ClearView Pattern Matching

CyberHound's ClearView platform gives schools the ability to detect 'at risk' or inappropriate behaviour. The unique platform analyses communications and search activity. This provides behavioural analysis to key staff, enabling support to be provided to students.

The platform also helps detect risks such as cyberbullying and can provide data to help identify issues of self-harm risks that can then be dealt with quickly and effectively.

Flexible Deployment

The platform is supplied with pre-defined policies that have been created over many years in consultation with schools, in-house experts and professional specialists such as psychologists.

Additional custom policies can be created. These can cover district specific content or additional languages. The platform supports any language and character set.

Exclusions are also recommended to prevent false positive reporting. CyberHound can provide default exclusion lists and ongoing recommendations to enhance these.

Default Policies

The standard policies are:

- Self-harm
- Eating disorders
- Radicalisation
- Aggression
- Extreme profanity
- Mild profanity (recommended for primary schools)
- Drugs
- Religious slurs
- Predatory behaviour
- Racism
- LGBTI slurs
- Bomb making

Many schools also create a custom rule as a "watch list" to add students if they demonstrate a need to watch more closely.

Metadata Reporting

CyberHound presents comprehensive metadata to users or to reporting platforms such as Splunk for presentation to executives within the school or district. The metadata captured includes:

- Platform used for communication / search
- User details from the platform
- User's profile URL
- Unique identifier of the user from the platform
- Email address (Office 365 or Gmail)
- User's display name
- User name from the proxy
- IP address of the device used
- Policy breached (i.e. name of the breach)
- Policy action taken
- Time stamp
- Body of the content that breached the policy
- Recipient details for the communication

Behavioural Analytics Policy Granularity

Policies can be set up flexibly to enable a district to provide flexible use of the policy engine. This can combine variables such as time of day, communication type or group. The platform can even provide granular policy enforcement within a platform – e.g. only focusing on Facebook messages and not wall posts, if required.

Supported Communication Types

ClearView has been built to scan the common communication or search tools used by students. It gains much information from this and does not need to support every form of internet-based activity to provide real-time behavioural analytics to enhance Cybersafety and student wellbeing.

Platforms supported are:

- Facebook
- Gmail
- Google search
- YouTube search
- Office 365 (school or district account email)
- Bing search
- Yahoo search
- Twitter

Within these platforms, CyberHound supports multiple communication types. I.e. within Facebook the platform covers wall posts, private messages, status updates, friend requests, etc.

Scanning of HTTPS and encrypted traffic from the above platforms is fully supported. This requires the implementation of a supported decryption environment and client security certificate on each device on the network.

CyberHound provides schools with the ability to optimise and manage their internet services. We help students engage in new forms of learning and help teachers confidently use digital content and resources without the worry of access, internet speed or reliability. For 17 years CyberHound has developed the most comprehensive learning enablement and cybersafety solution for schools and is now the benchmark for schools in Australia and internationally. CyberHound is part of the BigAir Group (ASX: BGL).

T 1300 737 060
E info@cyberhound.com
W **cyberhound.com**