Cyber Security Monitoring for IHEP Data Centers

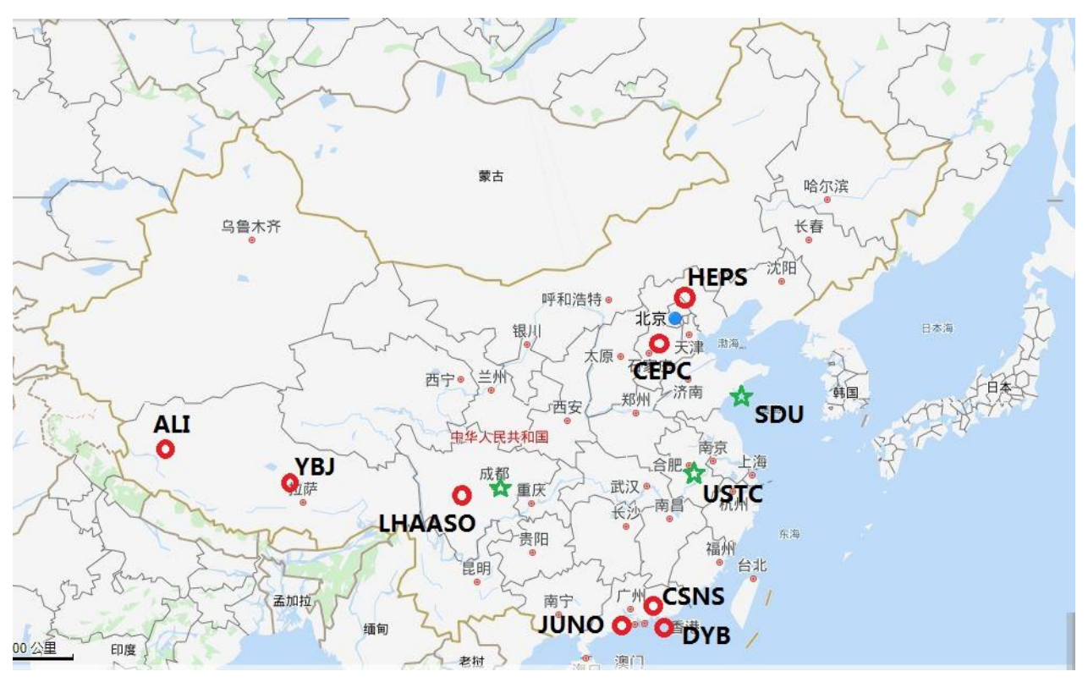
Tian Yan[1], Hao Hu[1], Dehai An[1], Fazhi Qi[1], Chen Jiang[2]

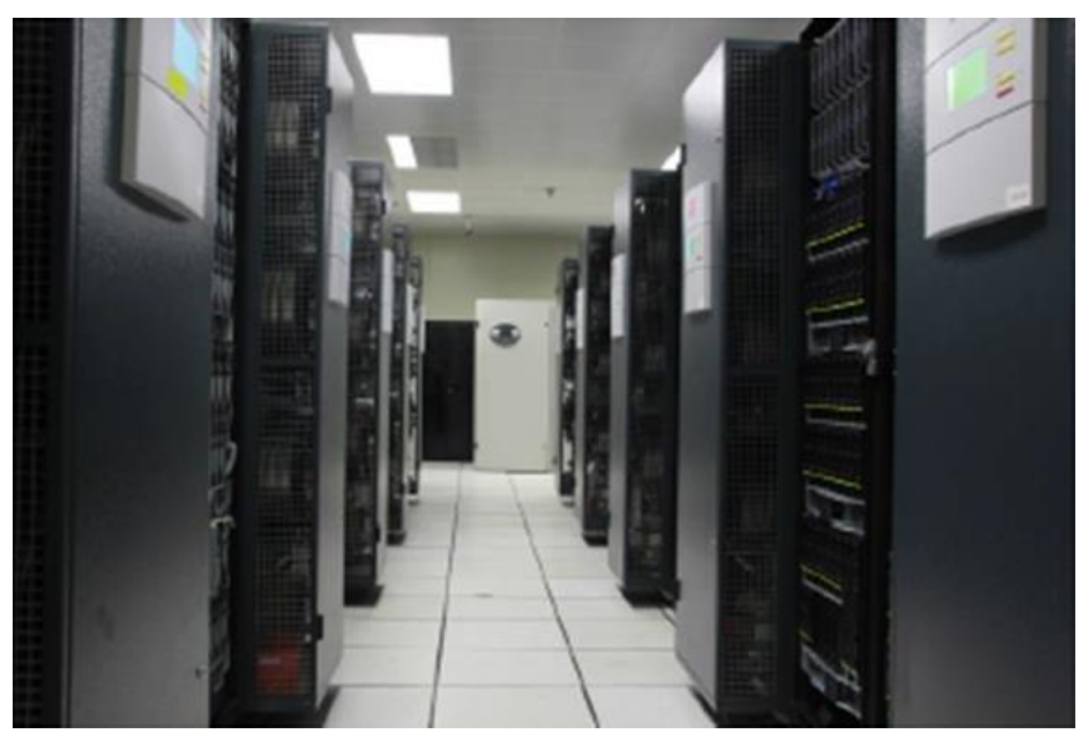
1. Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, P. R. China

2. Legendsec Information Technology (Beijing) Inc., Beijing 10085, P. R. China

IHEP Data Centers and Remote Sites

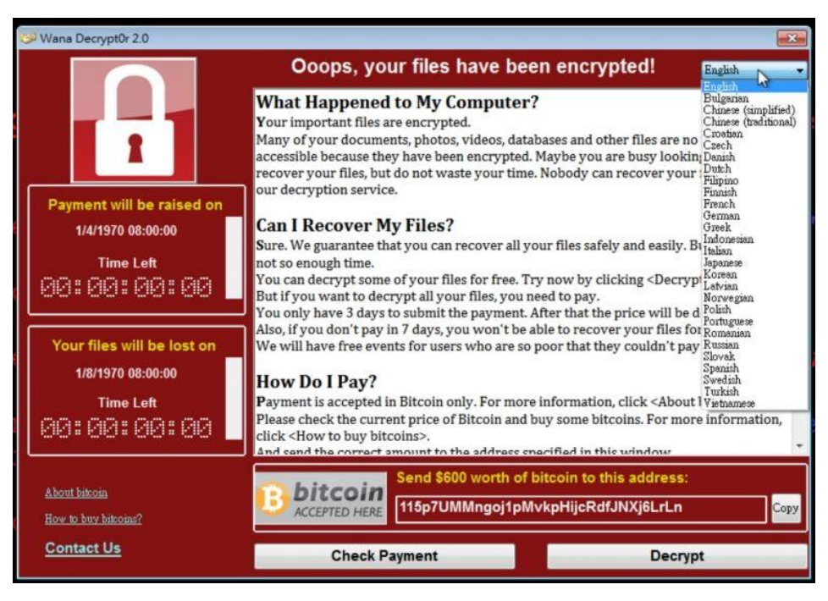
- Institute of High Energy Physics (IHEP), Chinese Academy of Sciences (CAS) is a national institute for fundamental researches in particle physics, particle astrophysics and cosmology.
- IHEP built and operates several large scientific facilities, such as BEPCII/BESIII, DYB, JUNO, HXMT, YBJ, LHAASO, CSNS, HEPS, etc.
- The red circles in the right map shows the location of remote facilities.
- IHEP has four data centers for data storage and processing, located in three cities. They totally have 850 square meter floor space, about 17k CPU cores and 20 PB storage.





Cyber Security Threats

- In recent years, along with the rapid development of large scientific facilities, various cyber security threats have becoming a noticeable challenge.
- The cyber security threat we faced recently:
  - ✓ intrusion
  - ✓ malware for mass scanning, DDoS attack, etc.
  - ✓ crypto-currency mining
  - ✓ ransomware
  - ✓ phishing
  - ✓ abuse of resources
  - ✓ violation of copyrights
  - ✓ attack third-party
- We have about 10 security events per year



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no
accessible because they have been encrypted. Maybe you are busy lookin
recover your files, but do not waste your time. Nobody can recover your
our decryption service.

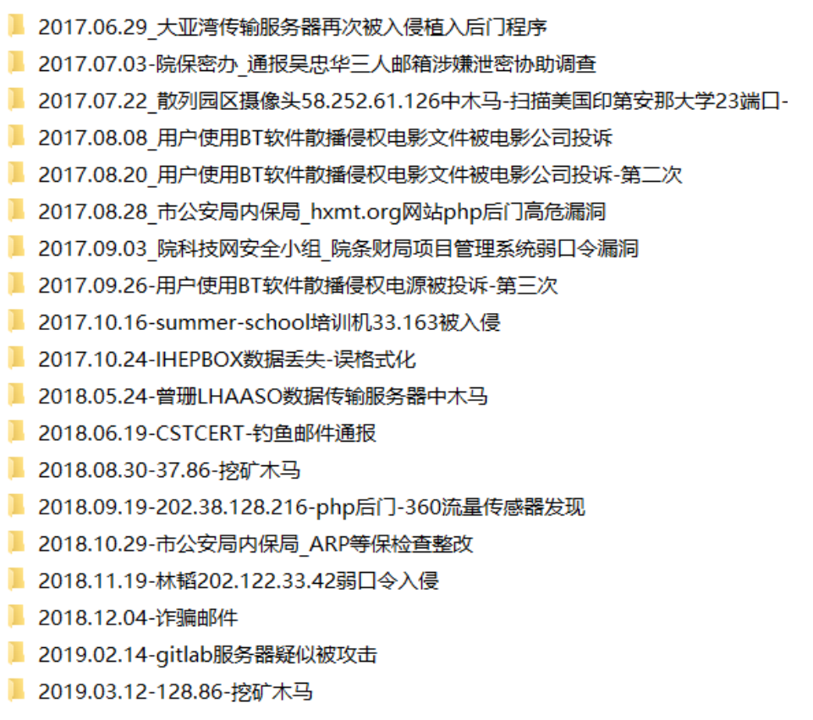
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. Bu
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be d
Also, if you don't pay in 7 days, you won't be able to recover your files for
We will have free events for users who are so poor that they couldn't pay

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About I
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

Payment will be raised on
1/4/1970 08:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 08:00:00
Time Left
00:00:00:00

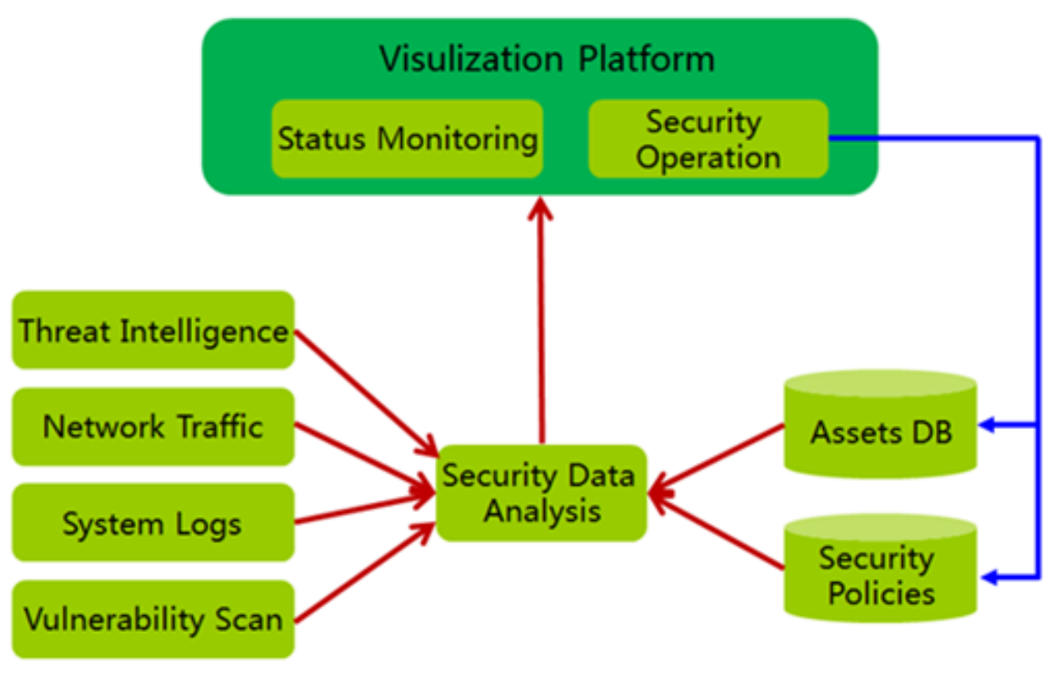
Send $600 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

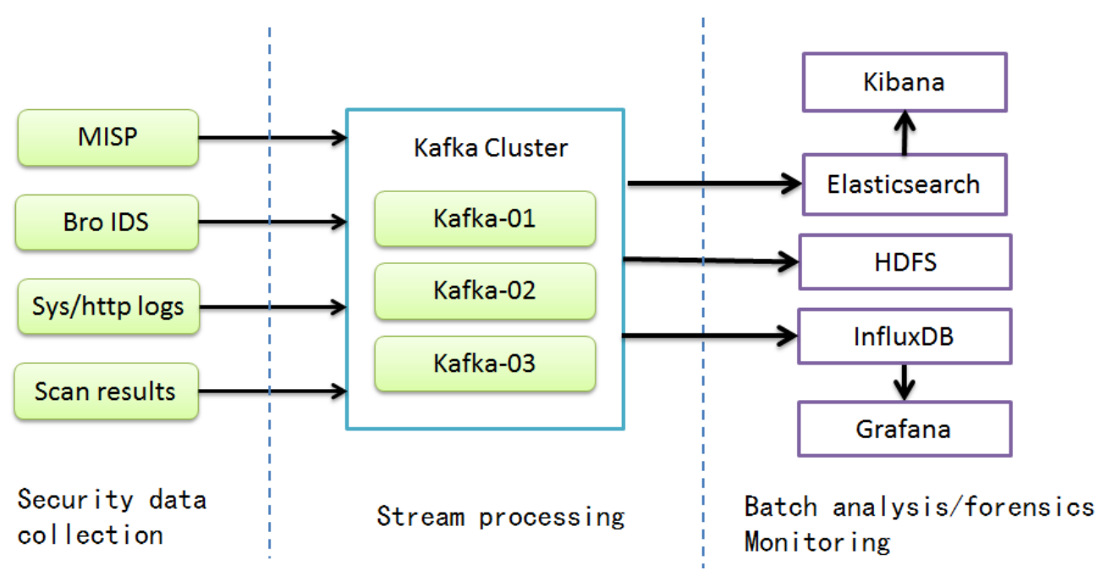


2017.06.29_大亚湾传输服务器再次被入侵植入后门程序
2017.07.03-院保密办_通报吴忠华三人邮箱涉嫌泄密协助调查
2017.07.22_散列园区摄像头58.252.61.126中木马-扫描美国印第安那大学23端口-
2017.08.08_用户使用BT软件散播侵权电影文件被电影公司投诉
2017.08.20_用户使用BT软件散播侵权电影文件被电影公司投诉-第二次
2017.08.28_市公安局内保局_hxmt.org网站php后门高危漏洞
2017.09.03_院科技网安全小组_院条财局项目管理系统弱口令漏洞
2017.09.26-用户使用BT软件散播侵权电源被投诉-第三次
2017.10.16-summer-school培训机33.163被入侵
2017.10.24-IHEPBOX数据丢失-误格式化
2018.05.24-曾珊LHAASO数据传输服务器中木马
2018.06.19-CSTCERT-钓鱼邮件通报
2018.08.30-37.86-挖矿木马
2018.09.19-202.38.128.216-php后门-360流量传感器发现
2018.10.29-市公安局内保局_ARP等保检查整改
2018.11.19-林韬202.122.33.42弱口令入侵
2018.12.04-诈骗邮件
2019.02.14-gitlab服务器疑似被攻击
2019.03.12-128.86-挖矿木马

Security Detecting and Monitoring

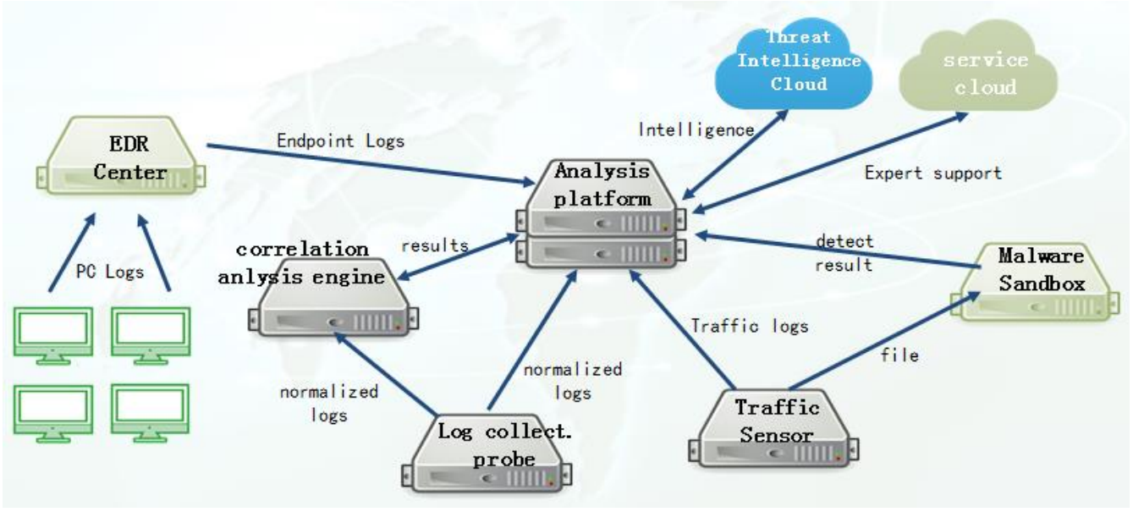
- The architecture of our cyber security detecting and monitoring system is shown in the right figure.
- The following security related data are collected and analyzed according to security policies and rules to find abnormality
  - ✓ threat intelligence
  - ✓ network traffic
  - ✓ system logs
  - ✓ vulnerability scan results
- The result of this data analysis is used in the visualization platform for security status monitoring, as well as used as input data for security operation.
- We take WLCG SOC as a reference to design a simple data analysis framework, shown in the right figure.

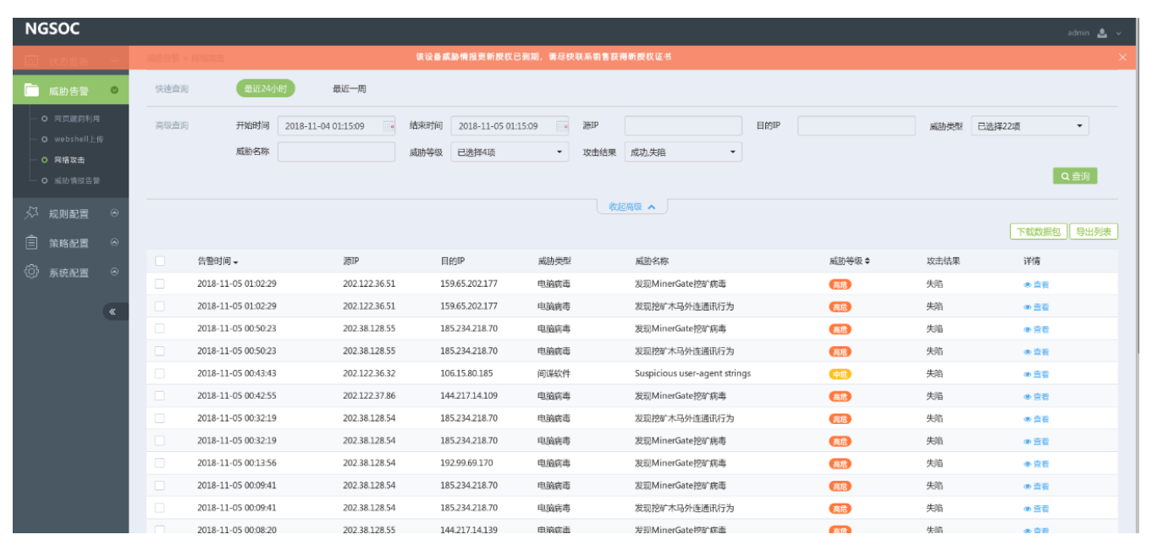


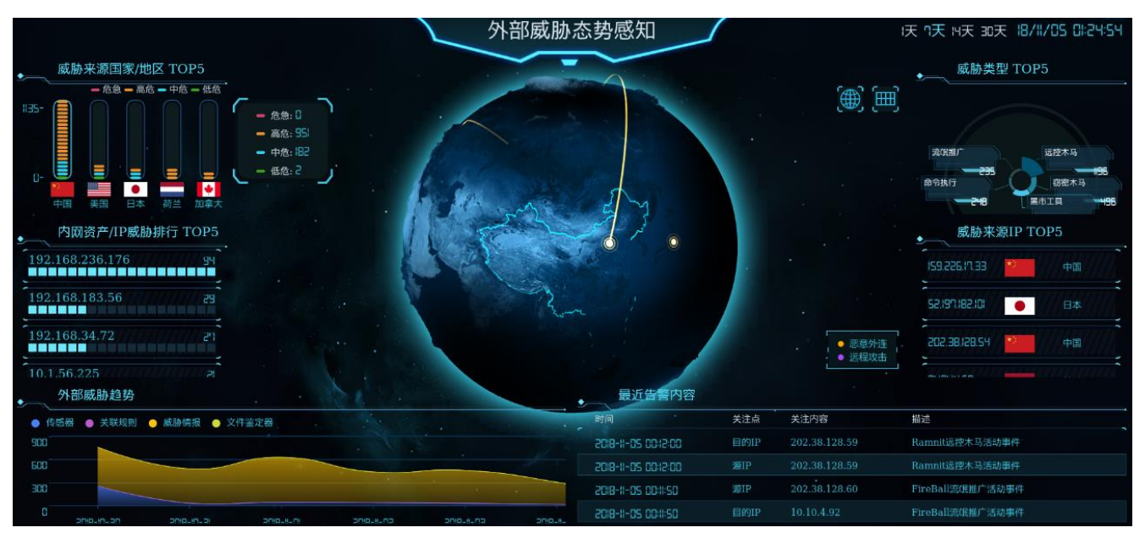


Working with Commercial SOC

- We can benefit from cross check of the results of open-source SOC and commercial SOC
- NGSOC is a commercial solution of SOC we chose to test, it is produced by Qi An Xin, which is a domestic security company in China
- Its major advantage is threat intelligence, Qi An Xin has 1300 PB security reference data.
- We start deploying and testing since Aug. 2018
- All the inbound/outbound traffic of IHEP data centers are taken as input data source
- It has already detected crypto-currency mining malware and web-shell in our servers
- The commercial SOC is easy to setup and maintain, but lack of flexibility.







Comparison between Two SOCs

- According to our experience of operating NGSOC and the open source MISP/Zeek based SOC, we found both of them have merits and demerits.
- Advantage of commercial SOC:
  - easier to setup, configure and maintain.
  - fantastic monitoring dashboard and easy-to-use web UI
  - more comprehensive and up-to-date threat intelligence
  - technical support from the provider
  - it is more friendly for non-expert users and these institutes which lack of manpower and experts on security.
- Advantage of open source SOC:
  - flexibility. The system can be customized to fit the special needs of different application scenarios.
  - Zeek has its only script language which can be used to writing new detecting patterns
  - can share intelligence between trusted academic institutions
  - we can store and handle the security data in our data center, we don't worry about the data leak.

The Monitoring Center

- To visualize the security threats and the security status we get from the SOCs, we deployed a large display in a dedicated monitoring room.
- It consists of 3x2 55 inch displays, as shown in the right figure.
- These 6 displays can be grouped in several ways to present different monitoring demands.

- If any questions and suggestions, please contact Tian Yan (yant@ihep.ac.cn).

中国科学院高能物理研究所
Institute of High Energy Physics
Chinese Academy of Sciences