Cloud Web Security Monitoring at IHEP

Tian Yan, Shan Zeng, Mengyao Qi, Qingbao Hu, Fazhi Qi

Computing Center, IHEP, CAS, China

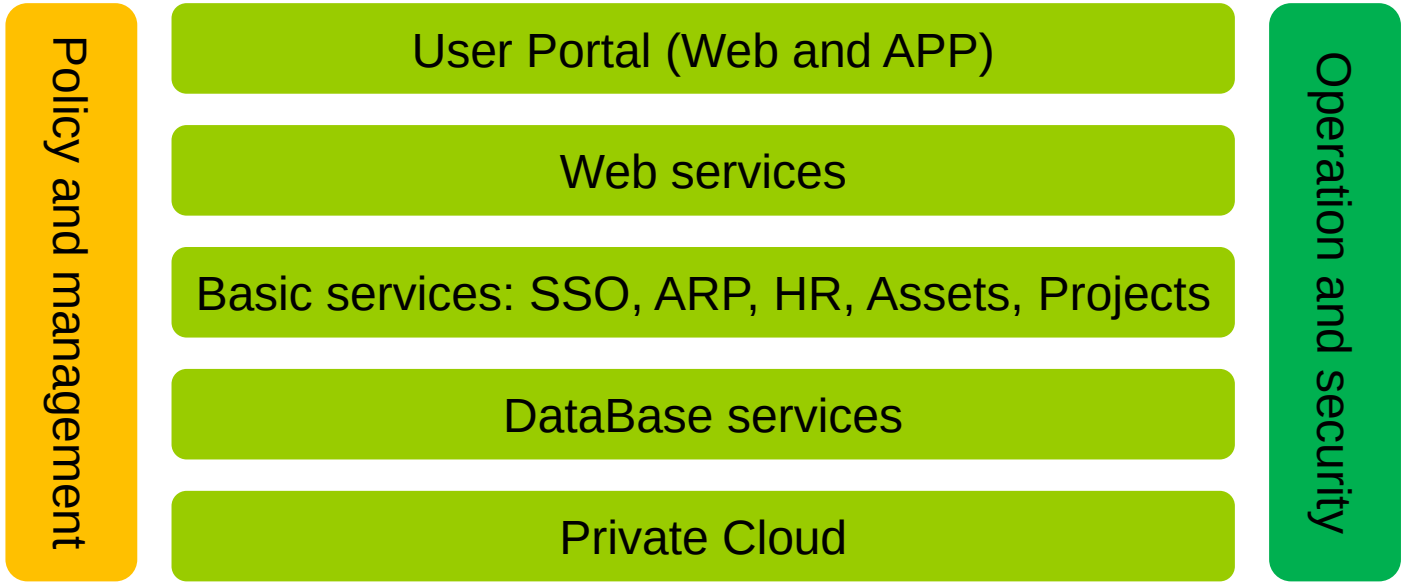
CHEP 2018, Sofia, Bulgaria, July 10th, 2018

Outline

- Introduction to IHEP private cloud for web services
- Cyber security threats
- Cyber security detection and monitoring system
- Summary

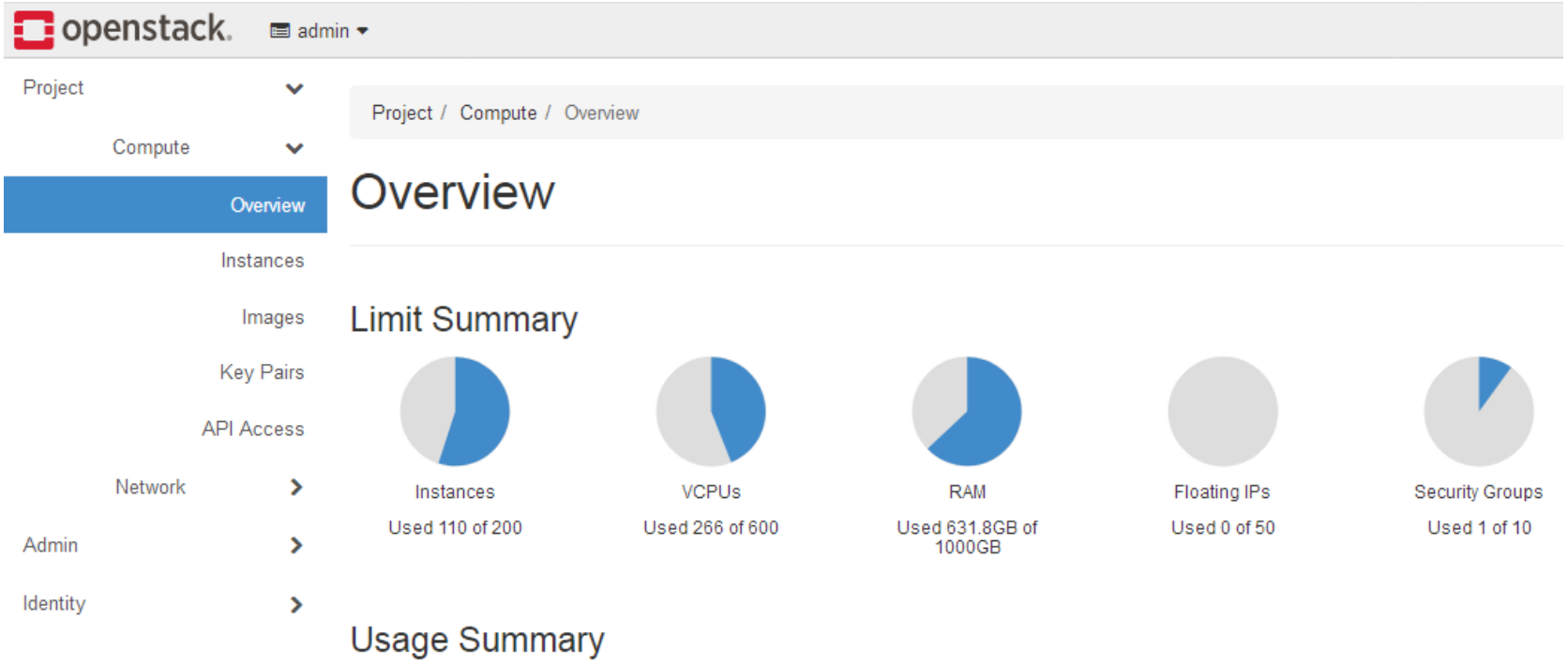
Web services at IHEP

- The IHEP computing center is responsible for
  - designing and deploying the public web services for all IHEP users
  - hosting web services designed and maintained by research groups
- Architecture are based on private cloud
  - old systems hosted by physical machines are migrating to cloud



IHEP private cloud for web services

- First deployed at 2013 with OpenStack Grizzly release
- Upgrade to Newton release at 2017
- Currently 110 virtual machines are running

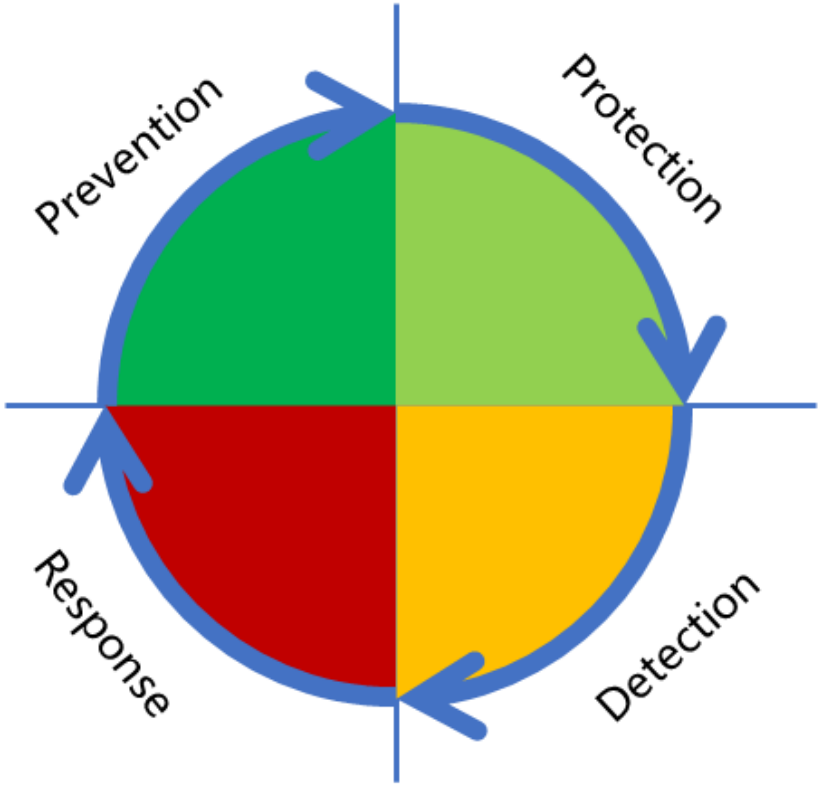


Cyber security threats

- The cyber security threats we faced recently:
  - intrusion
  - malware for mass scanning, DDoS attack, etc.
  - bitcoin minner
  - ransomware
  - attack third-party
  - webshell
  - …
- About 10 security events per year

Security risk control

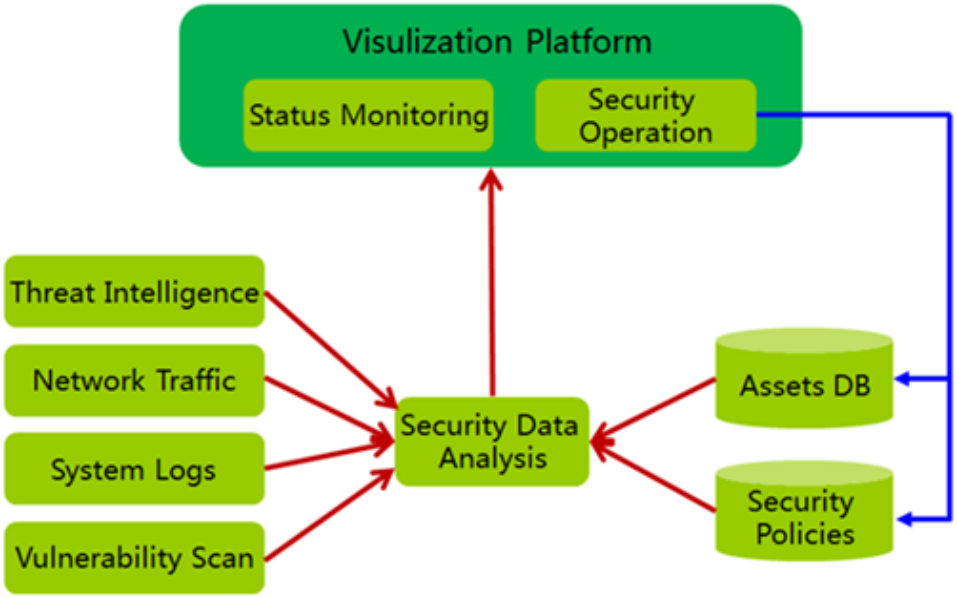
- Prevention
  - awareness & training
  - policy review
  - assessment and audit
- Protection
  - Firewall, WAF, etc
  - vulnerability scan and fix up
  - block malicious IPs
- Detection
  - traffic and logs analysis
  - threat intelligence
- Response
  - incident response



Cybersecurity Risk Control Model

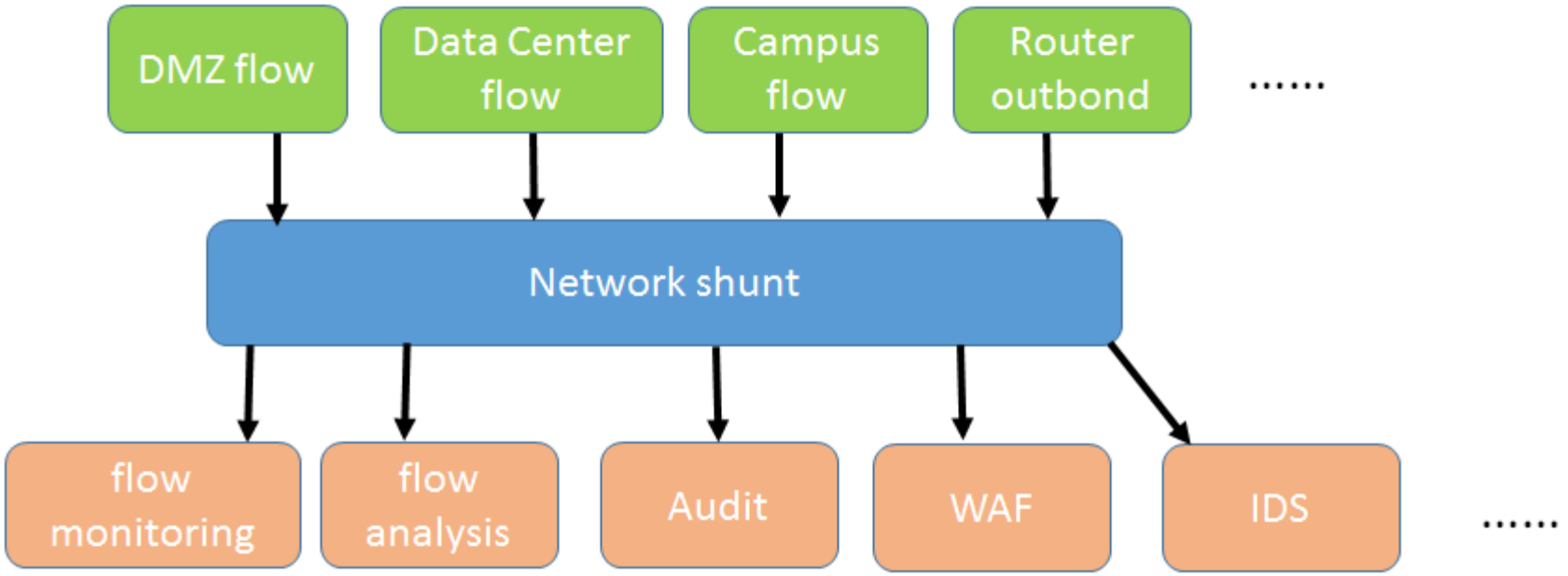
Detection and monitoring

- Security related data collection
  - network traffic
  - system logs
  - scan results
  - threat intelligence
- Analysis according to security policies and rules to find abnormality



Mirror network traffic

- Traffic from sub networks are mirrored by a network shunt
- Various monitoring/detection/analysis systems can be connected to the shunt, to get data as input source.
- We have a dedicated DMZ for cloud traffic



Bro IDS for traffic analysis

- Bro IDS (http://www.bro.org) is an opensource, flexible and powerfull tool for traffic analysis
- We deployed Bro at a physical machine with
  - 12 CPU cores
  - 64 GB memory
  - 8 TB disk capacity
  - 10 Gbps NICs

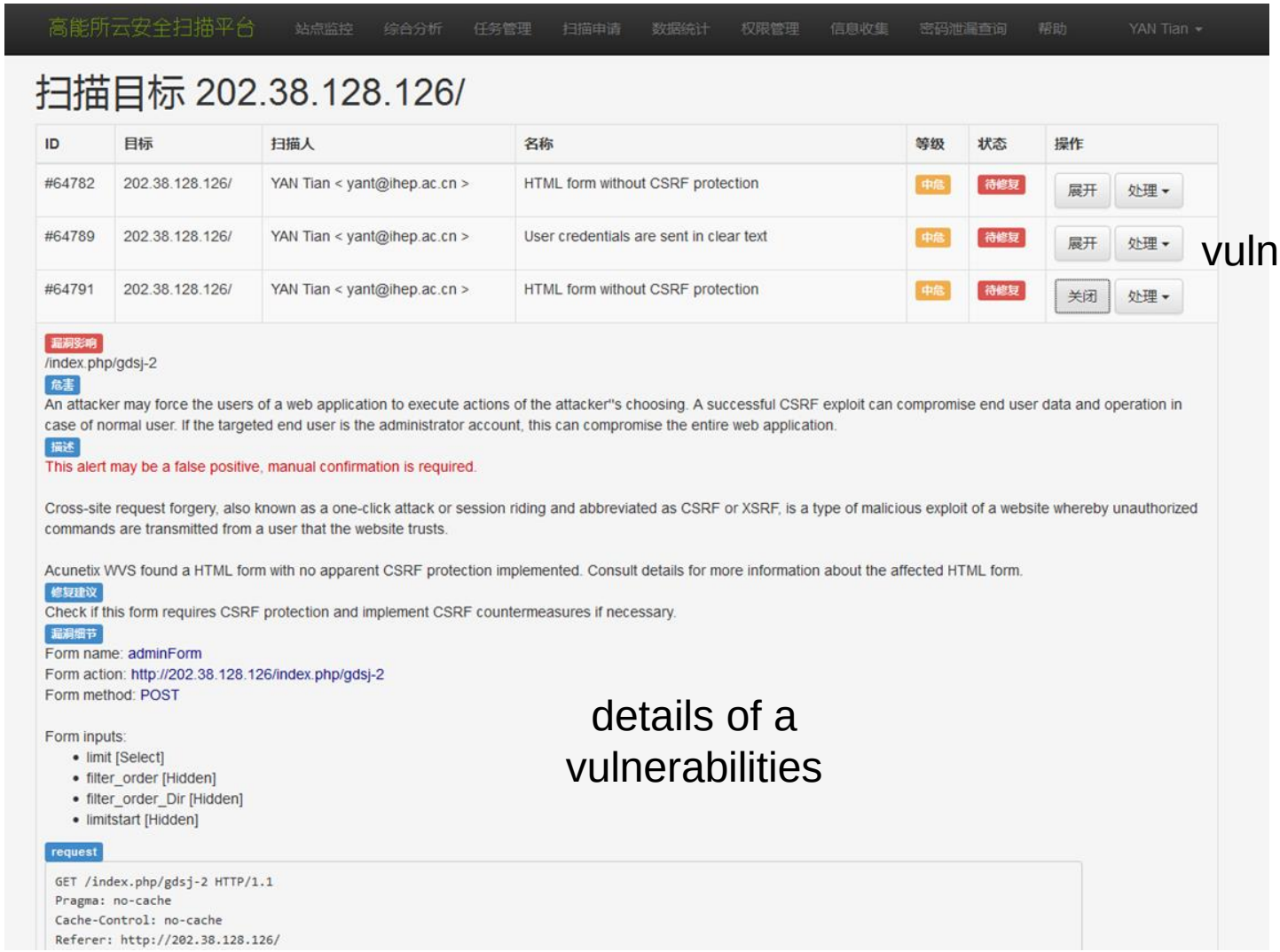
The Bro Network Security Monitor

```
[root@ndasectsgz ~]# broctl status
Name         Type    Host             Status    Pid    Started
logger       logger  localhost        running   16401  06 Feb 16:24:30
manager      manager localhost        running   16457  06 Feb 16:24:31
proxy-1      proxy   localhost        running   16535  06 Feb 16:24:33
worker-1-1   worker  localhost        running   16709  06 Feb 16:24:35
worker-1-2   worker  localhost        running   16711  06 Feb 16:24:35
worker-1-3   worker  localhost        running   16708  06 Feb 16:24:35
worker-1-4   worker  localhost        running   16710  06 Feb 16:24:35
worker-1-5   worker  localhost        running   16706  06 Feb 16:24:35
worker-1-6   worker  localhost        running   16707  06 Feb 16:24:35
worker-1-7   worker  localhost        running   16705  06 Feb 16:24:35
worker-1-8   worker  localhost        running   16702  06 Feb 16:24:35
worker-1-9   worker  localhost        running   16704  06 Feb 16:24:35
worker-1-10  worker  localhost        running   16703  06 Feb 16:24:35
[root@ndasectsgz ~]#
```

System and HTTP Logs

- System logs and HTTP logs can be collected after approval of system admins
  - /var/log/messages
  - /var/log/secure
  - /var/log/{wtmp,btmp}
  - /var/log/httpd/{access_log,error_log}
  - …
- Honeypot VMs are alse deployed to collect attack informations

Vulnerabilities scan results

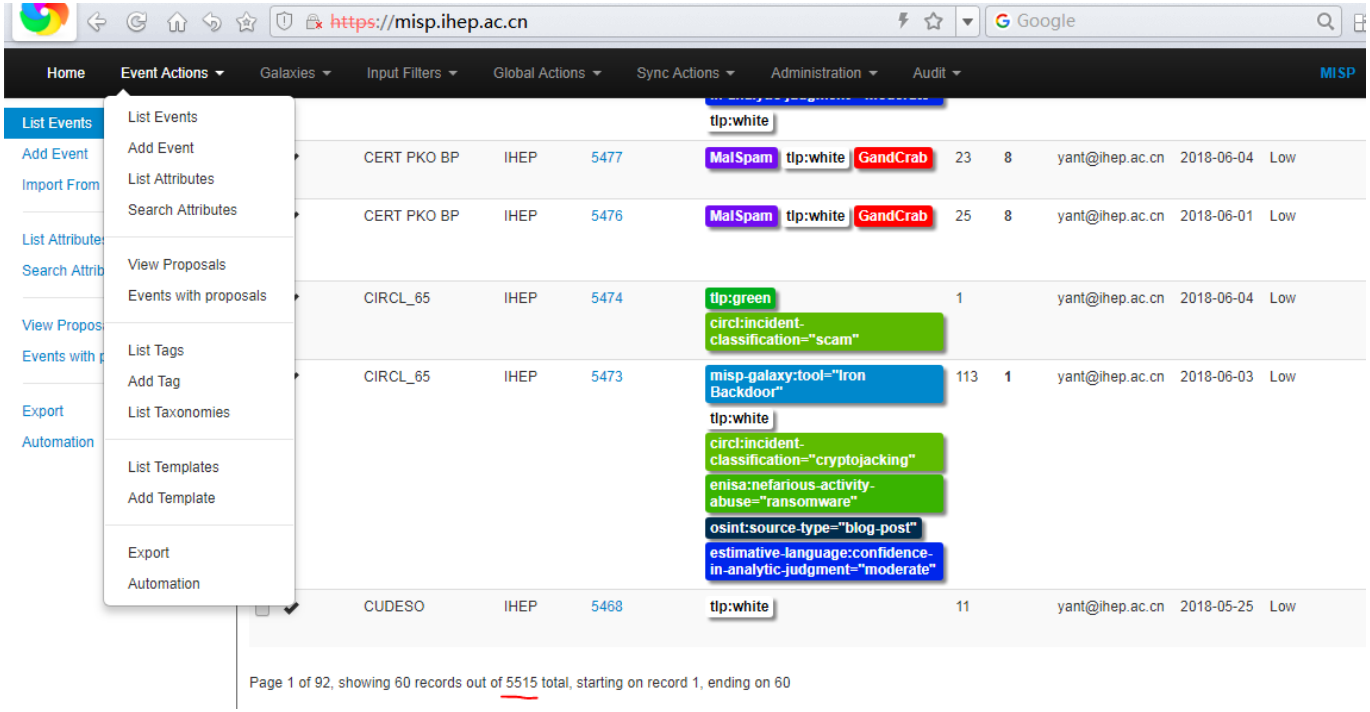


list of vulnerabilities

details of a vulnerabilities

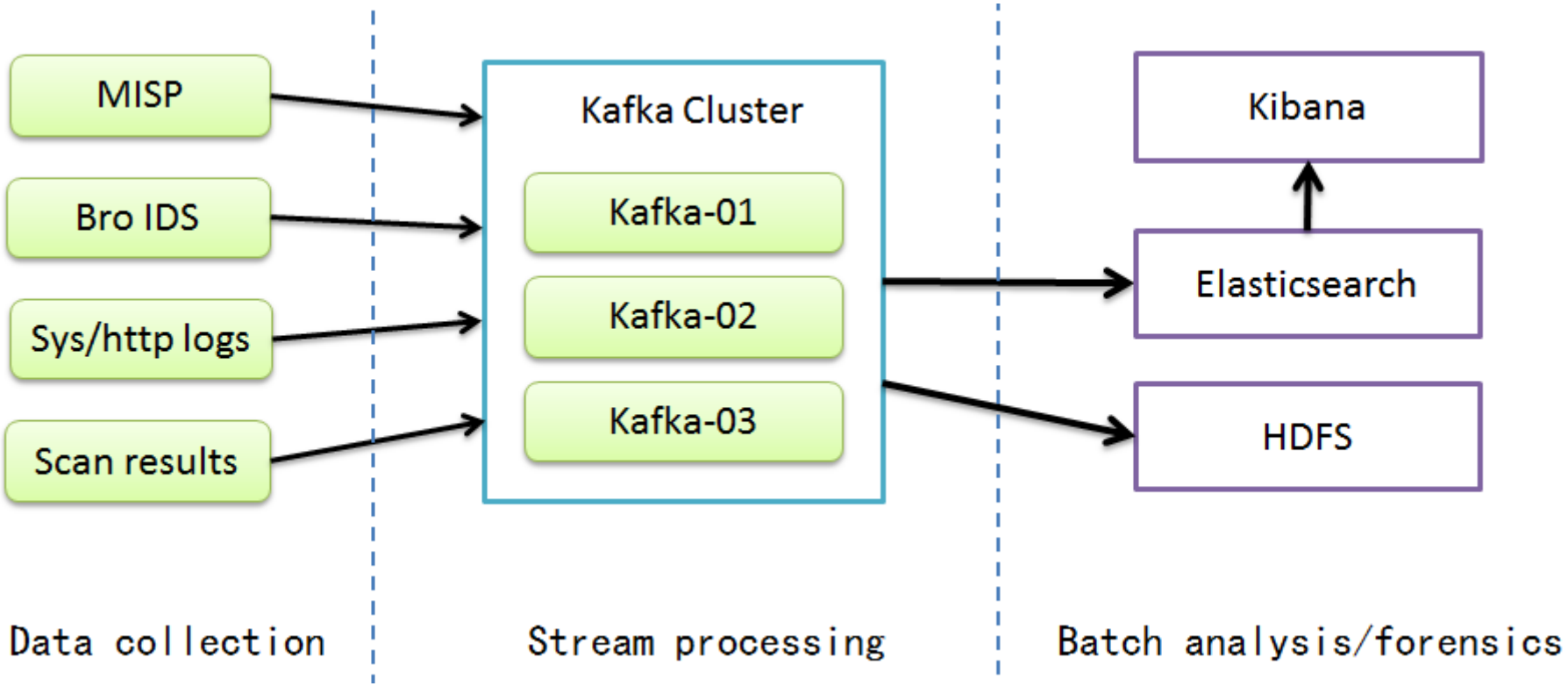
Threat Intelligence: MISP

- MISP: Malware Information Sharing Platform
  - http://www.misp-project.org/
- Sharing IoCs with WLCG MISP instance
  - currently 5500+ events



Data analysis

- Following CERN SOC architecture, we are deploying a simple security data anlysis framework



OSSIM Web UI for monitoring

- AlienVault open source SIEM (OSSIM) was deployed and we use its UI for monitoring
  - https://www.alienvault.com/products/ossim

Summary

- An brief introduction to IHEP private cloud for web services and it’s security status
- A prototype system for it’s security detection and monitoring is presented, which have already started to enhance the security of our web sevices.

Thanks

- Thank you very much for your attention!
- Q&A