

INLEIDING TOT HET DELEN VAN CYBER- SECURITY INFORMATIE

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

[FIRST.ORG/AFRICA CERT](https://www.first.org/afrika-cert)



MISP
Threat Sharing

- (11:00 - 15:00) MISP fundamentals

- In 2012 werd tijdens een werkgroep voor malware analyse duidelijk dat we werkten aan de analyse van dezelfde malware.
- We wilden onze informatie op een eenvoudige en geautomatiseerde manier met elkaar delen **om dubbel werk te voorkomen.**
- Christophe Vandeplass (toen werkzaam bij het CERT voor de Belgische Defensie) toonde ons zijn werk aan een platform dat uiteindelijk MISP werd.
- De eerste versie van het MISP-platform werd gebruikt door de MALWG en met hulp van **de toenemende feedback van gebruikers** konden we een verbeterd platform bouwen.
- MISP is nu uitgegroeid tot een platform waar de **ontwikkeling gestuurd wordt vanuit de gemeenschap.**

Het Computer Incident Response Centre Luxembourg (CIRCL) is een overheids initiatief om een antwoord te bieden op computerbeveiligingsbedreigingen en -incidenten.

CIRCL is het CERT voor de particuliere sector, gemeenten en niet-gouvernementele entiteiten in Luxemburg en wordt beheerd door securitymadein.lu g.i.e.

- CIRCL is gemandateerd door het ministerie van Economische Zaken en treedt op als het Luxemburgse nationale CERT voor de particuliere sector.
- CIRCL leidt de ontwikkeling van het Open Source MISP-platform voor het delen van dreigingsinformatie. Dit platform is wereldwijd gebruikt door veel militaire en inlichtingengemeenschappen, privébedrijven, de financiële sector, nationale CERT's en LEA's.
- **CIRCL beheert meerdere grote MISP-gemeenschappen die dagelijkse actief zijn in het delen van dreigingsinformatie.**



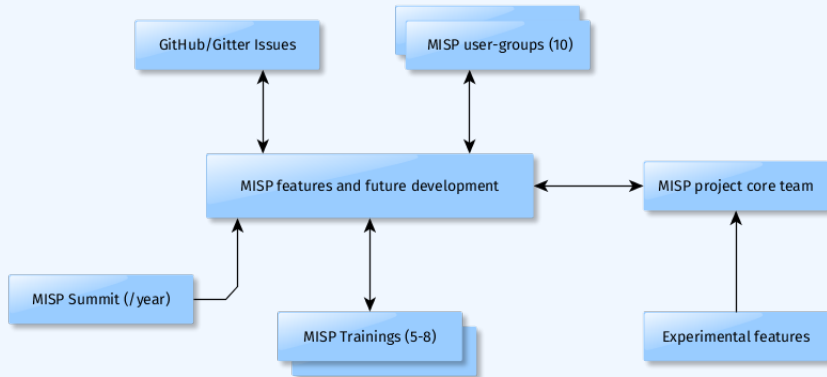
Co-financed by the European Union

Connecting Europe Facility

ONTWIKKELING GEBASEERD OP PRAKTISCHE FEEDBACK VAN DE GEBRUIKERS

- Er zijn veel verschillende soorten gebruikers van een informatie-uitwisselingsplatform zoals MISP:
 - ▶ **Malware-analysten** die bereid zijn om de indicatoren van hun analyse met collega's te delen.
 - ▶ **Beveiligingsanalisten** die voor operationele beveiliging zoeken naar indicatoren, deze valideren en gebruiken.
 - ▶ **Informatie-analysten** die informatie verzamelen over specifieke vijandige groepen.
 - ▶ De **politie** die vertrouwt op indicatoren om digitale onderzoeken te ondersteunen of op te starten.
 - ▶ **Risico analyse teams** die meer willen weten over nieuwe dreigingen, de waarschijnlijkheid van deze dreigingen en of deze dreigingen werden vastgesteld.
 - ▶ **Fraude analysten** die bereid zijn om indicatoren te delen om financiële fraude op te sporen.

HET BEHEERMODEL VAN MISP

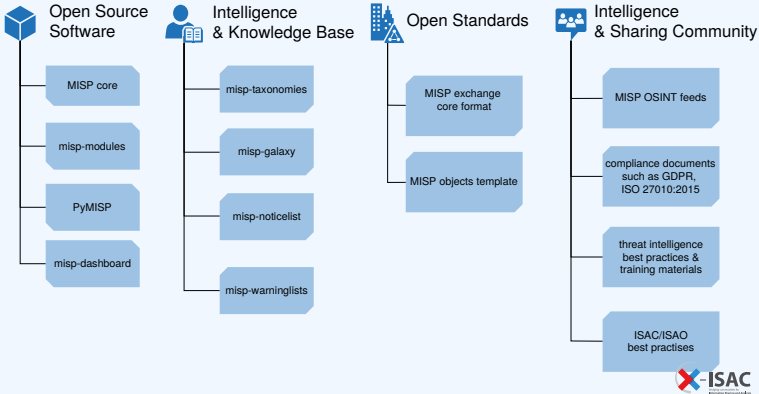


- Delen van indicatoren voor **detectie** doeleinden.
 - ▶ 'Heb ik geïnfecteerde systemen in mijn infrastructuur of onder mijn beheer?'
- Delen van indicatoren om te **blokkeren**.
 - ▶ 'Ik gebruik deze attributen om verkeer te blokkeren of om verkeer om te leiden.'
- Delen van indicatoren om **informatie te verzamelen**.
 - ▶ 'Informatie verzamelen over campagnes en aanvallen. Zijn deze campagnes met elkaar verbonden? Zijn ze gericht op mij? Wie zijn de tegenstanders?'
- → Deze doelstellingen kunnen soms tegenstrijdig zijn

- De problemen met het delen van informatie zijn vaak niet zozeer van technische aard maar eerder een kwestie van **sociale interacties** (b.v. **vertrouwen**).
- Juridische restricties¹
 - ▶ "Ons wettelijk kader staat ons niet toe om informatie te delen."
 - ▶ "Het risico op een informatielek is te hoog en het is te riskant voor onze organisatie of partners."
- Praktische beperkingen
 - ▶ "We hebben geen informatie om te delen."
 - ▶ "We hebben geen tijd om indicatoren te verwerken of om er te delen."
 - ▶ "Ons classificatie model past niet in uw model."
 - ▶ "De middelen voor het delen van informatie zijn gebonden aan een specifiek formaat en we gebruiken een ander formaat."

¹<https://www.misp-project.org/compliance/>

MISP PROJECT OVERZICHT

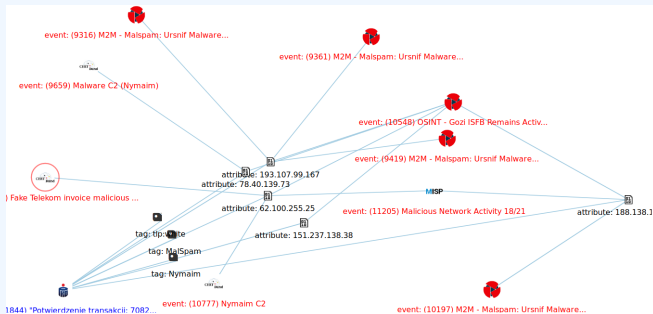


- MISP² is open source software voor het delen van dreigings-informatie.
- MISP heeft **een groot aantal functionaliteiten** die gebruikers ondersteunen bij het maken, samen werken aan en het delen van bedreigingsinformatie - bijv. flexibele groepen voor het delen van informatie, **automatische correlatie van gegevens**, importhulp, event distributie en voorstelling voor verbetering van attributen.
- Er is ondersteuning voor diverse formaten van IDS / IPS systemen (b.v. Suricata, Bro, Snort), SIEMs (b.v. CEF), host scanners (b.v. OpenIOC, STIX, CSV, yara), analyse tools (b.v. Maltego) of om DNS policies te implementeren (b.v. RPZ).
- Er is een breed aanbod aan MISP modules³ voor uitbreiding, import en export functionaliteiten.

²<https://github.com/MISP/MISP>

³<https://www.github.com/MISP/misp-modules>

CORRELATIES : EEN HULPMIDDEL VOOR ANALYSTEN

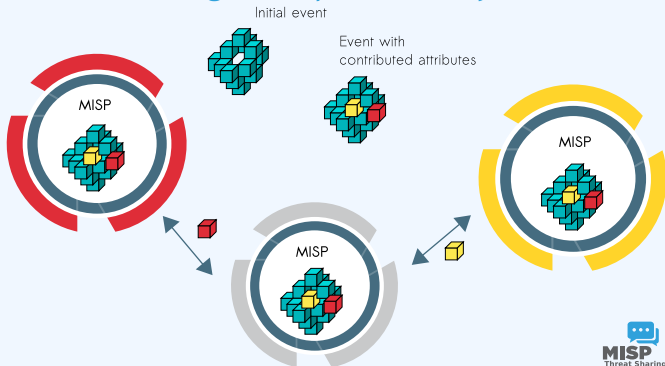


- Voor het **bevestigen van een bevinding** (b.v. is dit dezelfde campagne?), **of een analyse** (b.v. hebben andere analisten dezelfde hypothesis?), **bevestigen van een specifiek aspect** (b.v. werden deze sinkhole IP adressen gebruikt voor een campagne?) of het simpelweg uitzoeken of een **dreiging nieuw of onbekend is in je omgeving**.

- In het algemeen gaan gebruikers informatie delen met een groep met dezelfde objectieven of waarden.
- CIRCL beheert meerdere MISP-instanties met een aanzienlijke gebruikersbasis (meer dan 950 organisaties met meer dan 2400 gebruikers).
- **Vertrouwde** (gesloten) groepen die MISP gebruiken in een soort "eiland" modus (als een geïsoleerd systeem) of als een deels geconnecteerd systeem.
- De **financiële sector** (banken, ISACs, organisaties die betalingen verwerken) gebruikt MISP als een mechanisme voor het delen van informatie.
- **Militaire en internationale organisaties** (NATO, militaire CSIRTs, n/g CERTs,...).
- **Security bedrijven** die hun eigen gemeenschap starten (b.v. Fidelis) of een koppeling hebben met een MISP gemeenschap (b.v. OTX).

MISP BASISFUNCTIES VOOR GEDISTRIBUEERD DELEN

- De kernfunctionaliteit van MISP is het delen van informatie waarbij iedereen zowel een consument als een producent (bijdrager) kan zijn.
- Dit heeft als voordeel dat iedereen snel kan deelnemen, zonder de directe verplichting om zelf bij te dragen.
- Er is een lage drempel om het systeem te leren kennen.



- Een MISP event is een verzameling van contextueel verbonden informatie.
- Attributen⁴ starten initieel met een standaard groep van "cyber security" indicatoren.
- Attributen zijn puur **gebaseerd op gebruik**. De verbetering gebeuren voornamelijk op basis van praktische noden (**financiële indicatoren** in versie 2.4).
- Objecten zijn samengestelde attributen die verschillende datapunten beschrijven, opgebouwd uit templates van de gemeenschap en de gebruikers.
- Galaxies zorgen voor een granulaire context, classificatie en categorisatie van de gegevens gebaseerd op **dreigings actoren, preventie maatregelen** en de hulpmiddelen gebruikt door tegenstanders.

⁴attributen kunnen alles zijn zolang ze bijdragen aan het beschrijven van de intentie van het event, b.v. indicatoren, kwetsbaarheden ...

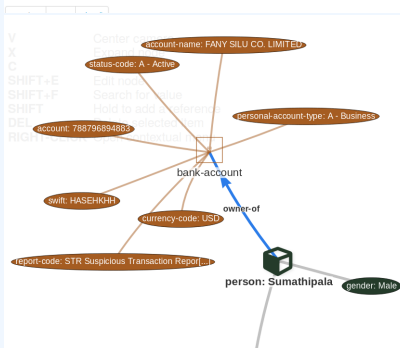
DELEN VAN TECHNIKEN VAN AANVALLEERS

- MISP heeft integratie op zowel event als attribuut niveau voor MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

| Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Exfiltration | Command and control |
|-------------------------------------|------------------------------------|---|----------------------------------|----------------------------------|--|--|------------------------------------|------------------------------------|---|---------------------------------------|
| Spearphishing Attachment | Scripting | Screen saver | File System Permissions Weakness | Process Hollowing | Secured Memory | Password Policy Discovery | AppleScript | Data from Information Repositories | Exfiltration Over Alternative Protocol | Standard Application Layer Protocol |
| Spearphishing via Service | Command-Line Interface | Login Item | AppCert DLLs | Code Signing | Input Capture | System Network Configuration Discovery | Distributed Component Object Model | Data from Removable Media | Exfiltration Over Command and Control Channel | Communication Through Removable Media |
| Trusted Relationship | User Execution | Trap | Application Shimming | Rookit | Bash History | Process Discovery | Pass the Hash | Man in the Browser | Data Compressed | Custom Command and Control Protocol |
| Replication Through Removable Media | Regsvcs/Regasm | System Firmware | Scheduled Task | NTFS File Attributes | Exploitation for Credential Access | Network Share Discovery | Exploitation of Remote Services | Data Staged | Automated Exfiltration | Multi-Stage Channels |
| Exploit Public Facing Application | Trusted Developer Utilities | Registry Run Keys / Start Folder | Startup Items | Exploitation for Defense Evasion | Private Keys | Peripheral Device Discovery | Remote Desktop Protocol | Screen Capture | Scheduled Transfer | Remote Access Tools |
| Spearphishing Link | Windows Management Instrumentation | LC_LOAD_DYLIB Addition | New Service | Network Share Connection Removal | Brute Force | Account Discovery | Pass the Ticket | Email Collection | Data Encrypted | Uncommonly Used Port |
| Valid Accounts | Service Execution | LSASS Driver | Sudo Caching | Process Doppelgänger | Password Filter DLL | System Information Discovery | Windows Remote Management | Clipboard Data | Exfiltration Over Other Network Medium | Multilayer Encryption |
| Supply Chain Compromise | CMSTP | Rc common | Process Injection | Disabling Security Tools | Two-Factor Authentication Interception | System Network Connections Discovery | Windows Admin Shares | Video Capture | Exfiltration Over Physical Medium | Domain Fronting |
| Drive-by Compromise | Control Panel Items | Authentication Package | Bypass User Account Control | Timestamp | LLMNR/NBT-NS Poisoning | Network Service Scanning | Remote Services | Audio Capture | Data Transfer Size Limits | Data Obfuscation |
| Hardware Additions | Dynamic Data Exchange | Component Firmware | Extra Window Memory Injection | Modify Registry | Credentials in Files | File and Directory Discovery | Taint Shared Content | Data from Network Shared Drive | | Connection Proxy |
| | Source | Windows Management Instrumentation Event Subscription | Sehuid and Setgid | Indicator Removal from Tools | Forced Authentication | Security Software Discovery | Application Deployment Software | Data from Local System | | Commonly Used Port |
| | Space after Filename | Change Default File | Launch Daemon | Hidden Window | Keychain | System Service Discovery | Third-party Software | Automated Collection | | Data Encoding |

ONDERSTEUNING VOOR EEN SPECIFIEK DATAMODEL

| Date | Org | Category | Type | Value | Tags | Galaxies | Comment | Correlate | Related Events |
|------------|-----|-----------------|--------------------------------|-------------------------------------|------|----------|---------|-------------------------------------|------------------|
| 2018-09-28 | | | | Name: bank-account References: 0 | | | | | |
| 2018-09-28 | | Other | status-code: text | A - Active | - | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Other | report-code: text | STR Suspicious Transaction Report | - | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Other | personal-account-type: text | A - Business | - | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Financial fraud | swift: bic | HASEHKHH | - | Add | | <input checked="" type="checkbox"/> | 3849 11320 11584 |
| 2018-09-28 | | Financial fraud | account: bank-account-er | 788796894883 | - | Add | | <input checked="" type="checkbox"/> | |
| 2018-09-28 | | Other | account-name: text | FANY SILU CO. LIMITED | - | Add | | <input checked="" type="checkbox"/> | |
| 2018-09-28 | | Other | currency-code: text | USD | - | Add | | <input type="checkbox"/> | |



- Indicatoren⁵
 - ▶ Indicatoren beschrijven een patroon dat kan gebruikt worden om verdachte of kwaadaardige traffic te detecteren.
- Attributen in MISP kunnen netwerk indicatoren (b.v. IP adressen), systeem indicatoren (b.v. tekst in het geheugen) of zelfs bank gegevens zijn.
 - ▶ Een **type** (b.v. MD5, url) is hoe een attribuut is beschreven.
 - ▶ Een attribuut behoort altijd tot een categorie (b.v. Payload delivery). Deze categorie plaatst het attribuut in een bepaalde context.
 - **Een categorie bepaalt de context** van een attribuut.
 - ▶ De IDS instelling op een attribuut bepaald of **dit attribuut automatisch** zal gebruikt worden voor **detectie** doeleinden.

⁵IoC (Indicator of Compromise) zijn een onderdeel van de indicatoren

- Gebruikers kunnen events of attributen bijvoegen via zowel de web interface, de API als via een vrije tekst veld.
 - ▶ Er zijn modules in Viper (een framework voor het analyseren van malware) om data in MISP in te vullen, via de vty of via IDA.
- Een bijdrage kan gebeuren door rechtstreeks een event aan te maken maar gebruikers kunnen ook de eigenaar van een event een **update voorstellen voor attributen**.
- Gebruikers zijn **niet gedwongen om één interface te gebruiken om gegevens aan MISP bij te voegen**.

VOORBEELD: VRIJE TEKST IMPORT IN MISP









Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

This is a sample text to show how indicators can be extracted. Just paste your text including indicators such as 23.100.122.175, host.microsoft.com, or b447c27a00e3a348881b0030177000cd in here and the tool will automatically detect the indicators and save them as attributes - after allowing you to make some last minute changes. For more information, visit <https://www.github.com/MISP/MISP>









Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

| Value | Category | Type | IDS | Comment | Actions |
|----------------------------------|------------------|----------|-------------------------------------|-----------------------------------|---|
| 23.100.122.175 | Network activity | ip-dst | <input checked="" type="checkbox"/> | Imported via the freetext import. |   |
| host.microsoft.com | Network activity | hostname | <input checked="" type="checkbox"/> | Imported via the freetext import. |   |
| b447c27a00e3a348881b0030177000cd | Payload delivery | md5 | <input checked="" type="checkbox"/> | Imported via the freetext import. |   |
| https://www.github.com/MISP/MISP | Network activity | url | <input checked="" type="checkbox"/> | Imported via the freetext import. |   |

ip-dst → ip-src

Update all comment fields

| Date | Org | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|------------|-----|------------------|----------|----------------------------------|-----------------------------------|----------------|-----|--------------|---|
| 2016-02-24 | | Network activity | hostname | host.microsoft.com | Imported via the freetext import. | | Yes | Inherit |   |
| 2016-02-24 | | Network activity | ip-dst | 23.100.122.175 | Imported via the freetext import. | 298 | Yes | Inherit |   |
| 2016-02-24 | | Network activity | url | https://www.github.com/MISP/MISP | Imported via the freetext import. | | Yes | Inherit |   |
| 2016-02-24 | | Payload delivery | md5 | b447c27a00e3a348881b0030177000cd | Imported via the freetext import. | | Yes | Inherit |   |

ONDERSTEUNING VOOR CLASSIFICATIES

- Het gebruik van tags is een simpele manier om een classificatie toe te voegen aan een event of attribuut.
- Een **classificatie moet globaal** in gebruik zijn om ook efficiënt te zijn.
- Gebruikers kunnen via een flexibel tagging systeem kiezen uit de meer dan 42 bestaande taxonomieën of ze kunnen hun eigen taxonomie bijvoegen.

| | | | | | | | | | | |
|------|---|---|---|-----------------|----|----|--|--------------------------|--|--|
| 18 | ✓ | ✗ | admiralty-scale-information-credibility="1" | admiralty-scale | 4 | 0 | | <input type="checkbox"/> | | |
| 19 | ✓ | ✗ | admiralty-scale-information-credibility="2" | admiralty-scale | 15 | 1 | | <input type="checkbox"/> | | |
| 20 | ✓ | ✗ | admiralty-scale-information-credibility="3" | admiralty-scale | 12 | 4 | | <input type="checkbox"/> | | |
| 21 | ✓ | ✗ | admiralty-scale-information-credibility="4" | admiralty-scale | 1 | 0 | | <input type="checkbox"/> | | |
| 22 | ✓ | ✗ | admiralty-scale-information-credibility="5" | admiralty-scale | 1 | 0 | | <input type="checkbox"/> | | |
| 23 | ✓ | ✗ | admiralty-scale-information-credibility="6" | admiralty-scale | 2 | 0 | | <input type="checkbox"/> | | |
| 12 | ✓ | ✗ | admiralty-scale-source-reliability="a" | admiralty-scale | 0 | 0 | | <input type="checkbox"/> | | |
| 13 | ✓ | ✗ | admiralty-scale-source-reliability="b" | admiralty-scale | 15 | 53 | | <input type="checkbox"/> | | |
| 14 | ✓ | ✗ | admiralty-scale-source-reliability="c" | admiralty-scale | 5 | 2 | | <input type="checkbox"/> | | |
| 15 | ✓ | ✗ | admiralty-scale-source-reliability="d" | admiralty-scale | 1 | 0 | | <input type="checkbox"/> | | |
| 16 | ✓ | ✗ | admiralty-scale-source-reliability="e" | admiralty-scale | 0 | 0 | | <input type="checkbox"/> | | |
| 17 | ✓ | ✗ | admiralty-scale-source-reliability="f" | admiralty-scale | 4 | 2 | | <input type="checkbox"/> | | |
| 1203 | ✓ | ✗ | adversary-infrastructure-action="monitoring-active" | adversary | 1 | 0 | | <input type="checkbox"/> | | |
| 1201 | ✓ | ✗ | adversary-infrastructure-action="passive-only" | adversary | 0 | 0 | | <input type="checkbox"/> | | |

- Delegeren van de publicatie van events naar andere organisaties (sinds MISP 2.4.18).
 - ▶ Deze andere organisatie kan dan eigenaar worden van het event en op deze manier zorgen voor de **pseudo-anonimiteit van de oorspronkelijke organisatie**.
- Definiëren van groepen om specifieke informatie mee te delen (vanaf 2.4).
 - ▶ De gemeenschappen om mee te delen kunnen lokaal of tussen verschillende MISP instanties gebruikt worden.
 - ▶ Het delen kan gebeuren op zowel **event** als **attribuut** niveau (b.v. financiële indicatoren met de financiële groepen en cyber security indicatoren met de CSIRT gemeenschap).

ONDERSTEUNING VOOR WAARNEMINGEN

The screenshot displays a user interface for managing security events. At the top, there is a table of 'Events' with columns for checkboxes, status, and actions. A tooltip for 'Sightings' is shown, indicating 'CIRCL: 2 (2017-03-19 16:17:59)'. Below the table, a 'Tags' section is visible, followed by a 'Sighting Details' panel. The 'Sighting Details' panel shows a status of 'No' and a count of '4 (2) - restricted to own organisation only.' for 'MISP: 2' and 'CIRCL: 2'. A 'Discussion' button is located at the bottom of the details panel.

| Events | | | |
|-------------------------------------|----|--|--|
| <input checked="" type="checkbox"/> | No | Sightings CIRCL: 2 (2017-03-19 16:17:59) | |
| <input checked="" type="checkbox"/> | No | (2/0/0) | |
| <input checked="" type="checkbox"/> | No | Inherit (0/0/0) | |

Tags

Date 2016-02-24

Threat Level High

Analysis Initial

Distribution Connected communities

freetext test

Sighting Details

No

MISP: 2 4 (2) - restricted to own organisation only.

CIRCL: 2

Discussion

- Gebruikers kunnen via **waarnemingen** de gemeenschap op de hoogte stellen van activiteit gerelateerd aan een indicator.
- Het is mogelijk om negatieve waarnemingen (false positives) en waarnemingen met een vervaldatum in te geven.
- Waarnemingen kunnen gebeuren via de web interface, de API of door STIX waarnemings-documenten te importeren.
- Er zijn verschillende toepassingen om indicatoren te rangschikken op basis van waarnemingen.

VERBETERINGEN VOOR HET DELEN VAN INFORMATIE IN MISP

- Valse posieven (false-positive) blijven een terugkerende uitdaging bij het delen van informatie.
- Vanaf MISP 2.4.39 hebben we het concept van `misp-warninglists`⁶ geïntroduceerd om de analisten te ondersteunen bij hun dagtaak.
- Dit zijn voorgedefinieerde lijsten van indicatoren die vaak een valse positieve zijn, zoals bijvoorbeeld RFC1918 netwerken of publieke DNS servers.

⁶<https://github.com/MISP/misp-warninglists>

ONDERSTEUNING VOOR HET DELEN BINNEN EN BUITEN EEN ORGANISATIE

- Zelfs binnen één en dezelfde omgeving kunnen er verschillende use cases zijn voor het gebruik van MISP (b.v. groepen die MISP gebruiken voor dynamische malware analyse en correlatie, andere groepen die het dan weer gebruiken voor het versturen van meldingen).
- Vanaf MISP 2.4.51, is er de optie om **lokale MISP** servers met elkaar te verbinden. Zo kan je verschillende niveaus van delen voorkomen en kan je van een gemengde synchronisatie gebruik maken, zowel binnen als buiten de organisatie.
- Er is ondersteuning voor feeds voor synchronisatie tussen vertrouwde en niet vertrouwde netwerken.

- We onderhouden de standaard CIRCL OSINT-feeds (TLP:WHITE geselecteerd uit onze gemeenschappen) zodat gebruikers snel aan de slag kunnen gaan met MISP.
- Het formaat van de OSINT-feed is gebaseerd op standaard MISP JSON-uitvoer van een externe TLS / HTTP-server.
- Aanvullende contentproviders kunnen hun eigen MISP-feeds leveren. (<https://botvrij.eu/>).
- Dit laat gebruikers toe om hun MISP-installaties te **testen en te synchroniseren met een echte gegevensset**.
- Dit kan bijdragen aan andere bronnen van dreigings informatie en helpt ook bij de analyse naar overlappende data⁷.

⁷Een steeds terugkerende uitdaging bij het delen van informatie

- **De manier van informatie delen ontstaat voornamelijk uit het gebruik** en het volgen van bestaande voorbeelden.
- MISP is uiteindelijk slechts een hulpmiddel, het belangrijkste is nog altijd de manier hoe je de informatie deelt. De tool moet u daarbij zo transparant mogelijk ondersteunen tijdens uw werk.
- Gebruikers moeten MISP kunnen aanpassen zodat zij een oplossing hebben voor de noden van hun gemeenschap.
- Het MISP project combineert open source software, open standaarden, best practices en gemeenschappen om informatie deling te realiseren.