MISP Threat Sharing - closing the gaps

MISP
Threat Sharing
SHARE YOUR BLOODY INDICATORS
GITHUB.COM/MISP

eCrimeLabs
https://www.ecrimelabs.com

eCrimeLabs
@DennisRand

Hvem er jeg

Startede med sikkerhed tilbage I 90'erne primært fokus på både offense og defense.

Arbejder ved JN Data med Incident Response og Threat Intelligence

Stifter af eCrimeLabs der har fokus på Hosting af MISP, Incident Response, Malware analyse, Threat Hunting og Threat Intelligence.

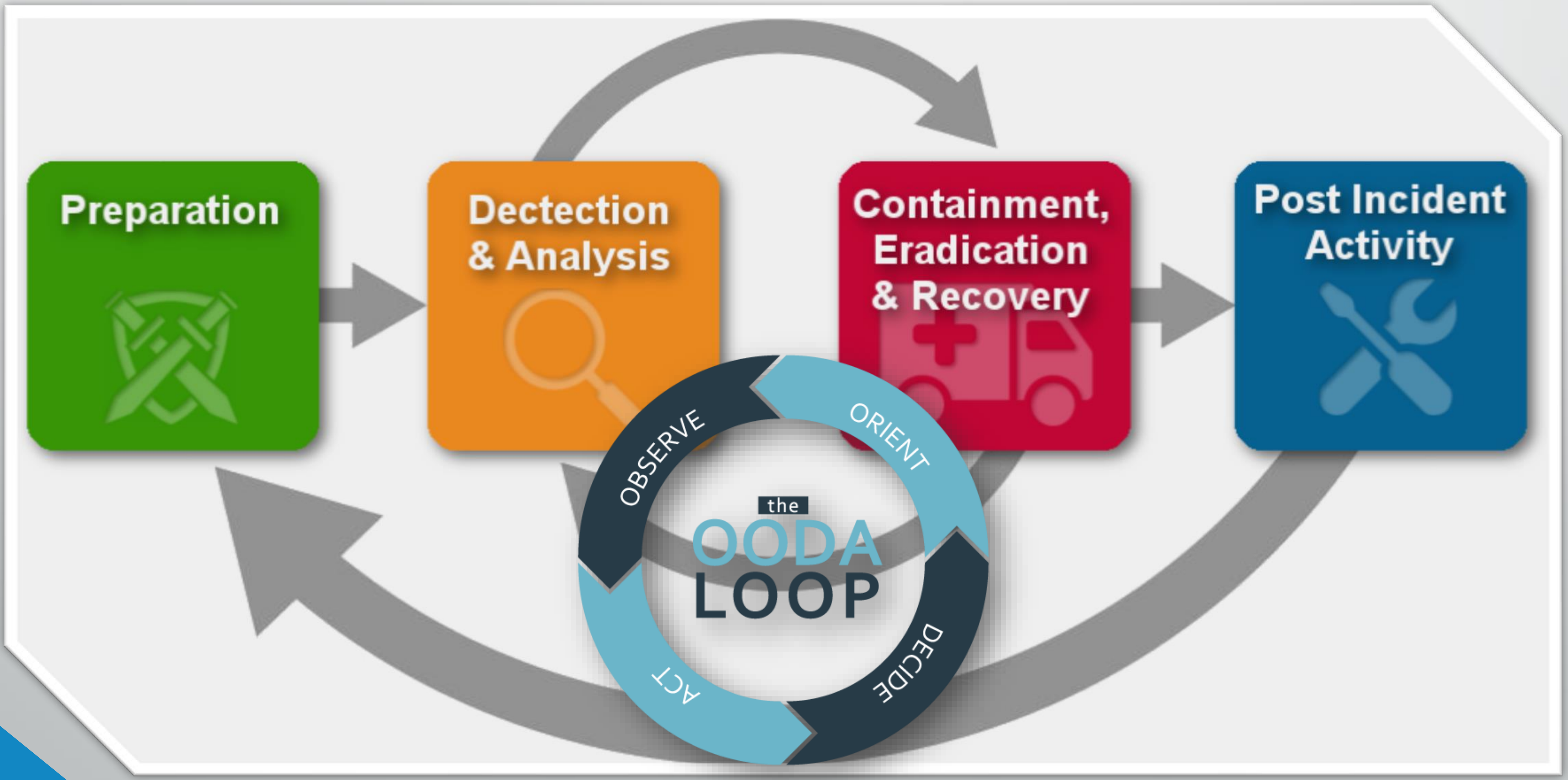
Contributor til MISP https://www.misp-project.org/contributors/

JN DATA det foretrukne valg
TDC Group
fortconsult
DKCERT COMPUTER SECURITY INCIDENT RESPONSE TEAM
NETRAGARD™ We protect you from people like us™
JYSKE BANK
PROTEGO din vished for sikkerhed
CSIS
VERISIGN

Agenda

- Hvem er jeg
- Termer og definitioner
- Hvad er MISP og hvor kommer det fra
- MISP anvendelse ideer/muligheder

Incident Life-cycle



Threat definitions

There is often a definition misuse or misunderstanding when talking about Threat terms

Threat Feed

A threat feed is a list of Indicators of Compromise (IOC). There are no context to this data besides the source and type. This data is distributed into security components such as Firewalls, IDS/IPS, Endpoint Detection and Response (EDR), SIEM, Log management, DNS etc.

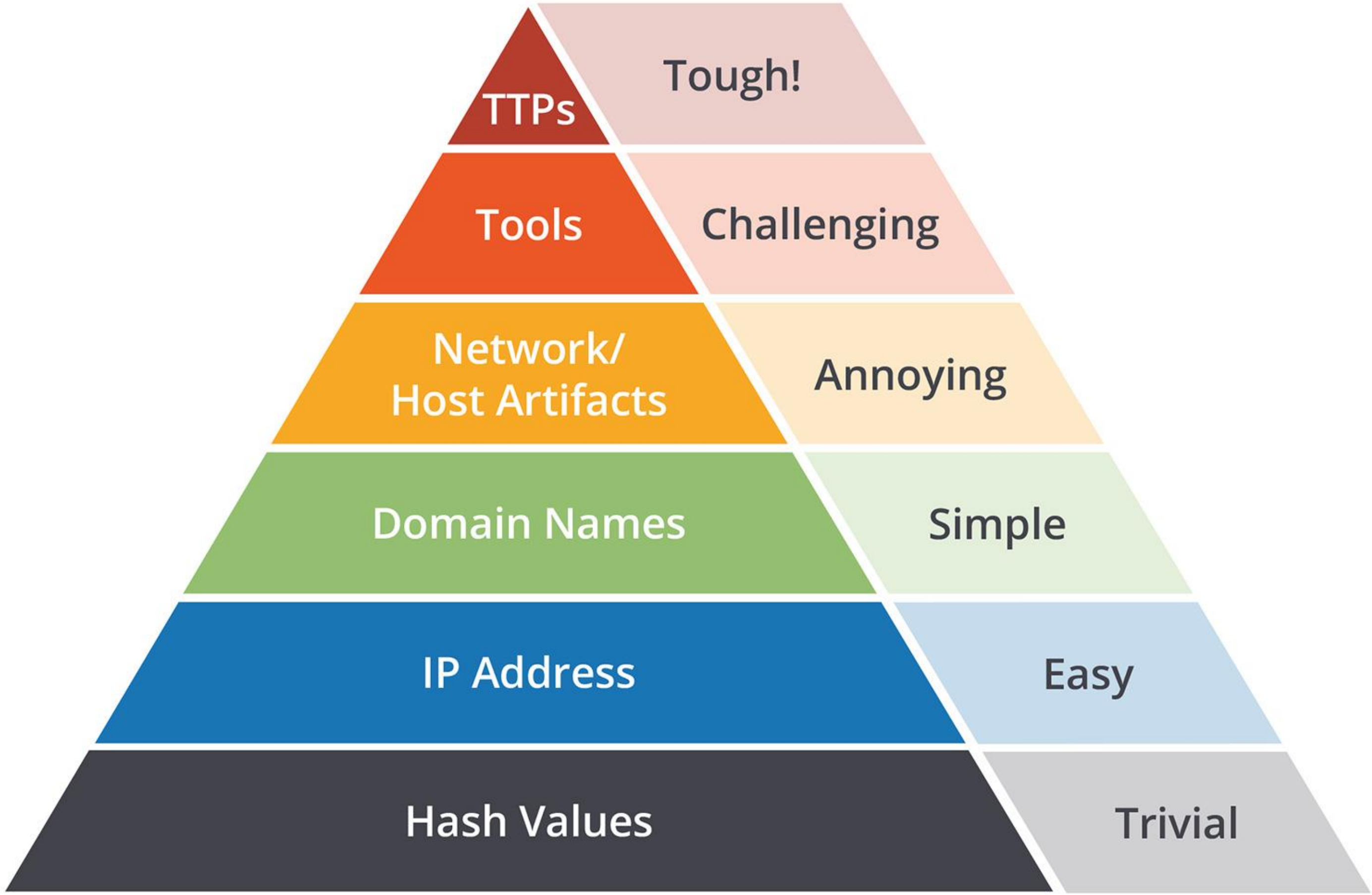
Threat data

Threat data is the next stage where you will have technical and possible threat-actor context to IOC's allowing organizations to evaluate the threats they have identified or could be exposed to.

Threat Intelligence

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response.

Pyramid of Pain



Source: David J. Bianco, personal blog

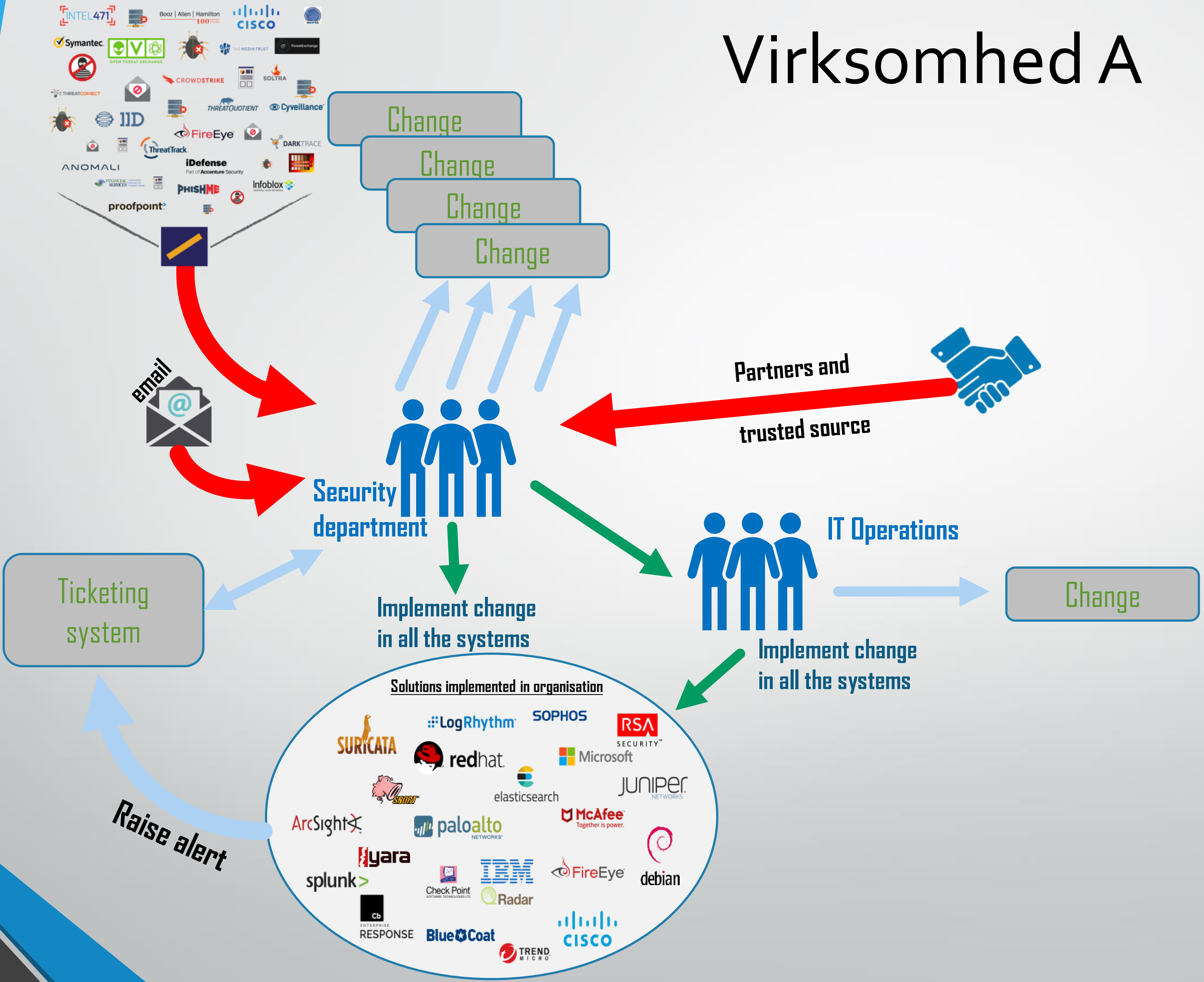
Hvor komplekst er det for vore modstandere at ændre adfærd og signature både teknisk og psykologisk

TTP → Techniques, Tools and Procedures

https://stixproject.github.io/documentation/concepts/ttp-vs-indicator/

eCrimeLabs

Virksomhed A



eCrimeLabs

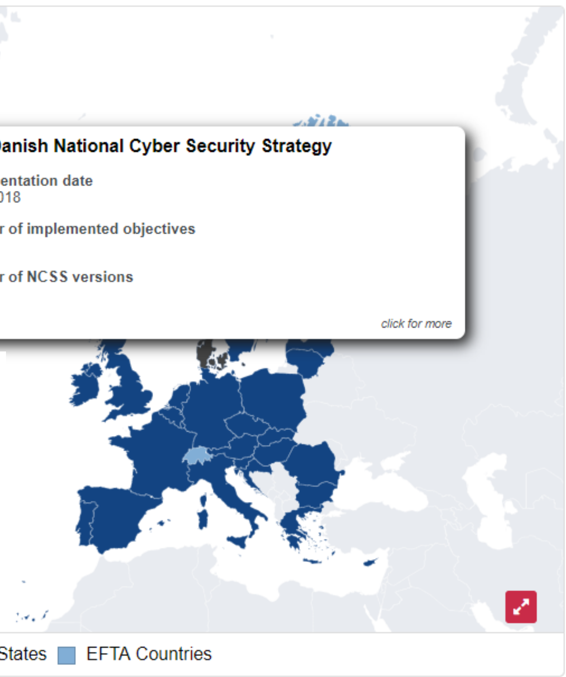
MISP Threat Sharing Platform

En opsamlings platform for Threat baseret data

Er defakto standard I forhold til threat sharing platform i EU

Co-financed by the European Union

Connecting Europe Facility



Danish National Cyber Security Strategy

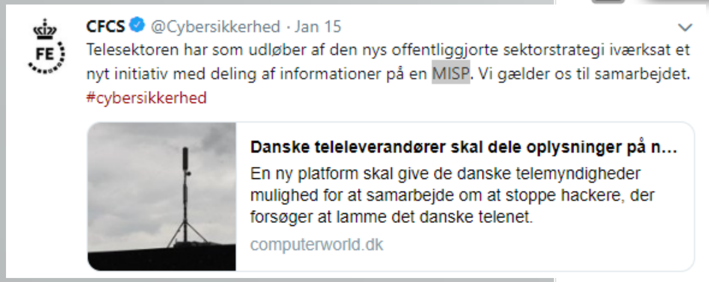
Implementation date
01/05/2018

Number of implemented objectives
11

Number of NCSS versions
1

click for more

■ EU Member States ■ EFTA Countries



CFCS @Cybersikkerhed · Jan 15

Telesektoren har som udløber af den nys offentliggjorte sektorstrategi iværksat et nyt initiativ med deling af informationer på en MISP. Vi gælder os til samarbejdet. #cybersikkerhed

Danske teleleverandører skal dele oplysninger på n...

En ny platform skal give de danske telemyndigheder mulighed for at samarbejde om at stoppe hackere, der forsøger at lamme det danske telenet.

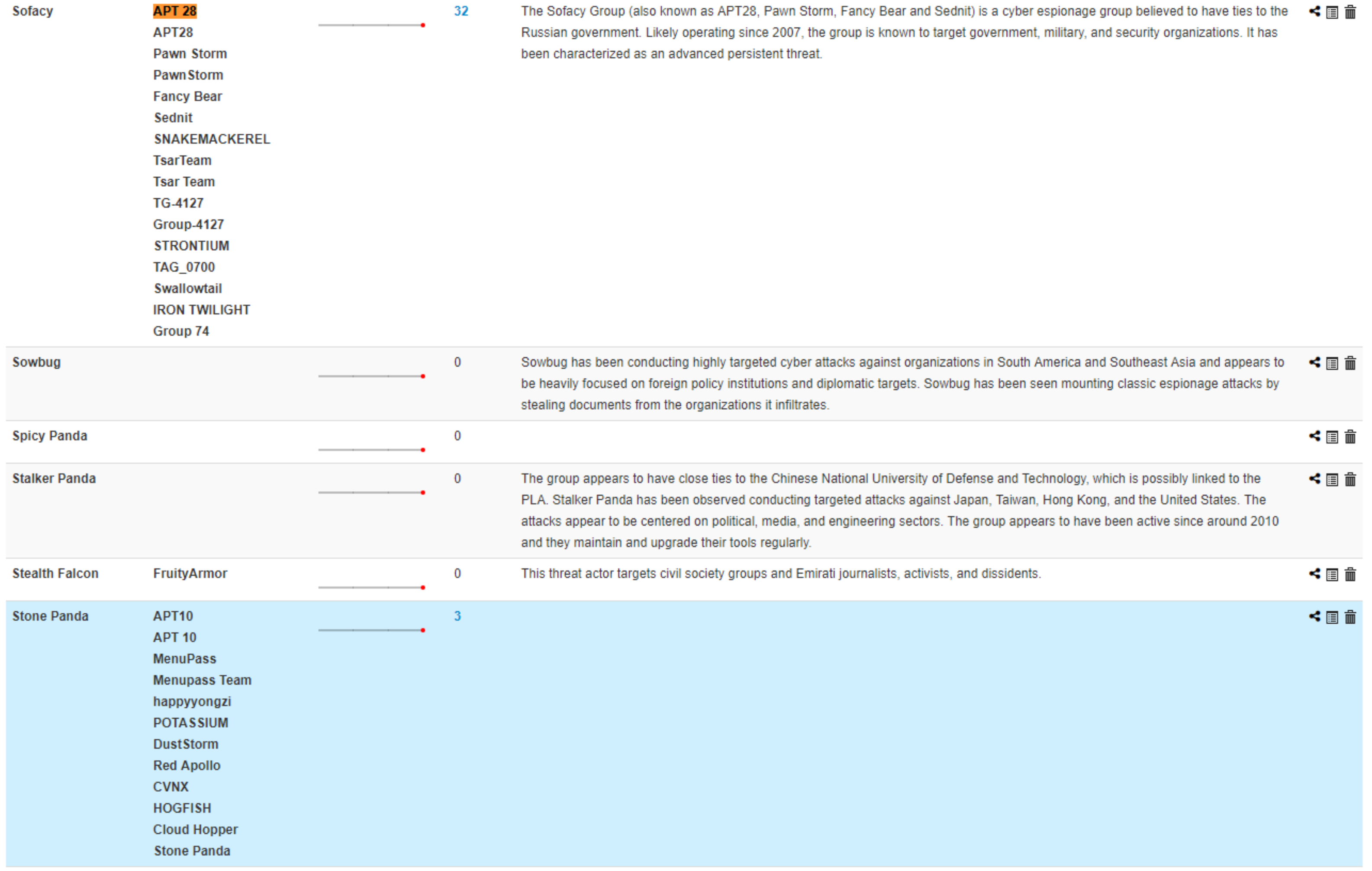
computerworld.dk

https://www.misp-project.org

Opslagsværk

- Find ud af noget mere omkring trussels aktører og malware familiar.

Anvend denne viden til at træne dig og/eller din virksomhed



Sofacy	APT 28 APT28 Pawn Storm PawnStorm Fancy Bear Sednit SNAKEMACKEREL TsarTeam Tsar Team TG-4127 Group-4127 STRONTIUM TAG_0700 Swallowtail IRON TWILIGHT Group 74	32	The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.
Sowbug		0	Sowbug has been conducting highly targeted cyber attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.
Spicy Panda		0	
Stalker Panda		0	The group appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. Stalker Panda has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States. The attacks appear to be centered on political, media, and engineering sectors. The group appears to have been active since around 2010 and they maintain and upgrade their tools regularly.
Stealth Falcon	FruityArmor	0	This threat actor targets civil society groups and Emirati journalists, activists, and dissidents.
Stone Panda	APT10 APT 10 MenuPass Menupass Team happyyongzi POTASSIUM DustStorm Red Apollo CVNX HOGFISH Cloud Hopper Stone Panda	3	

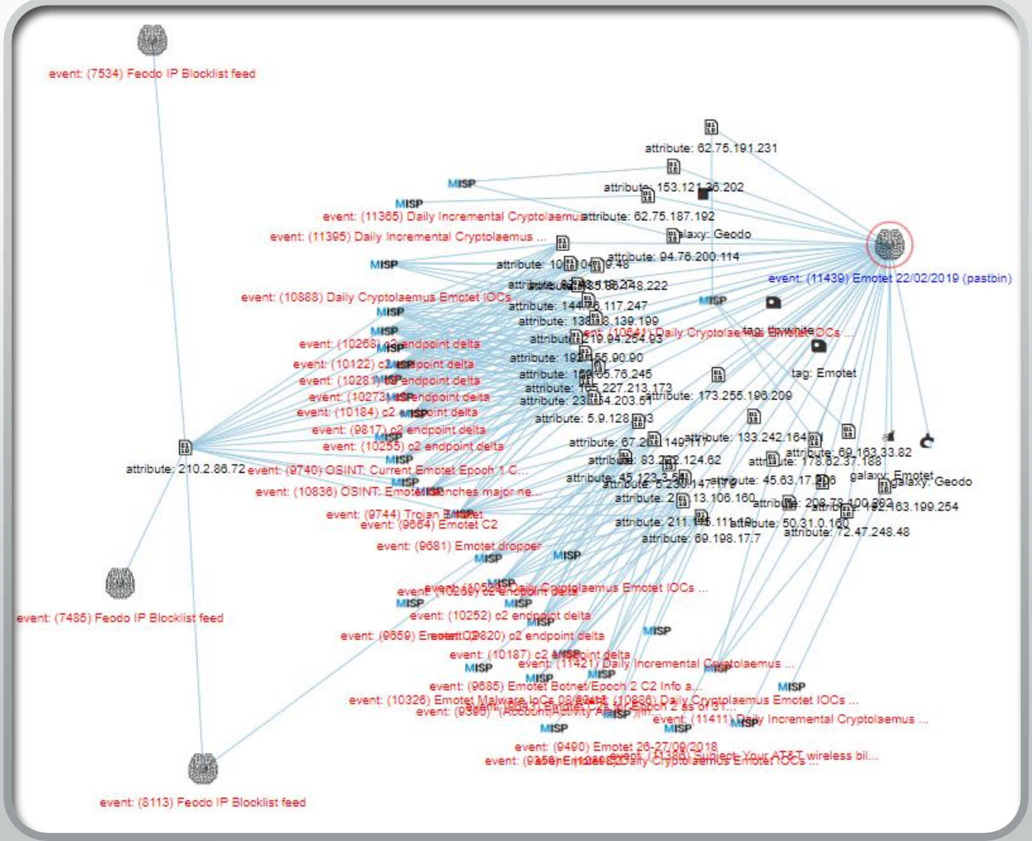
Central storage af Threat data

Mange modtager i dag threat data enten via

- Email
- PDF rapporter
- Websider
- M.v.

Hvordan kan man sikre at data/viden ikke går tabt ved nye medarbejdere eller over tid

Hvordan laver man kryds koorelation af data


event: (7534) Feodo IP Blocklist feed
attribute: 62.75.191.231
MISP
attribute: 153.121.36.202
event: (11365) Daily Incremental Cryptolaemus
attribute: 62.75.187.192
event: (11395) Daily Incremental Cryptolaemus ...
galaxy: Geodo
attribute: 94.76.200.114
event: (11439) Emotet 22/02/2019 (pastbin)
event: (10888) Daily Cryptolaemus Emotet IOCs
attribute: 144.76.117.247
attribute: 138.68.139.199
event: (10122) c2 endpoint delta
event: (10184) c2 endpoint delta
event: (9817) c2 endpoint delta
event: (10255) c2 endpoint delta
tag: Emotet
attribute: 173.255.196.209
attribute: 5.9.128.163
attribute: 133.242.164.31
attribute: 69.163.33.82
attribute: 210.2.86.72
event: (9740) OSINT: Current Emotet Epoch 1 C...
event: (10836) OSINT: Emotet launches major ne...
galaxy: Emotet
galaxy: Geodo
attribute: 45.63.17.206
attribute: 212.83.199.254
event: (9744) Trojan Emotet
event: (9664) Emotet C2
attribute: 50.31.0.160
attribute: 72.47.248.48
event: (9681) Emotet dropper
event: (7485) Feodo IP Blocklist feed
event: (10252) c2 endpoint delta
event: (10187) c2 endpoint delta
event: (11421) Daily Incremental Cryptolaemus ...
event: (9685) Emotet Botnet/Epoch 2 C2 Info a...
event: (10326) Emotet Malware IoCs 06/06/18
event: (11411) Daily Incremental Cryptolaemus ...
event: (9490) Emotet 26-27/09/2018
event: (8113) Feodo IP Blocklist feed

Crowdsourcing og sikker deling

- Vi er stærkere sammen
  - Et målrettet angreb ses ikke af sikkerhedsvirksomheder, men hvad med virksomheder I same branche, område, land, m.v.
  - Løses alt dette med MISP - NEJ

MISP Sharing Model

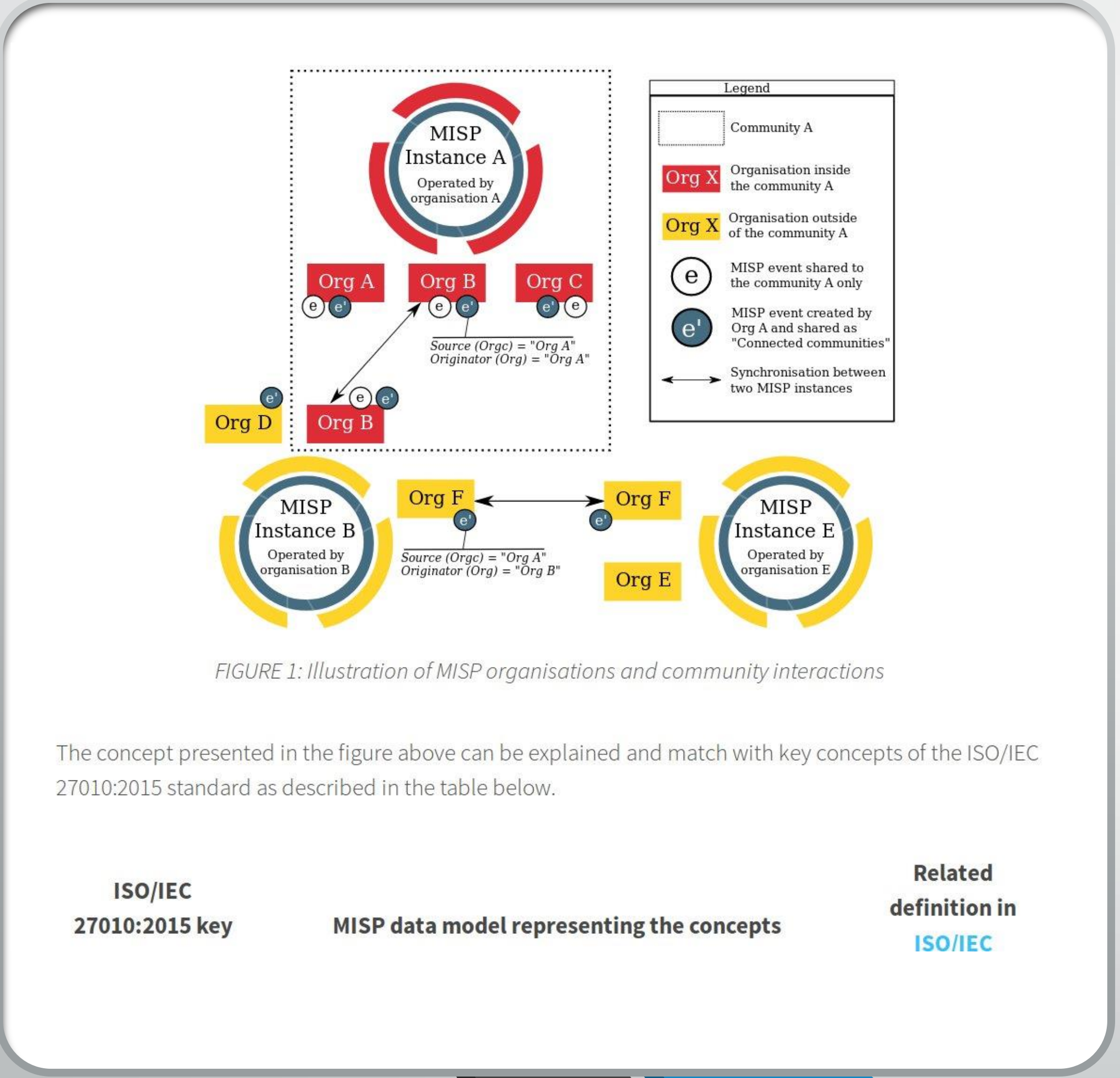
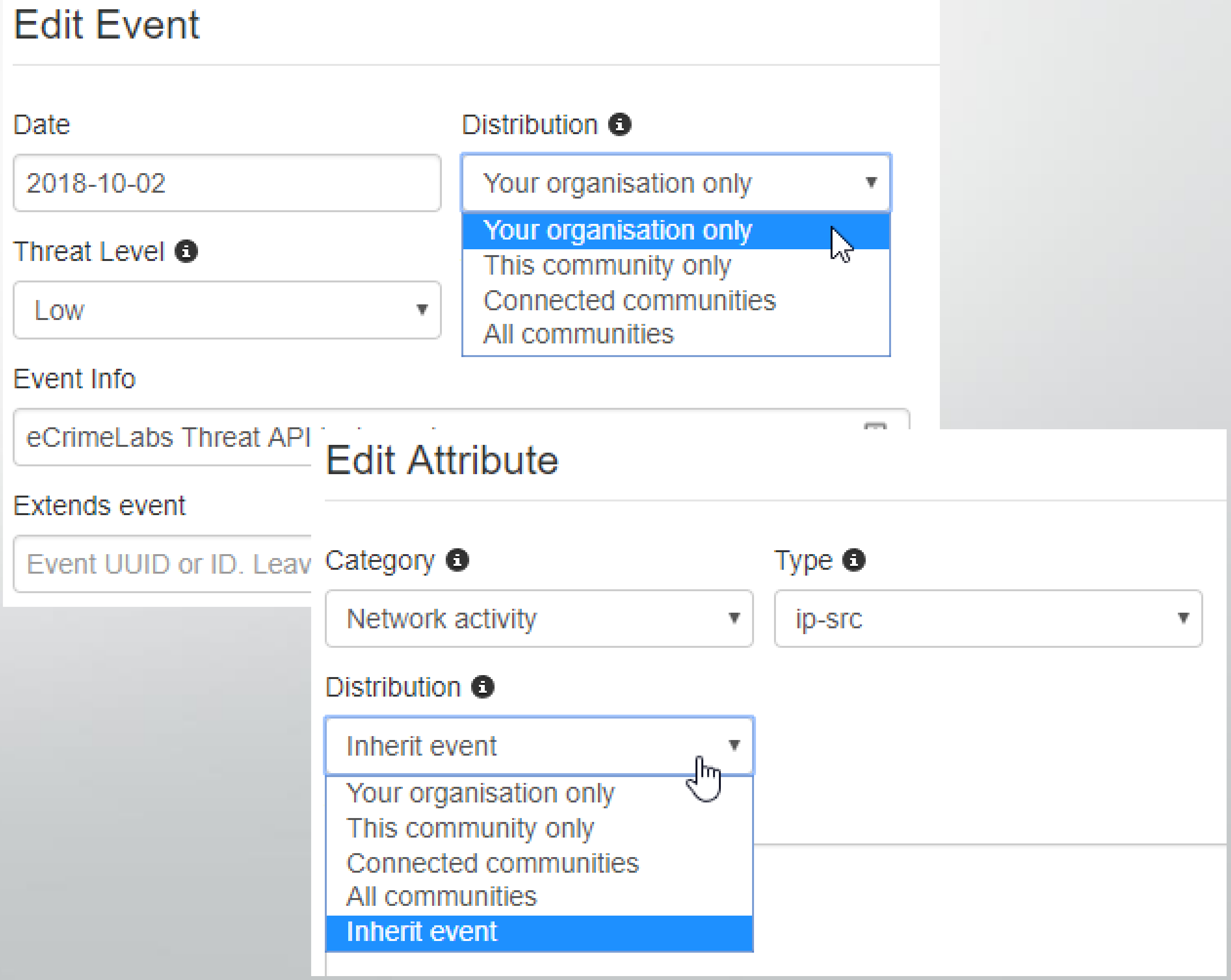

MISP Instance A
Operated by organisation A
Org A
Org B
Org C
e
e'
Source (Orgc) = "Org A"
Originator (Org) = "Org A"
Org D
Org B
Legend
Community A
Org X Organisation inside the community A
Org X Organisation outside of the community A
e MISP event shared to the community A only
e' MISP event created by Org A and shared as "Connected communities"
Synchronisation between two MISP instances
MISP Instance B
Operated by organisation B
Org F
Source (Orgc) = "Org A"
Originator (Org) = "Org B"
Org F
Org E
MISP Instance E
Operated by organisation E

FIGURE 1: Illustration of MISP organisations and community interactions

The concept presented in the figure above can be explained and match with key concepts of the ISO/IEC 27010:2015 standard as described in the table below.

ISO/IEC 27010:2015 key	MISP data model representing the concepts	Related definition in ISO/IEC



Edit Event

Date: 2018-10-02

Distribution: Your organisation only

- Your organisation only
- This community only
- Connected communities
- All communities

Threat Level: Low

Event Info: eCrimeLabs Threat API

Extends event: Event UUID or ID. Leav

Edit Attribute

Category: Network activity

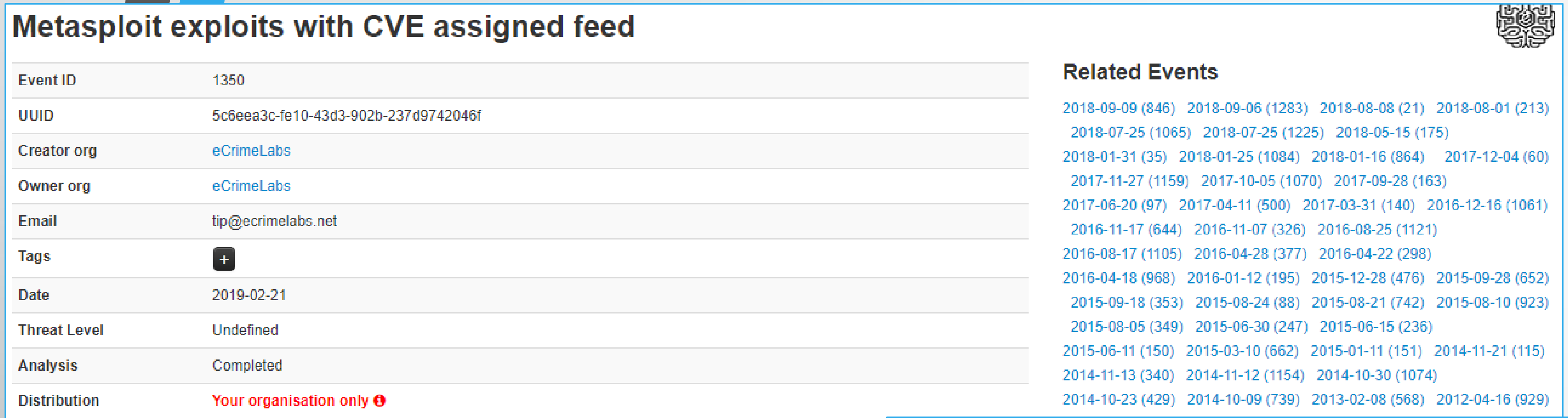
Type: ip-src

Distribution: Inherit event

- Your organisation only
- This community only
- Connected communities
- All communities
- Inherit event

Threat data vs Vulnerability management

"Anvend dit threat data til at hjælpe med prioritering af sårbarheder"

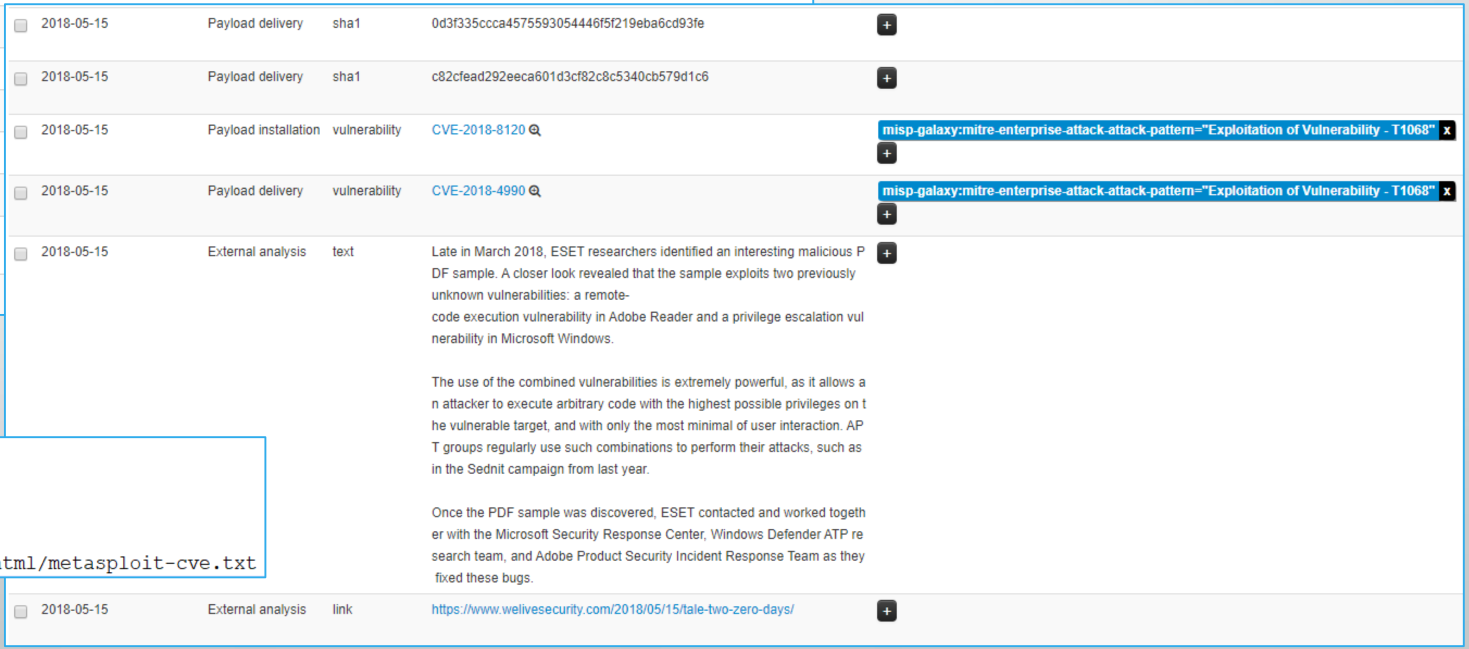


Metasploit exploits with CVE assigned feed

Event ID	1350
UUID	5c6eea3c-fe10-43d3-902b-237d9742046f
Creator org	eCrimeLabs
Owner org	eCrimeLabs
Email	tip@ecrimelabs.net
Tags	+
Date	2019-02-21
Threat Level	Undefined
Analysis	Completed
Distribution	Your organisation only
Info	Metasploit exploits with CVE assigned feed
Published	Yes (2019-02-22 06:10:07)
#Attributes	1777
First recorded change	2019-02-21 18:13:16
Last change	2019-02-21 18:13:16
Modification map	
Sightings	0 (0) - restricted to own organisation only.

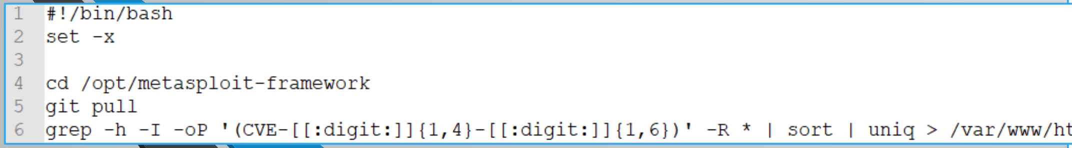
Related Events

2018-09-09 (846) 2018-09-06 (1283) 2018-08-08 (21) 2018-08-01 (213)
2018-07-25 (1065) 2018-07-25 (1225) 2018-05-15 (175)
2018-01-31 (35) 2018-01-25 (1084) 2018-01-16 (864) 2017-12-04 (60)
2017-11-27 (1159) 2017-10-05 (1070) 2017-09-28 (163)
2017-06-20 (97) 2017-04-11 (500) 2017-03-31 (140) 2016-12-16 (1061)
2016-11-17 (644) 2016-11-07 (326) 2016-08-25 (1121)
2016-08-17 (1105) 2016-04-28 (377) 2016-04-22 (298)
2016-04-18 (968) 2016-01-12 (195) 2015-12-28 (476) 2015-09-28 (652)
2015-09-18 (353) 2015-08-24 (88) 2015-08-21 (742) 2015-08-10 (923)
2015-08-05 (349) 2015-06-30 (247) 2015-06-15 (236)
2015-06-11 (150) 2015-03-10 (662) 2015-01-11 (151) 2014-11-21 (115)
2014-11-13 (340) 2014-11-12 (1154) 2014-10-30 (1074)
2014-10-23 (429) 2014-10-09 (739) 2013-02-08 (568) 2012-04-16 (929)



□	2018-05-15	Payload delivery	sha1	0d3f335ccca4575593054446f5f219eba6cd93fe	+
□	2018-05-15	Payload delivery	sha1	c82cfead292eeca601d3cf82c8c5340cb579d1c6	+
□	2018-05-15	Payload installation	vulnerability	CVE-2018-8120	misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation of Vulnerability - T1068" x +
□	2018-05-15	Payload delivery	vulnerability	CVE-2018-4990	misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation of Vulnerability - T1068" x +
□	2018-05-15	External analysis	text	Late in March 2018, ESET researchers identified an interesting malicious PDF sample. A closer look revealed that the sample exploits two previously unknown vulnerabilities: a remote-code execution vulnerability in Adobe Reader and a privilege escalation vulnerability in Microsoft Windows. The use of the combined vulnerabilities is extremely powerful, as it allows an attacker to execute arbitrary code with the highest possible privileges on the vulnerable target, and with only the most minimal of user interaction. APT groups regularly use such combinations to perform their attacks, such as in the Sednit campaign from last year. Once the PDF sample was discovered, ESET contacted and worked together with the Microsoft Security Response Center, Windows Defender ATP research team, and Adobe Product Security Incident Response Team as they fixed these bugs.	+
□	2018-05-15	External analysis	link	https://www.welivesecurity.com/2018/05/15/tale-two-zero-days/	+

http://metasploit.evilcorp.dk/metasploit-cve.txt



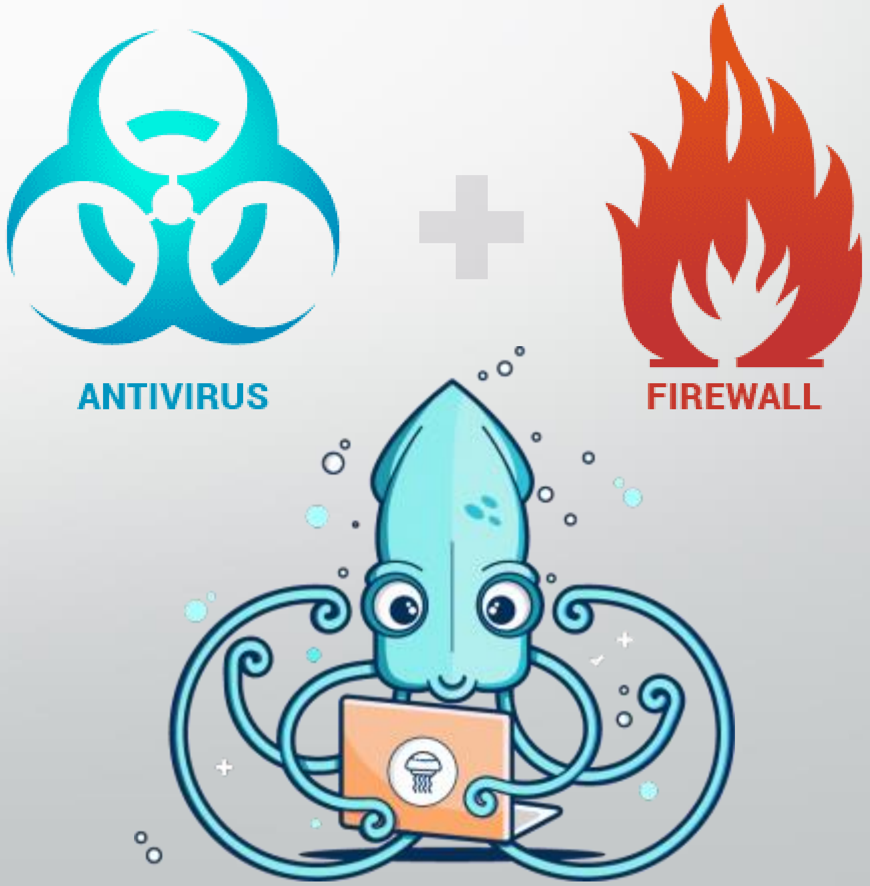
```
#!/bin/bash
set -x

cd /opt/metasploit-framework
git pull
grep -h -I -oP '(CVE-[[:digit:]]{1,4}-[[:digit:]]{1,6})' -R * | sort | uniq > /var/www/html/metasploit-cve.txt
```

Integrer MISP ind I dine sikkerheds komponenter

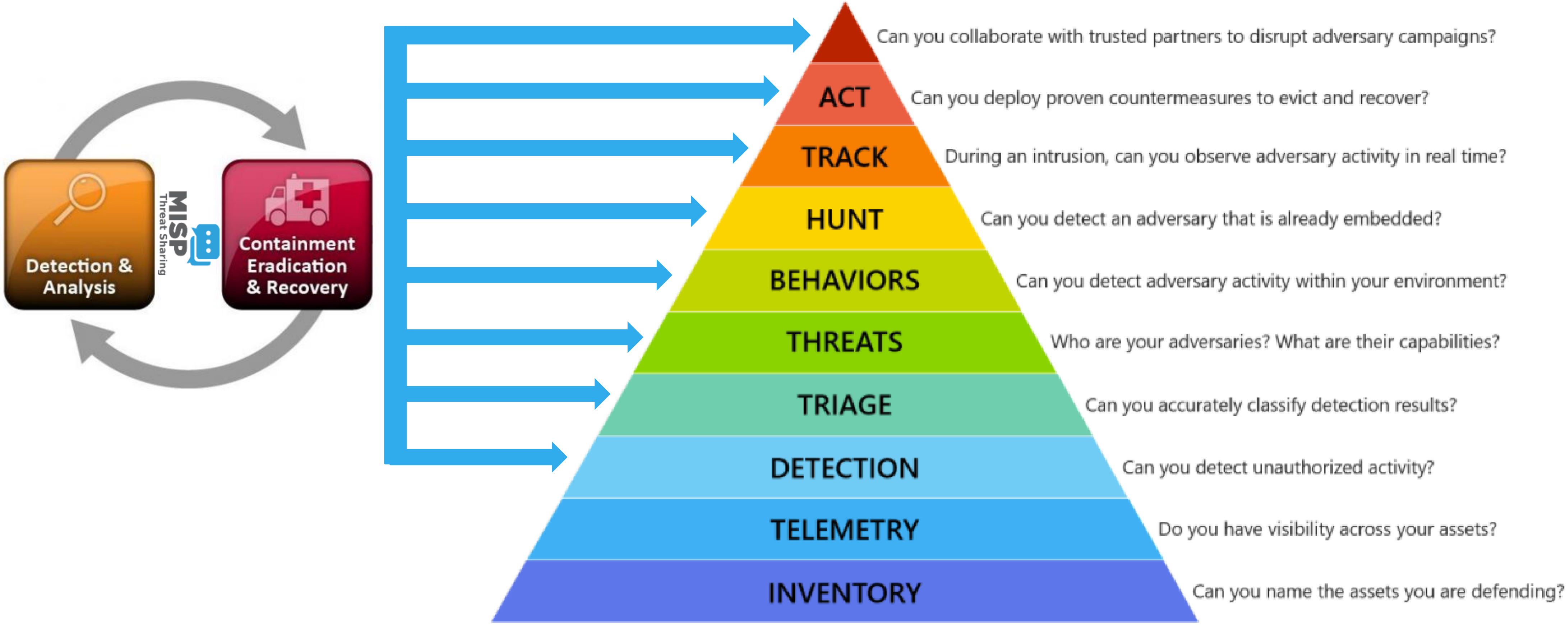
MISP har et åbent API, med mulighed for at trække det data ud du ønsker at anvende, og derved oprationaliserer dine threat data.

- Blokering
- Alarmering



The Incident Response Hierarchy of Needs

The Incident Response Hierarchy is modeled after Maslow's Hierarchy of Needs. It describes the capabilities that organizations must build to defend their business assets. Bottom capabilities are prerequisites for successful execution of the capabilities above them:



Detection & Analysis

MISP Threat Sharing

Containment Eradication & Recovery

Can you collaborate with trusted partners to disrupt adversary campaigns?

ACT — Can you deploy proven countermeasures to evict and recover?

TRACK — During an intrusion, can you observe adversary activity in real time?

HUNT — Can you detect an adversary that is already embedded?

BEHAVIORS — Can you detect adversary activity within your environment?

THREATS — Who are your adversaries? What are their capabilities?

TRIAGE — Can you accurately classify detection results?

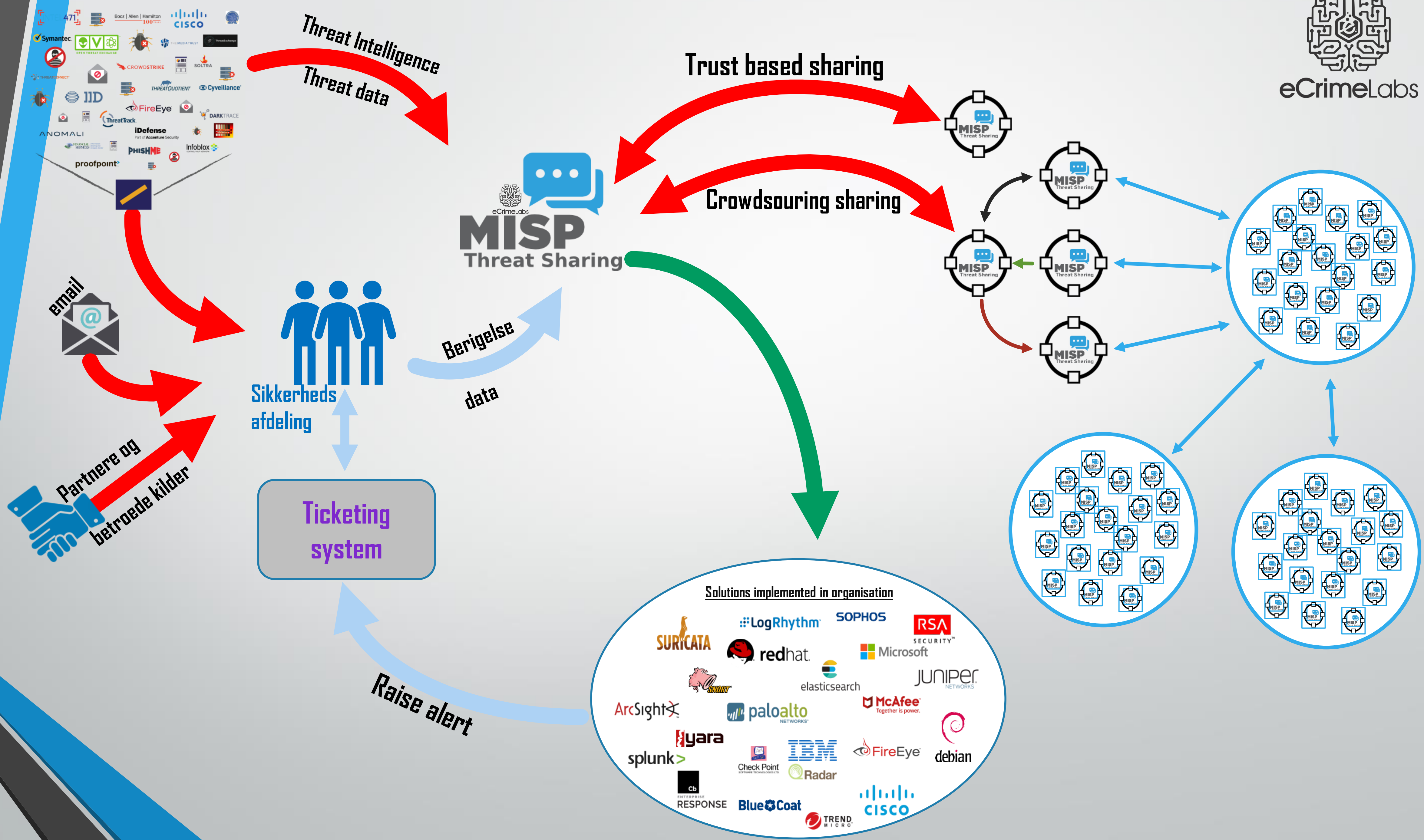
DETECTION — Can you detect unauthorized activity?

TELEMETRY — Do you have visibility across your assets?

INVENTORY — Can you name the assets you are defending?

https://holisticinfosec.blogspot.com/2016/12/the-dfir-hierarchy-of-needs-critical.html

eCrimeLabs



Threat Intelligence

Threat data

Trust based sharing

Crowdsouring sharing

eCrimeLabs MISP Threat Sharing

email

Sikkerheds afdeling

Berigelse

data

Partnere og betroede kilder

Ticketing system

Raise alert

Solutions implemented in organisation

Demo og spørgsmål

Links

- MISP Training Module 1 - An Introduction to Cybersecurity Information Sharing (https://www.youtube.com/watch?v=aM7czPsQyaI)
- MISP Training Module 2 - General usage of MISP (https://www.youtube.com/watch?v=Jqp8CVHtNVk)
- MISP Summit 2017 TheHive and MISP by Saâd Kadhi (https://www.youtube.com/watch?v=gndwirw9mFw)
- MISP Summit 2018: Cruising Ocean Threat Without Sinking Using TheHive, Cortex & MISP - Saâd Kadhi (https://www.youtube.com/watch?v=IDCcLjvSW1Y)
- MISP Documentation (https://www.misp-project.org/documentation/)
- Support portal for MISP (https://gitter.im/MISP/Support)