Contribution ID: **18** Type: **Oral Presentation**

A distributed framework for security operation center in the application of Institute of High Energy Physics (Remote presentation)

Tuesday, 21 March 2023 16:30 (30 minutes)

Security operations center (SOC) frameworks standardize how SOCs approach their defense strategies. It helps manage and minimize cybersecurity risks and continuously improve operations. However, current most of SOC frameworks are designed as the centralized mode which serves for the single organization. These frameworks are hard to satisfy the security operations scenarios that must simultaneously protect several organizations from cyber threats across the wide area network in the synergistic way. In this paper, we propose the distributed security operation center (DSOC) that provides the distributed working mechanism for multiple organizations over the wide area network by combining the security probes. The organizations within the DSOC framework are highly collaborative and mutual trust. The security probes of DSOC are deployed in the different organizations and can parse the network traffic for the organizations by Zeek. Besides, the security probes collect data from these organizations and the collected data is transferred over wide area network to the data analysis center of the DSOC. Especially, the data communication between security probes and data analysis center is encrypted to ensure the data security of every organization. The data analysis center adopts rule-based, AI-based and threat intelligence-based algorithms to detect cyber-attacks. The detection results are input into the automated response module in the DSOC. The automated response module is the client-server structure and the client are installed in the security probe. The server of the automated response sends commands across the wide area network to the target client of the security probe to block the attackers quickly, and meanwhile the communication between client and server in the response processes is encrypted. In addition, the threat intelligence component of DSOC can aggregation intelligence from the organizations and easily share to all organizations based on the distributed security probes. The DSOC also builds the security situation awareness system that visuals the cyber threats of every organization and set the permission to view the security situation by using access control for every organization. The DSOC has been applied to institute of high energy physics (IHEP) and deployed in several collaborative large scientific facilities and scientific data centers since 2021. The excellent security protections are persistently provided to all organizations within the DSOC framework.

Primary authors: WANG, Jiarong (Institute of High Energy Physics); LIU, Junyi; SUN, Qianran; YAN, Tian; AN, Dehai

Presenter: WANG, Jiarong (Institute of High Energy Physics)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations