



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)

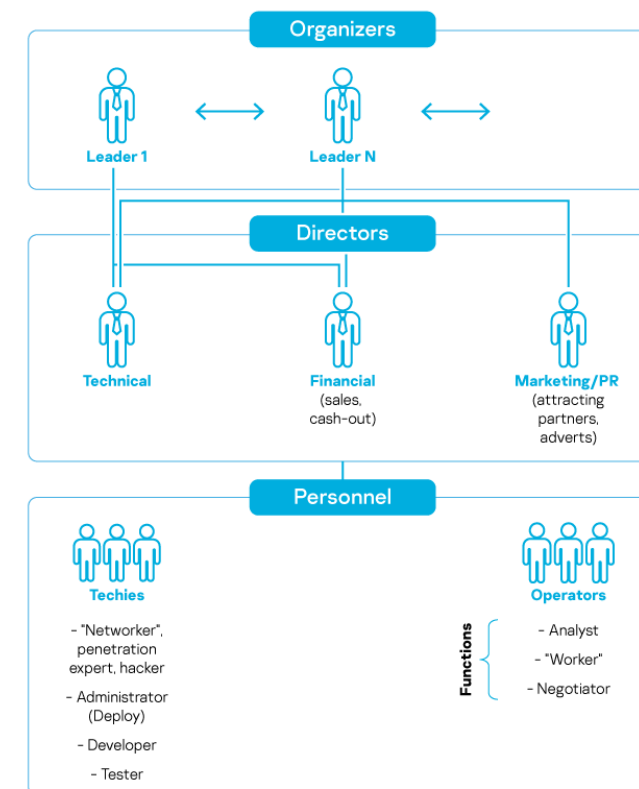


SOC WG Update

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



© 2021 AO Kaspersky Lab. All Rights Reserved

kaspersky

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

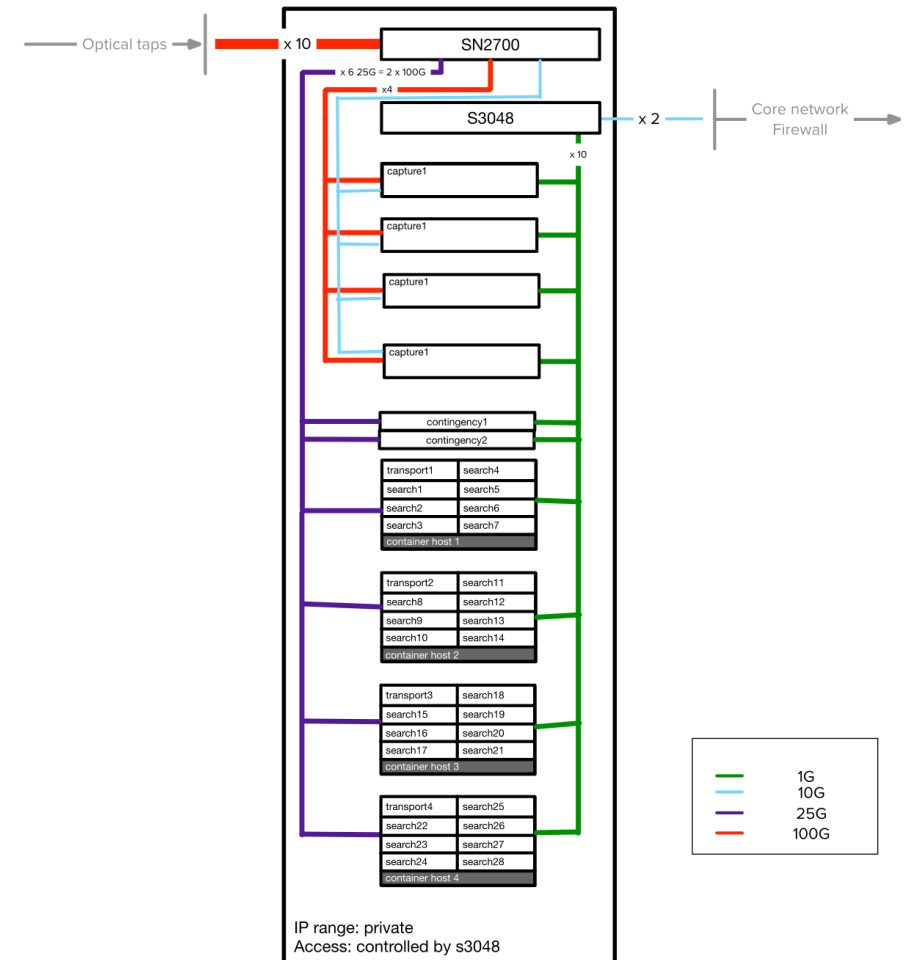
Recent SOC WG progress



- 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

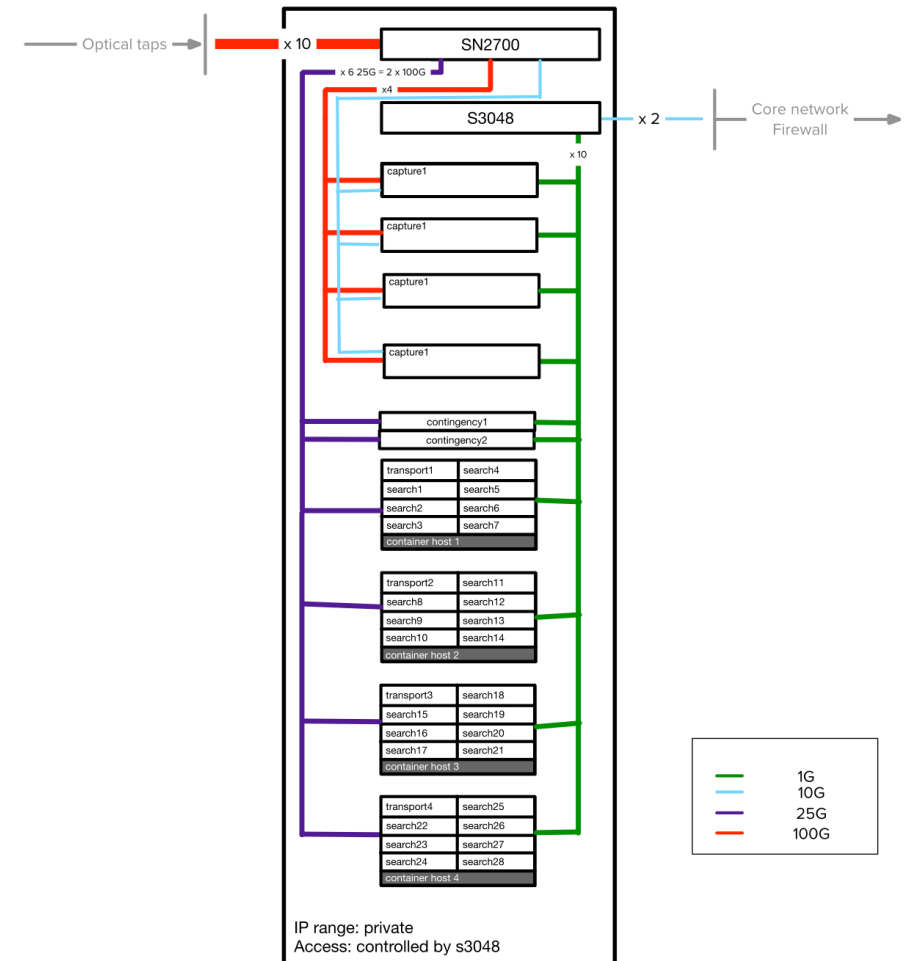
STFC SOC Project

- 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 ($\geq 100\text{G}$)



Questions ?

Full SOC Workflow

Liviu Vâlsan

MISP Threat Intelligence



Events - MISP

misp.cern.ch

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions API MISP Reports-Source Log out

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals

Export
Automation

Events

← previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next →

My Events Org Events

Enter value to search Filter

Published	Source org	Member org	ID	Clusters	Tags
✓	[REDACTED]	WLCG	26075	Sector Q Telecoms Q	tip:green Flubot Android
✓	[REDACTED]	WLCG	29933		tip:green cirl:incident-classification=scam cirl:topic=individual misp-galaxy:target-information=Luxembourg
✓	[REDACTED]	WLCG	30027		tip:white osint:source-type=block-or-filter-list
✓	[REDACTED]	WLCG	12069		tip:white misp:threat-level=low-risk cirl:incident-classification=scam veris:action:social:variety=Extortion
✓	[REDACTED]	WLCG	10442		cirl:topic=finance veris:attribute:integrity:variety=Fraudulent transaction TLP: Green tip:green TLP: white
✓	[REDACTED]	WLCG	29991		ecsirt:fraud=phishing tip:green
✓	[REDACTED]	WLCG	30023		tip:white osint:source-type=block-or-filter-list
✓	[REDACTED]	WLCG	28290		veris:action:social:variety=Phishing veris:attribute:confidentiality:data:variety=Credentials veris:action:malware:vectors=Email link veris:action:social:vectors=Email phishing:distribution=bulk-phishing misp-galaxy:mitre-attack-pattern=Phishing - T1566 tip:white PAP:WHITE veris:confidence=High estimative-language:confidence-in-analytic-judgments=high misp:confidence-level=completely-confident
✓	[REDACTED]	WLCG	30021		tip:green cirl:incident-classification=scam
✓	[REDACTED]	WLCG	26621	Threat Actor Q APT 29 Q	misp-galaxy:mitre-intrusion-set=APT29 - G0016 misp-galaxy:mitre-enterprise-attack-intrusion-set=APT29 - G0016 misp-galaxy:mitre-attack-pattern=Authentication Package - T1547.002

Could not locate the PGP public key.

Powered by MISP 2.4.148 - 2021-12-03 14:18:01

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

Access



CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account

Reminder: you have agreed to comply with the [CERN computing rules](#), in particular OC5. CERN implements the measures necessary to ensure compliance.

Use credentials

Username or Email address

Password

☐ Remember Username or Email Address [Need password help ?](#)

Use one-click authentication



[Sign in using your current Windows/Kerberos credentials \[autologon\]](#)

Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).



[Sign in using your CERN Certificate \[autologon\]](#)

You can get a CERN certificate on the [CERN Certification Authority website](#).

Use strong two factor authentication [show]

Sign in with a public service account

Some social account providers, e.g. Facebook, may use knowledge about your access to CERN for purposes such as profiling.



[Facebook, Google, Live, etc.](#)

Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.

Sign in with your organization or institution account



EduGain <https://edugain-proxy.igtf.net/simplesaml/saml2/idp>

[Why is my organisation not listed?](#)

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

Select a certificate

Select a certificate to which you want to authenticate edugain-proxy.igtf.net:443

Subject	Issuer	Serial
[redacted]	GEANT eScience Per...	00A9CA9F53CB305...

Creating a test MISP event



The screenshot shows the 'Add Event' form in the MISP interface. The browser address bar shows 'misp.cern.ch/events/add'. The form includes a sidebar with navigation links: List Events, Add Event (selected), Import from..., REST client, List Attributes, Search Attributes, View Proposals, Events with proposals, Export, and Automation. The main form area has a title 'Add Event' and a message: 'The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.' The form fields are: Date (2021-12-03), Distribution (Your organisation only), Threat Level (High), Analysis (Initial), Event Info (CMS exercise 2019), and Extends Event (Event UUID or ID. Leave blank if not applicable). A 'Submit' button is at the bottom. The footer shows 'Powered by MISP 2.4.148 - 2021-12-03 14:21:36'.

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

Tagging



The event has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

CMS exercise 2019

Event ID	30031
UUID	1788d275-1ce8-4a38-a2e2-fa6b7d5f8717
Source Organisation	EGI CSIRT
Member Organisation	EGI CSIRT
Creator user	
Tags	
Date	2021-12-03 14:22:28
Threat Level	High
Analysis	Initial
Distribution	Your organisation
Info	CMS exercise
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2021-12-03 14:22:28
Modification map	
Sightings	0 (0) - restricted to own organisation only.

—Pivots —Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports —Attributes —Discussion

30031: CMS exerci...

Galaxies

Could not locate the PGP public key.

Powered by MISP 2.4.148 - 2021-12-03 14:22:28

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

Adding IoCs



Objects - MISP

misp.cern.ch/objects/add/30031/106

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions API

Create Sync Config

Add Url Object

Object Template: Url v7

Description: url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.

Requirements: Required one of: url, resource_path

Meta category: Network

Distribution: Inherit event

Comment:

First seen date: Last seen date:

First seen time: HH:MM:SS.ssssss+T:TT Last seen time: HH:MM:SS.ssssss+T:TT

Expected format: HH:MM:SS.ssssss+T:TT Expected format: HH:MM:SS.ssssss+T:TT

Save	Name :: type	Description	Category	Value	IDS	Disable Correlation	Distribution	Comment
<input checked="" type="checkbox"/>	Url url	Full URL	Network activity	http://s524732349.onlinehome.fr/autocad.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	Payload URL for miner
<input type="checkbox"/>	Fragment text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	Other		<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	
<input type="checkbox"/>	Tld text	Top-Level Domain	Other		<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	
<input type="checkbox"/>	Port port	Port number	Network activity		<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	
<input type="checkbox"/>	Scheme text	Scheme	Other	-- Select an option --	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	

Could not locate the PGP public key.

Powered by MISP 2.4.148 - 2021-12-03 14:26:35

<https://misp.cern.ch/objects/add/30031/106#>

- 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



CMS exercise 2019

Event ID30031

UUID1788d275-1ce8-4a38-a2e2-fa6b7d5f8717

Source OrganisationEGI CSIRT

Member OrganisationEGI CSIRT

Creator user

Tags🔖 tipamber x 🗑 test x 🗑 + 🗑 +

Date2021-12-03

Threat Level🔴 High

AnalysisInitial

DistributionThis community only

InfoCMS exercise 2019

PublishedYes (2021-12-03 17:40:55)

#Attributes5 (2 Objects)

First recorded change2021-12-03 14:34:00

Last change2021-12-03 17:24:02

Modification map

Sightings0 (0) - restricted to own organisation only

—Pivots —Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports —Attributes —Discussion

X 30031: CMS exerci...

Galaxies

🗑 + 🗑 +

< previous next > view all

+ 🗑 🗑 🗑 Scope toggle Deleted ⚡ Decay score 🗑 SightingDB ⓘ Context 🗑 Related Tags 🗑 Filtering tool

Enter value to search 🔍

<input type="checkbox"/>	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
	2021-12-03		Object name: file										Inherit			
	References: 0															
<input type="checkbox"/>	2021-12-03		Payload delivery	md5:	31aa234f6a87d84b20bb66f42f4e383a			MD5 Hash of the miner	🗑	10675		🗑	Inherit	🗑 🗑 🗑 (0/0/0)	🗑 🗑 🗑	
				md5					🗑			🗑				
<input type="checkbox"/>	2021-12-03		Payload delivery	filename:	autocad.exe			File name of the miner	🗑			🗑	Inherit	🗑 🗑 🗑 (0/0/0)	🗑 🗑 🗑	
				filename					🗑			🗑				
<input type="checkbox"/>	2021-12-03		Payload delivery	sha1:	e64a4d87ce8499169354f38cee4fbc4c6cb0050f			SHA1 Hash of the miner	🗑	10675		🗑	Inherit	🗑 🗑 🗑 (0/0/0)	🗑 🗑 🗑	
				sha1					🗑			🗑				
<input type="checkbox"/>	2021-12-03		Other	size-in-bytes:	4096			File size of the miner	🗑	5178 14671			Inherit	🗑 🗑 🗑 (0/0/0)	🗑 🗑 🗑	
				size-in-bytes					🗑							
	2021-12-03		Object name: url										Inherit			
	References: 0															
<input type="checkbox"/>	2021-12-03		Network activity	url:	http://s524732349.onlinehome.fr/autocad.exe			Payload URL for miner	🗑	10675		🗑	Inherit	🗑 🗑 🗑 (0/0/0)	🗑 🗑 🗑	
				url					🗑			🗑				

Related Events

DL...	DigitalSide Malware report: MD5: 7c398429fa0547f08626c3a531a8ef71	1
2020-07-22		
WL...	Test simulated mock-up incident for training purposes -- do not use for pr...	3
2019-10-22		
FR...	OSINT report: McAfee - Operation GhostSecret (enriched)	1
2018-04-24		

API

MISP

Log out

Related Events

Test simulated mock-up incident for training purposes -- do not use for pr...
2019-10-22

Publish Event

Are you sure this event is complete and everyone should be informed?

Yes No

ATT&CK matrix +Event reports —Attributes —Discussion

Powered by MISP 2.4.148 - 2021-12-03 14:34:01

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	rwix1	http://s524732349.onlinehome.fr/autocad.exe Remove from IDS	1	2021-12-03	EGI CSIRT	tip: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 rwix1	rwix1.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	View details View details
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 rwix1	rwix1.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	View details View details

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

Opsgenie 4m ago
Intel::Notice: Intel hit on 31aa234f6a87d84b20bb66f42f4e383a at Files::IN_HASH (31aa234f6a87d84b20bb66f42f4e383a),...

Opsgenie 4m ago
Intel::Notice: Intel hit on e64a4d87ce8499169354f38cee4fbc4c6c b0050f at Files::IN_HASH (e64a4d87ce8499169354f38cee4fbc4c...

Opsgenie 4m ago
Intel::Notice: Intel hit on s524732349.onlinehome.fr/autocad.exe at HTTP::IN_URL (s524732349.onlinehome.fr/autocad.exe), Connectio

STFC



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 SOC's 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



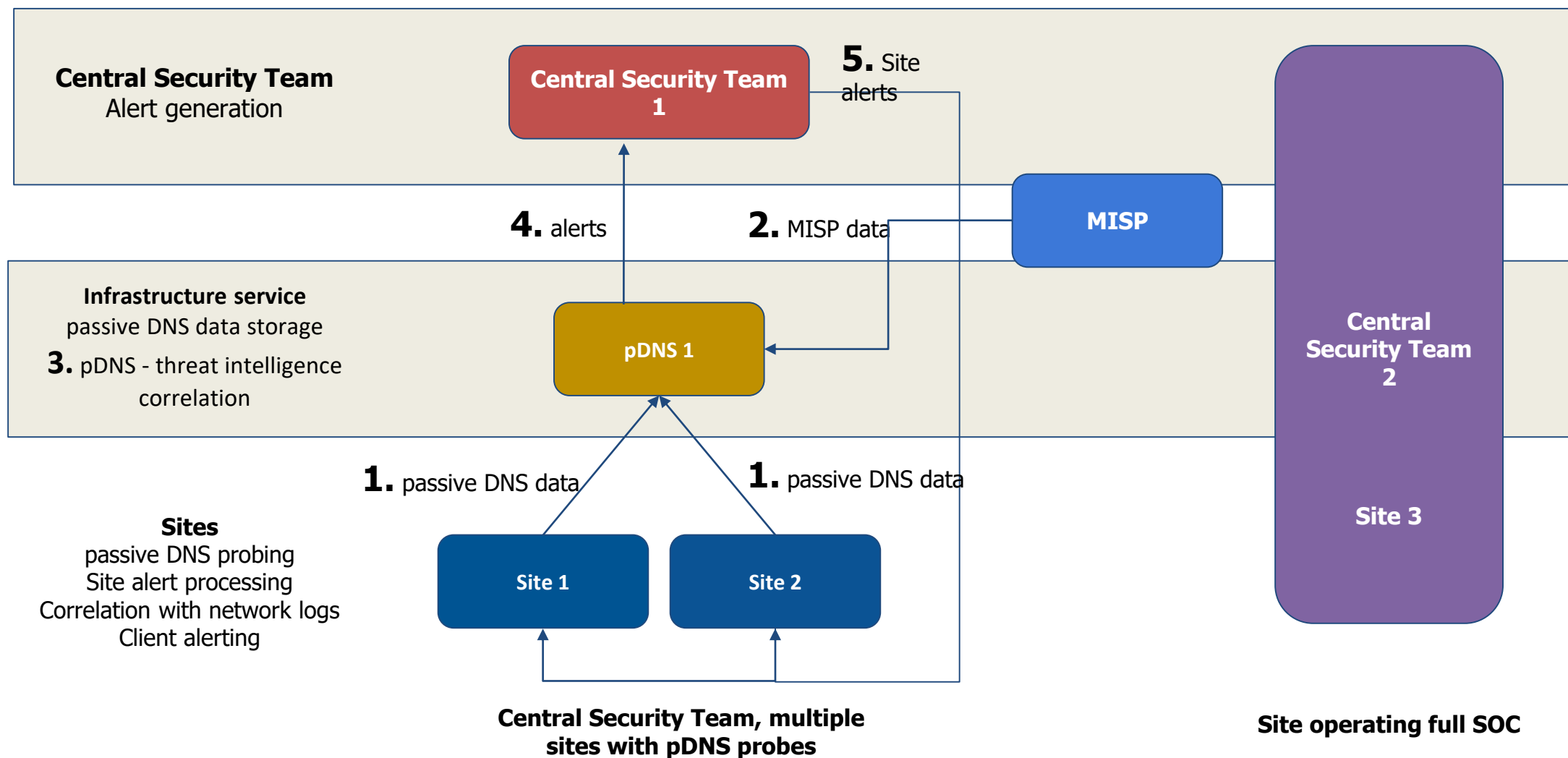
- CERN has a successful RPZ+DNS model with the Swiss health sector during the pandemic
 - 1 DNS server at CERN, 1 at GovCERT: 50 health organisations covered
 - \approx 3M queries/day
 - 5K – 10K blocked domains

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



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

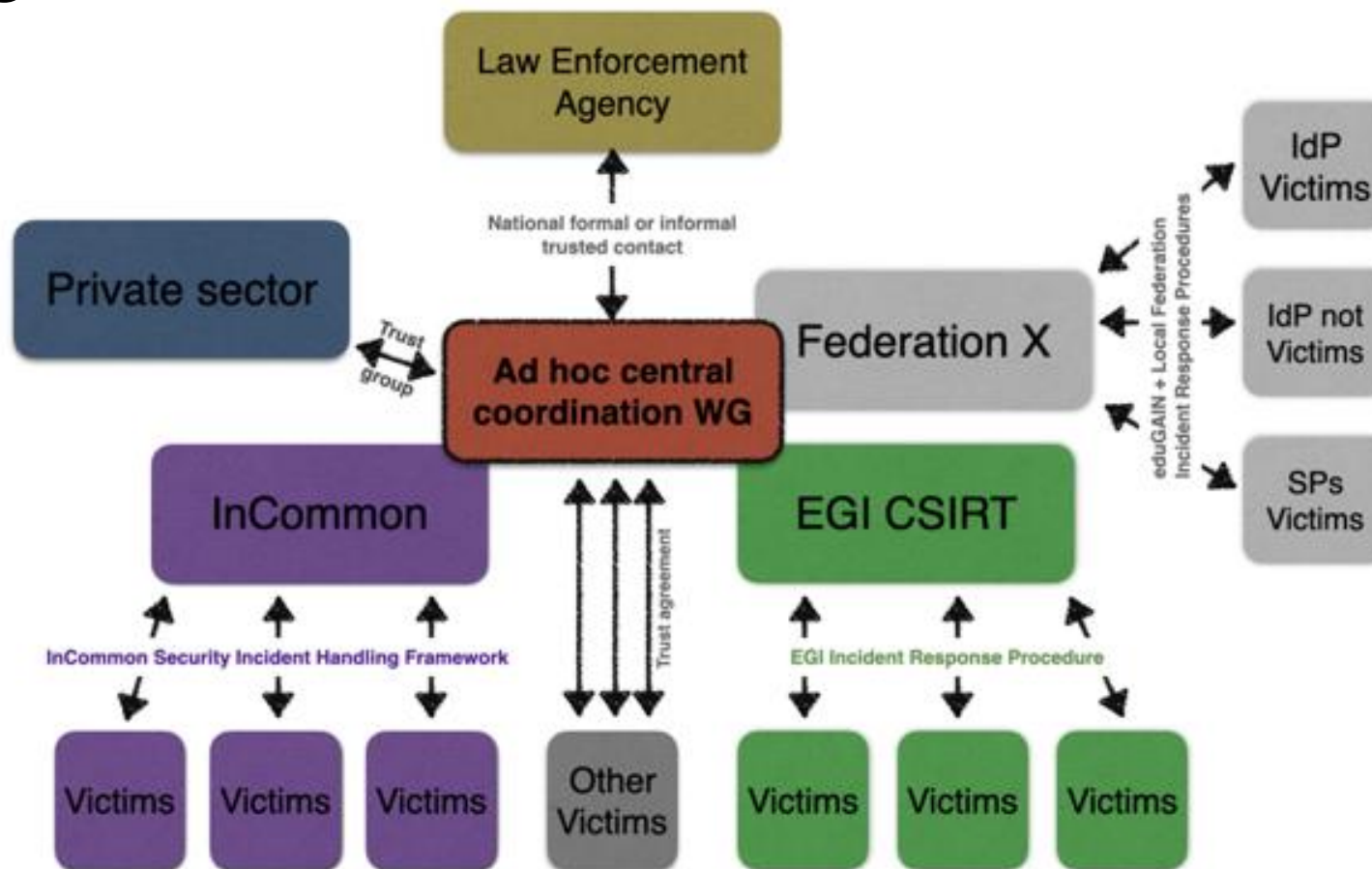


Questions ?

The SAFER operational security trust group

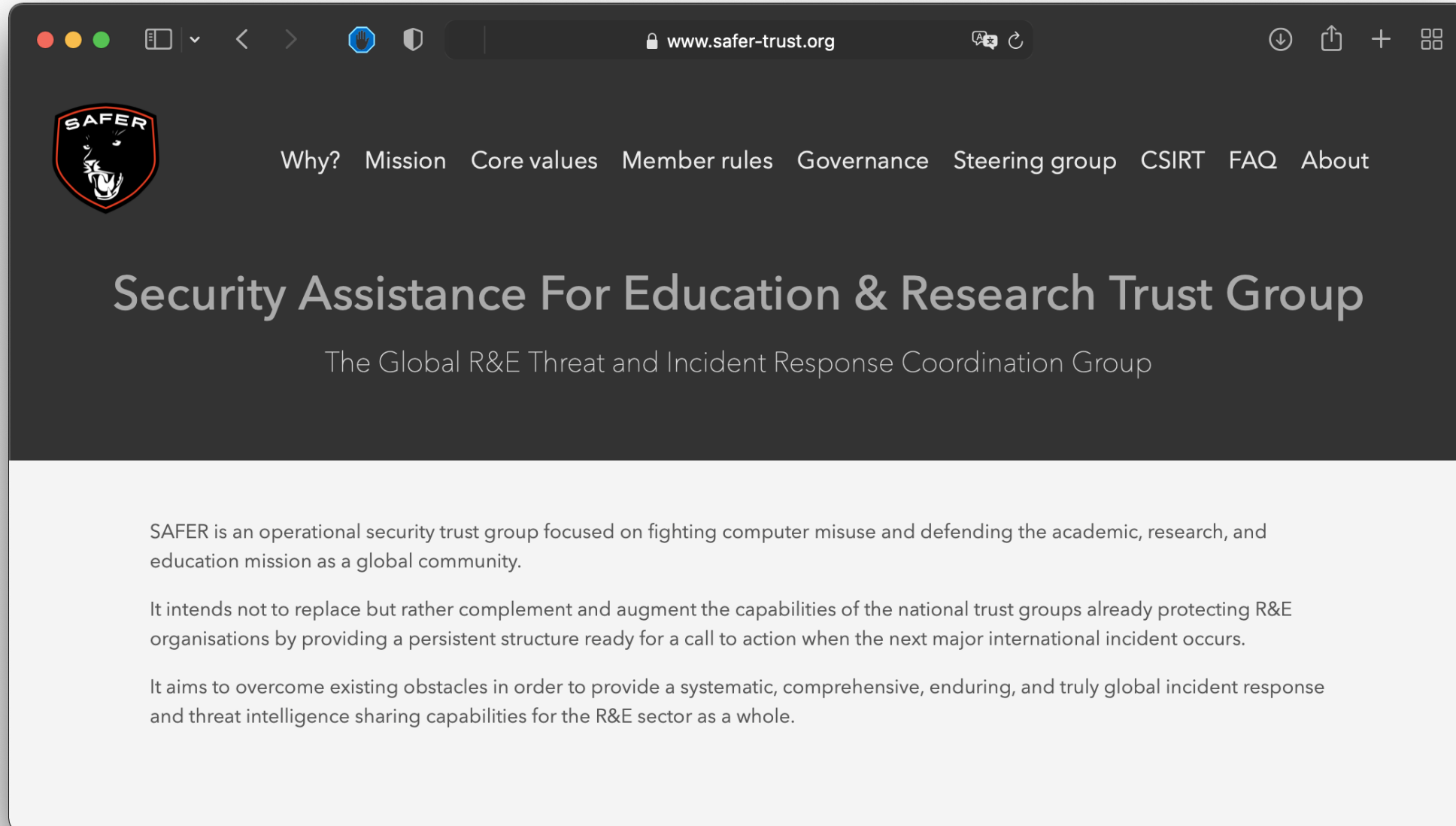
Romain Wartel

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