WLCG Operational Security

Romain Wartel
David Crooks
Liviu Vâlsan
Christos Arvanitis

Overview

- Introduction
- SOC WG update
- Full SOC workflow
- Plans for a pDNS based SOC deployment
- The SAFER operational security trust group

Introduction

Romain Wartel

WLCG security strategy

1. Place threat intelligence sharing at the core of daily security operations
   - Share specific threat intelligence (bad IP addresses, file hashes, etc.) in real time within the community
   - Produce relevant/target threat intelligence for WLCG
   - Enable the sites to leverage and make use of the threat intelligence

2. Improve WLCG's incident response capabilities
   - Attacks are global, and so must be the response
   - Bridge the cooperation gaps:
     - Lack of cooperation between "campus" and "grid" or "scientific" security teams
     - Lack of global coordination on global attacks within the research & education community
   - Consolidate traceability and incident response policies for clouds / federated identities

WLCG security plans for next 5 years

- **Security infrastructure**
  - Goal: Empower WLCG sites to make use of threat intelligence
  - Lead an open "Security Operation Center WG" (SOC) scoped at the whole R&E community
    - Get the relevant tools operational at the sites
      - Custom solution for large/mature sites to build + operate a security operation center
      - Turn-key VMs/containers for less experienced sites
    - https://wlcg-soc-wg.web.cern.ch

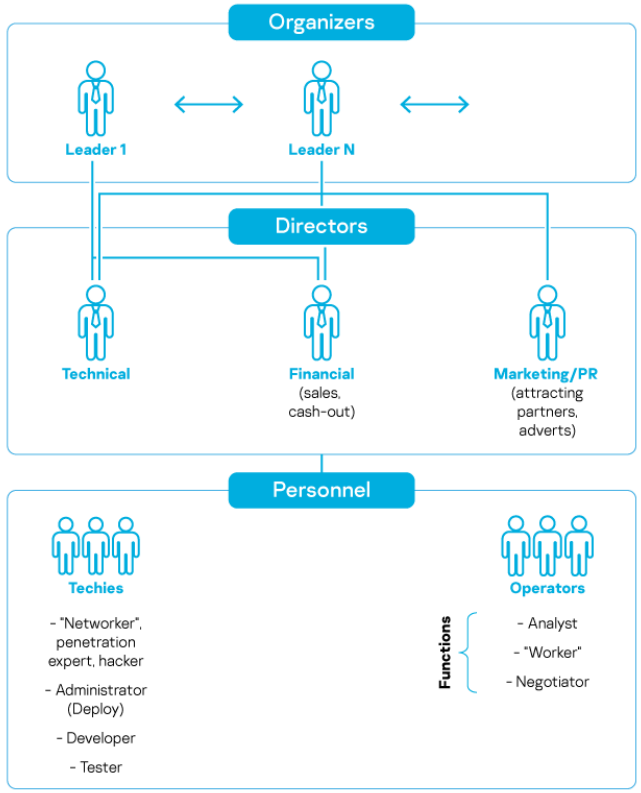
- **Global incident response trust group**
  - Ad-hoc / improvised is insufficient. No guaranteed response. Not sustainable
  - Highly vetted, closed trust group for daily security operations with US/EU/APAC reps
  - Incident response, actual threat intelligence sharing
  - Support security operations where needed to protect WLCG (astrophysics, HPC, etc.)
  - Reinforce EU-US cooperation (WLCG sites)

SOC WG Update

David Crooks

Landscape

- The world has changed
- In the past, biggest risk for academic security
  - Relatively simple, untargeted attacks
    - Belief that research computing was major risk
- This is no longer the case
  - Determined, well-resourced attackers
    - 9-5 jobs working on malware services
  - Phishing and identity theft are major risk
    - Research computing security can be major asset
- Big business: we are targets



kaspersky

https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

Landscape

- Over last year seen very high profile attacks
  - Particularly ransomware
  - Many in the press
- For an organisation an attack can be **catastrophic**
  - Months of complete organisational shutdown

- It is **essential** that we work together to defend our community

WLCG Security

- Active use of threat intelligence is a cornerstone of the WLCG Security strategy for the next 5 years

- This requires parallel activity in several related areas
  - Source of threat intelligence
  - Technical collaboration
  - High-level coordination (work with other initiatives)
  - Global operational security

Complete set of initiatives

- Source of threat intelligence available to entire sector
  - **Central R&E MISP instance** (hosted at CERN)
- Technical collaboration
  - **SOC WG**
- High level coordination
  - **WISE IR-TI**
- Global operational security
  - **EGI CSIRT, OSG Security, SAFER**

Recent SOC WG progress

- Continued development of Nikhef SOC
  - In operation
  - Operational hardware updates
  - Alerting is next focus

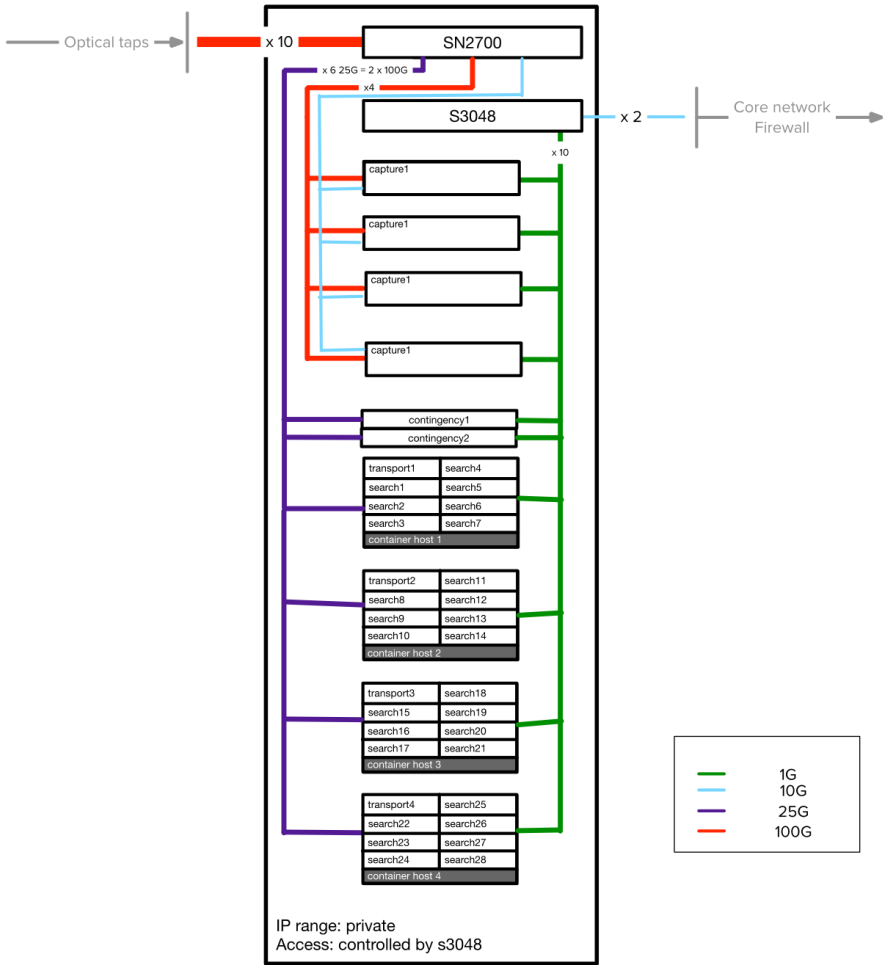
- AGLT2 update at HEPiX
  - Initial deployment and testing of new network capture nodes

Recent SOC WG progress

- EGI CSIRT building MISP into IR procedures
  - Important step in integration into our current procedures
    - Driver for adoption of threat intelligence sharing
  - See later this session
- Early stages of Kubernetes-based SOC
  - Training, demonstration and small site deployments
  - Broader context of cloud-based sites
  - Laying foundations for long term development
- STFC SOC project

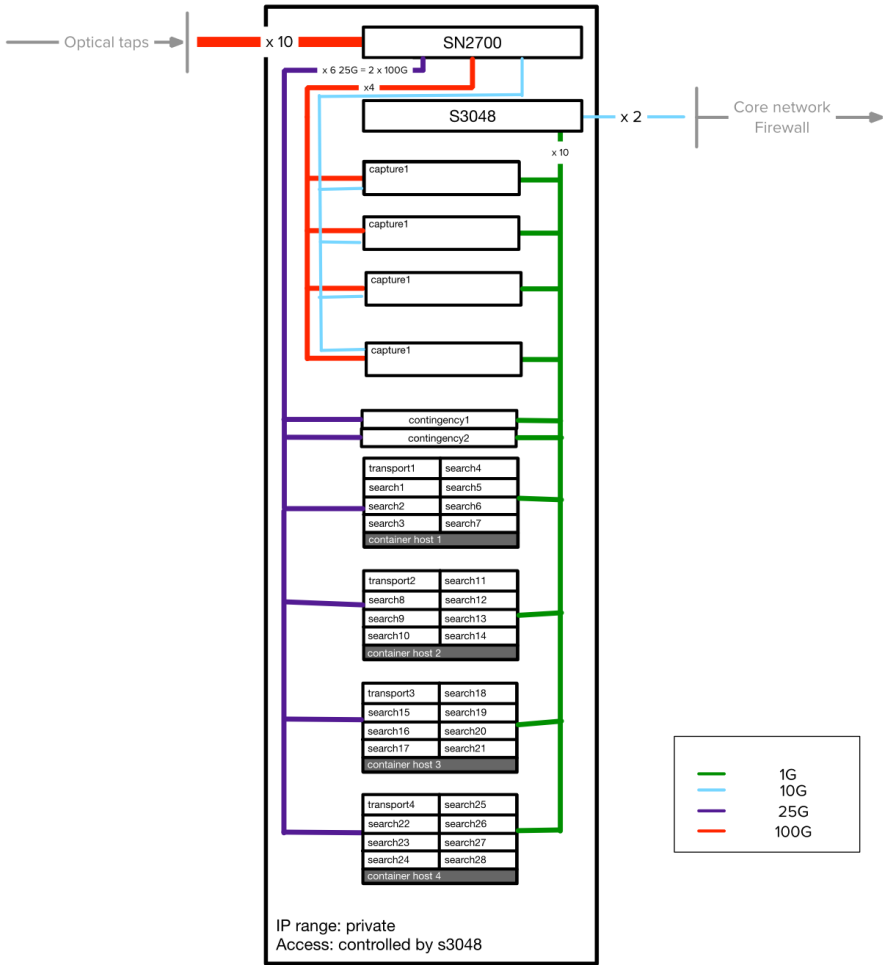
STFC SOC Project

- Monitor all STFC-RAL traffic and correlate it with threat intelligence
  - R&E MISP instance
- Monitoring will include
  - 2x100Gb/s Janet and
  - 1x100Gb/s LHCOPN links
- Couple to existing STFC procedures
- Following initial pilot phase, natural progression to other STFC sites
  - Design in discussion



STFC SOC Project

- Drive deployment of these capabilities across connected UK organisations
  - GridPP
  - IRIS infrastructure
    - STFC supported science
    - GridPP, HPC and Cloud providers
- Build capital proposal for funding calls



Future plans

- Plan deployment of SOC capabilities at GridPP and IRIS organisations
  - In partnership with Jisc
  - Target both technical and management levels
  - Build concrete capital proposal(s)

- Continue building WLCG Tier1 intelligence network
  - Renewed goal to give access to threat intelligence to all T1s
  - Contact all T1s to identify key contact

SOC WG next steps

- Seek participation in SOC working group
  - Aim for next WG meeting in new year
- Help to steer direction of working group
  - Community led with specific goals for different infrastructures (inc WLCG)
- After work earlier this year, identify work strands for 2022
  - New deployments
  - Experienced deployments developing use of threat intelligence
  - Dockerised deployments for small installs/training/demonstrations
  - High bandwidth networks (>=100G)

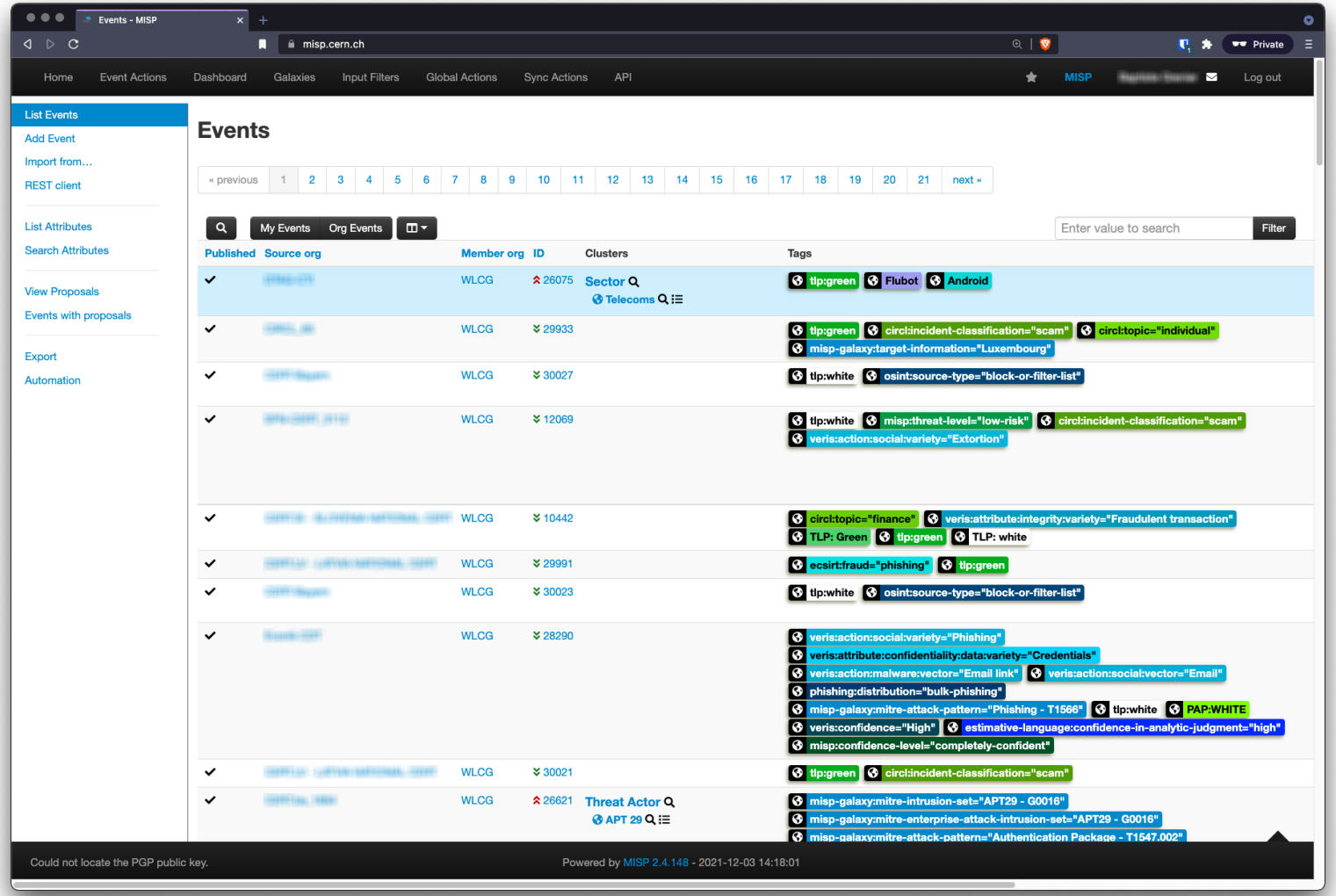

egi
CSIRT
WISE
COMMUNITY
WLCG
Worldwide LHC Computing Grid

Questions ?

Full SOC Workflow

Liviu Vâlsan

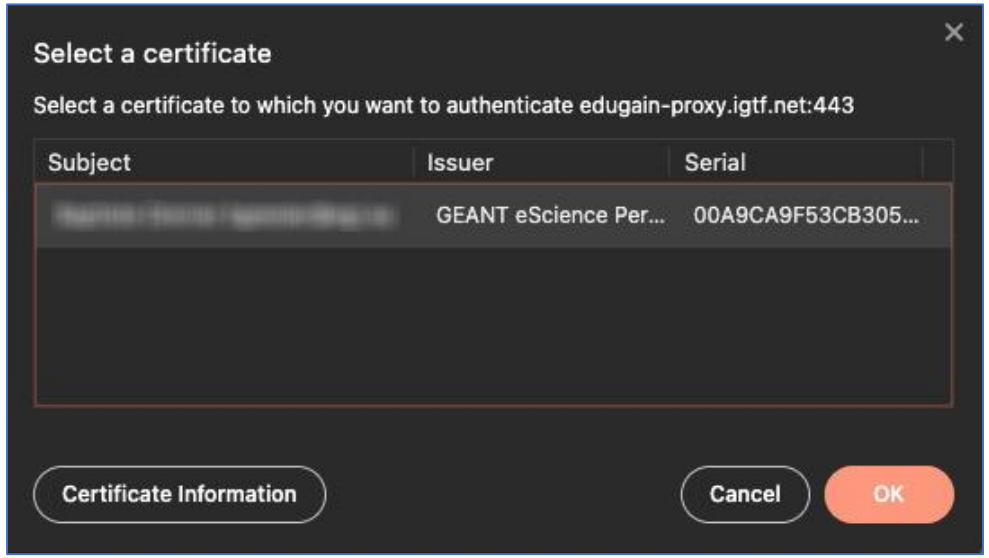
MISP Threat Intelligence



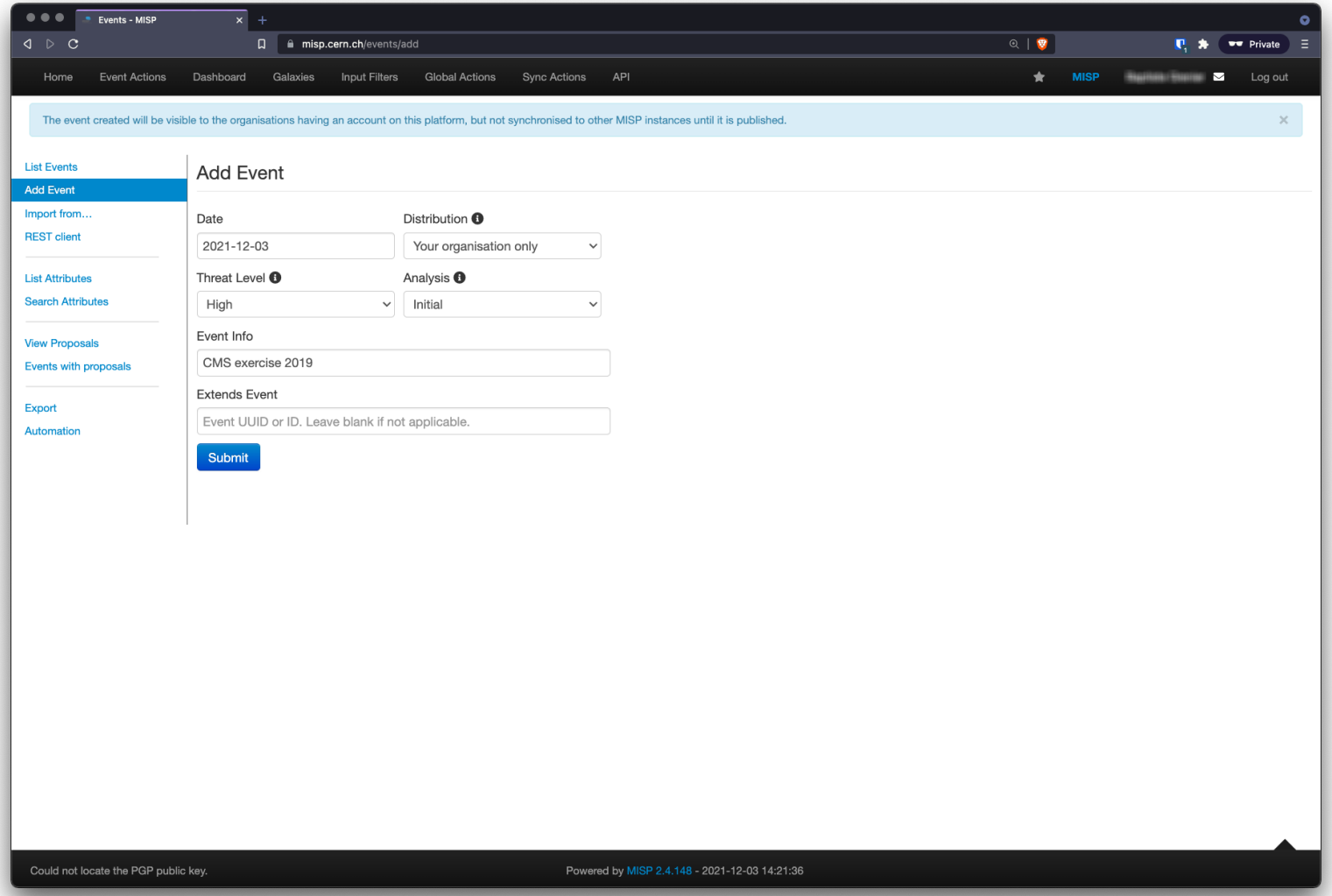
- Starting point is the WLCG MISP
- Threat intelligence platform providing access to Indicators of Compromise (IoCs)
- IoCs are contextualised and actionable

Access

- Access to the central instance behind the CERN SSO
- Federated identities supported
- Requires the IdP to assert SIRTFI
- IGTF proxy available

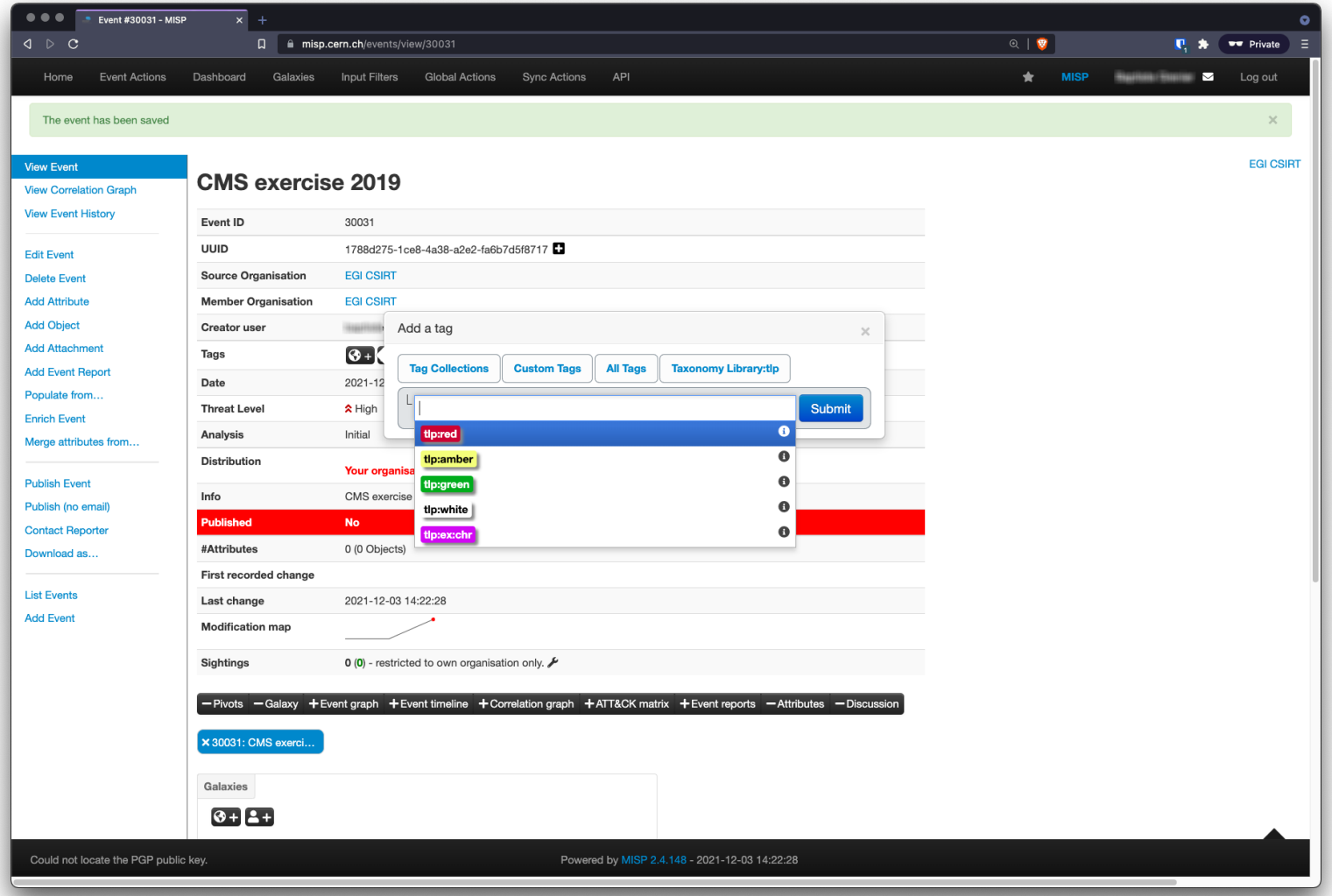


Creating a test MISP event



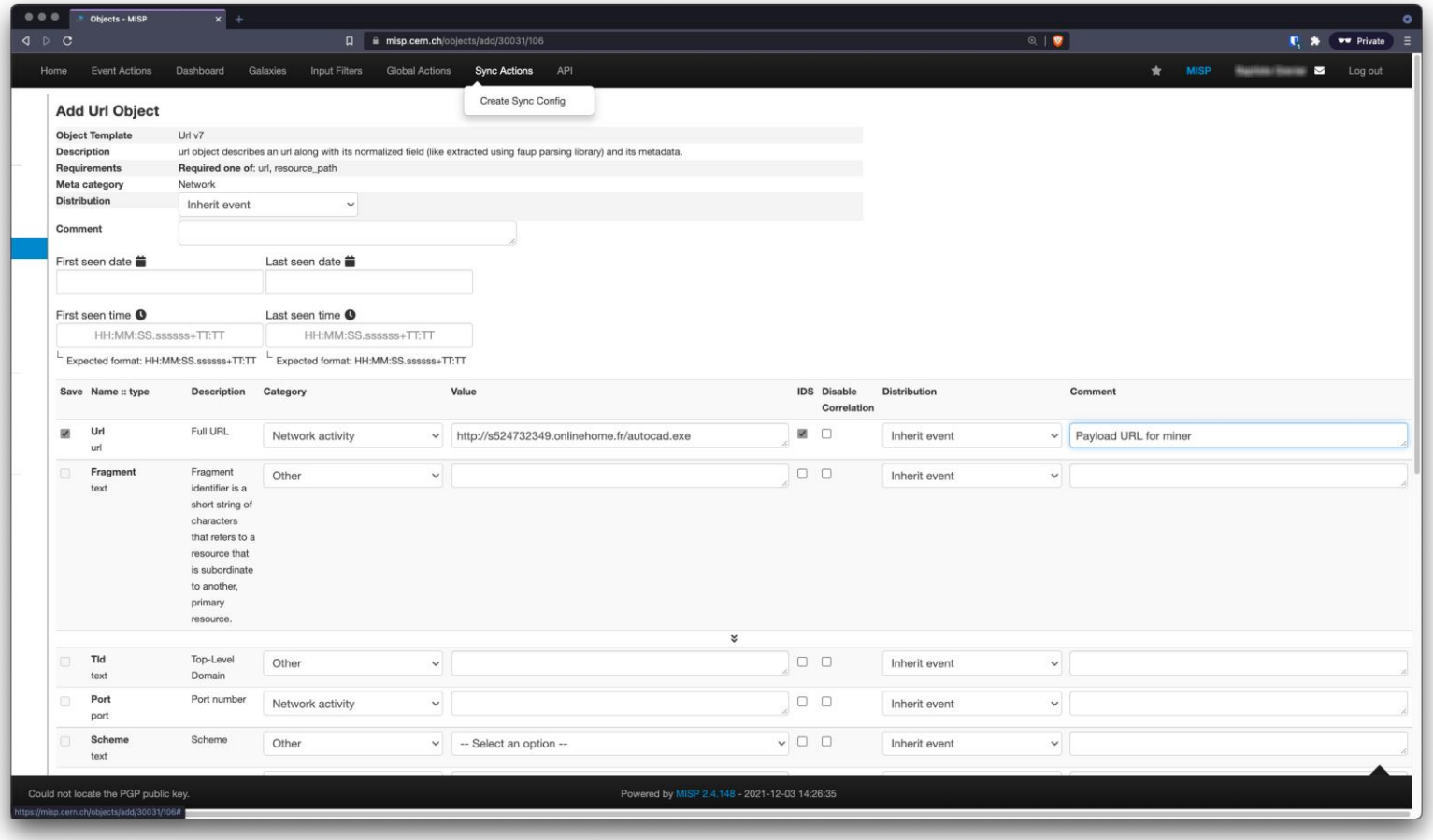
- Defining MISP event metadata including:
  - Description
  - Distribution
  - Threat level

Tagging



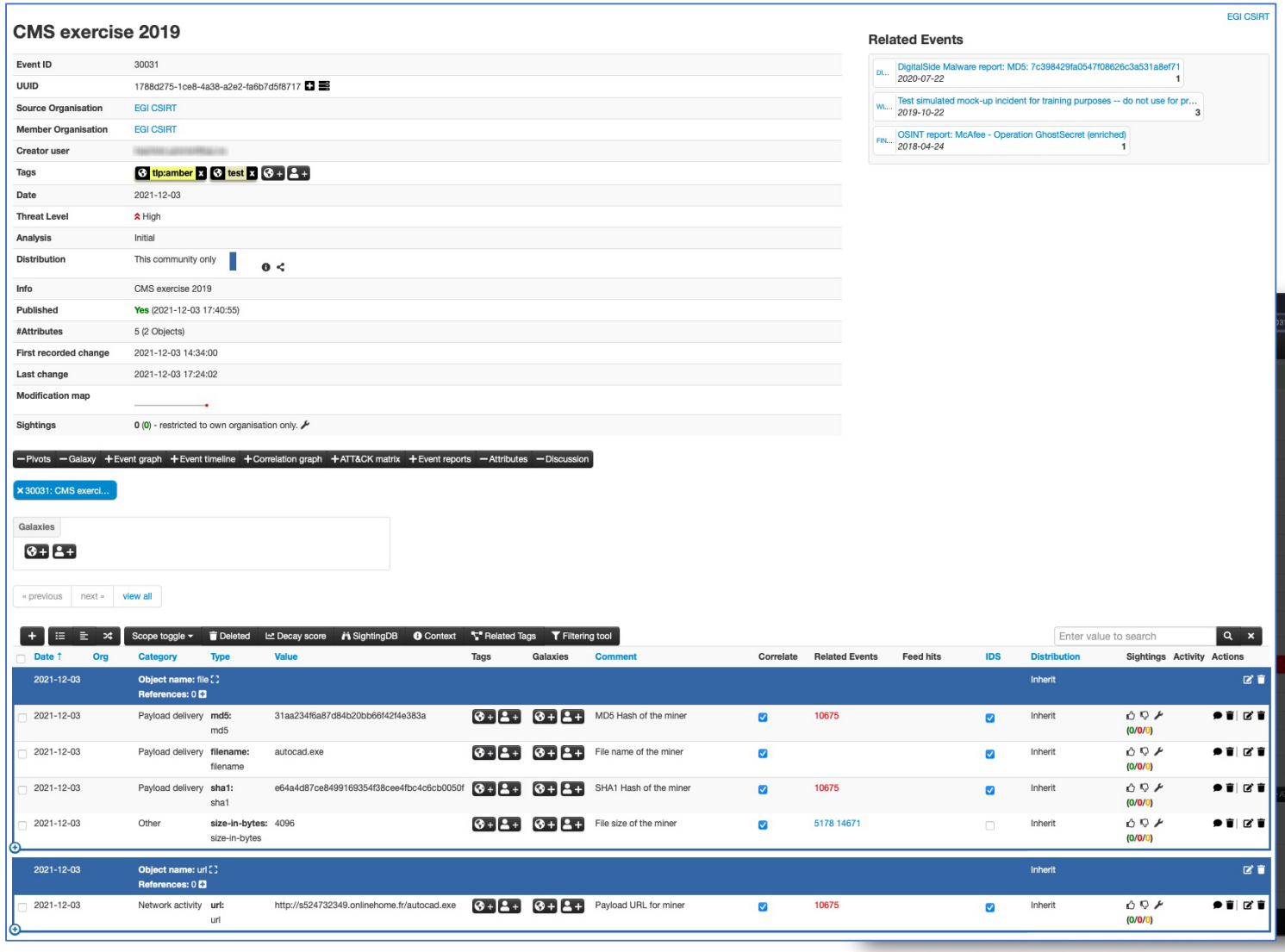
- MISP comes with support for a plethora of different taxonomies
- At least TLP tagging is highly recommended

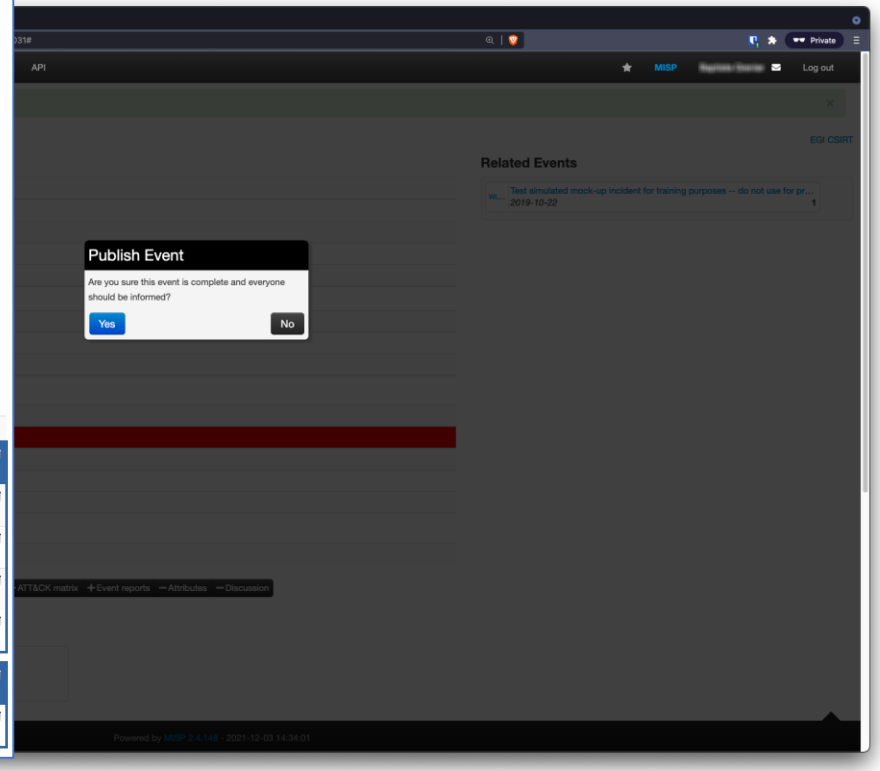
Adding IoCs



- IoCs can be added as stand alone attributes
- Or as objects (set of related attributes)
- IoC data:
  - Value
  - Type
  - Category
  - IDS use
  - Comment

Once ready publish the event





Alerting

[EGI CSIRT] CMS exercise 2019 [d7746a6d]
To: Liviu Valsan,
Reply-To: Liviu Valsan

Summary

MISP event	CERN devices	IoCs detected	Total # of IoCs	Publication	Organisation	Tags
CMS exercise 2019	rwlx1	http://s524732349.onlinehome.fr/autocad.exe Remove from IDS	1	2021-12-03	EGI CSIRT	tlp:amber test

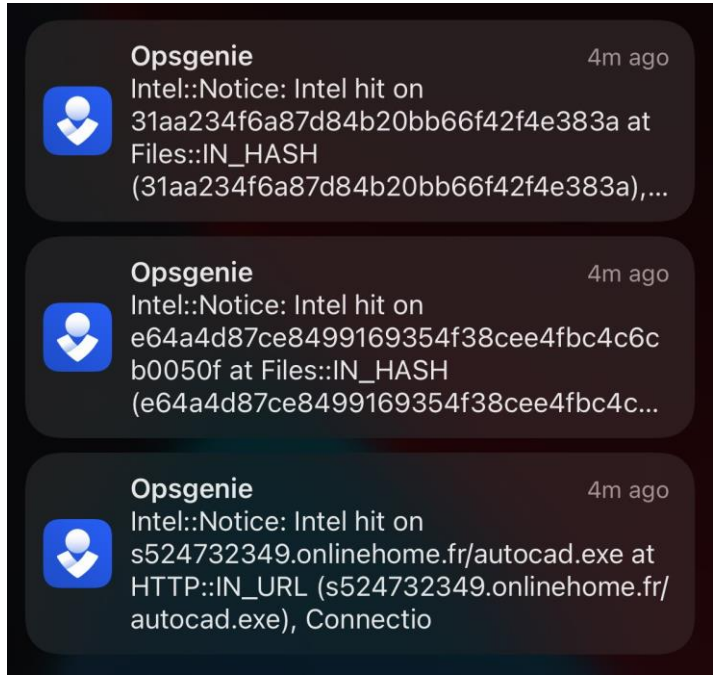
Basic connection details

Time	IoC triggering alert	IoC date	IoC comment	Source	Source host	Source country	Source organisation	Destination	Destination host	Destination country	Destination organisation	Protocol	Other actions
2021-12-03 14:45:36	http://s524732349.onlinehome.fr/autocad.exe	2021-12-03 14:34:00	Payload URL for miner	188.185.125.210:40752 rwlx1	rwlx1.cern.ch	CH	CERN	217.160.0.113:80 IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE	217-160-0-113.elastic-ssl.ui-r.com	DE	1&1 Internet AG	http	
2021-12-03 14:46:35	http://s524732349.onlinehome.fr/autocad.exe	2021-12-03 14:34:00	Payload URL for miner	188.185.125.210:40750 rwlx1	rwlx1.cern.ch	CH	CERN	217.160.0.113:80 IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE	217-160-0-113.elastic-ssl.ui-r.com	DE	1&1 Internet AG	http	

bro_http additional details

Time	Source	Destination	Host	URI	Referrer	Method	Status code	Status message	Resp body len	Other actions
2021-12-03 14:46:56	188.185.125.210:40752	217.160.0.113:80	s524732349.onlinehome.fr	/autocad.exe		GET	200	OK	4096	Search VirusTotal
2021-12-03 14:46:35	188.185.125.210:40750	217.160.0.113:80	s524732349.onlinehome.fr	/autocad.exe		GET	200	OK	4096	Search VirusTotal

CERN



STFC


egi
CSIRT
WISE
COMMUNITY
WLCG
Worldwide LHC Computing Grid

Questions ?

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
  - Deploying network monitoring + threat intelligence infrastructure is an unrealistic scenario for many sites
  - Only a very small fraction of WLCG sites have a production SOC

We have to lower the entry barrier

Motivation

- Current state
  - Direct support to large/mature sites to setup SOC platforms and improve threat intelligence capabilities
  - Provide other/smaller/less mature sites with a minimalist SOC design (still non-trivial)

pDNS SOC

Alternative approach

- Host central SOCs at a selected number of mature sites
- Ingest passive DNS data focusing on a great subset of threat intelligence
  - Deploy passive DNS (pDNS) probes to sites collecting data
  - Correlate pDNS data with threat intelligence (MISP)
  - Generate alerts sent to central security teams for handling
  - Rely on a network of regional DNS servers (RPZ+DNS) for blocking of malicious domains
  - pDNS becomes critical for a DNS based SOC

pDNS SOC

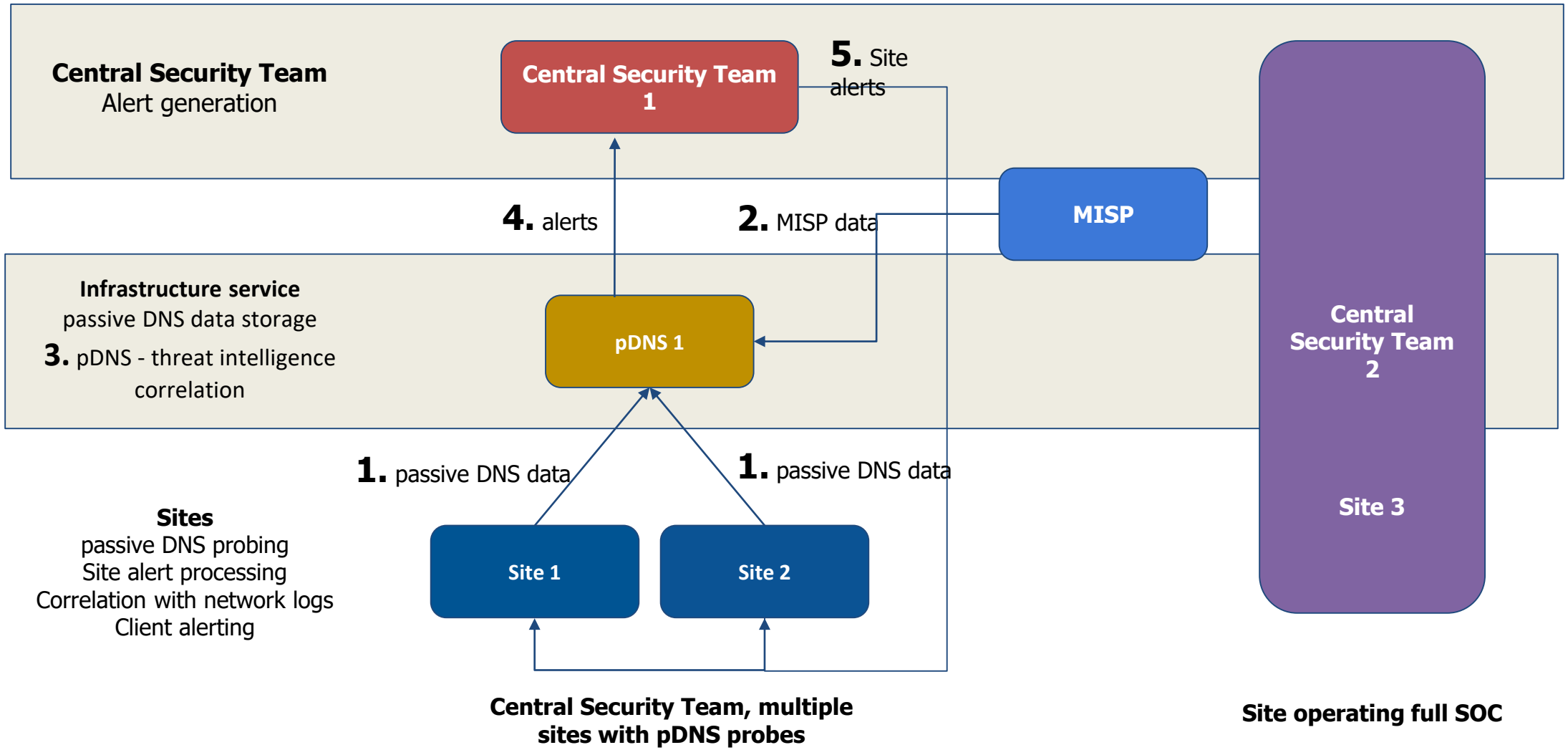
- CERN has a successful RPZ+DNS model with the Swiss health sector during the pandemic
  - 1 DNS server at CERN, 1 at GovCERT: 50 health organisations covered
  - ≈ 3M queries/day
  - 5K – 10K blocked domains

Passive DNS

- What is passive DNS?
  - A database of full historical DNS records originating from DNS server probes
  - Only DNS record - domain associations stored
  - Clients making DNS queries are stripped out, preserving privacy

- How can passive DNS data be useful?
  - Detect traffic to well-known malicious websites
  - Used in incident response lifecycle
  - Answer questions impossible to answer using standard DNS
    - Which IPs were associated with a domain name over time?
    - What domain names are hosted by a given nameserver?
    - What domain names point into a given IP network?

pDNS SOC


Central Security Team
Alert generation
Central Security Team 1
5. Site alerts
MISP
4. alerts
2. MISP data
Infrastructure service
passive DNS data storage
3. pDNS - threat intelligence correlation
pDNS 1
Central Security Team 2
Site 3
1. passive DNS data
1. passive DNS data
Sites
passive DNS probing
Site alert processing
Correlation with network logs
Client alerting
Site 1
Site 2
Central Security Team, multiple sites with pDNS probes
Site operating full SOC

Current state

- Evaluation of existing solutions for passive DNS sensors
- Design of passive DNS data with threat intelligence correlation solution (in collaboration with GovCERT)

Next steps

- pDNS packaging for a turn-key and lightweight solution
- PoC in Q1 2022
- Testing
- Select teams/sites to operate central SOC instances (alerting)
- Select sites for pilot pDNS sensor deployment
- Open sourcing


egi
CSIRT
WISE
COMMUNITY
WLCG
Worldwide LHC Computing Grid

Questions ?

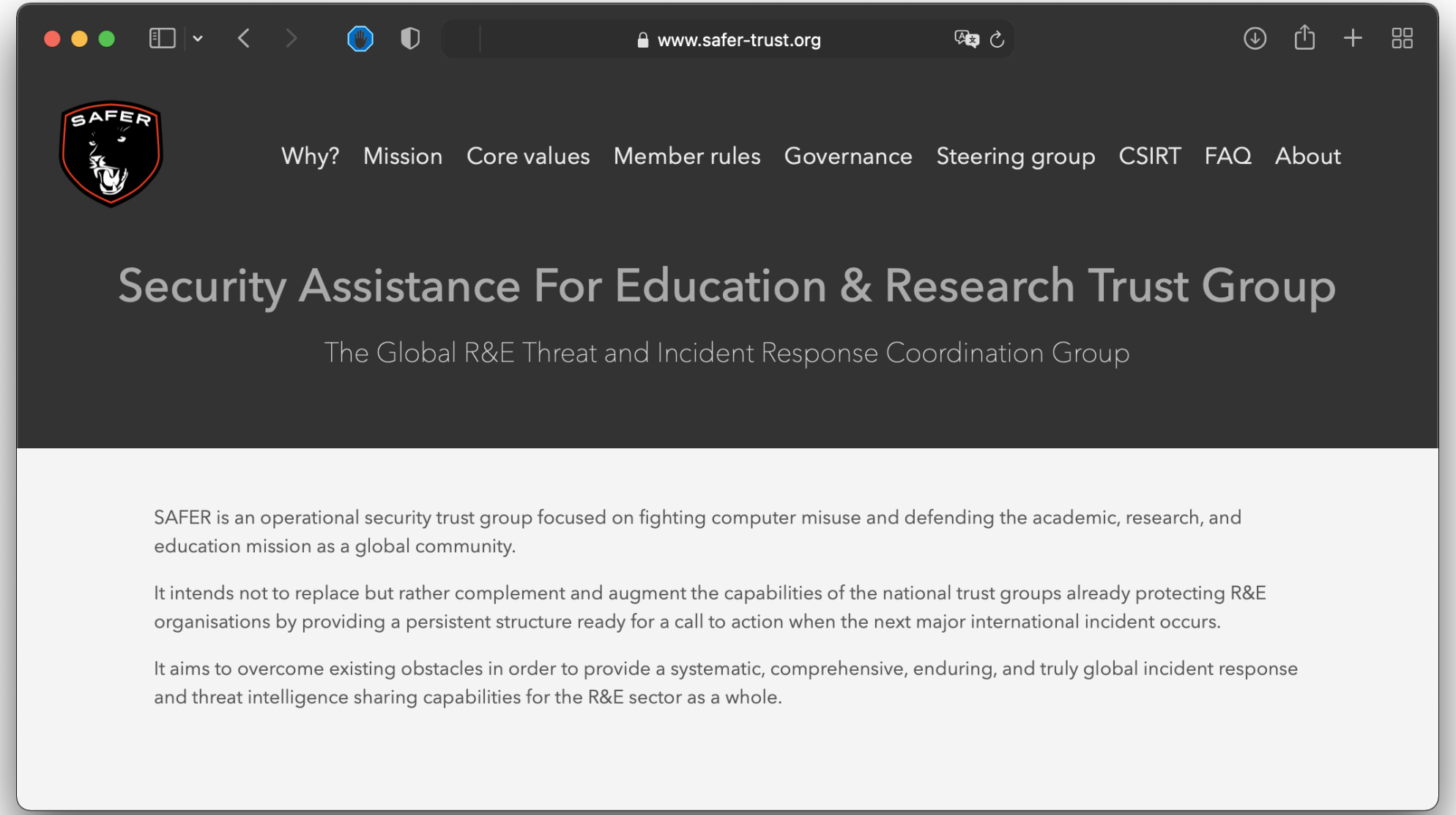
The SAFER operational security trust group

Romain Wartel

Central coordination is nobody's job

Example of how ad hoc trust groups provide "Central coordination" for most global intrusions affecting the R&E sector

Announcing SAFER



Announcing SAFER

- Why?
  - Defending R&E services and people as a global community
  - Concerted and global effort to connect existing groups

- What?
  - Systematic, comprehensive, enduring, and truly global incident response and threat intelligence sharing capabilities for the R&E sector as a whole.
  - Help to other organisations (e.g. WLCG sites) could take the form of:
    - Sharing threat intelligence to support daily security operations
    - Providing informal emergency incident response assistance
    - Offering members' unique or rare security expertise to support an investigation

SAFER: a huge step forward

…+ more founding members supporting anonymously

We expect many security experts to join!

Contacts

- David Crooks (david.crooks [at] stfc.ac.uk)
- Liviu Vâlsan (liviu.valsan [at] cern.ch)
- Romain Wartel (romain.wartel [at] cern.ch)
- Christos Arvanitis (christos.arvanitis [at] cern.ch)

- SOC WG
  - Website: wlcg-soc-wg.web.cern.ch
  - Documentation: wlcg-soc-wg-docs.web.cern.ch
  - Mailing list: wlcg-soc-wg [at] cern [dot] ch

Thank you!

Questions and discussion