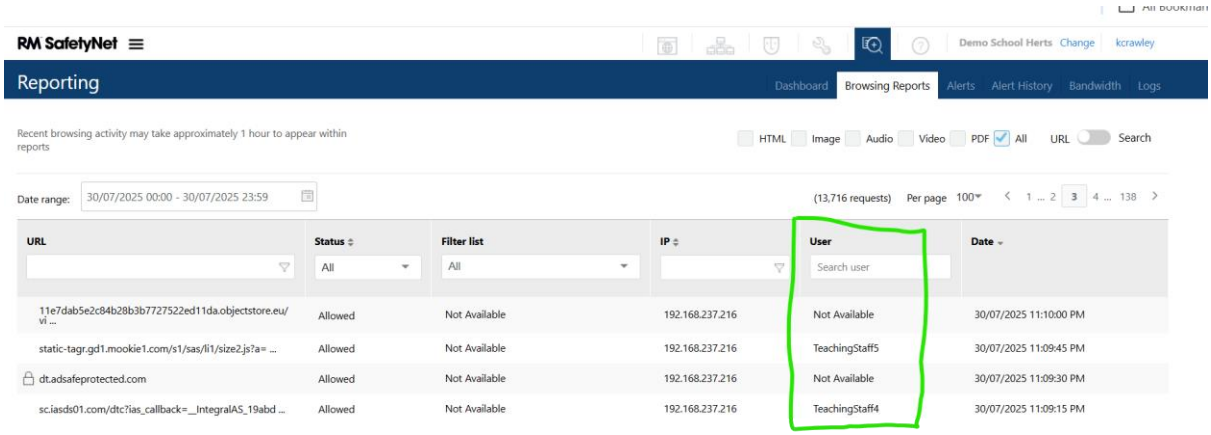
Another challenge is that alerts can also be triggered on the school’s transparent proxy network, which is often used for guest wireless users. As the transparent proxy is segregated from the school’s network, user identification will also be a problematic.

Identifying the individual

On receiving the alert, the school will need to log into SafetyNet to interrogate the browsing reports. To access SafetyNet, schools will need to browse to https://safetynet.rm.com and enter the required credentials. If the school does not have their credentials, then they will need to contact the HFL Broadband Support Team by emailing support@hfleducation.org or by phoning 01438 544466 (option 1 followed by option 2).

Once you have logged into SafetyNet. You should then be able to see 1) The time and date that the activity occurred 2) The internal IP address and possibly the school user ID. If the User ID is recorded, you will be able to carry out the relevant investigations with the person in question.

If you just have the internal IP address, and no user ID, then your IT Support will hopefully help in identifying the user ID or the device the activity occurred from. You will need to speak to them and provide them with the internal IP address and date/time ASAP.



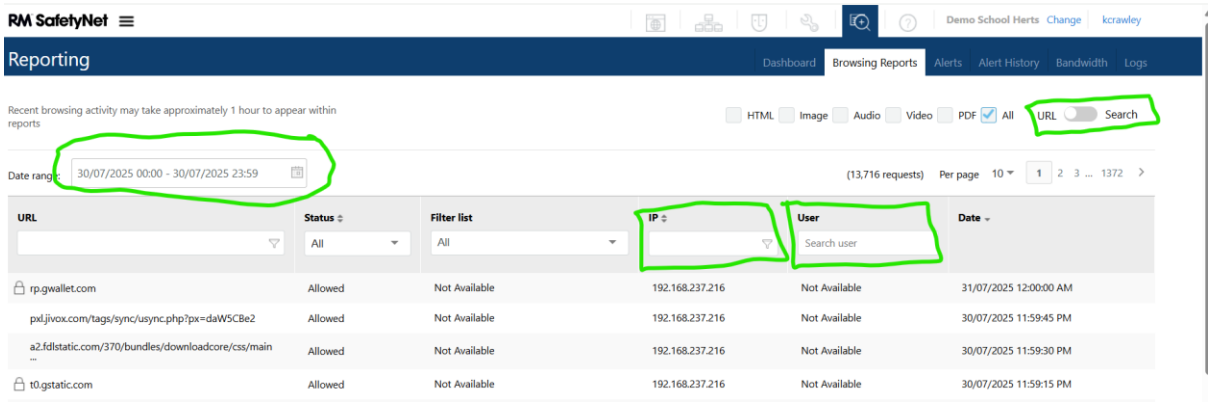
Reviewing the activity

Within the SafetyNet browsing reports, you can use the search fields at the top of the report

to obtain relevant information. We recommend that you to check the activity of the IP address/username immediately before and after the alert was triggered, by entering their IP address or username into the fields.

You can also update the date and time you are looking at. This should help put together a picture as to what the user's motives were. There will be false positives.

Please note that when using the browsing reports tool in RM Safetynet, lots of activity is recorded. The more specific you can be in the search fields, the more the returned data will be relevant. At the top right-hand corner you can now, move the slider across from 'URL' to 'Search'. The report will then provide details of internet searches the user/IP address has looked up, rather than listing all the URLs accessed. This can often be insightful.



Advice

Should you have any further queries, please contact the HFL Broadband Support Team.