SUNET

MISP

pettai@sunet.se

MISP 101

- Åtkomst
- Samlade IOC:er från Threatfeed och det vi bidrar med
  - Statistik på våra egna bidrag
- (Automatisk) korrelering av olika attribut
  - Exempel på det (Historik)
- IOC-lookup
- Automation
  - REST API för att exportera data
  - Äldre API finns för att exportera tex. Zeek-format
- Hur vill ni använda MISP/datat?
- Framtid

SUNET

MISP åtkomst?

https://wiki.sunet.se/display/SUNETCERT/MISP

Åtkomst

För att kunna nyttja tjänsten måste man vara SWAMID-medlem och ha en IdP (det är endast federerad inloggning till MISP-instansen). För att få sitt inloggningskonto aktiverat i MISP-instansen måsta du först logga in en gång (via https://misp.cert.sunet.se) och sedan meddela din IRT-ansvarige ditt eget EPPN (format: uid@realm), så att hen kan aktivera kontot.

SUNET

MISP data

Statistics

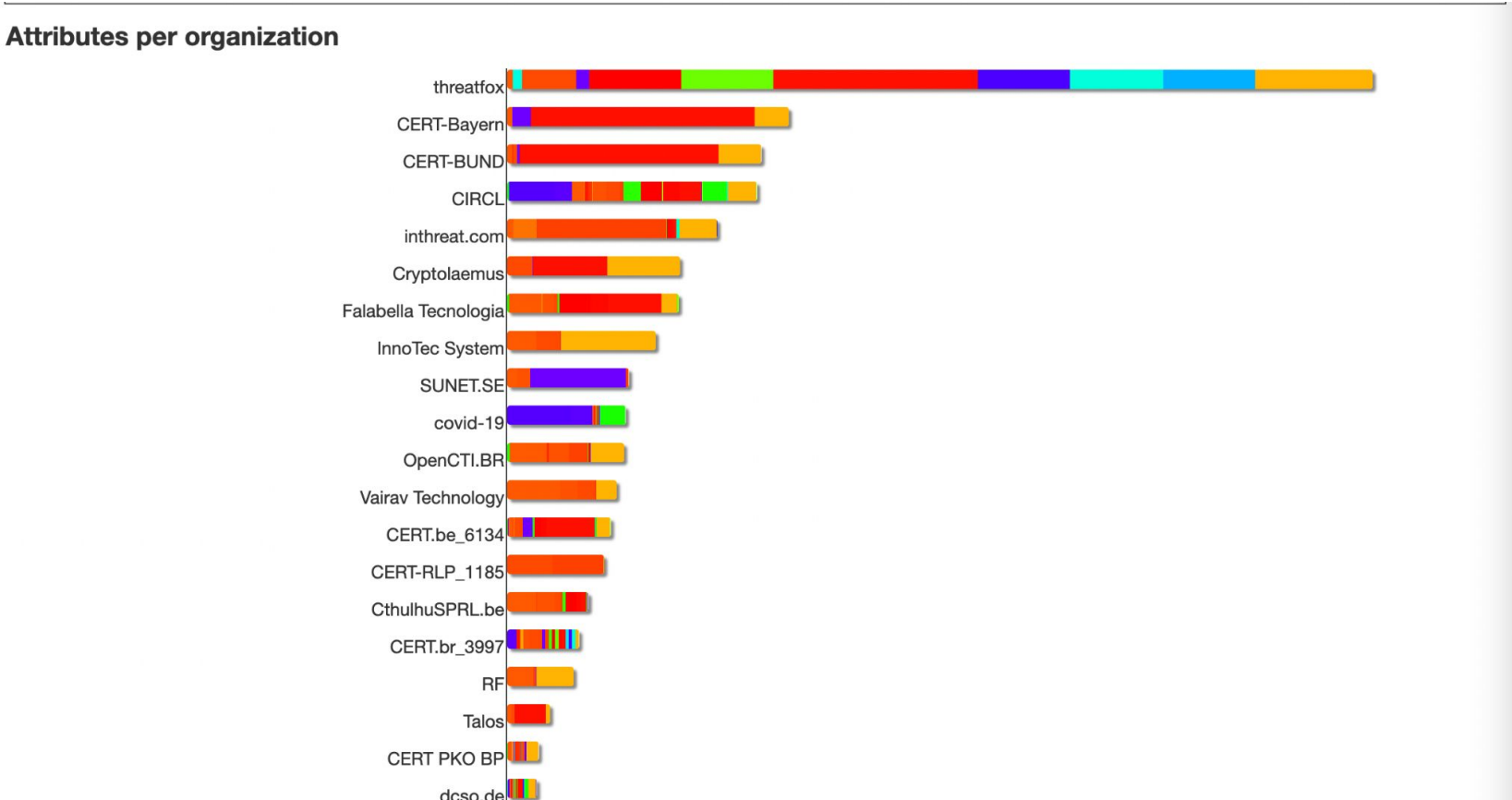
Usage data | Organisations | User and Organisation statistics | Tags | Attribute histogram | Sightings toplists | Galaxy Matrix

Some statistics about this instance. The changes since the beginning of this month are noted in brackets wherever applicable

Events	90566 (+321)
Attributes	6518186 (+121711)
Attributes / event	72
Correlations found	53422611
Proposals active	1285
Users	131
Users with PGP keys	2 (1.5%)
Organisations	907
Local Organisations	31
Event creator orgs	469
Average Users / Org	4.2
Discussion threads	3 (0)
Discussion posts	3 (0)

SUNET

MISP data



SUNET

MISP data

Statistics

Usage data | Organisations | User and Organisation statistics | Tags | Attribute histogram | Sightings toplists | Galax

Organisation list

Quick overview over the organisations residing on or known by this instance.

Local organisations | Known remote organisations | All organisations

Logo	Name	Users	Events	Attributes	Nationality	Type	Sector	Activity (1 year)
BTH.SE	BTH.SE	1	0	0				
CHALMERS.SE	CHALMERS.SE	6	4	7				
DU.SE	DU.SE	5	0	0				
EDUID.SE	EDUID.SE	1	0	0				
FHS.SE	FHS.SE	2	0	0				
GU.SE	GU.SE	3	0	0				
HB.SE	HB.SE	3	0	0				
HIG.SE	HIG.SE	2	0	0				
HJ.SE	HJ.SE	3	1	20				
HKR.SE	HKR.SE	2	0	0				
IRF.SE	IRF.SE	1	1	1				
KAU.SE	KAU.SE	3	1	3				
KI.SE	KI.SE	4	0	0				
KTH.SE	KTH.SE	6	0	0				
LIU IRT	LIU IRT	1	0	0				
LIU.SE	LIU.SE	7	4	229				
LNU.SE	LNU.SE	3	0	0				
LTU.SE	LTU.SE	12	0	0				
LU.SE	LU.SE	7	77	491				
MDH.SE	MDH.SE	5	0	0				
MIUN.SE	MIUN.SE	2	0	0				
NONE	NONE	2	2	6209				
ORU.SE	ORU.SE	3	0	0				
SLU.SE	SLU.SE	1	0	0				
SMHI.SE	SMHI.SE	1	0	0				
SU.SE	SU.SE	7	6	7				
SUNET.SE	SUNET.SE	18	253	210600				
UMU.SE	UMU.SE	7	0	0				
USER.UU.SE	USER.UU.SE	3	1	8				
UU-CSIRT	UU-CSIRT	1	2	54				
UU.SE	UU.SE	0	0	0				

MISP data

Ex.

Kika på vad LU (Lunds Universitets IRT) rapporterat in i MISP:

https://misp.cert.sunet.se/organisations/view/77

Kika på Talos (Cisco) rapporterade data i MISP:
https://misp.cert.sunet.se/organisations/view/427

SUNET

MISP data (historik)

Inrapporterade attributen med flest antal korrelaringar:

IP-adress: 185.176.27.26(/24) (sågs senast 2020)
Filnamn: a.exe
Domännamn: ptr.ruvds.com (sågs senast 2018)
Malware-namn: Dridex
CVE: CVE-2012-0158
APT: APT28 (sågs senast 2020)
ASN: AS44901 BELCLOUD (sågs senast 2019)
Hash: f34d5f2d4577ed6d9ceec516c1f5a744

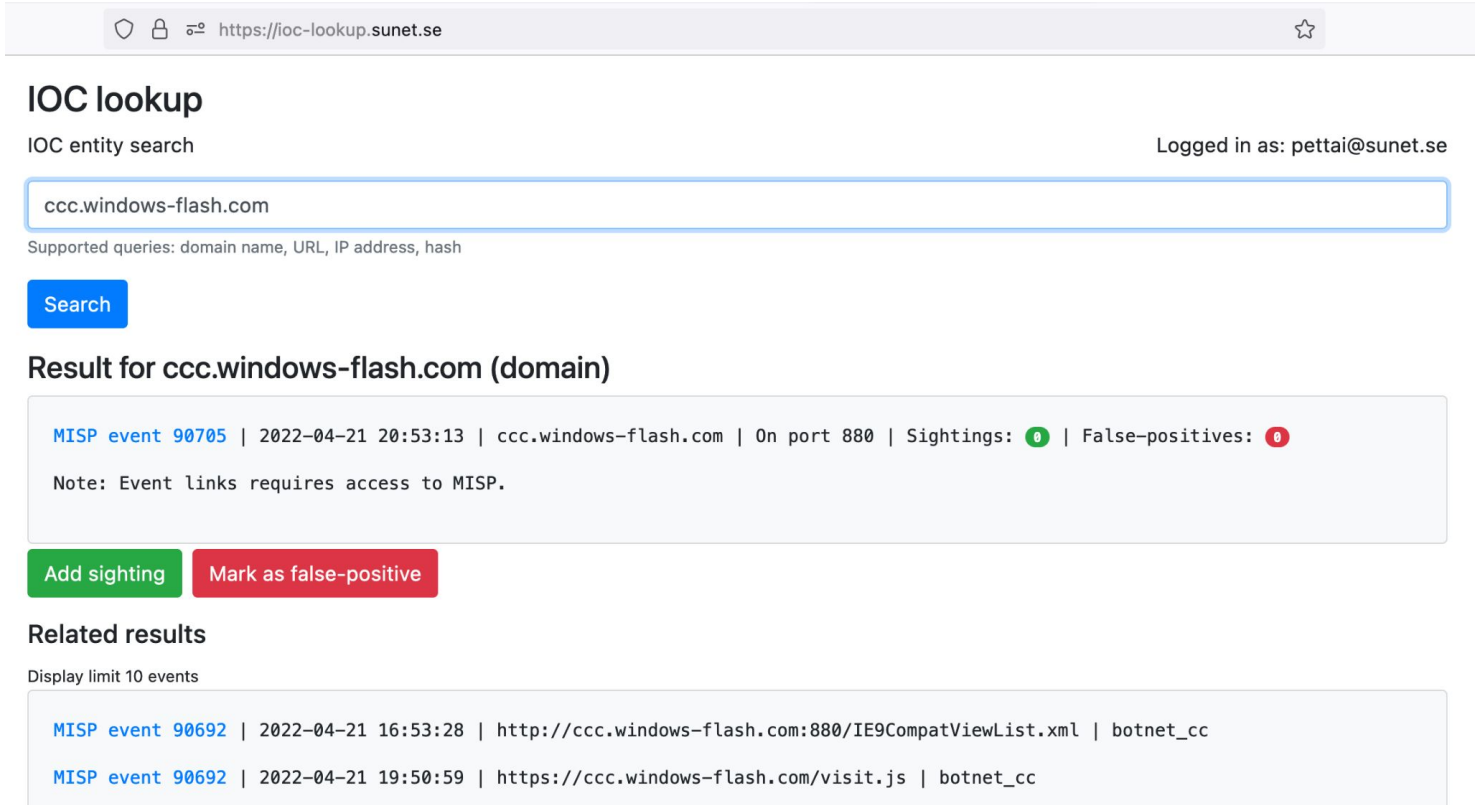
IOC-Lookup

“MISP made easy”:

https://IOC-Lookup.sunet.se

SUNET

IOC-Lookup



SUNET

MISP attribut (sökbara)

md5 sha1 sha256 filename pdb filename|md5 filename|sha1 filename|sha256 ip-src ip-dst hostname domain domain|ip email email-src eppn email-dst email-subject email-attachment

email-body float git-commit-id url http-method user-agent ja3-fingerprint-md5 jarm-fingerprint favicon-mmh3 hassh-md5 hasshserver-md5 regkey regkey|value AS snort bro zeek community-id

pattern-in-file pattern-in-traffic pattern-in-memory filename-pattern pgp-public-key pgp-private-key ssh-fingerprint yara stix2-pattern sigma gene kusto-query mime-type identity-card-number cookie

vulnerability cpe weakness attachment malware-sample link comment text hex other named pipe mutex process-state target-user target-email target-machine target-org target-location

target-external btc dash xmr iban bic bank-account-nr aba-rtn bin cc-number prtn phone-number threat-actor campaign-name campaign-id malware-type uri authentihash vhash ssdeep

imphash telfhash pehash impfuzzy sha224 sha384 sha512 sha512/224 sha512/256 sha3-224 sha3-256 sha3-384 sha3-512 tlsh cdhash filename|authentihash filename|vhash filename|ssdeep

filename|imphash filename|impfuzzy filename|pehash filename|sha224 filename|sha384 filename|sha512 filename|sha512/224 filename|sha512/256 filename|sha3-224 filename|sha3-256 filename|sha3-384

filename|sha3-512 filename|tlsh windows-scheduled-task windows-service-name windows-service-displayname whois-registrant-email whois-registrant-phone whois-registrant-name whois-registrant-org

whois-registrar whois-creation-date x509-fingerprint-sha1 x509-fingerprint-md5 x509-fingerprint-sha256 dns-soa-email size-in-bytes counter datetime port ip-dst|port ip-src|port hostname|port mac-address

mac-eui-64 email-dst-display-name email-src-display-name email-header email-reply-to email-x-mailer email-mime-boundary email-thread-index email-message-id github-username github-repository

github-organisation jabber-id twitter-id dkim dkim-signature first-name middle-name last-name full-name date-of-birth place-of-birth gender passport-number passport-country passport-expiration

redress-number nationality visa-number issue-date-of-the-visa primary-residence country-of-residence special-service-request frequent-flyer-number travel-details payment-details

place-port-of-original-embarkation place-port-of-clearance place-port-of-onward-foreign-destination passenger-name-record-locator-number mobile-application-id chrome-extension-id cortex boolean anonymised

MISP Automation

Din resa börjar här:

https://misp.cert.sunet.se/events/automation

SUNET

MISP Automation

Sök ut och exportera datat i färdiga format:

- CSV
- JSON
- Snort
- Suricata
- XML

SUNET

MISP Automation

```
% curl -s -H "Accept: application/json" -H
"Content-type: application/json" -H
"Authorization: USER_AUTH_KEY_GOES_HERE" -X POST
https://misp.cert.sunet.se/attributes/restSearch
-d
'{"returnFormat":"csv","type":["domain","hostnam
e","ip-dst|port","ip-src|port"],"tags":["!OUTDAT
ED","Cobalt
Strike"],"last":"14d","to_ids":"true"}'
```

SUNET

MISP Automation

"5eea90e2-556b-4250-afa4-12ce2d721240",90590,"Network activity","hostname","cs.qaxqax.xyz","On port 8443",1,1650371931,"","","","",""

"412e60ac-5f7e-4f15-b52e-f6ee246e8b24",90590,"Network activity","hostname","www.flash-com.tk","On port 8443",1,1650371932,"","","","",""

"e1821586-bf7c-4a68-85ad-d943948ff3fd",90590,"Network activity","hostname","ns1.d2efeg4h4.com","On port 80",1,1650371932,"","","","",""

"bb3bce30-bd3b-48e4-baa6-469ba27f95d2",90590,"Network activity","hostname","xyz.moonmu.isasecret.com","On port 99",1,1650371933,"","","","",""

"fe18f3d7-584b-4cf5-ae01-26435610d0e5",90590,"Network activity","hostname","update.releasemyapps.com","On port 1443",1,1650371933,"","","","",""

"06a4e55c-67c7-4a09-9acb-0d63ea53321c",90590,"Network activity","hostname","abc.flash-com.tk","On port 8443",1,1650371933,"","","","",""

"d7657187-0734-4ec4-9847-58a95a3ebefb",90590,"Network activity","hostname","cc.peakyblinders.uk","On port 8080",1,1650371933,"","","","",""

"8a0b6550-3201-443e-9ed1-4c29a7160a10",90590,"Network activity","hostname","zh.h365sf.tk","On port 443",1,1650371933,"","","","",""

"b446969b-2130-4ef8-b338-7c1dcbe4b75e",90590,"Network activity","hostname","www.generalconsolidated.com","On port 443",1,1650371933,"","","","",""

"5937ce98-17ee-4ff1-af4e-121cf74ebbed",90590,"Network activity","hostname","jt.tnnd.ml","On port 2087",1,1650371933,"","","","",""

"01ad5e61-27e5-4a7e-b708-296fb9a93ca9",90590,"Network activity","hostname","c2.eduazure.gq","On port 20041",1,1650371933,"","","","",""

"492786bd-fdf7-4bb7-8a8c-afe1f8056bd7",90590,"Network activity","hostname","update.chaitin.cc","On port 2087",1,1650371933,"","","","",""

"540497c6-d454-4bf6-a5c6-d258cee11c01",90590,"Network activity","hostname","combo.sechack.online","On port 443",1,1650371934,"","","","",""

"0bbf15dc-5f52-4b24-a755-a682325c18ad",90590,"Network activity","hostname","www.klycnmik.com","On port 443",1,1650371934,"","","","",""

"d22ef603-7448-4677-b6e5-84179a9dae48",90590,"Network activity","hostname","downloads.lastupdatebd.com","On port 1080",1,1650371935,"","","","",""

"082692e4-d7c0-411b-9c53-6b25267441c4",90590,"Network activity","hostname","zx.mylovelylab.com","On port 443",1,1650371935,"","","","",""

"5fb1c86a-6390-4603-b1af-adf094b34f42",90590,"Network activity","hostname","xc.mylovelylab.com","On port 443",1,1650371935,"","","","",""

"3266a456-4944-4b00-a0ca-3651a40d2844",90590,"Network activity","hostname","cv.mylovelylab.com","On port 443",1,1650371935,"","","","",""

"ae522615-0b73-4312-b333-25009e9b2c77",90590,"Network activity","hostname","cv.sharedresourcesltd.com","On port 443",1,1650371935,"","","","",""

"e23be8c9-8ec2-40d4-b126-5e63e7fb5ed8",90590,"Network activity","hostname","xc.sharedresourcesltd.com","On port 443",1,1650371935,"","","","",""

"707ab87b-5857-4895-bff2-b2c2ab6b2660",90590,"Network activity","hostname","zx.sharedresourcesltd.com","On port 443",1,1650371935,"","","","",""

SUNET

MISP Automation

Använd PyMISP

```
pettai@dator:~% pip3 install PyMISP
```

SUNET

MISP Automation

```
misp_url = 'https://misp.cert.sunet.se/attributes/restSearch'
misp_key = 'USER_TOKEN_GOES_HERE'
misp_verifycert = False
relative_path = ''
body = '{ "returnFormat": "csv", "type": ["domain", "hostname","ip-dst|port","ip-src|port"], "tags": ["!OUTDATED", "Cobolt Strike"], "last": "14d", "enforceWarninglist": "true
", "to_ids": "true" }'

from pymisp import PyMISP
misp = PyMISP(misp_url, misp_key, misp_verifycert)
misp.direct_call(relative_path, body)

with open('cobolt-strike.csv, 'w', encoding='UTF-8') as file:
   file.write(str(misp.direct_call(relative_path, body)))
```

SUNET

MISP Framtid

Vad vill du använda MISP/datat till?

På vilket sätt?

...

SUNET

MISP Framtid

- Uppdatera nuvarande miljö (nytt DC)
- Ny MISP (striktare intag av data)
  - Mer indata via automation
  - Nya användare
  - Utbyte med bla SIKT
- Nuvarande MISP lever kvar med historiskt data…

SUNET