Police CyberAlarm FAQ Sheet

What data does Police CyberAlarm Collect?

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

The data sent only includes metadata (logs) relating to the suspicious activity from internet facing gateways such as firewalls. They are simply logs about how data was sent/received through your internet gateway (IP Addresses for external connections, amount of data transferred and the port used to process the data, date and time).

The Police CyberAlarm system can also scan the member organisation's website and external IP addresses sending regular reports of any known vulnerabilities.

What is included in the reports?

Police CyberAlarm reports summarise suspicious traffic and potential attacks, visible to your organisation, from the internet. Details include the top sources and the ports malicious users are using for their attacks against your systems.

The data is split between attacks originating from attackers in the UK and those from outside the UK.

Reports show member organisations how they are being attacked, and by whom, so that they can better protect themselves. We aim to work with member organisations to ensure that they are making the most of the data collected. If there is a breakdown of data that would be beneficial to members then please get in touch.

How is Police CyberAlarm Installed?

There are two options available for the installation of Police CyberAlarm:

- VMWare Virtual Appliance - simply copy and paste the provided URL into VMWare's management console.
- As a software installation on a Linux device - requires CentOS 7 Minimal on either a physical or virtual device.

Full instructions are provided once you receive your code to join Police CyberAlarm.

Who has access to the data collected?

The data collected by Police CyberAlarm is viewable only by police, police staff and when authorised or required to do so by law to select third parties.

What will the police do with the data I send them?

Data received by the Police CyberAlarm central server is used to create regular reports on suspicious and potential malicious activity seen by individual organisation, as well as reports identifying threat trends seen across the organisation's network. Organisations 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. Helping police to; Prepare and Protect organisations, Pursue and Prosecute cyber criminals. Making the UK secure and resilient to cyber threats, prosperous and confident in the digital world.

What is suspicious activity?

Police CyberAlarm identifies suspicious activity as network traffic which is blocked by the member organisation's firewall or that is believed to be unwanted. This will include activity where the suspect is attempting to scan for vulnerable ports or making repeated attempts to gain access to an organisation's system using known attack methods.

What restrictions will be placed on the use of such data?

Only communications data pertaining to suspicious activity will be collected and, to the extent that any data is mis-identified, this will not be stored and will be erased as soon as possible. Restrictions will be imposed in relation to the use of data collected to ensure compliance with legal obligations.

Police CyberAlarm FAQ Sheet

How long will Police CyberAlarm store the data for?

Logs collected by the Data Collector are analysed by the collector as they are received to remove any obviously non-malicious logs. These events are not sent to the Central Server. Once logs arrive at the central server they are analysed within minutes (even seconds) of the event being received by the collector, both individually and against the Central Server, to determine if these logs are malicious.

For example, a log which is a request to connect using port 3389 may be deemed as non-malicious. However if the Central Server correlates that the same IP address made rejected requests to port 3388, 3387, 3386, etc. then this would become part of a potentially malicious port scan.

Any log which, following analysis, at both the Data Collector and the Central Server is still deemed to be non-malicious within 24 hours of arrival at the Central Server will be deleted.

The maximum amount of time that a non-malicious log is within the system would be circa 24hours. However, in order to allow for circumstances such as maintenance or system updates, the maximum time the logs may be kept is up to 5 working days before deletion.

If a log file, deemed as suspicious, has no further activity within a 9 month period the relevance of the data is reduced and its retention is no longer considered to be necessary or proportionate. All suspicious logs collected by the system are deleted on a 9-month cycle.

Why does anything need to be installed onsite?

The log messages from internet facing devices are not encrypted. To ensure security Police CyberAlarm installs a small collector on your network. Typically this would be installed within your DMZ to gather the data from suspicious and or malicious traffic. The data is then encrypted and compressed before being securely transmitted to the Police CyberAlarm central processing servers.

Does Police CyberAlarm need to be installed on every device in the organisation?

No, Police CyberAlarm is a stand-alone system which sits in its own server environment. The collector gathers and encrypts the suspicious data from your internet gateway before sending it back to the central Police CyberAlarm processing servers. No software need be installed on any other devices and multiple gateways can feed data to a single Police CyberAlarm collector.

How does Police CyberAlarm handle VPN/encrypted bits of traffic?

As Police CyberAlarm does not collect any of the transmitted data, encrypted data and VPN traffic has no impact on the ability of the Police CyberAlarm system to collect metadata of suspicious traffic.

Does the Police CyberAlarm system take any action to prevent attacks?

Police CyberAlarm is a monitoring system and as such does not interfere with any of the traffic on your internet gateways.

Responsibility for decisions on how to action any reported data is solely owned by the member organisation.