CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

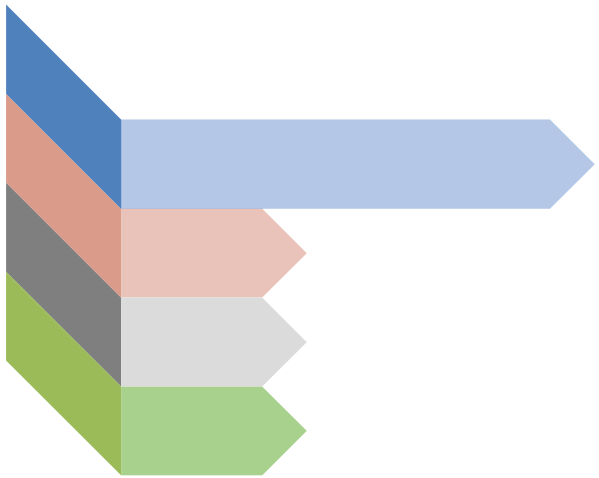
可信云大会

中国·北京 2019.7.2-3

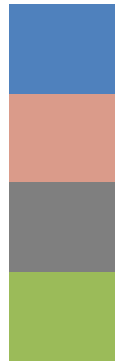
《面向云计算的安全解决方案 第一部分：态势感知平台》标准解读

演讲人：孔松

kongsong@caict.ac.cn



背景介绍



安全形势日益严峻，传统安全体系遭遇瓶颈

全球网络安全态势日益严峻，非法利用和破坏信息系统成为有组织的犯罪行为，攻击手段和工具日新月异，带来的损失难以估量。

云计算成为新一代关键信息基础设施，为企业 IT 建设带来便利的同时，也让安全边界变得模糊甚至消失，安全体系建设亟需突破。

安全数据量大，重复告警；

设备孤立，难以有效协作；

被动防御遭遇瓶颈；

环境复杂，缺少宏观视角。

大数据、人工智能迅速发展，提供技术支撑

面临的问题

安全数据量大

安全数据种类多

安全事件割裂

整体状况难以描述

大数据技术

海量存储

支持多种数据类型

并行计算

高效查询

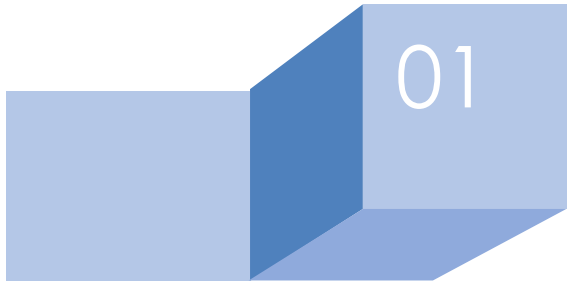
人工智能技术

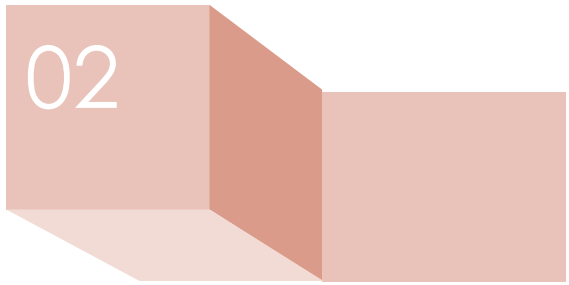
智能检测

智能预测

政策驱动，为产业发展指明方向

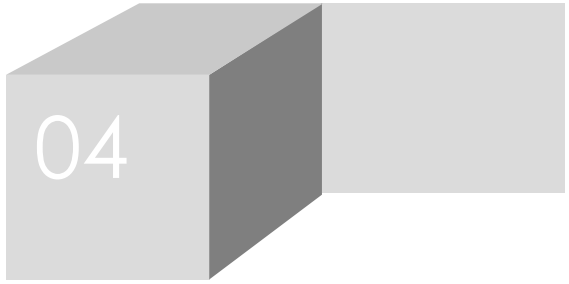
2015年公安部《关于加快推进网络与信息安全通报机制建设的通知》，明确要求建设**网络安全态势感知监测通报平台。**





国务院《“十三五”国家信息化规划的通知》明确提出要全天候全方位感知网络安全态势，**加强网络安全态势感知、监测预警和应急处置能力建设。**

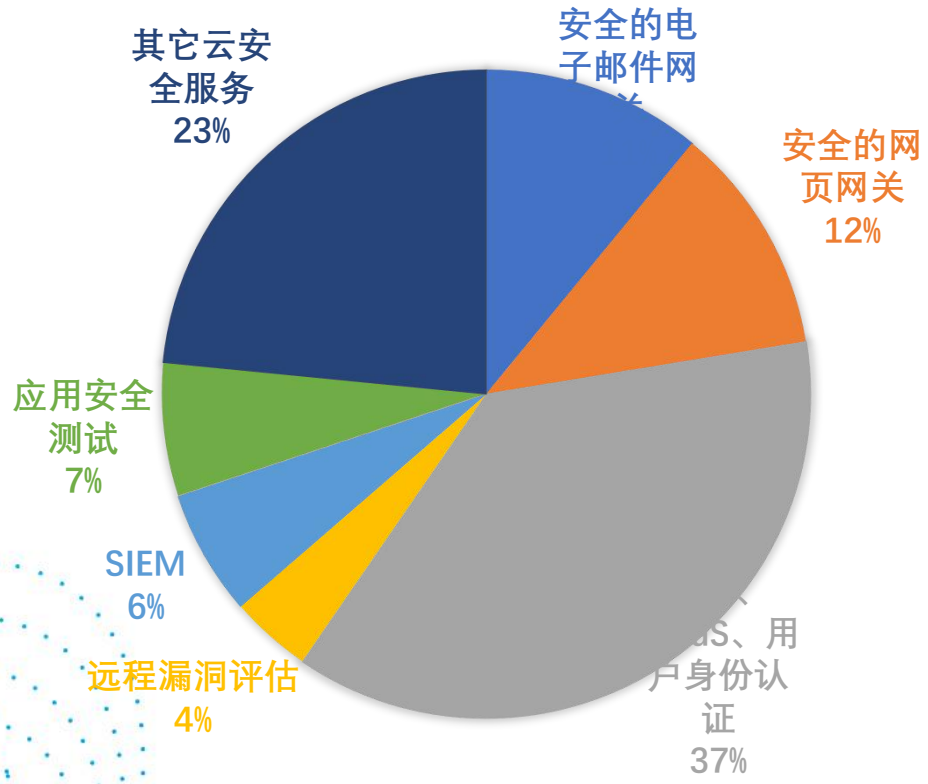
《中华人民共和国网络安全法》提出建立**网络安全监测预警与信息通报制度**，将网络安全监测预警和信息化通报法制化。



2016年4月19日，习近平总书记在网络安全与信息化工作座谈会上提出：要梳理正确的网络安全观，加快建设关键信息基础设施安全保障体系，**全天候全方位感知网络安全态势**，增强网络安全防御能力和威慑能力。

市场发展迅速，企业纷纷布局相关产品

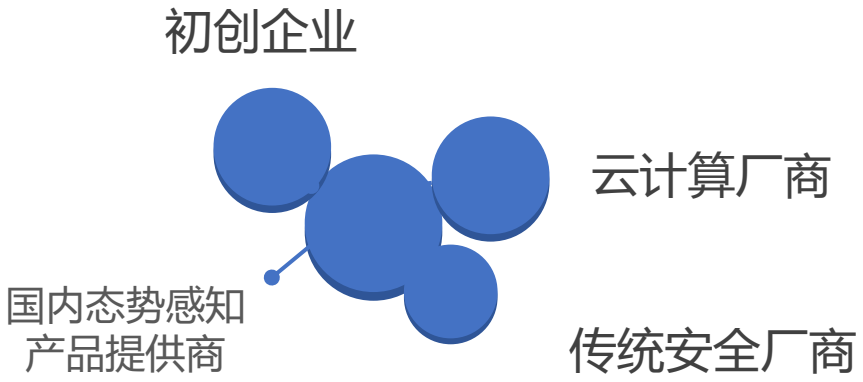
2018年全球云安全产业结构



来源：Gartner前瞻产业研究院
总规模：6862.9百万美元

- 2018年全球SIEM市场达430百万美元
- 预计2020年全球SIEM市场达606.7百万美元
- 同比增长**41.09%**

- 2017年我国态势感知市场规模约20亿人名币
- 预计2020年我国态势感知市场规模达50亿元
- 同比增长**150%**



态势感知竞争环境复杂，缺少标准规范产业有序发展

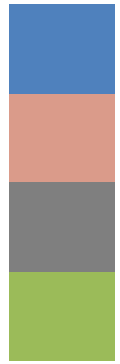
什么是态势感知?

哪些是基本功能?

与SOC有什么区别?

功能要实现到什么程度?

工作介绍



制定面向云计算的态势感知标准，规范产业有序发展

TRUSTED CLOUD SUMMIT
可 信 云 大 会

中国信息通信研究院牵头
联合**数十家科技公司**，开展面向云计算的态势感知标准研究

腾讯、神州泰岳、华为、数梦工场、京东云、浪潮云、中兴通讯、烽火通信、华大基因、国舜、安恒、新华三、移动政企、白山云、华云、楚天云、贝斯平、360、畅捷通

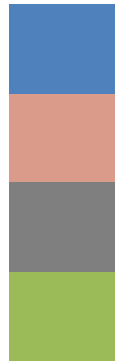
2019年3月26日

2019年4月9日

2019年5月10日

2019年6月21日

标准内容



面向云计算的安全态势感知平台定义

认知一定时间和空间内的环境要素，理解其意义，并预测它们即将呈现的状态，以实现决策优势

态势感知

指利用大数据、机器学习等技术，对安全态势相关的**海量数据**进行提取与多维度**关联分析**，提供对安全风险的监控与告警、处置与响应、**大屏展示**和**趋势预测**的平台。

态势感知平台

感知环境为用户云计算环境。
部署方式分两种：
SaaS模式
私有化部署

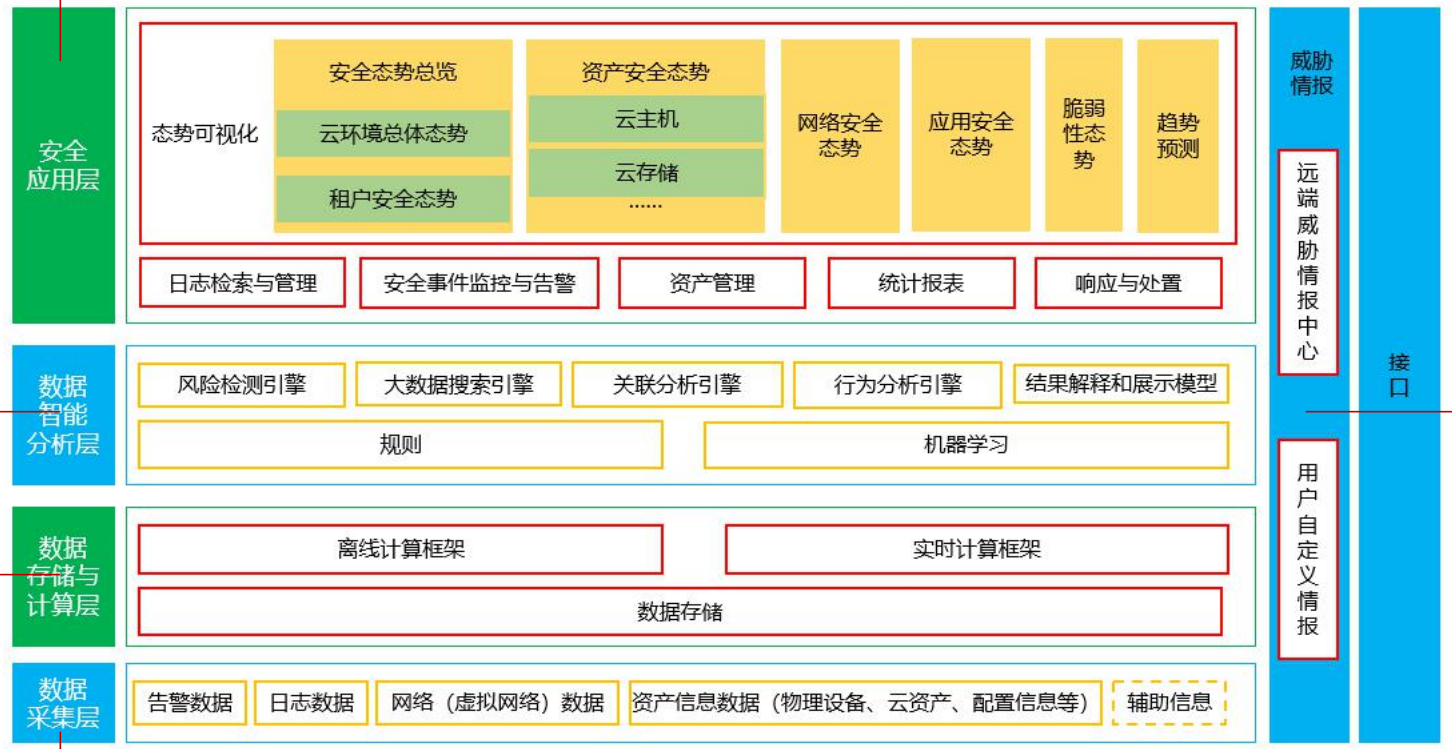
面向云计算的态势感知平台

面向云计算的安全态势感知平台功能框架

基于不同安全管理目标的多种安全应用模块

建立多种数据分析引擎，为不同安全管理目标提供支撑

对数据进行存储，通过计算框架完成数据智能分析层中各算法逻辑所需的海量数据计算



为态势感知平台提供额外的数据支撑，提高风险问题的识别准确率

对云环境下安全态势相关的多种异构数据进行采集与预处理

面向云计算的安全态势感知平台特点

- 数据采集能力能够适应云环境下资产的动态变化
- 与云管理平台的关联
- 多租户的划分和管理
- 与云环境联动，实现平台自身计算能力、存储能力的弹性扩展
- 跨云的管理能力

面向云计算的安全态势感知平台建设原则

01 易用性
快速部署
使用与帮助文档
专家支持

02 动态性
支持的数据源的发展
威胁情报中心的发展
算法模型优化升级

03 兼容性
与原系统架构的兼容
与第三方设备/软件/厂商的兼容

04 可靠性
不低于99.95%的可靠性
不影响用户的业务
多可用区部署

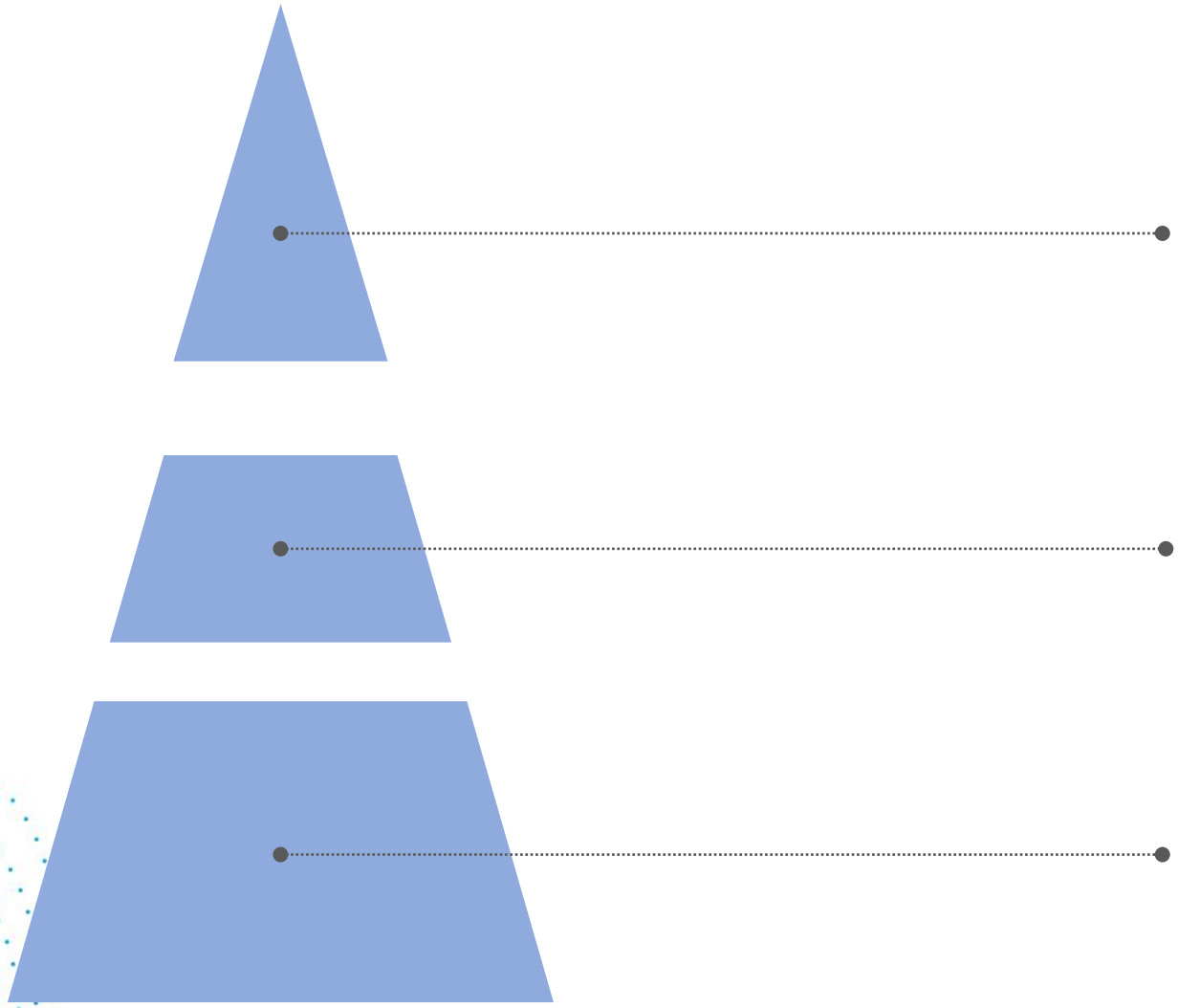
05 通用性
大部分通用+小部分定制开发

06 可管理性
用户管理
权限管理

07 安全性
平台自身具备安全防护能力

08 可扩展性
API接口和层级结构
功能模块化
计算、存储和网络的弹性扩容
分布式部署和级联部署

数据采集层能力要求



数据预处理

支持结合和非结构化数据
数据完整性、一致性和准确性校验
归一化、分类、过滤和合并处理

数据采集能力

自主采集
用户导入
接入采集传感器数据
获取跨云数据

数据源

安全设备、安全软件或云安全服务产生的**告警数据**
云管平台、系统或服务产生的**日志数据**
网络（虚拟网络）数据
资产信息，物理设备、云上资产、配置信息等
辅助信息，用户注册信息、组织架构、业务信息等

数据存储与计算层能力要求

数据存储

支持PB级别数据量的存储
敏感数据加密存储
多副本备份
存储时间
存储位置

数据计算框架

实时计算框架

↓

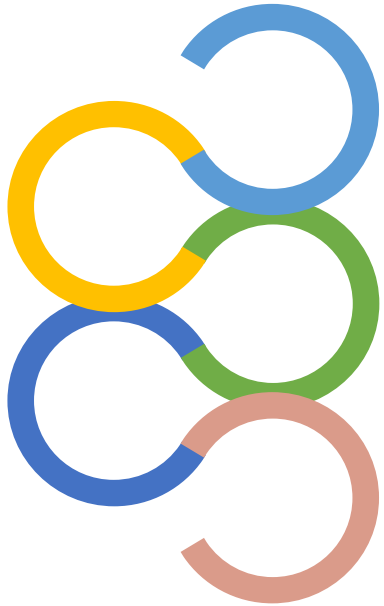
静态数据批处理

离线计算框架

↓

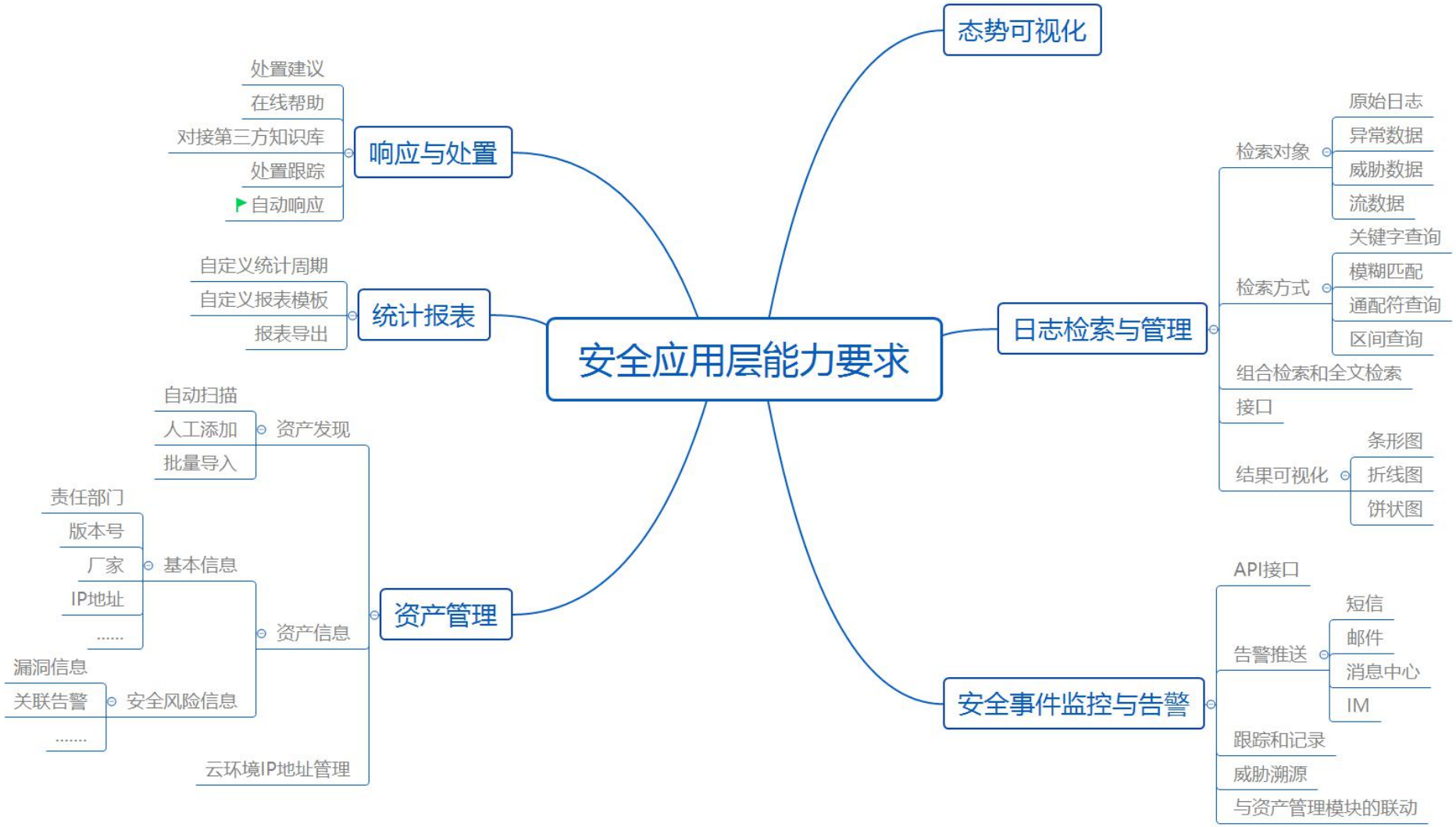
动态数据实时分析

数据智能分析层能力要求



- 风险检测
  - 风险检测模型/集成第三方
  - 模型组件，用户自定义场景
- 行为分析
  - 用户异常行为
  - 网络异常行为
  - 应用异常行为
- 关联分析
  - 多维度（时间、空间）
  - 与行为分析关联
  - 关联分析规则组
  - 告警信息聚类
- 大数据搜索
- 结果解释和展示
  - 可视化、交互分析模型
  - 评分模型

安全应用层能力要求


安全应用层能力要求
态势可视化
响应与处置
处置建议
在线帮助
对接第三方知识库
处置跟踪
自动响应
统计报表
自定义统计周期
自定义报表模板
报表导出
资产管理
资产发现
自动扫描
人工添加
批量导入
资产信息
基本信息
责任部门
版本号
厂家
IP地址
.....
安全风险信息
漏洞信息
关联告警
.....
云环境IP地址管理
日志检索与管理
检索对象
原始日志
异常数据
威胁数据
流数据
检索方式
关键字查询
模糊匹配
通配符查询
区间查询
组合检索和全文检索
接口
结果可视化
条形图
折线图
饼状图
安全事件监控与告警
API接口
告警推送
短信
邮件
消息中心
IM
跟踪和记录
威胁溯源
与资产管理模块的联动

态势可视化

安全态势总览

云环境安全状态打分评级
云主机地域分布和总体安全状态
安全风险总数和类型分布图
历史趋势图
租户安全态势（私有化部署）

资产安全态势

资产总数
风险资产和处置情况
按风险对资产归类展示
历史趋势图

网络安全态势

攻击来源地分布
攻击时间分布
攻击类型分布
历史趋势图

应用安全态势

云上应用安全状态

按风险系数进行排序

脆弱性态势

操作系统、中间件等的漏洞

漏洞总数、类型分布和危害等级

趋势预测

安全事件周期性预测

攻击类型和地域的预判

威胁情报能力要求

威胁情报数据更新

威胁情报的主动拉取

威胁情报的自动推送

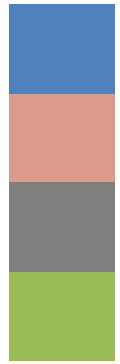
威胁情报的查询

多种主流格式

批量导入

实时添加

工作计划



未来工作计划

建立健全云计算安全标准体系：

态势感知平台
安全运营中心
安全责任划分模型
身份识别与访问管理
云WAF
云抗DDoS
……

标准制定

测试评估

19年下半年开展云计算安全解决方案评估：

面向云计算的态势感知平台
面向云计算的安全运营中心
基于云计算的业务安全解决方案（金融反欺诈）
……

CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

可 信 云 大 会

中国·北京　2019.7.2-3

THANKS