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

冬奥实战化安全运行之威胁运营服务

初雪峰　冬奥项目组网络安全监控经理

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

运营目标

所有威胁可监测、可溯源、可处置

发现攻击	攻击结果	攻击溯源（内部）	攻击应对	攻击预防	攻击定性
多种手段发现攻击 1、安全设备、基础日志（终端侧、流量侧、服务器侧、IT设施审计日志） 2、威胁情报/通告 3、威胁狩猎	验证攻击是否成功？ 1、日志 99% 2、人工验证 1%	怎么打进来的？对我造成了哪些影响？影响范围？ 日志	是否要启动应急？业务是否需要恢复？还是只是封堵攻击IP？后续监测及防护措施？	1、通告 2、脆弱性检查	谁攻击了我？攻击组织？是否针对性？是否需要特别关注？

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

运营难点

01 如何保证监测的全，所有攻击都能感知到

02 如何保证所有攻击都能得到验证，可以溯源原因及影响

03 如何保障所有告警可以快速监测处置，不遗漏

04 如何保证攻击成功之后能够快速将影响降到最低

05 如何做到对所有攻击者能形成定性结论

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

全日志接入

PDC/SDC

阿里云
云主机、云安全中心、WAF、云防火墙、OSS、NAS、
应用系统等

流量探针
流量分析平台

日志

场馆...

防火墙，流量探针，IDS，交换机，终端设备等

日志

PNC/SNC

安全监控平台

1. 接入安全日志、告警日志、审计日志、应用系统日志
2. 接入主机资产、网络资产、终端资产数据
3. 基于攻防场景驱动数据质量优化：接入终端进程日志、DNS解析日志、终端security日志等。

日志

安全监测
防火墙、WAF、上网行为管理 、漏洞扫描、资产探查系统、流量分析平台、流量探针、文件沙箱、SOAR、锡安平台等

终端安全
天擎、EDR、椒图、虚拟化、身份签发服务器、准入控制台服务器、天狗、Linux主机、Windows终端

网关设备
负载均衡、堡垒机、蜜罐、SWG代理服务器、SDWAN管理中心、SDWAN中心节点、IPSEC VPN、SSL VPN、密码机、SMAC防火墙统一管理平台、堡垒机统一管理平台、流量解密防火墙等

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

攻击视角验证

通过攻击检验告警的准确性、规则的有效性、系统和防护设备等数据源的完整性

- 实战攻防演习检验告警规则
- 渗透测试检验告警规则
- 应急处置检验溯源数据
- 攻击人员从攻击视角挑战告警规则、日志完整性

制度、流程、技术

- 集中化运行
  - 监控岗、研判岗、专家岗使用统一平台进行事件研判，便于事件快速扭转
  - 数据完整度高，研判分析更便捷
- 每条告警定位到岗
  - 每个安全岗位人员定岗定责
  - 每条平台产生的告警都能精确到具体监测、分析的责任人，责任边界清晰
- 建模规则优化
  - 将平台告警量降到每人每天可分析的数量

奇安信

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

建设安全铺垫

01

能找到

资产清晰，所有受害IP可快速定位部门及责任人

02

能控制

所有入网终端/服务器部署天擎/椒图，可快速下发查杀及进行一键隔离

03

能封堵

部署有防火墙统一策略管控，可从网络层快速掐断攻击联系

04

能恢复

有充足的安全应急预案，并且各业务备有各自的应急预案

奇安信

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

专家团队支撑

- 样本分析
- 威胁情报
- 白泽

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

运行态网络安全岗位设置

网络安全值班经理

网络安全值班副经理

网络安全运维(经理)

- 安全网关类设备运维岗
- 服务器安全软件运维岗
- 终端安全软件运维岗
- IAM&KMC运维岗
- 安全平台类运维岗

网络安全监控(经理)

- 终端安全监控岗
- 服务器安全监控岗
- 应用安全监控岗
- 网络安全态势监控岗

- 分析研判岗
  （威胁、日志）

复用

网络安全专家(现场)

- 技术评估
- 威胁狩猎

复用

网络安全应急(主管)

- 事件分析研判
- 事件应急处置

网络安全专家
(外部)

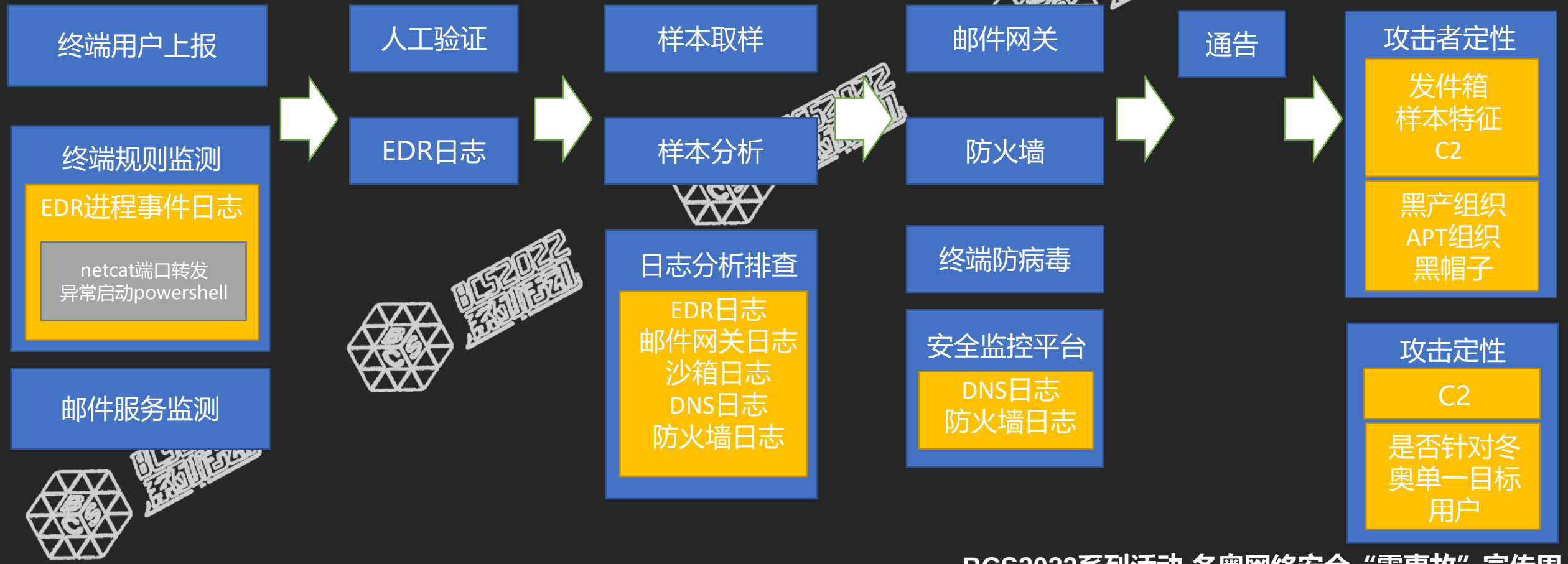
- 样本分析专家
- 威胁情报专家
- 安全分析师

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

运营场景

- 钓鱼邮件

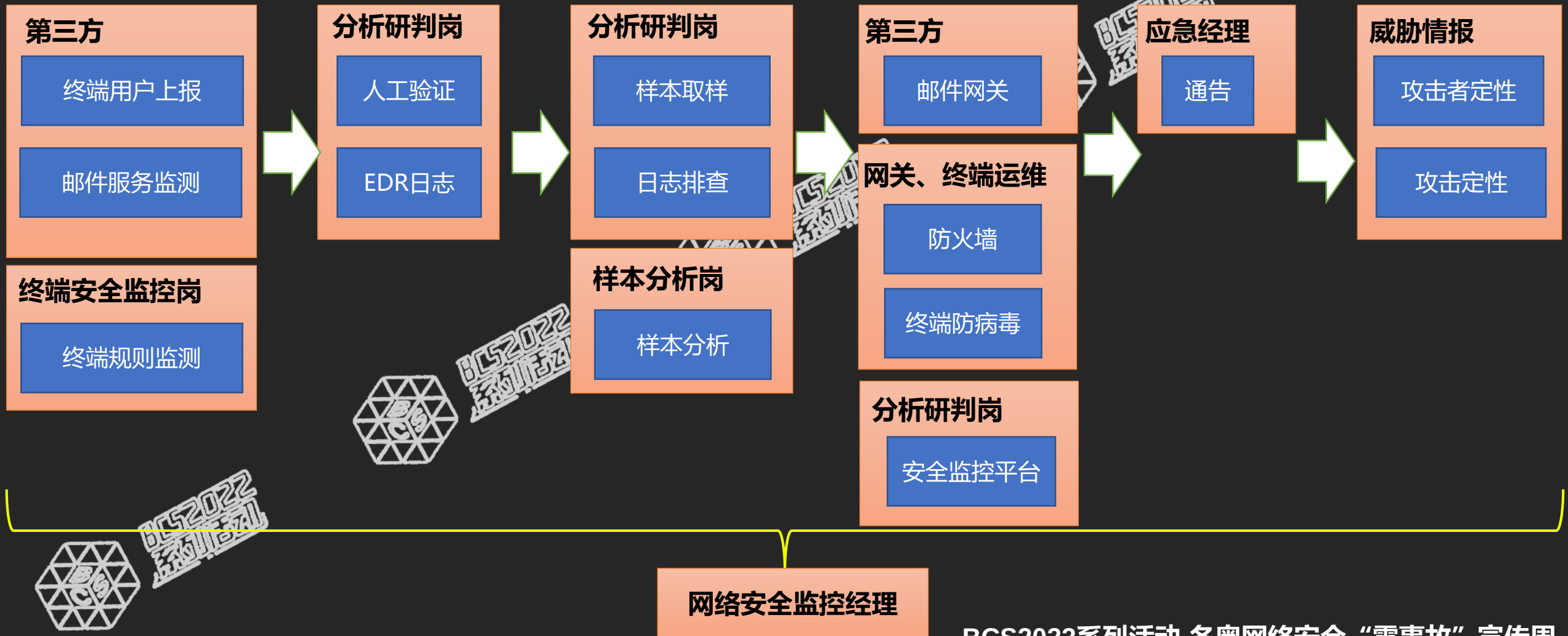
邮件服务为云端SAAS服务，所以在发现钓鱼邮件攻击层面，会稍显滞后性



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

运营场景

- 钓鱼邮件-岗位及流程扭转



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

THANKS