CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

可信云大会

中国·北京　2019.7.2-3

北京燃气集团云安全实践分享

演讲人：方铁城

北京燃气简介

北京燃气
BEIJING GAS

气融万物，惠泽万家

北京市燃气集团是全国最大的单体城市燃气供应商，管网规模、燃气用户数、年用气量、年销售收入均位列全国前茅。天然气应用范围已经从民用炊事发展到工业、采暖、制冷、发电、燃气汽车、分布式能源等诸多领域，北京燃气已经成为中国燃气行业最具影响力的品牌之一

北京市

第一个登陆境外资本市场的公用事业企业

行业内

第一个取得高新技术企业资质的集团级企业（2011年）

国内

第一个单体城市天然气购销量突破百亿的企业（2014年）

第一个单体城市日天然气购入量破亿的企业（2015年）

全球

北京市年用气量仅次于莫斯科，达全球第二（2016年）

2017年10月26日，李雅兰董事长当选为**IGU 2021—2024年任期主席**，北京同时获得2024年第29届世界燃气大会主办权。

云的分类

用户使用 | 甲方IT提供 | 私有云提供商提供 | 公有云服务商提供

	私有云			公有云		
传统架构	IaaS	Paas	Saas	IaaS	Paas	Saas
人	租户	租户	租户	租户	租户	租户
数据	数据	数据	数据	数据	数据	数据
应用	应用	应用	应用	应用	应用	应用
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime	Runtime
中间件	中间件	中间件	中间件	中间件	中间件	中间件
操作系统	操作系统	操作系统	操作系统	操作系统	操作系统	操作系统
	虚拟化	虚拟化	虚拟化	虚拟化	虚拟化	虚拟化
	Hypervisor	Hypervisor	Hypervisor	Hypervisor	Hypervisor	Hypervisor
安全	主导定制安全	主导定制安全	主导定制安全	购买安全	购买安全	安全
物理服务器	物理服务器	物理服务器	物理服务器	物理服务器	物理服务器	物理服务器
网络和存储	网络和存储	网络和存储	网络和存储	网络和存储	网络和存储	网络和存储
数据中心	数据中心	数据中心	数据中心	数据中心	数据中心	数据中心

云安全的注意事项

共同要求	私有云	公有云
合规要求（等保2.0）	与现有安全架构的融合	对各层服务水平协议的承受度
安全投资估算	纵深防御	合同（甲乙责任、默认条款、免责条款）
架构安全		安全审计
安全风险（人、技术、流程）		业务形态所需安全
数据安全		安全回退方案

等保2.0中的云安全

第三等级

安全通用要求
- 1安全物理环境 (10)
- 2安全通信网络 (3)
- 3安全区域边界 (6)
- 4安全计算环境 (11)
- 5安全管理中心 (4)
- 6安全管理制度 (4)
- 7安全管理机构 (5)
- 8安全管理人员 (4)
- 9安全建设管理 (10)
- 10安全运维管理 (15)

+

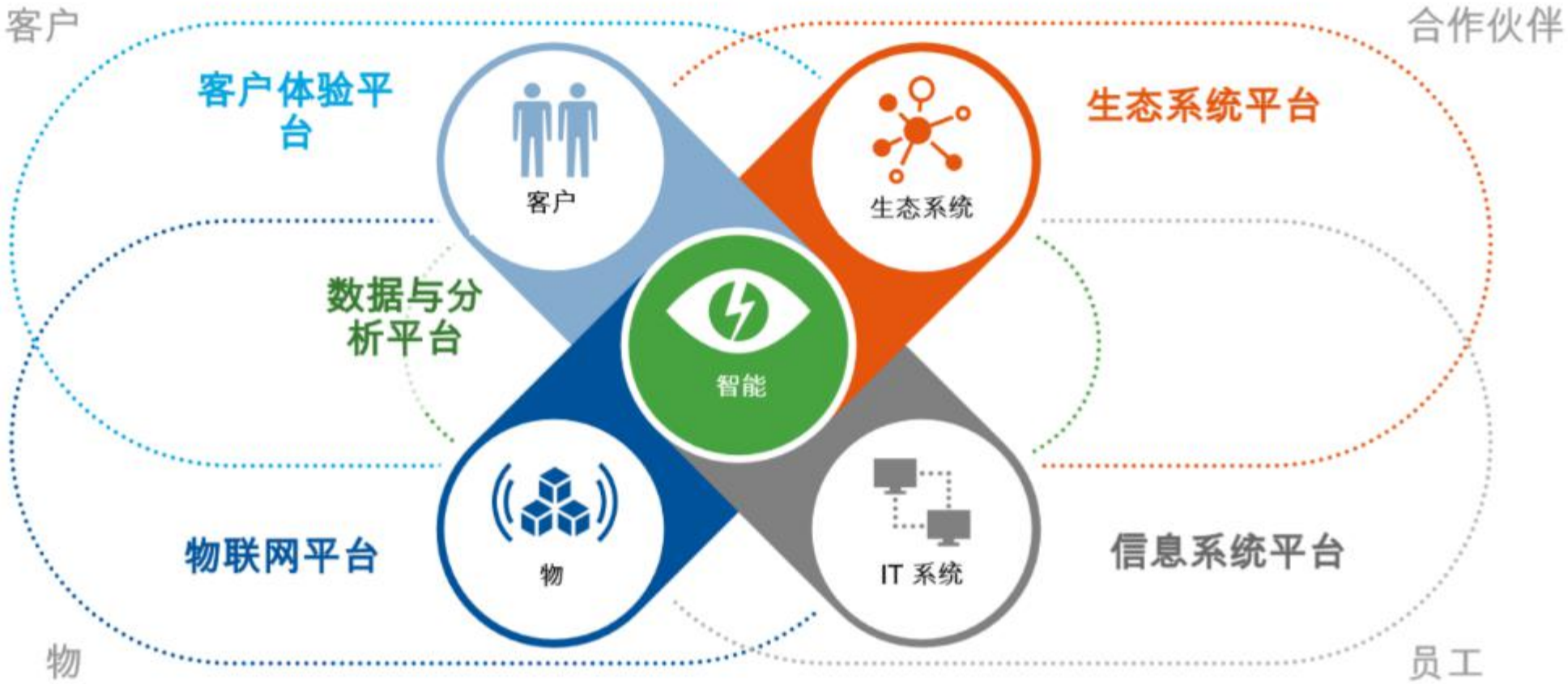
云计算安全扩展要求
- 1安全物理环境
  - 1基础设施位置
    - 应保证云计算基础设施位于中国境内
- 2安全通信网络
  - 1网络架构
- 3安全区域边界
  - 1访问控制
  - 2入侵防范
  - 3安全审计
- 4安全计算环境
  - 1身份鉴别
  - 2访问控制
  - 3入侵防范
  - 4镜像和快照保护
  - 5数据完整性和保密性
  - 6数据备份恢复
    - a云服务客户应在本地保存其业务数据的备份。
  - 7剩余信息保护
- 5安全管理中心
  - 1集中管控
- 6安全建设管理
  - 1云服务商选择
    - b应在服务水平协议中规定云服务的各项服务内容和具体技术指标
    - c应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
    - e应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。
  - 2供应链管理
- 7安全运维管理
  - 1云计算环境管理

+

其他要求

北燃云平台建设规划

参考Gartner数字化平台架构、GE Predix平台、中石化ProMACE平台，规划燃气数字化云平台。



北燃云平台建设目标

北燃云整合北京燃气信息资源，建设集中、协同的技术支撑平台，营造敏捷安全的IT环境，支撑业务应用，为实现数字转型奠定基础。

01

搭建北燃云，作为数字化转型基础

- 引入先进的“厚平台薄应用”理念，北燃云作为数字化转型的一部分重要内容

02

为企业数字化转型提供全方位支撑

- 在IaaS、PaaS、SaaS方面进行业务支撑
- 微服务支撑
- 敏捷能力支撑

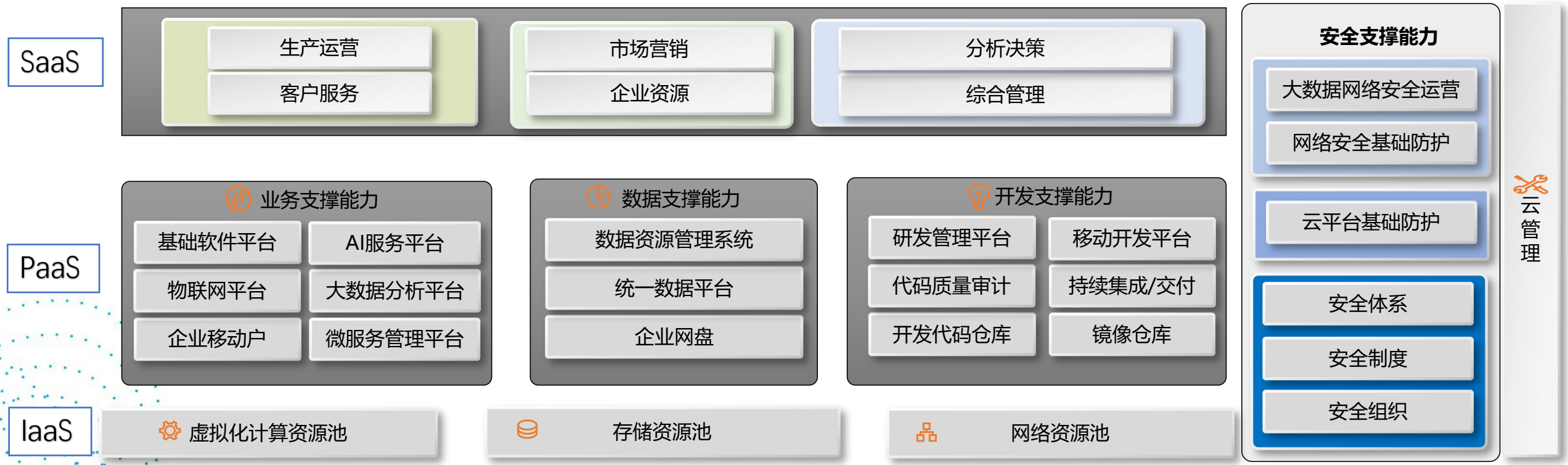
03

在云平台上结合大、物、移、智等技术，实现北燃数字化转型

- 通过与现有成熟智能应用技术的有效结合，在北燃云上快速开发或部署基于语音识别、用户行为分析、管网智能应用等技术，实现数字转换新业务，快速提高燃气智能化应用水平，解决企业疑难问题，增强客户服务体验，提高企业运营能力与企业竞争力。

北燃云平台功能架构

- **平台承载各个业务应用：**平台与应用解耦、硬件与软件分离、基础设施云化、平台持续演进、核心架构自主掌控、应用快速构建。
- **平台服务范围：**根据业务特征整合资源，提供IaaS、、PaaS、SaaS业务支撑、开发支撑等能力。



安全组织

网络安全和信息化领导小组

组长	**董事长、总经理**
副组长	**各相关集团领导**
成员	**集团总部各部室正职、各专业机构主要负责人、集团所属各单位书记、总经理**

按照上级单位网络安全和信息化工作方针、政策以及北京燃气集团发展战略，统一领导集团网络安全和信息化发展，确立网络安全和信息化宏观战略规划、方针政策，对网络安全和信息化重要问题进行决策。

网络安全和信息化领导小组办公室

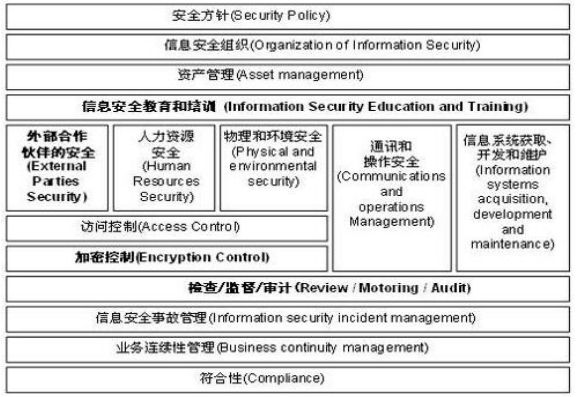
办公室主任	**主管副总**
副主任	**网络安全总监、网络安全副总监、相关领导**

设置专职安全督查岗位，办公室主要职责：
1、贯彻落实领导小组制定的发展战略、方针政策、总体规划及专项技术规划，研究制定相应实施方案；
2、负责组织网络安全和信息化规划的落地；
3、负责组织制定网络安全与信息化相关制度、流程、标准及规范；
4. 负责审议集团网络安全与信息化年度计划草案；
5. 负责组织审议网络安全与信息化重大项目相关方案和报告；
6. 负责网络安全与信息化工作的指导、监督、检查及考核工作；
7. 负责网络安全整体管理，落实网络安全检查、评估、整改及考核工作；
8. 负责协调解决重大网络安全问题和网络安全事件的应急响应工作；
9. 协调、处置网络安全与信息化工作遇到的问题；
10. 承办领导小组交办的其他事项。

集团各部室、各专业机构以及各分子公司

安全体系

通过对标国际网络安全标准，2015年完成信息档案中心ISO27001的信息安全管理体系国际认证工作，并于2018年完成三年一次的信息安全管理体系认证换证工作。




bsi.

Audit Plan 评审日程表 – CAV2 监督审核

Report No.:8643981
报告编号:

No. of Manday(s) 评审人天数:2.5MD+1.5 MD offsite
Sheet Number 页 数: 1 of 3

Client Name 客户名称: 北京市燃气集团有限责任公司信息档案中心 79595162-6			
Registered Address 认证地址: 中国北京西城区西直门南小街 22 号 100035			
Tel No. 电话号码: +86 10 63913717	Fax No. 传真号码: +86 10 66205670	E-mail 电邮地址: shenyanfong@bjgas.com	
Audit Objectives 审核目的: 确认被认证组织的管理体系在认证范围的所有方面是否有效运行并满足认证标准的要求。			
Scope of Registration 认证范围: 信息档案中心为集团公司提供经营管理类信用环境建设和维护、信息化标准化和编码建设、数据资源管理、信息安全管理、信息化基础设施建设和维护以及档案管理的服务。这参照了 2015-8-24 发布的版本为 1.0 的适用性声明。			
Accreditation Mark(s) 认证标志: ANAB	BSI Reference 内部参考: 47380260	T-code 专业技术代码:T05 B	
Management Standard 认证标准:	ISO27001: 2013		
Management System Manual ref. 管理系统文件:	综合管理体系手册		
Opening Meeting Date/Time 首次会议日期/时间:	21/9/2017 9:00- 9:20		
Closing Meeting Date/Time 末次会议日期/时间:	22/9/2017 16:30- 17:30		
Company Representative 公司代表:	申 彦 龙 先生		

BSI Audit Team BSI 审核组: 具有本次审核代码(T/P/S)的成员:

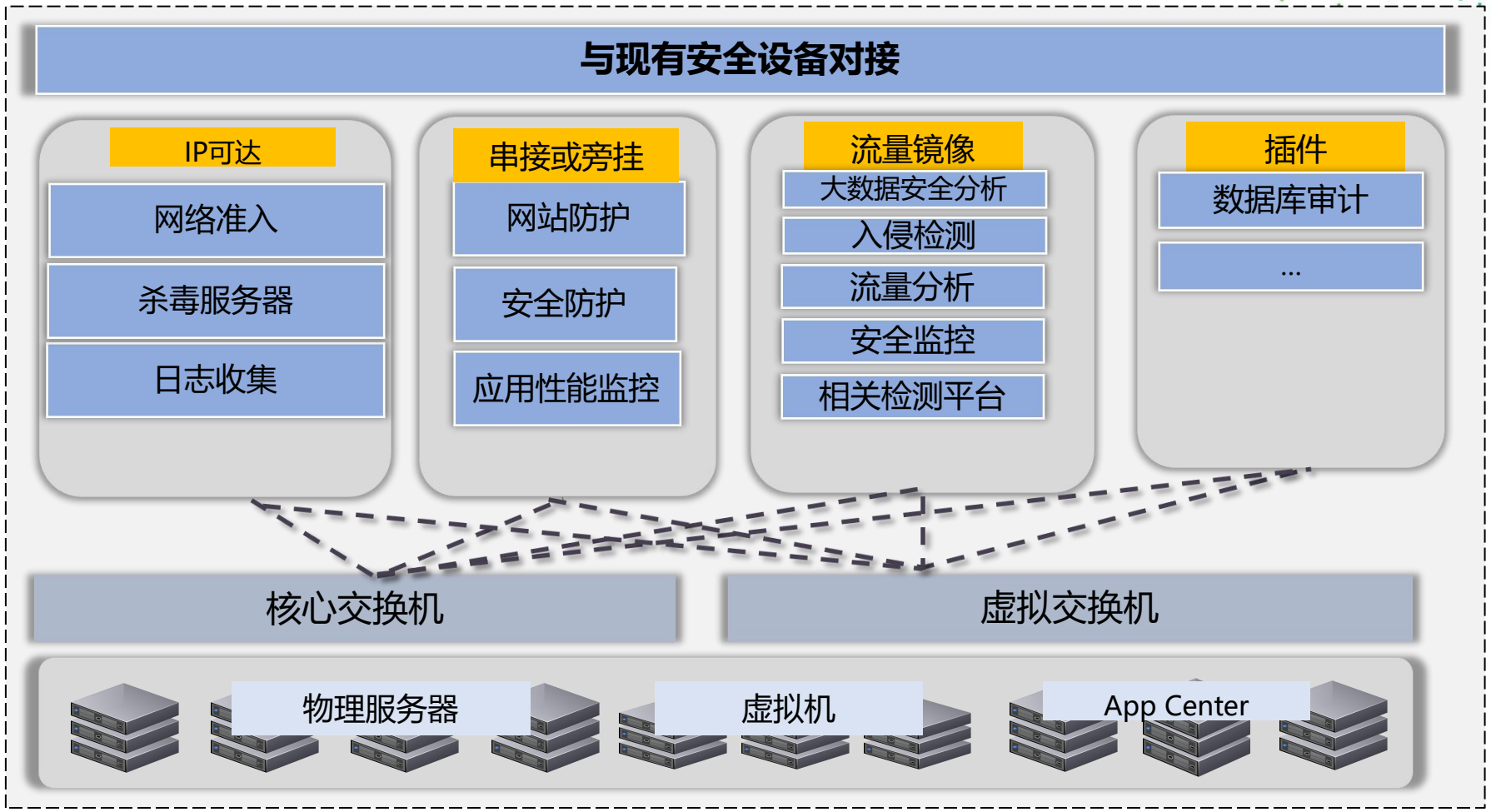
Team Leader 组长:	Ms. Liyan Jin 金立艳女士 15652190658	(Team A 组一)	T05/P27001A
组员:	Mr. Vincent Pan 潘炳	(Team B 组二)	T05/P27001A

通过开展风险评估、网络安全制度体系的修订和完善、建立内部信息安全测量指标、组织内部的信息安全审核，最终通过信息安全外部审核机构的审核。

云平台基础防护

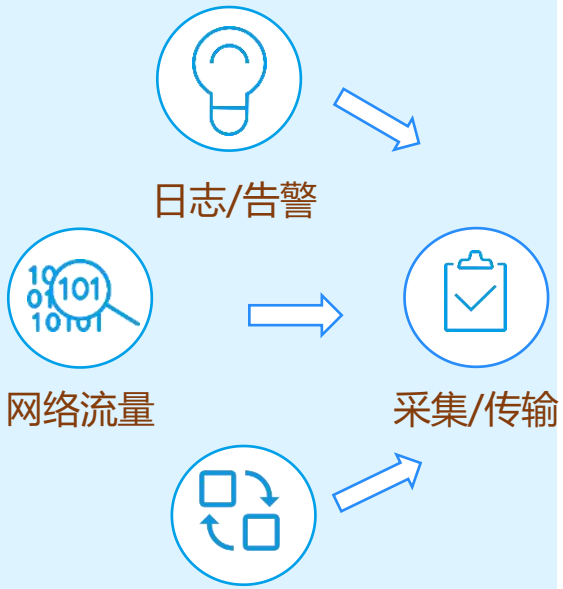

安全管理
安全监控
安全合规
法规遵从
虚拟机安全
VM异常行为防护
VM安全体检
VM状态监控
VM防火墙
VM防病毒
云平台虚拟机安全
(防盗门内)
云平台安全
私有网络隔离
VM内存隔离
VM存储隔离
传输加密
存储加密
分布式防火墙
云平台租户安全
(防盗门)
边界网络安全
防火墙管理
流量清洗
入侵检测
入侵防御
第三方服务
管理系统安全
双因素认证
Web安全
子账号
权限控制
云平台基础安全
(防盗门外)
机房基础设施安全

与现有安全架构进行融合



基于已知风险的安全运营

风险收集



分析预警

- 场景分析
- 交互/可视化
- 机器学习
- 深度学习
- 关联分析
- 威胁情报
- 特征匹配
- 统计模型

大数据分析平台

应急处置

短信预警 + 值守预警

判断

快速应急小组（裁决之刃）

设备联动

应急处置

漏洞修复 + 回溯分析

加固提升

- 新购安全设备
- 安全策略优化
- 漏洞修复
- 人员培训考核

基于未知风险的安全运营

风险收集

- 渗透测试
- 安全测评
- 攻防演习
- 安全检查
- 情报收集

分析预警

应急处置

纵深防御

- 减少攻击面
- 增加攻击难度
- 路径设伏
- 全程监控
- 高危人工审计

分析预警

大数据安全分析平台每天产生告警97条，平均每天检测到安全事件3起，一般安全事件响应时间在5分钟以内，有效对安全事件进行检测、监控和处置，保障业务连续性。

设备日志+流量

应用

主机

安全设备

网络设备

总计接入300+

资产信息

VPN信息，终端信息

主机信息，人员信息

总计接入6000+

日志入库

>8亿 条/天

日志量

>1.5T/天

规则利用率80%

- 平台内置820种安全规则库

误报率低于10%

- 根据业务特点建立31个安全场景

严重：2 条

警告：33条

提醒：62条

部分分析场景规则举例

威胁大类	威胁小类	威胁描述
配置错误	网络配置错误	端口中断，地址冲突，DNS配置错误
	主机配置错误	root用户登录，未关闭SSH密码登录
	应用配置错误	网站出现大量5xx访问
		数据库查询异常（次数，响应时间）
违规行为	权限审计	绕过堡垒机登录
		敏感数据访问和操作
	终端审计	开启未知或违规服务
		内网机器非法外连
	内容审计	检测到即时通讯/P2P流量
数据安全	数据外发	u盘大量拷贝文件或大量打印文件
		内网机器向外网大量发送文件
	数据泄露	特定账号从FTP下载大量文件
		FTP账号被暴力破解后窃取数据
		数据库dump操作（数据库拖库）
	数据破坏	特定账号FTP下载文件后上传同名文件
		发现勒索软件
		数据库危险操作或高危命令
账户安全	登录位置异常	多地点异常登录
	登录状态异常	web后台登录次数异常
		多账号登录或同账号多设备登录
	账户状态异常	账号权限异常
		账号密码异常-密码频繁更改
		异常账号或组创建

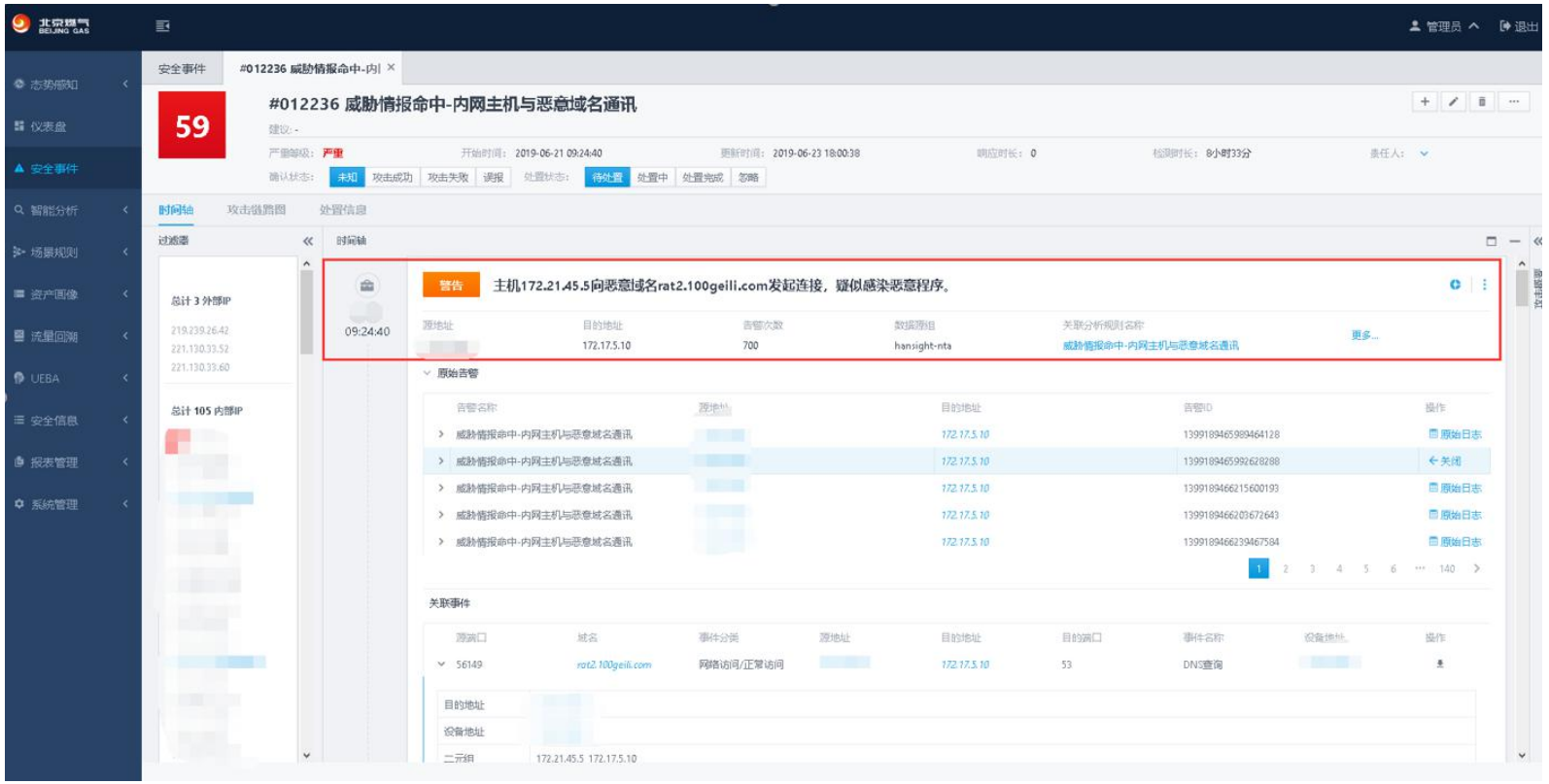
威胁大类	威胁小类	威胁描述
恶意代码	蠕虫	蠕虫传播
		疑似Conficker蠕虫活动
	病毒木马	主机感染病毒，清除病毒失败等
		发现广告程序、黑客工具等
		发现网页木马
		检测到缓冲区溢出事件后发现后门木马连接
	僵尸网络	发现大规模僵尸主机
网络攻击	网站安全	访问异常（高频、异常user-agent访问、robots访问等）
	普通攻击	通用web攻击
		web恶意漏洞扫描
		webshell上传和连接攻击
	关联攻击	网站被植入webshell后发起大量连接或网络扫描
		攻击者登录web后台后尝试上传或植入webshell
		web网页扫描后，发生恶意漏洞攻击或扫描
	主机安全	主机登录安全（账号暴力破解、登录频率异常）
		网络设备认证失败
		内网机器发起攻击（DDoS，web，远程漏洞）
	服务安全	针对特定主机telnet暴力破解
		针对特定主机或账号的FTP暴力破解
		针对主邮件服务器主机或邮件账号的暴力破解，发送频率过高或发送垃圾邮件
		针对数据库主机或账号的暴力破解
		针对VPN主机或账号的暴力破解
	网络安全	网络行为异常（ARP攻击，广播风暴，流量连接和大小异常）
		网络扫描（端口扫描，主机扫描）

部分应急处置案例

外网扫描事件	• 快速定位扫描行为的源头，阻止安全入侵行为
内网挖矿病毒事件	• 挖矿病毒爆发，快速定位被感染主机，及时清除病毒并加固，增加实时检测的漏洞利用行为
外包项目组勒索病毒事件	• 外包项目组携带勒索病毒接入办公网，及时发现并阻断，避免病毒进一步传播
内网主机与恶意域名通讯	• 发现内网主机短时间内发起大量的DNS查询，及时处置，避免内网主机可能的进一步入侵行为。

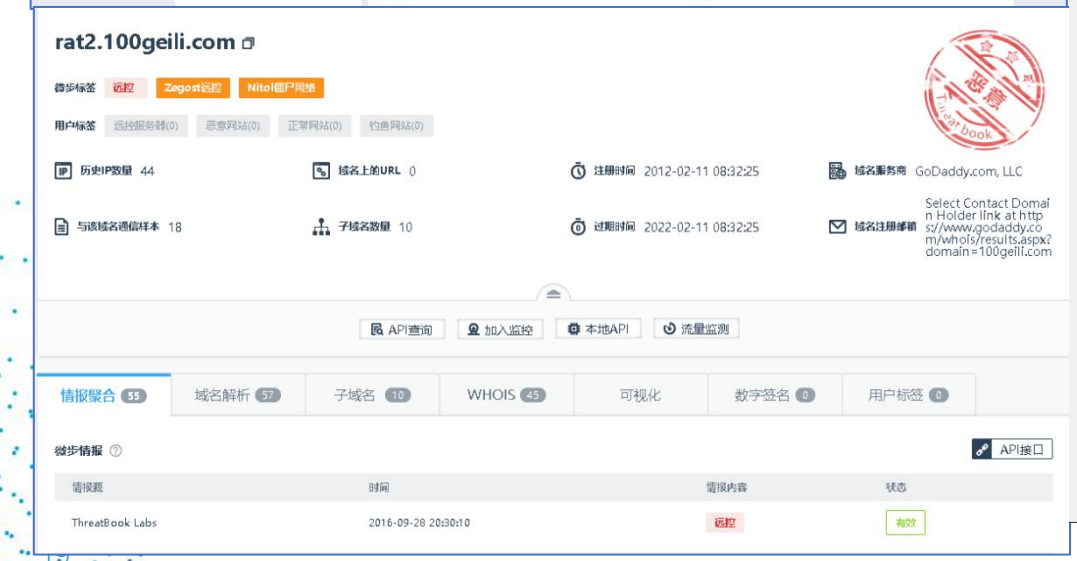
处置案例-内网主机与恶意域名通讯

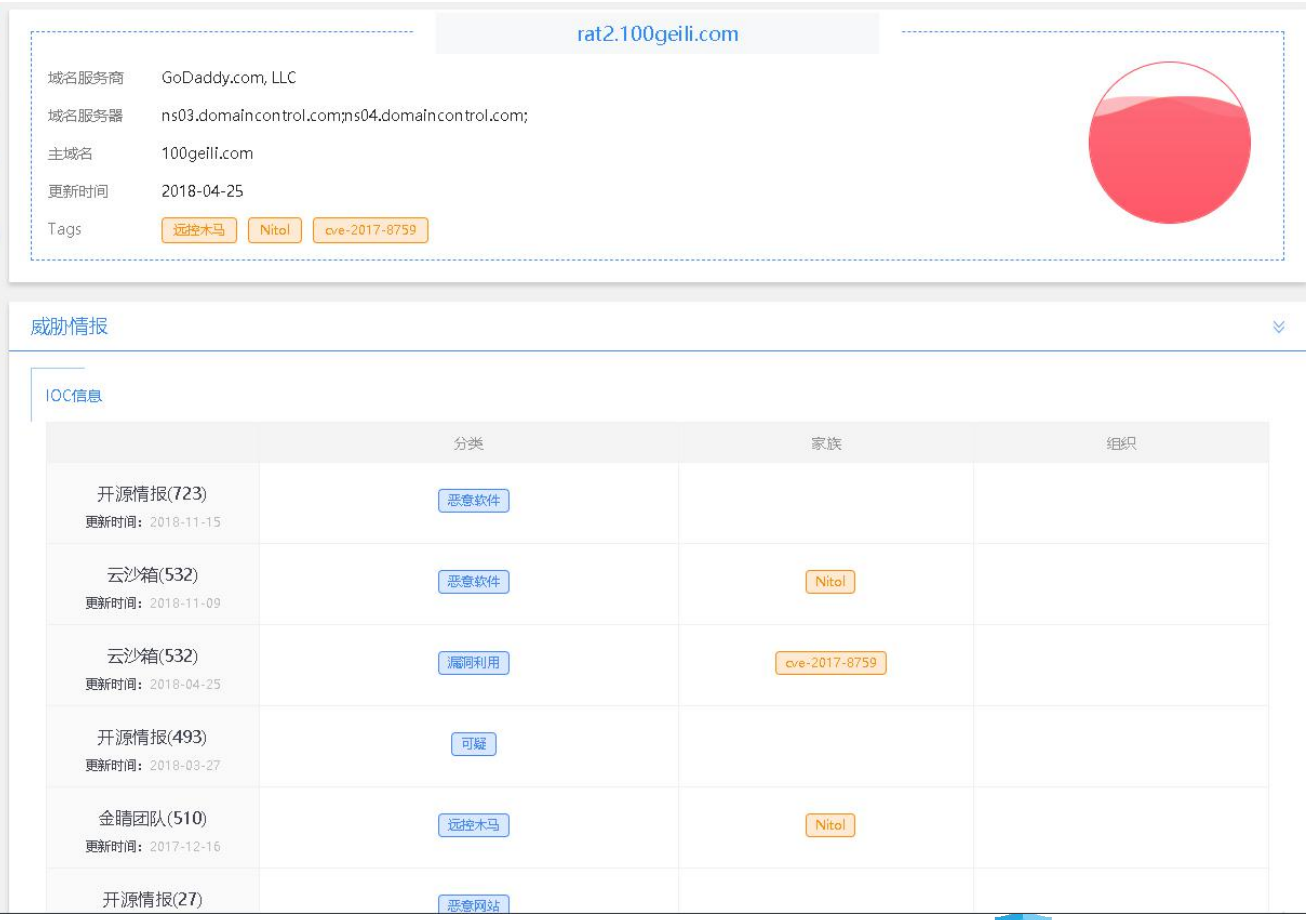
- 2019年6月，大数据安全分析平台告警“威胁情报命中-内网主机与恶意域名通讯”，发现内网主机短时间内发起大量的DNS查询，查询域名疑是恶意域名。



处置案例-关联威胁情报

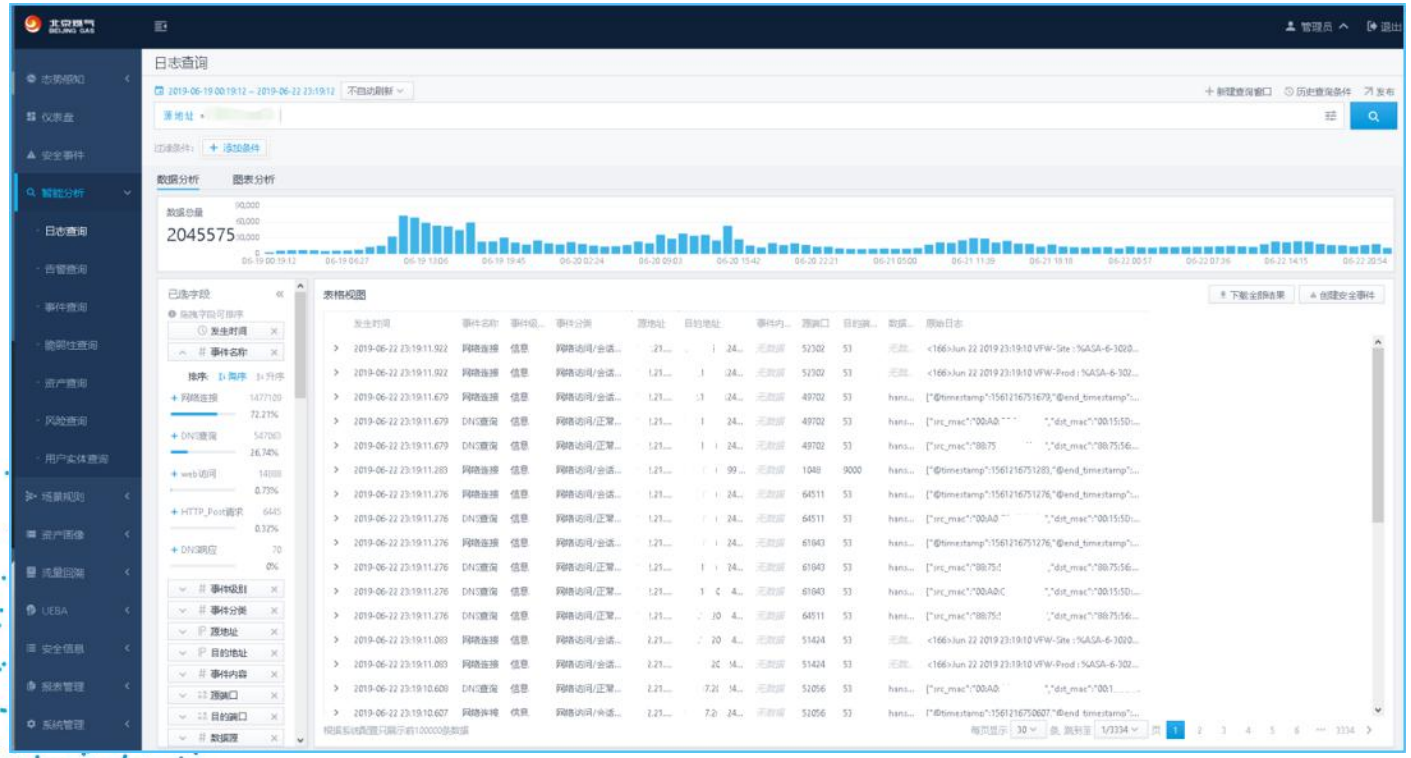
- 将域名关联到威胁情报，发现多家情报标识远控域名，结合告警产生频繁，内网主机疑是感染木马病毒。

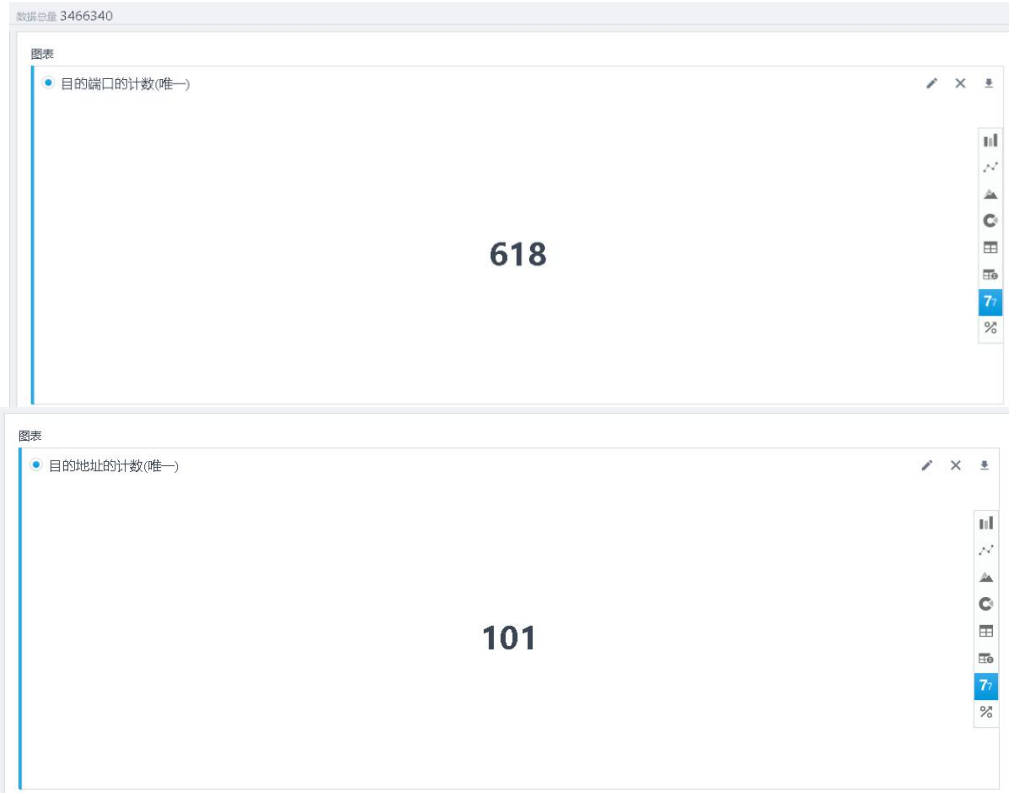




处置案例-历史日志回溯

- 将内网地址下发到原始日志，发现该IP在6.16到6.22之间一直处于活跃状态，且有大量的DNS查询，时间推前，发现除了53端口还存在大量端口连接信息，该主机可能在感染木马后，有对内网主机进行端口探测的行为。





处置案例-应急处置过程

1. 大数据分析平台告警“威胁情报命中-内网主机与恶意域名通讯”。
2. 快速应急小组接到报警后，第一时间根据该终端MAC地址进行断网处置。
3. 同时，根据MAC地址和收集到的终端主机信息，得到终端位置和使用人员姓名。
4. 同时，通知终端维护单位到公司现场进行终端病毒查杀。
5. 计算机终端运维单位达到现场进行病毒查杀。

CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

可 信 云 大 会

中国·北京　2019.7.2-3

THANKS