What is Police CyberAlarm?

Police CyberAlarm is a free tool to help members understand and monitor for potential malicious activity. This service is made up of two parts; monitoring and vulnerability scanning.

Police CyberAlarm acts like a “CCTV camera” monitoring the traffic seen by a member’s connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities. The data collected by the system does not contain any content of the traffic. The system is designed to protect personal data, trade secrets and intellectual property.

Members of Police CyberAlarm will become part of the wider UK cyber defence network, sharing collected data with Police for analysis at local, regional and national levels to identify trends, react to emerging threats and identify, pursue and prosecute cyber criminals.

Vulnerability Scanning can be added and used to scan an organisations website and external IP addresses, providing regular reports of all known vulnerabilities.

How Does Police CyberAlarm Work?

Police CyberAlarm members are required to install a ‘Police CyberAlarm Virtual Server’ on their systems which will be used to collect and process traffic logs identifying suspicious activity from their firewall/internet gateway. Police CyberAlarm Virtual Server is easy to install using the downloadable virtual appliance, offering one-click installation.

Once a Police CyberAlarm Virtual Server has been installed it will securely collect, encrypt and send the suspicious activity data to the central servers allowing it to be analysed. The data sent only includes metadata (logs) relating to the suspicious activity from internet facing gateways such as Firewalls. The Police CyberAlarm system will scan the member organisations website and external IP addresses sending regular reports of any known vulnerabilities.

Data collected is used to create regular reports on suspicious and potentially malicious activity seen by individual members, as well as reports identifying threat trends seen across the member network. Members can use this reported intelligence to update their defences to better protect themselves from cyber threats.

This data is also used by the Police to evaluate and track trends in cybercrime and take enforcement action where appropriate. Police CyberAlarm will help organisations to Prepare for and Protect against cyber threats and will support the Police in Pursuing and Prosecuting cyber criminals.

Police CyberAlarm was implemented with ease and provides essential proactive intelligence of external cyber security threats. With the regular reporting received from Police CyberAlarm, we are now equipped to secure against any new vulnerabilities as they are detected.

Gordon Perkins LGSS | Northamptonshire County Council
Police CyberAlarm Member Benefits

**Regular Reporting**

Member organisations who join Police CyberAlarm receive regular reports detailing suspicious and potential malicious activity seen by their firewalls/internet gateways. These reports can then be used by members to further investigate issues, update security configurations and deliver training where needed.

**Intelligence Feeds**

Data from the Police CyberAlarm system is used to provide feeds detailing the latest threats discovered across the member network, giving all members the ability to update configurations and other security measures to better protect against future cyber threats.

**Vulnerability Scanning**

Police CyberAlarm vulnerability scanning can be used to scan an organisation's website and external IP addresses for known vulnerabilities. These regular reports can increase an organisation's cyber security and help protect from known suspicious activity vector's.

**Increase Efficiency of Evidence Gathering**

As Police CyberAlarm provides details to the Police automatically, evidence from internet facing logs will be in the Police’s possession prior to an incident being reported. This can help both the Police and victim organisations to progress investigations more quickly.

How Members Help the Police

**Continuous Reporting**

Through regular reporting, Police CyberAlarm provides customisable views of local, regional and national cybercrime incidents and trends. This reporting allows Police Cybercrime Units to adapt their support to meet the emerging threats as they evolve.

**Active Intelligence**

Police CyberAlarm also allows Police to supplement the suspicious activity data, gathered by Police CyberAlarm, with Open Source Intelligence (OSINT) to aid investigations and prosecutions of cyber criminals. This capability is also used to allow individual forces to identify local attacks on local victims which can then be dealt with more swiftly.

**Staying Ahead of the Criminals**

By using the data provided by Police CyberAlarm members, Police are able to stay up to date with both the latest threats and potentially emerging threat actors. This will allow officers to be better informed when engaging with organisations and members of the public, offering more relevant guidance on how to protect from cyber threats.

cyberalarm.police.uk

The report we receive from the Cyber Alarm has been invaluable, not only are we able to block IP's attempting malicious attacks, it also helps inform our Board of Directors of the scale of the problem in a non-technical way. This ensures that resources within the business can be directed proportionately and appropriately.

Nicola Petts Group IT, IG, Vendor Manager | Christchurch Group