Contribution ID: **37** Type: **Oral Presentation**

A comprehensive security operation center based on big data intelligent detection and threat intelligence sharing

Thursday, 25 March 2021 10:50 (20 minutes)

The continued growth of cybersecurity incidents calls for effective cybersecurity monitoring solutions. The operation of security operation centers (SOCs) is the recommended best practice to which large and medium-size enterprises rely for the detection, notification, and ultimately response to cybersecurity incidents. However, traditional SOCs using passive defense can not meet the current cybersecurity situation. In this talk, a comprehensive SOC is introduced which employs big data intelligent detection and threat intelligence sharing technology to detect and respond cybersecurity incidents rapidly and proactively. First, the SOC collects a wide variety of data including network traffic, server logs, security incidents, assets and vulnerability information. The collected data is stored in a big data storage platform for the following threat detection. Second, the SOC provides scalable cybersecurity incidents detection framework which can combine the detection performance of multiple detectors. Every detector can analyze behavior anomaly based on the data on the big data storage platform and multiple detectors can be correlated for further analysis. Third, the SOC can uniformly manage and respond the incidents identified from detection framework. At the same time, visualization is adopted to reveal the cybersecurity situation of entire enterprise. Besides, the SOC can share threat intelligence between multiple threat intelligence sharing instances and enrich threat intelligence by incorporating cybersecurity incidents from security incident response platform. The framework of SOC is referred to CERN and is customized to make it is practical and deployable for the Institute of High Energy Physics to discover, identify, understand, analyze, and respond to cybersecurity incidents from a global perspective.

Primary author: Dr JIARONG, Wang (IHEP)

Co-authors: Mr DEHAI, An (IHEP); Mr QI, Fazhi (Institute of High Energy Physics,CAS); Ms HU, Hao (Institute of High Energy Physics); Mrs LANXIN, Ma (IHEP); Dr YAN, Tian (IHEP)

Presenter: Dr JIARONG, Wang (IHEP)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations