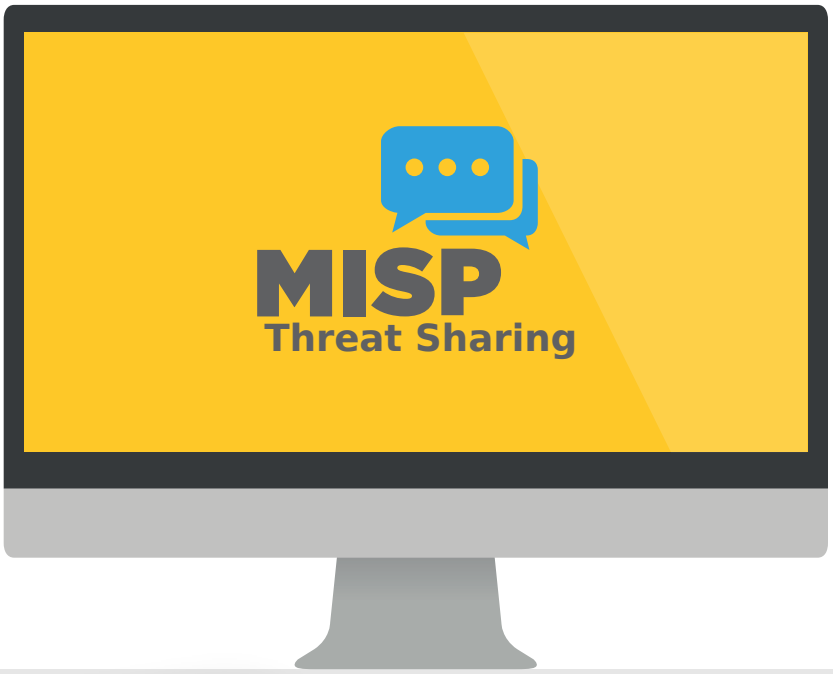
Best practice

MISP en informatie delen over incidenten



CYBERVEILIG NEDERLAND

Inhoudsopgave

- STANDAARD WERKWIJZE MISP VOOR INCIDENT RESPONSE EN INFORMATIEDELEN 3
- HET GEBRUIK VAN MISP 3
- WELKE INCIDENT-INFORMATIE WISSELEN WE UIT? 3
- MISP-WERKWIJZE 4
  - OPBOUW VAN EVENTS 5
  - OPBOUW VAN OBJECTEN EN ATTRIBUTEN 5

Standaard werkwijze MISP voor incident response en informatiedelen

Binnen Cyberveilig Nederland werken we aan het verbeteren van informatie-uitwisseling. Met name als het gaat om dreigingsinformatie is er sprake van steeds verdergaande samenwerking tussen securitybedrijven onderling en samenwerking met de Nederlandse overheid. In de toekomst zal deze samenwerking verder verbreden naar andere samenwerkingspartners.Door informatie-uitwisseling te verbeteren kunnen we de cyberdreiging in Nederland verminderen en de weerbaarheid tegen cyberincidenten verhogen.
Om samenwerking zo goed mogelijk tot stand te brengen is het verstandig om afspraken te maken over de wijze waarop informatie wordt vastgelegd en gedeeld. Op die manier kunnen betrokken organisaties beter de ontvangen informatie verwerken en analyseren.

Het gebruik van MISP

Een veelgebruikt platform voor informatieuitwisseling is MISP (zie https://www.misp-project.org/). Diverse van de leden en samenwerkingspartners van Cyberveilig Nederland maken gebruik van dit open source platform. Om te komen tot een effectieve informatie-uitwisseling is het wenselijk dat organisaties die informatie over cyberincidenten willen uitwisselen, deze op een uniforme wijze vastleggen.

Dit document introduceert een standaard werkwijze voor het gebruik van MISP voor de leden van Cyberveilig Nederland, maar idealiter ook voor andere organisaties die werken met MISP en (in de toekomst) willen deelnemen aan initiatieven over informatie-uitwisseling. Het gaat hier om het introduceren van een best practice.

De werkwijze is vooralsnog gericht op het uitwisselen van informatie over cyberincidenten en veronderstelt basiskennis van MISP.

De werkwijze gaat voornamelijk over operationele en tactische informatie over cyberincidenten en het vastleggen hiervan op uniforme wijze: het algemeen gebruik van MISP, zoals het aanmaken van Events, Objects en Attributes en hoe deze te voorzien van Tags en Clusters.

Dit document borduurt voort op de best practices van het team dat MISP ontwikkelt. Informatie over deze best practices is te vinden op https://www.circl.lu/doc/misp/best-practices/. Het document gaat in op hoe informatie over incidenten wordt vastgelegd. Er wordt niet beschreven welke soort incidenten wanneer worden vastgelegd, of hoe deze worden gedeeld. Dat kan per initiatief om informatie te delen verschillen.

Dit document is bedoeld voor organisaties die (in de toekomst) willen deelnemen aan informatie-uitwisselingsprogramma's. Het is geschreven voor incident responders en threat intel analisten, en veronderstelt enige basiskennis over begrippen binnen MISP zoals Events, Objects, Attributes, Tags en Clusters.

Welke incident-informatie wisselen we uit?

Volgens het Cybersecurity Woordenboek is een incident een gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken.

Informatie over incidenten die in een MISP-omgeving kan worden opgenomen betreft operationele informatie, zoals lijsten van Indicators of Compromise (IOCs), aangevuld met tactische informatie en context. Denk hierbij bijvoorbeeld aan gebruikte MITRE ATT&CK technieken, maar ook aan informatie over hoe de eventuele gesprekken en onderhandelingen met de daders verliepen.

Met deze tactische informatie wordt – zo compleet als mogelijk – de gehele set van gebeurtenissen binnen het incident beschreven. Zowel de operationele als tactische informatie is daarbij relevant, dus ook de operationele IOCs, ten behoeve van geautomatiseerde detectie en correlatie met al afgehandelde incidenten.

Door zowel operationele als tactische informatie op te slaan en uit te wisselen, maken we het mogelijk om een gezamenlijk beeld te vormen van wat er gebeurt in Nederland rondom de verschillende cyberincidenten en kan de weerbaarheid worden verhoogd en de dreiging worden verminderd.

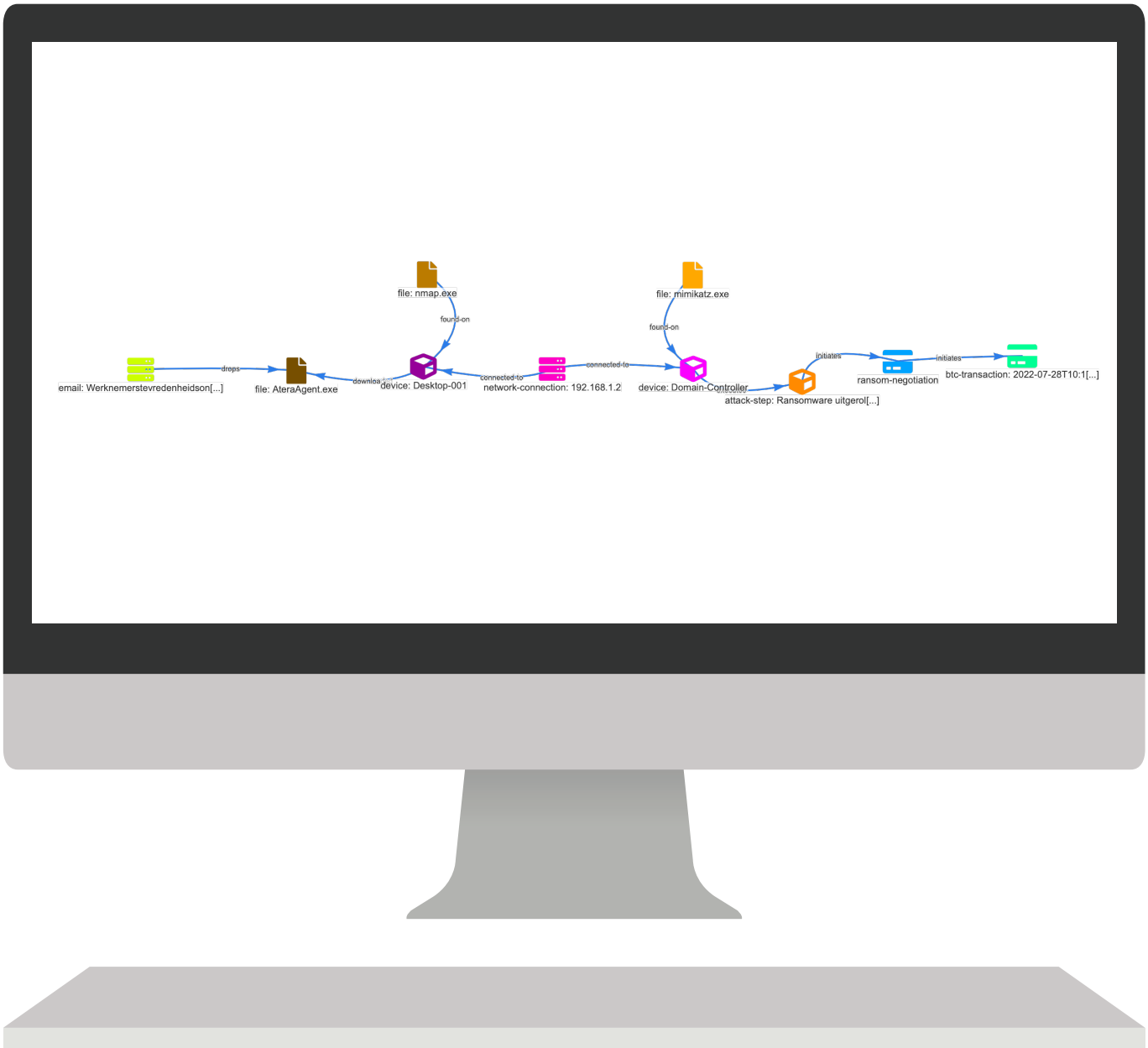
MISP-werkwijze

Onderstaande paragraaf legt verder uit hoe de voorgestelde werkwijze eruitziet op gebied van:

- Opbouw van Events
- Opbouw van Objecten en Attributen

Er is bij deze werkwijze een voorbeeld gevoegd van een gemodelleerd incident in MISP JSON-formaat, dat gebruikt kan worden om meer inzicht te krijgen. Dit bestand bevat een fictief en versimpeld ransomwareincident. Het is opgebouwd volgens de hieronder beschreven wijze.

Na importeren van dit event in een MISP-server, ziet de Event graph er als volgt uit:

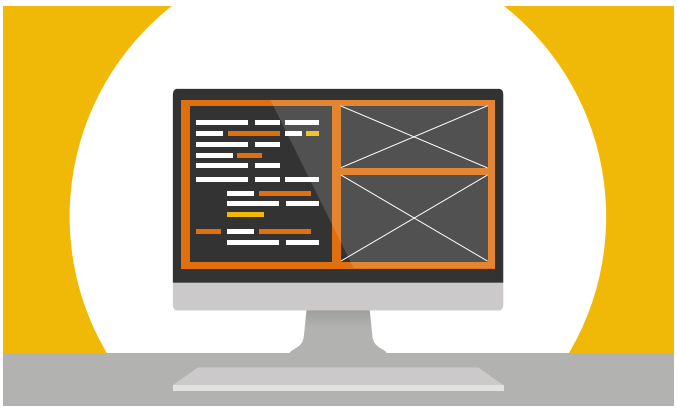


Opbouw van Events

Cyberincidenten worden in de basis binnen MISP gemodelleerd in Events. Events worden zo veel als mogelijk opgebouwd uit Objects die standaard met MISP worden meegeleverd. Het groeperen van Attributes in Objects geeft meer context aan deze attributen mee en maakt daarmee de informatie rijker. Soms zijn er meerdere Object-types te kiezen. Het is van belang om telkens het best passende Object-type te selecteren dat past bij het betreffende cyberincident.

Tip: Als je een set al bestaande Attributes selecteert, en op de knop “Group selected attributes into an object” drukt, laat MISP de best passende Object-types zien.

Mocht er geen geschikt Object-type zijn, kun voor het type temporal-event gekozen worden. Hiermee wordt een gebeurtenis op tactisch niveau omschreven, inclusief Tags en Clusters.



Events worden op top-level minstens getagd met Tags uit de volgende taxonomieën:

- Een tag uit de TLP-taxonomie
- Een tag uit de PAP-taxonomie

Voor wat betreft Clusters bevatten ze:

- Alle binnen het event gebruikte ATT&CK-clusters (Als je eerst alle Attributes van een ATT&CK-cluster voorziet, kun je deze daarna eenvoudig selecteren op Event-niveau.)
- Een Cluster uit de Country-galaxy
- Een Cluster uit de Sector-galaxy
- Een Cluster uit de door Trellix ter beschikking gestelde actor-galaxy

Trellix stelt voor leden van Cyberveilig Nederland twee Galaxies beschikbaar die uitgebreid en up-to-date threat actors en hun tools omschrijven. Voor niet-leden raden we aan gebruik te maken van de standaard met MISP meegeleverde Actor-galaxy. Deze wordt minder frequent bijgewerkt, maar zorgt wel voor een goed uitwisselbare categorisering.

Door deze Clusters toe te voegen worden Events makkelijk te sorteren en vindbaar gemaakt. Ook helpen ze met het achteraf statistisch analyseren: zijn er bijvoorbeeld sectoren die vaker slachtoffer worden van een incident dan andere?

Opbouw van Objecten en Attributen

Losse Attributes worden getagd met minstens de volgende taxonomieën:

- Unified Kill Chain
- Ransomware Roles (indien het een ransomware gerelateerd Event betreft)

Indien het Attribute een TLP- of PAP-waarde kent die afwijkt van het gehele Event, wordt het Attribute getagd met deze afwijkende waarde.

Als attributen gemarkeerd worden als geschikt voor IDS-gebruik middels de IDS-vlag, is het gebruikelijk dat deze vlag na enige tijd weer uitgezet wordt. Immers, IOCs blijven niet oneindig goed. Conform het MISP-model is het aan de delende/creërende organisatie om deze vlag (al dan niet automatisch) op enig moment uit te zetten en het Event te herpubliceren. Uiteraard staat het ontvangende organisaties vrij om deze vlag eerder zelf uit te zetten.

Verder worden Attributes van Clusters uit de volgende Galaxies voorzien:

- MITRE ATT&CK Patterns
- De door Trellix beschikbaar gestelde Threat Actor library
- De door Trellix beschikbaar gestelde Tool library

Objecten kunnen niet zelf getagd worden, in plaats daarvan wordt het meest kenmerkende Attribute van een Object getagd. Merk op dat het “meest kenmerkende” niet per se het meest unieke Attribute is. Bij bijvoorbeeld een file-object is het meest kenmerkende Attribute de filename – dat is makkelijker te herkennen dan bijvoorbeeld een hash.

Objecten kunnen refereren naar andere Objecten. Dat is een handige manier om weer te geven dat bijvoorbeeld een kwaadaardige e-mail een bepaald bestand gedropt heeft. Het is verstandig zoveel als mogelijk gebruik te maken van deze referenties. Dat helpt om een volgorde in de gebeurtenissen terug te lezen.

Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld. Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op cyberveilignederland.nl

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10

Deze uitgave is mede mogelijk gemaakt door:

CYBERVEILIG NEDERLAND