Plans for a pDNS based SOC deployment

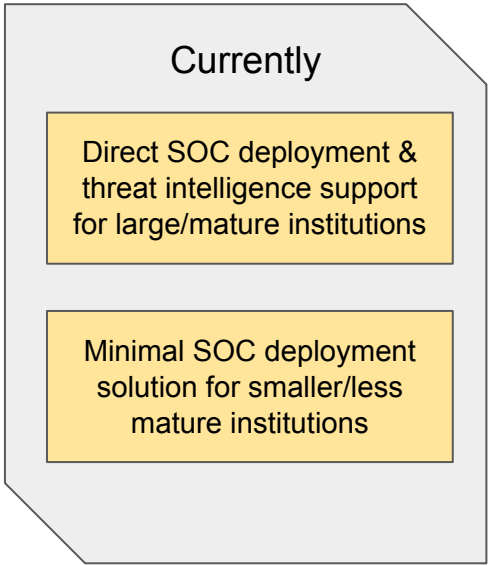
Christos Arvanitis

Motivation

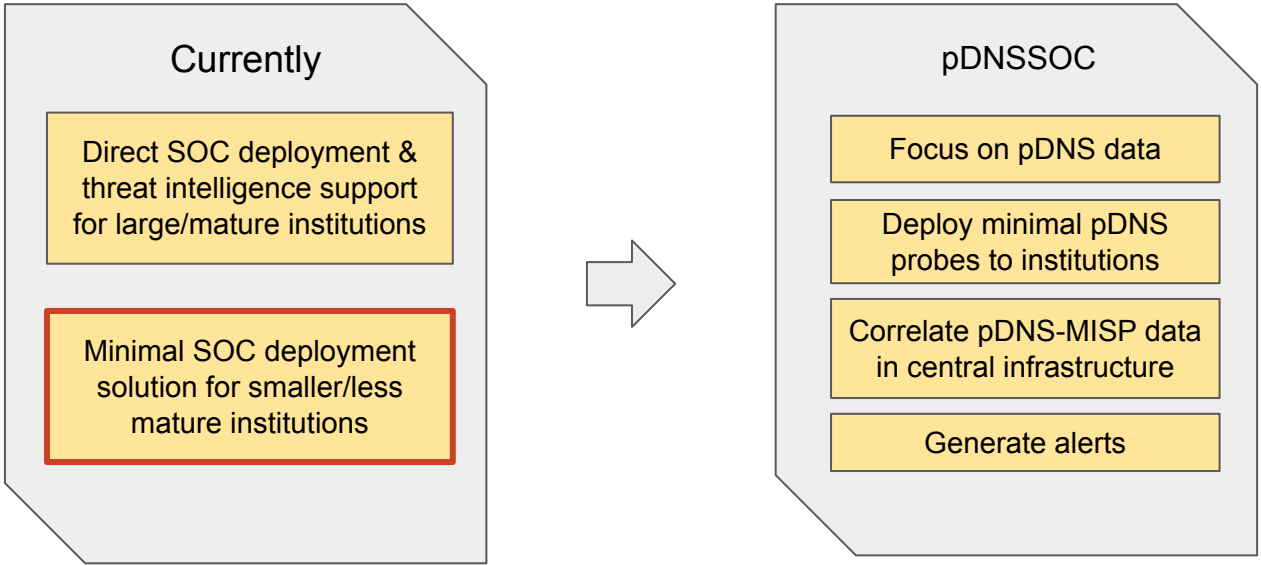
- Building a SOC is hard
  - Setting up a fully-fledged threat intelligence platform is extremely difficult for most sites
  - Network monitoring + threat intelligence infrastructure is an unrealistic scenario for many academic institutions
  - Only a very small fraction of WLCG sites have a production SOC

We have to lower the entry barrier

Current approach



Passive DNS(pDNS) based SOC

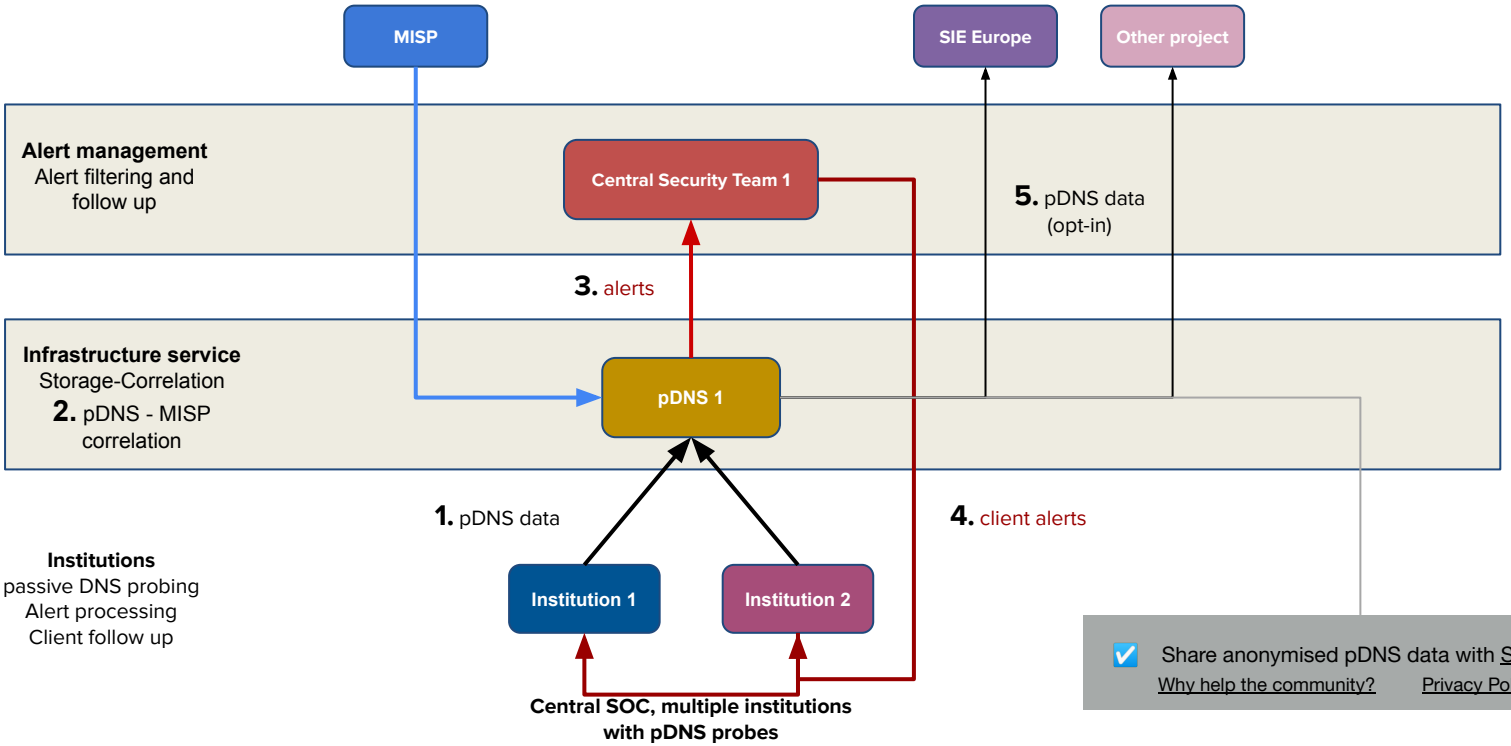


Passive DNS

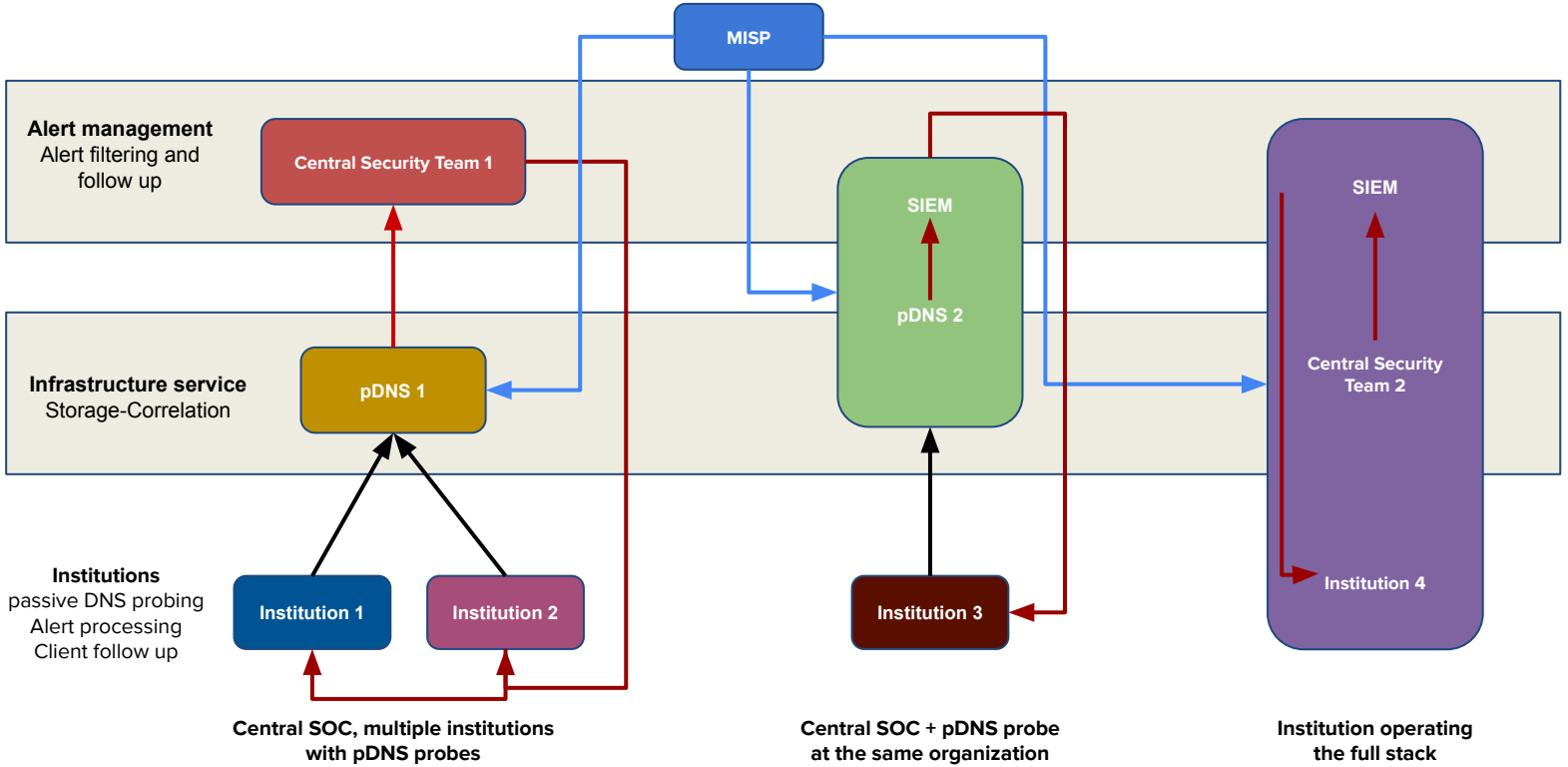
- What is passive DNS?
  - Historical DNS records originating from DNS server probes
  - Only DNS record - domain associations stored
  - DNS client information is stripped out, preserving privacy

- How can passive DNS data be useful?
  - Detect traffic to well-known malicious websites
  - Used in incident response lifecycle
  - Historical details beyond standard DNS

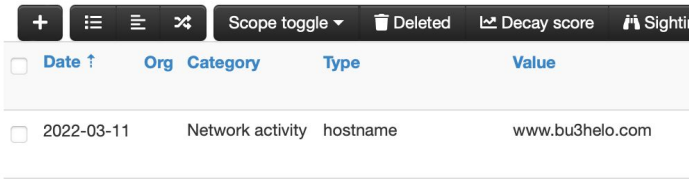
Deployment

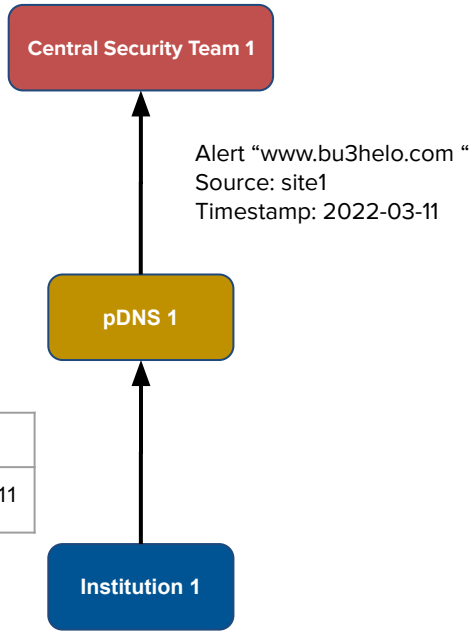

MISP
SIE Europe
Other project
Alert management
Alert filtering and follow up
Central Security Team 1
5. pDNS data (opt-in)
3. alerts
Infrastructure service
Storage-Correlation
2. pDNS - MISP correlation
pDNS 1
1. pDNS data
4. client alerts
Institutions
passive DNS probing
Alert processing
Client follow up
Institution 1
Institution 2
Central SOC, multiple institutions with pDNS probes
Share anonymised pDNS data with SIE Europe
Why help the community?
Privacy Policy

Deployment


MISP
Alert management
Alert filtering and follow up
Central Security Team 1
SIEM
pDNS 2
SIEM
Central Security Team 2
Infrastructure service
Storage-Correlation
pDNS 1
Institutions
passive DNS probing
Alert processing
Client follow up
Institution 1
Institution 2
Institution 3
Institution 4
Central SOC, multiple institutions with pDNS probes
Central SOC + pDNS probe at the same organization
Institution operating the full stack

pDNSSOC - Alerting





First Seen	Last Seen	TYPE	TTL	Query	Answer
2022-03-11	2022-03-12	A	60	www.bu3helo.com	71.51.115.11

Current state

- pDNS Sensor data ingestion design
- pDNS data - MISP threat intelligence correlation engine design
- Interface for searching queries

Next steps

- pDNS sensor packaging for a turn-key and lightweight solution
- Select sites for pilot pDNS sensor deployment
- Establishing a community around pDNSSOC
  - https://github.com/CERN-CERT/pDNSSOC

If you want to participate:

- Declare interest to deploy a pDNS sensor and send data at pdnssoc-contact@cern.ch