奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

天眼在北京2022冬奥会的安全经验分享

孙伟 奇安信集团攻防BG解决方案经理

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

“APT”一定是冬奥会面对的首要网络安全威胁

天眼系统——在冬奥网络中看全、看清、看透APT攻击的“眼睛”

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

往届奥运会遭遇APT的安全警示

政治目的	经济目的	网络恐怖主义	个人情绪宣泄

- 奥运会全球瞩目，是一个国家向世界展示的绝佳契机，也因此成为一些网络黑客“炫技”的舞台。近几届奥运会中，黑客从未缺席。
- 从历届奥运会的网络攻击来看，黑客往往试图攻击网站、影响门票销售或制造政治影响，或中断直播网络，影响赛事直播；不法分子还利用虚假票务网站获取经济利益或用户信息。

Rio2016

2016年里约奥运会期间，政府和赞助商网站遭到APT攻击，大量数据泄露，卖假票、搞诈骗

PyeongChang 2018

2018年平昌冬奥会开幕期间，黑客攻击使得互联网和广播系统中断、奥运会网站瘫痪数小时、奥林匹克场馆周围的本地Wi-Fi短时无法使用，开幕式直播信号中断

TOKYO 2020

2020年东京奥运会期间，发生信息遭到窃取和泄露事件，开幕式前夕，发现伪装成为PDF图标的钓鱼恶意程序，试图钓鱼相关工作人员；截获了大量的网络攻击和钓鱼邮件。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥期间高级威胁建设面临的挑战

基础数据覆盖不全

冬奥云数据中心以及场馆面临网络数据数据覆盖不全问题，尤其缺少云内东西向流量

缺少安全补位能力

冬奥业务访问数据首先会经过基础安全设备FW、WAF等的流量过滤，但过滤完毕后缺少查漏补缺手段，一旦被突破即无法监测防御，导致缺少安全防御补位能力

未知威胁发现不足

面对冬奥各种业务访问传递的各类文件，缺乏有效检测流量中是否存在恶意文件，无法及时发现可能存在的未知威胁

缺少全量网络行为日志

缺少业务网络访问行为全量数据，会导致冬奥期间发生的安全事件分析缺少数据支撑，如果发生某些安全事件，将对溯源分析取证造成较大障碍

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥组委对网络安全总体的规划要求

- 规划中明确要求，冬奥组委信息技术网络、云基础设施以及信息系统执行等保三级标准；
- 规划中明确指出，冬奥会必须做好防护大规模、高强度、有组织网络攻击准备；
- 根据《北京2022年冬奥会和冬残奥会网络安全总体规划（2019-2022）》中重点任务要求，其中提到“网络流量监测”措施在应对攻击定位及防御处置工作起到的重要技术作用；

落实网络安全合规性要求。依据国家网络安全、个人信息保护等方面的法律法规和技术规范开展网络安全保障工作，确保建设合规、管理合规、使用合规、运维合规。北京冬奥组委信息技术网络、技术网络等网络、云基础设施、信息系统原则上执行网络安全保护等级的第三级标准。

国际体育赛事已经成为黑色产业和敌对势力的重点目标。历届奥运会都会遭受不同程度的网络攻击，北京冬奥会必须提前谋划，做好应对大规模、高强度、有组织网络攻击的准备。

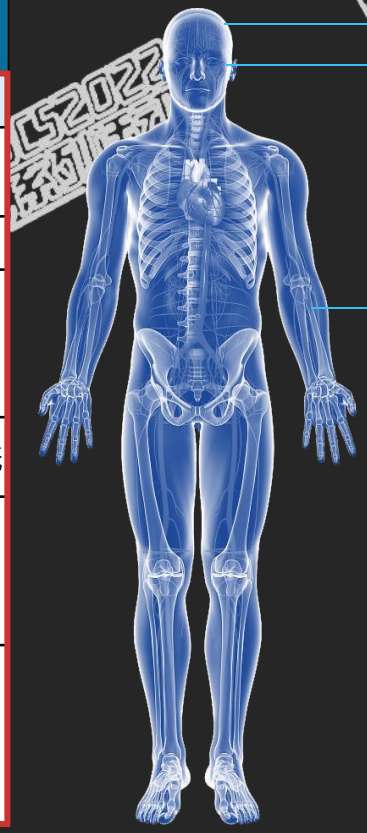
（1）北京冬奥组委信息技术网络。承载奥林匹克赛事管理、奥林匹克数据分发、北京冬奥组委日常办公等业务应用，覆盖机关办公区、延庆运行中心、张家口运行中心和各奥运场馆，划分竞赛服务、日常办公等多个网络域。网络安全保护等级为第三级，重点做好信息化资产管理、网络边界防护、网络准入和访问控制、网络行为管控、网络流量监测和日志审计等安全措施，对攻击源进行定位、对攻击行为进行阻断，实施对 DDoS、DNS 挟持、渗透等互联网攻击的防御与处置工作。网络安全状态由北京冬奥组委网络安全态势感知平台统一监控。

天眼在冬奥实战化态势感知中的定位

- 冬奥期间，天眼系统针对全网、云平台的流量采集、检测和分析，实时生产告警，追求“纤毫必现”；
- 流量异常是发现威胁最快的检测方式。天眼系统对全网流量数据进行分析，第一时间发现异常行为，形成告警，并同步到运营态势感知，供安全运营人员分析和研判；
- 天眼也会对流量进行分析，和运营态势感知不同的是，天眼主要基于机器的大数据分析，不太依赖于人工。

“三合一”实战化态势感知在冬奥/冬残奥会中的部署

	监管态势感知	运营态势感知	攻防态势感知
对应产品	网络安全态势感知与协调指挥平台	态势感知与安全运营平台（NGSOC）	新一代安全感知系统（天眼）
扮演角色	**大脑**	**躯干**	**眼睛**
应用场景	奥运安全监控中心等	奥运安全监控中心	2个网络中心、2个云数据中心、12个竞赛场馆、21个非竞赛场馆、以及场外合作伙伴
主要使用者	央办、奥组委领导、管理人员	安全运营人员	自动化检测分析、对人依赖较低
采集和处理数据	依托大禹平台、汇集包括运营态势感知提交的高危告警、安全事件、通告等数据	各设备、系统的网络安全日志和系统日志；来自攻防类态势感知同步的告警	全网、云平台的流量
主要职责	向上汇报报告、支撑决策；向下发布通告、助力指挥调度	支撑“持续监测-通报预警-分析研判-快速处置-态势感知-追踪溯源”的安全闭环运行体系	发现威胁、联动响应与拦截



大脑：网络安全态势感知与协调指挥平台

眼睛：新一代安全感知系统（天眼）

“看清、看透、看全”，更加贴近一线，第一时间“看到”威胁

躯干：态势感知与安全运营平台

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

天眼在冬奥零事故中发挥的作用效果

冬奥期间，天眼系统作为“三合一”实战化态势感知（指挥态势、运营态势、攻防态势）重要组成部分，结合“运营态势”、“指挥态势” 实现”三级态势建设”在大型项目中首次成功落地实践。

1.覆盖云数据中心及场馆全区域	2.解决云数据中心监控盲区	3.APT、未知威胁、高级定向攻击发现	4.安全事件溯源取证	5.支撑能力输出
天眼全流量采集覆盖冬奥全网2个云数据中心、2个网络中心及33个场馆的网络流量	天眼采集冬奥云数据中心东西向、南北向全流量原始网络流量数据，实现对云上全网安全监控不留盲区	天眼对冬奥全量网络数据检测分析，深度挖掘及行为分析，利用威胁情报、机器学习规则、静动态沙箱等检测技术，主动发现APT攻击、未知威胁、高级定向攻击等安全威胁	天眼基于全流量原始数据，经过深度数据包协议字段解析提取，形成完整的网络访问日志数据，补充解决了云上系统日志、审计日志信息方面的不足问题	天眼告警数据按需外发冬奥集中监控平台，提供能力输出，实现冬奥网络基础设施威胁一体化监测

攻防态势感知(天眼)

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

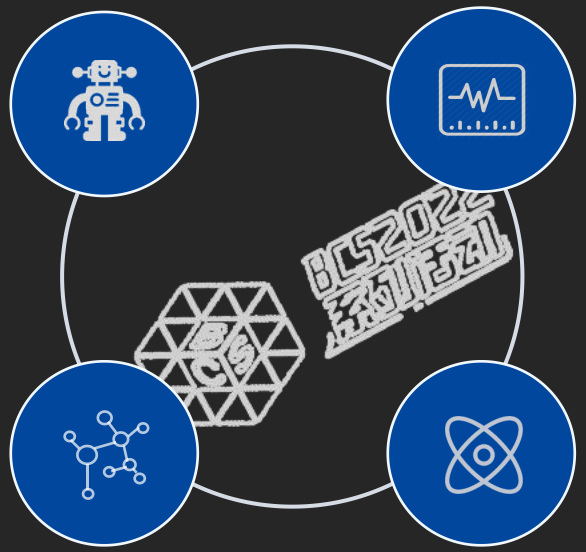
天眼在冬奥中应用的关键安全技术

智能机器学习引擎检测技术

基于天眼自主研发的QNA威胁检测引擎，采用200多种协议解码+DPI、NBT机器学习、 SQLparser、webshell沙箱等底层检测技术，流式检测、精准告警；

全量详实网络流量日志数据

天眼基于全流量原始数据，经过深度数据包协议字段解析提取，生成全量且完备的网络日志数据，这些数据提供系统日志缺少的关键字段信息，尤其涉及严重影响威胁分析的字段；



动静态结合的未知恶意文件检测分析

采用虚拟环境模拟方法，利用动静态结合检测分析技术，全面分析恶意代码恶意行为，细粒度检测漏洞利用和恶意行为，深度动态分析环境多达40种以上；

攻击线索图形分析定位技术

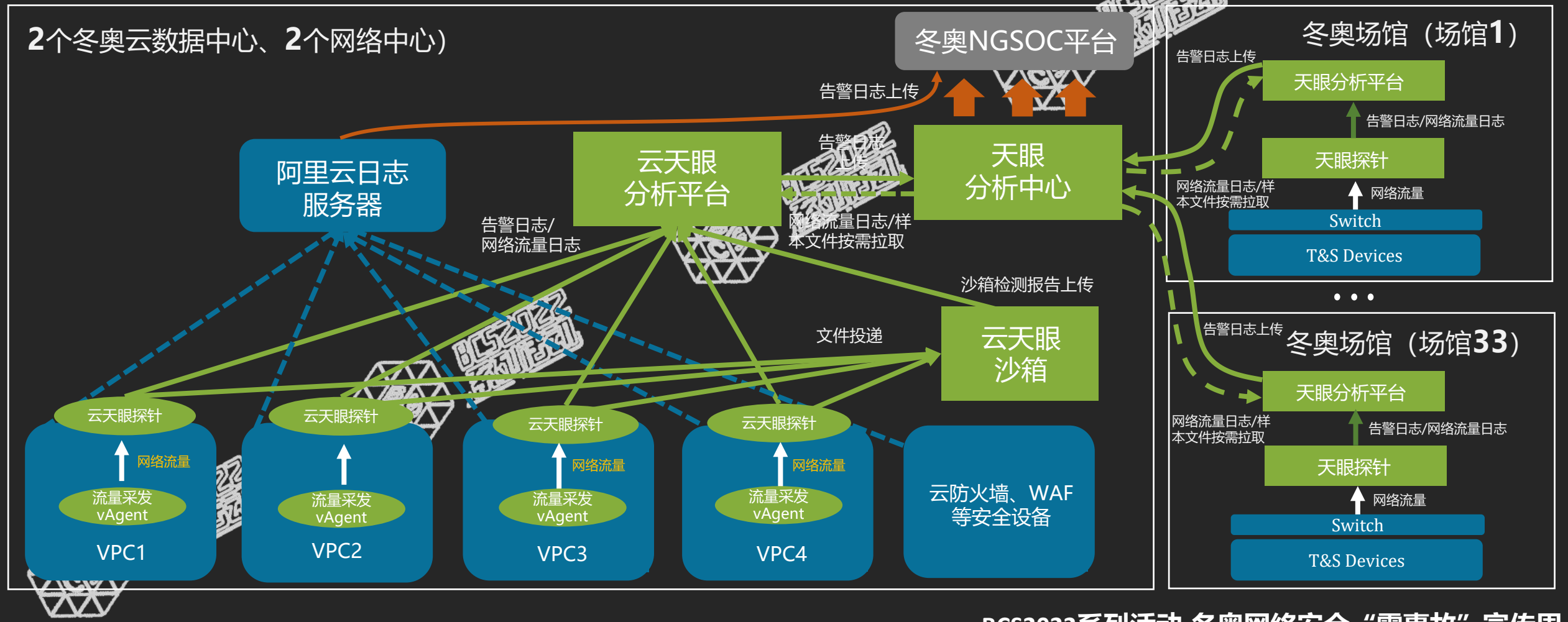
针对未知威胁的分析和挖掘，天眼基于多起点、多维度的威胁狩猎拓线，利用内置ATT&CK模型助力威胁感知提升，更加精确、快速发现和定位攻击者非法活动与攻击阶段。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

天眼在冬奥中的逻辑运行架构

- 冬奥云数据中心云主机侧安全部署流量采发vAgent并采集封装网络流量输出至云天眼探针，云天眼探针对原始流量集中预处理、检测、分析，产生告警日志、网络流量日志上传云天眼分析平台。最后告警日志统一上传天眼分析中心，由天眼分析中心集中上传告警至冬奥NGSOC平台；其中天眼分析中心会按需拉取各分析平台网络流量日志或样本文件；
- 云天眼探针从网络流量中还原提取文件，将文件投递至云天沙箱中执行静动态检测，执行结果检测报告上传云天眼分析平台；



奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

天眼在冬奥中取得的成绩

BCS2022系列活动

实时主动告警，持续威胁发现

自动检测发现威胁，自动上报，降低对人依赖度

全网流量采集处理，为监测分析提供数据支撑

存储处理流量日志数(条) 1074亿	
发现威胁告警数 5,008,746个	发现恶意样本数 54个
发现推进修复漏洞数 9,135个	发现APT组织攻击嗅探 28,790次
网内APT攻击告警 0个	流量覆盖范围 冬奥全网 （2个云数据中心东西向/南北向流量、2个网络中心、12个竞赛场馆、21个非竞赛场馆等）

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥背后故事：天眼为何能在冬奥上云？

1.冬奥云数据中心初建期，天眼不在安全规划内

冬奥云数据中心建设初期在顶层设计规划方案里设计了一整套安全规划，甚至为此专门开发了一套云上威胁监测分析(SIME)系统

2.多轮奥组委专家技术评审讨论

围绕云上威胁监测分析(SIME)系统是否已具备了高级威胁检测能力？是否还需要天眼上云部署？冬奥组委组织了多轮专家技术评审

3.天眼上云最终通过专家技术评审

经过多轮评审，最终冬奥组委经过质询和讨论形成的意见：

“天眼就像摄像头，能持续录制犯罪过程，警察查看的时候随时可以回放，而防火墙、WAF等安全设备是相机，只能记录某个时刻，单靠日志分析还是不够。”

“日志和流量采集、分析对于网络安全防护十分必要，两者各有所长，互为补充，无法相互替代。”

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周