Contribution ID: **537** Type: **Poster**

Cyber security monitoring for IHEP data centers

Thursday 7 November 2019 16:15 (15 minutes)

In recent years, along with the rapid development of large scientific facilities and e-science worldwide, various cyber security threats have becoming a noticeable challenge in many data centers for scientific research, such as DDoS attack, ransomware, crypto-currency mining, data leak, etc.

Intrusion and abnormality detection by collecting and analyzing security data is an important measure for enhancing the sensitivity of security status perception, level of security protection, and agility of security incident response. However, as the scale of data center growing, it's difficult to use a single security box to process the large volume of various data generated by network traffic, device and host logs, threat intelligence, and so on.

In high energy physics (HEP) community, people are trying to establish a security operation center (SOC) for handle this problem. We are also trying to build a cyber security monitoring and analysis framework at Institute of High Energy Physics (IHEP), Chinese Academy of Sciences. At IHEP, we have four data centers, located in three different cities in China, the largest one has 4x10 Gbps IPv4 and IPv6 dual-stacked internet connection, and 2x80 Gbps inner data center network. It's really a challenge for us to handle the security related data generated by such a set of information assets.

In this framework, Malware Information Sharing Platform (MISP) is deployed for threat intelligence exchanging with collaborated HEP institutes and universities. Network traffic is collected from switches and firewalls flows to a Zeek instance for traffic analysis. All the security data like Zeek logs, hosts/web logs, security device logs, along with vulnerability scanning results and assets detection results, etc., are are collected by Flume/Logstash/Syslog to a data pipeline named Kafka cluster. In this cluster, there are some Spark jobs running for stream processing, which are aimed at rapid intrusion and abnormality detection as well as data correlation and enrichment. Then all the processed data are written to Elasticsearch, MySQL and InfluxDB, and then visualized by Kibana and Grafana. Moreover, we also deployed a commercial SOC product for cross-checking, and we imported the threat intelligence data from the cloud of the product provider.

Consider for promotion

No

Authors: YAN, Tian (Institution of High Energy Physics, Chinese Academy of Science); Ms HU, Hao (IHEP); Mr AN, Dehai (IHEP); FAZHI, Qi (IHEP); Mr JIANG, Chen (Legendsec Information Technology (Beijing) Inc.,)

Presenter: FAZHI, Qi (IHEP)

Session Classification: Posters

Track Classification: Track 7 –Facilities, Clouds and Containers