Police Cyber Alarm - A review

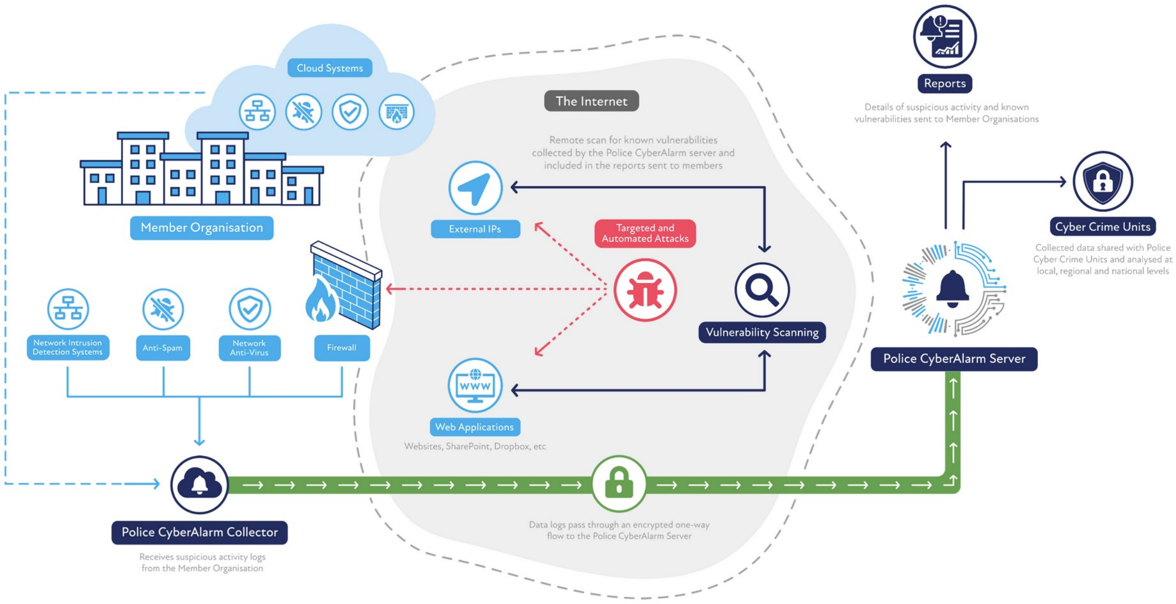
Introduction

The Police CyberAlarm (PCA) service is funded by the Home Office and developed by Pervade Software. Originally designed for small businesses, the PCA service is now being recommended to schools as part of their cyber security regime. If, for example, a school uses the government's Risk Protection Arrangement (RPA) for its insurance, one of the conditions for the Cyber Insurance element is that members register with the PCA (See Section 14, Conditions of Cover [3], p109).

The PCA service consists of an on-site "Data Collector" (DC). The DC gathers logs from the network's internet gateways (typically firewalls), encrypts and then transfers them to the central CyberAlarm (CA) server. The CA server analyses the logs and returns reports to the site. No proactive measures are taken, but the reports may provide information that would be useful in, for example, hardening the firewall rules against known threats.

As well as the monitoring service PCA also provides vulnerability scanning of external IPs and public-facing web applications.

The information gathered is shared with the Police Cybercrime units and used to monitor the scale of threat nationally and inform their policies


Cloud Systems
Member Organisation
Network Intrusion Detection Systems
Anti-Spam
Network Anti-Virus
Firewall
Police CyberAlarm Collector
Receives suspicious activity logs from the Member Organisation
The Internet
Remote scan for known vulnerabilities collected by the Police CyberAlarm server and included in the reports sent to members
External IPs
Targeted and Automated Attacks
Vulnerability Scanning
Web Applications
Websites, SharePoint, Dropbox, etc
Data logs pass through an encrypted one-way flow to the Police CyberAlarm Server
Reports
Details of suspicious activity and known vulnerabilities sent to Member Organisations
Cyber Crime Units
Collected data shared with Police Cyber Crime Units and analysed at local, regional and national levels
Police CyberAlarm Server

Source: https://www.cyberalarm.police.uk/assets/img/pcs_diagram.png

Installation

In order for a school to use the Police’s free CyberAlarm tool, they must first register and note the registration code before downloading the Data Collector server and installation instructions. Once the DC has been installed, it must be registered with the remote CyberAlarm server using the registration code previously noted.

The DC comes in two versions: pre-installed on a VMWare Virtual Appliance, or the software can be downloaded and installed on hardware or virtualisation system running CentOS 7.

The installation notes suggest that the DC is installed a DMZ but do not emphasize the point. Our view is that while this may be desirable, many school networks do not have either the system or expertise to set up a DMZ.

Suitability

The fact that the PCA was initially designed with SMEs in mind has resulted in a design decision that makes the PCA tool unsuitable for large aggregations of schools (school trusts, RBCs, Local Authorities, etc.). The PCA relies on the ability of the DC to be sent logs from a local internet-facing device. Schools within a WAN (e.g. those using an RBC or LA network) do not have their own public IP address, so the “source” of all requests to their Gateway device will be a private IP within the WAN and unsuitable for analysis by the central CA server.

If a DC is installed at the RBC or LA level (i.e. within the aggregator’s network), then the activity reported on will be against the external IP of the aggregator and not of the individual school rendering the value of the report moot.

If a school has public IP and its own internet-facing Gateway or Firewall, it will fall into the PCA expected use case and may provide some valuable security information.

Use

Once configured, logs can be exported to the DC from internet-facing devices. In most cases, this will be the local firewall but may include, for example, internet-facing proxies, web servers or web-filtering systems.

Some filtering of the logs is performed before being exported to the central CyberAlarm server for analysis: log lines with internal source addresses will be deleted, as will messages deemed to be non-malicious. The PCA program is only interested in external traffic: i.e. with a source IP is outside the local network.

For security, the logs are encrypted (256bit AES) before being transferred to the central server where they are analyzed. Requests which are deemed non-malicious are deleted within 24 hours. Lines that appear suspicious, but have no further linked activity, are deleted after six months. There is more information in the CyberAlarm Tool Privacy Policy.

The data collected does not contain any organizational data and "*is designed to protect personal data*, *trade secrets and intellectual property*" (source). It does, however, include IP addresses, ports, the amount of data transferred, and timestamps that could potentially identify users. The Privacy Policy provides more detail on the data collection and processing legalities.

What data is transferred to PCA?

There is little on the PCA website to indicate exactly what data is uploaded to the central server, but some assumptions can be made. Firstly, lines containing an internal *source* address will be removed. Secondly, those log entries which are not deemed suspicious are also removed. This leaves those lines that are, or may be suspicious to be uploaded in their entirety: this may include IPs (external and internal), ports, timestamps, data quantities, and any other information embedded in the logs supplied. It would be sensible, therefore, to audit any logs that a site is considering sharing with the PCA to check that no requests from external IPs contain information that could readily identify a user.

The removal at the local DC level of lines "not deemed to be potentially malicious activity" begs the question of what is deemed potentially malicious if the point of the CyberAlarm is to use the data collected nationally to discover such activity? Will removing these entries locally, i.e. before transmission to the Central Server, hinder the search for new, malicious requests?

The CA website states that "*Police CyberAlarm identifies suspicious activity as network traffic which is blocked by the member organisations 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.*"

Is this useful for most schools? If the activity is already blocked, then what else can be done? How useful is it to know you have been scanned if all ports that are not required are already blocked? Finally, only "known attack methods" are being identified as suspicious, which raises the question of how up-to-date this database of known threats is, how often it is updated, and by whom. And how is traffic "*believed to be unwanted*" defined?

What is reported?

Few details are provided on what the reports consist of, and there are no examples or screenshots on their site. This FAQ states that the reports summarize suspicious activity, including the top sources and ports that malicious actors are attempting to use to attack the network. The reports are divided into suspicious activity originating from within the UK, and from outside the UK. The report may be a simple list of IPs and ports, but no further details are provided.

One RBC has installed a DC for testing purposes but has, at the time of writing (May 2022), not had any CyberAlarm reports back, so there may be issues with the reporting mechanism.

Security concerns

Since the Police CyberAlarm was launched in 2020, several reports of lack of security in CyberAlarm software itself have been reported. In particular, Paul Moore has been a consistent critic of CyberAlarm's security, first raising issues in a blog post (24/11/2020) where he highlighted various flaws. The NPCC disputed the claims, and it turned out that the wrong link was posted on the CA site so that a development version was downloaded instead of the production one. Paul Moore posted a new blog (02/12/2020) where he explained the issue and re-tested the live version where he found many of the same flaws, although some had been addressed. In a recent post (19/04/2022), Paul Moore again re-tested CyberAlarm and contends that there are issues that still need to be addressed. This to-and-fro has been picked up in The Register, TechMonitor and ITPro. Whether it was because of these reports or not, the NPCC published a tender notice for a new supplier to further develop CyberAlarm, as reported in TheRegister, March 2021.

Throughout this saga, the NPCC has disputed the majority of Paul Moore's findings and insists that the product is secure and has been tested by other independent organizations quoting both Prism Infosec and Arcanum on the PCA site.

A more recent statement (14/06/22) from Bytes Software Services Ltd is available on the Police Cyber Alarm site and is worth reading in full. Byte was engaged to review all the security issues raised by Paul Moore (referred to throughout the statement as the "security researcher") and provide an independent view on their validity and seriousness. In summary, Byte found that the issues that were raised were valid but that the "defence-in-depth model" of the system mitigated the potential of any attack. In particular they note that "*The lower risk identified by the DFIM team was found to be due to* ***additional security controls*** *and backend security measures that the* ***security researcher had no ability to see or test*** *from the collector. Without the additional context being available, these risks would always appear higher.*" (our emphasis).

Summary

The Police CyberAlarm service is provided via a downloadable Server (the "Data Collector") available either as a virtual appliance (VMWare) or software that can be installed on hardware or other virtualization system running CentOS 7. In either case, the server will need to be installed on the local network (preferably in a DMZ) so that internet-facing devices can forward their logs to it.

As currently configured, CyberAlarm is **not** appropriate for schools that do not have a direct internet connection or public IP address (e.g. schools that connect to the internet via their LA's private network infrastructure).

Once installed and registered with CyberAlarm, logs are sent to the Data Collector, which removes lines deemed not to be suspicious, encrypts the remainder and forwards them to the Police's central CyberAlarm server for analysis. Only inbound traffic is collected: all lines with a source IP within the local network are discarded. It is also important to note that no content is collected, only details of the connection itself.

Any suspicious activity discovered from the analysis is reported back to the site so they can take the action necessary to prevent or mitigate further attempts. The data collected is used to build a national profile of malicious activity and support the Police in tackling Cybercrime with non-malicious data deleted within 24 hours or, if it was originally classified as suspicious but with no further linked events, after six months.

For schools using, or wishing to use, the government-backed Risk Protection Arrangement Cyber insurance scheme, registration with CyberAlarm is a requirement. Registration with CyberAlarm does not in itself require the server to be installed and used so the insurance will still be available to those sites that do not wish to use, or are unsuitable for, CyberAlarm. However, by registering with CyberAlarm schools can benefit from the Vulnerability Scanning service which may highlight areas where security could be improved.

References

Police CyberAlarm *Home Page*. Available at: https://www.cyberalarm.police.uk (Accessed:12 May 2022)

Police CyberAlarm *Register*. Available at: https://www.cyberalarm.police.uk/register/ (Accessed: 12 May 2022)

Police CyberAlarm *Privacy Policy*. Available at: https://www.cyberalarm.police.uk/cyber-alarm-tool-privacy-policy/ (Accessed: 12 May 2022)

Police CyberAlarm *What data is collected?* Available at: https://www.cyberalarm.police.uk/#faq2 (Accessed: 12 May 2022)

Police CyberAlarm *Funded and Trusted by Police*. Available at: https://www.cyberalarm.police.uk/security/ (Accessed: 12 May 2022)

Department for Education *Risk protection arrangement (LAP) local authority maintained schools (LAMS*). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064042/RPA_membership_rules_LAMS.pdf (Accessed: 12 May 2022)

Moore,P. (24 November 2020) *CyberAlarm: An independent security review... and why you should avoid it*. Available at: https://paul.reviews/cyberalarm-an-independent-security-review-and-why-you-should-avoid-it/(Accessed: 12 May 2022)

Moore, P. (02 December 2020) *CyberAlarm: Testing the "production version"... and why you should avoid it*.Available at: https://paul.reviews/cyberalarm-testing-the-production-version-and-why-you-should-avoid-it/ (Accessed: 12 May 2022)

Moore, P. (19 April 2022) *Police CyberAlarm: Abysmal security, yet again. Available at:* https://paul.reviews/police-cyberalarm-abysmal-security-yet-again/(Accessed: 12 May 2022)

The Register (9 December 2020 *Bitter war of words erupts between UK cops and web security expert over alleged flaws in Cyberalarm monitoring tool*. Available at: https://www.theregister.com/2020/12/09/cyberalarm_pervade_software_npcc_kerfuffle/ (Accessed: 12 May 2022)

The Register (10 March 2021) *Brit cybercops issue tender to rip and replace their formerly flaw-ridden CyberAlarm tool*. Available at: https://www.theregister.com/2021/03/10/police_cyberalarm_pervade_software_new_ten der/ (Accessed: 12 May 2022)

Tech Monitor (26 March 2021) *UK cyber policing gains new alarm bells. Available at:* https://techmonitor.ai/technology/cybersecurity/uk-cyber-policing-gains-new-alarm-bells (Accessed: 12 May 2022)

ITPro (20 April 2022) *Report: UK businesses are less secure when using police-endorsed cyber security tool*. Available at: https://www.itpro.co.uk/security/367442/report-uk-businesses-are-less-secure-when-using-uk-police-endorsed-cyber-security (Accessed: 12 May 2022)

Police CyberAlarm (14 June 2022) *Bytes public statement in relation to Police CyberAlarm.* Available at: https://cyberalarm.police.uk/security/4.0.1.0-statement/ (Accessed: 07 July 2022)