OpenKAT

Kwetsbaarheden Analyse Tool

INTRODUCTIE

INHOUD

1. OpenKAT: **Kwetsbaarheden Analyse Tool**

OpenKAT heeft als doel het monitoren, registreren en analyseren van de status van informatiesystemen. OpenKAT scant netwerken, analyseert kwetsbaarheden en maakt toegankelijke rapporteren. Het integreert de meest gebruikte netwerktools en scansoftware in een modulair framework, heeft toegang tot externe databases zoals shodan en combineert de informatie uit al deze bronnen in overzichtelijke rapportages.

Wat OpenKAT toevoegt aan de beschikbare security en monitoringstools is het vermogen om de output van verschillende bronnen te combineren ten behoeve van de analyse. Het combineert informatie over security, configuratie, assets etc in een datamodel en doet daar analyse op.

Dankzij het objectgeorienteerde datamodel en de forensisch geborgde database bevat OpenKAT een compleet overzicht en een tijdlijn van de bewaakte systemen. Hiermee is de ontwikkeling door de tijd inzichtelijk te maken voor analyse en bewijsbaar voor audits en controles.

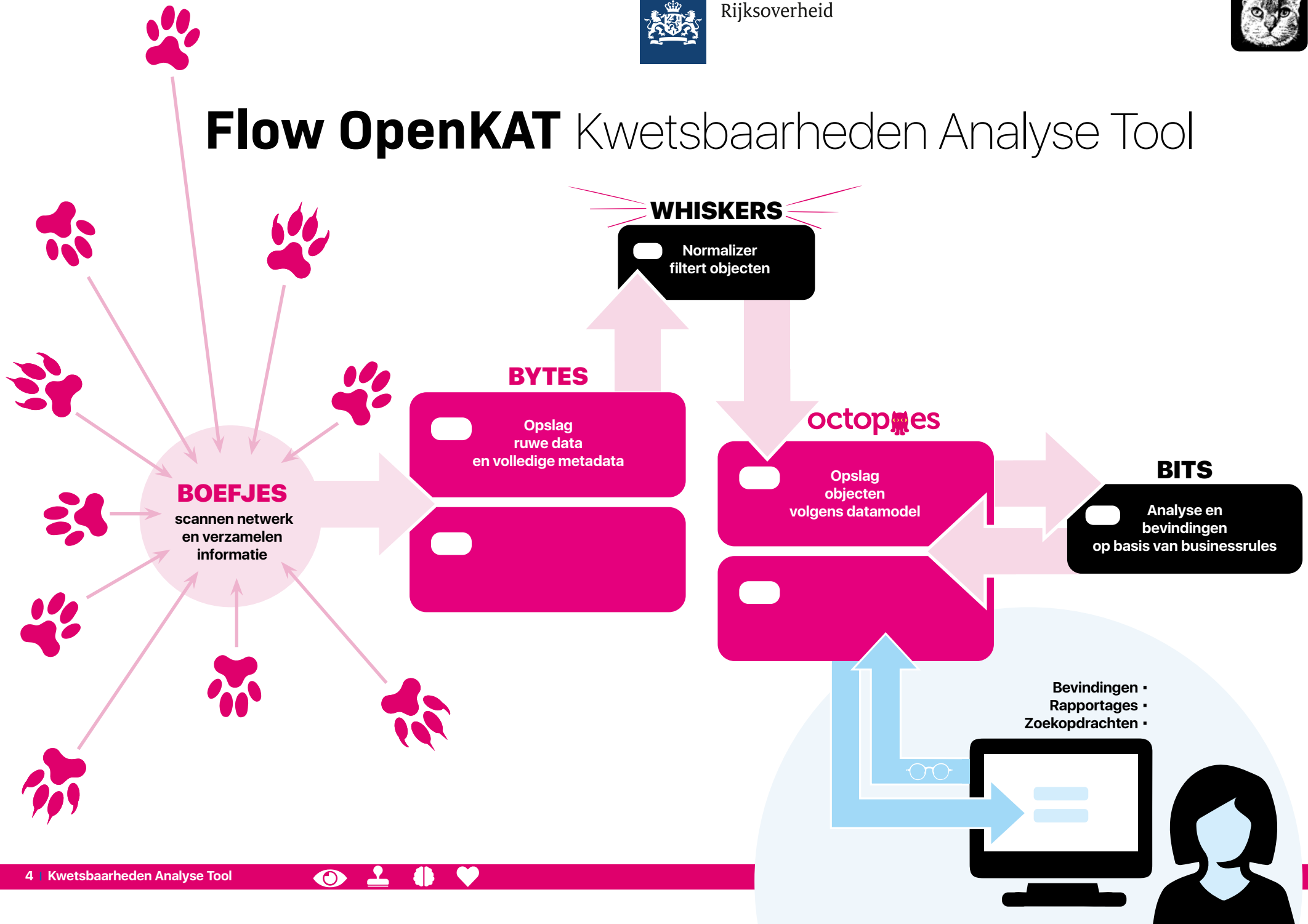
OpenKAT is de publiek beschikbare versie van KAT, de Kwetsbaarheden Analyse Tool van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS). KAT ontstaan toen tijdens de coronapandemie een groot aantal systemen moest worden beveiligd. De kern van dit systeem wordt nu als OpenKAT publiek beschikbaar gemaakt, zodat het door iedereen kan worden gebruikt.

De kracht van OpenKAT is dat het modulair en eenvoudig uit te breiden is. Dit kan op basis van het bestaande datamodel, aangevuld met bijvoorbeeld specifieke toepassingen zoals IoT of M2M communicatie. Het kan ook worden uitgebreid naar andere domeinen, bijvoorbeeld op het gebied van compliance, zolang er maar sprake is van een logische samenhang van informatie.

OpenKAT wordt onder de EU Public Licence beschikbaar gesteld als open source software. Dit houdt in dat de software vrij beschikbaar is, aangepast mag worden en verder kan worden verspreid binnen de voorwaarden van de licentie.

Hierdoor kunnen toevoegingen eenvoudig publiek gemaakt worden en zijn ze bruikbaar voor de hele community van OpenKAT gebruikers.

Flow OpenKAT Kwetsbaarheden Analyse Tool



2. OpenKAT: **Basisconcepten**

Centraal in OpenKAT zijn de objecten en het datamodel. Objecten ontstaan door het verzamelen en analyseren van informatie. De gevonden objecten worden aan de hand van business rules geanalyseerd, wat tot bevindingen leidt die als objecten in het datamodel worden opgenomen. Het datamodel helpt bij het speuren naar meer informatie, door de logische samenhang van objecten. Aan de hand van nieuwe objecten wordt weer naar informatie gezocht, waarmee de cirkel rond is.

2.1 Objecten, het datamodel en recursiviteit

De informatie die OpenKAT verzamelt wordt opgeslagen als objecten. Deze objecten zijn onderdeel van een datamodel. Het datamodel is de logische samenhang van alle objecten en biedt de basis voor analyse en rapportages. Bij OpenKAT zit een datamodel geschikt voor informatiebeveiliging, maar het kan worden uitgebreid of aangepast voor andere toepassingen. Een object is bijvoorbeeld 'een IP adres' of 'een hostname'.
Als er een hostname is, verwacht OpenKAT op basis van het datamodel ook een IP-adres en mogelijke open poorten. Afhankelijk van de vrijwaring die gegeven is wordt hier vervolgens op gescand, wat weer meer informatie oplevert, die weer aanleiding kan zijn voor nieuwe scans. Dit proces gaat door tot OpenKAT het gehele datamodel voor deze hostname heeft afgezocht. Hoe ver OpenKAT gaat met zoeken hangt af van de vrijwaringen.

2.2 Vrijwaringen

OpenKAT werkt met een systeem van vrijwaringen voor het scannen, gekoppeld aan 'intrusion levels'. Hiermee wordt voor een context (b.v. een organisatie) een vrijwaring en de intensiteit van de scan bepaald. Per boefje wordt het level aangegeven, om zo te voorkomen dat onverhoopt een productiesysteem in de problemen komt. Hier zit een balans in: als OpenKAT een risico vormt dan geldt dat voor alle actoren die toegang hebben tot dit betreffende systeem en is dat al een bevinding waard.

Intrusion levels of vrijwaringen:
* L1 is 'niet aanraken'
* L2 is 'aanraken op het niveau normale gebruiker'
* L3 is 'detecteerbaar scannen'
* L4 is 'intensief scannen'

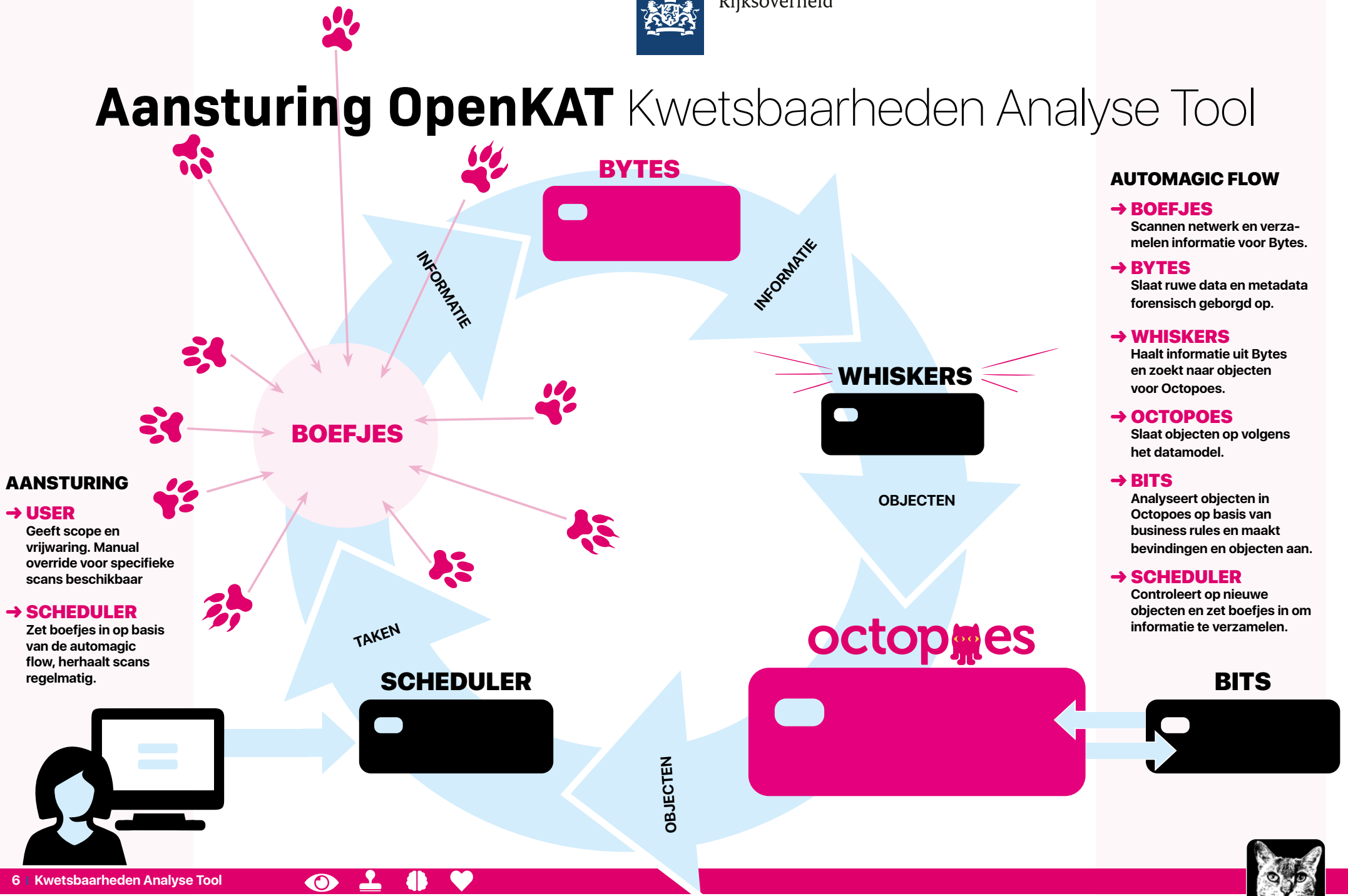
2.3 Gebruikers en organisaties

Het scannen en rapporteren zijn in OpenKAT verschillende systemen met aparte gebruikers. Er is een red team user, die het systeem een bepaalde opdracht en vrijwaring geeft ('scan dit netwerk, met dit intrusion level'). Op basis hiervan verzamelt OpenKAT informatie en worden objecten aangemaakt en opgeslagen in de database.

De rapportages worden gemaakt door een aparte rapportage-user met leesrechten op de database met objecten. Deze user heeft toegang tot de objecten, kan door de tijd kijken naar de scans die gedaan zijn en ziet welke bevindingen het systeem heeft aangemaakt.

Database
Indien OpenKAT gebruikt wordt voor verschillende organisaties krijgt elke organisatie een eigen database. Zo is er tussen de organisaties een volledige scheiding mogelijk. OpenKAT kan wel over meerdere databases zoeken, om bijvoorbeeld een compleet beeld te krijgen van het gebruik van bepaalde software of bij specifieke kwetsbaarheden.

Aansturing OpenKAT Kwetsbaarheden Analyse Tool



AANSTURING

→ USER
Geeft scope en vrijwaring. Manual override voor specifieke scans beschikbaar

→ SCHEDULER
Zet boefjes in op basis van de automagic flow, herhaalt scans regelmatig.

AUTOMAGIC FLOW

→ BOEFJES
Scannen netwerk en verzamelen informatie voor Bytes.

→ BYTES
Slaat ruwe data en metadata forensisch geborgd op.

→ WHISKERS
Haalt informatie uit Bytes en zoekt naar objecten voor Octopoes.

→ OCTOPOES
Slaat objecten op volgens het datamodel.

→ BITS
Analyseert objecten in Octopoes op basis van business rules en maakt bevindingen en objecten aan.

→ SCHEDULER
Controleert op nieuwe objecten en zet boefjes in om informatie te verzamelen.

3. OpenKAT: **Systeemopbouw**

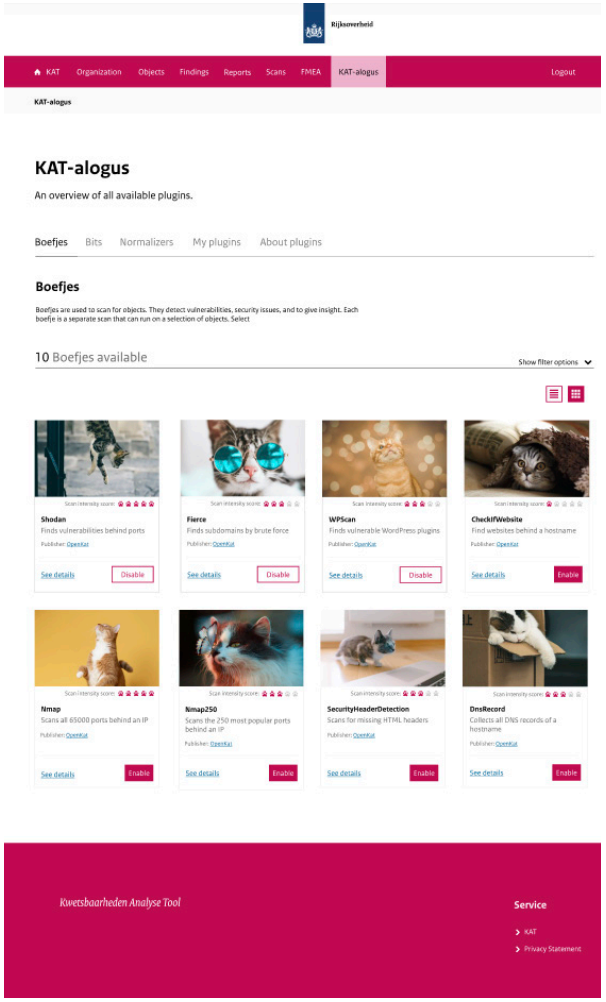
Het systeem kent vier delen: informatieverzameling, opslag, analyse en rapportage.

3.1 **Verzamelen:** Boefjes en Whiskers

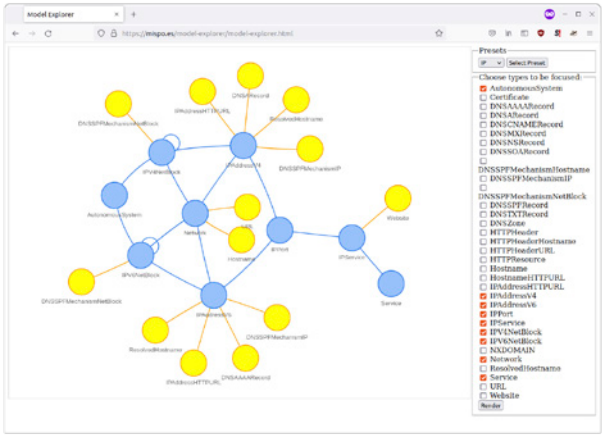
Boefjes verzamelen de informatie voor OpenKAT. Het zijn scripts die een tool kunnen aanroepen of zelf informatie verzamelen. Ze geven het resultaat aan Whiskers, de normalizer die er objecten uit probeert te filteren. Deze objecten passen in het datamodel dat wordt gebruikt. Boefjes leven in de KAT-alogus en worden afhankelijk van de situatie ingezet. De scheduler zet boefjes in afhankelijk van de vraag, de beschikbare vrijwaring (het 'intrusion level') en de gevonden informatie. Zo leidt een scan tot nieuwe gegevens, die op basis van de business rules bevindingen opleveren. Dat kan weer tot nieuwe inzet van boefjes leiden, die aanvullende delen van een systeem scannen.

3.2 **Opslag:** Bytes en Octopoes

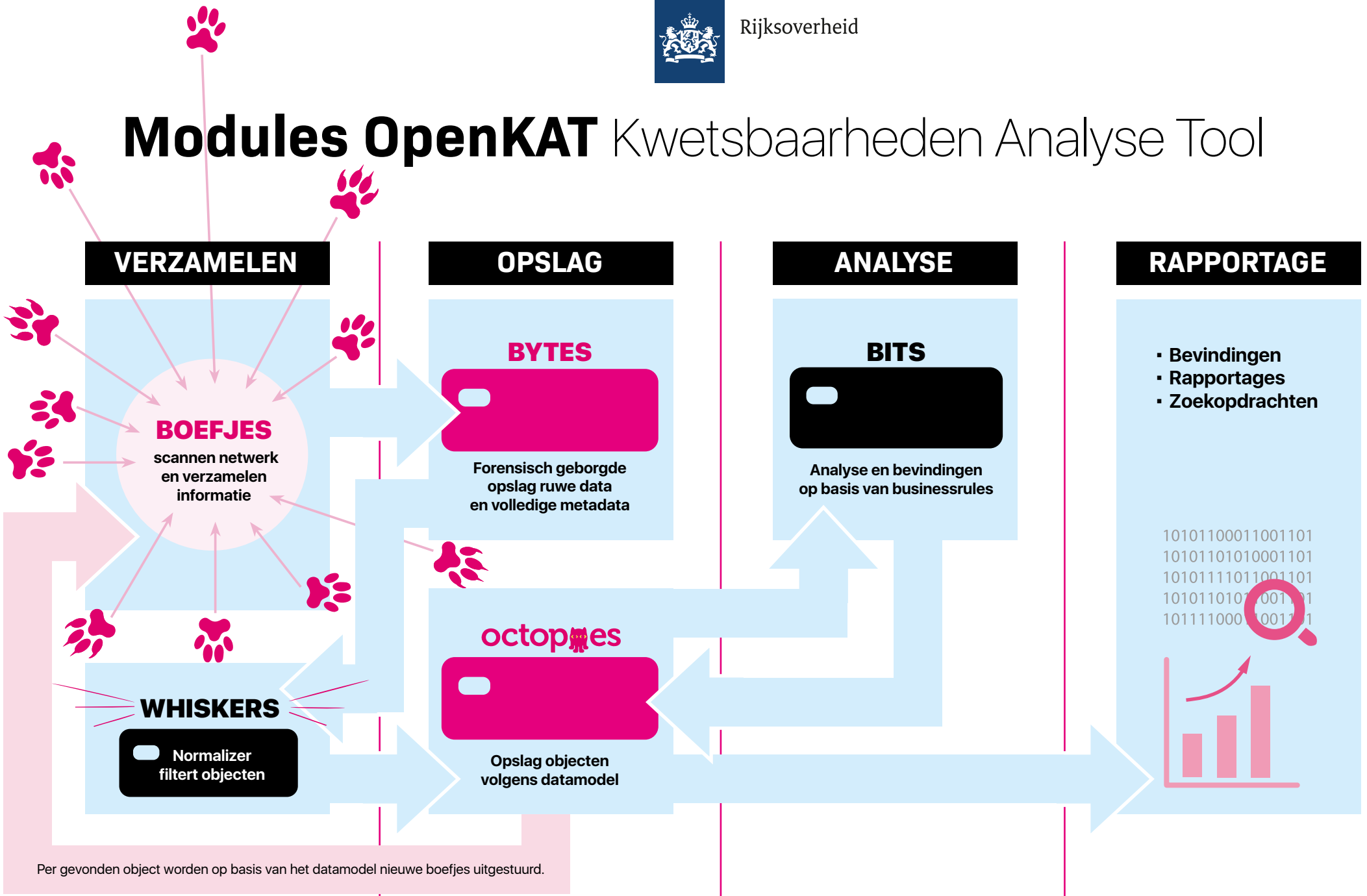
De objecten worden opgeslagen in Octopoes, de database met objecten die voor analyse



toegankelijk is. Hier zijn objecten in logisch verband en in de tijd te bekijken. Alle originele informatie wordt samen met metadata apart opgeslagen in Bytes. Dit kan gebruikt worden om de totstandkoming van objecten en bevindingen te controleren.
Het datamodel is onderdeel van Octopoes en wordt ook wel aangeduid als de 'knowledge graph' of het geweten van OpenKAT. In de standaard installatie is een datamodel opgenomen dat geschikt is voor informatiebeveiliging. Dit kan worden aangevuld of aangepast aan de specifieke situatie waarin OpenKAT wordt gebruikt. In de ontwikkelfase zijn al partijen betrokken die OpenKAT willen benutten voor



Modules OpenKAT Kwetsbaarheden Analyse Tool

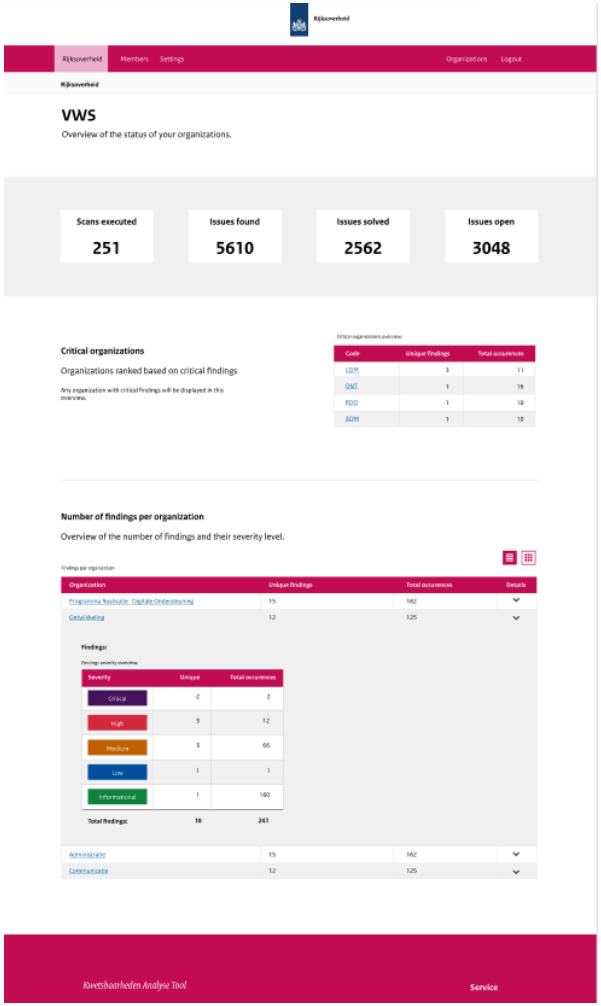


3. OpenKAT: **Systeemopbouw**

het controleren van bepaalde administratieve aspecten van certificering, wat goed aansluit op de huidige toepassing.
Bytes slaat alle originele informatie op inclusief de volledige metadata in ondertekende records. De observatie door OpenKAT en het proces dat leidde tot een object en eventuele conclusies is hiermee reproduceerbaar en herleidbaar, wat ook forensische borging genoemd wordt. In de metadata zit bijvoorbeeld ook de softwareversie van OpenKAT, van het boefje en van de eventuele externe scantools, zodat te traceren is waarom bepaalde waarnemingen wel of niet gedaan zijn.

3.3 **Analyse:** Bits

De objecten in de database kunnen worden geanalyseerd aan de hand van businessrules, die zijn opgenomen in Bits. Zo is een lijst met open poorten die bij een IP adres hoort in de ene situatie prima, maar leidt het in een andere situatie tot een bevinding. Een bevinding bij een bepaald object wordt ook als object in Octopoes opgeslagen, en kan leiden tot meer scans of andere acties.
Bits zijn net als Boefjes en Whiskers modulair, aanpasbaar en eenvoudig toe te voegen. Een Bit kan leiden tot nieuwe bevindingen en kan meer Boefjes op pad sturen. Dat wil zeggen dat een bevinding op basis van een businessrule kan leiden tot aanvullende scans of acties vanuit OpenKAT.



3.4 Rapportages

Rapportages kunnen op een paar manieren worden gemaakt. In de standaard installatie van OpenKAT zitten een aantal opties om rapportages te maken:

➜ **Bevindingenrapport:**
met alle bevindingen op basis van de businessrules zoals:
- configuraties
- oude software
- ports
- ontbrekende headers
- ssl problemen en certificaten
- SPF en mail configuratie

➜ **Specifieke rapportages:**
- DNS rapportage
- Internet.nl (gedeeltelijk)
- ssl report met certificaten

➜ **GraphQL**
- Eenvoudige ingang voor zoekopdrachten

4. OpenKAT: **Use cases**

De standaard installatie van OpenKAT kan een bijdrage leveren aan de monitoring en beveiliging van informatiesystemen en netwerken. Op dit moment zijn een aantal typische usecases voorhanden, door de modulaire opbouw is het systeem eenvoudig aanpasbaar.

➜ **Z-CERT: monitoring van de systemen van aangesloten organisaties**
Z-CERT wil OpenKAT inzetten om de perimeter van de bij haar aangesloten organisaties te monitoren. Ze zijn betrokken bij de ontwikkeling en helpen mee om OpenKAT geschikt te maken voor de permanente monitoring van de bij Z-CERT aangesloten organisaties.

➜ **Ministerie van VWS: monitoring van systemen in de pandemie**
Het Ministerie van VWS heeft KAT gebouwd om de systemen van testaanbieders te kunnen monitoren. Daarnaast zijn er andere modules beschikbaar die onder andere loganalyse doen ten behoeve van de fraudebestrijding. Deze maken echter geen onderdeel uit van OpenKAT.

Door de modulaire opbouw zijn de mogelijkheden van OpenKAT groot. Denk aan de integratie van OpenKAT in configuratie- en assetmanagement waarbij je op basis van verschillende bronnen eenvoudig een historisch overzicht kunt genereren, of aan de uitbreiding van OpenKAT naar meer administratieve processen zoals de koppeling met een op certificering gericht informatiebeheersysteem en contractmanagement.

5. OpenKAT: **Hoe kun je bijdragen?**

Waar tijdens de coronapandemie de nadruk lag op het laten werken van de systemen is er nu ruimte om 'te oogsten'.

VWS wil de software waar mogelijk op een praktische manier toegankelijk maken. De github van het ministerie van VWS is hiervoor beschikbaar. Iedereen is welkom.

Een bijdrage aan OpenKAT kan al door de code toe te passen en bruikbare toevoegingen te doen. Het is ook mogelijk om structureel samen te werken met het team, door je als organisatie, gebruiker of ontwikkelaars aan te sluiten bij het netwerk rondom OpenKAT.

Neem hiervoor contact op met **meedoen@openkat.nl.**

6. OpenKAT: **Licentie**

OpenKAT wordt als open source software beschikbaar gesteld onder de EUPL 1.2. De gebruiker krijgt op grond hiervan het recht deze software te draaien, te kopiëren, aan te passen en verder te distribueren.

De licentie heeft als doel de door een gebruiker gewijzigde softwarecode bij verspreiding ook in de openbare en vrije beschikbaarheidssfeer te houden. Anderen kunnen dan eveneens van de aanpassingen profiteren. De opname van plug-ins in de KAT-alogus wordt geregeld in een aparte overeenkomst die tussen VWS en de maker van een plug-in geldt.

Ook deze plug-ins vallen onder de EUPL 1.2. De opzet van de plug-ins maakt het wel mogelijk een koppeling te maken met software die onder een andere licentie valt, zoals bij veel scantools het geval is.

7. OpenKAT: **Betrokkenen**

OpenKAT groeit dankzij het werk van velen. Een aantal organisaties denken en helpen vanaf het eerste begin mee, zijn early adopters of anderszins betrokken bij de ontwikkeling van OpenKAT.

ZA CERT

catharina een santeon ziekenhuis

Bravis ziekenhuis

SDB GROEP zorgvernieuwend!

Secundity

CERT-WM

Auditdienst Rijk
Ministerie van Financiën