Myndigheten
för civilt försvar

Arbetssätt och rutiner MISP-SE

Innehållsförteckning

Myndigheten
för civilt försvar

Versionshantering

Version	Datum	Vad	Vem
1.0	2025-03-05	Fastställer version 1.0 (utestående frågor kommer att hanteras till senare version)	AB
1.1	2025-12-05	Helhetsöversyn.	HR
1.2	2025-01-20	Ändring från ”MSB” till ”Myndigheten för civilt försvar”. Förtydligande kring distribution.	HR

Myndigheten
för civilt försvar

Introduktion

Syftet med detta dokument är att beskriva och definiera de arbetsmetoder och standardiserade rutiner som ska följas i MISP-SE:s för att säkerställa en effektiv, konsekvent och högkvalitativ arbetsprocess. Dokumentet ska användas som stöd av roller som arbetar regelbundet med MISP-SE.

Avgränsningar

Arbetssätt och rutiner beskriver inte hur användare praktiskt ska gå tillväga för att publicera event eller på andra sätt arbeta i MISP. För praktisk vägledning hänvisas till CIRCL:s[1] användarguide.

Anslutning till MISP-SE

Ansökan

Ansökan om medlemskap i MISP-SE görs till CERT-SE utifrån instruktionerna på cert.se. För att bli medlem krävs att organisationen uppfyller samtliga villkor. När ansökan är godkänd genomförs följande steg för anslutning.

Organisationsadministratör

För varje organisation som ansluter sig via webbgränssnitt registreras en person som organisationens administratör ”Org-Admin”. Denna användare förfogar över utökade rättigheter för sin organisation och kan själv lägga till och administrera användare i sin organisation. Därvid måste Org-Admin säkerställa att ytterligare användare i dennes organisation får kännedom om användarvillkoren. Org-Admin får endast skapa konton för medlemmar i sin organisation, som har behov av det innehåll som tillhandahålls i MISP-SE.

Synk-användare

Organisationer som ansluter sig via API behöver skapa en synk-användare för automatiskt utbyte av information mellan MISP-SE och organisationens MISP-instans. Mer information om denna roll finns på CIRCL:s webbsida.

Avslut av användare

Org-Admin kan ta bort användare i den egna organisationen. Myndigheten för civilt försvar tar bort användarkonton (ej Org-admin) som varit inaktiva de senaste 90 dagarna.

[1] Computer Incident Response Center Luxembourg.

Myndigheten
för civilt försvar

Användning av MISP

När en användare skapar ett nytt event i MISP behöver användaren tagga informationen. Det innebär att användaren taggar eventet och informationen med olika slags attribut som dels berikar informationen, dels underlättar sökbarhet och möjlighet till filtrering för mottagare.

Det finns möjlighet att välja mellan ett flertal redan definierade taggar eller att skapa nya/egna taggar. Myndigheten för civilt försvar rekommenderar användare att primärt använda redan definierade taggar för att skapa möjlighet till enklare spårbarhet, hitta korrelation och förstå informationen.

I följande avsnitt beskrivs vilka rutiner som **ska**[2], **bör**[3] och **kan**[4] följas av användare i MISP-SE.

Principer för delning och användning av information i MISP-SE

Nedan principer är tillägg till de användarvillkor som beskrivs i dokumentet Allmänna villkor MISP-SE, och som respektive ansluten organisation har åtagit sig att följa.

1. Information delas så skyndsamt som möjligt. Snabbt tillgängliggörande av information prioriteras före perfektion.
2. Initialt delas tillräckligt med information för att mottagaren ska kunna agera. I ett senare skede kan ytterligare information läggas till för mer kontext.
3. Berikning av andra organisationer event uppmuntras.
4. Information som delas bör utgå från observationer användaren/organisationen själv har gjort.

Vilken information delas i MISP-SE?

Den information som delas i MISP-SE kan delas in i olika kategorier och informationstyper. De *vanligaste* kategorierna av information som delas i MISP-SE rör:

- Phishing
- DoS/DDoS
- Malware-data
- Uppgifter om intrångsförsök (se *Pyramid of Pain*).

Observera att kategorierna inte innebär någon begränsning utan endast anger en indikation om vanligast förekommande. För nya användare av MISP rekommenderar Myndigheten för civilt försvar att användare börjar med delning av event om phishing.

Därtill kan ett flertal andra kategorier av information också förekomma, såsom rapporter om cyberhot och kampanjer, bedrägerier, finansiella hot, hot kopplat till leverantörskedja eller tredjepartsrisker.

Några av de vanligaste typerna av information som delas i MISP-SE är:

- IP-adresser till angripare (eller påstådda angripare)
- Domäner från komprometterade (eller förmodat komprometterade) webbplatser
- Specifika webbadresser med skadligt innehåll

[2] Rutiner som *ska* följas ska betraktas som obligatoriska krav.
[3] Rutiner som *bör* följas ska betraktas som rekommendationer.
[4] Rutiner som *kan* följas ska betraktas som förslag som följs om användaren bedömer det som lämpligt.

- Signaturer eller hashar av filer med skadligt innehåll
- E-postadresser som sprider skadligt innehåll eller phishing
- Hotdetekteringsregler baserade på nätverksbeteende (SNORT-regler), eller detektion av skadligt innehåll (YARA-regler)
- Specifika webbläsarheaders, såsom "user-agent" med flera.

Vilken information delas inte MISP-SE?

I MISP-SE ska det inte delas information av följande karaktär:

- Information om scanners src-IP.
- Återpublicering av event från publika feeds.

Distribution av event

I MISP finns olika långtgående möjligheter att distribuera ett event. Se CIRCL:s instruktioner för mer information. Notera att lokala användare i MISP-SE (webbgränssnitt) måste välja *connected communities* för att även API-anslutna organisationer ska kunna ta del av publicerat event.

Hur ska information taggas?

Syftet med att tagga information utifrån förutbestämda taxonomier och ramverk är att underlätta för användare, såsom för att skapa en lättöverskådlig bild av eventet och för att ensa data vilket gör det lättare att filtrera.[5]

Det är upp till varje ansluten organisation att bedöma vad som ska delas, hur och till vem.

Reference Security Incident Taxonomy (RSIT)

RSIT är en taxonomi för incidenter och är inkluderad i MISP *by default*. Om en incidentkategori kan anges för att definiera händelsetyp, så bör RSIT-taxonomin användas.

Traffic Light Protocol (TLP)

Den metod som ska användas för att märka information i MISP-SE är TLP. Informationsdelning sker från en informationskälla, till en eller flera mottagare. Endast etiketter som anges i denna standard anses giltiga. Mer information om TLP och dess olika nivåer återfinns på https://www.first.org/tlp/.

- Om TLP-nivå inte är angiven **ska** TLP:AMBER förutsättas.

I MISP-SE får information upp till TLP AMBER+STRICT delas. Organisationer och användare som är nya till MISP rekommenderas att börja dela information märkt TLP:CLEAR eller TLP:GREEN.

Det är av högsta vikt att TLP-märkningen följs. Om en organisation inte efterlever dessa regler riskerar organisationen att uteslutas från MISP-SE.

Permissible Acition Protocol (PAP)

Permissible Action Protocol (PAP) introducerades 2016 i taxonomierna för MISP, som underhålls och utvecklas av CIRCL. PAP anger i vilken utsträckning en viss information kan exponeras. Tanken är att

[5] För mer information om taxonomier enlig CIRCL:s misp-project och internationell best practice, se exempelvis https://www.circl.lu/doc/misp/taxonomy/#taxonomies samt https://www.misp-project.org/taxonomies.html#_misp_taxonomies

definiera en uppsättning möjliga åtgärder med hänsyn till den information som den kan avslöja för en illvillig aktör. Se mer information om PAP och dess olika nivåer på https://cert.ssi.gouv.fr/csirt/sharing-policy/.

- Om PAP-nivån inte är definierad **ska** PAP:GREEN förutsättas.

Källors och informations tillförlitlighet och trovärdighet

Källor och information kan ha olika tillförlitlighet och trovärdighet. Event-information om detta **kan** inkluderas i MISP-SE genom användning av Admirality-scale som är inkluderad i MISP *by default*.

Taxonomi för händelsetyper

Event **bör** berikas med händelsespecifika taggar för att ge mottagaren bättre information att agera utifrån. I bilaga 1 beskrivs innebörden av några av de vanligaste taggarna i MISP.

Språk

Informationen som delas i MISP-SE ska företrädesvis vara på engelska. Syftet är att arbeta enligt det etablerade arbetsspråket i MISP och därmed underlätta samarbeten, överföring av information med mera.

Galaxies

MISP-galaxer och kluster används för att sätta data i ett sammanhang. Jämfört med det relativt enkla konceptet med taggar och taxonomier gör de det möjligt att lägga till mer komplexa datastrukturer. Det finns *default vocabularies* tillgängliga i MISP Galaxy men de kan skrivas över, ersättas eller uppdateras efter behov. *Vocabularies* kommer från befintliga standarder (t.ex. STIX, Veris, ATT&CK och så vidare). I MISP-SE används befintliga standarder.

Att skapa ett event

Event Info

Rubriken är avgörande för att mottagare snabbt ska få en överblick, förstå vad eventet handlar om och kunna göra en första bedömning om relevans för den egna organisationen.
Myndigheten för civilt försvars riktlinjer är därför att rubriken ska vara informativ, tydlig och som utgångspunkt inte innehålla samma information som finns i själva eventet.

Huvudregeln är att följande information alltid bör vara inkluderad:

- Vad för händelse/typ av larm (såsom phishing scam)
- Vad händelsen avser (kampanj, insamling eller liknande).

Summering

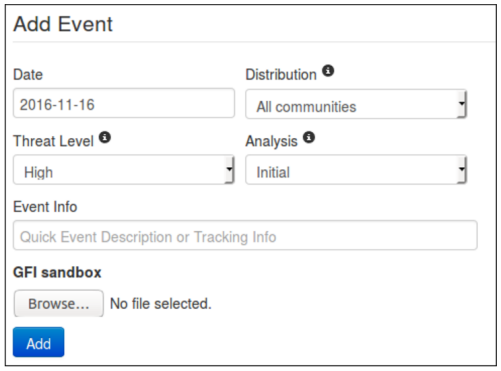
Datum: Datumet för när rapporten skapades.

Distribution: Beskriver vilken spridning rapporten har, om den är offentlig etc.

Threat level: Beskriver risken för att andra organisationer som tar emot informationen ska drabbas utifrån ”låg”, ”medium” eller ”hög”.

Analysis: Beskriver det aktuella stadiet i analysen, om analysen är klar eller inte.

Event info: Är samma som namnet eller titeln på eventet.



Taggar

Observera att nedan taggar utgör exempel på hur användare kan märka sin information för att berika den men att samtliga *inte* är obligatoriska.

- **Typ:** Hur informationen är hämtad. Exempelvis OSINT[6].
- **OSINT:** Beskriver att data samlats in från offentligt tillgängliga källor. Denna kan även beskriva vilken typ av OSINT det handlar om. Exempelvis lifetime- den kommer troligtvis för alltid att vara en öppen källa
- **TLP:** Beskriver vilken informationsklassning eventet har
- **Region:** I vilket/vilka geografiska områden som problemet har detekterats
- **Sektor:** Beskriver vilka sektorer som tycks beröras av attacken
- **OBJECTS:** Var de hämtat rapporten ifrån
- **Attributes:** Själva IOC:erna i eventet, t.ex. länkar som kan leta reda på innehållet i filerna, oavsett om filnamnet har ändrats eller inte.

Ge feedback på event

Sightings

Användare i MISP-SE rekommenderas att använda *sightings* för att flagga för korrekta iakttagelser eller false positives. Detta görs genom ikonerna ”tumme upp” och ”tumme ner” i MISP.

Bilden nedan är hämtad från CIRCL. På deras webbsida beskrivs *sightings* ytterligare.

I MISP-SE använda *sightings* på följande sätt:

- **Tumme upp:** Verifierar ett attributs giltighet (true positve).
- **Tumme ner:** Signalerar en false positive. Alltså när något flaggas som ett hot men i själva verket inte är det.

Båda funktionerna bidrar till att optimera informationsdelningen och responsen på cyberhot i MISP-SE.

[6] Open source intelligence.

Myndigheten
för civilt försvar

Bilaga 1 – beskrivning av taggar för händelsetyper

DOS/DDOS

Amplification-attack	Amplification attack. For example, DNS or NTP amplification type attacks where the targets address is spoofed in a DNS or NTP query. The adversary sends a tiny query which results in a large response. Typically used in volumetric attacks.
Reflected-spoofed-attack	Reflected and Spoofed attack. Adversary sends SYN packet to legitimate service with source spoofed as target, this results in retransmitted SYN-ACK packets from the legitimate service.
Slow-read-attack	Slow Read attack. The adversary sends a request to target and reads the response one byte at a time, this uses up resources on the target service for a long time.
Flooding-attack	Flooding attack. Usually, SYN flood with the objective to waste resources on stateful firewalls.
Post-attack	Large POST HTTP attack. The adversary sends large amounts of data to form-handling URIs wasting request parsing resources on the target.

Phishing

Fake-website	Adversary controls a fake website to phish for credentials or information.
Email-spoofing	Adversary sends email with domains related to target. Adversary controls the domains used.
Clone-phishing	Adversary clones an email to target potential victims with duplicated content.
Voice-phishing	Adversary uses voice-based techniques to trick a potential victim to give credentials or sensitive information. This is also known as vishing.
Search-engines-abuse	Adversary controls the search engine result to get an advantage.
Sms-phishing	Adversary sends an SMS to a potential victim to gather sensitive information or use another phishing technique at a later stage.
Business email compromise	Adversary sends an email containing a malicious artefact from a legitimate business email address which has connections to you as an individual or your organisation.
Spear-phishing	Adversary attempts targeted phishing to a user or a specific group of users based on knowledge known by the adversary
Bulk-phishing	Adversary attempts to target a large group of potential targets without specific knowledge of the victims.
Whaling	Adversary attempts to target executives and high-level employees (like public spokespersons).