MISP

INTELLIGENCE SHARING

Informatie delen met MISP

Een inleiding tot bruikbare informatie en samenwerking

MISP Project / CIRCL

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

Referentie: 3 november 2026

Wat u na deze inleiding kunt uitleggen

- Wat u met MISP deelt en waarom context belangrijk is.
- Hoe u ontvangers en een bruikbare vervolgstap kiest.
- Hoe feedback gedeelde informatie verbetert.

Begin met een gezamenlijke vraag

- 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 leren ze samen en wat blijft onzeker?

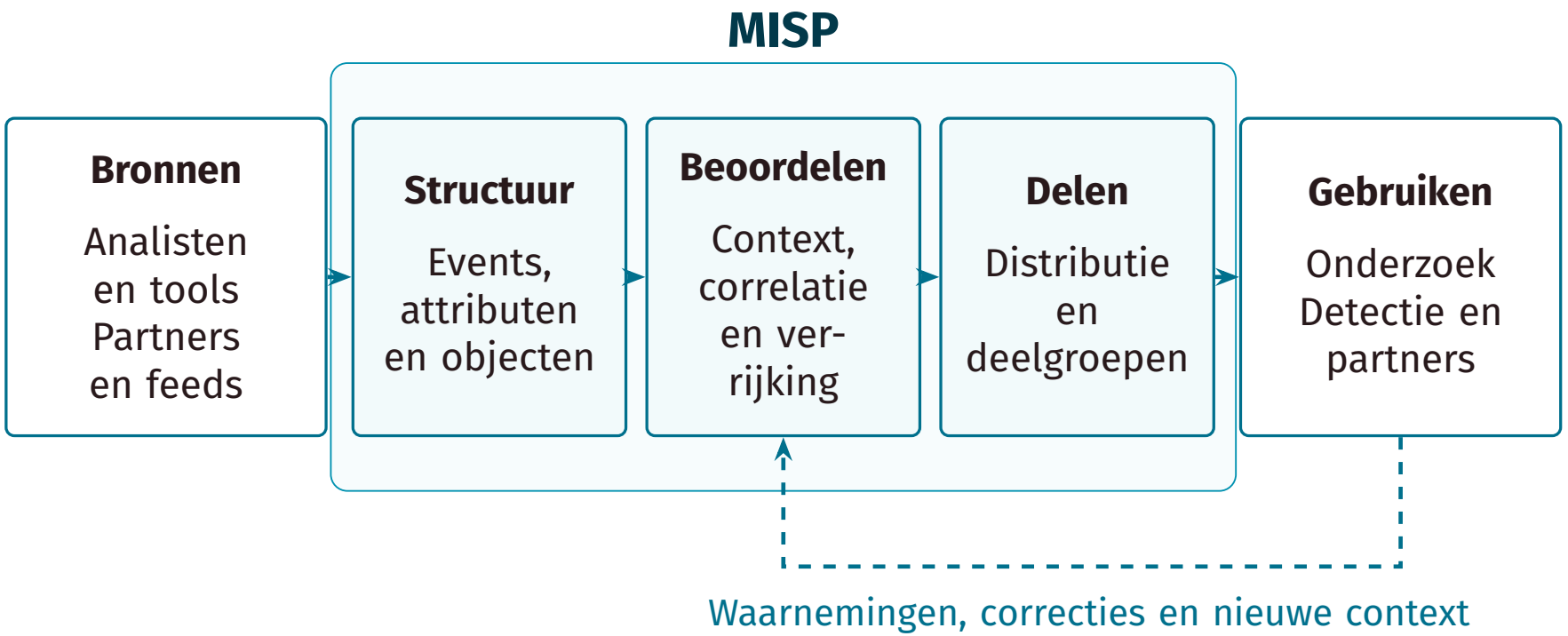
MISP maakt waarnemingen herbruikbaar

- Open source software om gestructureerde informatie te delen.
- Een plek om dreigingsinformatie te verzamelen en beoordelen.
- Samenwerking tussen mensen, tools en teams.
- Context voor onderzoek, detectie en respons.

Bewaar de waarneming samen met de context

- Event: de context van het rapport of onderzoek.
- Attribuut: één getypeerde waarneming, zoals een domein.
- Object: samenhangende attributen volgens een sjabloon.
- Tags en Galaxies: classificatie en gestructureerde context.

Van waarnemingen naar gedeelde context



Een correlatie is een aanknopingspunt

- Een gedeelde waarde kan relevante rapporten verbinden.
- Controleer bron, tijdstip en omliggende waarnemingen.
- Denk aan gedeelde infrastructuur, hergebruik en foutpositieven.
- Een overeenkomst bewijst geen oorzaak of attributie.

Kies de actie voordat u de uitvoer kiest

- Onderzoeken: gebruik context om betere vragen te stellen.
- Detecteren of zoeken: zoek relevante waarnemingen in uw data.
- Blokkeren: pas beoordeeld beleid toe met aanvaardbare impact.

Kies wie de informatie mag ontvangen

- Stel distributie en deelgroepen bewust in.
- Controleer event, attributen en beoogde ontvangers.
- Gebruik labels zoals TLP naast toegangscontroles.
- Controleer publicatie en instellingen vóór uitwisseling.

Kwaliteit groeit door feedback

- Leg herkomst, betrouwbaarheid en bruikbare tijdcontext vast.
- Beoordeel treffers op waarschuwingslijsten en verrijking.
- Voeg waarnemingen, correcties en foutpositieve meldingen toe.
- Herbeoordeel oude informatie en het beoogde gebruik.

Een deelgemeenschap heeft werkafspraken nodig

- Spreek doel, deelnemers en verwachte bijdragen af.
- Bepaal hoe informatie wordt behandeld, beoordeeld en verbeterd.
- Begin met een kleine vertrouwde groep en bruikbare informatie.
- Verbind andere gemeenschappen als het beleid dat toelaat.

Maak van een obstakel een eerste stap

Obstakel	Bruikbare eerste stap
Weinig tijd	Deel een kleine, gestructureerde waarneming met de bron.
Onzekerheid	Benoem wat bekend, onbekend en voor correctie vatbaar is.
Verschillende tools	Spreek begrippen af en gebruik ondersteunde uitwisselingsformaten.
Verplichtingen	Beoordeel doel, ontvangers en toepasselijk beleid met de verantwoordelijken.

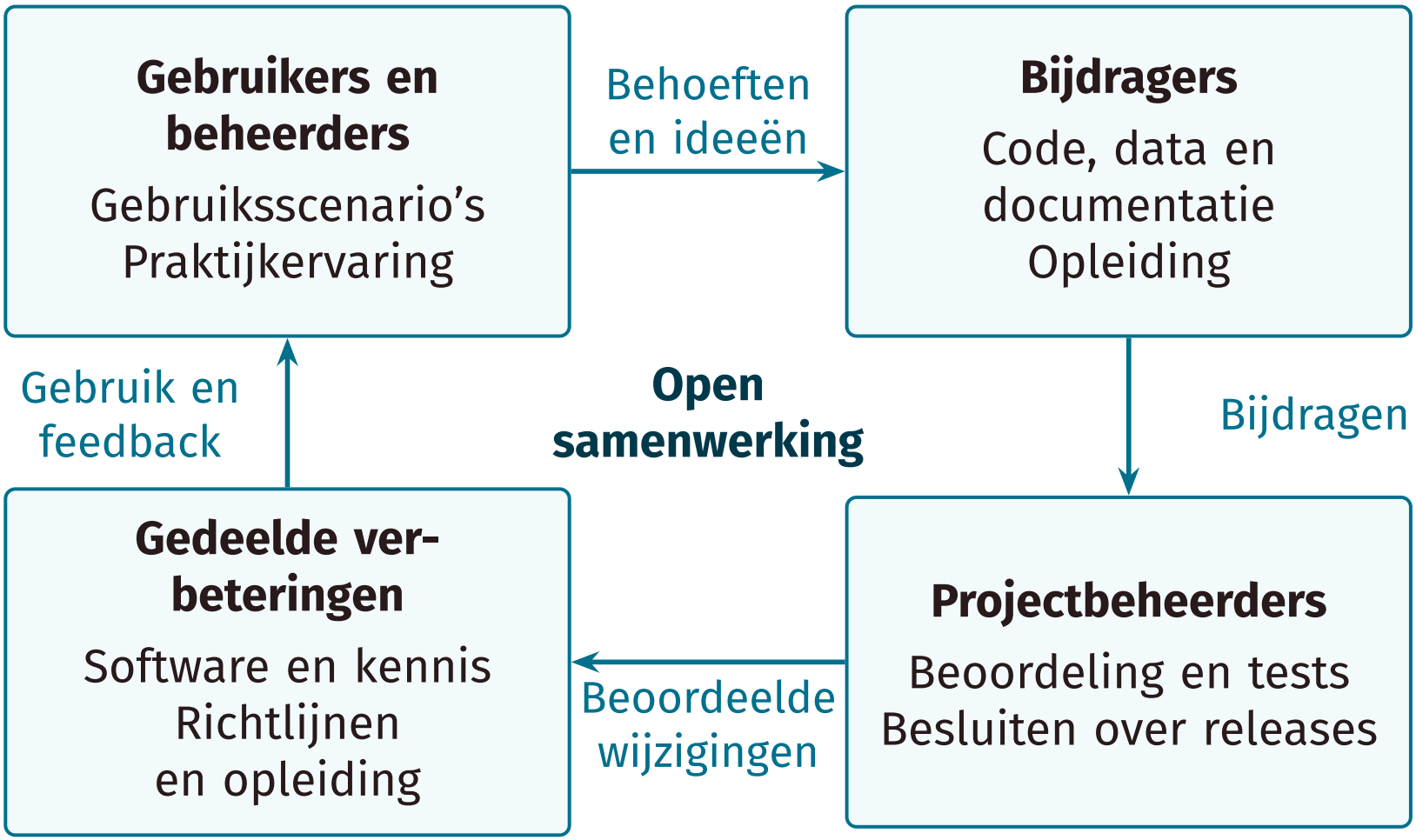
Het project begon met een praktische behoefte

- Malwareanalisten wilden dubbel werk voorkomen.
- Praktische feedback liet het vroege platform groeien.
- CIRCL en een bredere gemeenschap ontwikkelen MISP verder.
- Code, kennis en opleiding zijn bruikbare bijdragen.

Het MISP-project is meer dan één toepassing

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 geeft MISP vorm



Eerste oefening: leg een bruikbaar record uit

1. Maak een privé, ongepubliceerd event voor de fictieve casus.
2. Voeg domein en IP toe met bron, tijd en onzekerheid.
3. Leg een mogelijke correlatie en passende vervolgstap uit.
4. Beoordeel ontvangers en omgang vóór publicatie.

Ga verder met de taak die u nodig hebt

- Dagelijkse analyse: MISP-gebruik en tags.
- Meer context: objecten, Galaxies en informatiekwaliteit.
- Integratie: de workshops REST-API en PyMISP.
- Gemeenschappen beheren: administratie en deelpraktijken.

Deel bruikbare context en blijf die verbeteren

- Structureer de waarneming en behoud de betekenis.
- Kies doelgroep en actie bewust.
- Gebruik feedback om kwaliteit en begrip te verbeteren.