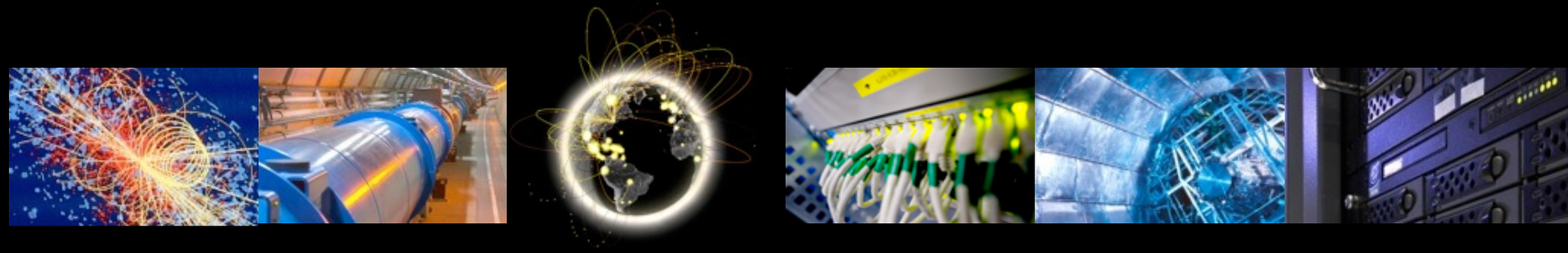
DNS-based SOC infrastructure for WLCG

Sep 2021



WLCG
Worldwide LHC Computing Grid

CERN

Threat intelligence strategy

- Empowering WLCG sites with SOC technologies (SOC WG)
  - Harvesting local system and network logs
  - Local data enrichment (when mature enough)
  - Threat intelligence sourcing (local sources, private feeds, and, WLCG MISP instance)
  - Correlation
  - Alerts on past events and new logs

- Making quality threat intelligence available to WLCG sites (CERN, SAFER)
  - Collected from trusted partner (governments, private sectors, trust circles)
  - Produced by WLCG security teams based on incident response

Challenges

- Building a SOC is hard
  - Leveraging threat intelligence proves extremely difficult for most sites
  - Only a very small fraction of WLCG sites have a production SOC

- Current plan: 2 levels of operations
  - Support large/mature sites directly to improve their capability
  - Provide other/smaller/less mature sites with a minimalist SOC design (still non-trivial)

DNS-based SOC

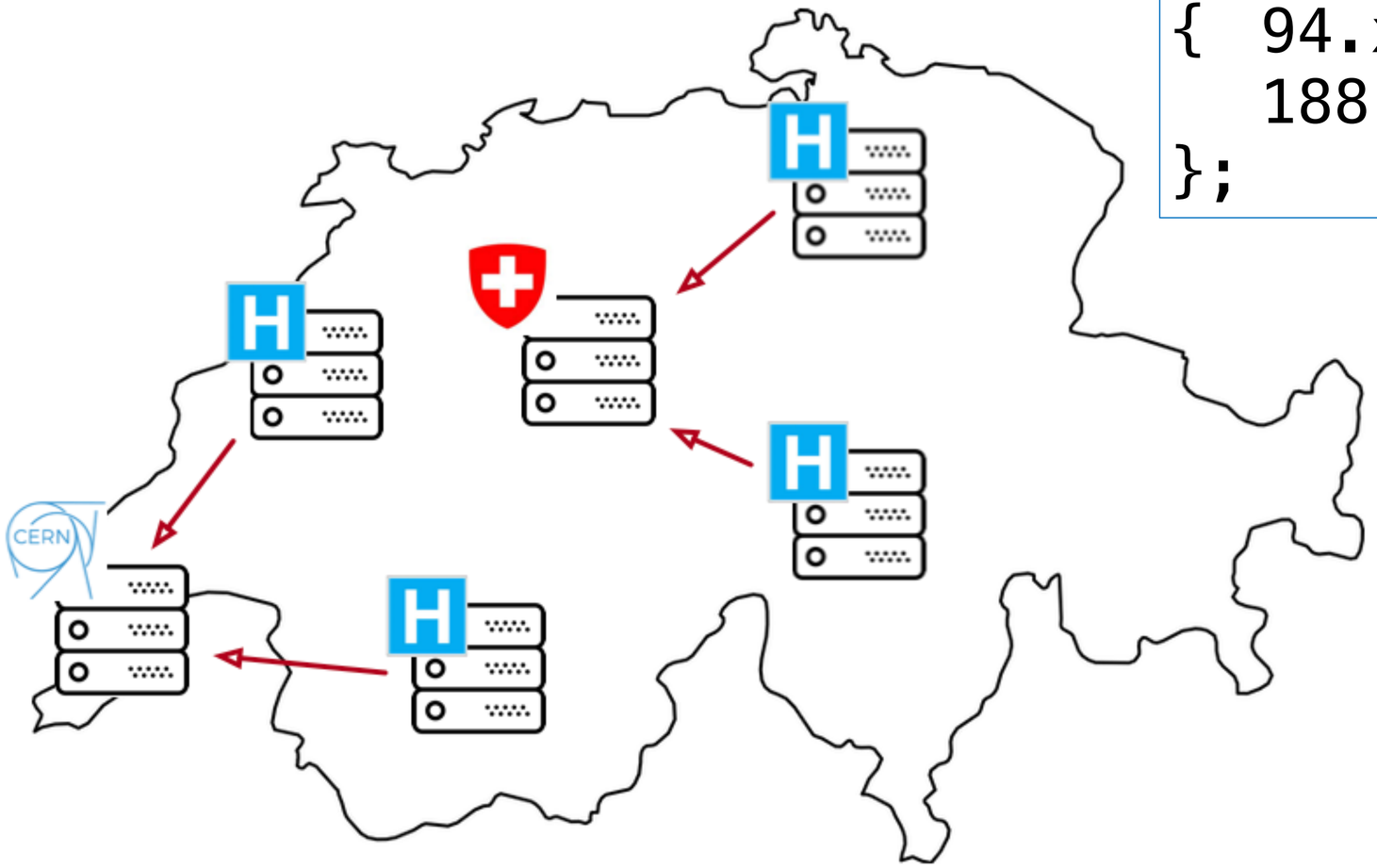
- An alternative or complementary approach could be to:
  - Central SOCs at a selected number of mature sites (1 per region?)
  - Use a subset of threat intelligence available and focus on DNS data
    - pDNS sent by sites to a central SOC for analysis
    - Rely on a network of regional DNS servers for analysis + blocking of malicious domains

- CERN has a successful model with the Swiss health sector during the pandemic
  - 1 DNS server at CERN, 1 at GovCERT: 50 health organisations covered

DNS to the Rescue!

- 17th March 2020: Team decides setting up a Secure DNS Resolver
- 18th March 2020 : Asking CERN if they would participate – They do!
- 20th March 2020 : First system is up and ready for testing
- 6th April 2020 : First health care organisation is protected
- 17th Sept 2021: 50 organisations are protected. There are about 3M queries / day and 5K – 10K Domains being blocked.

DNS to the Rescue!




```
forwarders
{  94.x.x.x;
   188.x.x.x;
};
```

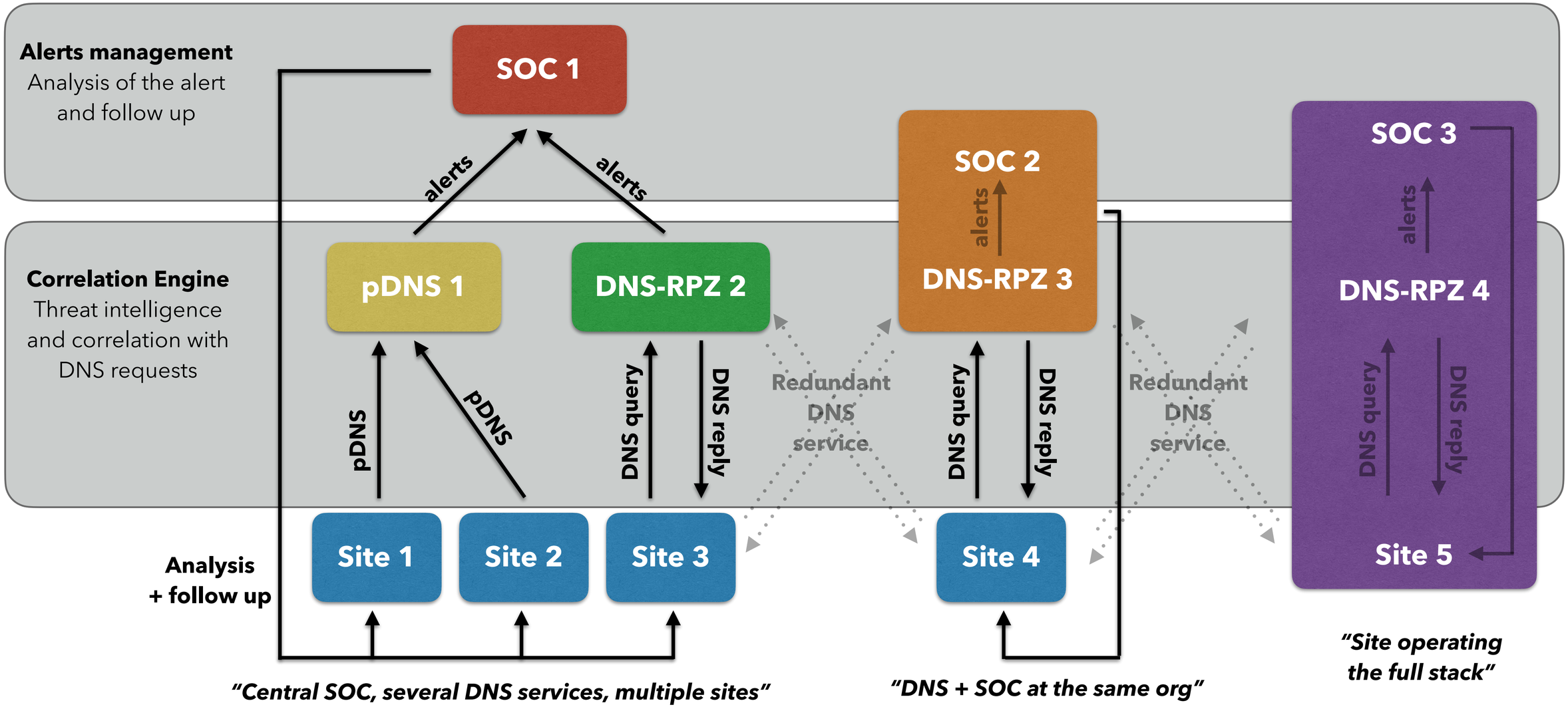
DNS-based SOC for WLCG

- WLCG could leverage the experience learned with the health sector
  - Start a small pilot service with a handful of sites
  - Two DNS-based offerings:
    - **pDNS**: passive DNS data sent by sites to a SOC for analysis (replaying pDNS files daily)
    - **RPZ+DNS**: Rely on a network (for reliability) of regional DNS servers:
      - For blocking well-known malicious domains based on available RPZ feeds
      - For alerting based on correlation of DNS data with threat intelligence (MISP)

- Two services components (can be at different locations):
  - **Infrastructure service**: operates the containers/VMs running the DNS services (pDNS or RPZ+DNS)
  - **SOC service**: local (site itself), regional (NGI) or central (EGI/WLCG) analysis and managements of alerts

DNS-based SOC for WLCG

- Multiple deployment models and integration levels (one organisation per colour)



Next steps

- Containerising infrastructure services
  - Produce a container to automatically deploy
    - **pDNS service:**
      - Collect domain/IP threat intelligence data from the WLCG MISP instance
      - Receive (SCP) pDNS data daily
      - Replay the pDNS data and correlate it with indicators
      - Send resulting alerts to a SOC (local or remote)
    - **RPZ+DNS**
      - Receive and reply to DNS requests
      - Block well-known malicious domains based on available RPZ feeds
      - Collect domain/IP threat intelligence data from the WLCG MISP instance
      - Correlate incoming DNS queries it with indicators
      - Send resulting alerts to a SOC (local or remote)
  - Identify teams/sites to operate the SOC (receive, analyse alerts, contact victim(s))
  - Identify sites for a pilot service