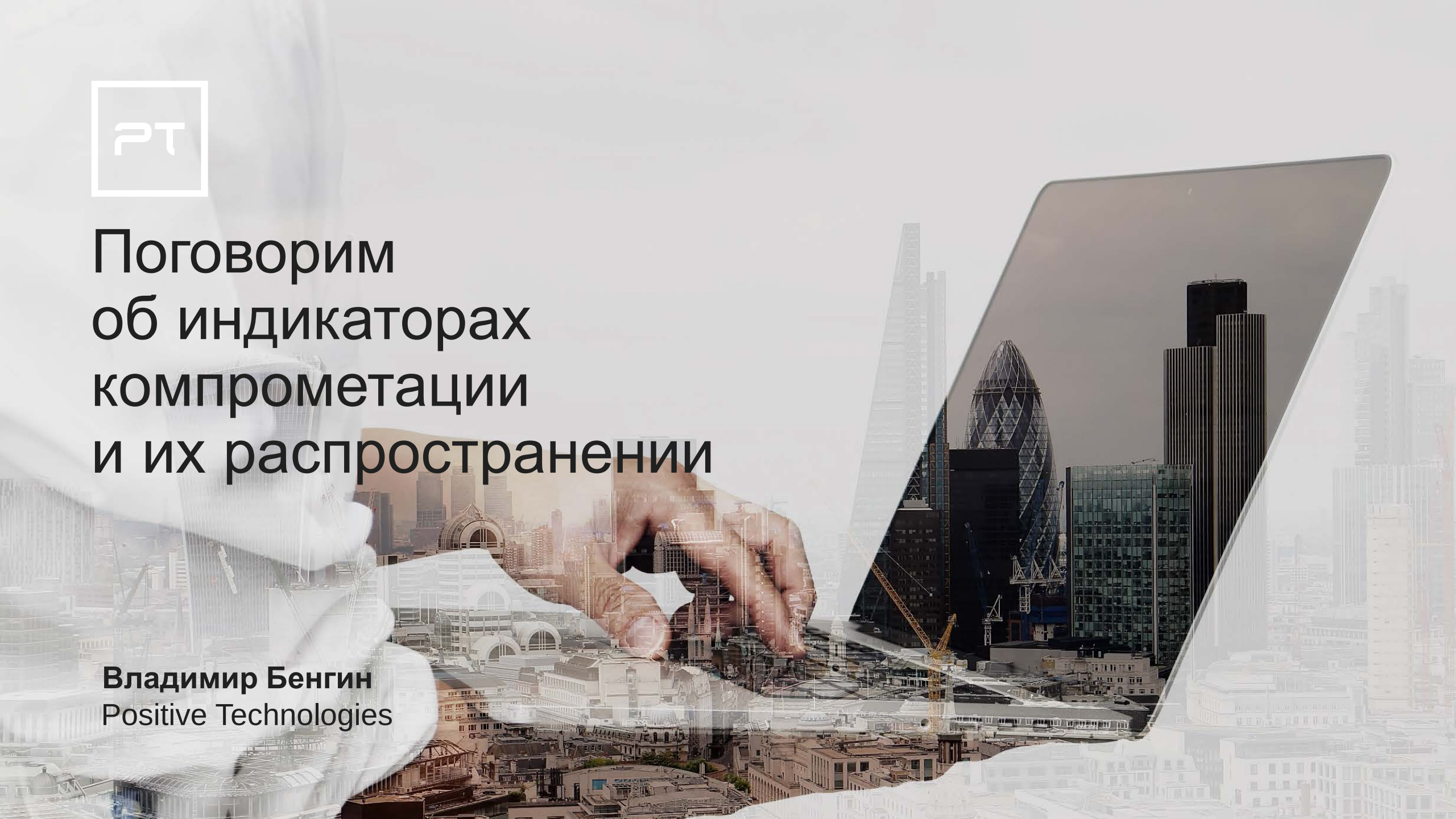


Поговорим об индикаторах компрометации и их распространении

Владимир Бенгин
Positive Technologies

О чем пойдёт речь?

goo.gl/dbUphr
#SOC Технологии

1 Индикатор компрометации (Indicator of Compromise, IoC, ИОК) – артефакт, наблюдаемый в сети или на операционной системе, с высокой степенью достоверности указывающий на компьютерный инцидент

Domains **IP Address** **Hash file** **URLs** **Mail address**

Mail messages **CVE** **Process** **Certificates** **Regkey** и многое другое…

2 IOC Feeds (фиды) – каналы, по которым поставляются индикаторы компрометации

3 OpenIoC, MISP, STIX – общепринятые форматы описания индикаторов компрометации

4 Не пойдёт речь об IOA, TTP, ATT&CK, … и других модных словах

Как используют фиды

goo.gl/dbUphr
#SOC Технологии

1 Дополнительный инструмент оперативного выявления и блокировки массовых атак

Интегрировать с инфраструктурой для работы на потоке (выявление > блокировка)

2 Средство выявления таргетированных атак

Использовать в рамках ретроспективы и расследований

Вопросы:
Как вы используете фиды сегодня? Как бы вы хотели их использовать?

Рынок коммерческих подписок

goo.gl/dbUphr
#SOC Технологии

2016

Единичные продажи

2018

200–300 млн. рублей
~60 клиентов

Kaspersky **GroupIB** **Eset**

ЦБ (ФинЦЕРТ) **НКЦКИ**

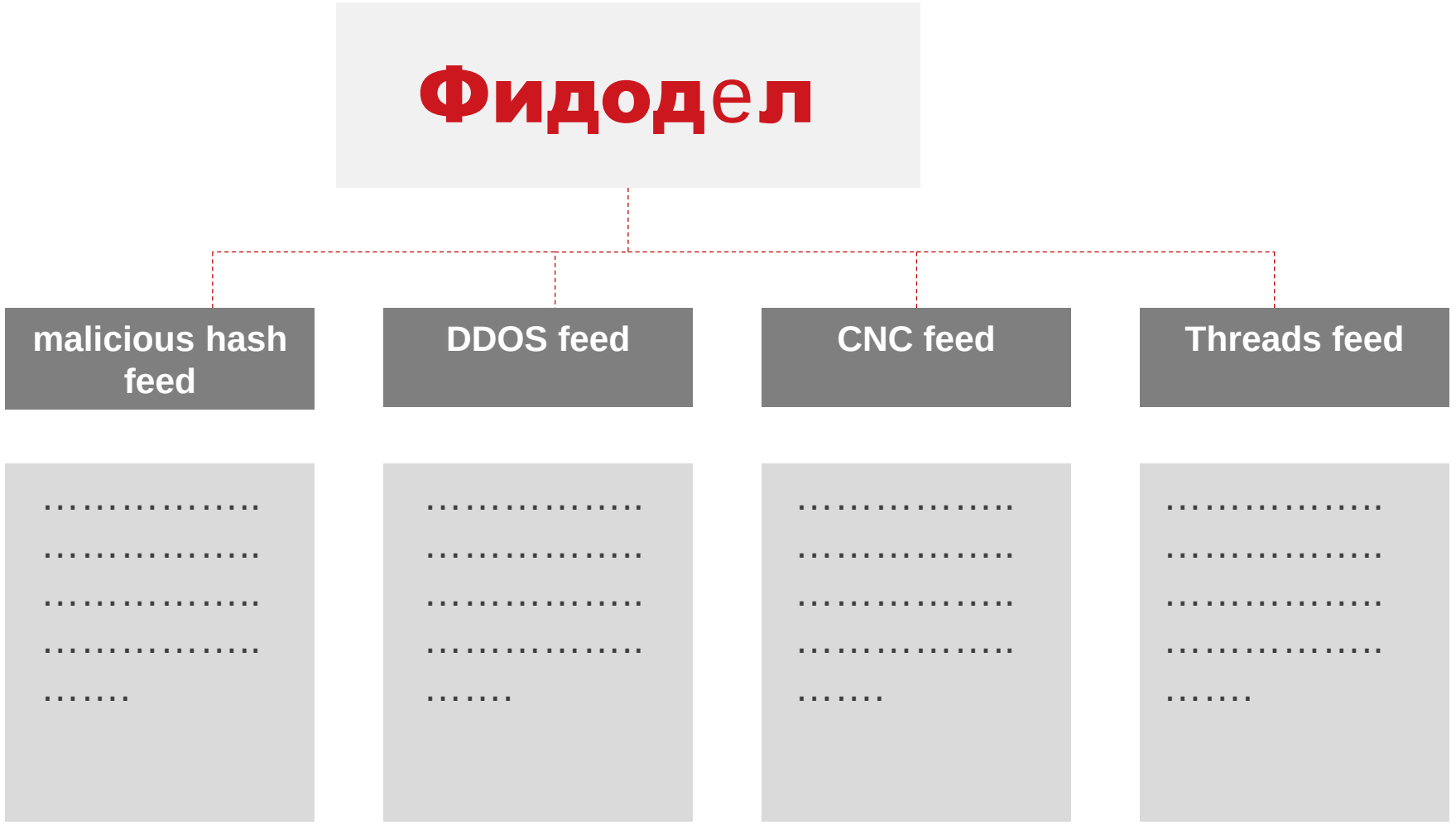
Feodo Tracker **FireHOL** **MalwareDomain List** **Ransomwaretracker** **AlienVault**

ZeuS Tracker **MISP CERT LU** **MISP inThreat** **MISP Fidelis** **Facebook**

Вопрос: Покупаете ли вы фиды?

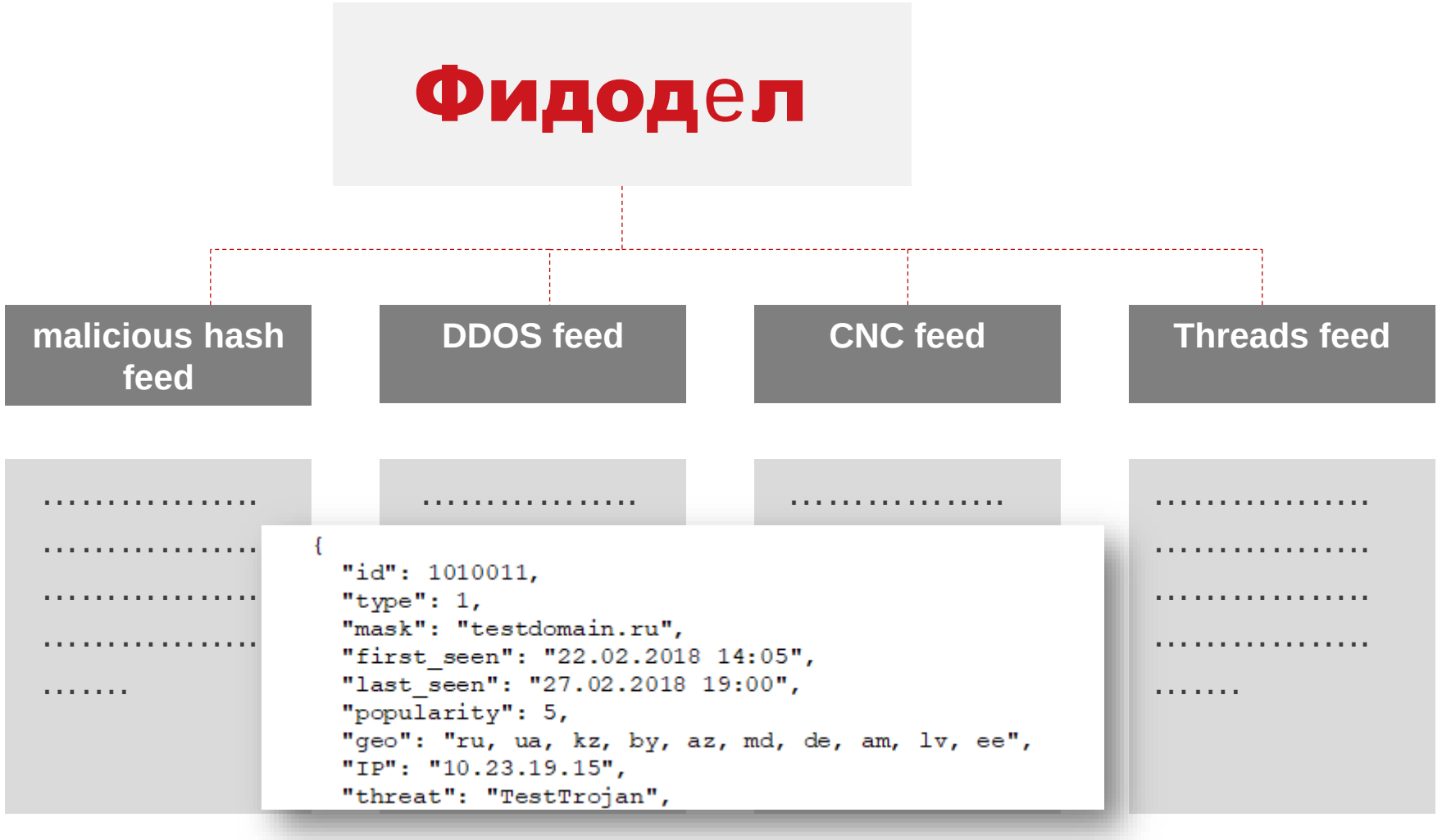
Матчасть #1

goo.gl/dbUphr
#SOC Технологии



Матчасть #1

goo.gl/dbUphr
#SOC Технологии



Матчасть #2

goo.gl/dbUphr
#SOC Технологии

CNC Feeds

с 01.02.2019 по 07.02.2019

IP – 5 907
(act 563)

Domains – 305 351
(act 4682)

Матчасть #2

goo.gl/dbUphr
#SOC Технологии

CNC Feeds

с 01.02.2019 по 07.02.2019

IP – 5 907
(act 563)

Domains – 305 351
(act 4682)

IP – 760
(act 10)

Domains – 2568
(act 24)

Матчасть #2

goo.gl/dbUphr
#SOC Технологии

CNC Feeds

с 01.02.2019 по 07.02.2019

IP – 5 907
(ACT 563)

Domains – 305 351
(ACT 4682)

Пересечение:
IP – 32
Domains – 44

IP – 760
(ACT 10)

Domains – 2568
(ACT 24)

Сложности в работе с фидами

goo.gl/dbUphr
#SOC Технологии

0 Ошибки в фидах

1 Большой объём постоянно обновляемой информации

2 Территориальная и отраслевая специфика

3 Форматы не совсем едины

Сложности в работе с фидами

goo.gl/dbUphr
#SOC Технологии

0

nalog.ru

8.8.8.8

Ошибки в фидах

1

Большой объём постоянно обновляемой информации

2

Территориальная и отраслевая специфика

3

Форматы не совсем едины

Сложности в работе с фидами

goo.gl/dbUphr
#SOC Технологии

0

Ошибки в фидах

nalog.ru

8.8.8.8

1

Большой объём постоянно обновляемой информации

4500 domains\week

2

Территориальная и отраслевая специфика

3

Форматы не совсем едины

Сложности в работе с фидами

goo.gl/dbUphr
#SOC Технологии

```
{
  "id": 1010011,
  "type": 1,
  "mask": "testdomain.ru",
  "first_seen": "22.02.2018 14:05",
  "last_seen": "27.02.2018 19:00",
  "popularity": 5,
  "geo": "ru, ua, kz, by, az, md, de, am, lv, ee",
  "IP": "10.23.19.15",
  "threat": "TestTrojan",
  "whois": {
    "domain": "testdomain.ru",
    "created": "01.09.2016",
    "updated": "01.09.2017",
    "expires": "01.09.2018",
    "name": "Domain",
    "org": "Registrator Co",
    "registrar_name": "Registrator Co",
    "NS": "ns.dns.com, ns2.dns.com",
    "NS_ips": "12.49.92.92, 12.49.92.93"
  }
```

1 Большой объём постоянно обновляемой информации

4500 domains\week

2 Территориальная и отраслевая специфика

3 Форматы не совсем едины

Сложности в работе с фидами

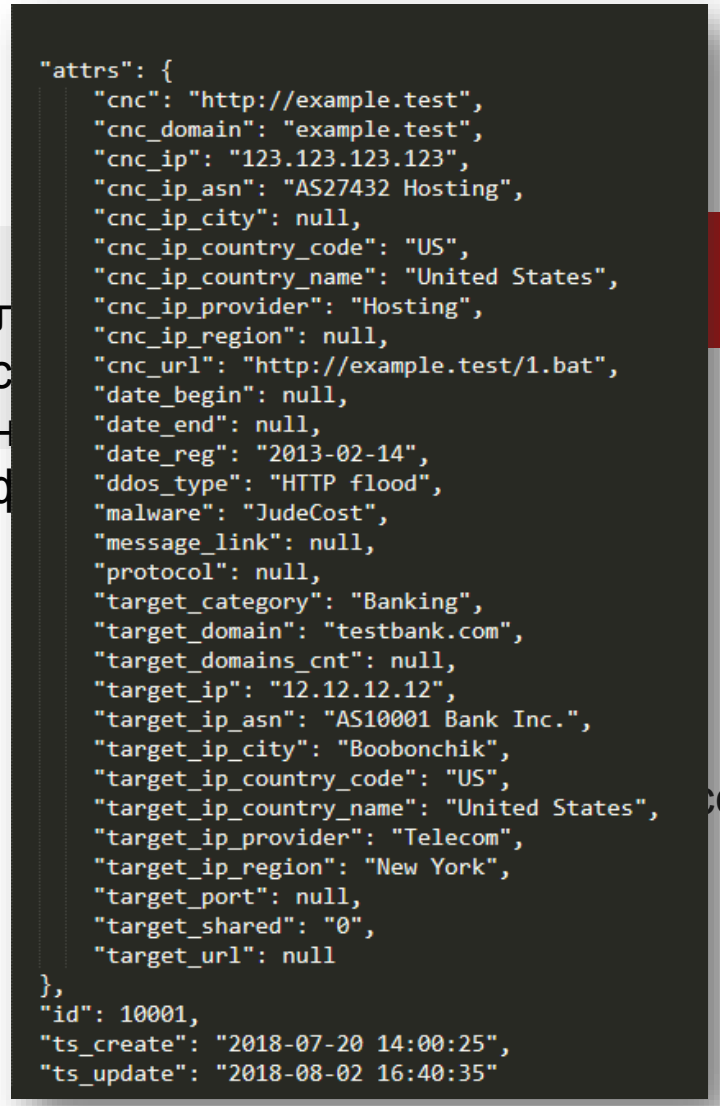
goo.gl/dbUphr
#SOC Технологии

```
{
  "id": 1010011,
  "type": 1,
  "mask": "testdomain.ru",
  "first_seen": "22.02.2018 14:05",
  "last_seen": "27.02.2018 19:00",
  "popularity": 5,
  "geo": "ru, ua, kz, by, az, md, de, am, lv, ee",
  "IP": "10.23.19.15",
  "threat": "TestTrojan",
  "whois": {
    "domain": "testdomain.ru",
    "created": "01.09.2016",
    "updated": "01.09.2017",
    "expires": "01.09.2018",
    "name": "Domain",
    "org": "Registrator Co",
    "registrar_name": "Registrator Co",
    "NS": "ns.dns.com, ns2.dns.com",
    "NS_ips": "12.49.92.92, 12.49.92.93"
  }
```

1

Бол
пос
обн
инф

Территориальная и
отраслевая специфика



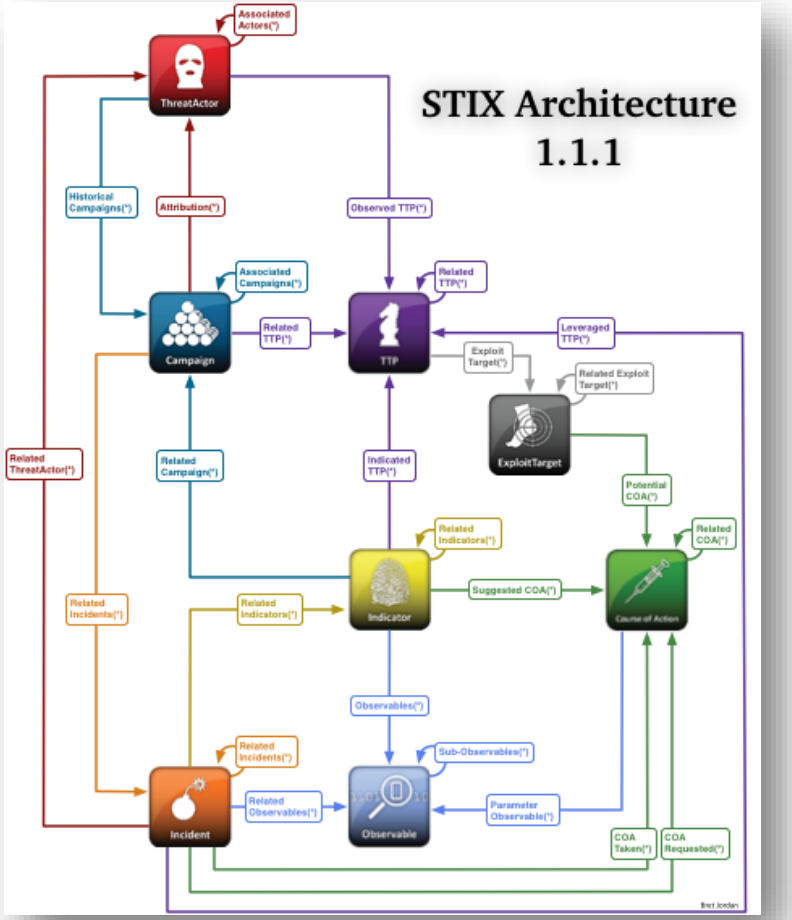
```
"attrs": {
    "cnc": "http://example.test",
    "cnc_domain": "example.test",
    "cnc_ip": "123.123.123.123",
    "cnc_ip_asn": "AS27432 Hosting",
    "cnc_ip_city": null,
    "cnc_ip_country_code": "US",
    "cnc_ip_country_name": "United States",
    "cnc_ip_provider": "Hosting",
    "cnc_ip_region": null,
    "cnc_url": "http://example.test/1.bat",
    "date_begin": null,
    "date_end": null,
    "date_reg": "2013-02-14",
    "ddos_type": "HTTP flood",
    "malware": "JudeCost",
    "message_link": null,
    "protocol": null,
    "target_category": "Banking",
    "target_domain": "testbank.com",
    "target_domains_cnt": null,
    "target_ip": "12.12.12.12",
    "target_ip_asn": "AS10001 Bank Inc.",
    "target_ip_city": "Boobonchik",
    "target_ip_country_code": "US",
    "target_ip_country_name": "United States",
    "target_ip_provider": "Telecom",
    "target_ip_region": "New York",
    "target_port": null,
    "target_shared": "0",
    "target_url": null
},
"id": 10001,
"ts_create": "2018-07-20 14:00:25",
"ts_update": "2018-08-02 16:40:35"
```

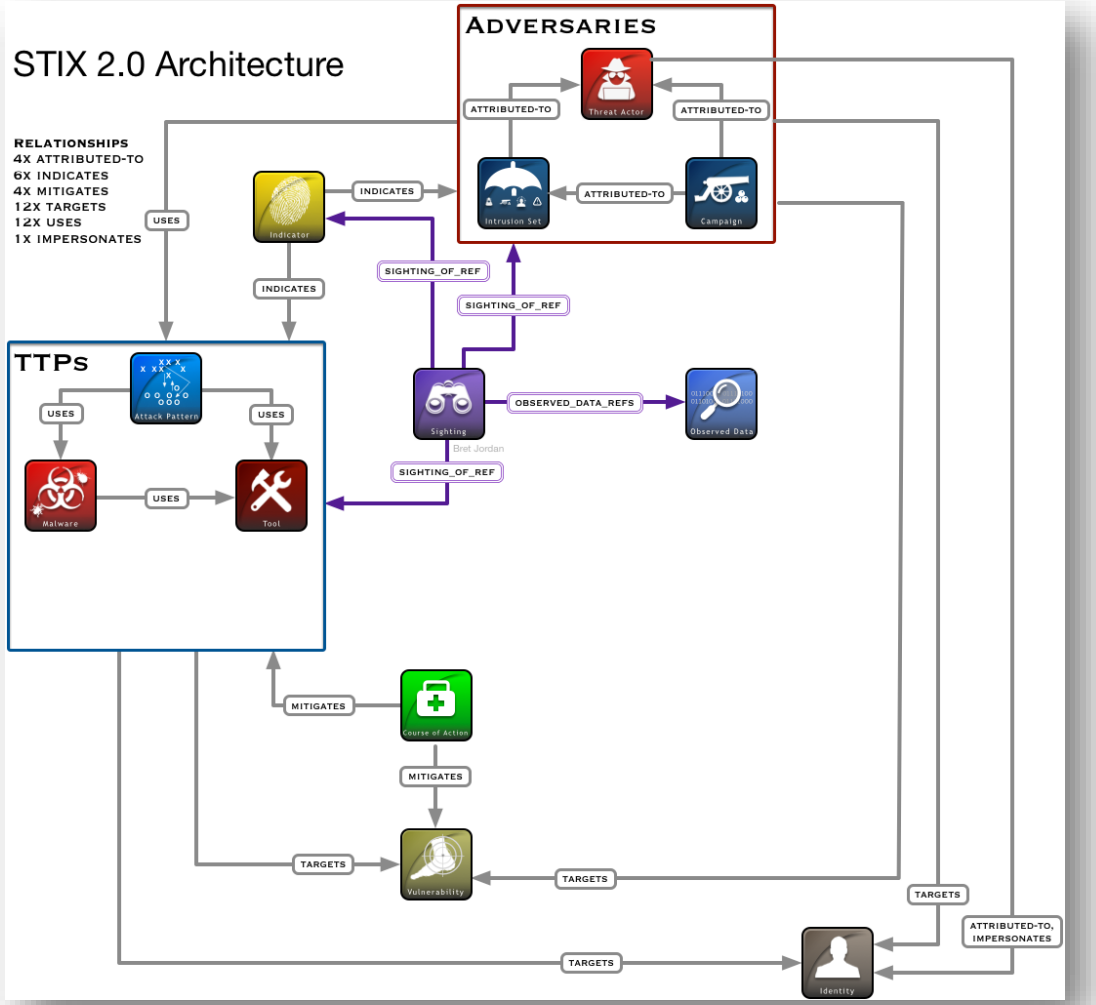
совсем

Ода STIX

goo.gl/dbUphr
#SOC Технологии

Раньше был OpenIOC**, потом все стали говорить** – STIX, **сегодня есть STIX v2**

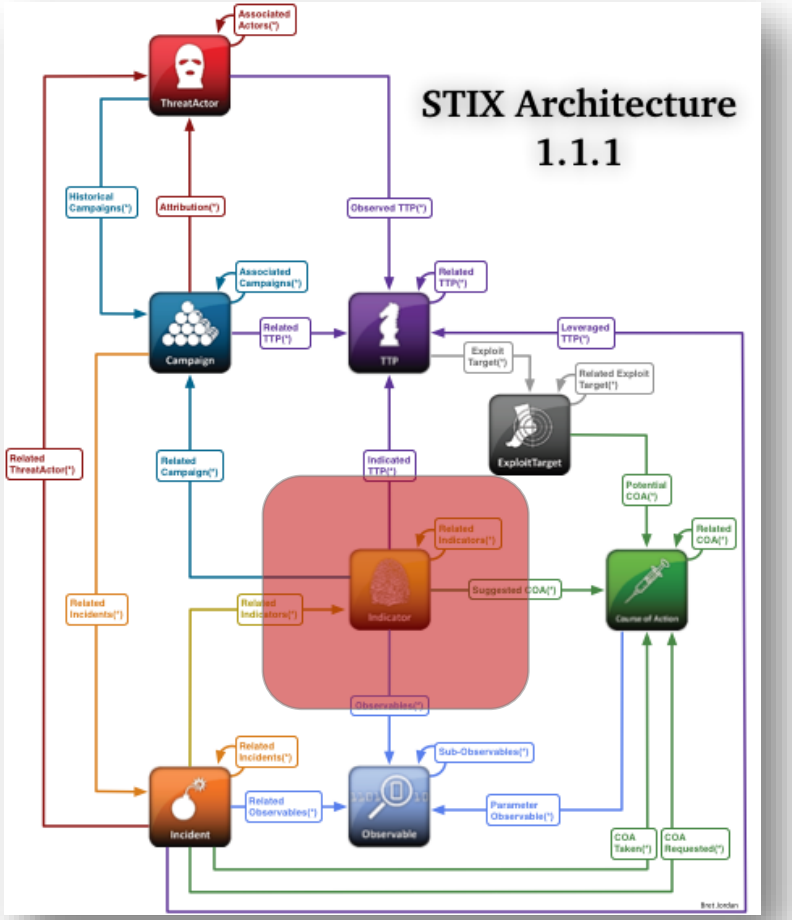


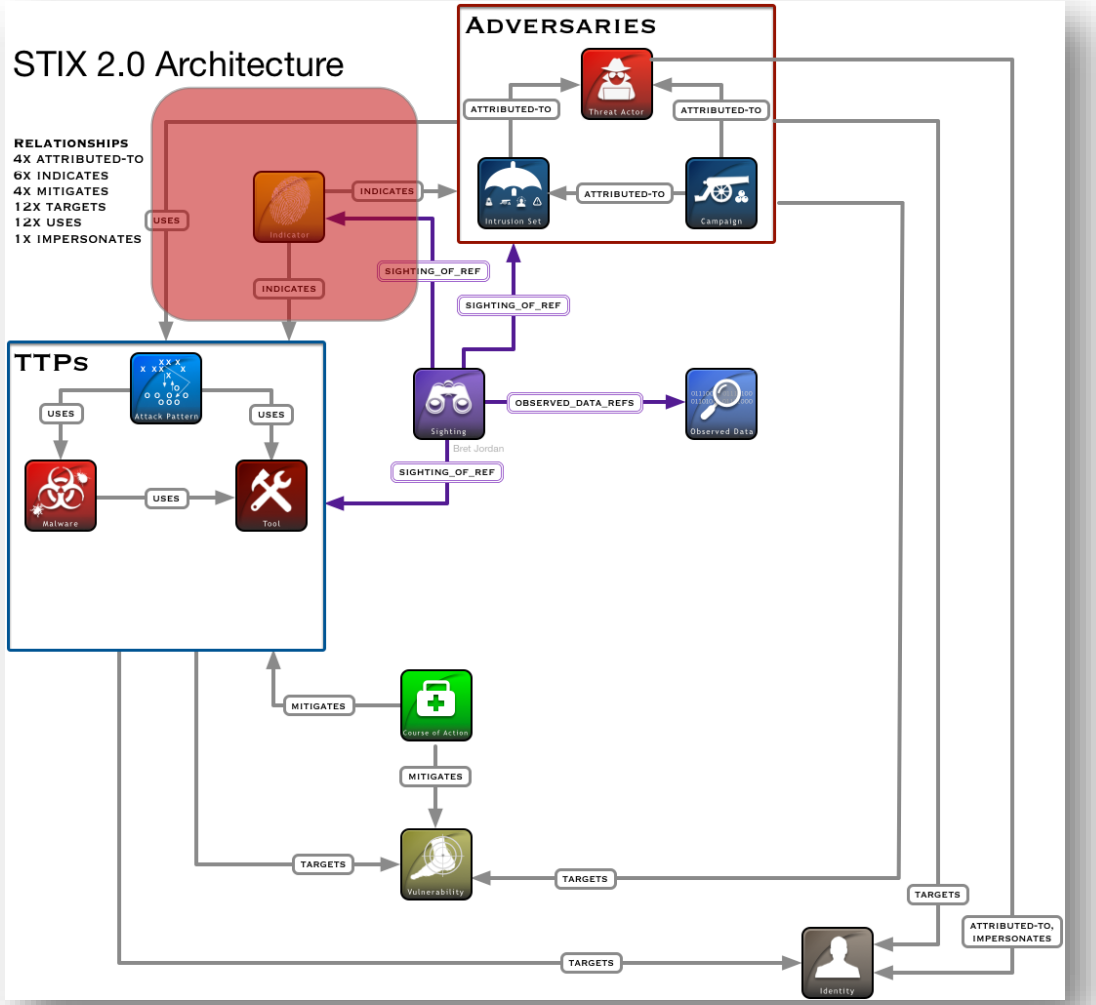


Ода STIX

goo.gl/dbUphr
#SOC Технологии

Раньше был OpenIOC**, потом все стали говорить** – STIX, **сегодня есть STIX v2**

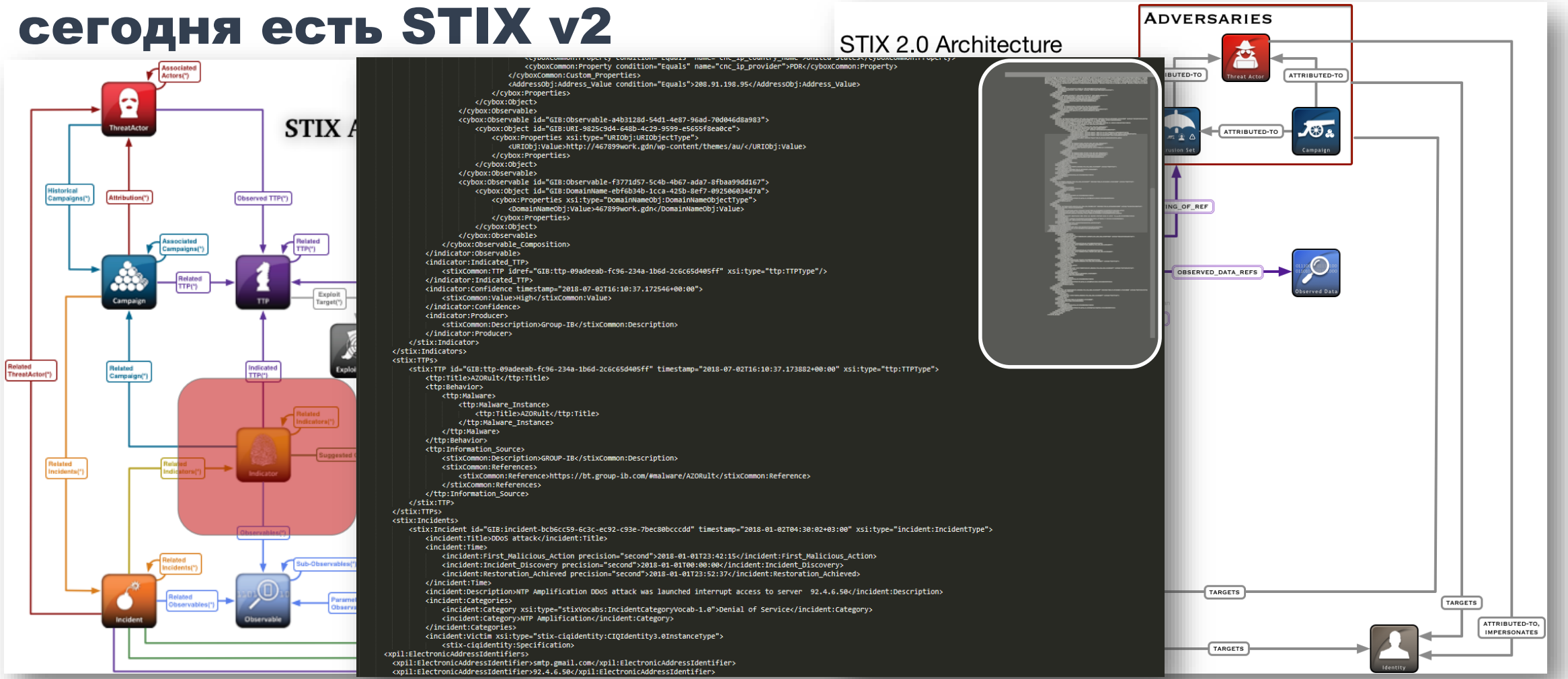




Ода STIX

goo.gl/dbUphr
#SOC Технологии

Раньше был OpenIOC**, потом все стали говорить** – STIX, **сегодня есть STIX v2**



Пути решения (продвинутый)

goo.gl/dbUphr
#SOC Технологии

- Приобрести фиды у различных вендоров;
- Привести записи к единой модели данных и поместить в хранилище;
- Обогатить дополнительной полезной информацией (WHOIS, песочницы, IDS, подписка на VirusTotal…);
- Хранить все данные исторически;
- Рассчитывать пересечение между атрибутами разных фидов;
- Собирать статистику срабатываний индикаторов.

В итоге организация формирует для себя собственный набор IoC (полный, чистый, релевантный).
Но это немного сложно…

Cybsi

Вопрос: Хотели бы вы такую систему? Строите ли её уже сегодня?

Пути решения (ФинЦЕРТ)

goo.gl/dbUphr
#SOC Технологии

- Учтена территориальная и отраслевая специфика;
- Positive Technologies поставляет в ФинЦЕРТ необходимые компоненты в рамках второй очереди
- ФинЦЕРТ организационно уже сегодня умеет работать в рамках данного процесса

Банки РФ

Cybsi

Бюллетени

Необходимо активное вовлечение участников (больше принимаемой информации, больше покрытие в фиде).

Вместе можно сделать что-то интересное…

Вопрос: Готовы ли отдавать телеметрию? Готовы ли поставлять в ФинЦЕРТ больше информации?

Спасибо

Владимир Бенгин

VBengin@ptsecurity.ru