

# Threat intelligence

[stephane.louis@l-a.lu](mailto:stephane.louis@l-a.lu)

When intelligence is used as a proactive  
Cyber defensive mean

15 december 2017 @ Paul Lambin

# Planning

- Some definitions
- Threat intelligence
  - Why ?
  - How ?

# Planning

- **Some definitions**
- Threat intelligence
  - Why ?
  - How ?

# A few definitions

- **CERT**
  - Computer Emergency Readiness Team
- **CSIRT**
  - Computer Security Incident Response Team
- **IOC**
  - Indice Of Compromission

# A few definitions

- 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 to that menace or hazard. – **Gartner**

The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators – **SANS Institute**

# Threat Intelligence : Why ?

- Leveraging threat intelligence to build proactive cybersecurity



# Planning

- Some definitions
- Threat intelligence
  - Why ?
  - **How ?**

# Building intelligence : How ?

- Basic principle is to feed defensive systems with intelligence knowledge
  - With IOC feeds
    - Free
    - Proprietary
  - Sharing IOC



# Building intelligence : How ? - MISP

- MISP : Malware Information Sharing Platform



## Events

« previous

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20































21

next »

Q

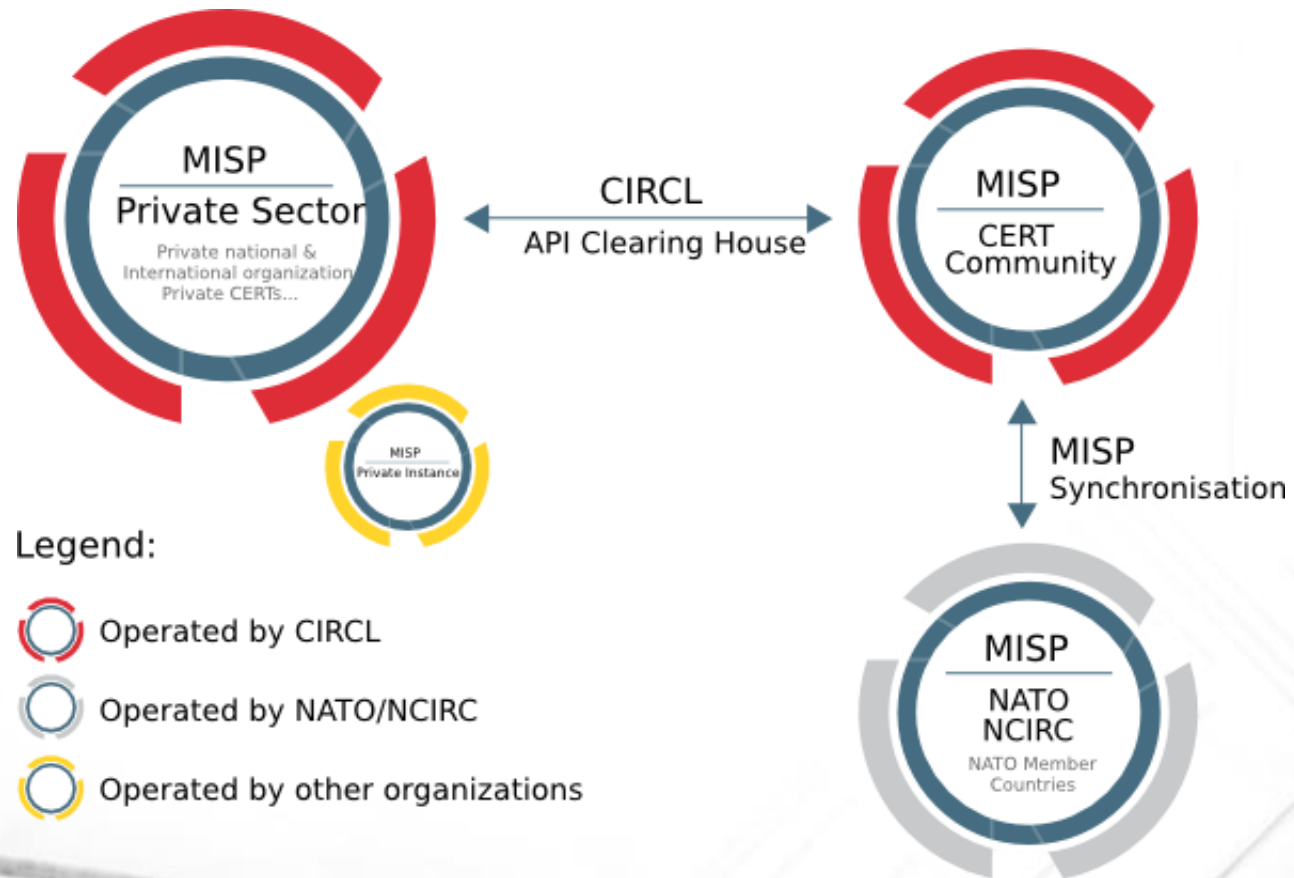
My Events

Org Events

| Published | Org   | Id   | Clusters | Tags  | #Attr. | #Corr. | #Sightings | Date       | Threat Level | Analysis  | Info   |
|-----------|---|------|----------|---|--------|--------|------------|------------|--------------|-----------|--|
| ✕         |    | 5606 |          |    | 91     | 9      |            | 2016-12-19 | Low          | Initial   | Locky 2016-12-19 : Affid=3, DGA=556677 - "Payslip for the month Dec 2016." - "Payslip_Dec_2016_123456.doc" |
| ✓         |    | 5612 |          |    | 49     | 11     |            | 2016-12-20 | Low          | Initial   | Locky 2016-12-20 : Affid=3, DGA=556677 - "for printing" - "Certificate_123456.xls"                         |
| ✓         |    | 5608 |          |             | 237    | 4      |            | 2016-12-19 | Low          | Completed | Kaspersky Lab: Spearphishing attack hits industrial companies  |
| ✓         |   | 5601 |          |     | 247    | 3      |            | 2016-12-19 | Low          | Ongoing   | Malicious android apk delivery infrastructure  |
| ✓         |  | 5613 |          |     | 17     | 14     |            | 2016-12-20 | Low          | Ongoing   | "Uw Factuur" KPN malspam delivers Cerber   |
| ✓         | SwissPost   | 5611 |          |     | 41     | 3      |            | 2016-12-06 | Medium       | Completed | Diamond Fox / "Rechnung * 2828" / "beleg 3421.doc"   |
| ✓         |  | 5609 |          |     | 3      |        |            | 2016-12-19 | Low          | Completed | Phishing domains and kits hosted at 159.203.85.113   |
| ✓         | SwissPost   | 5610 |          |     | 22     | 3      |            | 2016-11-12 | Medium       | Completed | Diamond Fox / "Re: Revised Invoice" / documents.exe  |
| ✓         |  | 5607 |          |      | 20     | 9      |            | 2016-12-19 | Low          | Initial   | Osiris - Locky via Microsoft Office macro  |

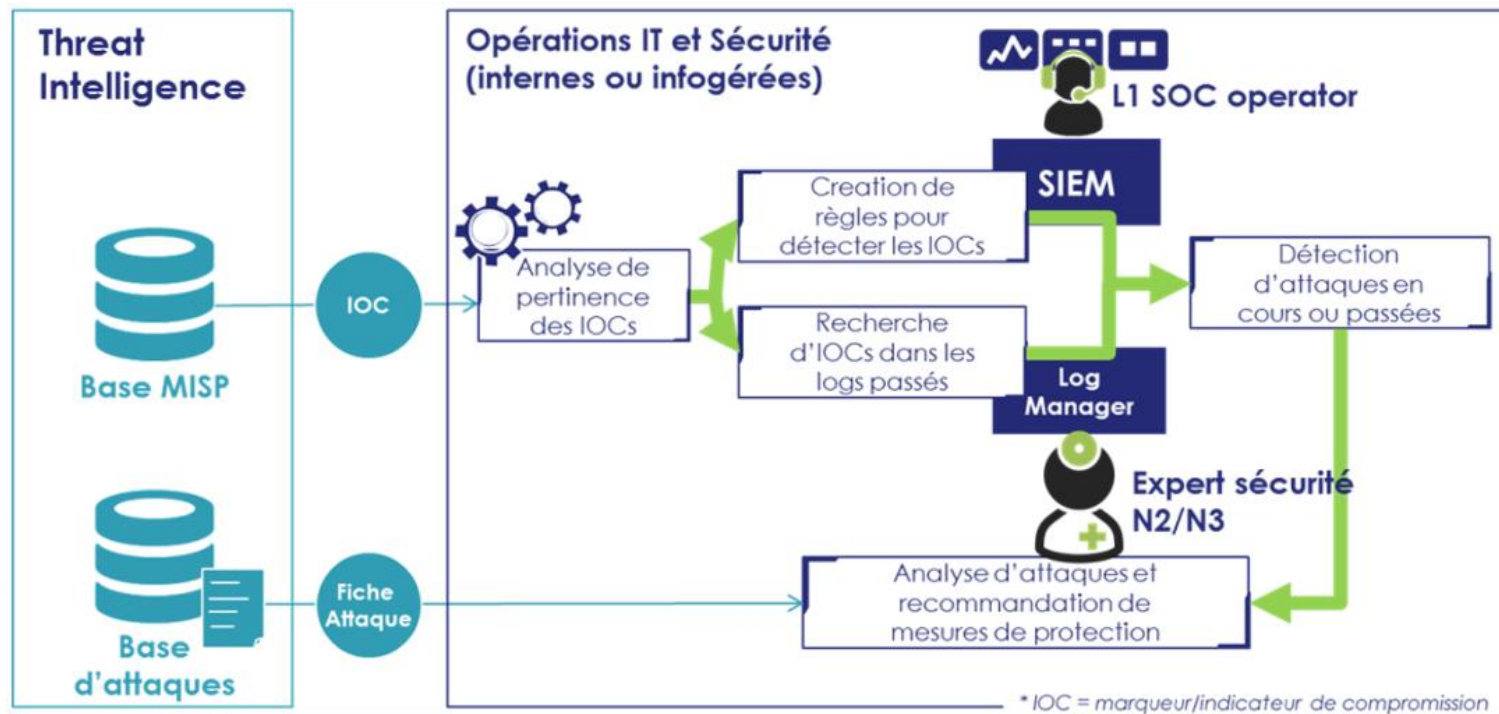
# Building intelligence : How ? - MISP

- MISP are interconnected together



# Building intelligence : How ? - MISP

- MISP : Malware Information Sharing Platform



# Building intelligence : How ? - MISp

- At EU level each country must have an office to analyse CyberThreat
  - Belgian CCB

# Take away

- Threat intel enable proactive cybersecurity
- Threat intel gather intelligence about threat landscape
- Threat intel share intelligence by exchanging IOC
- Following EU regulation, each EU country must have a threat intel platform in order to protect its OIV (Organisme d'Importance Vitale)

**Take it  
away**



tenki หอขอบคุณคุณ takk спасибо kam sah hamnida  
дзякуй hvala תודה dhanyavadagalu tack  
gracias blagodaram mési xièxie tanemirt  
arigatô djere deuf rahmet enkosi mochchakkeram trugarez dank je  
ačiū manana diolch dziekuje akun bedankt danke kop khun krap faafetai lava  
dhanyavad gratias ago tau shukriya ありがとう kia ora dankon děkuji  
teşekkür ederim bayarlalaa gràcie kaitos spat  
sagolun murakoze mahalo didi madioba sukriya obrigada obrigada chnorakaloutioun  
taiku misaotra welalin chokrane rahmat dakujem  
terima kasih nandri 謝謝 mersi najis tuke  
asante grazie mauruuru go raibh maith agat merci nanni vinaka  
matondo căm on ban paldies ngiyabonga