



SOC WG: ISGC 2024

David Crooks

Liviu Vâlsan



Agenda

- SOC Hackathon
- pDNSSOC
- Status updates
- Training
- Next steps



SOC Hackathon 2024



- Recent hackathon in CERN last week
- 24 participants in person
 - 11 organisations from 6 countries represented
- ~9 online

SOC Hackathon 2024



- Lightweight solutions for facilities with fewer resources
- Identifying concrete plans for different infrastructures
 - Including WLCG
- Deployment of MISP docker solution developed by Jisc
 - And development of OIDC config options: pull request open on Github project
 - Support for Shibboleth looks promising
- Development of Zeek docs
 - And documentation processes
- Deeper look at using MISP
 - Taxonomies, Feeds, Warning Lists, ...
- People and process

SOC Hackathon 2024



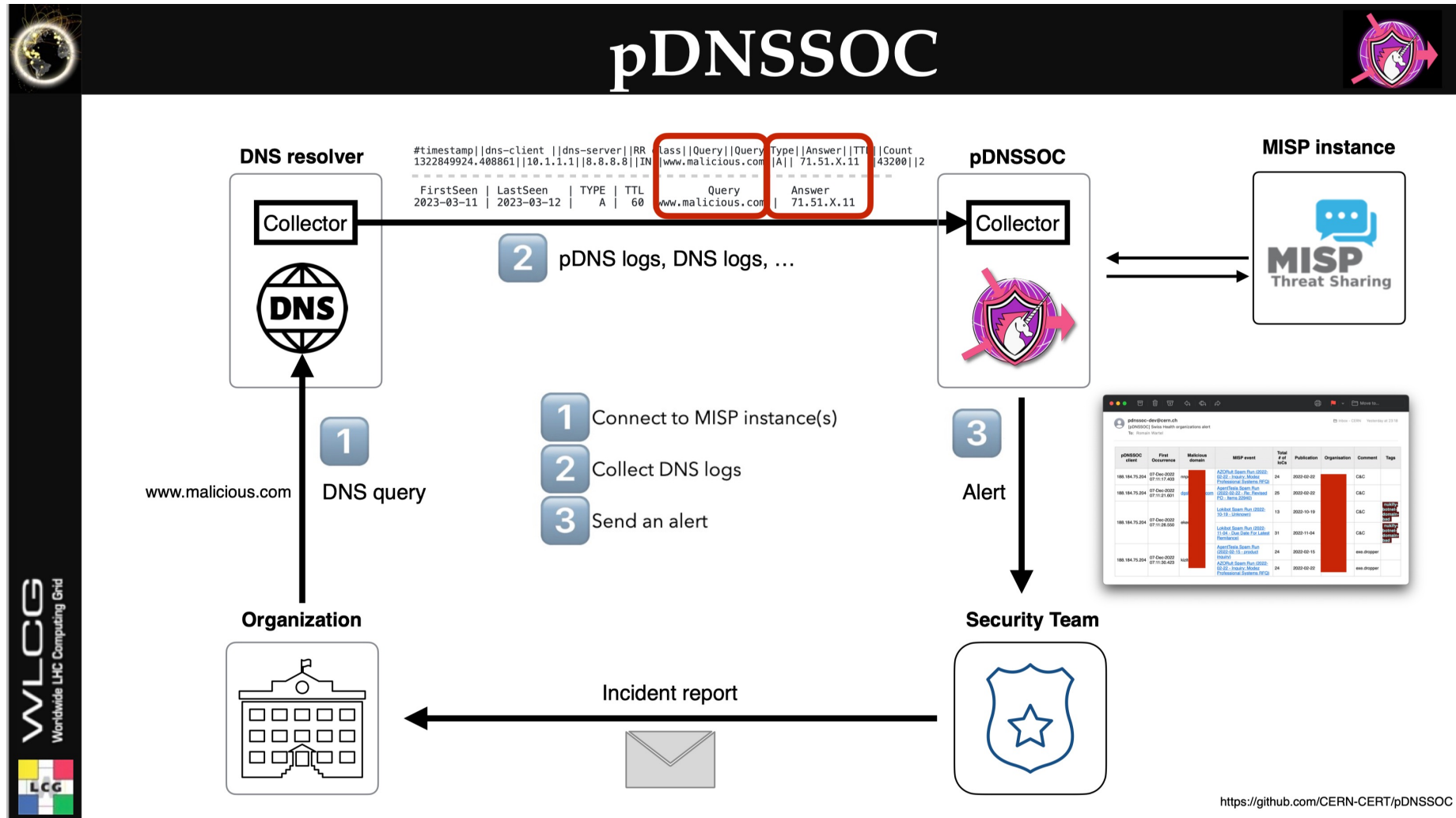
- Unconference format used again to guide content based on interests and needs of those present
- Again effective, but ended up this time with more of a set of full sessions with a smaller amount of breakouts than last time
 - Small team breaking out to work on MISP OIDC config was very effective
- Focus next time on slightly more formal unconference process, with emphasis on identifying key technical work in advance to help make breakout sessions most useful

pDNSSOC

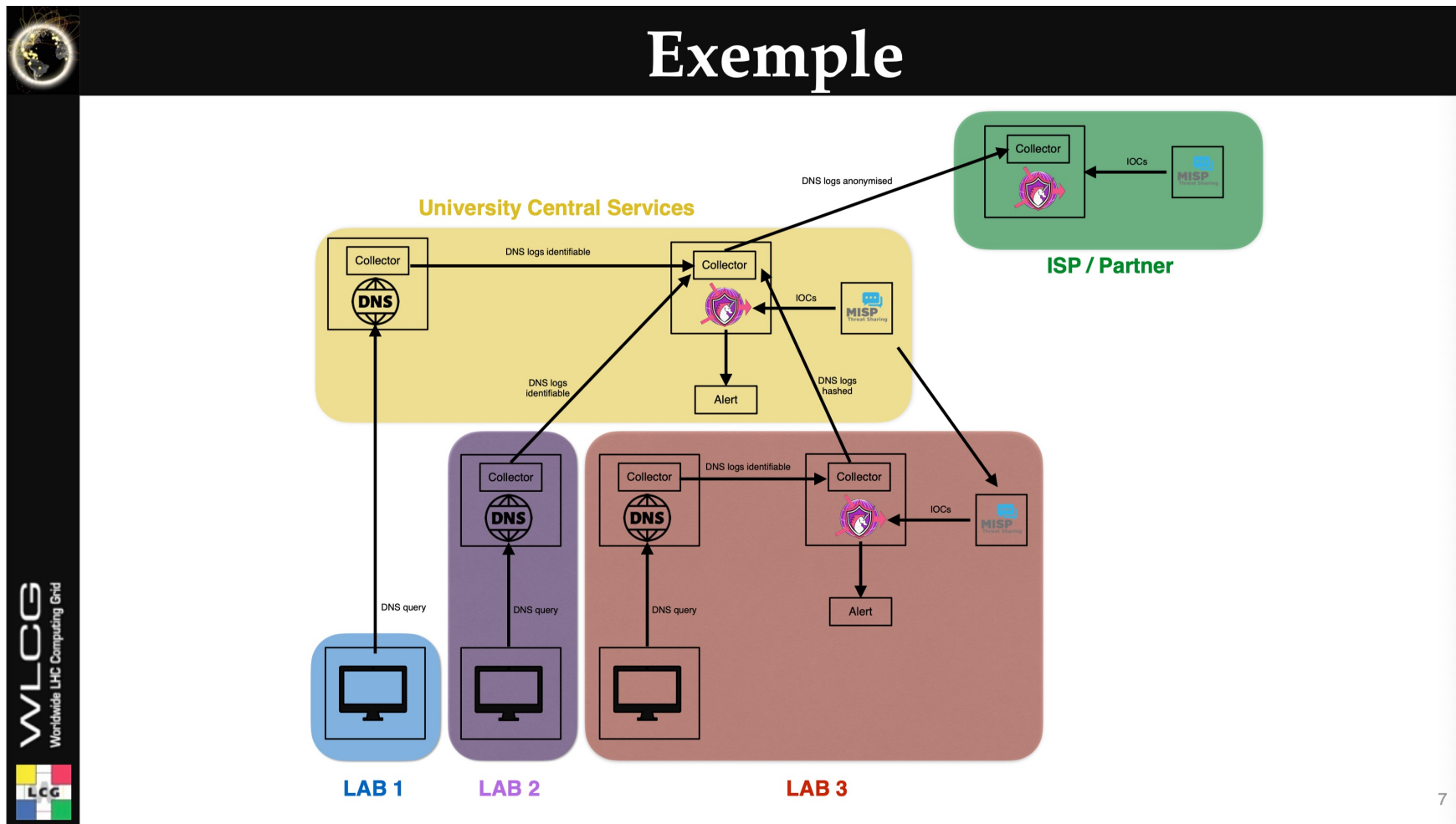


- Deploying a full-scale SOC requires sustained effort, people, processes and technology
- Many/most smaller facilities or sites may not be in a position to take this route
- Identify lightweight "80%" alternative that can make best use of threat intel without significant resource
 - DNS
- pDNSSOC

pDNSSSOC



pDNSSOC



pDNSSOC



- Interest in deploying pDNSSOC in a number of areas
- Looking at how to support pDNSSOC development in the longer term



Status updates

STFC Deployment



- Focus on config management
- Monitoring of both LHC OPN links being commissioned
 - Low capture loss monitoring for both links ($\sim 0.05\%$ / worker thread)
 - Re-engineered load balancing structure in place on aggregation switch
- Security-first Aquilon archetype used for both VM and bare metal machines
 - Working with Rocky9
- OpenSearch cluster in place

STFC Deployment

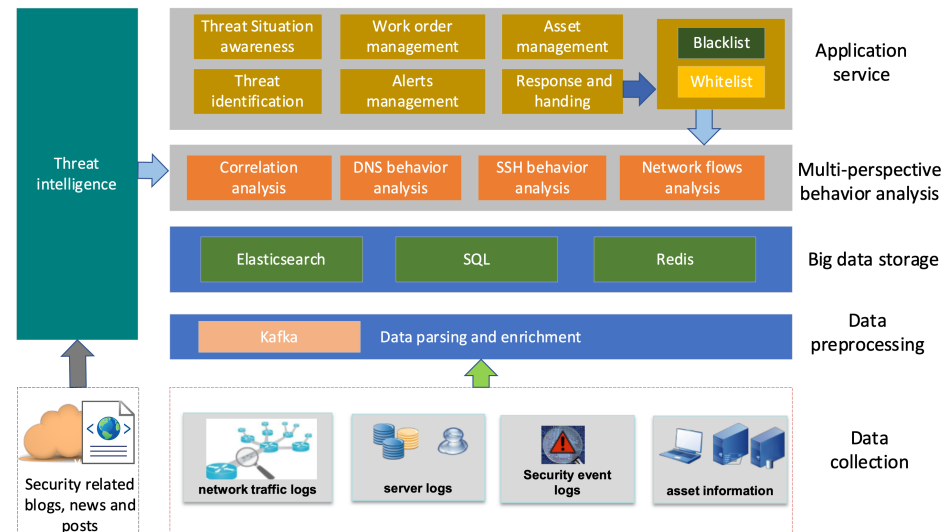


- Kafka and logstash are done and working in development
 - Next are config management and deployment to hardware
- New MISP instance in testing
 - Based on Jisc deployment model
 - Snag fixing network connectivity to UKRI infosec team
- Working across STFC to building operational processes

Status update: IHEP

IHEP SOC

- The Security Operation Center(SOC) proposed in 2021 in IHEP is effective
 - minimize cybersecurity risks
 - improve security operations
- Five data processing layers



Status update: IHEP



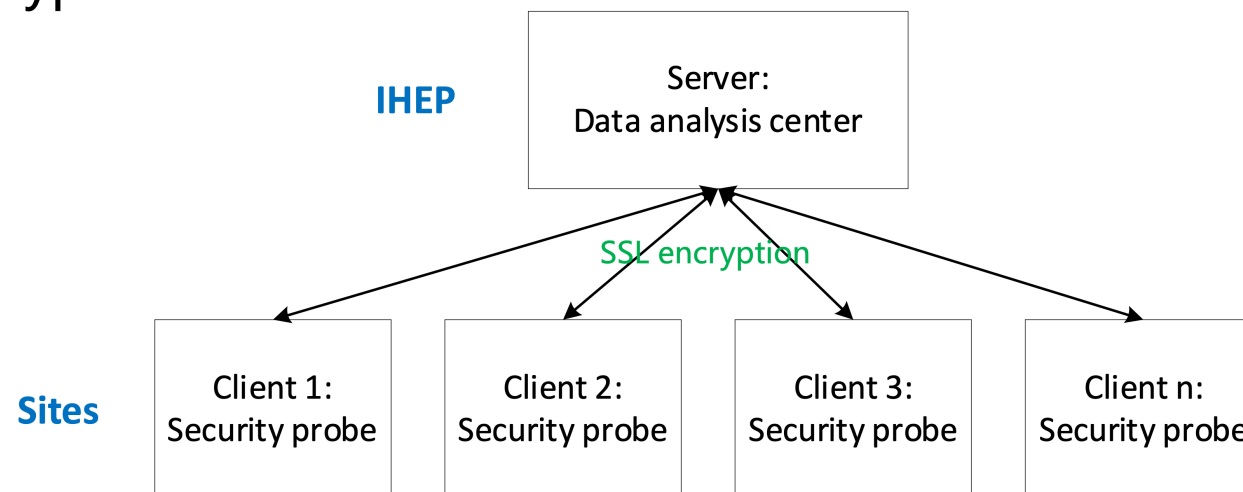
IHEP SOC

- The current framework of SOC can only serve for a single organization
- Facing the new requirement :
 - Providing defense for several collaborative large scientific facilities and scientific data centers across the wide area network
- Update the existing framework to adapt the demand
 - Build the probe in several sites
 - Adopt the distributed framework cross the wide area network

Status update: IHEP

Distributed framework

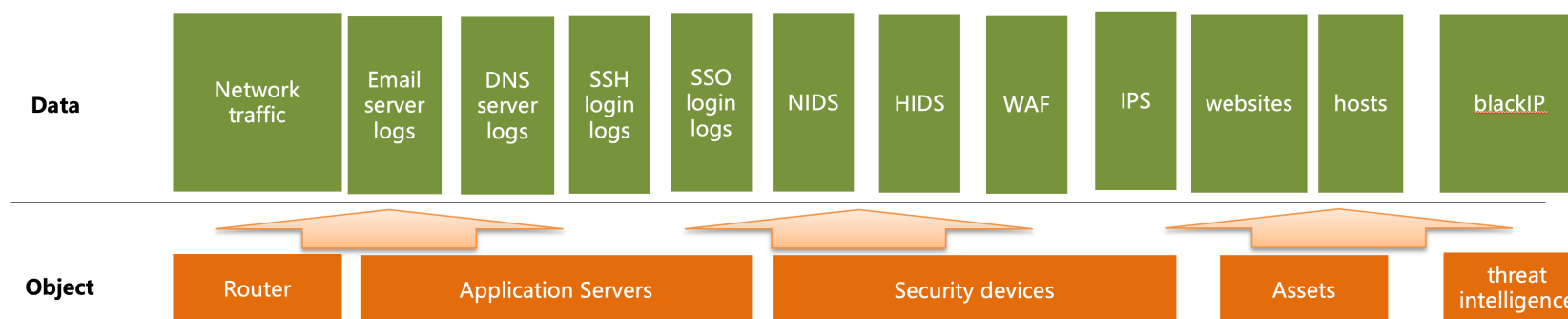
- Client end & server end
 - The client end is deployed in every site
 - The server end is deployed in IHEP
- All sites within the DSOC are highly collaborative and mutual trust
- Encryption



Status update: IHEP

Data collection of security probe

- Security probe collects security data of every site
- Network traffic and security device logs
 - Rsyslog: firewall, IPS, other devices logs
 - Zeek parses raw network packets
- Send the collected data to the data analysis center in IHEP
 - Filebeat : stream data
 - Encrypted transmission over wide area network



Status update: IHEP

Applications

- The DSOC has been applied to institute of high energy physics (IHEP) and deployed in 5 collaborative large scientific facilities and 4 scientific data centers



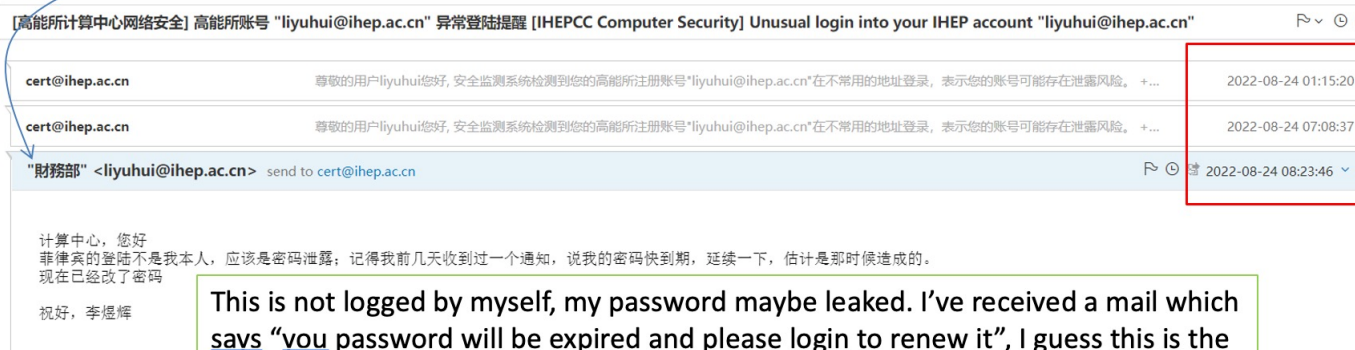
Status update: IHEP

Applications

■ Examples:

- A user's email account was leaked because of phishing mail
- The intruder logged into his account at mid-night
- The DSOC sends an unusual login alert email to the user
- The user read our notice in the morning and changed his password

His name is changed to "The financial department"
The intruder plans to use his account to send phishing mails



[高能所计算中心网络安全] 高能所账号 "liyuhui@ihep.ac.cn" 异常登陆提醒 [IHEPCC Computer Security] Unusual login into your IHEP account "liyuhui@ihep.ac.cn"

From	Subject	Time
cert@ihep.ac.cn	尊敬的用户liyuhui您好, 安全监测系统检测到您的高能所注册账号"liyuhui@ihep.ac.cn"在不常用的地址登录, 表示您的账号可能存在泄露风险. +...	2022-08-24 01:15:20
cert@ihep.ac.cn	尊敬的用户liyuhui您好, 安全监测系统检测到您的高能所注册账号"liyuhui@ihep.ac.cn"在不常用的地址登录, 表示您的账号可能存在泄露风险. +...	2022-08-24 07:08:37
"财务部" <liyuhui@ihep.ac.cn>	send to cert@ihep.ac.cn	2022-08-24 08:23:46

计算中心, 您好
菲律宾的登陆不是我本人, 应该是密码泄露; 记得我前几天收到过一个通知, 说我的密码快到期, 延续一下, 估计是那时候造成的。
现在已经改了密码

祝好, 李煜辉

This is not logged by myself, my password maybe leaked. I've received a mail which says "you password will be expired and please login to renew it", I guess this is the reason.
I've changed my password, thanks!

Training



- PocketSOC-NG again used in security school in 2023
 - Similar to first edition
 - Retuning of access mechanism and refactoring of material
- Graduate project in place at STFC to improve deployment process and training materials, to begin in a few weeks
 - Goal of straightforward deployment to cloud environment with scalable number of clients

SOC WG scope



- Discussed previously that the role of the working group is to focus on technical reference designs and deployment methodologies for security operations centres technical stacks
- However, SOC's are made up of technology, **people and processes**
- The latter two aspects are too important to exclude from this work, so the working group will now expand its scope to include exploration of these topics
 - Especially building on experience of both production SOC's and those in process of deployment

SOC Hackathon (Late 2024)



- Initial planning already underway for next edition
- Aim for ~9 month cadence: split between once and twice a year
- Plan for next hackathon in November (avoiding December)
 - Looking for volunteers to host
- Identify soon work that the working group should engage with over the next months to provide best basis for workshop

Next steps



- Continuing theme of this work is identifying where a full-scale SOC is appropriate, versus a lightweight approach using something like pDNSSOC
- Goal for this year is to have clear guidance, infrastructure dependent
- Underlying driver continues to be the importance of threat intelligence
- People and processes are vital for a long term, full-scale SOC activity



Questions?