阿里安全峰会
ABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

安全智能云

连接传统企业安全措施的新药方

TianJi Partners

天际友盟 CEO / 杨大路

传统上我们这样解决企业安全问题

防火墙（FW）

边界防御

侵入保护系统（IPS）

漏洞扫描

终端防护

侵入检测系统（IDS）

塔式防御

分区分域

纵深防御

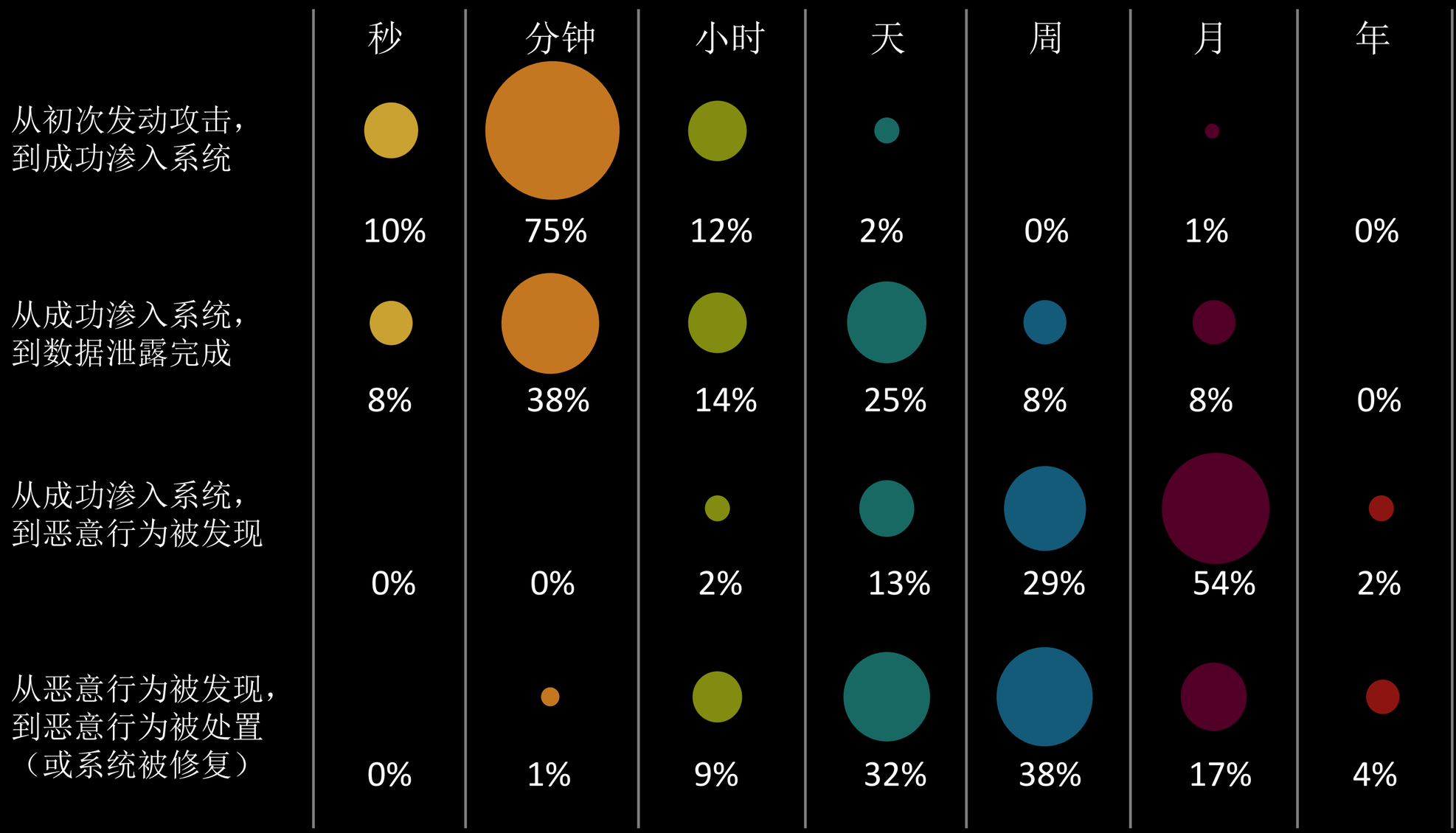
网络准入

网络隔离

身份认证

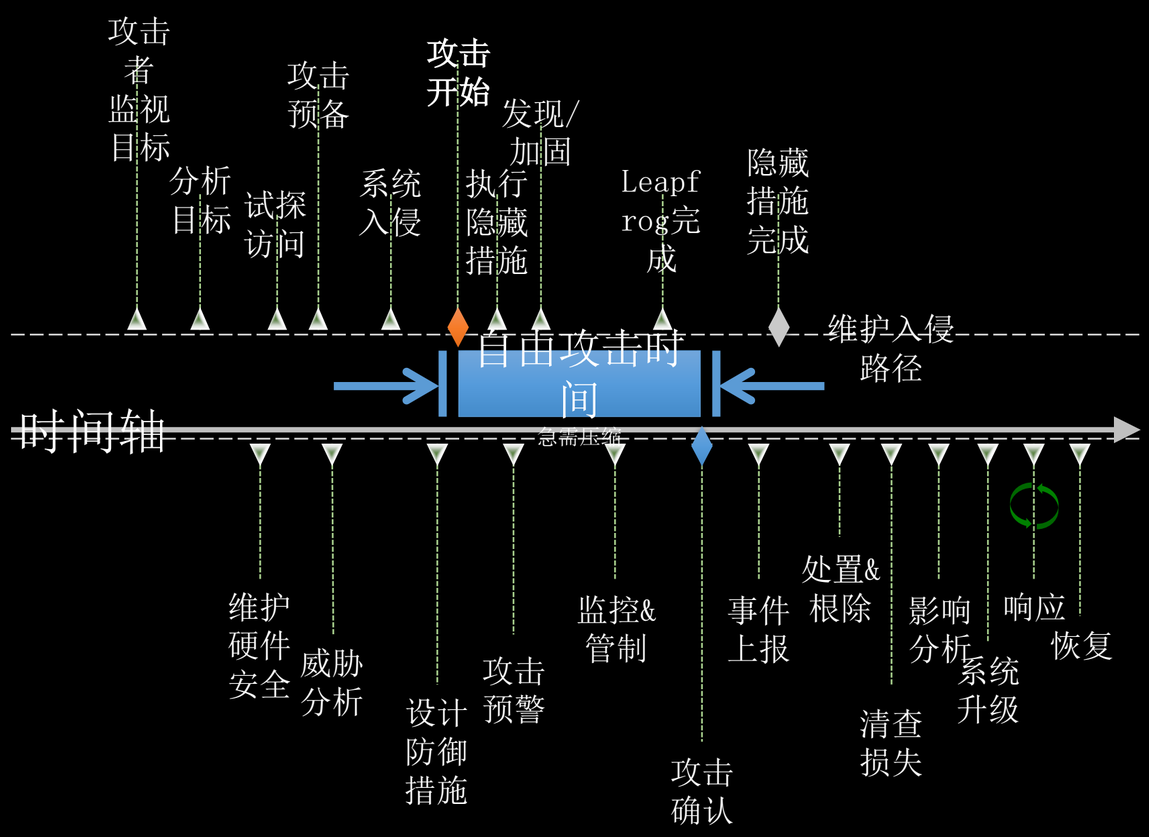
传统思路下，我们只会严防死守

数据泄露事件的不同阶段，所耗用时间级的百分比统计



攻击技术飞跃，传统防护手段失效

我们需要重新思考防御体系



以缩短攻击者的“自由攻击时间”为主要目的

- 产品规则响应速度
- 产品间差异问题
- 以“行动”为核心
- 以“有效性”为目标

三个方法

- 基于证析方法的安全情报体系
- 基于自动化的应急响应体系
- 基于安全智能的纵深防御体系

TianJi Partners

和你一起创造更安全的未来

基于证析方法的情报体系

TianJi Partners

和你一起创造更安全的未来

构建安全情报平台

全面的资产情报

有效的威胁情报

及时的漏洞情报

准确的事件情报

丰富的专家储备

自动化响应手段

整合能力是核心竞争力

- 所有数据都放在自己的“碗里”并不是最佳模式
- 让有经验的安全专家能够“专心的”分析数据
- 情报是基于证据的知识，需要传统安全措施（设备）来发挥作用

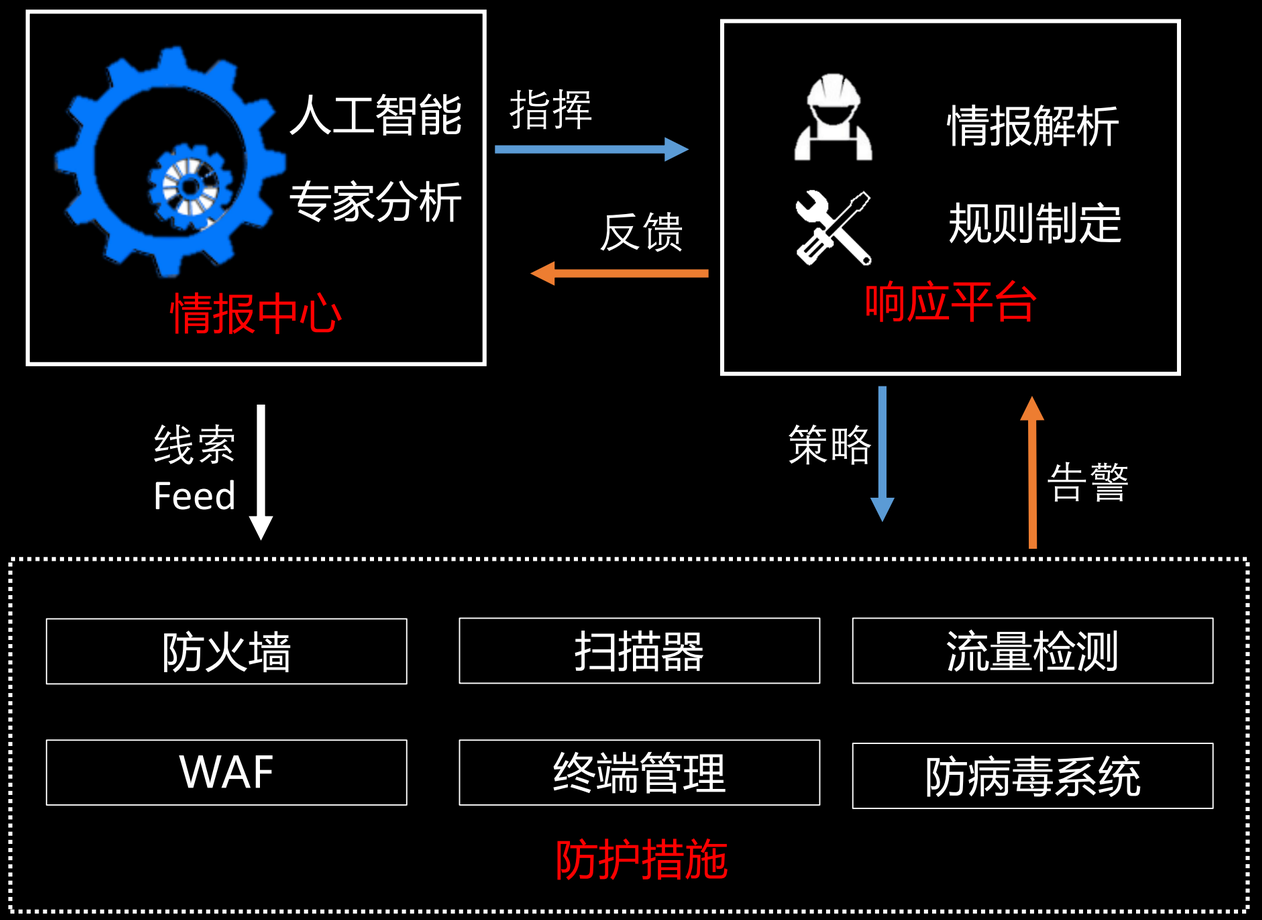
TianJi Partners

和你一起创造更安全的未来

基于自动化的应急响应体系

TianJi Partners

和你一起创造更安全的未来



自动化应急响应机制

TianJi Partners

和你一起创造更安全的未来

漏洞情报：Apache Struts 访问限制绕过漏洞 (CVE-2016-4431)

影响范围：Apache Group Struts2 2.3.20 - 2.3.28.1

解决措施：补丁S2-040

情报获取

总部SIC

响应方式

补丁下载

数据统计

SIEM资产库统计

每天扫描

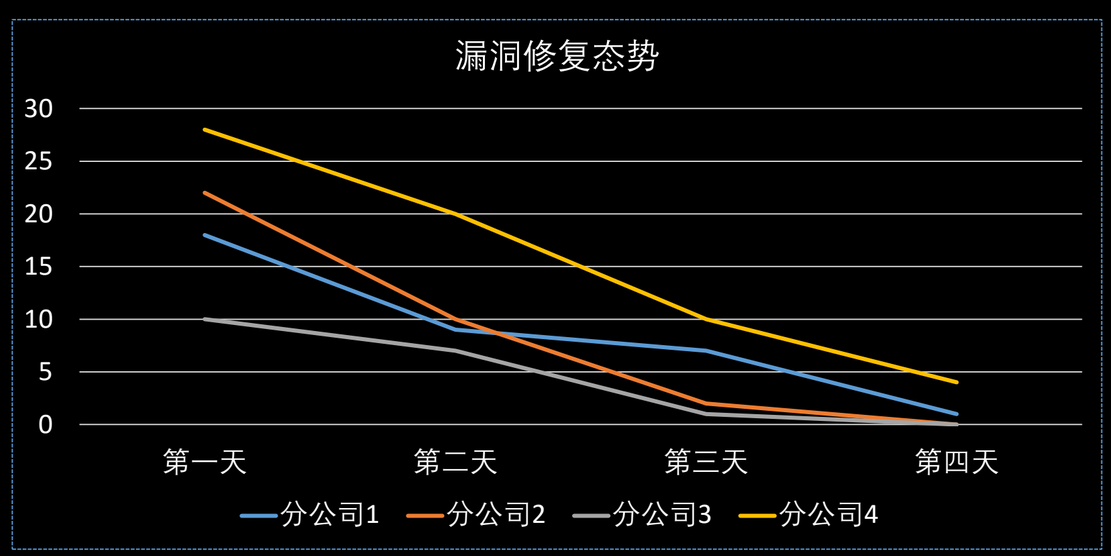
扫描器遍历内网

影响范围

涉及4个分支机构，78个应用系统

状态跟踪

修补确认



针对漏洞情报的自动化响应

TianJi Partners

和你一起创造更安全的未来

基于安全智能的纵深防御体系

重新定义纵深防御

- 通过前置导入的风险评估，针对性建立安全基线
- 依据安全基线制定安全情报的分类订阅和使用方式
- 对安全风险进行持续监控，形成安全态势感知能力
- 快速事件响应、动态风险评估、主动基线策略调整

传统安全措施与安全智能云服务的连接

- 扩充了对全球安全数据的分析
- 对当前热点情报信息进行处理
- 执行实时事件关联与威胁溯源分析
- 缩短事件响应时间
- 提升针对安全事件的综合分析能力

TianJi Partners 关于天际友盟

- 国内安全威胁情报服务的先行者
- 国内首个安全威胁情报联盟 —— 烽火台
- 以专注聚合、分析、交换为目标的安全智能云服务
- IBM X-Force 中国安全情报合作伙伴

和你一起创造更安全的未来

www.sec-un.com