Contribution ID: **113** Type: **分会报告**

大装置和科学数据中心网络安全保障平台总体设计与实现

Sunday, 30 June 2024 16:15 (15 minutes)

国家重大科技基础设施是为探索未知世界、发现自然规律、实现技术变革提供极限研究手段的大型复杂科学研究装置（系统），是突破科学前沿、解决经济社会发展和国家安全重大科技问题的物质技术基础。由于大多数重大科技基础设施必须对国内外用户高度开放，使得依托重大科技基础设施开展的科研活动、应用研发等工作面临着包括工业控制安全、互联网安全以及数据安全等在内的多方面安全威胁。为了应对日益严重的网络安全威胁，保障重大科技基础设施及其科研活动的网络安全，建设面向重大科技基础设施的网络安全技术平台已经迫在眉睫。

本报告介绍大装置和科学数据中心网络安全保障平台总体设计与实现，该平台架构包括：安全数据采集层、安全数据预处理层、安全数据存储层、安全数据分析层、安全数据应用层和威胁情报层。安全数据采集层实现复杂多源异构安全类数据的采集，包含网络流量数据、日志数据、脆弱性数据以及资产数据等；安全数据预处理层实现数据的实时处理，包括安全数据解析、富化等；安全数据存储层利用大数据存储、关系数据库等平台实现多源异构安全类数据的存储；安全数据分析基于多源异构安全类数据，利用规则分析、统计分析、机器学习、深度学习、图学习等智能检测算法实现威胁建模、监测和发现；安全数据应用层利用可视化技术、自动化工作流程等方式，实现态势感知、事件处置响应、资产和漏洞管理等能力；威胁情报层通过自动采集、人工事件调查等方法和途径，实现威胁情报收集、应用和共享。以上的不同逻辑层之间通过联动协作，形成了安全威胁建模、安全信息感知、安全事件分析、安全事件预警及安全事件应急处置的一体化的网络安全技术平台，有效保障依托大装置和科学数据中心开展的科研活动、应用研发等业务可持续发展。

Summary

Primary author: Dr 王, 佳荣

Co-authors: Dr 颜, 田; Mr 安, 德海; Mr 郭, 超奇; Ms 刘, 🄵怡; Mr 许, 应衡; Mr 王, 嘉瑞; Mr 刘, 禹; Dr 齐, 法制

Presenter: Dr 王, 佳荣

Session Classification: 科研信息化管理与系统