WLCG SOC WG: ISGC 2021

David Crooks

Liviu Vâlsan

Introduction

- The threats faced by R&E are increasingly
  - Sophisticated
  - Highly profitable for the actors involved

- The more sophisticated the attack, the more likely it is that it will pass undetected for longer

- HEPiX update (Liviu Vâlsan)

Introduction

- We are not protected from these by our domain
  - Several recent examples of large scale, high profile attacks involving research and education institutions across the world

- R&E is a highly heterogeneous environment
  - Some sites have robust monitoring and experience
  - Others are already stretched for resource and less experience

Introduction

- We all face the same threats
- Why not then work together and share intelligence?
  - In addition to sharing our experience and collaborate in deploying the necessary infrastructure
- How do we do this?

Introduction

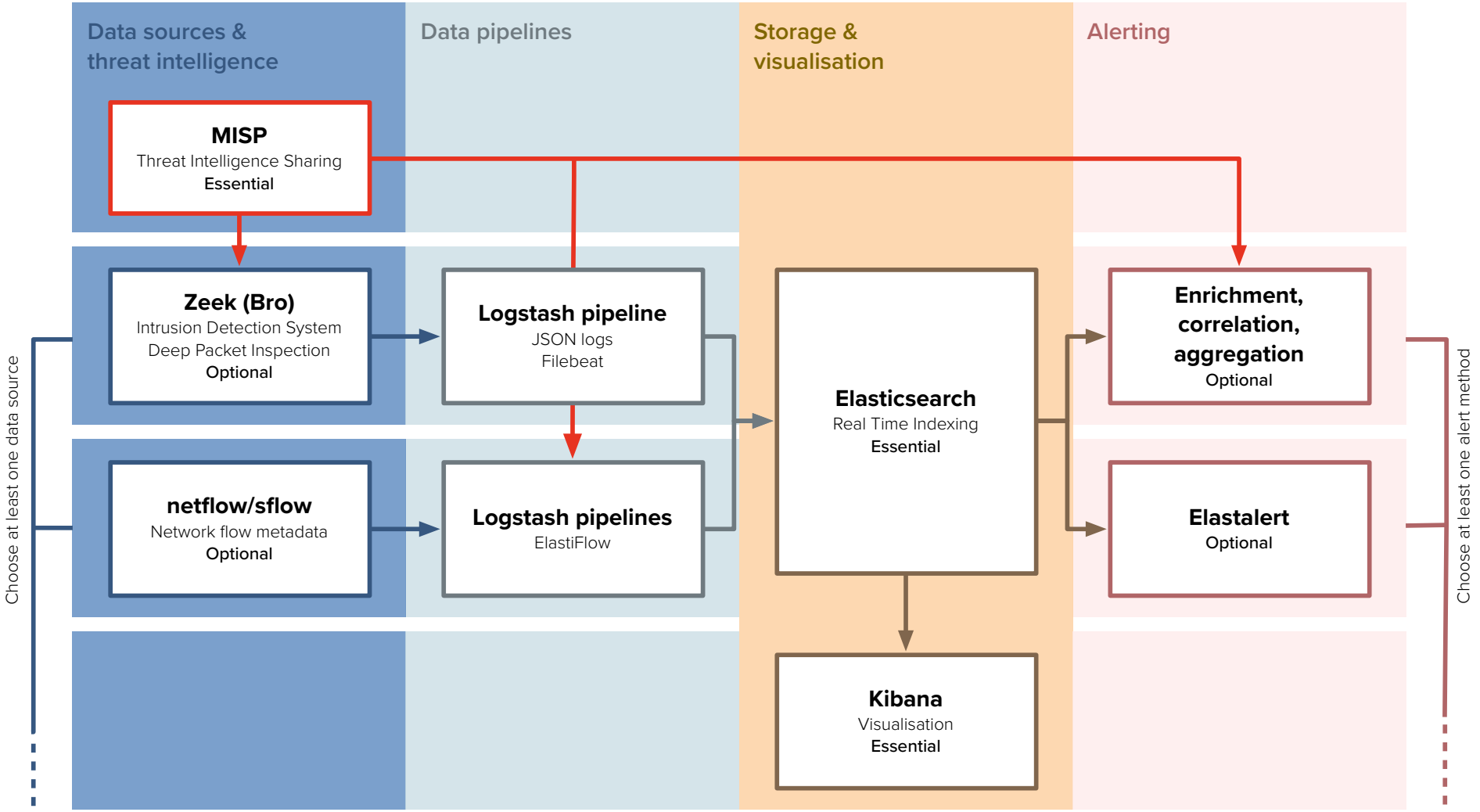
- Share intelligence
  - Threat intelligence sharing platform
- Make active use of that intelligence
  - Robust network monitoring
  - Storage, visualization, correlation and alerting

Security Operations Centres Working Group

- Allowing WLCG sites to digest and make active use of threat intelligence is a cornerstone of the WLCG security strategy
- The WLCG Security Operations Centre WG was established to enable the deployment of security tools to enable this
  - But also including members from the wider academic research community

- The working group is mandated to create reference designs to allow sites to
  - Ingest security monitoring data
  - Enrich, store and visualize this security data
  - Alert based on matches between the stored data and threat intelligence
  - Indicators of Compromise or IoCs

Technology stack: Initial Model



ISGC Security Workshop

- Thank you to everyone that attended our session!
  - Very useful workshop
- Demonstrated demo traffic triggering logs at multiple sites
- Planning to follow up on some ideas for future events
  - Feedback from attendees very welcome

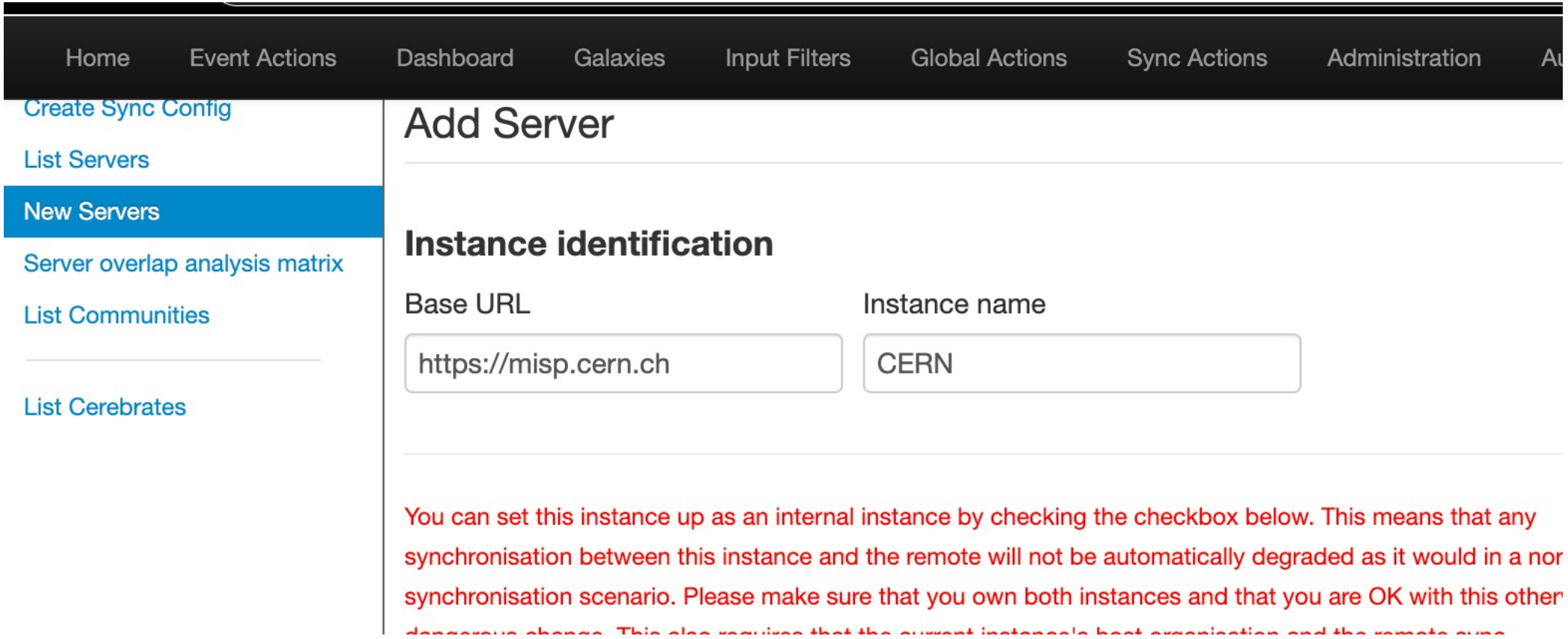
Progress and plans update

- ASGC
- AGLT2
- Nikhef
- STFC/RAL

ASGC

- SOC in place
- Syncing with the central MISP instance
- Framework of collaboration on threat intel sharing with KEK and IHEP

SOC Setup at ASGC



Configuring the central MISP instance on the local MISP instance at ASGC

SOC Setup at ASGC

Jobs

Purge job entries:

Completed | All

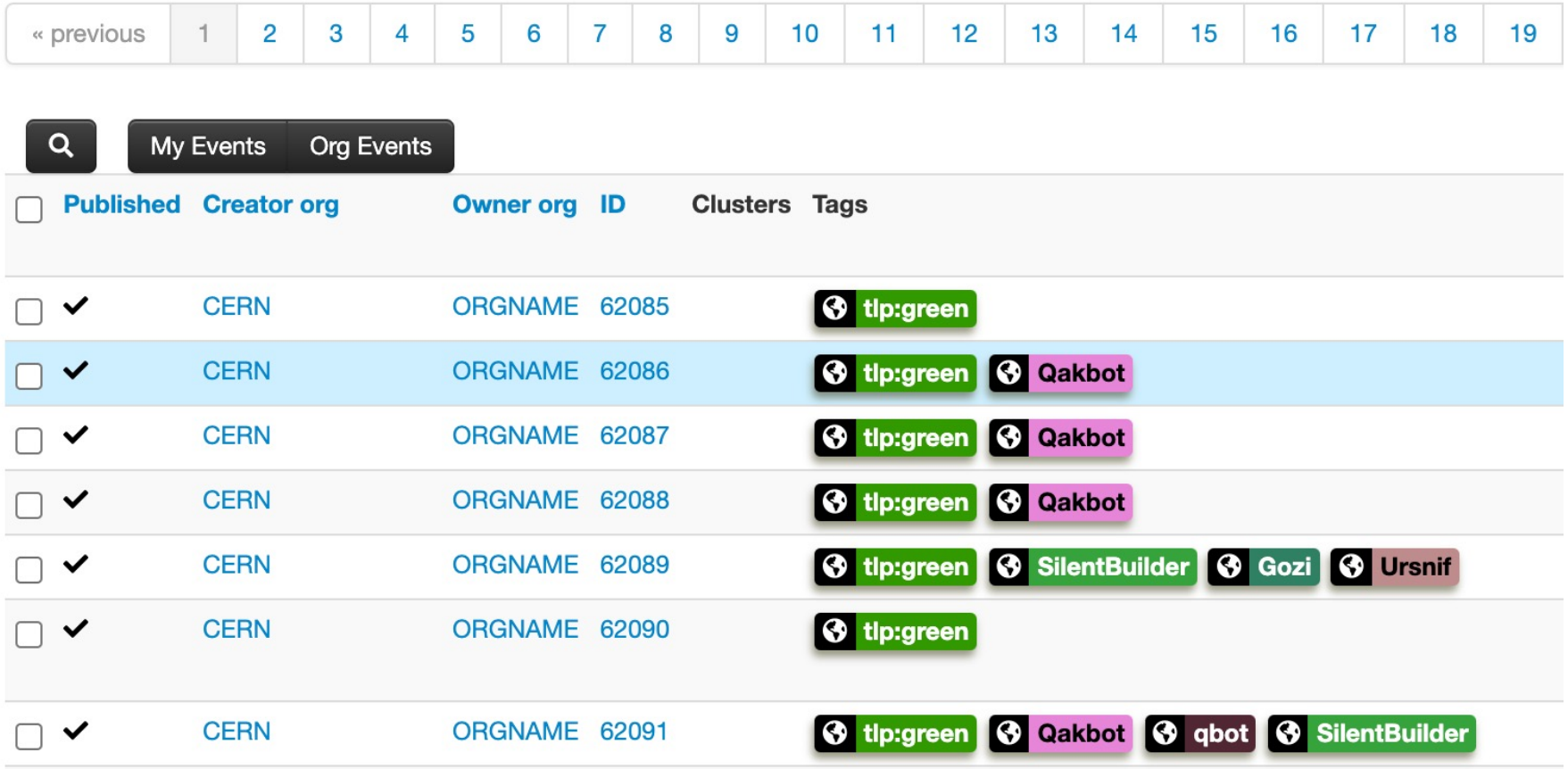
« previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | next »

All | Default | Email | Cache

Id	Date created	Date modified	Process ID	Worker	Job type	Input	Message	Organisation name	Status	Retries	Progress
63013	2021-03-19 09:19:46	2021-03-19 09:19:57	4a23585172f0a4c7a78459139ab11e0a	default	pull	Server: 4	Pulling 15113 events.	SYSTEM	Unknown	0	10%

Pulling events from the central MISP instance

SOC Setup at ASGC



Sample of events synchronised from the central MISP instance

SOC Setup at ASGC

```
#! /bin/bash
PREF=/opt/misp
source $PREF/config/setauth.sh

FEEDDIR="$PREF/config/feeds"
FEEDFILE=$FEEDDIR"/testdata.txt"

mkdir -p $FEEDDIR

touch $FEEDFILE
AUTHKEY="[redacted]"
AUTH_KEY="Authorization: $AUTHKEY"

curl -k -s --header "$AUTH_KEY" https://[redacted]/attributes/bro/download/ > $FEEDFILE
[root@asgc-cap bin]# cat pull_misp.sh | grep -v AUTHKEY=
#! /bin/bash
PREF=/opt/misp
source $PREF/config/setauth.sh

FEEDDIR="$PREF/config/feeds"
FEEDFILE=$FEEDDIR"/testdata.txt"

mkdir -p $FEEDDIR

touch $FEEDFILE
AUTH_KEY="Authorization: $AUTHKEY"

curl -k -s --header "$AUTH_KEY" https://[redacted]/attributes/bro/download/ > $FEEDFILE
```

Script used to export IoCs from MISP in Zeek format

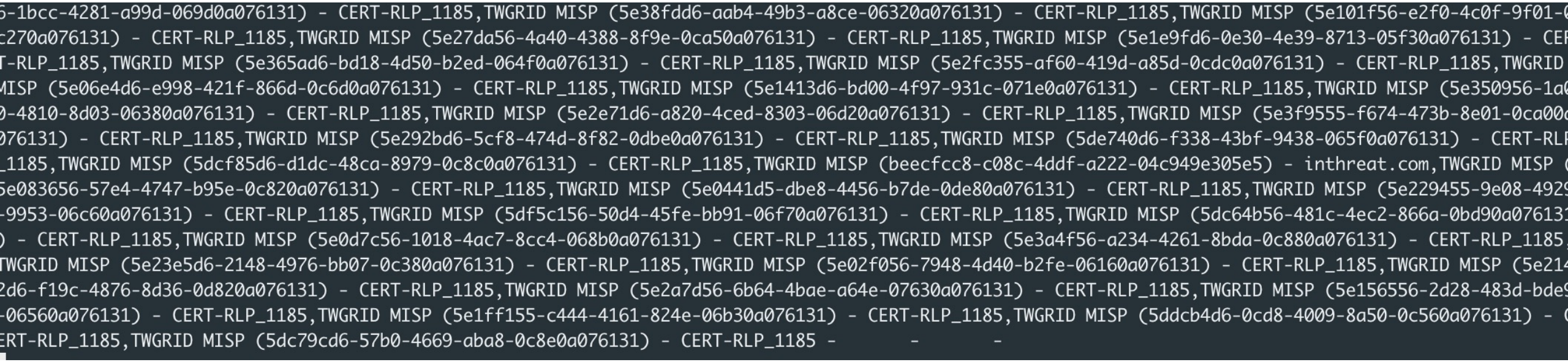
SOC Setup at ASGC

```
# Uncomment this to source zkg's package state
# @load packages
#
redef ignore_checksums = T;
redef Intel::read_files += {"/opt/misp/config/feeds/testdata.txt"};

@load policy/frameworks/intel/seen
```

Configuring Zeek's intel framework to use the Indicators of Compromise

SOC Setup at ASGC



Checking the intel log for hits on the monitored IoCs

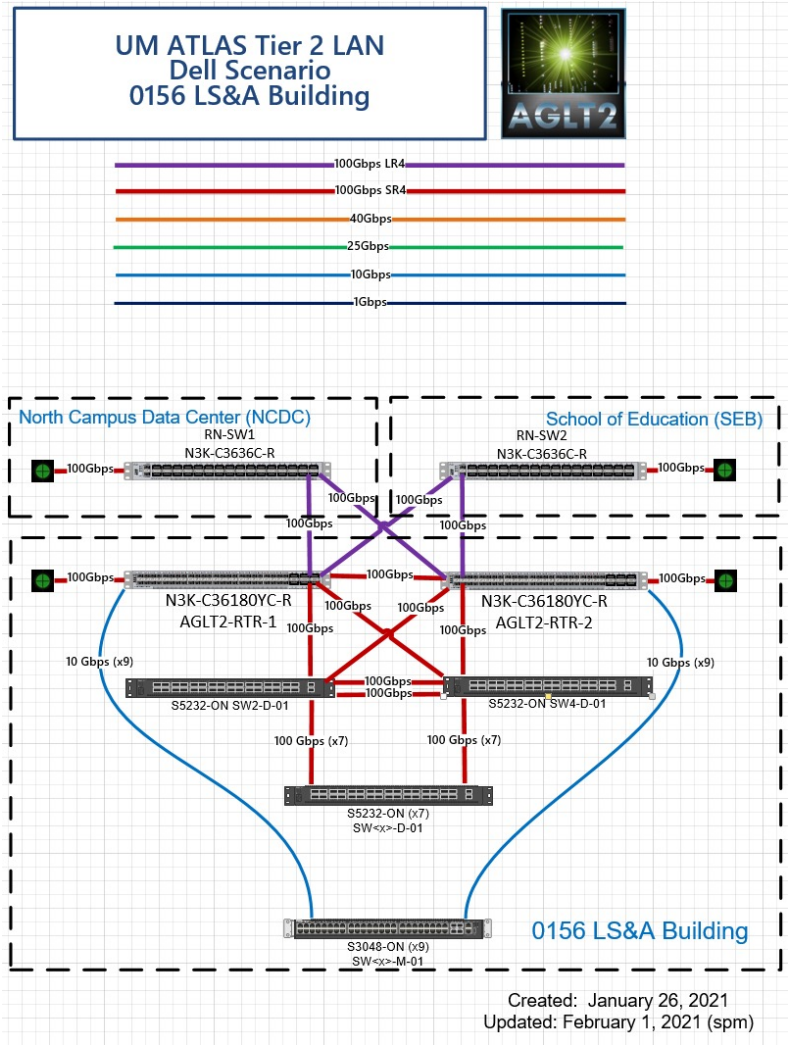
AGLT2

- The ATLAS Great Lakes Tier-2 (AGLT2) has been using Zeek+MISP+ELK for a few years now
- Current deployment is monitoring 2x40G WAN links
  - Single 10G connection to Merit Networks
- Single Dell R630 server
  - two dual-ported Intel XL710 40G NICs
  - on-board Broadcom 10G port

AGLT2

- AGLT2 network will undergo a significant refresh
  - 2x40G links replaced by much more resilient network
  - based upon 100G connections

AGLT2


UM ATLAS Tier 2 LAN
Dell Scenario
0156 LS&A Building
AGLT2
100Gbps LR4
100Gbps SR4
40Gbps
25Gbps
10Gbps
1Gbps
North Campus Data Center (NCDC)
School of Education (SEB)
RN-SW1
N3K-C3636C-R
RN-SW2
N3K-C3636C-R
100Gbps
N3K-C36180YC-R
AGLT2-RTR-1
N3K-C36180YC-R
AGLT2-RTR-2
10 Gbps (x9)
S5232-ON SW2-D-01
S5232-ON SW4-D-01
100 Gbps (x7)
S5232-ON (x7)
SW<x>-D-01
S3048-ON (x9)
SW<x>-M-01
0156 LS&A Building
Created: January 26, 2021
Updated: February 1, 2021 (spm)

AGLT2

- This will require a new Zeek monitoring infrastructure
  - Two servers and 8 100G LR4 optics
    - monitor the purple connections in the previous diagram
  - require 8 ports of 100G LR4 to monitor both directions over all links.
  - New hardware chosen based upon the Dell R7525 platform
    - incorporate four Mellanox Bluefield-2 NICs
- 3 undergraduates working on
  - deploying, testing and tuning the new hardware to run Zeek
  - implement the WLCG-SOC suggestions in this context
- We expect to have an operational system by mid-summer 2021

Nikhef

- During the conference, just had an update in the preceding talk
  - 100G monitoring in 2U!
- For readers in the future they can be found here

- Great progress

- Useful experience
  - Especially in light of many sites moving to (multiple) 100G links

STFC

- Refreshing existing CloudSOC deployment based on sflow

- Graduate working on
  - deployment of Zeek against Tier1
  - Uplift of Elasticsearch service ACLs
    - Both for this project and general local use

- Deploying system to integrate intelligence from misp.cern.ch with STFC firewalls
  - Some preparatory work for this in progress

UK update

- Within IRIS eInfrastructure started the 2021 series of security workshops
- The next one, to be scheduled soon, will focus on central logging and threat intelligence
  - Scope includes Grid, HPC and Cloud sites
- Advanced planning in place to give direct access to misp.cern.ch to Jisc NREN

Central MISP update

- Sharing agreement in place and available
  - For access, please talk to Romain
  - wlcg-security-officer@cern.ch
- Specific focus increasing scope from HEP to other R&E communities
- Giving access to intelligence to new sites both via
  - direct API access
    - Highly encouraged as first step prior to separate MISP instance
  - MISP sync
- Prefer eduGAIN federated authentication
  - For users with grid certificates, success with IGTF Certificate Proxy

Coordination for 2021

- Looking now at WG goals for the year
  - Coordination meeting next week

- WLCG: Focus on Tier1 sites
  - continuing rollout of SOC technology
  - giving access to threat intelligence

- REN-ISAC
- ASGC-IHEP-KEK framework
- UK
  - IRIS
  - Jisc

Conclusions

- More sites rolling out SOC technology and ingesting threat intelligence
- Demonstration of workflow well in place
- 2021 marks a major push to connect between regions to collaborate in this area
- Please join us!

WLCG SOC WG

- David Crooks (david.crooks@stfc.ac.uk)
- Liviu Vâlsan (liviu.valsan@cern.ch)

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