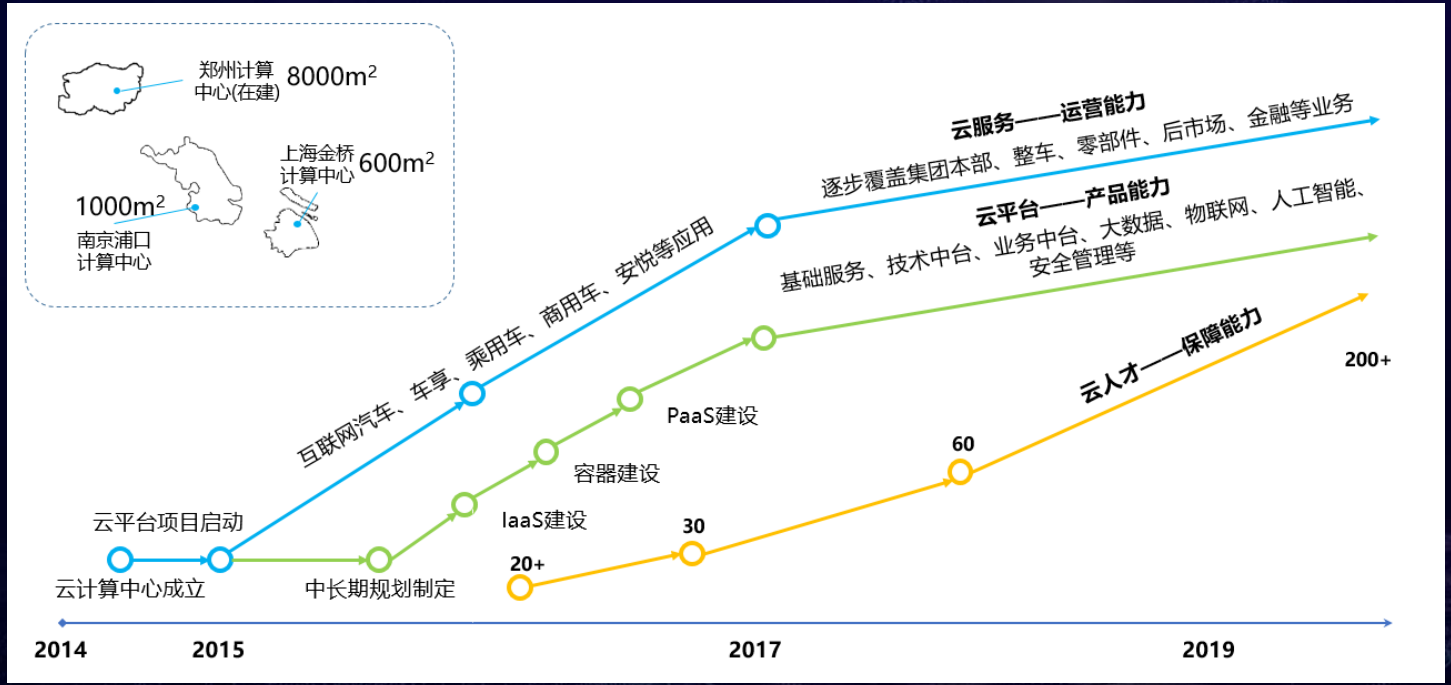

CSS
互联网安全领袖峰会
Cyber Security Summit
Tencent 腾讯
腾讯安全
上汽云中心全场景安全建设
万争 上汽云中心
高级安全工程师

上汽云发展历程


郑州计算中心(在建) 8000m²
上海金桥计算中心 600m²
1000m²
南京浦口计算中心
云计算中心成立
云平台项目启动
中长期规划制定
互联网汽车、车享、乘用车、商用车、安悦等应用
IaaS建设
容器建设
PaaS建设
20+
30
60
200+
云服务——运营能力
逐步覆盖集团本部、整车、零部件、后市场、金融等业务
云平台——产品能力
基础服务、技术中台、业务中台、大数据、物联网、人工智能、安全管理等
云人才——保障能力
2014
2015
2017
2019

上汽云安全服务

01 安全咨询服务

等级保护、信息安全管理体系
SDL、安全规范、安全架构咨询与评审

02 基础安全服务

抗DDOS、WAF、主机漏洞管理、基线检查、
安全监控、应急响应

03 应用安全评估与加固

模拟黑客渗透测试
发现风险点、提出安全建议
App安全检测及加固

04 物联网、车联网安全

提供基于数字证书的可信身份认证、防篡改
防抵赖、加解密等功能,支持移动端、IoT
车载端等平台，保障FOTA\SOTA升级
通信链路、终端等方面安全、车联网软件安全防护
蓝牙钥匙及安全

05 入侵防御态势感知

网络威胁可视化
利用大数据和机器学习检测安全入侵事件

06 网站防篡改

保护网站不受非法篡改
及时发现风险，维护企业形象

云上租户的自身安全

风险类别	风险级别
应用安全	
访问控制	
实例安全	
逻辑资源	
物理设施	
基础网络	

低 高

租户	上汽云

低 高

面临的安全威胁

安全评估
漏洞发现

自动扩散
传播广泛

利益链驱使
信息泄露或销毁

目的性强
数据窃取或破坏生产

如何做威胁发现？

建立全量数据计算平台发现威胁行为的安全体系

采集汇聚，实时监控，回溯分析用户网络流量及安全相关日志信息

数据采集
安全事件

100W/天

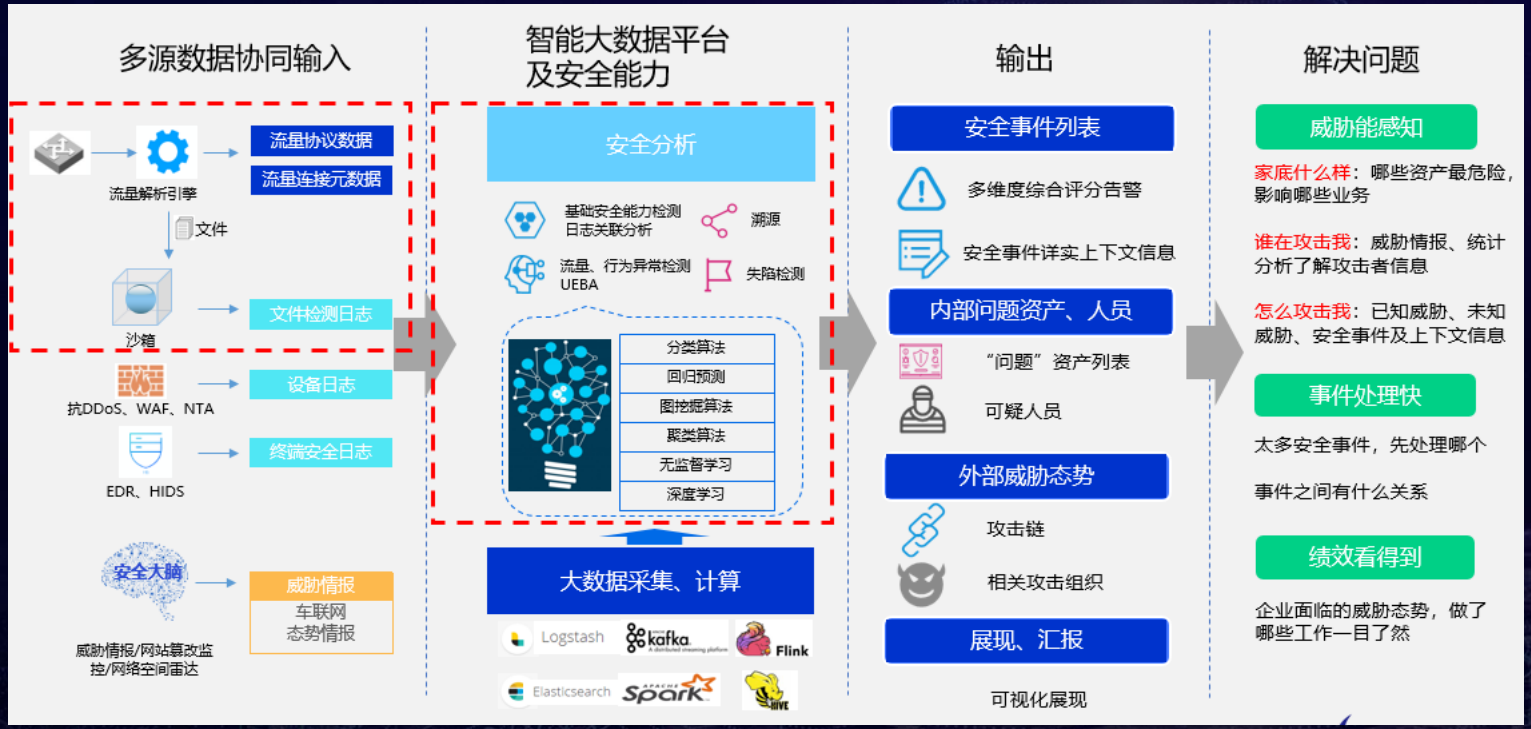
关联分析
检测模型

100+个

安全溯源
处置响应

< 5分钟

全场景安全能力检测架构



全场景安全能力建设

业务安全	Nginx	Tomcat	ThinkPHP	Struts 2
流量异常	科来	NTOP	sFlow	NetFlow
安全溯源	Sysmon	Osquery	Auditd	Zeek
主机安全	BruteForce	Webshell	Trojan/Virus	
流量安全	IDS	TI	Sandbox	文件还原
基础安全	IPS	Firewall	WAF	Anti-DDOS

全场景关联分析

流量入侵与服务器异常日志关联提高告警可靠性

通过行为链关联分析来确定高危漏洞是否影响到重要资产！？

数据归一化

服务器日志监控

基于安全基线的异常行为发现

异常登录、异常进程、异常账号

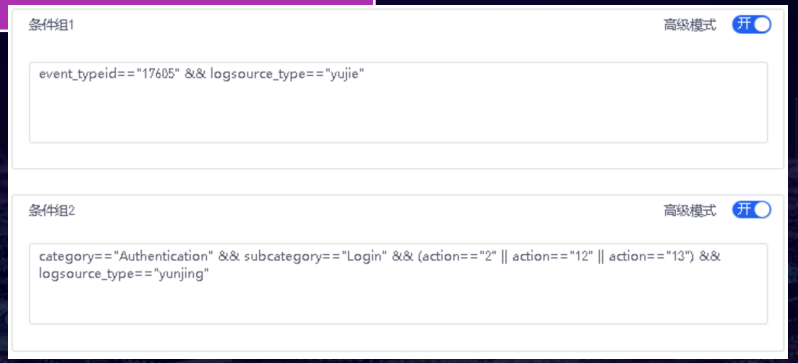
数据归一化

行为链关联分析

流量威胁监控

流量匹配ThinkPHP攻击特征

“index|2F5C|think|5C|”（index/\think\）



全场景关联分析

Web中间件与主机入侵日志关联自动溯源攻击源

不仅在主机侧对Webshell进行处置，同时也发现攻击路径，从而封堵入口！

主机检测Webshell文件

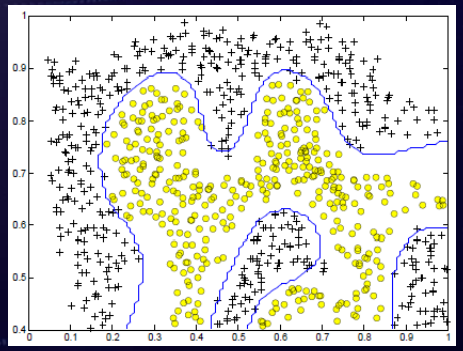
中间件日志详细记录Webshell上传路径

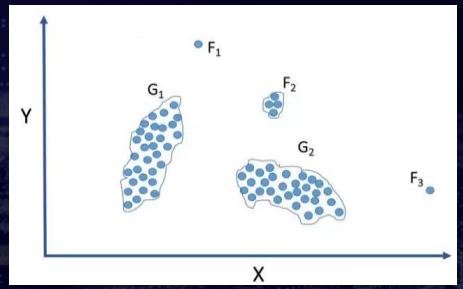
通过时间序列分析Webshell上传行为的上下文，并关联事件形成告警

全场景关联分析

AI与安全技术结合主打业务安全

基于分类结果，抽取异常行为特征，作为有监督分类特征、有监督模型训练、自动化分类识别异常





全场景关联分析

AI与安全技术结合发现行为异常

DNS安全、UDP通讯心跳异常、TCP通讯心跳异常

时间	可信度	子类别	事件描述
2019-07-22 22:47:10	5	DGA可疑域名	

src_ip:10.[redacted]254.249 domain:jjixsfqak.com datatime:2019071719 src_port:14924 timestamp
w_id:1002375977537728 dest_port:53 rcode:NXDOMAIN dest_ip:202.96.209.5
src_ip:10.129.254.249 domain:ehzejp.com datatime:2019071718 src_port:24644 timestamp:
d:2148148692074015 dest_port:53 rcode:NXDOMAIN dest_ip:114.114.114.114
src_ip:10.[redacted]254.249 domain:zke1ev3n.me datatime:2019071016 src_port:32267 timestamp
w_id:554633109953093 dest_port:53 rcode:NXDOMAIN dest_ip:114.114.114.114
src_ip:10.129.254.249 domain:qgizgnuzdaxru.host datatime:2019070520 src_port:4101 time
xru.host flow_id:1956731920253143 dest_port:53 rcode:NXDOMAIN dest_ip:223.5.5.5
src_ip:10.[redacted]254.249 domain:jqveynocrjuqru.HOST datatime:2019070520 src_port:12767 ti
rjuqru.host flow_id:472071246043199 dest_port:53 rcode:NXDOMAIN dest_ip:114.114.114.
src_ip:10.[redacted]254.249 domain:yumunvfkubcmdip.HOST datatime:2019070520 src_port:5801
nvfkubcmdip.host flow_id:2076853624646617 dest_port:53 rcode:NXDOMAIN dest_ip:202
src_ip:10.[redacted]254.249 domain:rwtxrvvrnympob.host datatime:2019070520 src_port:49516 ti
ympob.host flow_id:554652780678262 dest_port:53 rcode:NXDOMAIN dest_ip:223.5.5.5
src_ip:10.[redacted]254.249 domain:mzyfmeox.HOST datatime:2019070520 src_port:22042 timest
ost flow_id:2063320178373294 dest_port:53 rcode:NXDOMAIN dest_ip:202.96.209.5

异常分	异常类型	源IP	目的IP
5	TCP网络心跳	10.1[redacted].10.48	10.1[redacted].66.98
5	TCP网络心跳	10.1[redacted].88.24	10.1[redacted].74.241
5	TCP网络心跳	10.1[redacted].76.10	10.1[redacted].74.241
5	TCP网络心跳	10.1[redacted].110.52	10.1[redacted].74.241
5	TCP网络心跳	10.[redacted].19.224	10.1[redacted].55.28
5	TCP网络心跳	10.1[redacted].88.84	10.1[redacted].74.241
3	UDP网络心跳	10.[redacted]9.170.35	8.8.8.8


感 谢 聆 听


感 谢 聆 听


感 谢 聆 听