



“MASC = secure, anonymous and automatically search for vulnerability’s”

## // Magic automatic software Checker (MASC)

Every software developer knows the struggle to find bugs in open source software (CVE’s) as soon as possible. Most of the time it has to be checked manually which is an time-consuming process.

Online software could be dangerous as criminals could identify which open source software (incl. versions) are used by the organization.

With use of the MASC organizations are able to check automatically on CVE’s without having the risk that criminals could confiscate these information.

### MASC

The Magic Automatic Software Checker is running on one hardware appliance, which consist of four different components. The MASC checks continuously and anonymous for new CVE’s. If a new CVE is found, it will directly send a push message to the user/server.

**Phase 1 – Anonymous download CVE database**  
The complete CVE database will be downloaded and put on a FTP server to send to the ‘safe area’.

While downloading the full CVE database it is impossible for anyone to know which software (versions) are used by the user.

### Phase 2 – Secure data communication

The MagiCtwin Diode consists of a TX- and RX side. The CVE database will be put on a FTP file and send via the TX side over to the RX side. The RX side sends the data automatically to the right FTP server on the secure side.

It is also possible to put the FTP file on the RX side ‘ready for collection’ and sends the data over after the user gave permission.

It is physically impossible to send data from the RX- to the TX side.





“De security of your data is our mission - Cybersecurity with a personal touch”

### Phase 3 – Check on new CVE's

From now on, the data are in the secure- and offline area of the MASC. The CVE database will be compared with the own database (where is put which open source software and versions are used by the organization).

In order to minimize the data traffic, the new CVE database will be compared with the last available one. Only the new CVE's will be check with the own created database.

### Phase 4 – Push notification to right network/ person

In case there is a match, a push message will be immediately send to the right person or network. This depends on the internal policy where to send these notifications to.

With the MASC it is possible to analyze the vulnerability within seconds of publication.

### Anonymous

The use of MASC is fully anonymous as always the complete CVE database will be downloaded and not a small changed part revealing your own used software. After the data is in the secure offline area, it will be checked against the registered software in your own database.

### Secure

By using the MagiCtwin Diode the MASC requires only a limited internet accessibility.

All confidential data is stored in the offline and secure area of the MASC. It is physically impossible to send data from this area to the internet.

### Automatically

Depends on the configuration, the MASC checks continuously on new CVE's. The user could be notified by the MASC just after a few seconds the vulnerability is published.