奇安信

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

建设银行网络安全防护体系演进及威胁情报探索应用

陈德锋 中国建设银行

网络攻击成全球第三大威胁

网络攻击成为全球仅次于“极端天气”和“自然灾害”的**第三大威胁**。根据世界经济论坛（WEF）发布的《2018年全球风险报告》显示，全球经济正在渐渐恢复，但**网络安全风险**在进一步升级。

电信诈骗成为社会新公害

根据2019年“猎网平台”数据显示，网络诈骗从业人数超过160**万**人，诈骗“年产值”达到1152**亿**元，成为继赌博、色情产业之后，中国的**第三大黑色产业**，甚至成为一些地区的“支柱性产业”。

数据泄露风险大幅提高

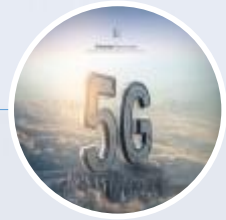
2018年全球总共泄露数据达**50亿**条，是2017年的**2倍**，2016年的**10倍**；

2019年仅一季度泄露数据已达**45.3亿条**，接近**2018年总量**。地下数据产业成为庞大的灰色产业链。

银行面临安全威胁的原因

全面线上化

银行业整体“电子渠道替代柜面业务量”达到90%以上。



金融场景化

金融服务深度融入场景是未来金融发展方向。

服务智能化

服务手段越来越智能，服务主体越来越智能。

建设银行安全防护体系演进历程

被动防御加固阶段


NAS
DMZ
ACL
Executive
VA
PDC
BDC
EMAIL
DNS
CRM
SAN
NAS
SAN
ACL
ANTI
Data Center
ACL
Research & Development
Financial

智能主动防御阶段

SAAS (Security as a Service)

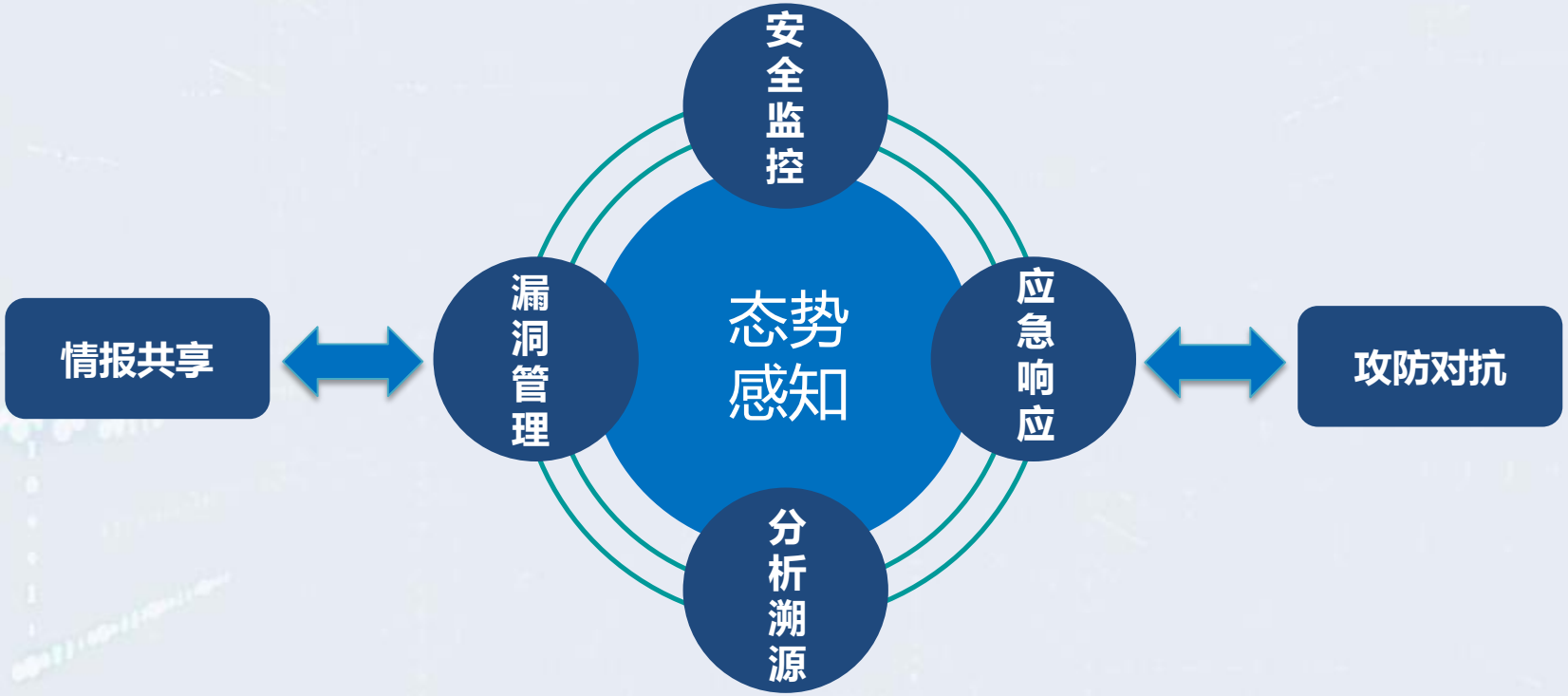
安全 即 服务

- 覆盖全部对象
- 应对全部威胁
- 提供全面防护

- 安全平台可扩展
- 安全功能组件化
- 安全服务可定制

- 集中安全服务
- 集中策略管理

主动对抗智能运营阶段



建设银行威胁情报应用框架

溯源分析

结合安全分析中心监测的本地数据提供情报关联，实现虚实映射，定位同源攻击、挖掘虚拟身份等

主动防御

利用外部情报，主动采取防护措施，降低外部入侵风险。

策略联动

实现情报数据的与安全防护设备的实时联动，提高威胁检测和防护能力。

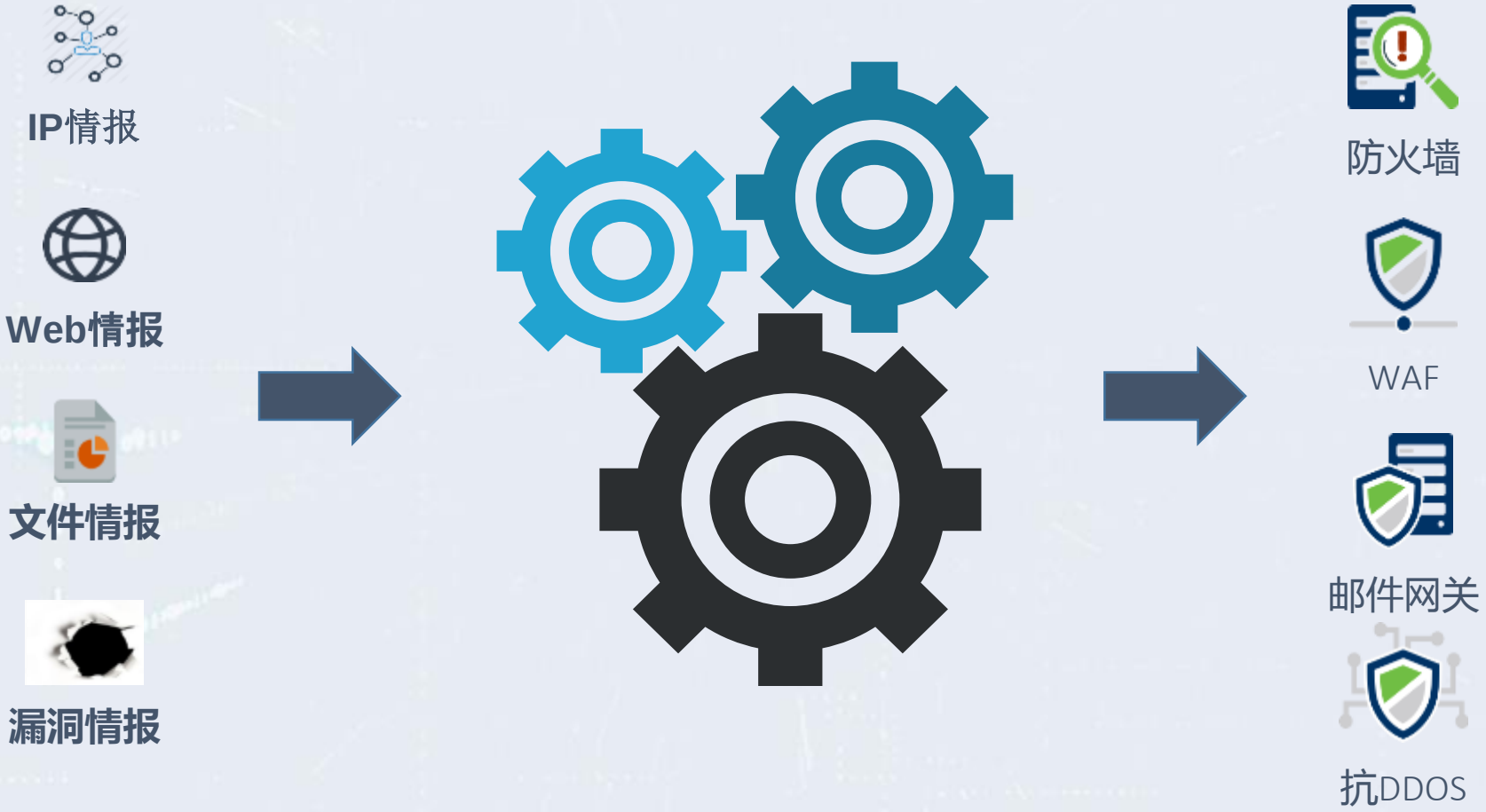
主动防御

6月16日23点，我行得到Apache axis存在0day高危漏洞的情报。

17日凌晨1点，全行协同完成所有受影响应用系统的排查、修补方案制定和实施工作。

1:21分，我行就监测发现了利用此漏洞攻击我行互联网应用系统的情况。

策略联动



溯源分析

确定攻击对手

还原攻击手法

掌握攻击者实力

了解攻击意图

未来工作展望

完善外部机构的威胁情报共享机制

增强金融行业威胁情报共享和联动指挥调度


谢谢观赏！