MISP

INTELLIGENCE SHARING

Inleiding tot het delen van informatie

Van waarneming naar bruikbare beslissingen met MISP

MISP Project / CIRCL

https://www.misp-project.org/

Referentie: 3 november 2026

Wat u na deze inleiding kunt

- Uitleggen hoe waarnemingen bruikbare gedeelde context worden.
- Gegevens, interpretatie en operationele actie onderscheiden.
- Bewust ontvangers en een uitwisselingsmethode kiezen.
- Beschrijven hoe feedback informatie bruikbaar houdt.

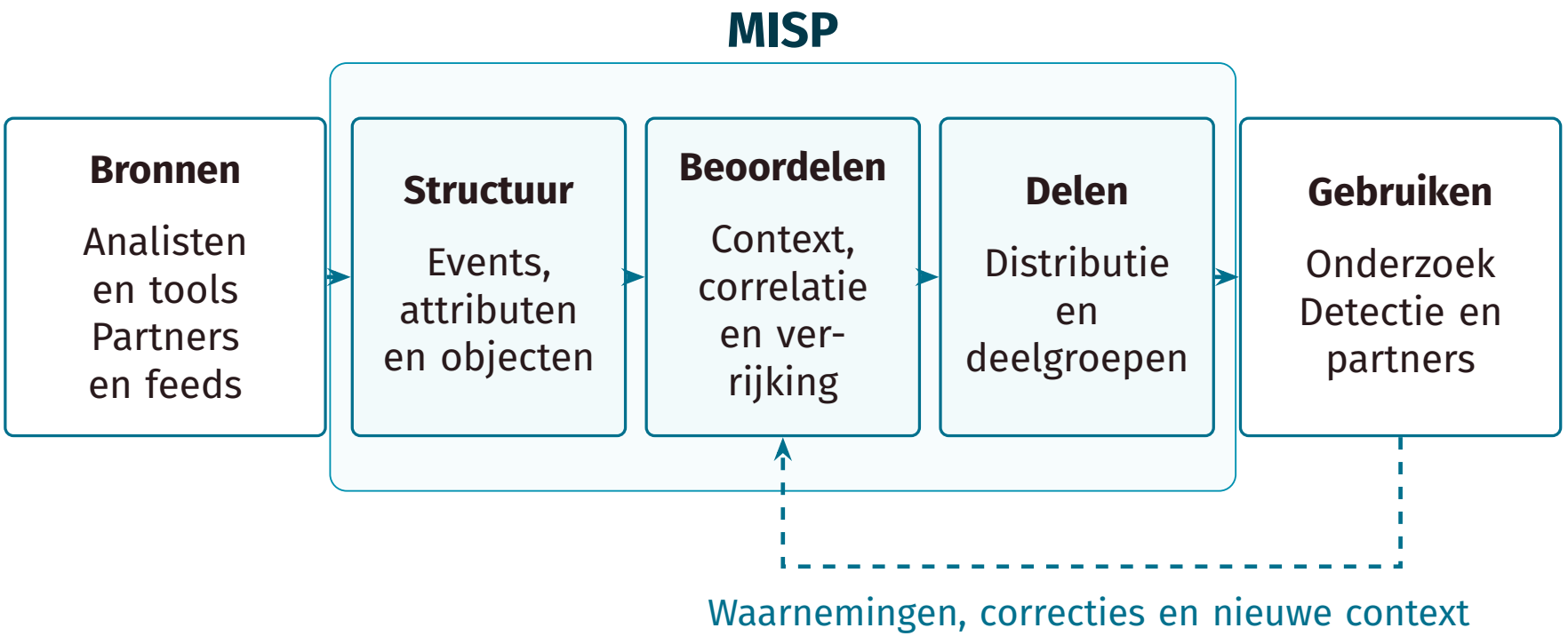
Eén casus, twee teams

- Team A onderzoekt een verdacht aanmeldbericht.
- Het registreert `login-support.example` en `192.0.2.25`.
- Team B zag hetzelfde domein in een ander rapport.
- Wat kunnen ze hergebruiken? Wat moeten ze nog vaststellen?

MISP ondersteunt mensen en hulpmiddelen

- Een opensourceplatform voor gestructureerde informatie-uitwisseling.
- Waarnemingen verzamelen van analisten, tools en partners.
- Gegevens verbinden en beoordelen met behoud van context.
- Bruikbare invoer voor onderzoek, detectie en respons leveren.

Van waarnemingen naar gedeelde context



Een klein model voor een bruikbaar record

Tags en Galaxy-clusters voegen context toe; sightings geven waarnemingen terug.

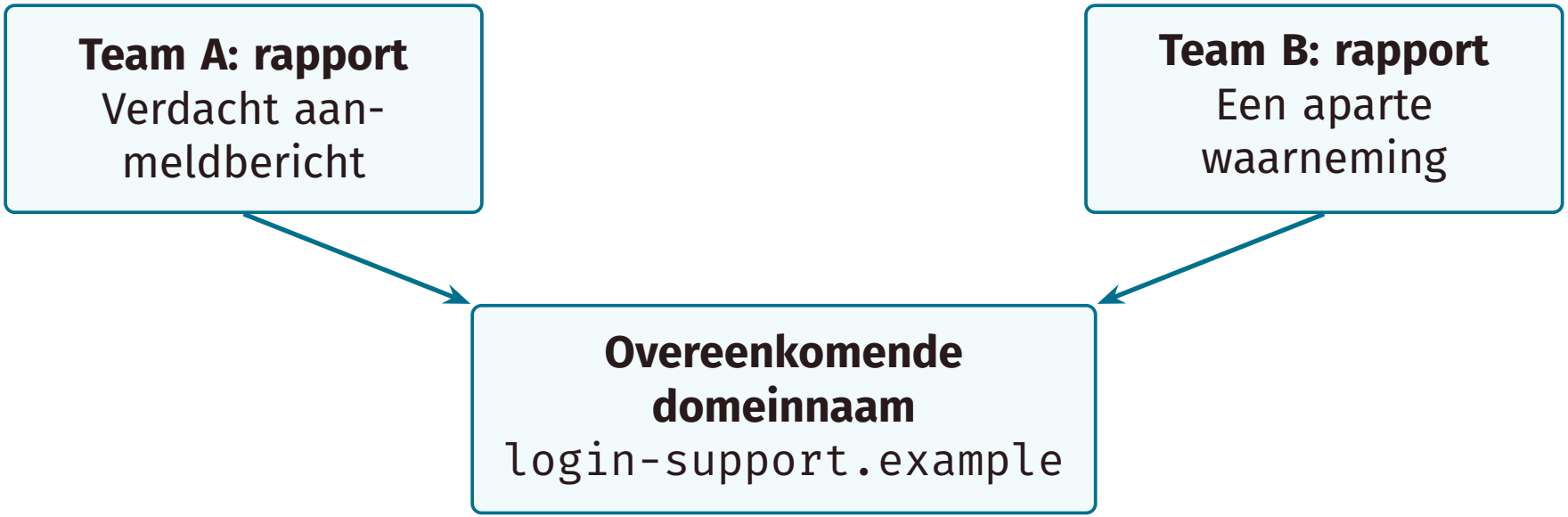
Beschrijf de waarneming vóór u handelt

- Type: de vorm van een waarde, zoals `domain` of `ip-dst`.
- Categorie: een brede indeling naar context.
- Commentaar, bron en tijd: wat onderbouwt de waarneming?
- `to_ids`: selectie voor uitvoer, geen bewijs.

Voeg classificatie en herbruikbare kennis toe

- Taxonomietags geven gedeelde classificatietermen.
- Galaxy-clusters voegen kennis en relaties toe.
- ATT&CK-technieken beschrijven onderbouwd gedrag.
- Houd waarneming, beoordeling en onzekerheid uit elkaar.

Een correlatie stelt een vraag



Vergelijk bronnen, tijden en context.
Een overeenkomst bewijst geen gedeelde actor of campagne.

Eén record kan verschillende acties ondersteunen

- Onderzoeken: rapporten vergelijken en een hypothese toetsen.
- Detecteren of hunten: relevante waarnemingen zoeken.
- Blokkeren: beleid toepassen en de gevolgen beoordelen.
- Beslissing vastleggen en aangeven hoe die wordt herzien.

Kies ontvangers met de MISP-instellingen

Distributiekeuze	Beoogde reikwijdte
Alleen uw organisatie	De organisatie die eigenaar is.
Alleen deze gemeenschap	De lokale MISP-gemeenschap.
Verbonden / alle gemeenschappen	Breder delen volgens uitwisselingsregels.
Sharing group	Een expliciet bepaalde groep ontvangers.

Omgangslabels en toegang hebben elk een taak

- TLP 2.0 communiceert verwachtingen over verdere verspreiding.
- Distributie en sharing groups regelen zichtbaarheid in MISP.
- Beoordeel gevoelige details, doel en ontvangerverplichtingen.
- Een label alleen dwingt geen toegestane doelgroep af.

Publiceren is een bewuste stap

1. Beoordeel het record, de bron en het beoogde gebruik.
2. Controleer distributie en tags op de relevante niveaus.
3. Bevestig de ingestelde sync-, feed- of exportbestemming.
4. Publiceer of wissel uit volgens het afgesproken beleid.

Instanties wisselen geselecteerde informatie uit

MISP-instantie C
In dit voorbeeld
geen
netwerkuitwisseling

Geen automatisch wereldwijd netwerk.
Ook handmatige over-
dracht vraagt controle.

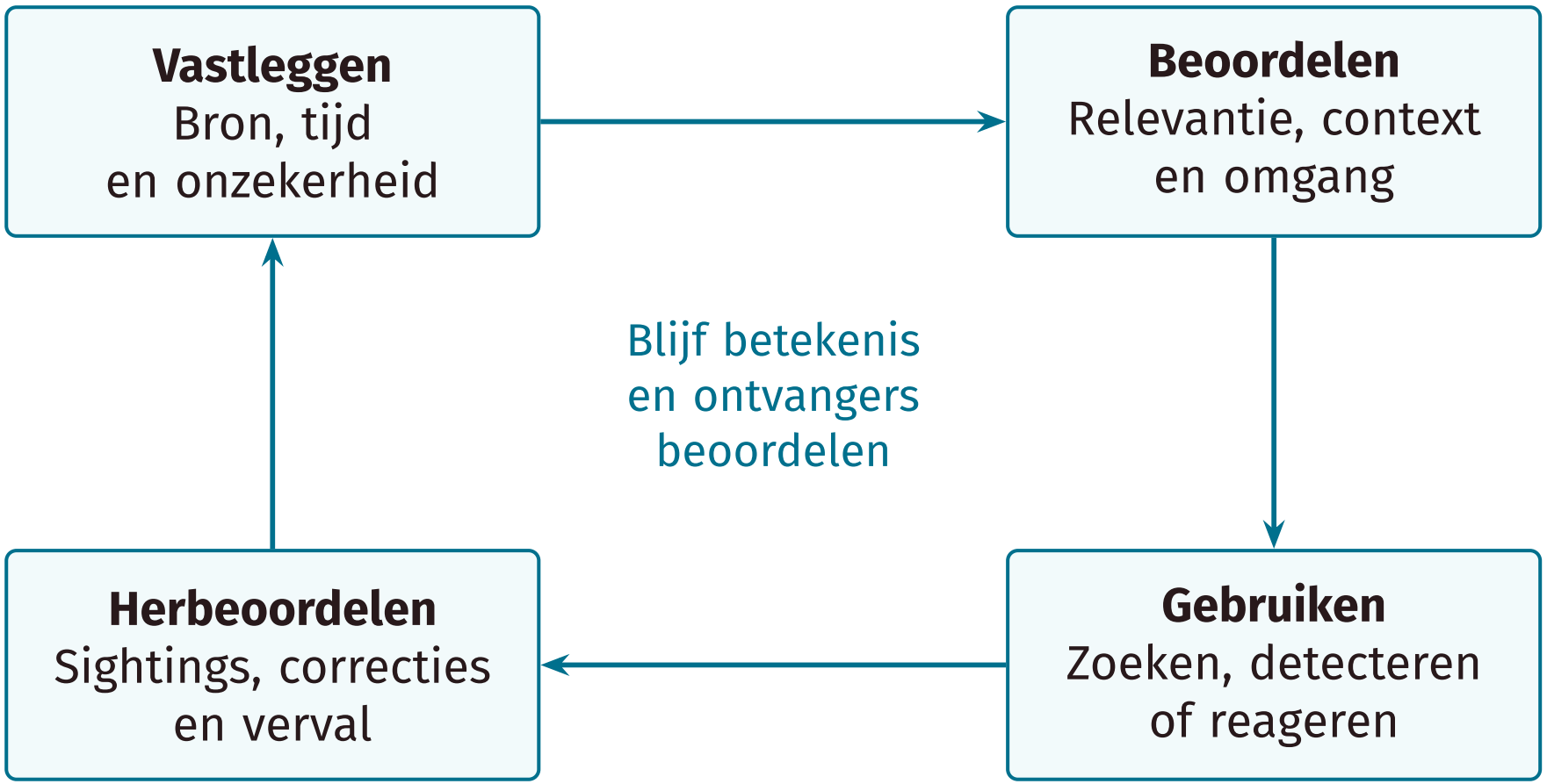
Kies de uitwisselingsmethode bij het doel

- Synchronisatie: gerichte uitwisseling tussen MISP-instanties.
- Feeds: gegevens ophalen bij een ingestelde leverancier.
- API en exports: een specifieke afnemer verbinden.
- Handmatige overdracht: bestand en bestemming beoordelen.

Werk samen met duidelijke verantwoordelijkheid

- Eigenaarschap geeft aan wie het event onderhoudt.
- Proposals laten anderen attribuutwijzigingen voorstellen.
- Extended events voegen context van een andere organisatie toe.
- Spreek af wie correcties ontvangt en opvolgt.

Kwaliteit vraagt een terugkerende beoordeling



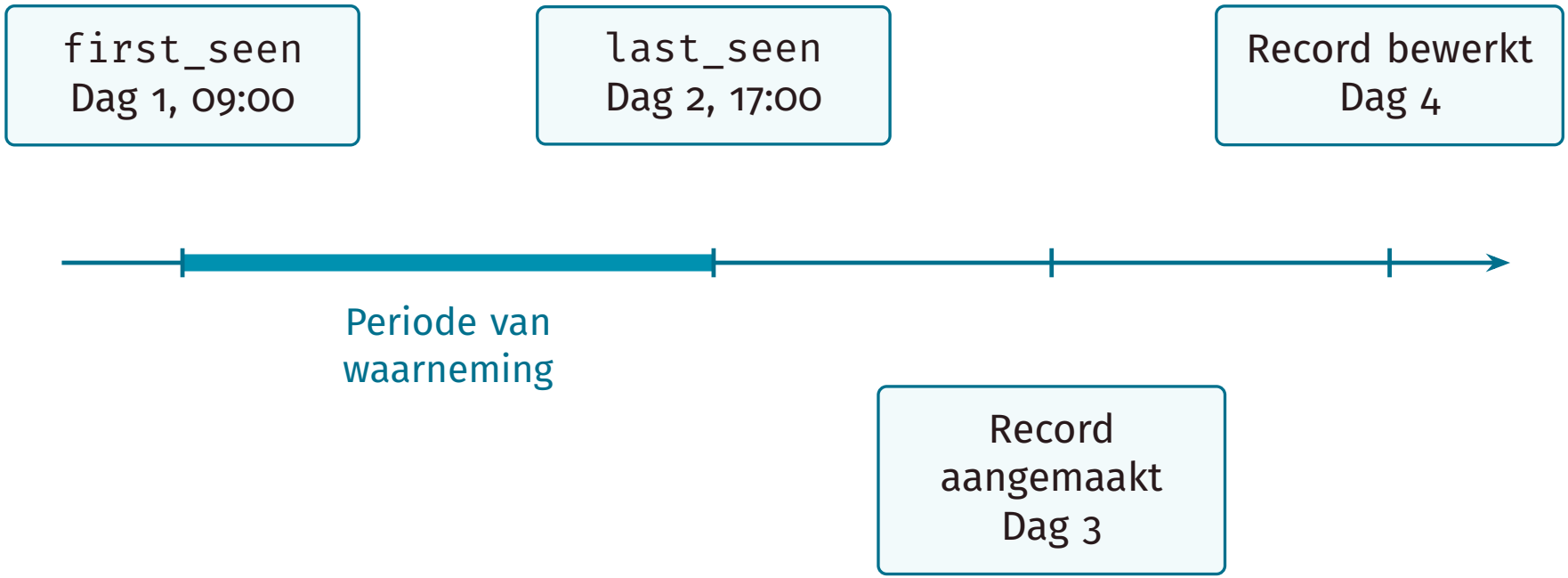
Gebruik hulpmiddelen met eigen beoordeling

- Warninglists signaleren mogelijk misleidende waarden.
- Verrijking voegt context uit gekozen bronnen toe.
- Vergelijk herkomst en houd onzekerheid zichtbaar.
- Controleer wat een externe module naar de leverancier stuurt.

Sightings geven verschillende soorten feedback

- Sighting: een waarneming van het datapunt.
- False positive: feedback over een ongeschikte interpretatie.
- Expiration: feedback dat de relevantie is geëindigd.
- Voeg bron en tijd toe; spreek af hoe feedback wordt gebruikt.

Waarnemingstijd verschilt van recordtijd



Fictieve datums. Een wijziging betekent geen nieuwe activiteit.

Ouderdom en decay helpen bij herbeoordeling

- Waarnemingen hebben verschillende nuttige levensduren.
- Een decaymodel geeft een beoordelings- of filtersignaal.
- Beoordeel het model, sightings en het beleid van de afnemer.
- Bewaar historische context na operationeel verval.

Automatiseer een beoordeelde beslissing

- Gebruik de REST API en PyMISP voor afgebakende processen.
- Filter voor de afnemer, het doel en de doelgroep.
- Test met fictieve gegevens en inspecteer de uitvoer.
- Breng feedback terug en behandel fouten expliciet.

Een gemeenschap heeft werkafspraken nodig

- Spreek doel, deelnemers en bijdragen af.
- Bepaal omgang, correctie en escalatie.
- Begin met een kleine vertrouwde groep en nuttige records.
- Herzie afspraken als mensen en toepassingen veranderen.

Maak van een obstakel een eerste bijdrage

Obstakel	Een nuttige eerste stap
Weinig tijd	Deel een kleine waarneming met een bron.
Onzekerheid	Benoem wat bekend en corrigeerbaar is.
Andere tools	Spreek termen en ondersteunde formaten af.
Verplichtingen	Beoordeel doel en ontvangers met verantwoordelijken.

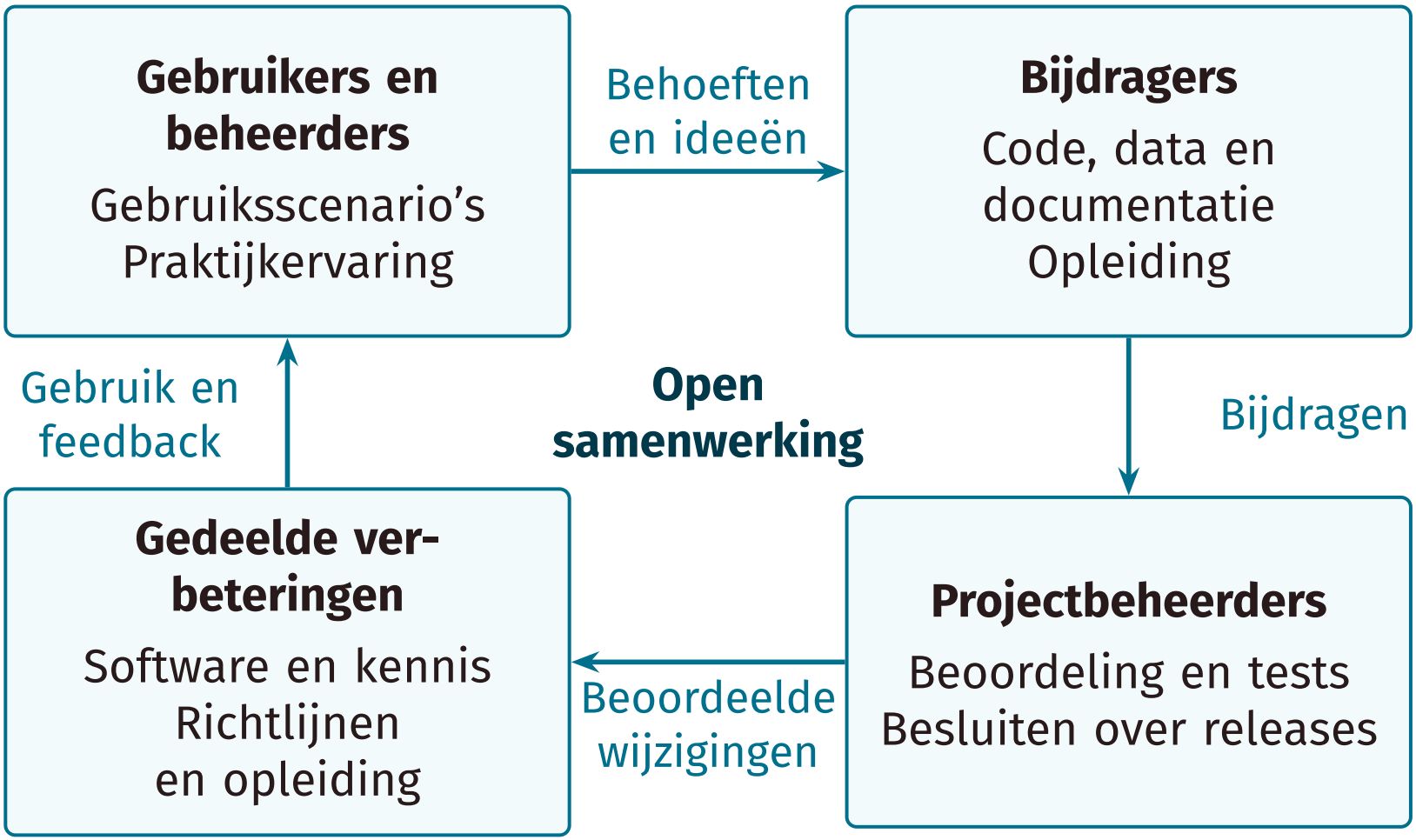
Het project begon met een praktische behoefte

- In 2012 wilden malwareanalisten dubbel werk voorkomen.
- Het vroege platform van Christophe Vandeplas werd MISP.
- CIRCL en een bredere gemeenschap verbeteren het project.
- Bijdragen omvatten code, gedeelde kennis en opleiding.

Het MISP-project heeft vier aanvullende delen

Software	Kennis	Standaarden	Gemeen-schappen
MISP-platform REST-API en PyMISP misp-modules	Taxonomieën Galaxies Waarschuwings-lijsten	Gegevens-formaten Begrippen Object-sjablonen	Vertrouwde partners Gedeelde werkwijzen Opleiding en feedback

De gemeenschap verbetert het project



Oefening: maak de casus bruikbaar voor Team B

1. Ontwerp een event met het fictieve domein en IP-adres.
2. Leg bron, tijd, relatie en onzekerheid uit.
3. Kies beperkte ontvangers en een onderbouwde vervolgactie.
4. Beschrijf hoe een correctie Team B bereikt.

Nabespreking: leg de beslissingen uit

- Het gedeelde domein is een spoor, geen attributie.
- Een object groepeert een door de bron onderbouwde relatie.
- Omgangslabels en zichtbaarheid vragen beide controle.
- Een zoekactie kan eerder verantwoord zijn dan blokkeren.
- Een correctie heeft een eigenaar en een terugweg nodig.

Ga verder met de taak die u nodig hebt

- Dagelijkse analyse: gebruik, tags en objecten.
- Context en kwaliteit: Galaxies en indicatorverval.
- Integratie: REST API, PyMISP en feeds.
- Gemeenschapsbeheer: administratie en deelpraktijken.

Deel context, kies bewust en blijf verbeteren

- Structureer waarnemingen met behoud van betekenis.
- Kies ontvangers en acties volgens afgesproken beleid.
- Gebruik feedback voor correctie en herbeoordeling.
- Draag ook werkwijzen en kennis bij.