



**DHC** 东华软件股份公司  
DHC Software Co., Ltd

# 抗“疫”有情，网安联信创生态在线沙龙伴你行！

抗“疫”公益系列活动之十九（二）

## 运维视角下的网络安全建设

马虹斌 网络技术事业部

东华软件股份公司

# 重保之年

- 谁领导
- 谁参与(行业)
- 谁攻击
- 谁防御
- 谁被通报批评
- 谁被表扬
- 战场打扫，（八卦一下）

## HW行动

红蓝对抗  
实战化

一场声势浩大的**运动**

网络安全的本质在于对抗，  
对抗的本质在于攻防两端能力的持续较量

提高企业安全团队对抗能力的一次关键契机。

重点演练应急响应流程和制度，

常态化落地的安全检测和防护手段。

# 01

## 国内安全高速发展的大趋势

抗“疫”公益系列活动之十九（二）·

DHC SOFTWARE

## ▶ 安全行业高速发展的驱动因素

### 1. 傅鸪爽攷標啞

- 2019年12月 《等保2.0》 正式实施
- 2018年6月公安部发布《网络安全等级保护条例（征求意见稿）》
- 2017年6月《网络安全法颁布》
- 2016年12月《网络空间安全战略》发布
- 2016年习主席4.19讲话
- 2014年中央网络安全和信息化小组成立

### 2. 撓埒賴慳標啞



大数据



云计算



物联网



移动办公

企业数字化转型战略

### 3. 枝村厄鸪齋韜零韜



有组织

目的明确

影响严重

## 安全行业市场的新浪潮



——数据出自2019年中国网络安全分析报告

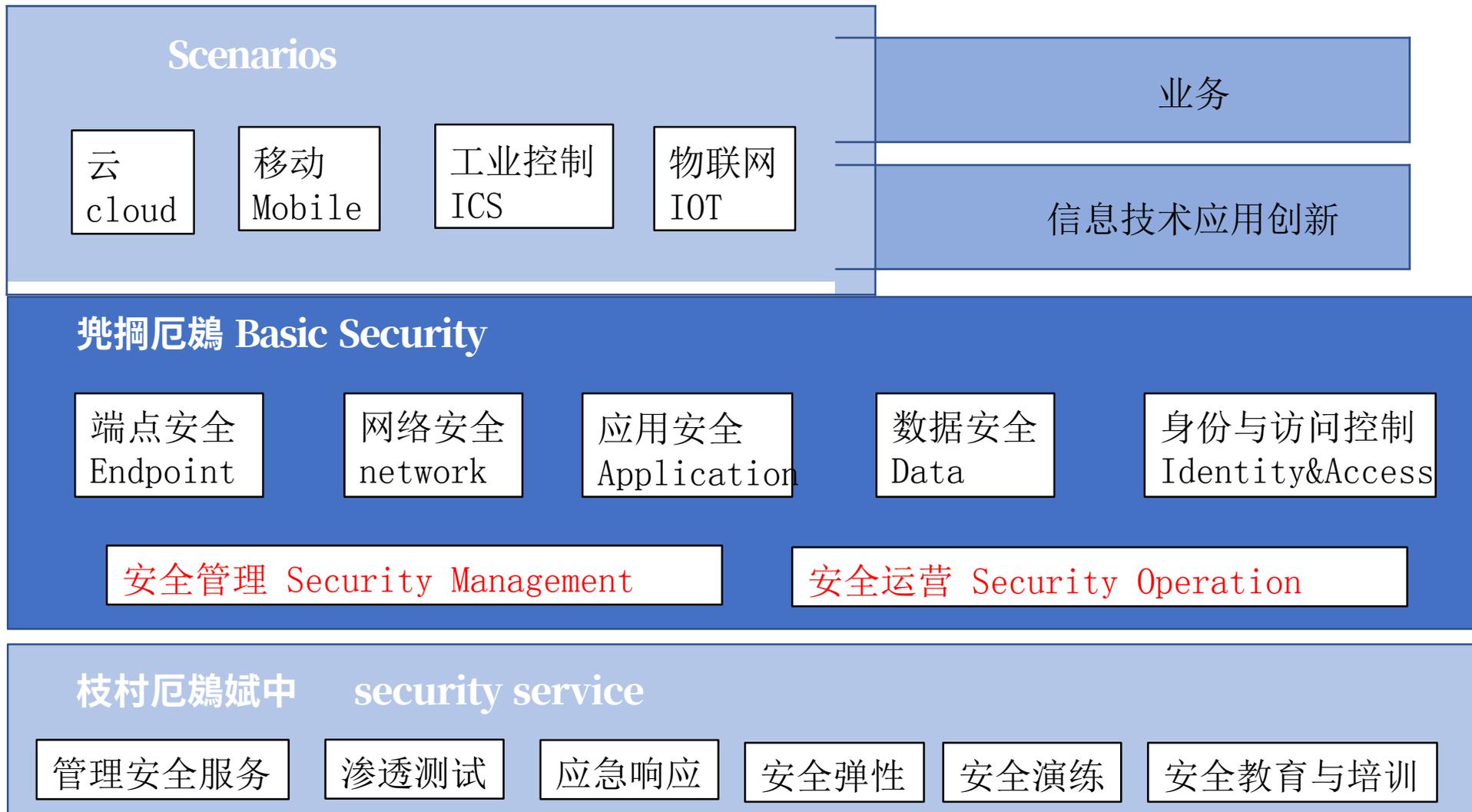


## 鞣扩泔脞

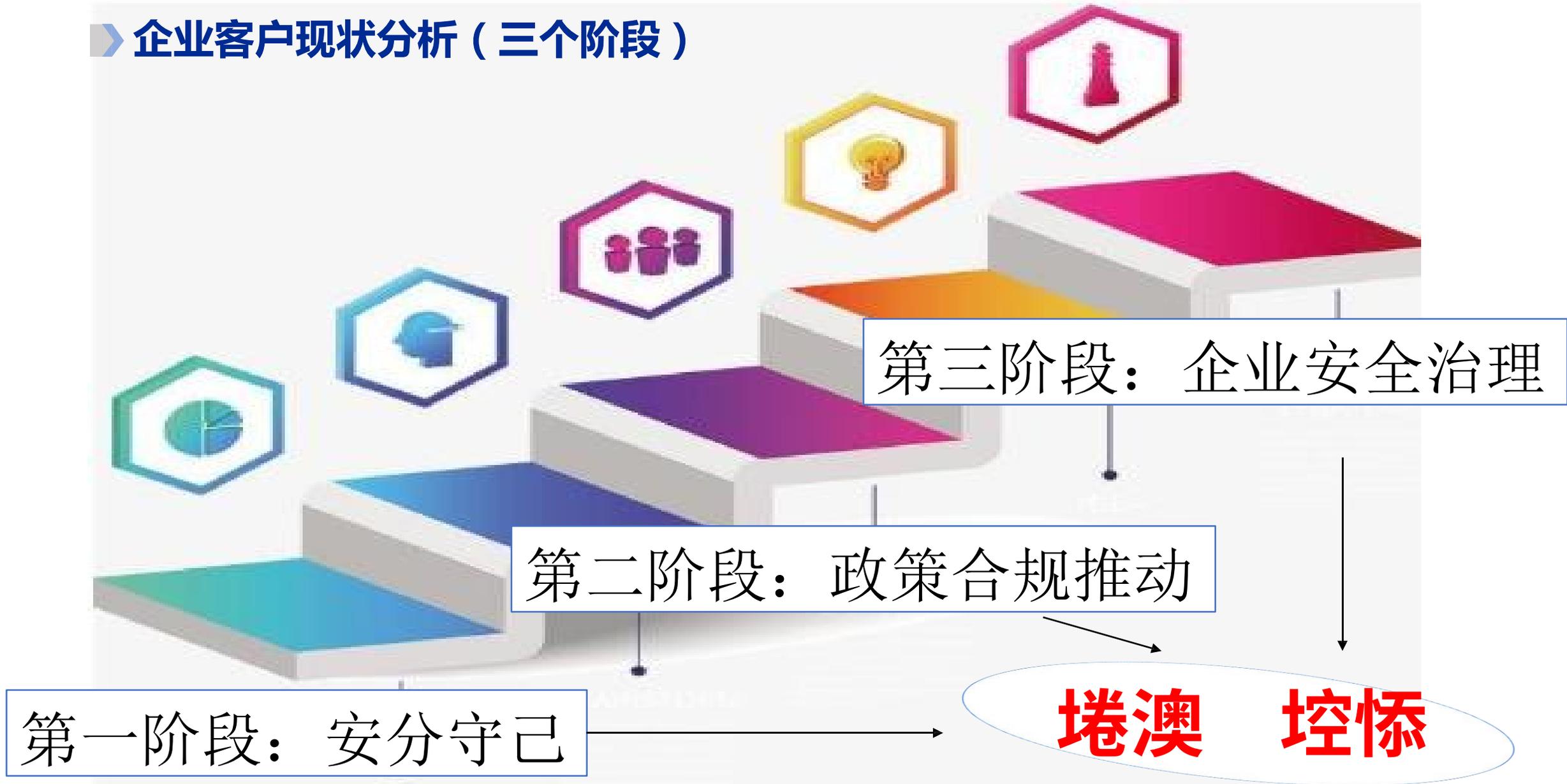
- ✓ “人”是最强的防护武器
- ✓ “人”的薄弱环节（恶意的、失误的、捕鲸、鱼叉）
- ✓ “人”才缺口及职业素养
- ✓ “人”工智能

抗“疫”公益系列活动之十九（二）·

## ▶ 我国网络安全的产业分类



## 企业客户现状分析（三个阶段）



# 02

## 日常运维遇到的安全平台建设的问题

抗“疫”公益系列活动之十九（二）·

DHC SOFTWARE

## ▶作为安全管理员所遇到的困扰——工具困扰



- 1.涉拘 鵠+澳費担杓 +厄鵠担杓 +
- 2.娶 奶刘闾闾 担峽鵠靛 政炳+
- 3.函 鸚攷 担峽瓏 +

## ▶ 全球到处都缺人，您那边缺人吗？反正我缺人——人员困扰

- 您的客户有安全团队吗？
- 您的客户安全团队有几人？（个，十，百，千）
- 安全团队有安全分析师吗？
- 安全团队是7\*24工作吗？
- 请问，安全分析师有工具吗？平台吗？
- 企业每年的安全预算比重，占信息化（IT的比重）。
- 安全会议会有高层人员参加吗？



抗“疫”公益系列活动之十九（二）·

# 03

## 作为客户如何使用好平台工具

抗“疫”公益系列活动之十九（二）·

DHC SOFTWARE

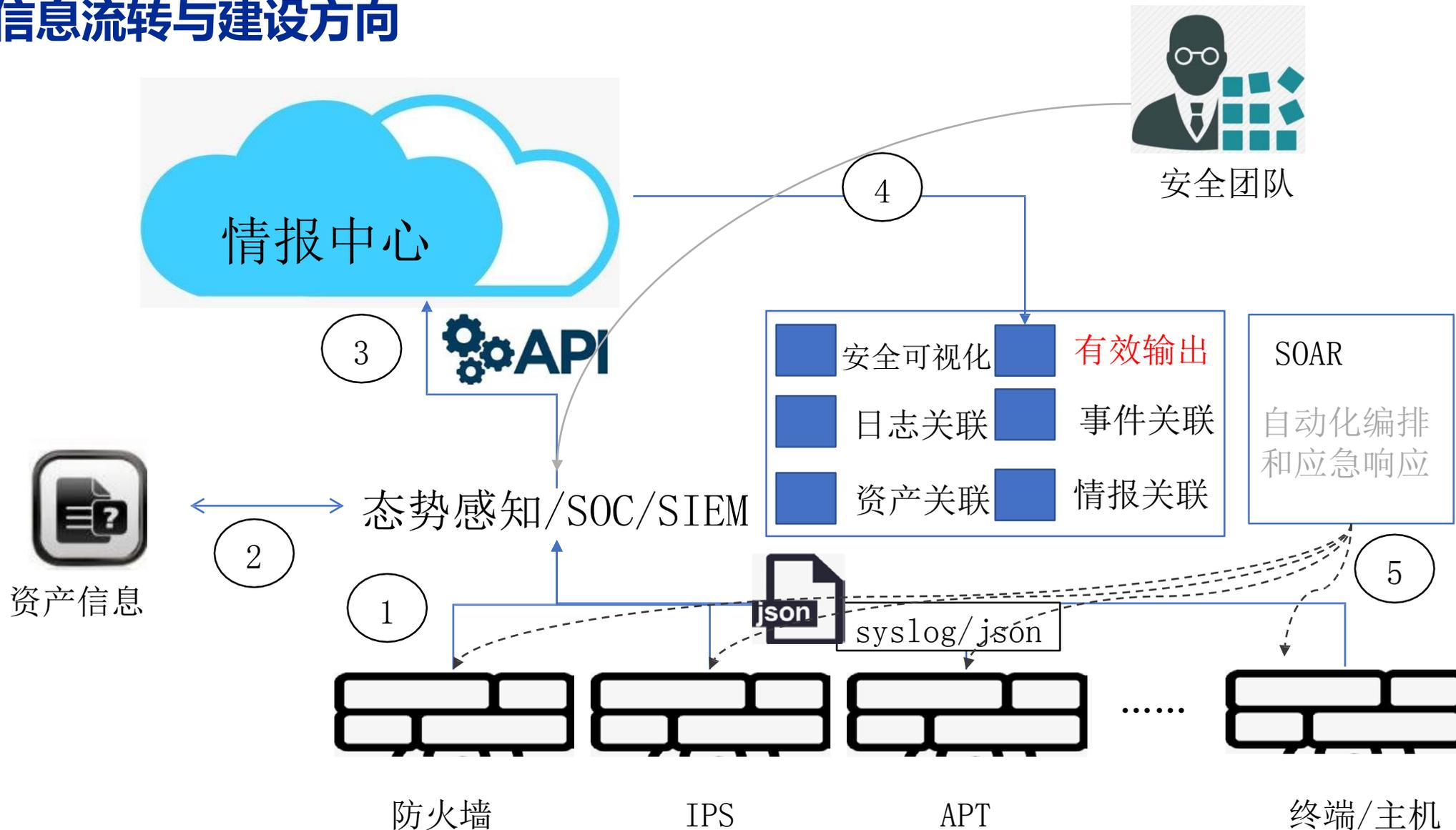
## ▶ 态势感知具体是什么？

态势感知=事件安全收集整理+可视化+安全响应和服务  
是项目型的、是非产品化的、离不开反复沟通的

## ▶ 为什么态势感知项目常常遇到的困难

- 数据收集与集成难——沟通成本（探针都是同一厂商的除外）
- 可视化效果难——众口难调，返工
- 安全服务难——人员成本

## 信息流转与建设方向



## ▶ 企业安全运维我们所要考虑的

1. 带入什么样的厂商进来？自研或是外采？
2. 安全人员的培养, 实战化的经验
3. 事前做好基线，事中处理闭环，事后做好复查
4. 高层的支持和配合

## 未来整体的安全趋势

- 监管，从所未有的强势
- 投入，企业加大安全方面资金投入
- 甲方安全团队的组织结构会发生剧烈的变化
- “黑天鹅”事件，事件会越来越多
- 混合云带来的安全风险
- 数据安全，数据合规，跨境数据安全
- 自主可控服务

## 畅谈聊下2020年的安全市场的大趋势

远程安全维护模式初见端倪（安全SaaS服务初体验）  
教育与医疗行业安全将爆发（重点行业受监管影响）  
中小型安全厂商抱团取暖（生态建设方向开放）

**东华：软件领军，国际名企！**

THANKS

FOR YOUR ATTENTION

