POLICE

CYBERALARM

Helping organisations monitor and report the malicious activity they face from the internet

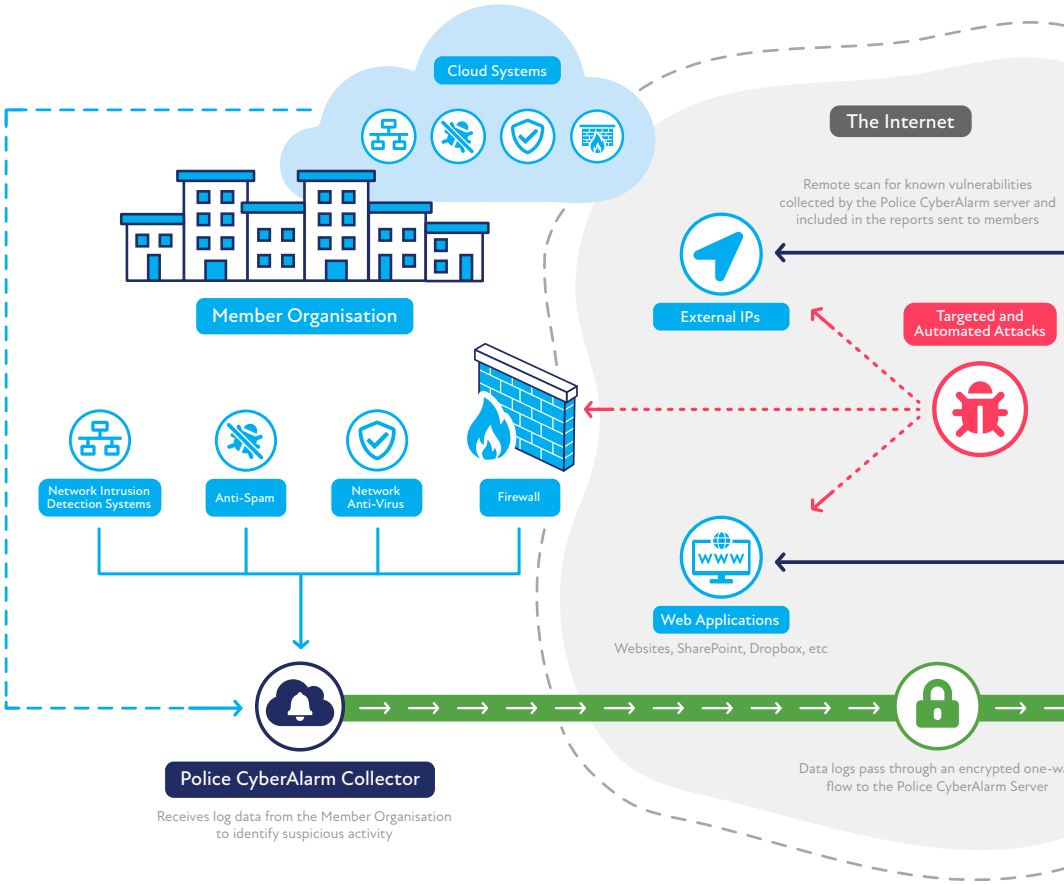
Become a member by registering online at cyberalarm.police.uk

What is Police CyberAlarm?

As a member, Police CyberAlarm is a **FREE** tool to help you understand and monitor malicious cyber activity against your network. This service is made up of two parts: monitoring and vulnerability scanning.

Police CyberAlarm will detect and provide regular reports of **SUSPICIOUS CYBER ACTIVITY,** enabling your business or organisation to identify and take steps to minimise your vulnerabilities.

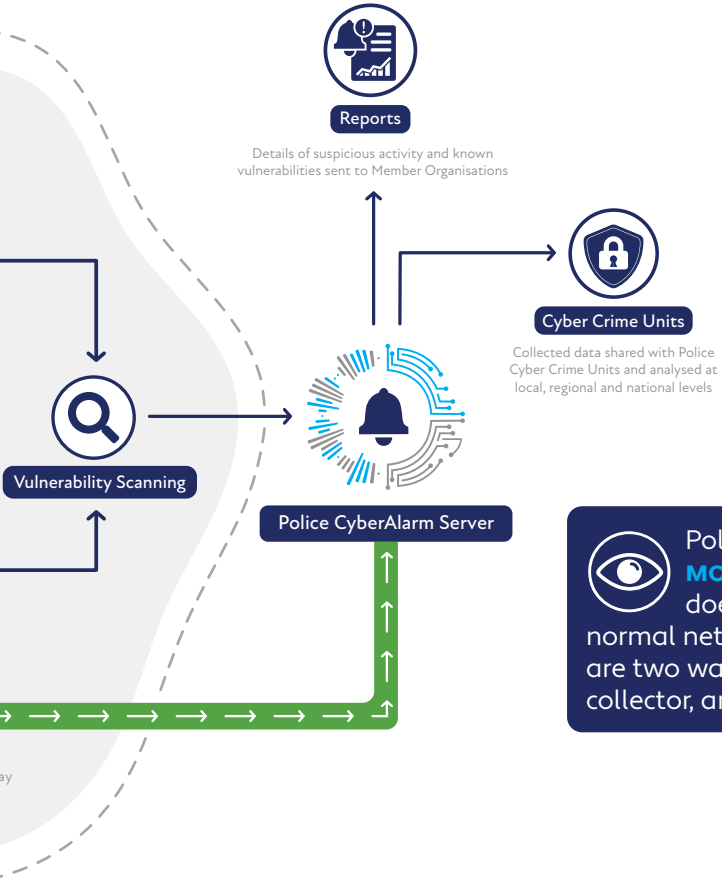
The data collected by the system only contains summary information (meta data and header information) about communications your business or organisation receives from the internet. The system is designed to **PROTECT PERSONAL DATA,** trade secrets and intellectual property.



Check out our FAQs on the Police CyberAlarm website

FREE
TOOL FOR YOUR BUSINESS

Once you become a Police CyberAlarm member you install a virtual or physical **'POLICE CYBERALARM COLLECTOR'** which is used to collect and process traffic logs to enable the identification of suspicious and malicious activity from any of your firewall/internet gateway, Network Intrusion Detection/Prevention system (IDS/IPS), Network Anti-Virus and Anti-Spam filters.



Police CyberAlarm is a **MONITORING SYSTEM** and does not interfere with normal network operations. There are two ways to install the data collector, and both are easy to do.

Network Anti-Virus Scanning

What is it?

Files sent through the internet can sometimes **CONTAIN VIRUSES** that are designed to install malware on the recipient's device. Most organisations will install Anti-Virus (AV) software on their desktop computers and laptops to protect their users, however this does not protect other devices such as switches and routers.

Network AV provides an additional **LAYER OF PROTECTION** for users as well as protecting network devices and other systems that do not have AV software installed. These systems reconstitute the original data item being sent in order to scan it for malicious computer code.

How will it help protect my business?

The logs from these devices can be used to monitor the types and source of virus entering your network and identify the steps needed to further protect from these sources and **IMPROVE YOUR CYBER SECURITY** position.

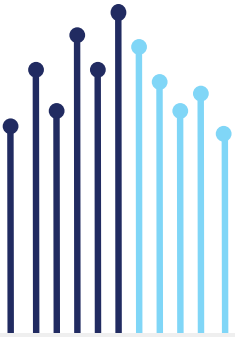
ANTI-VIRUS LOGS contain information about the source of the email and the IP address of the intended recipient, as well as the message subject and attachment name but do not contain the body of any communication.

Network Intrusion Detection Systems & Intrusion Protection Systems monitoring

What is it?

Whilst **FIREWALLS BLOCK MALICIOUS TRAFFIC** at the internet gateway based on rules defined by a network administrator, many organisations add a further security layer by monitoring their own networks for suspicious activity using Network Intrusion Detection Systems (IDS) and Intrusion Protection System (IPS) devices.

These systems inspect packet-level data which has been allowed by your organisation's firewall device. The rules that NIDS/IPS use to determine if data is wanted or not are more complex than a firewall and include threat intelligence feeds of **KNOWN BAD SOURCE** IP addresses as well as inspection of the whole packet, not just the header.



How will it help protect my business?

Collecting and analysing this data highlights traffic that may be allowed through the firewall but which is likely malicious, allowing member organisations to further **IMPROVE THEIR CYBER SECURITY AWARENESS** and security posture.

The logs sent to Police CyberAlarm contain the source and destination IP address of the traffic, and a summary of the access attempt.

Anti-SPAM

What is it?

Anti-SPAM systems catch malicious traffic that Network Anti-Virus scanning, Network Intrusion Detection Systems (NIDS) and Intrusion Protection Systems (IPS) cannot.

Anti-SPAM works with email in a similar way to Network AV, rebuilding the original data and **SCANNING IT** rather than inspecting packets.

How will it help protect my business?

Member organisations can share logs relating to the potentially malicious emails with Police CyberAlarm, where the logs can be analysed and reported.

The logs sent to Police CyberAlarm contain information about the **SOURCE OF THE SUSPECTED SPAM**, the email address of the intended recipient, the subject line and attachment name but not the body of the email. Anti-SPAM logs will reflect emails which have been blocked before reaching the end user, and will therefore not include information about emails which reach the end user but are diverted to a 'Junk' folder.

Signing up to provide information about these logs gives Police CyberAlarm the ability to collect information on attempted attacks which could be targeting your organisation via email.

Vulnerability Scanning

What is it?

Police CyberAlarm Vulnerability Scanning can be used to scan an organisation's website URLs and external IP addresses for known vulnerabilities. These regular monthly vulnerability scans helps to **KEEP YOUR NETWORK SAFE** by identifying new threats that your external IPs and website URLs may face.

How will it help protect my business?

In order to scan for vulnerabilities the Police CyberAlarm system will **SCAN YOUR URLS AND IP ADDRESSES** to identify which services they allow requests to, for example if the system is a web server then it will allow web requests. The scanner software next attempts to identify the software and version on your system that is providing the service and compares these to international databases of registered security vulnerabilities and, where possible, tests to check if your organisation is vulnerable. These reports can increase an organisation's cyber security by helping protect from common vulnerabilities.

Every registered security vulnerability has a unique Common Vulnerability Exposures (CVE) code which can be used to look up the systems and versions affected by the vulnerability, its severity, as well as information on how best to mitigate and remediate the vulnerability. Police CyberAlarm scans periodically to provide reports on new vulnerabilities that have been discovered for your organisation's systems and, where possible, **PROVIDES INFORMATION** from the CVE data to help your team remediate the vulnerability.

Firewall

What is it?

A Firewall is an **IT NETWORK DEVICE** and is a usually the first bastion of protection against internet threats, it is a very simple technology that blocks or allows data based on pre-determined rules defined by your system administrator.

The rules are based on basic information in the “header” of each packet such as the source address, destination address and the port that the data is being sent via, by only using information in the header, firewalls are very fast and add almost no delay to the transmission.

How will it help protect my business?

A firewall blocks the majority of unwanted and malicious requests from the Internet, so it is vital that Police CyberAlarm collect and analyse the logs from firewall devices.

The logs provide information about what access was attempted, when and by what device. From this information we are not only able to **DETECT** whether an event could be suspicious, but also **DETERMINE** where it came from and how it tried to access your network.

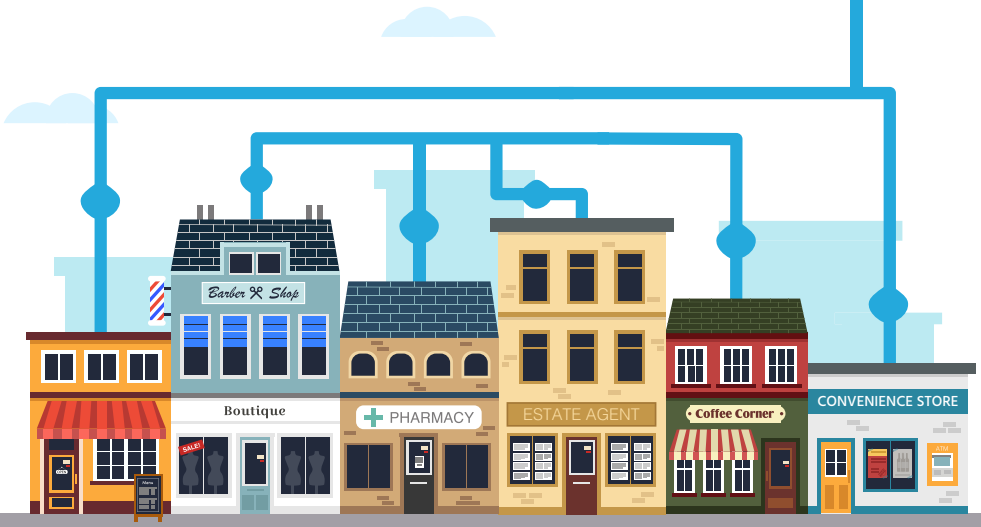
What information does Police CyberAlarm collect and how is it used once collected?

The Police CyberAlarm Data Collector installed on your site first **IDENTIFIES SUSPICIOUS DATA** and by doing so automatically filters out any internal traffic and data from known trusted sources.

The remaining data is then **ENCRYPTED** and transmitted to the Police CyberAlarm servers where it is collated, verified, analysed and shared between police forces allowing them to identify new trends, patterns, and cyber-attacks.

It is also then possible to identify whether there are **REPEATED TRENDS OR PATTERNS** on particular services, products, or devices. This information can be used to inform advice and guidance to member organisations and others, as well as to enable the police to take enforcement action.

Each member organisation will benefit from their own report which will include the identification of the new trends and attacks allowing them to better defend themselves against such attacks.



How will it help protect my business?

The data collected by the Police CyberAlarm system does not contain the body of communications. There is no risk to personal data, trade secrets or intellectual property.

By becoming a Police CyberAlarm member, not only are you helping to protect your business, you are also helping the police to build a bigger picture of the extent of malicious cyber activity locally, regionally and nationally. Police are able to stay up to date with both the latest threats and identify potential cyber criminals.

Benefits to Member Organisations

Reporting

Members benefit from regular **INTELLIGENCE REPORTING**, through their 'Member Summary Threat Report', summarising suspicious activity detected in the external traffic logs sent to their Police CyberAlarm collector.

In addition to this report, members who opt in for vulnerability scanning will also receive a 'Vulnerability Assessment Report'. This report details **ANY KNOWN POTENTIAL VULNERABILITIES** and the CVE codes for those vulnerabilities to help better protect the organisation.

Regular Reporting

All members will receive regular reports that contain analysis of their own data, including advice on how to address suspicious cyber activity being reported by their security devices.

Threat Intelligence

As the scheme continues to grow, members will receive reports of regional and national threats and trends identified by Police CyberAlarm.

Vulnerability Analysis

Members who choose to have their cyber assets digitally scanned for vulnerabilities will receive a full breakdown of any issues found.

Helping Police

All members contributing data to the scheme are doing so knowing that they are helping UK Police to build a better picture of cyber threats and will receive a digital member badge.

MEMBER
POLICE
CYBERALARM

- Sign up online at cyberalarm.police.uk
- Complete online registration
- Install Police CyberAlarm Collector
- Forward Firewall Traffic Logs
- Receive Member and Threat Reports

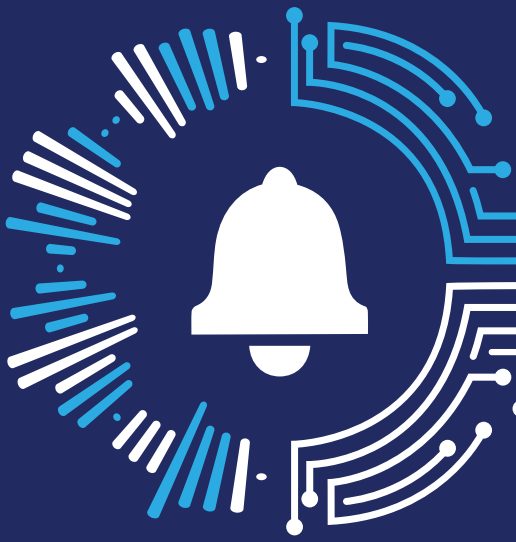
For more information about Police CyberAlarm and the data it collects check out our FAQs

cyberalarm.police.uk

You can also keep up to date with the latest news about PCA and threats by following us on social media:

@policecyberalarm

@PolCyberAlarm



NPCC
National Police Chiefs' Council

Become a member by registering online at cyberalarm.police.uk