OpenKAT
Vulnerability Analysis Tool

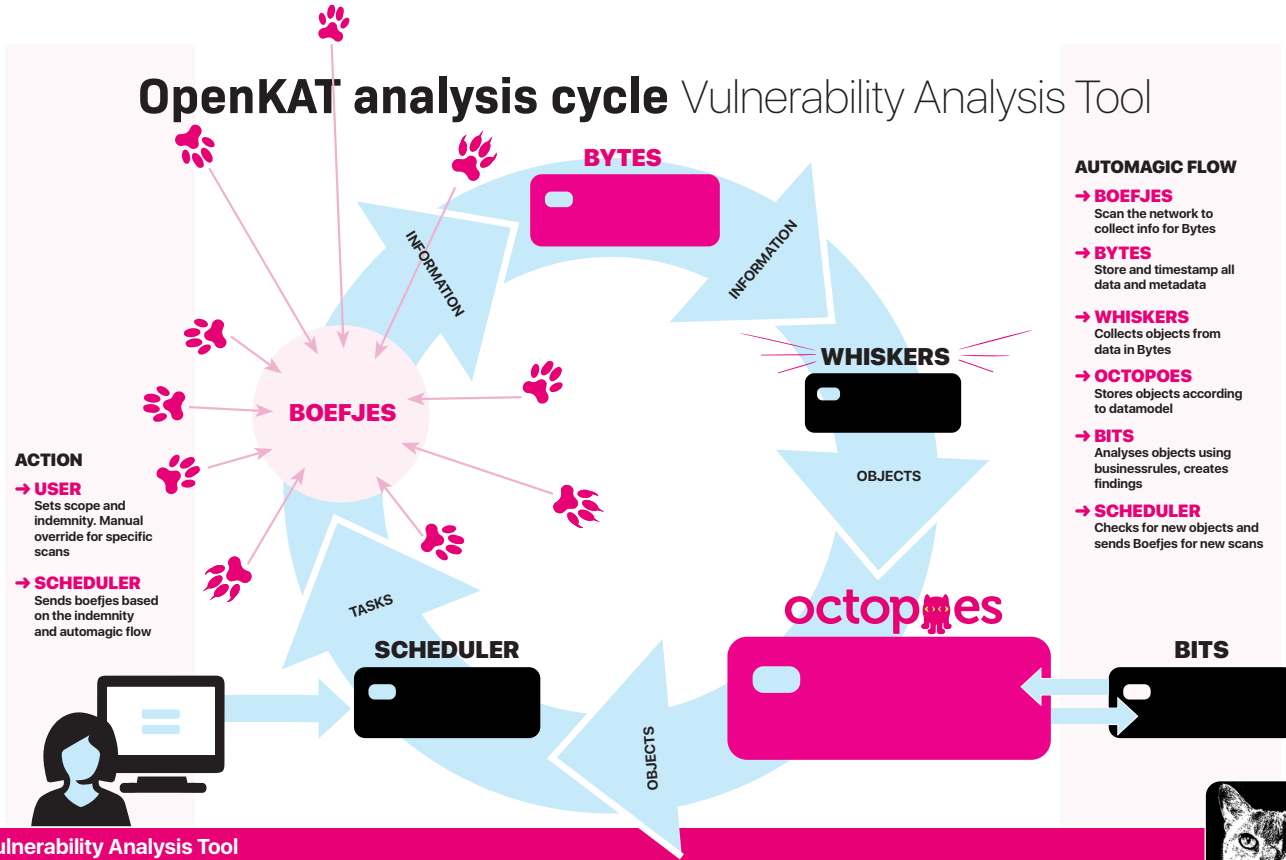
What is OpenKAT?

OpenKAT is a monitoring tool and vulnerability scanner created by the Dutch Ministry of Health during the vaccination campaign. New systems and functions were developed at high speed and monitoring was needed.

OpenKAT combines information from different sources and tools, scans automatically and allows for broad analysis and vulnerability detection. It is a modular framework for automagic monitoring or larger systems.

OpenKAT is useful if you have a complex or large system and a wish to know if there are vulnerabilities and configuration mistakes hiding somewhere. Most security incidents are caused by known vulnerabilities and small errors. OpenKAT finds them before they are found.

OpenKAT analysis cycle Vulnerability Analysis Tool



Why was OpenKAT built?

The Dutch Ministry of Health built OpenKAT to monitor the infrastructure for the Dutch COVID app CoronaCheck. OpenKAT was made 'in house' at the Ministry.

The vaccination campaign created some IT security dilemmas, which OpenKAT tries to solve:

- **Scale**
In the Dutch vaccination campaign, a lot of organisations are involved, all with their own systems and development teams.

- **Dynamics**
COVID doesn't stick to the plan. The government reacted quickly with measures announced in press conferences, leading to new systems and functions at a weekly basis.

- **Focus**
Most security incidents are caused by known vulnerabilities, configuration mistakes and human error. We also want to find the mistake in the latest update or rollout.

Which problem does OpenKAT solve?

OpenKAT was created as a monitoring tool with automation, flexibility and traceability in mind.

Being a modular framework based on a datamodel, it has plugins for datacollection, automatic scanning, businessrules for analysis, external timestamps on all original data and practical reports.

- **Framework**
The open structure allows you to modify, tweak and add tools for scanning, storage, analysis and reports. With such flexibility and seperation of tasks, the bits almost fall out. It allows for easy adaptation to new developments.

- **Plugins for scanning**
'Boefjes' or little rascals do the scanning, ranging from a small script to external tools with a wide range of inputs. New threat around the corner? Build a boefje to catch it, and as all data is stored you might be able to find vulnerable systems right away.

- **External timestamps**
All output from the scans is stored, with its metadata, hashed and timestamped by an external server. This allows you to 'prove' which information was collected, how and when.

- **Datamodel**
To combine information from several sources OpenKAT uses an extendable datamodel with objects. An IP adress is such an object, and can be found through different tools and through logical relations in the datamodel.

- **Automagic scanning**
OpenKAT will scan for new information, using the logic in the datamodel. The results of the scans spark new actions, just as time passing starts new scans to refresh and check the state of the systems in the OpenKAT database.

- **Indemnity per user and organisation**
The intensity of a scan can be set in the system, by giving it indemnity for a certain level of intrusion. OpenKAT can be set to a level where it might bring down a system so it needs an "OK" from the user for such steps.

- **Findings and reports**
Results of the analysis are available for easy viewing in the frontend, per PDF or through the API. Reports for common use cases are preprogrammed, and the system is ready to be adapted to specific questions.

The future of OpenKAT

OpenKAT receives a lot of love from the Ministry of Health in the Netherlands, has a growing community around it and is mentioned in several policy documents. One of the main ideas is to develop the system into a compliance analysis tool supporting 'Information Security Management Systems' as used during common certification processes. This requires additional work and thought.

You are invited by the OpenKAT community to join: come in, it's open! OpenKAT has been released as EU PL 1.2 software. The current community is growing fast and would love to have you on board!

Using OpenKAT

OpenKAT has been published under EU PL 1.2, is available as sourcecode and in several other ways for easy installation. All documentation and manuals can be found through **www.openkat.nl**. Beware, most is in Dutch until now, we are in the process of translating all documentation. Contact us: **meedoen@openkat.nl**.