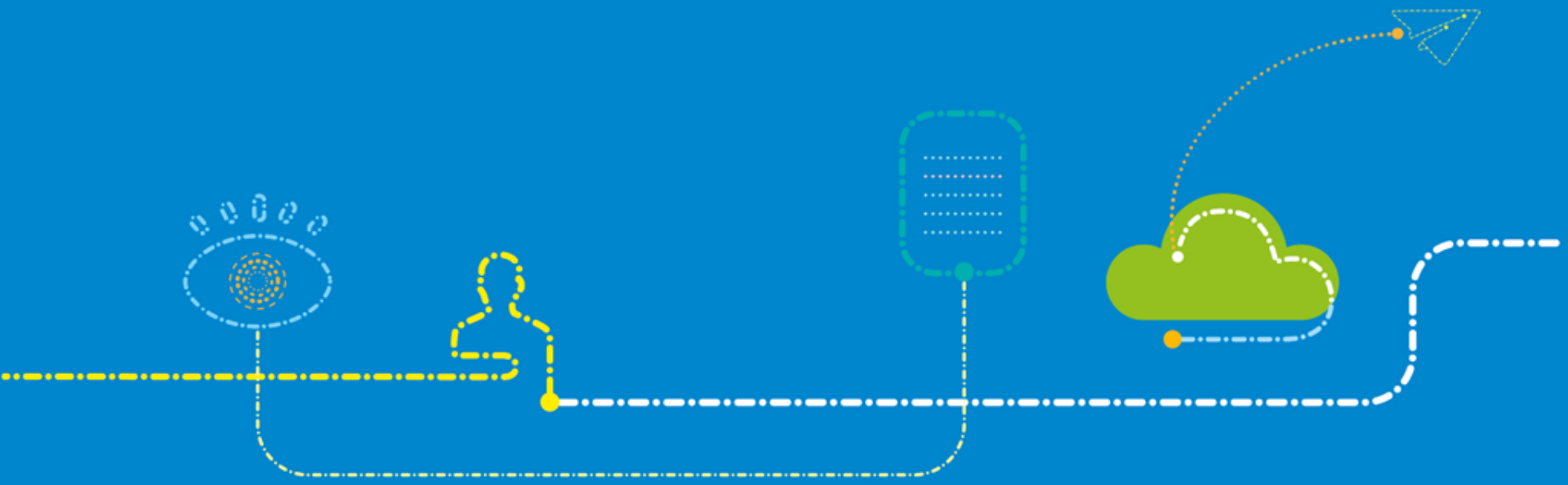
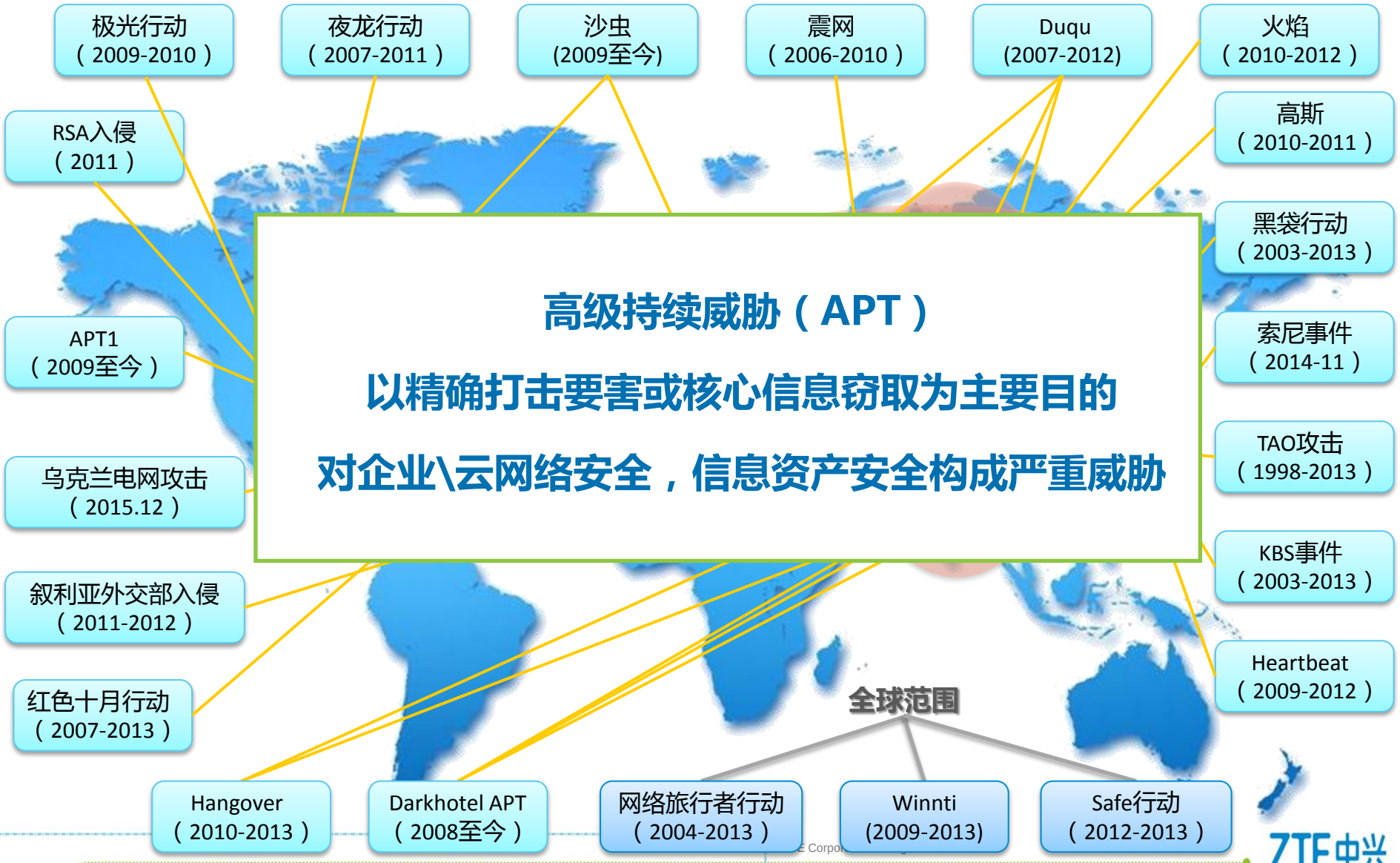
网络流量异常行为分析系统

ZTE中兴
未 来，不 等 待

中兴通讯 APT防御
2016年7月



背景：APT攻击事件遍布全球，是网络空间安全面临的重大挑战



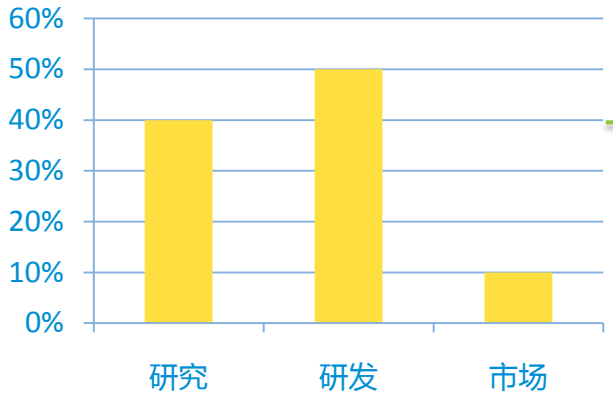
传统入侵\异常检测系统，应付APT，显得吃力

- **经典威胁检测系统，基于报文内容特征匹配以及统计阈值**
  - 特征已知的威胁，检测效果好
  - **对APT这类特征未知的威胁，几乎束手无策**

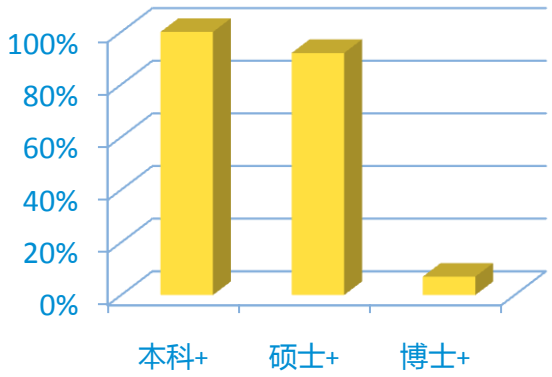
- **基线检测系统，基于统计来标定和预测正常范围，流量\行为明显偏移时，判为异常**
  - 受到突发事件冲击时，误报率会显著增高
  - **APT善于自我隐藏，很难引起统计变化，难以检测**

ZTE中兴，APT分析检测系统：发现未知威胁，捉拿APT

研究、研发、市场三个子团队



硕士学历以及以上92%



“严守”网络大门

文件动态行为分析系统

“排查”网络内部流量

网络流量异常行为分析系统

APT分析检测系统

APT分析检测系统的亮点：不用事先知道威胁的“特征”，适合检测特征未知的威胁，应对APT

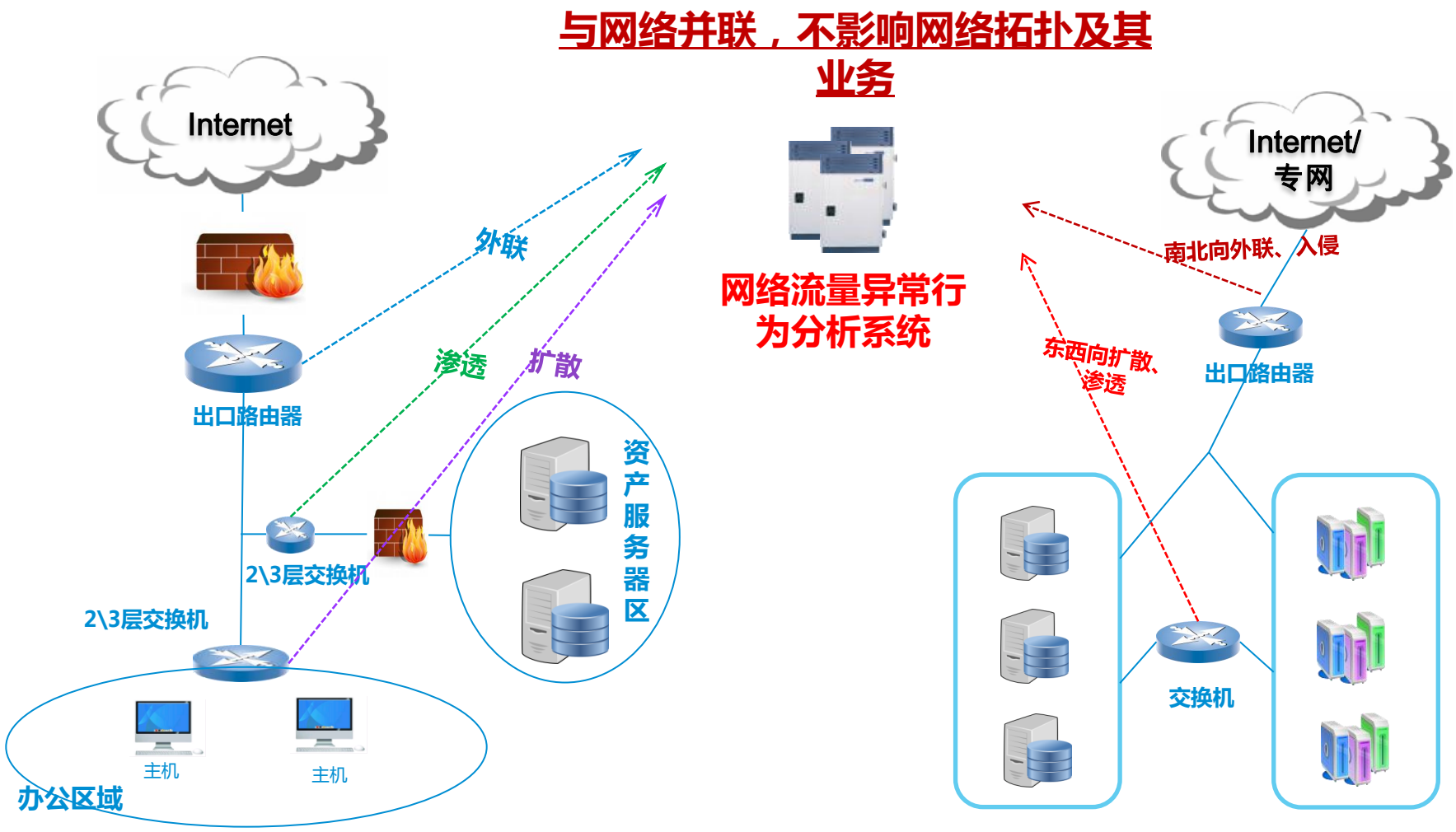
核心价值：

- 解决政企、IDC、云自身的网络安全痛点
- 作为IDC、云Provider的增值服务为其租户提供安全服务
- 协同构建APT防御堡垒

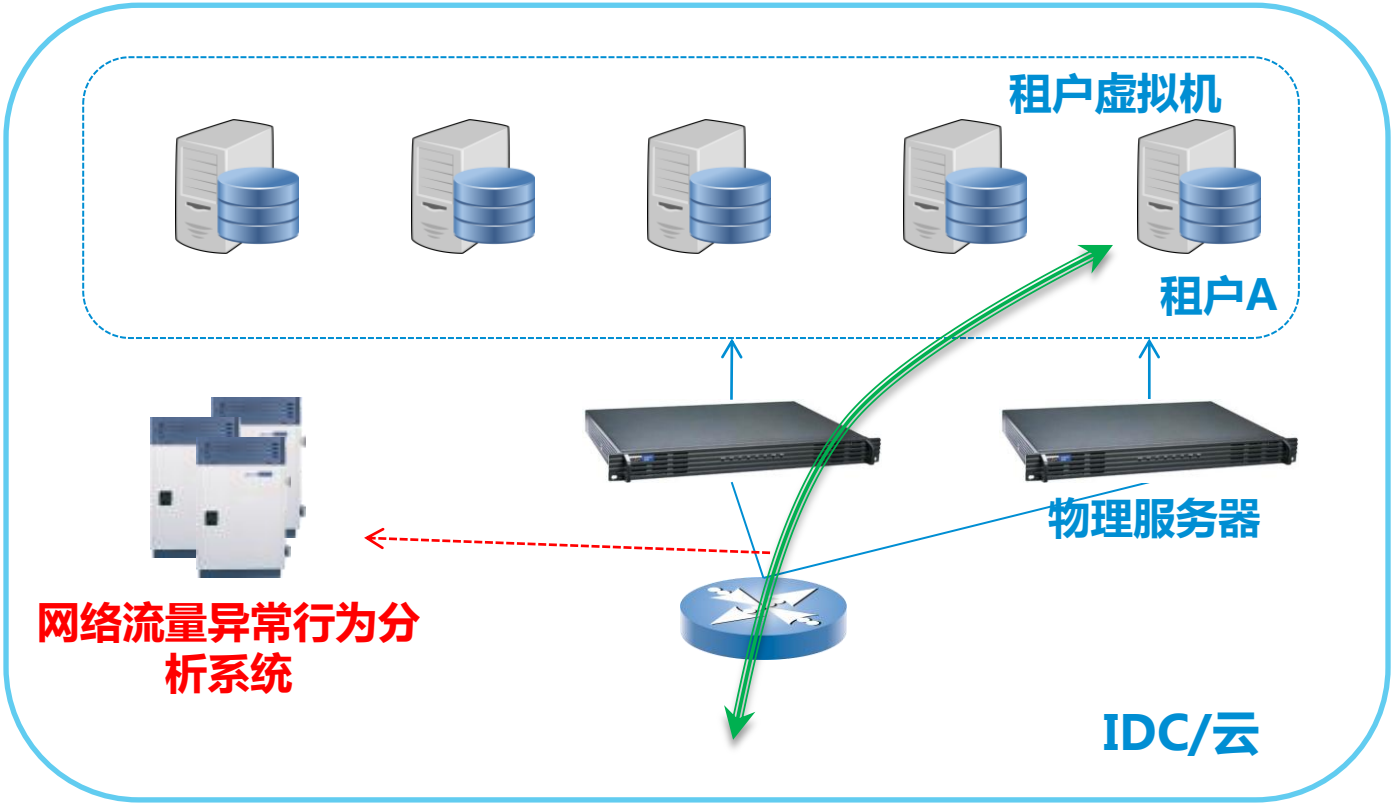
“文件”

“流量”

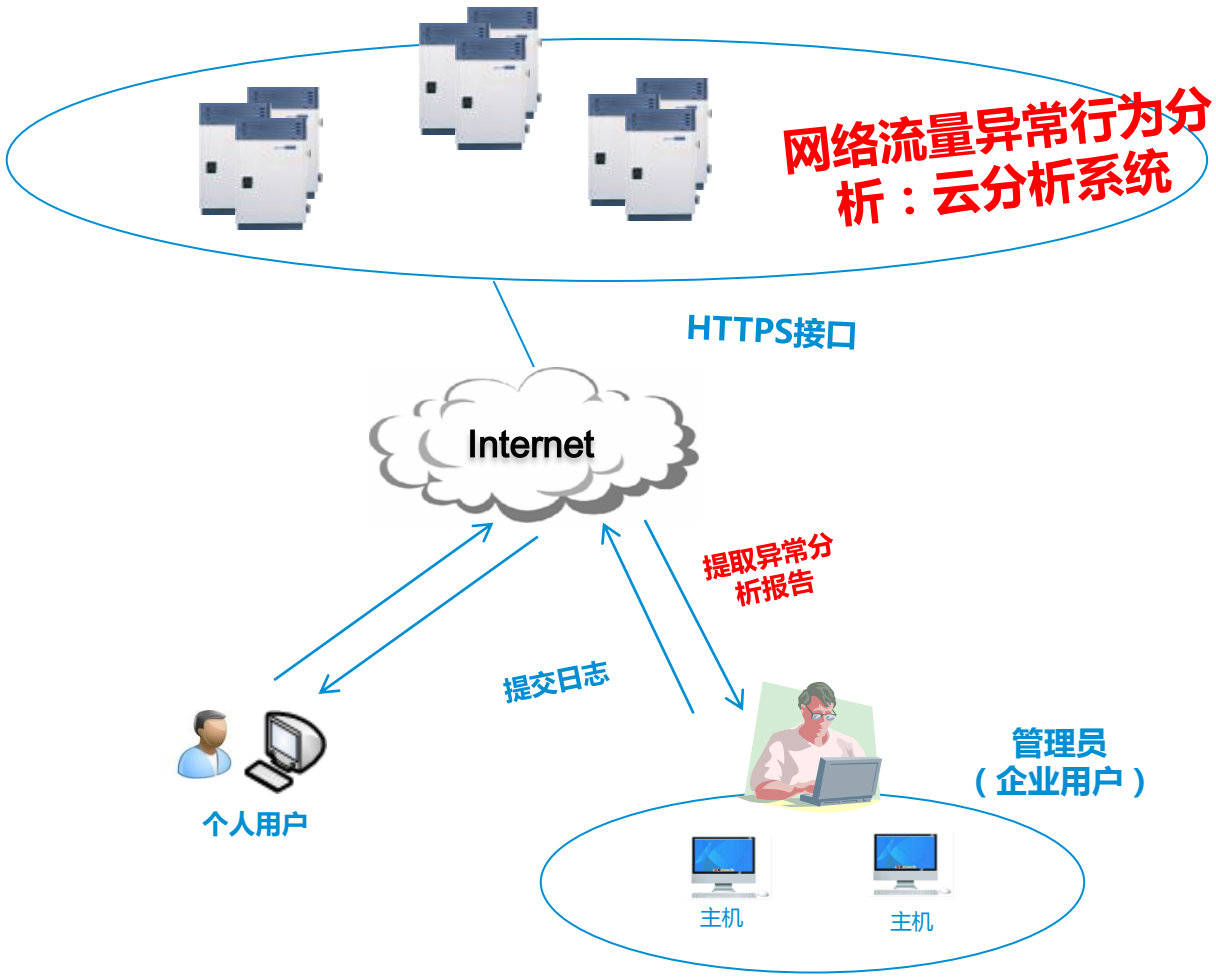
商业模式A：为政企、IDC、云服务Provider提供安全服务，检测分析外联、渗透、扩散等潜在风险，预警安全事件



商业模式B：作为IDC、云服务Provider的安全增值业务，为租户提供增值服务

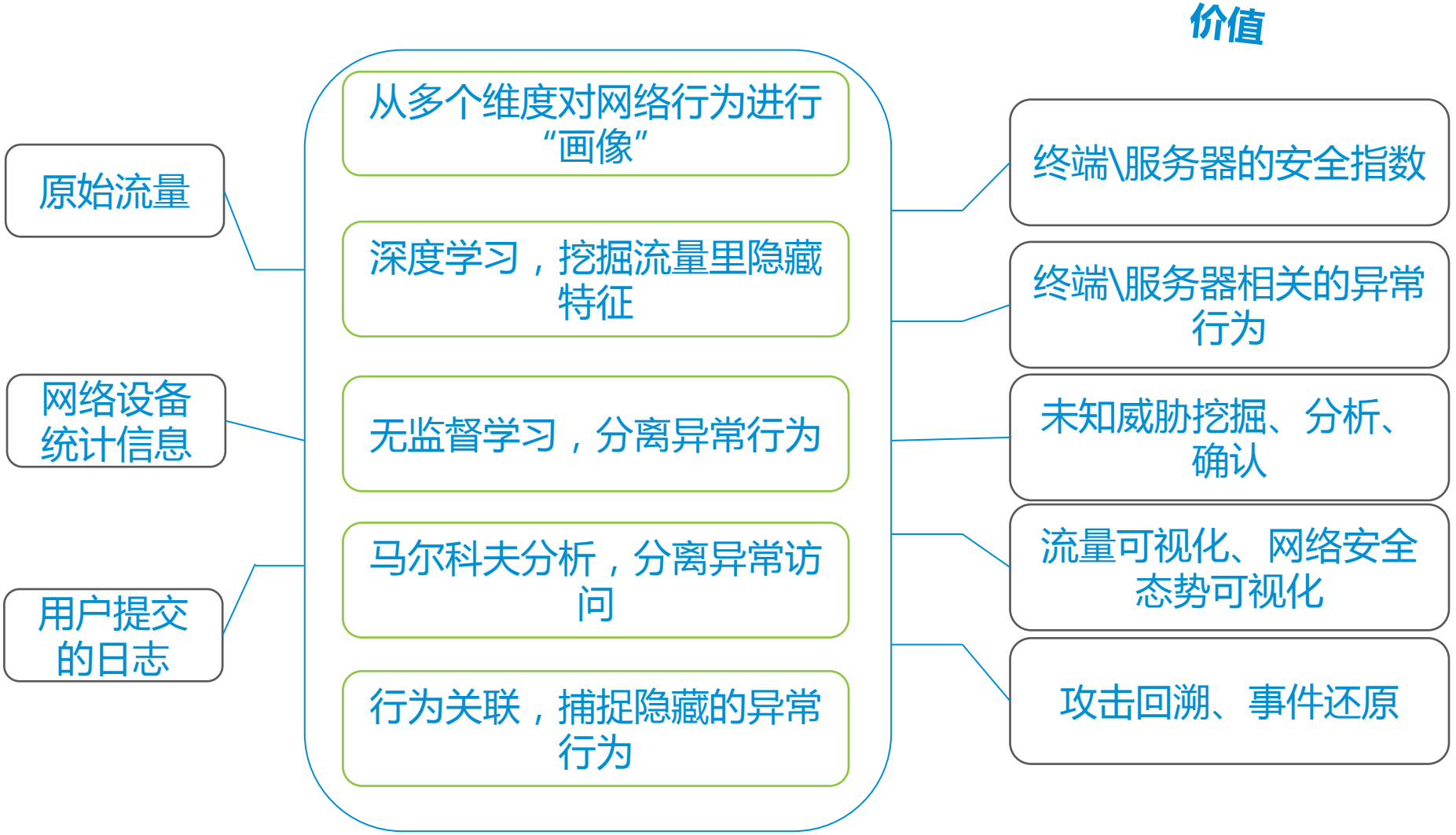


商业模式C：以云的形式为个人\企业用户提供流量日志分析服务，捕捉潜藏的异常行为



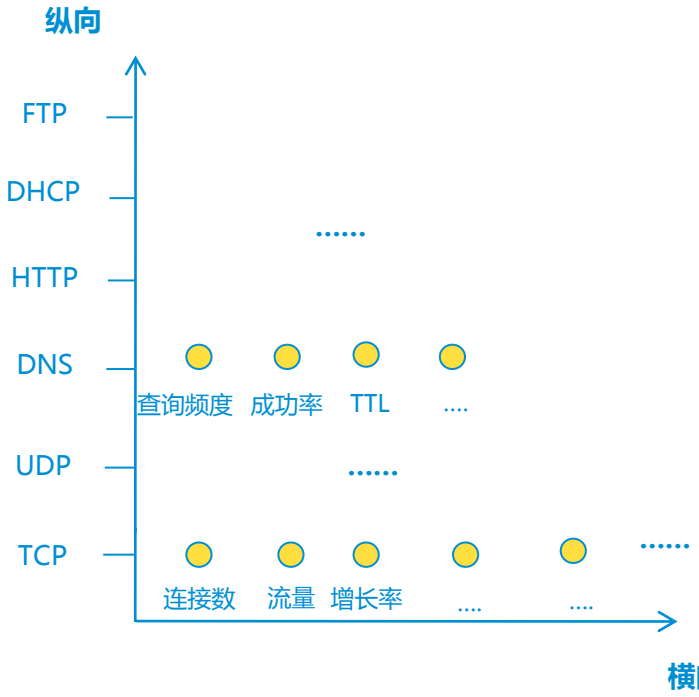
➢支持常用开源流量LOG工具；多种方法结合，充分保护用户隐私

网络流量异常行为分析系统，主要技术亮点



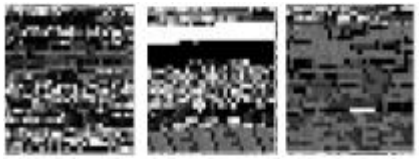
技术亮点之：应用深度学习技术挖掘隐藏特征

从多个维度对流量行为“画像”



深度学习多用于计算机视觉，图像处理

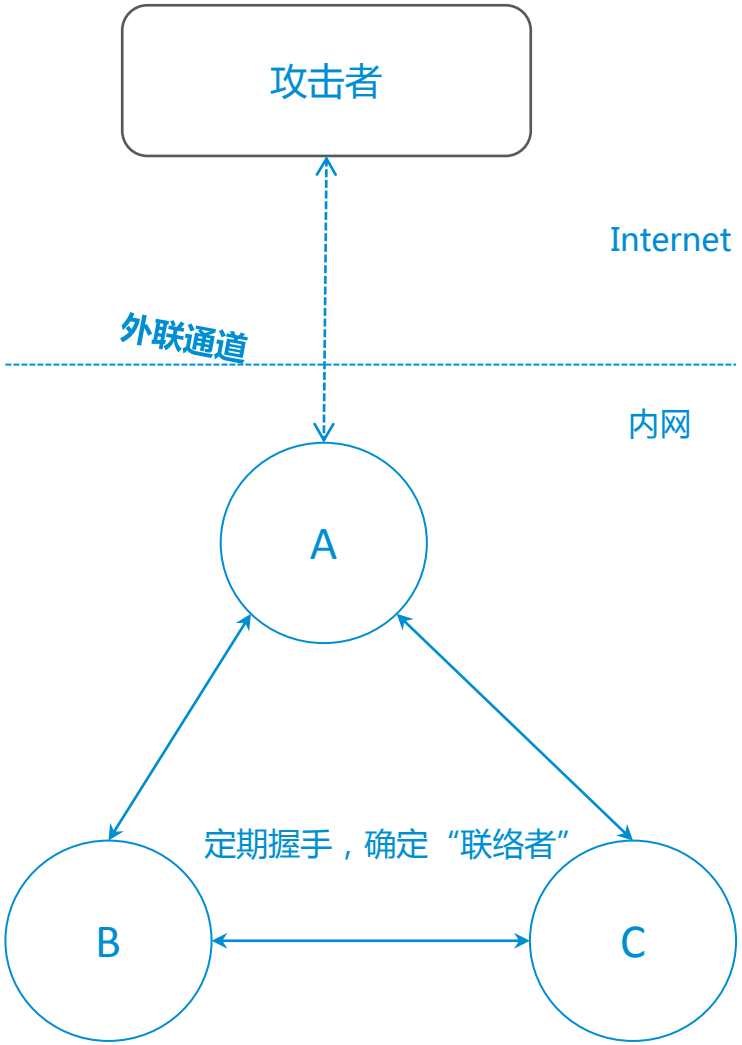
看作为图像



潜藏特征自动挖掘

- **机器学习的痛点：样本收集、特征总结**
- **对“画像”后的流量应用深度学习，挖掘隐藏特征，用以进一步分析**

技术亮点之：无监督学习，用不同分辨窗口分离异常行为



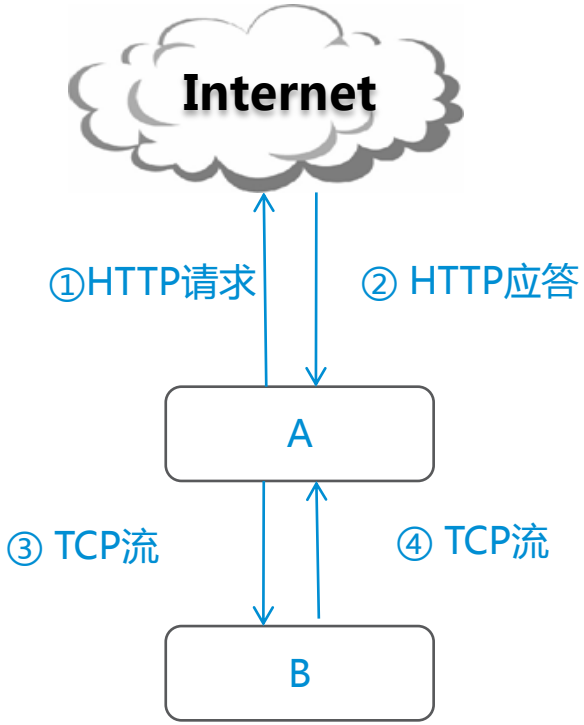
- **基线分析的痛点：异常行为引起统计值明显变化时，才有较好的检测效果**
- **分离异于大众的“小众”，它源于APT的可能性更大**

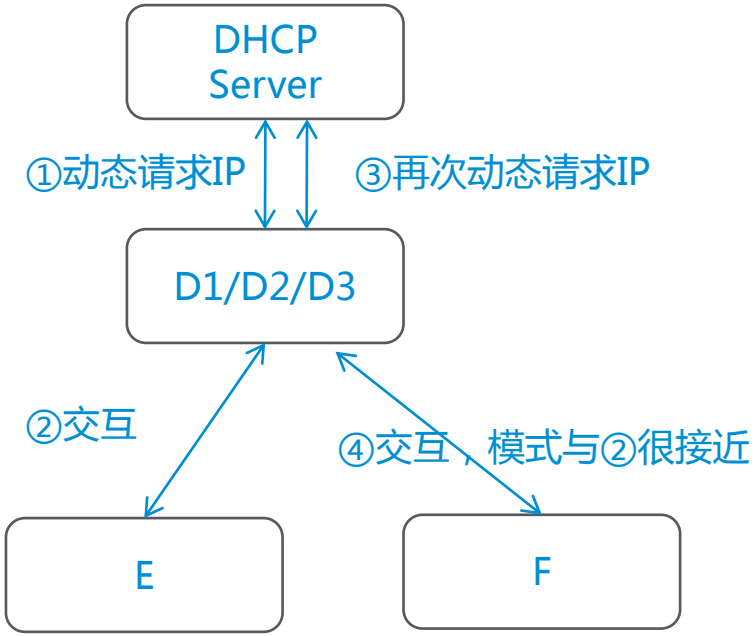
行为异常检出实际案例，一：

三个终端位于内网；为了隐蔽，A维护外联通道；为了可靠，A失效时，新的“联络者”负责外联。

断定A、B、C同处于一个“朋友圈”；“朋友圈”里的流量“长”的不可思议的“像”

技术亮点之：多重行为关联，发掘隐蔽的异常行为





行为异常检出案例，二：

A和B间有交互，A与一个WEB站点间有交互；两种交互持续胶着；

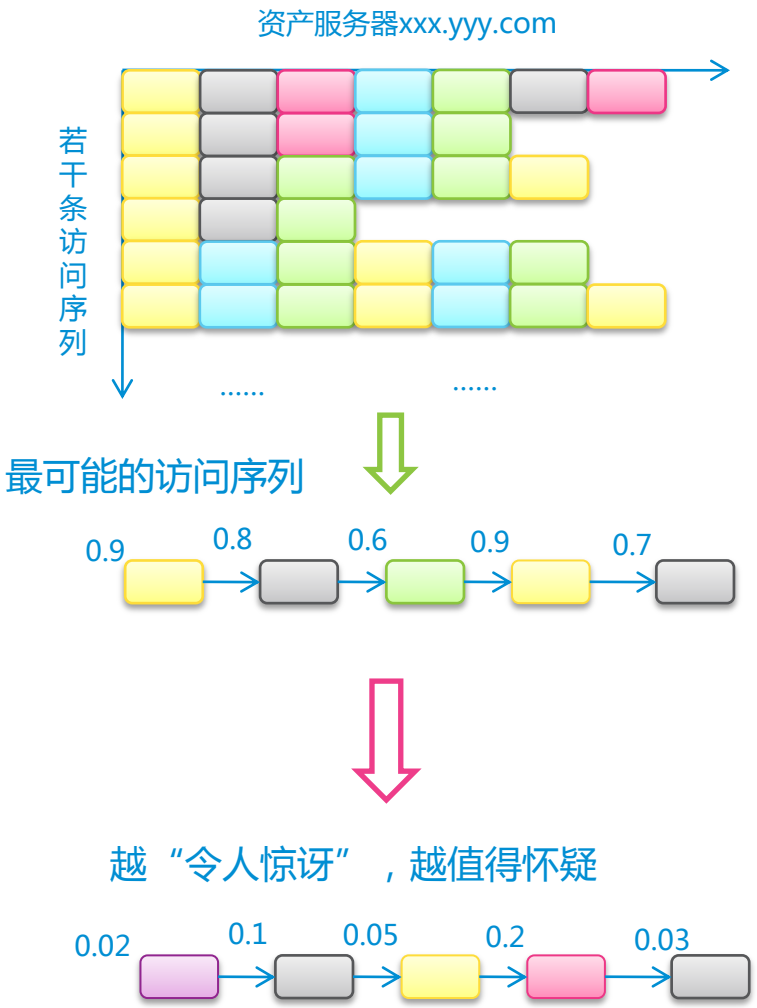
经分析，A被攻击者作为攻击跳板的可能性非常大

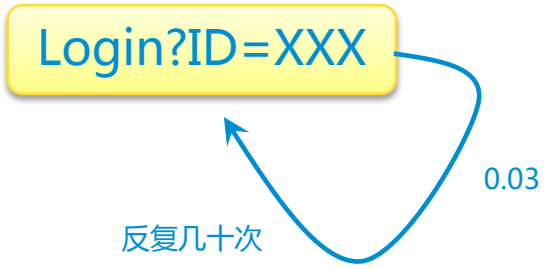
行为异常检出案例，三：

IP地址D1\D2\D3属于同一子网，它们与其它多个终端E、F、G,...间的交互的模式很像，同时穿插有DHCP行为；

经查实， D1\D2\D3是同一终端，它对多台主机的关键端口执行了低速扫描。为了隐蔽，它会更改自己IP以及MAC

技术亮点之：马尔科夫随机过程用于检测资产服务器异常访问



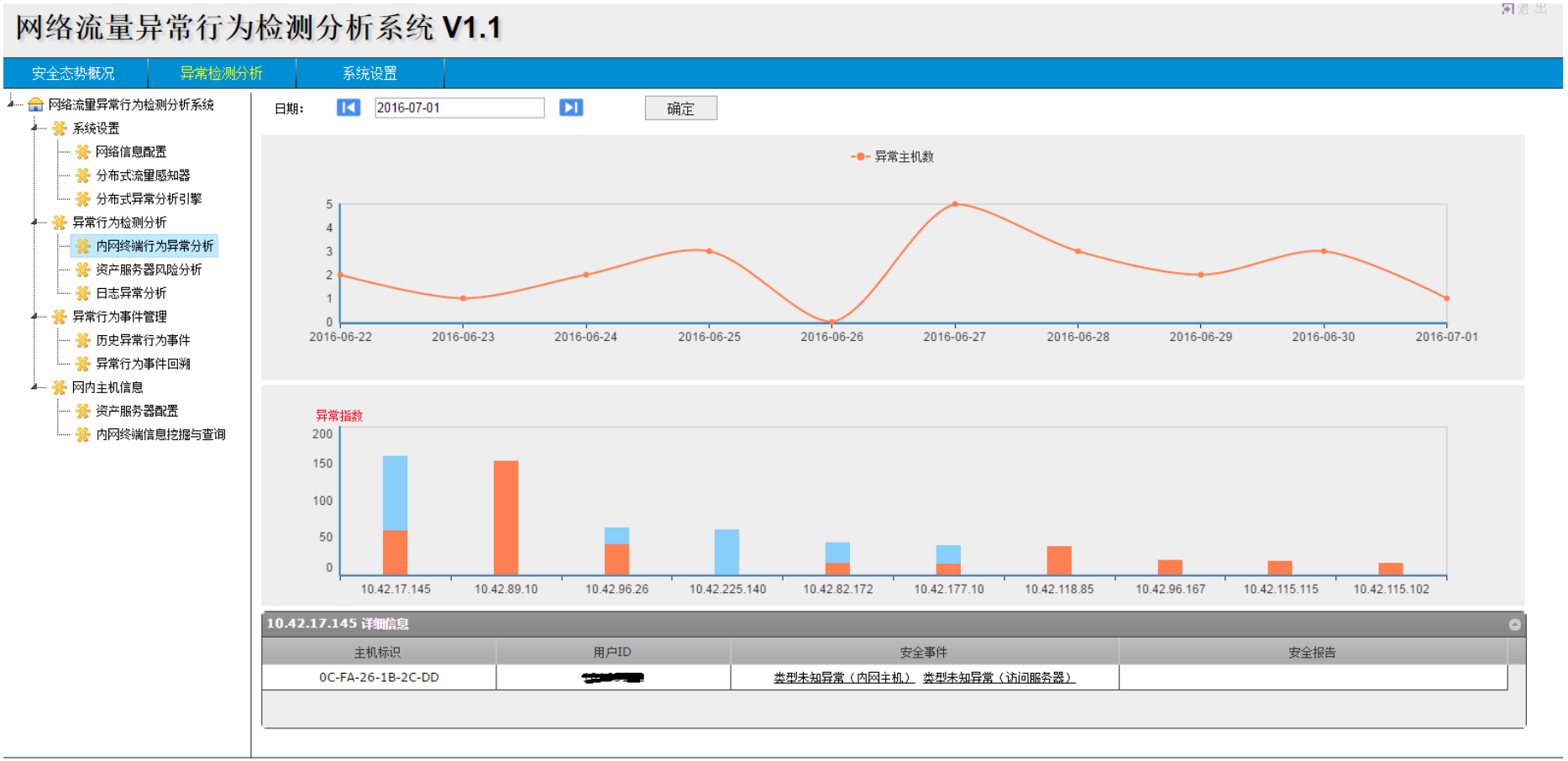


行为异常检出案例，四：

A访问服务器时，始终“登陆页->登陆页”上跳转；“登陆页->登陆页”的转移概率仅不到3%，该序列足够“令人惊讶”。

经查实，A在尝试不同用户的用户名和密码。

ZTE中兴，APT检测分析：网络流量异常行为分析系统



- 部署在南京某大型企业，网内包含5000+PC和20+资产服务器，平均流量为4Gbps
- 检出高风险的行为异常事件30+起，经安全专家逐一核实，误报率<10%
- 该企业也部署了传统威胁检测设备，但对上述未知威胁基本毫无知觉

ZTE中兴，APT检测分析：文件动态行为分析系统，具备商用条件

- 部署在南京某大型企业的网络入口，覆盖全国各分支，员工8万+，平均每天检出高危邮件附件>10个；捕获多次高级攻击事件，包括针对该企业多名高管的定向攻击
- 捕获的高危恶意软件样本，主流杀毒软件(Mcafee)不能当天检出；部分高危样本与Virustotal(集成50多家杀毒软件）同步检出甚至更早

谢谢！

未来，不等待