MISP Threat Sharing - closing the gaps

CYBERHACK

eCrimeLabs

https://www.ecrimelabs.com

About

eCrimeLabs
@DennisRand

I started working and being interested in with security in the 90's original focus was **offense** and now more into **defense**.

Working at JN Data with Incident Response and Threat Intelligence

Founder of eCrimeLabs with focus on Hosting of MISP, Incident Response, Malware analyse, and Threat Intelligence.

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

TDC Group
JN DATA det foretrukne valg
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

- ~~About~~
- Background on MISP Threat Sharing Platform
- Terms and definitions
- MISP usage ideas and potentials

MISP Threat Sharing Platform

A collection platform for storing and sharing threat based data/intelligence

Is the defacto standard in relation to sharing platform in EU, and gain more and more foothold.

Co-financed by the European Union

Connecting Europe Facility

MISP

Threat Sharing

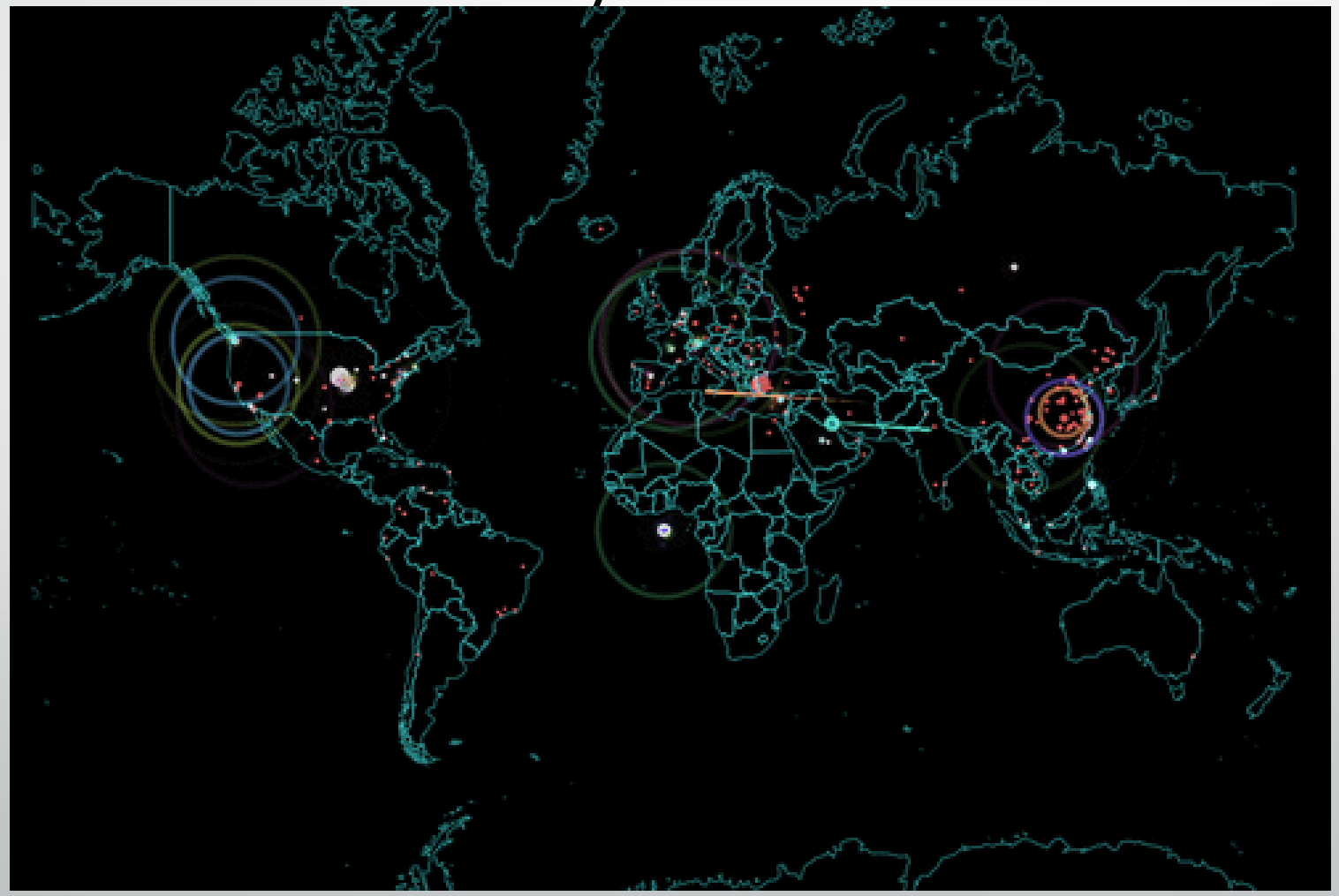
SHARE YOUR BLOODY INDICATORS

GITHUB.COM/MISP

https://www.misp-project.org

Threat

How could you define it ?



Threat data definitions

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

Threat Feed

A threat feed is a list of often **IP's**, **domains** or **Checksums**. There are no context to this data besides the source and type. This data is distributed into security components such as Firewalls, IDS/IPS, End-point Detection and Response (EDR), SIEM, Log management, DNS etc.

Threat data

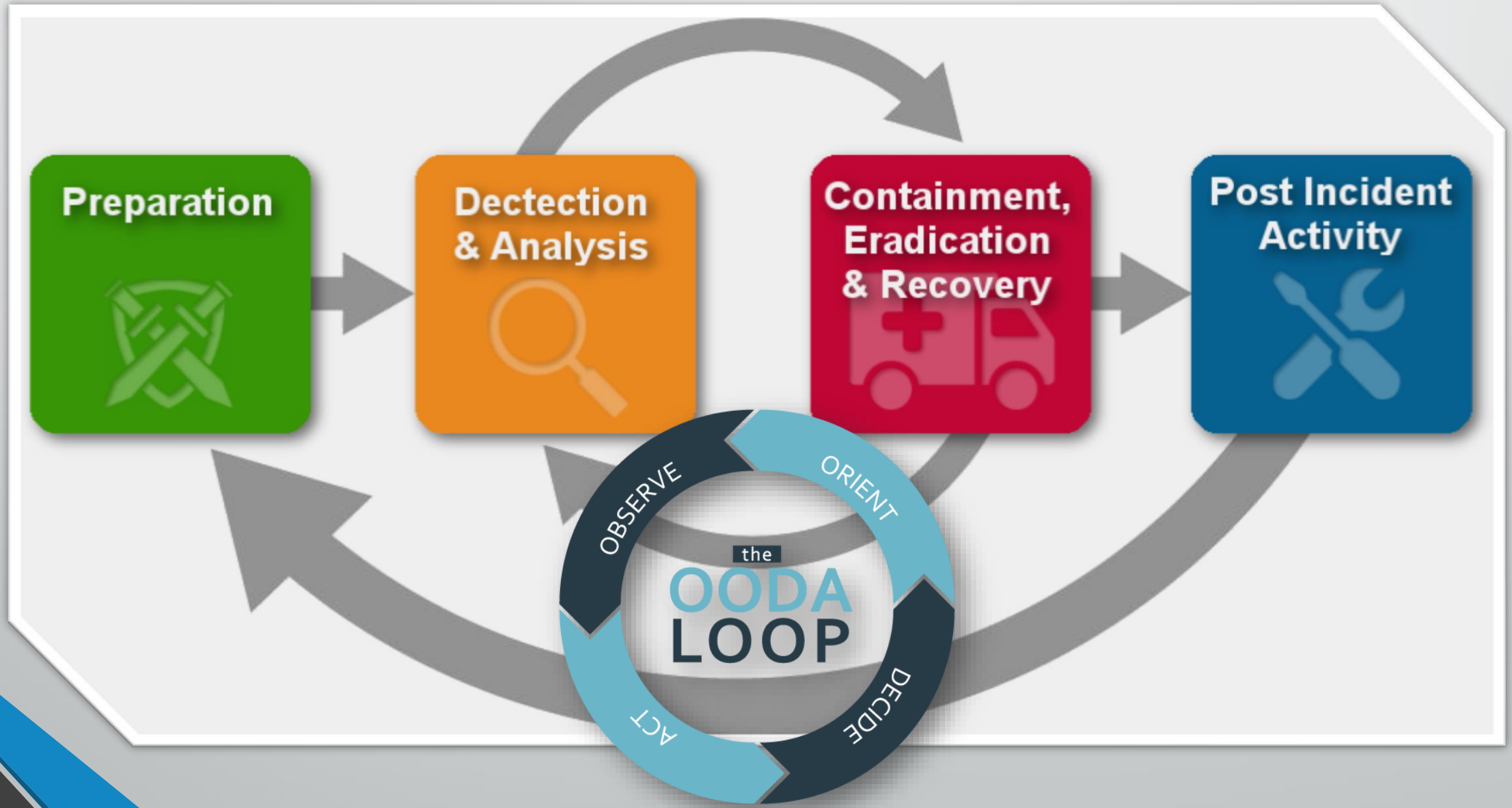
Threat data is the next stage where you will have technical and possible threat-actor context to IOC's allowing organizations to evaluate the threats they have identified or could be exposed to.

Threat Intelligence

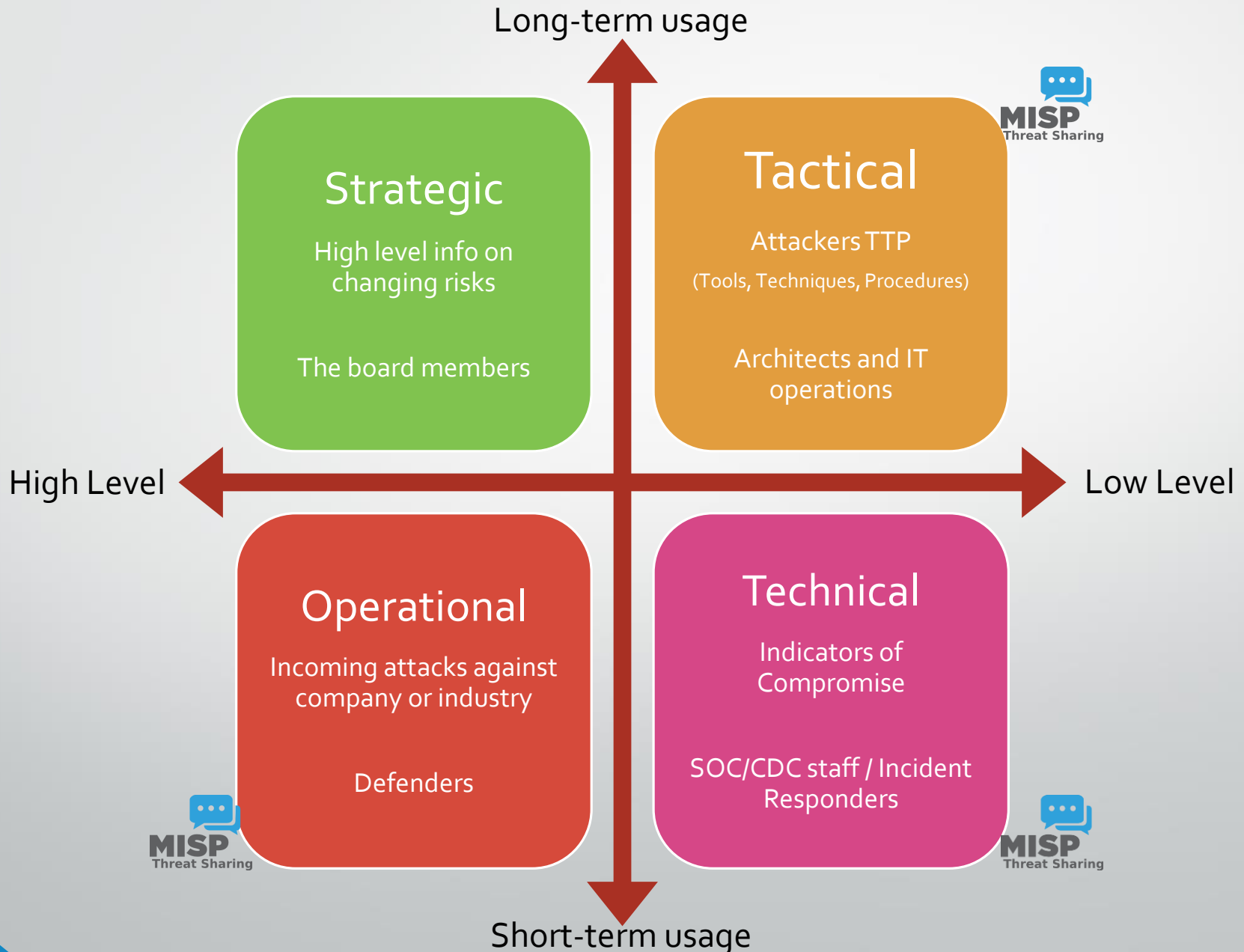
Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response.

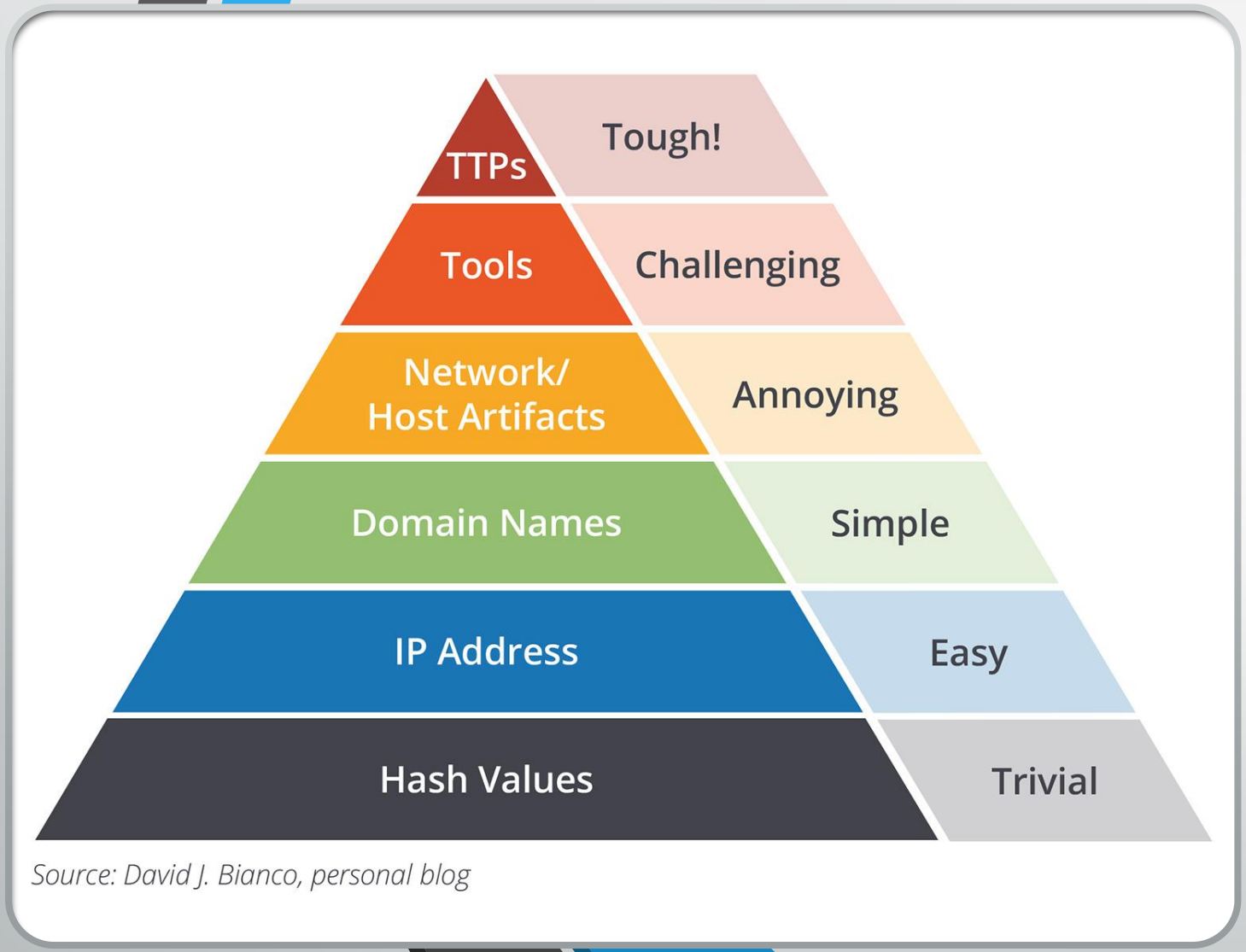
Incident Life-cycle

eCrimeLabs



Type of Threat Intelligence





Source: David J. Bianco, personal blog

Pyramid of Pain

The typical complexity for adversaries to change behaviors and signatures.

Both technical and psychological.

TTP → Techniques, Tools and Procedures

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

Learning platform

- Learn about threat actors and TTP's on malware families.

  Can be used to gain knowledge and train you and your company.

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	

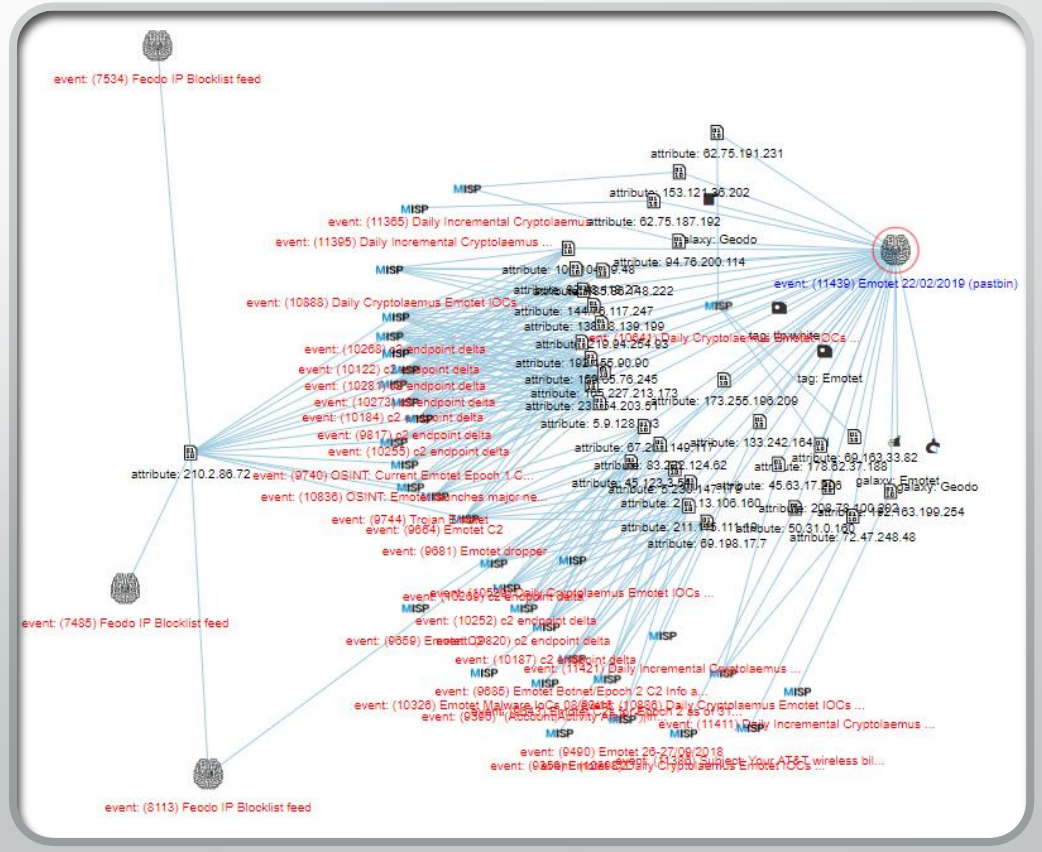
Centralized storage of Threat data

Many receives information of threats through

- Email
- PDF rapports
- Websites
- Etc.

Using a platform like MISP to store this data ensures that you can “easily” on-board new employees over time.

Also by centralizing these data you can perform cross-correlation of data over time.



Crowdsourcing and secure sharing model

- We are stronger together
  - A targeted attack is often not seen by security companies, but what about companies in the same business or country.
  - Does MISP solve everything – NO

But **#SharingIsCaring**

MISP Sharing Model

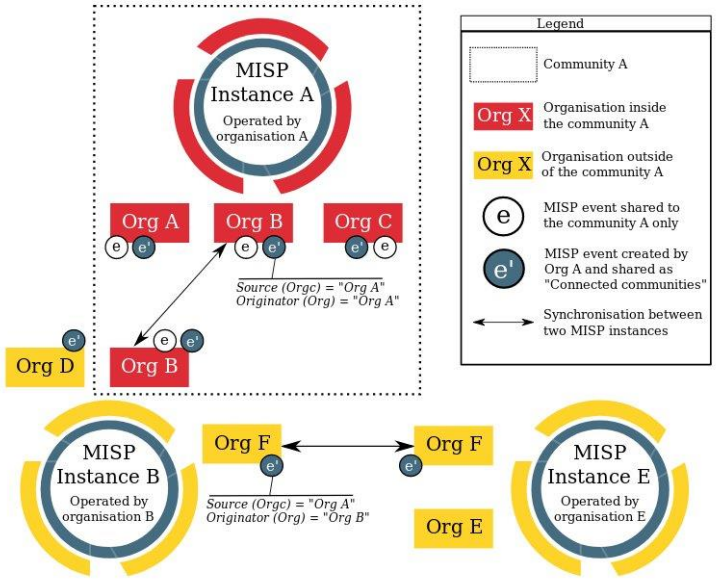
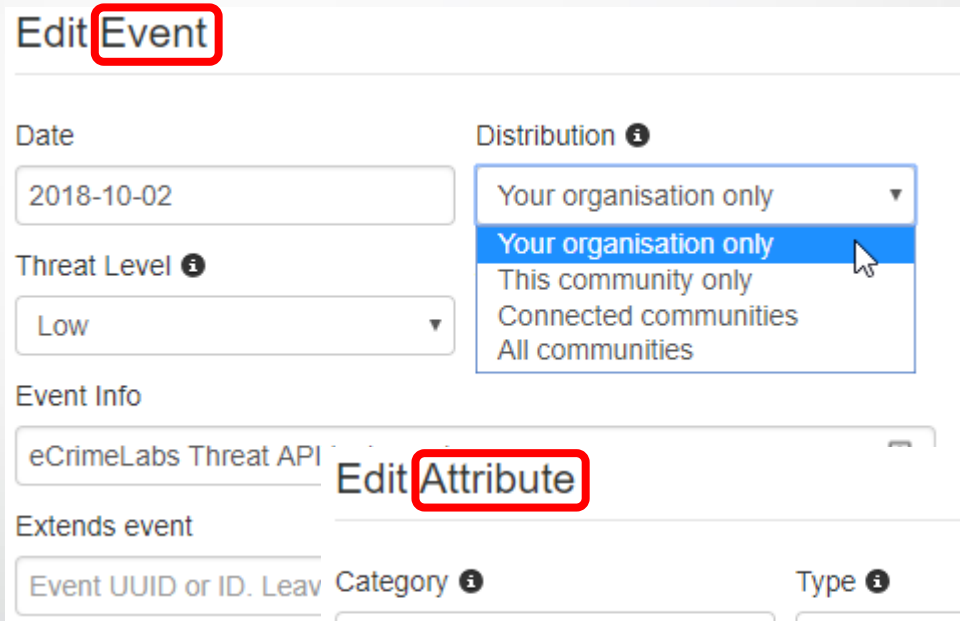
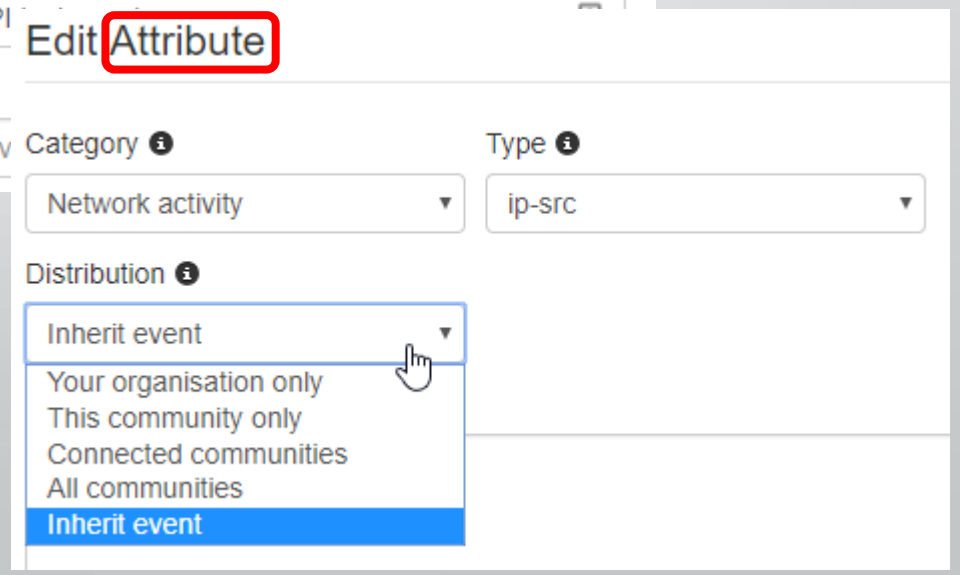


FIGURE 1: Illustration of MISP organisations and community interactions

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





Threat data vs Vulnerability management

"Threat data can also be used in prioritization of vulnerabilities"

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

https://misp.ecrimelabs.net/events/view/12316

Integrate MISP into your security components

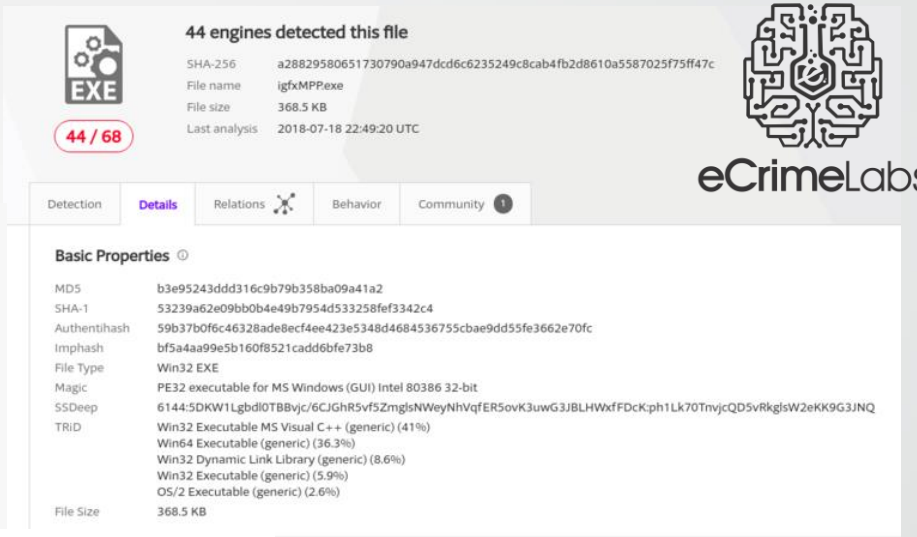
eCrimeLabs

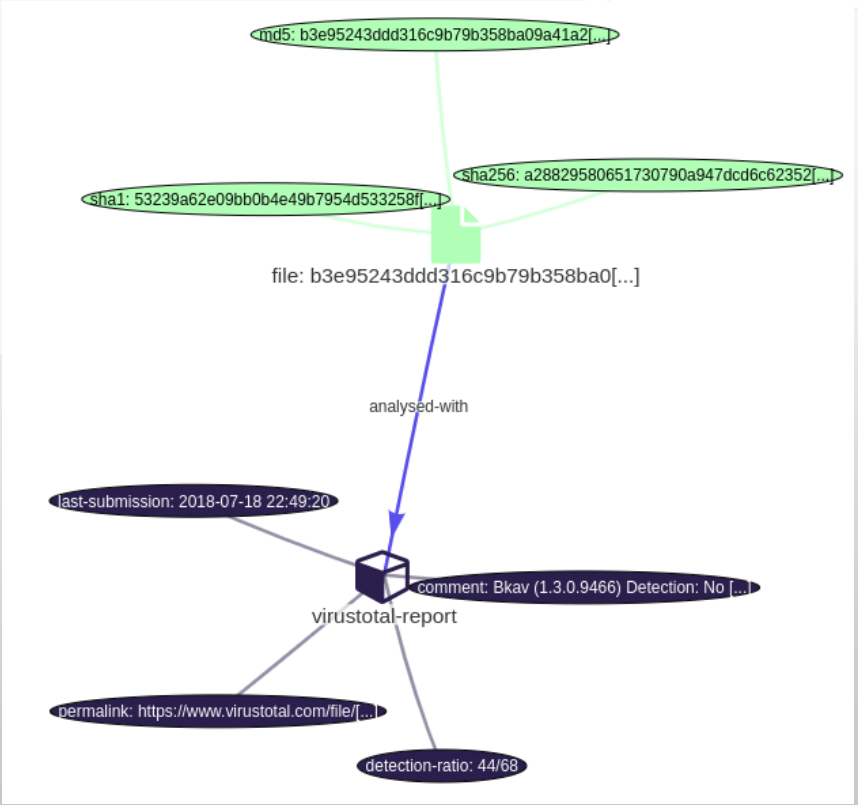
MISP has an open API, where you can extract any specific data you would like, thereby utilizing your threat data into your current infrastructure.

- Blocking
- Alerting

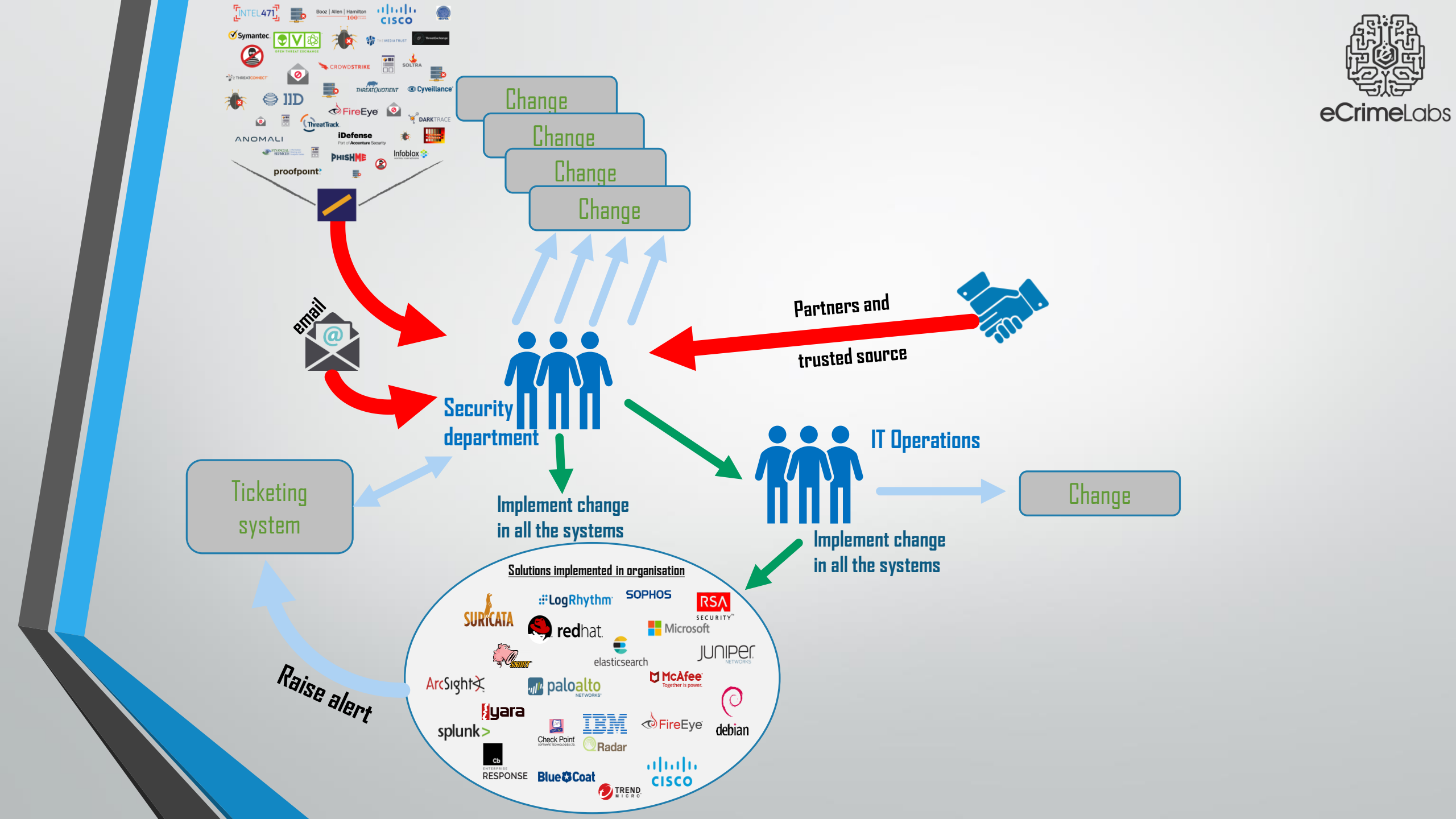
Example of MISP API usage

```
~# python3 vt2misp.py -u 5b53275a-003c-4dcc-b4ce-710f9f590eb0 -a "USBGuard" --force -c 7657fcb7d772448a6d8504e4b20168b8
Virustotal to MISP
(c)2018 eCrimeLabs
https://www.ecrimelabs.com
----------------------------------------

- Checking if checksum is valid - true
- Checking if UUID format is valid - true
- UUID for MISP event detected
- Checksum 7657fcb7d772448a6d8504e4b20168b8 was not detected in the event
- The artefact was found on Virustotal
- Creating object(s)
        * Permalink: https://www.virustotal.com/file/54bc950d46a0d1aa72048a17c8275743209e6c17bdacfc4cb9601c9ce3ec9a71/analysis/1532138638/
        * Detection: 64/67
        * Last scan: 2018-07-21 02:03:58

        * MD5: 7657fcb7d772448a6d8504e4b20168b8
        * SHA1: 84c7201f7e59cb416280fd69a2e7f2e349ec8242
        * SHA256: 54bc950d46a0d1aa72048a17c8275743209e6c17bdacfc4cb9601c9ce3ec9a71
        ------------
        * VirusTotal detections:
                Bkav (1.3.0.9466) Detection: W32.ZeustrackerZS.Trojan
                MicroWorld-eScan (14.0.297.0) Detection: Gen:Variant.Kazy.8782
                CMC (1.1.0.977) Detection: Trojan.Win32.Lebag!O
                CAT-QuickHeal (14.00) Detection: Trojan.Ramnit.A
                |...
                Qihoo-360 (1.0.0.1120) Detection: Win32/Trojan.544

        ------------
- The MISP objects seems to have been added correctly to the event....
```





https://www.ecrimelabs.com/blog/2018/7/21/tool-for-adding-hashes-with-virustotal-data-to-misp-event

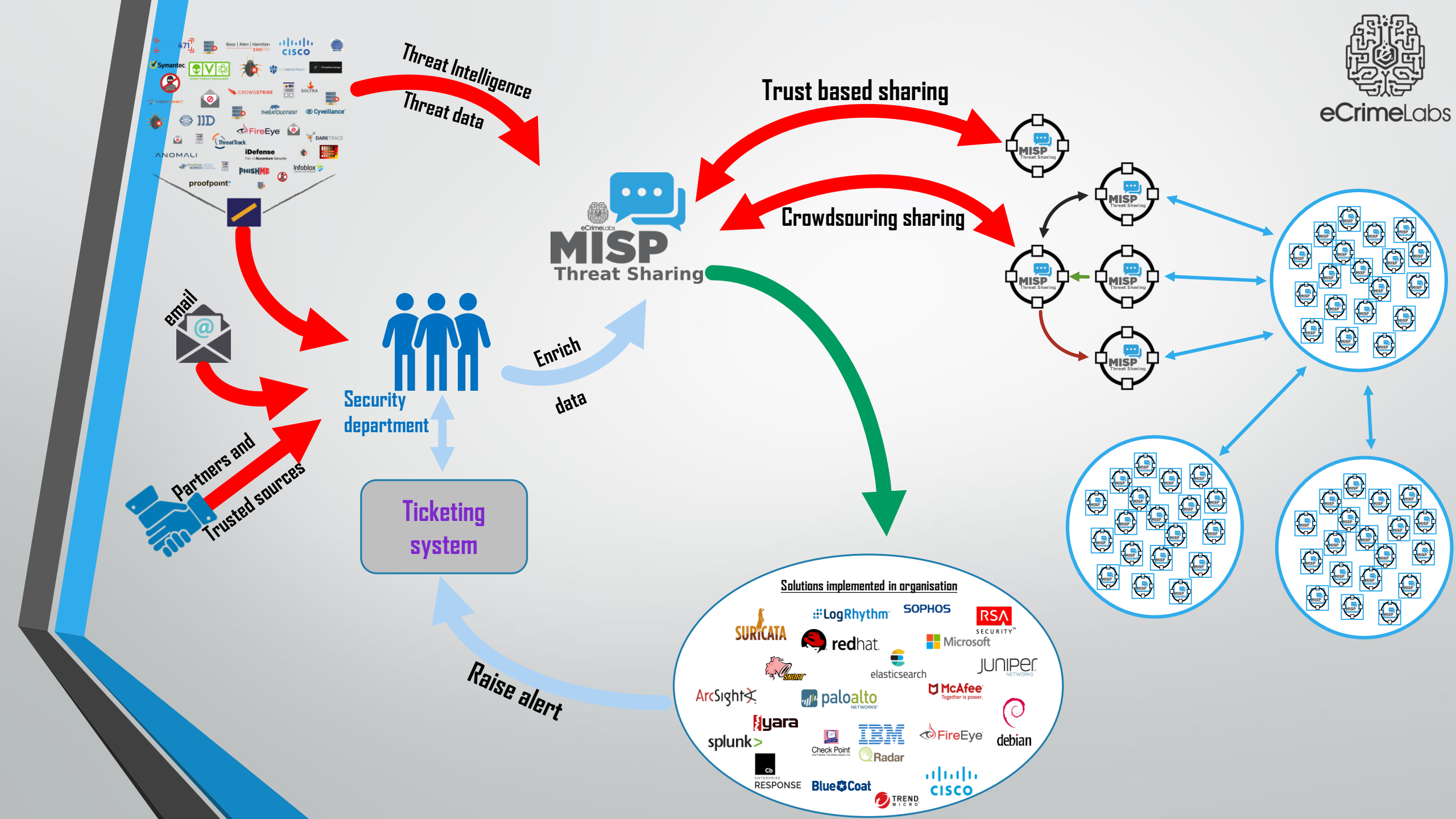

Change
Change
Change
Change
email
Partners and
trusted source
Security
department
Ticketing
system
Implement change
in all the systems
IT Operations
Change
Implement change
in all the systems
Raise alert
Solutions implemented in organisation
eCrimeLabs

The Incident Response Hierarchy of Needs

eCrimeLabs

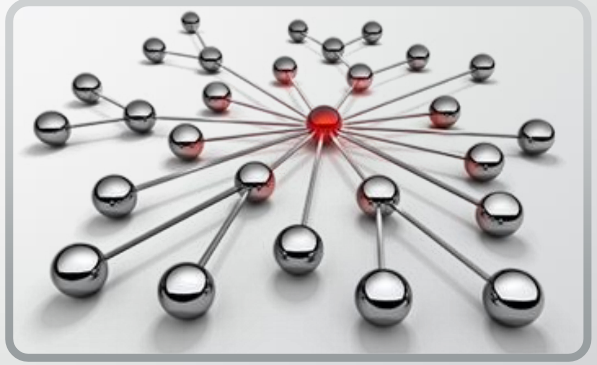
The Incident Response Hierarchy is modeled after Maslow's Hierarchy of Needs. It describes the capabilities that organizations must build to defend their business assets. Bottom capabilities are prerequisites for successful execution of the capabilities above them:

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


Threat Intelligence
Threat data
Trust based sharing
Crowdsouring sharing
MISP
Threat Sharing
eCrimeLabs
email
Partners and
Trusted sources
Security
department
Enrich
data
Ticketing
system
Raise alert
Solutions implemented in organisation
eCrimeLabs

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)



- eCrimeLabs Github page (https://github.com/ecrimelabs)
- eCrimeLabs website (https://www.ecrimelabs.com)

Questions

https://www.ecrimelabs.com

@DennisRand
@eCrimelabs

REDACTED