pDNSSOC

Correlating DNS logs with MISP threat intelligence

CHRISTOS ARVANITIS
PAU CUTRINA VILALTA
ROMAIN WARTEL

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

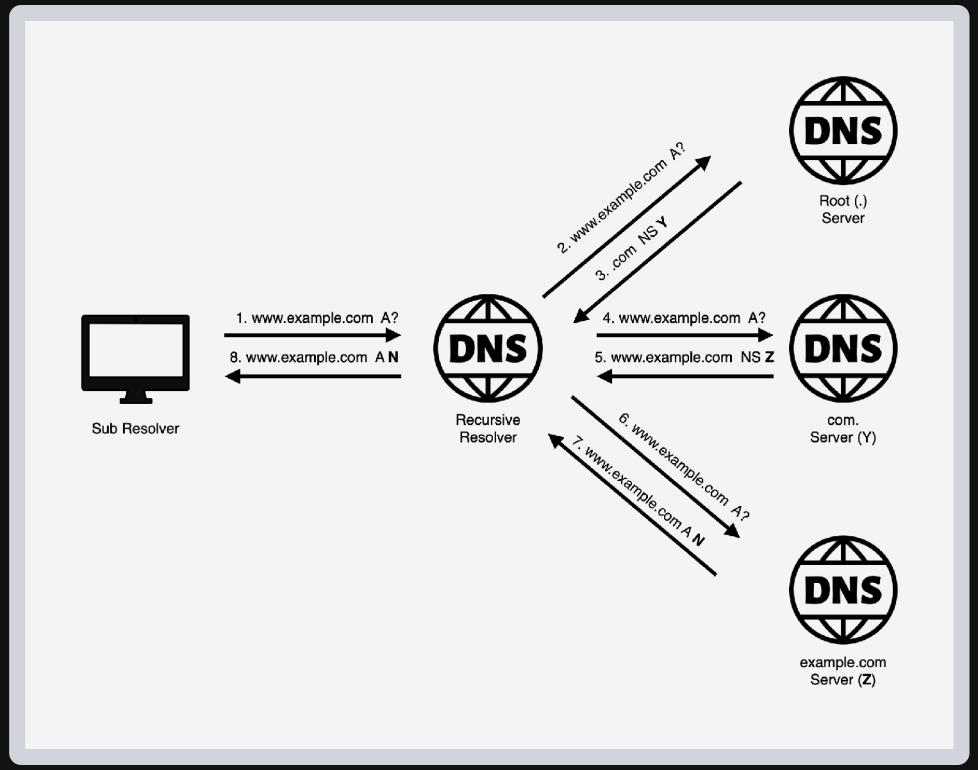
NSF Cybersecurity Summit
October 23-26, 2023

Overview

- DNS basics
- MISP
- pDNSSOC
- Deployment
- Case Study
- Privacy
- Fine-tuning
- Status & Future goals

DNS basics

` curl -XGET example.com `



DNS

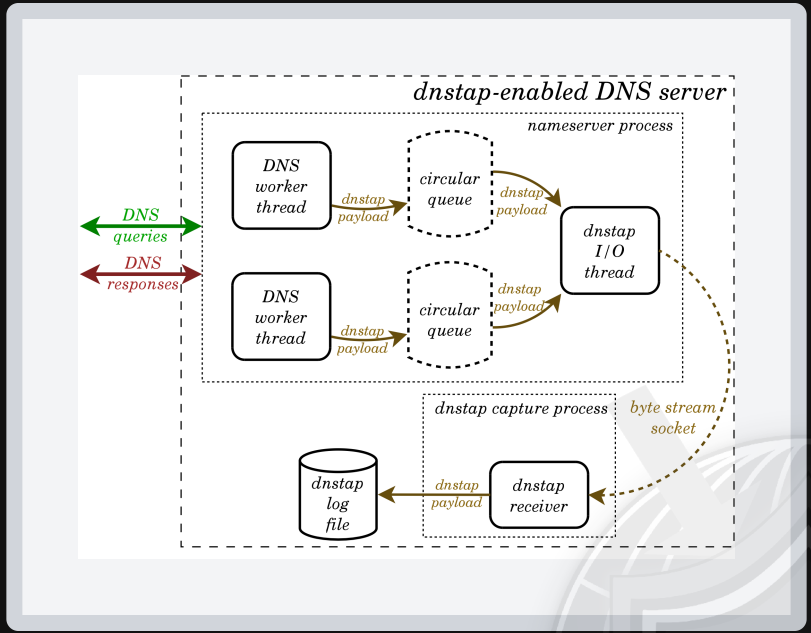
How to get logs

- DNS server logs
  - missing information, performance issues
- Async (pcap, BPF)
  - If not fast enough, DNS still available
- Multiple packets (EDNS)
  - Reassembling queries and responses is difficult
- Zeek
  - Amazing tool, targetting only mature organizations
- dnstap
  - Message types tightly bound to the agent triggering them
  - Easy to filter out duplicate information and PII

DNS

DNSTAP

- Log generation directly into DNS server
- No packet capture
- Combining DNS requests and responses
- Can replicate state not directly in packet capture (was this a cached reply?)
- Based on Protocol Buffers
- Available on major DNS server implementations (e.g. BIND, Unbound, PDNS,)



https://dnstap.info/Architecture/

DNS

DNSTAP

```
26-Oct-2023 16:32:12.081 client
@0x7fbb3e321480 185.80.*.*#36851 (example.com):
query: example.com IN TYPE65 + (DNS_SERVER_IP)
```

Server Query Logs

```
{
  "family": "IPv4","protocol": "UDP",
  "query-ip": "188.184.*.*","query-port": "56537",
  "response-ip": "50.116.16.111",
  "dns": {
    "rcode": "NOERROR", "qname": "malicious.top",
    "qtype": "A",
    "flags": {
      "qr": true, # Response to query
      "aa": true, # Authoritative Answer
    },
    "resource-records": {
      "an": [{ "name": "malicious.top", "rdatatype": "A",
          "ttl": 60, "rdata": "50.116.16.111"}],
    },
  },
  "operation": "CLIENT_RESPONSE", "identity": "dnstap_client"
    "timestamp-rfc3339ns": "2023-09-10T20:16:18.913238827Z",
}
```

DNSTAP logs

DNS

Passive DNS

- Stored collection of historical DNS resolution data
- Format:

```
{
  "count":8068,
  "time_first":1401296056,
  "time_last":1656049207,
  "rrname":"home.cern.ch.",
  "rrtype":"A",
  "bailiwick":"cern.ch.",
  "rdata":["188.184.9.235"]
}
```

- Useful at
  - Locating domains connected to known malicious addresses
  - Fraud and domain name infringement detection
  - Pinpointing newly-registered domains, typosquatting,...

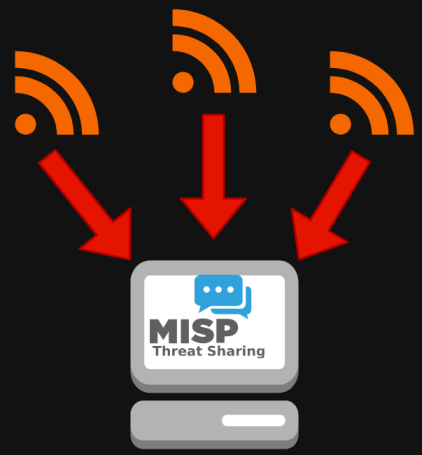
MISP

How does it work?

- Install and setup MISP

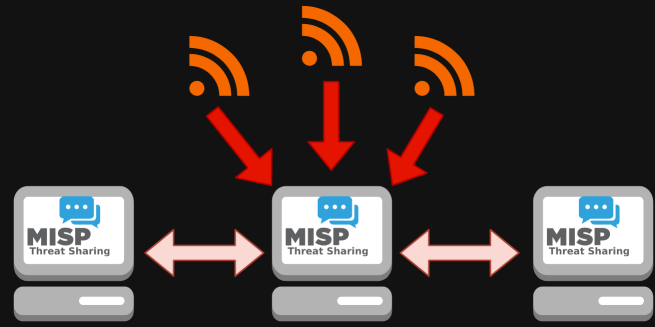
How does it work?

- Install and setup MISP
- Consume threat intelligence feeds
  - Free or Commercial
  - IPs, domains, hashes, TTPs ...



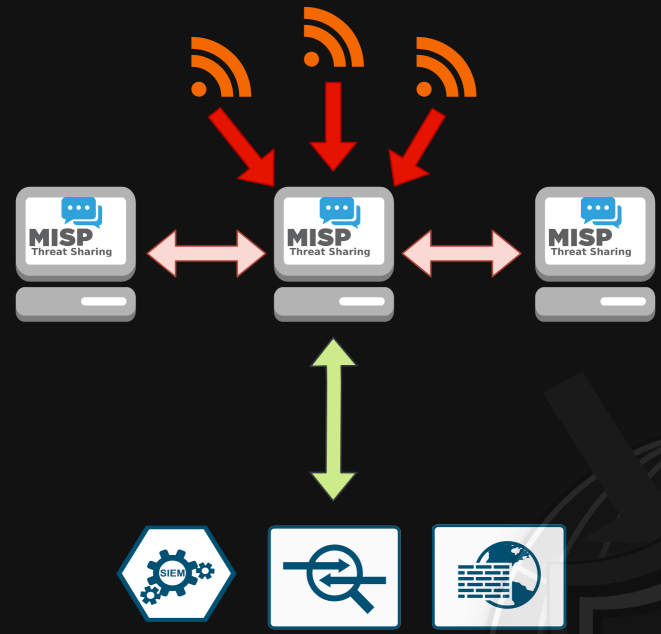
How does it work?

- Install and setup MISP
- Consume threat intelligence feeds
  - Free or Commercial
  - IPs, domains, hashes, TTPs ...
- Sync with other MISP instances
  - Sector specific
  - Government



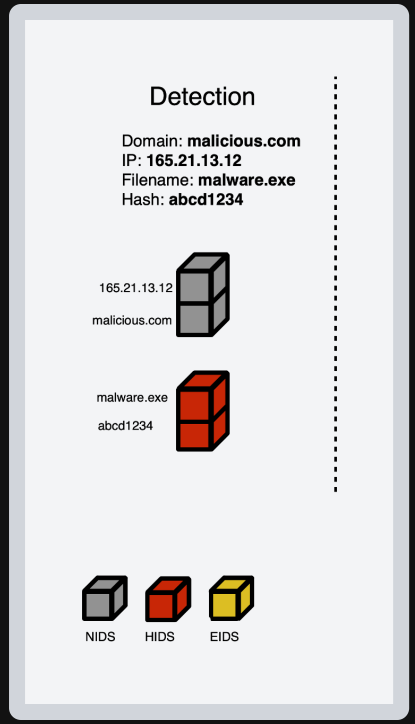
How does it work?

- Install and setup MISP
- Consume threat intelligence feeds
  - Free or Commercial
  - IPs, domains, hashes, TTPs ...
- Sync with other MISP instances
  - Sector specific
  - Government
- Consume & update IOCs
  - Enrich logs, push to SIEM, IDS, Firewalls



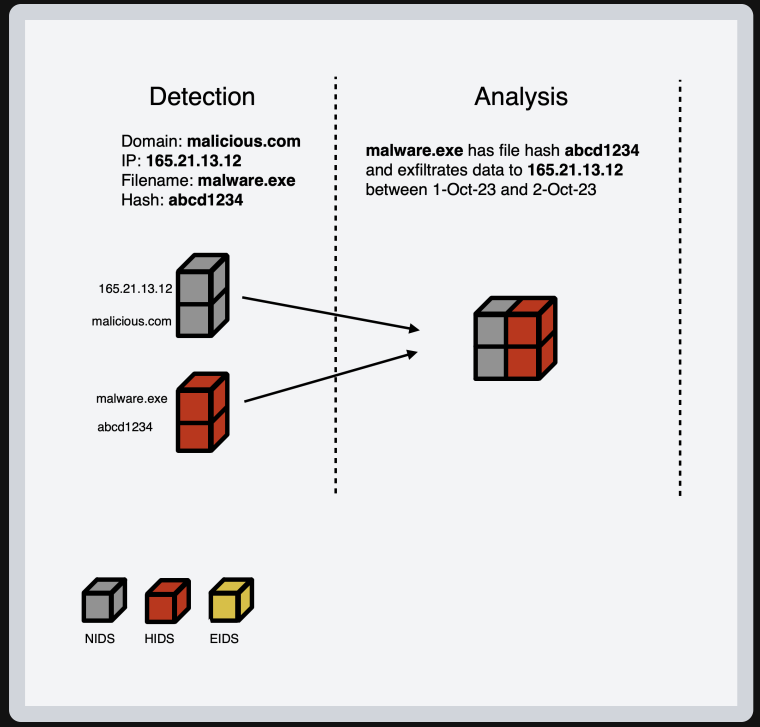
MISP

Malware Information Sharing Platform



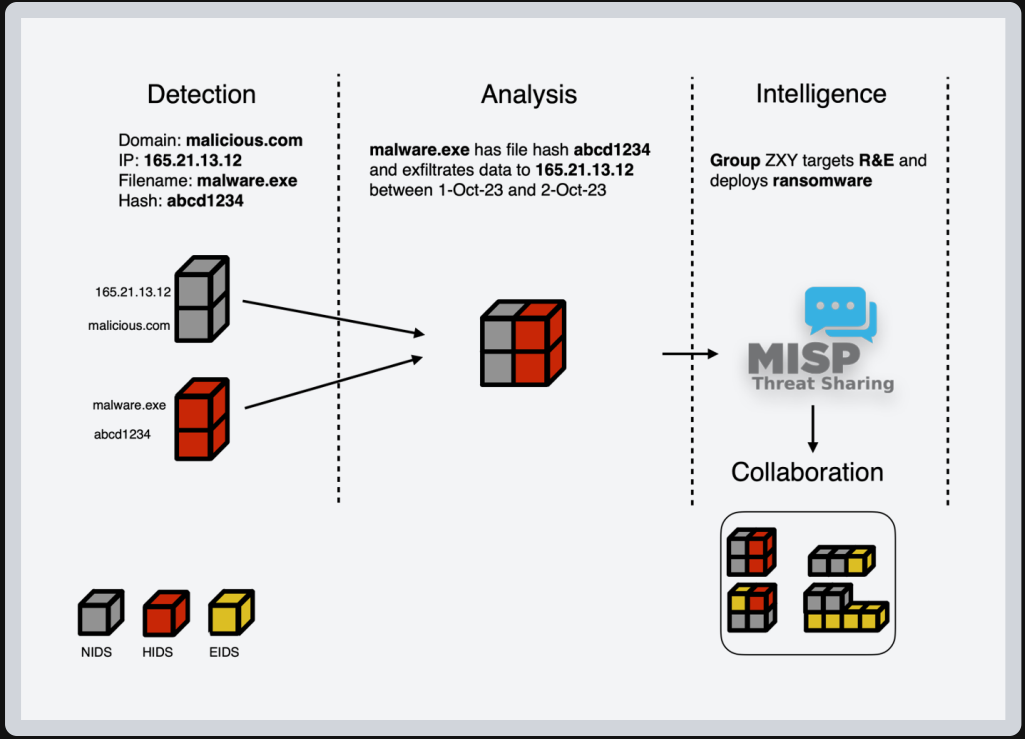
MISP

Malware Information Sharing Platform



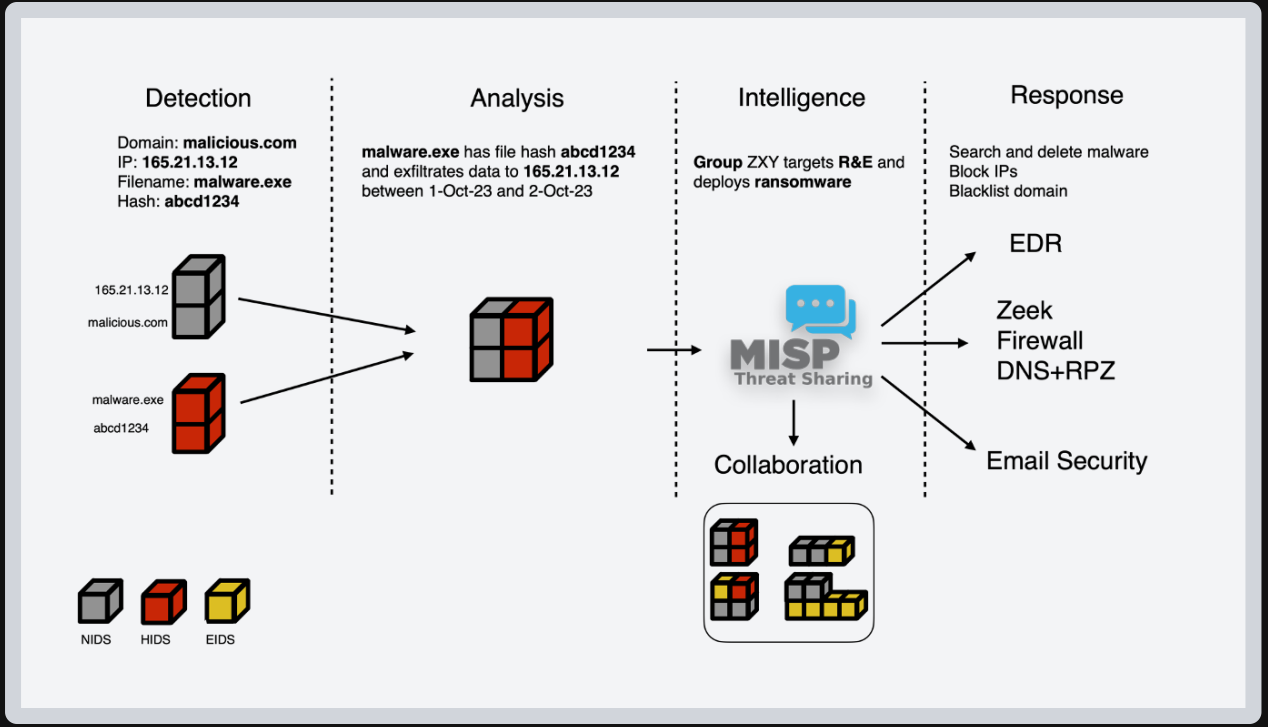
MISP

Malware Information Sharing Platform



MISP

Malware Information Sharing Platform



pDNSSOC

pDNSSOC Objectives

- Respond as a global community
- Introduce shared intelligence as a **core value**
- Immediate propagation of the intelligence across all network
- Respect confidentiallity (TLP)
- Respect **privacy** of users
  - Ensure GDPR compliance

Mature organizations can allocate resources for network monitoring and correlation

We aim to lower the entry barrier for small organizations enabling correlation with quality intelligence

pDNSSOC Overview

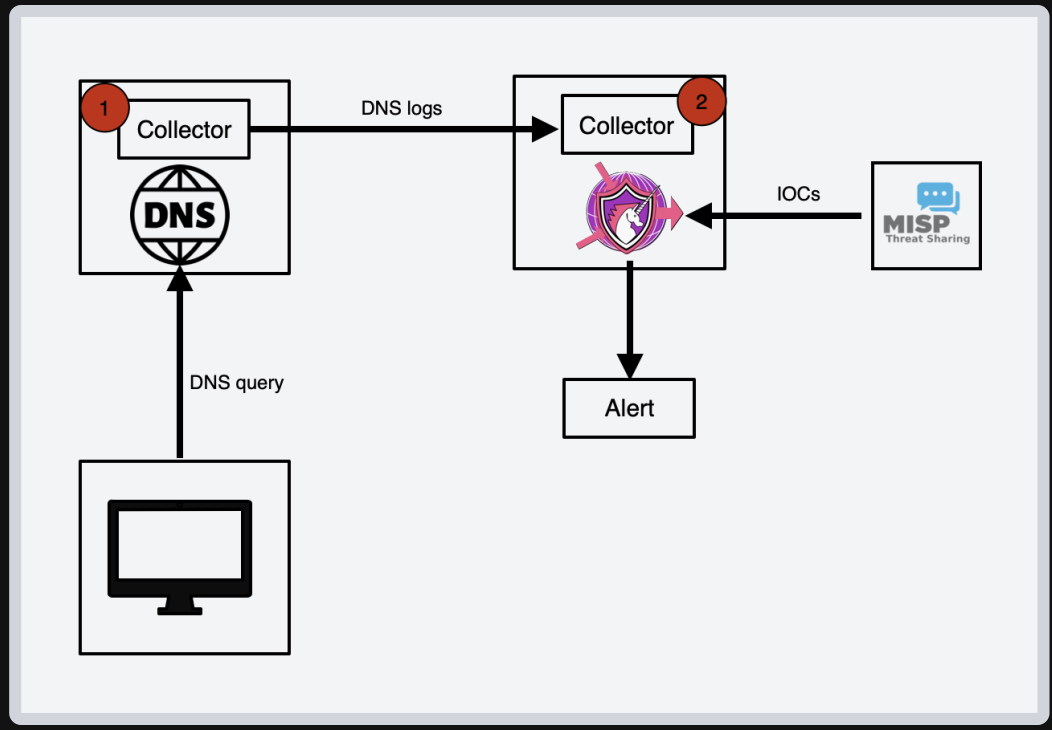
- **Minimizing** DNS Server interventions
- Straightforward configuration
- Little to no expertise required
- **No impact** on DNS Server performance

- Implementation tightly coupled with MISP Threat Sharing
- All components are Open source, backed by the community

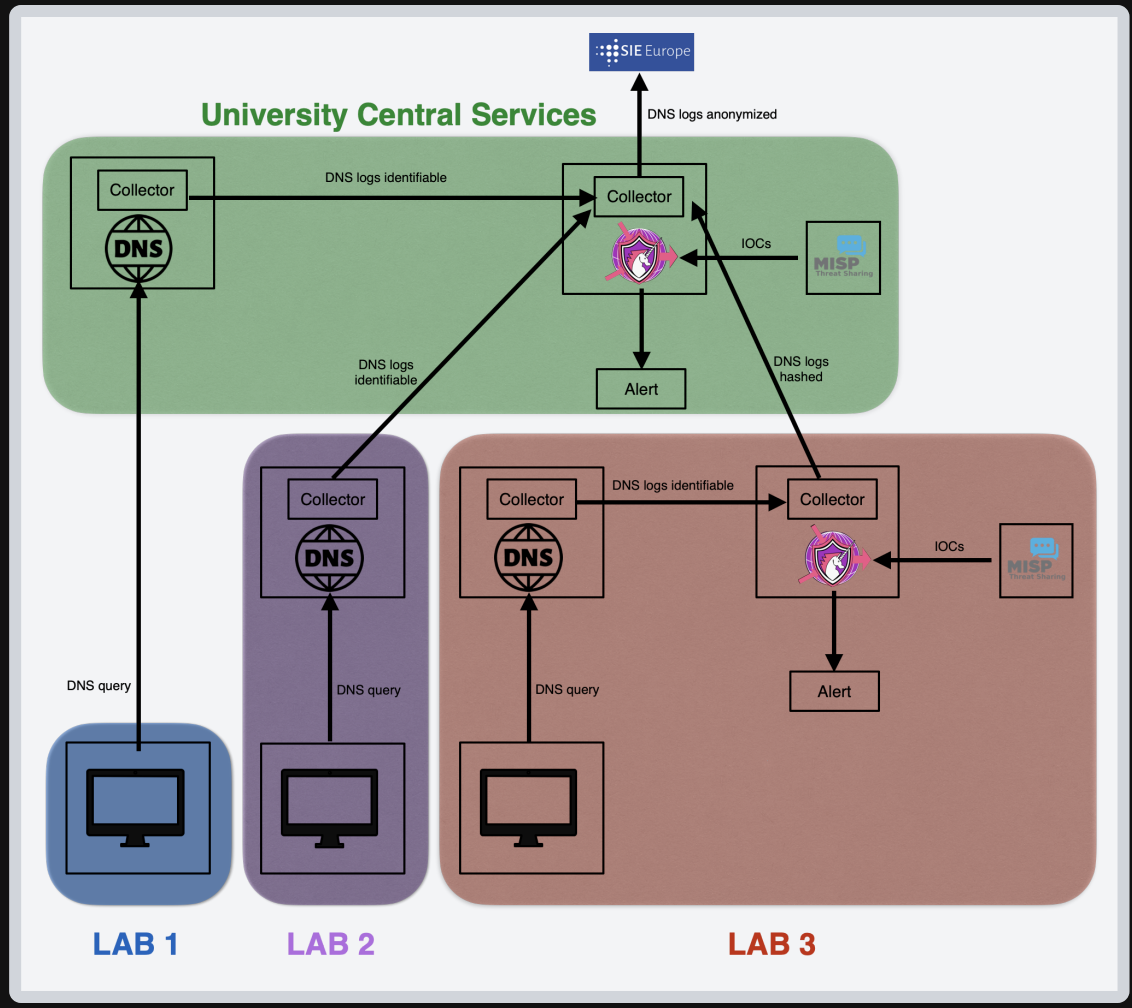
- Different levels of privacy, ensuring flexibility for collaborations

pDNSSOC

Overview

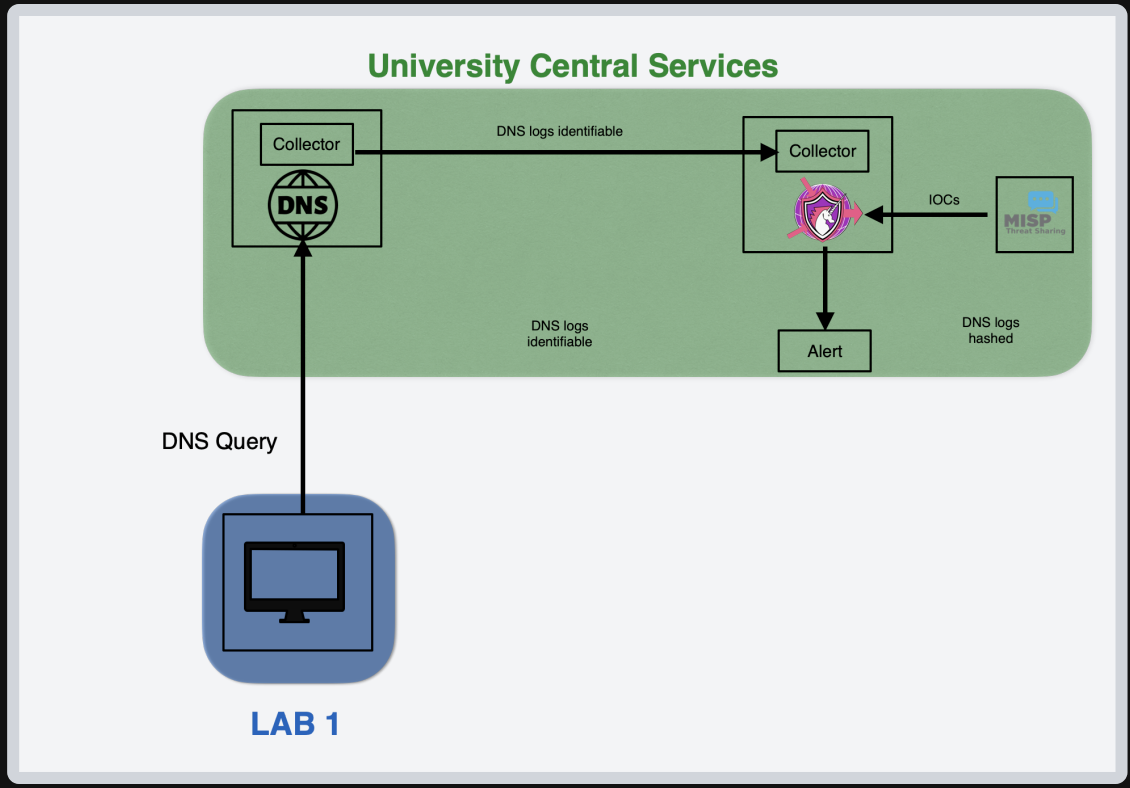


Deployment


SIE Europe
University Central Services
DNS logs anonymized
Collector
DNS logs identifiable
Collector
DNS
IOCs
MISP
Threat Sharing
DNS logs identifiable
Alert
DNS logs hashed
Collector
DNS
Collector
DNS logs identifiable
Collector
DNS
IOCs
MISP
Threat Sharing
DNS query
DNS query
DNS query
Alert
LAB 1
LAB 2
LAB 3

Case study

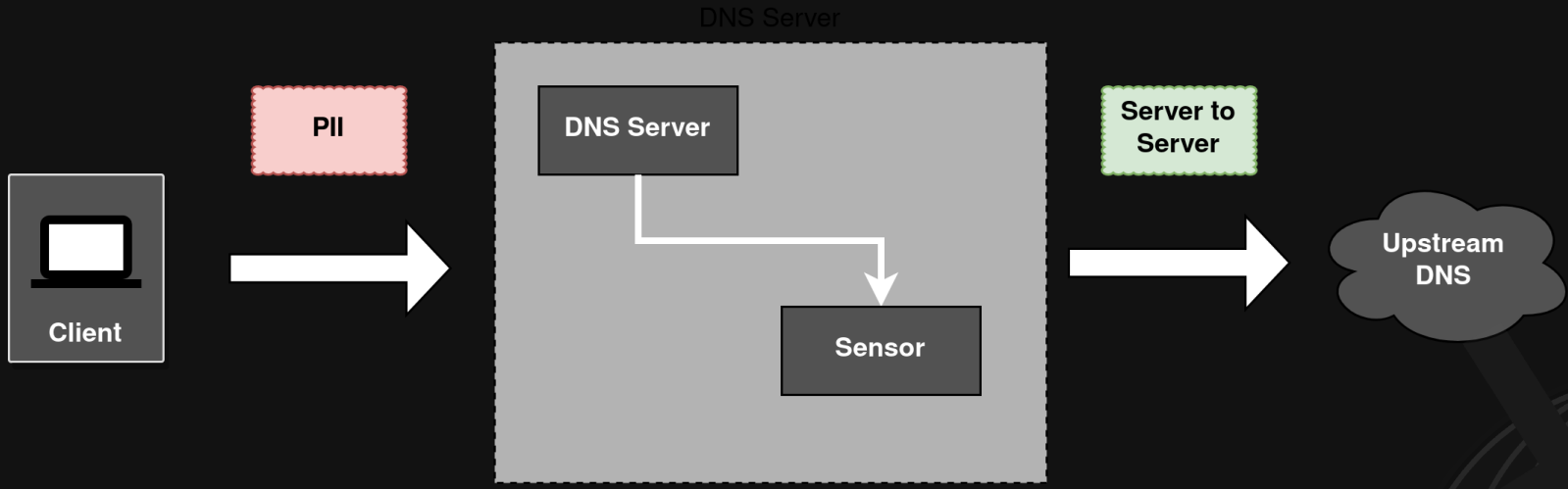
Ransomware group targetting R&E


University Central Services
Collector
DNS
DNS logs identifiable
Collector
IOCs
MISP
Threat Sharing
DNS logs
identifiable
Alert
DNS logs
hashed
DNS Query
LAB 1

Privacy

Privacy

Sensor positioning



Fetching only logs above the recursive ensures client privacy as only server to server communication is transmitted.

Privacy

Sensor positioning

DNSTAP

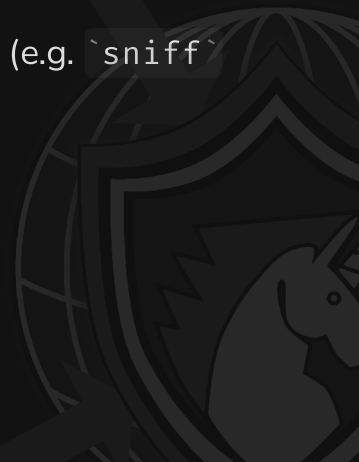
```
// dnstap config (BIND)
dnstap {
    resolver response;
};
...
```

- Suggested, when DNSTAP is available

Sensor

```
transforms:
  filtering:
    log-queries: false
    log-replies: true
    keep-queryip-file: "recursors.txt"
```

- Flexible, collector agnostic (e.g. `sniff` compatible)



Privacy

Masking client IP

Cases where no filtering can be applied or above the recursive filtering is not possible

```
{
    ...
    "query-ip": "188.184.*.*",
    ...
}
```

Mask part of the ip address

```
{
    ...
    "query-ip": "40307c253772c29ca7fb...",
    ...
}
```

Replace client ip by sensor id

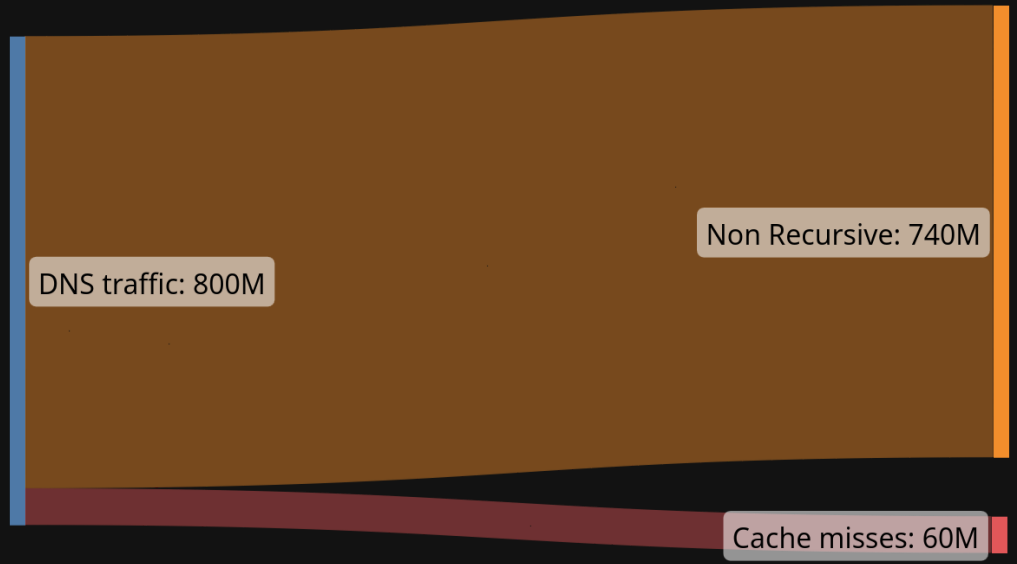
```
{
    ...
    "sensor_id": "aabda123afd74...",
    ...
}
```

Hash client ip

Fine-tuning

Fine-tuning

Data size



- Processing only above the recursive traffic (cache misses) results in significantly less data.
- At CERN, cache misses account for 5% of the total DNS traffic

`Fine-tuning`

False positives

- Enforce well known and trusted warninglists in MISP (e.g. List of public DNS servers, top 1000 websites, scanners)
- Make use of `` `to_ids` `` flag on all searches
- Define different timestamp filters per IOC taxonomy:

```
# pdnssoc-cli configuration
periods:
  generic: # Take into account only attributes that have been published for the past month
    delta:
      days: 30
  tags:
  - names:
      - "APT" # Fetch all APT tagged without time restrictions
    delta: False
```

Status & Future goals

Status & Future goals

CERN-CERT/pdnssoc

- Fully Open Source
- Currently in deployment for various organizations
- Collecting feedback and tailoring the implementation

Future

- Provide (opt-in) direct output to Passive DNS databases
- Build an active community around the tool, both for development and support

Thank You!