

TRUCS 2019

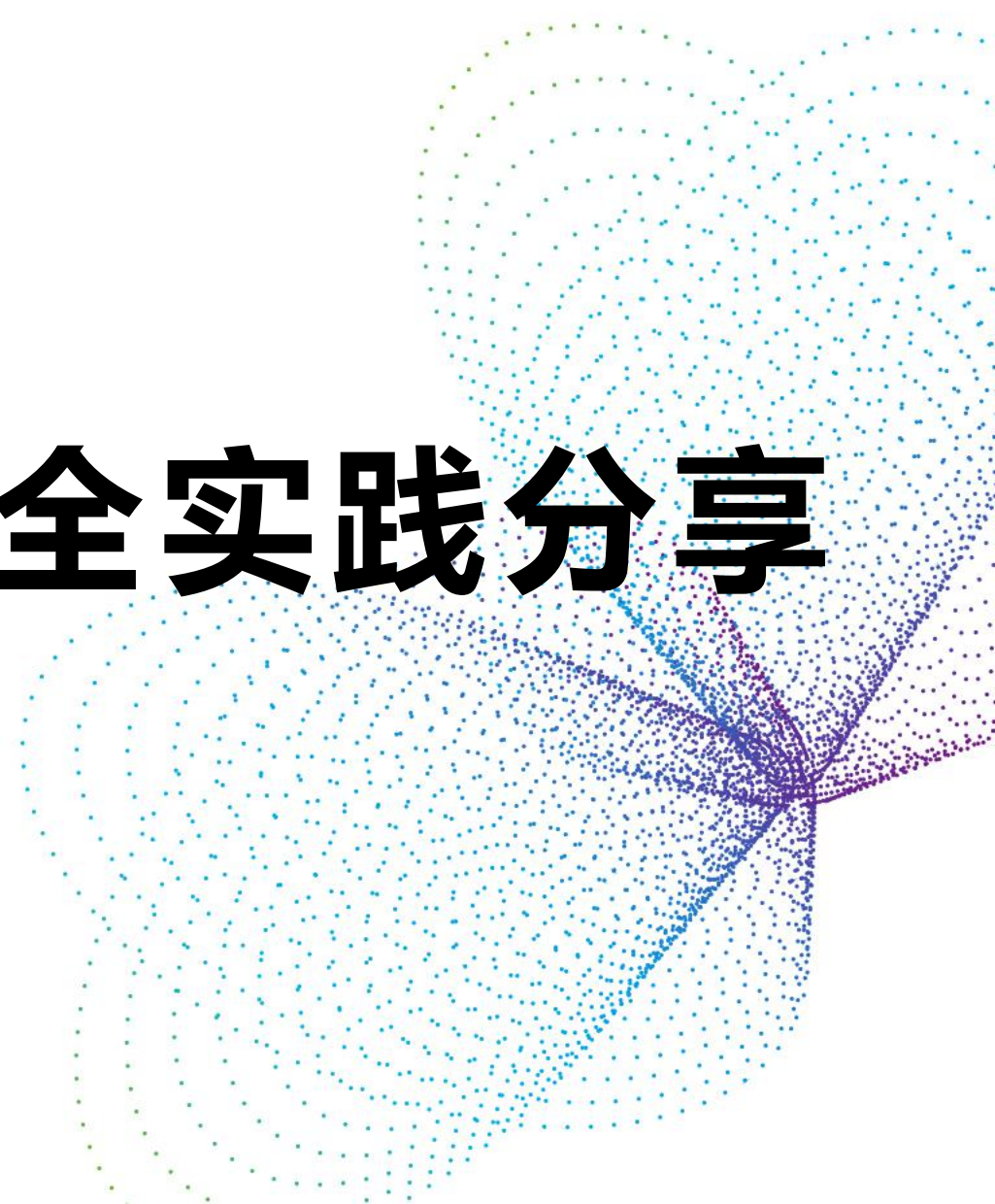
TRUSTED CLOUD SUMMIT

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

TRUSTED CLOUD SUMMIT
可信云大会



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

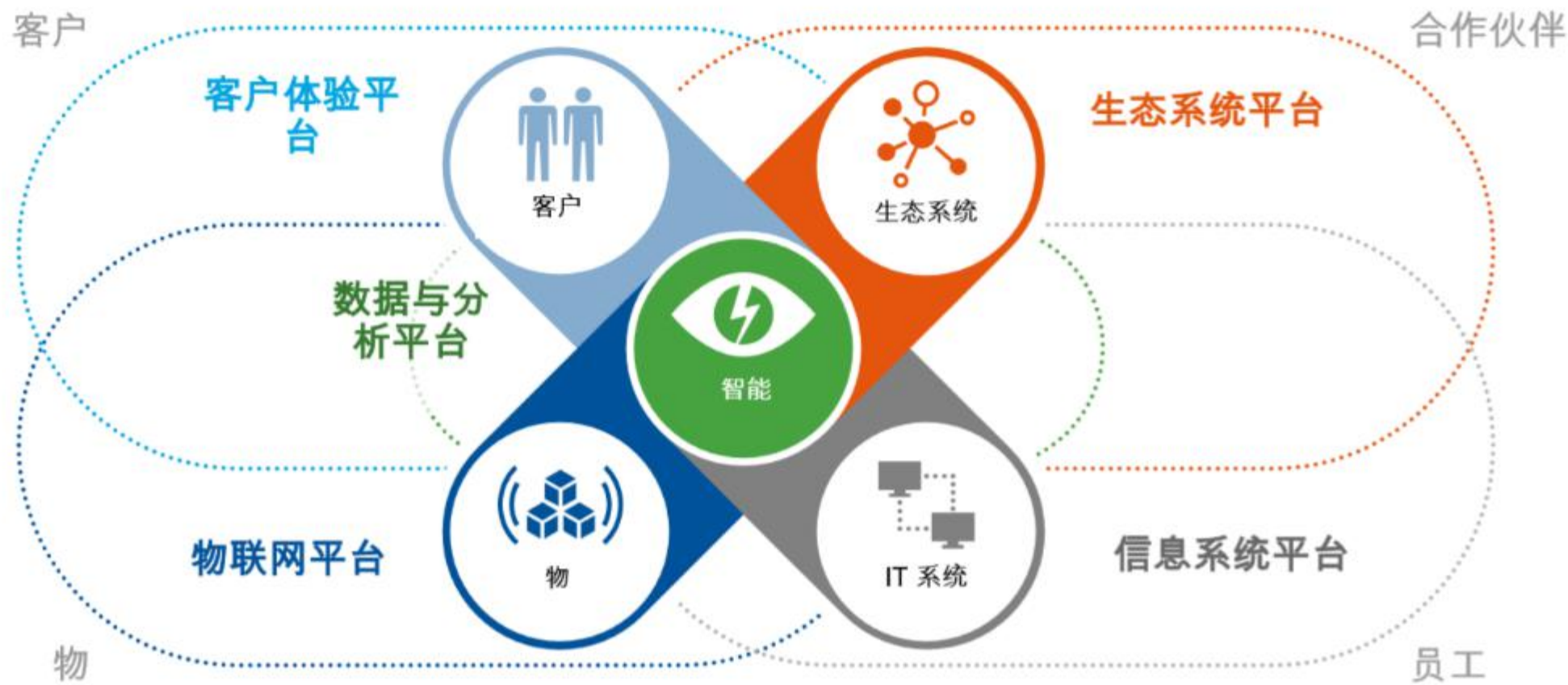
- 1安全物理环境
 - 1基础设施位置 应保证云计算基础设施位于中国境内
- 2安全通信网络
 - 1网络架构
- 3安全区域边界
 - 1访问控制
 - 2入侵防范
 - 3安全审计
- 4安全计算环境
 - 1身份鉴别
 - 2访问控制
 - 3入侵防范
 - 4镜像和快照保护
- 5安全管理中心
 - 4数据完整性和保密性
 - 6数据备份恢复 a云服务客户应在本地保存其业务数据的备份。
 - 7剩余信息保护
- 5安全管理中心
 - 1集中管控
- 6安全建设管理
 - 1云服务商选择
 - b应在服务水平协议中规定云服务的各项服务内容和具体技术指标
 - c应在服务水平协议中规定云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。



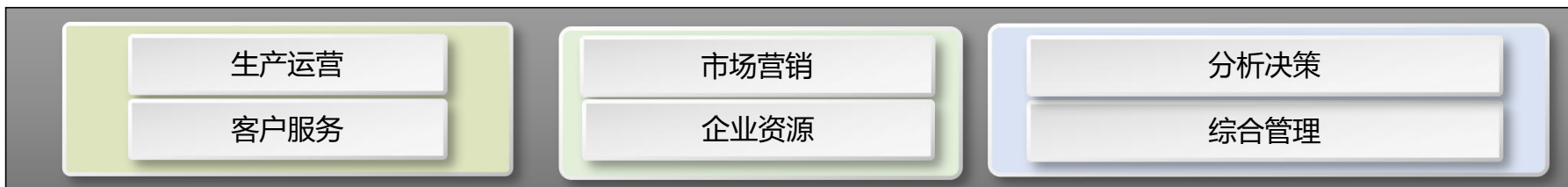
北燃云平台建设目标



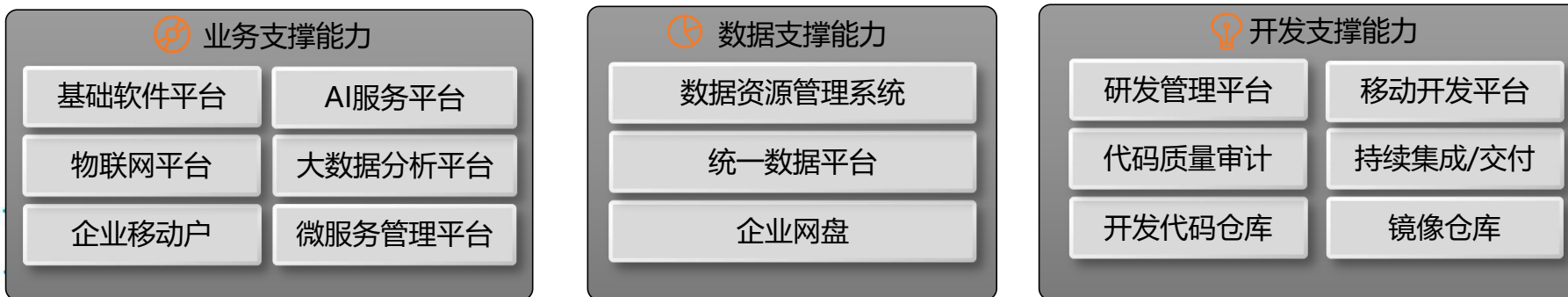
北燃云平台功能架构

- **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。

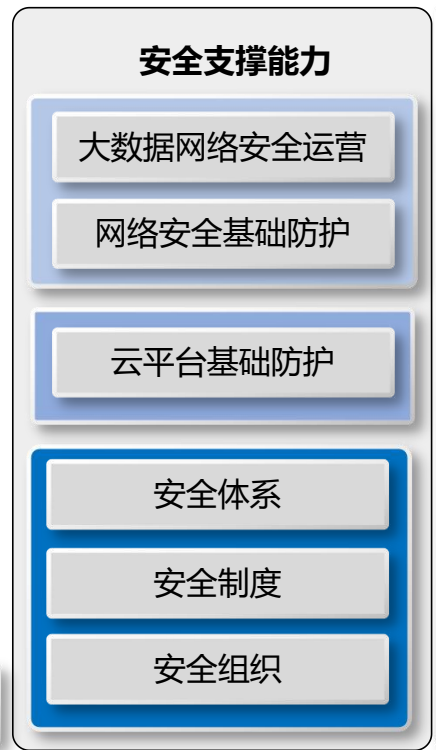
SaaS



PaaS



IaaS



云管理

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

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

集团各部室、各专业机构以及各分子公司

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。

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。

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。



安全方针 (Security Policy)				
信息安全组织 (Organization of Information Security)				
资产管理 (Asset management)				
信息安全教育和培训 (Information Security Education and Training)				
外部合作 伙伴的安全 (External Parties Security)	人力资源 安全 (Human Resources Security)	物理和环境安全 (Physical and environmental security)	通讯和 操作安全 (Communications and operations Management)	信息系统获取、 开发和维护 (Information systems acquisition, development and maintenance)
访问控制 (Access Control)				
加密控制 (Encryption Control)				
检查/监督/审计 (Review / Monitoring / Audit)				
信息安全事故管理 (Information security incident management)				
业务连续性管理 (Business continuity management)				
符合性 (Compliance)				

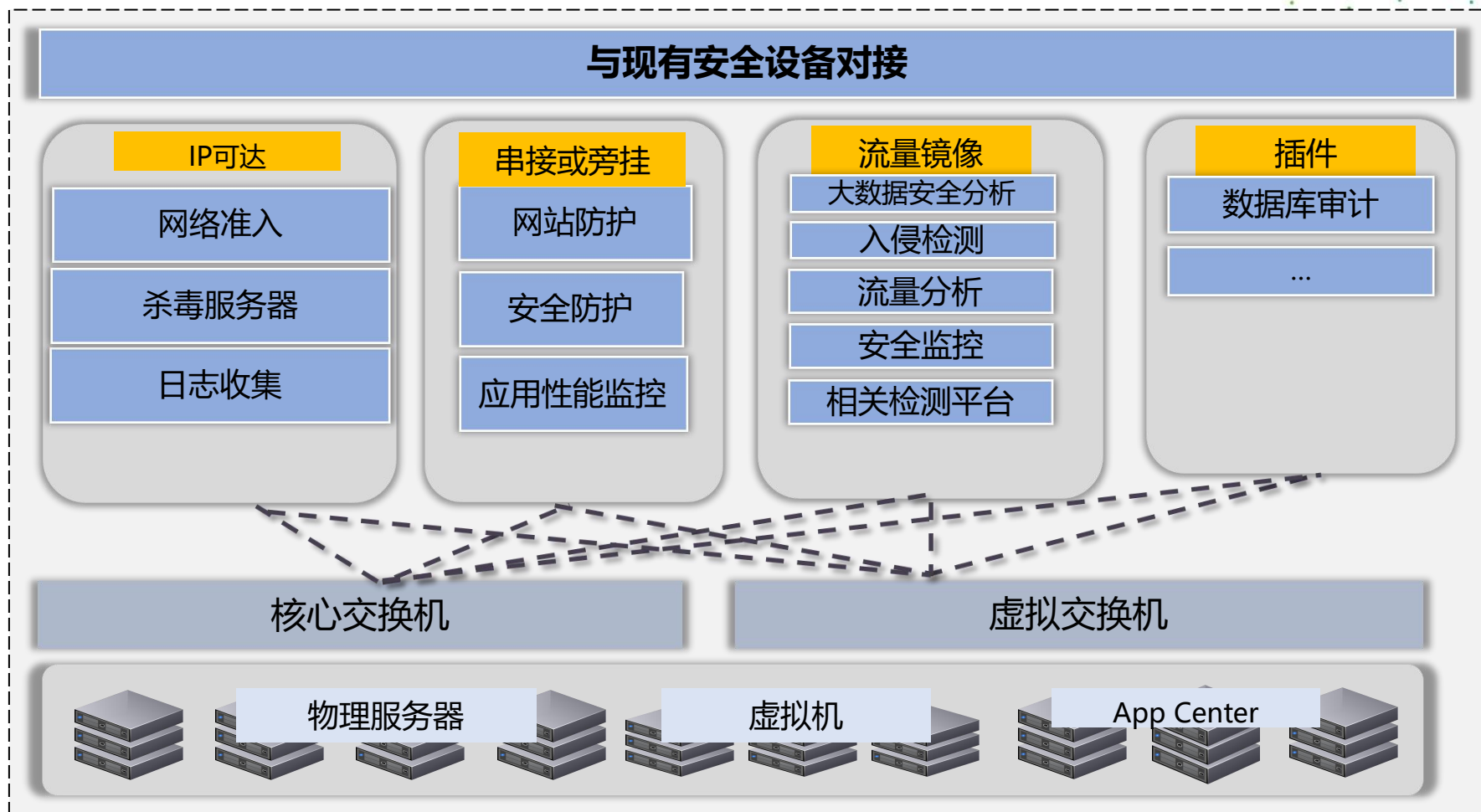
Audit Plan 评审日程表 - CA2 监督审核		Report No.: 0543981-	bsi.
		报告编号: 0543981-	
		Sheet Number 页数: 1 of 3	
No. of Mandates 评审人数: 2 (SMD) + 1.5 (M) others			
Client Name 客户名称: 北京中电信息档案有限公司 认证的单元: 7895162-6-			
Registered Address 注册地址: 中国北京海淀区中关村东路22号 100029			
Tel No. 电话号码: +86 10 62913171		Fax No. 传真号码: +86 10 62926970	
E-mail 电邮地址: shenyan@bjgas.com			
Audit Objectives 审核目的: 确认被认证组织的管理体系在认证周期的有效期内是否有效运行并满足认证标准的要求。			
Scope of Registration 注册范围: 信息档案中心为集团公司提供信息安全管理咨询服务和培训, 信息安全咨询和培训, 数据安全管理, 信息安全运营, 信息化系统建设和运维以及运营管理的业务。这包括了2015-24 年度的成本为 1.0 的长期性服务。			
Accreditation Mark(s) 认证标志: ANAB		BSI Reference 内部编号: 4758209-	
Management Standard 认证标准: ISO27001 - 2013		T-code 专业服务机构 TSCB	
Management System Manual ref. 管理手册文件: 综合管理手册			
Opening Meeting Date/Time 首次会议日期/时: 21/05/2017 09:00-09:30			
Closing Meeting Date/Time 末次会议日期/时: 22/05/2017 18:00-17:30			
Company Representative 受审核方代表: 申彦星 先生			
BSI Audit Team BSI 审核组:		持有本次审核代码 (TAPS) 的成员:	
Team Leader 组长: Ms. Lijun Jin 金文娟女士 15652190558-	(Team A 组一):	T05P27001A-	
组员: Mr. Vincent Pan 潘锐	(Team B 组二):	T05P27001A-	

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

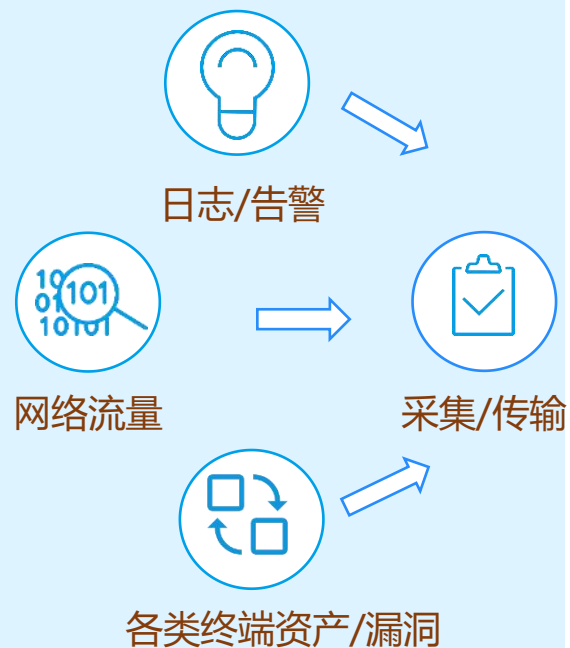


与现有安全架构进行融合

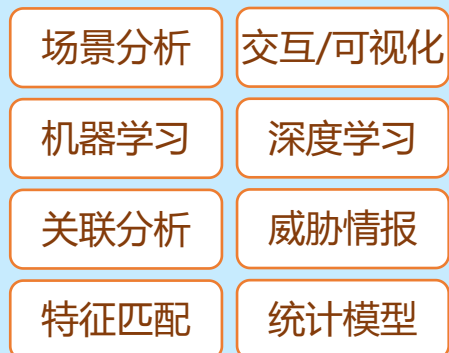


基于已知风险的安全运营

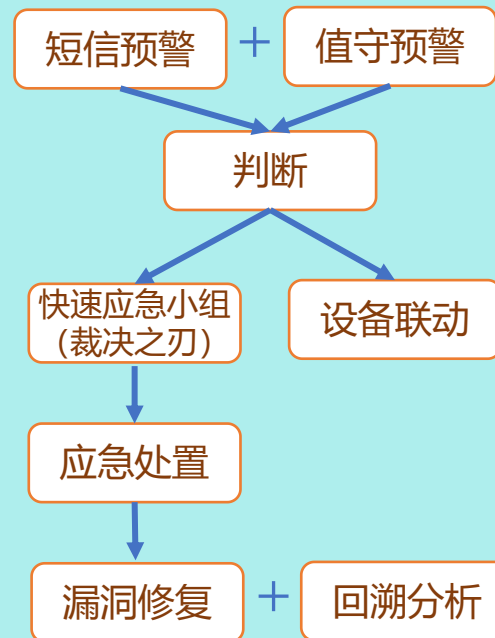
风险收集



分析预警



应急处置



加固提升



基于未知风险的安全运营

风险收集



渗透测试



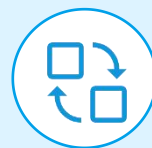
安全测评



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



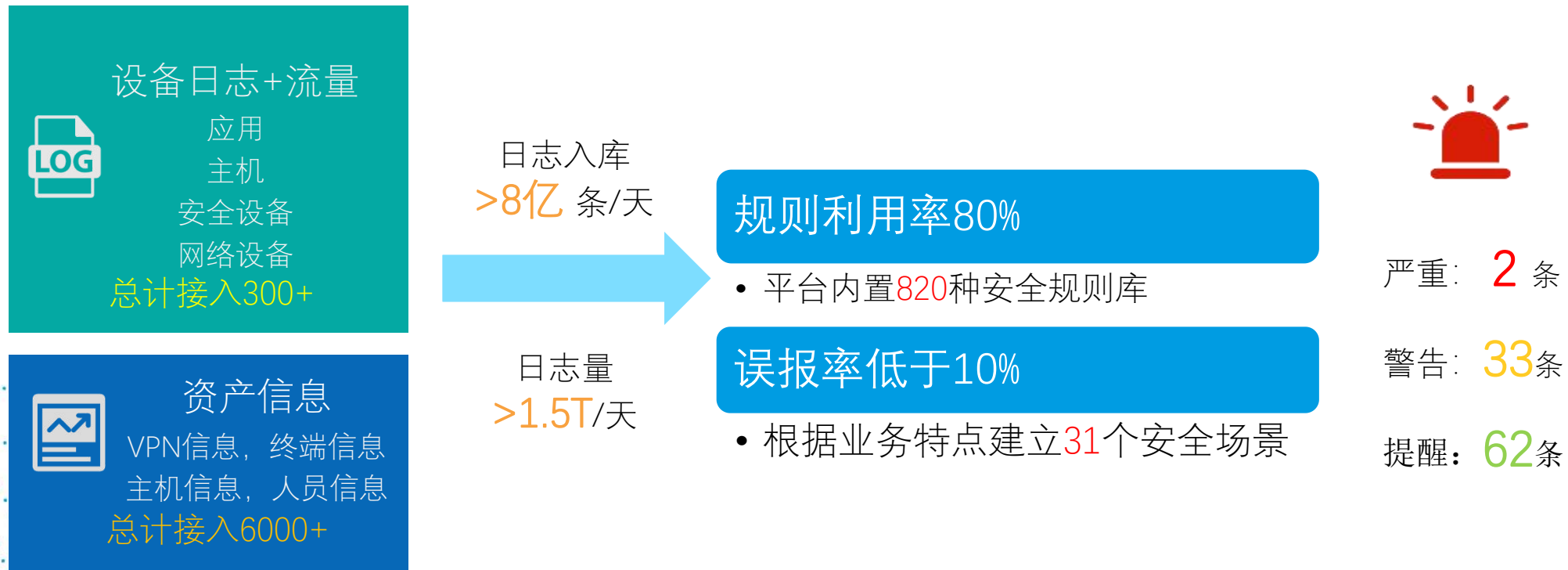
全程监控



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。



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
		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
网络安全	针对VPN主机或账号的暴力破解	
	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。

The screenshot displays a security event interface for Beijing Gas. The main alert is titled "#012236 威胁情报命中-内网主机与恶意域名通讯". It shows a warning level of "严重" (Severe) and a status of "未知" (Unknown). The alert details include the start time (2019-06-21 09:24:40) and update time (2019-06-23 18:00:38). The response time is 0, and the detection time is 8小时33分 (8 hours 33 minutes). The responsible person is listed as "管理员".

The alert content is: **警告 主机172.21.45.5向恶意域名rat2.100geili.com发起连接，疑似感染恶意程序。**

The interface also shows a timeline of events. A table lists the original alerts:

告警名称	源地址	目的地址	告警ID	操作
威胁情报命中-内网主机与恶意域名通讯		172.17.5.10	1399189465989464128	原始日志
威胁情报命中-内网主机与恶意域名通讯		172.17.5.10	1399189465992628288	← 关联
威胁情报命中-内网主机与恶意域名通讯		172.17.5.10	1399189466215600193	原始日志
威胁情报命中-内网主机与恶意域名通讯		172.17.5.10	1399189466203672643	原始日志
威胁情报命中-内网主机与恶意域名通讯		172.17.5.10	1399189466239467584	原始日志

Below the table, there is a section for related events:

源端口	域名	事件分类	源地址	目的地址	目的端口	事件名称	设备地址	操作
56149	rat2.100geili.com	网络访问/正常访问		172.17.5.10	53	DNS查询		

At the bottom, there is a table for the destination address and device address:

目的地址	设备地址
二元组	172.21.45.5 172.17.5.10

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。

威胁情报分析: rat2.100geili.com

威胁情报 域名解析 注册信息 关联域名 数字证书

开源情报

情报来源	最近看到	威胁类型
TTC	2015/03/23	木马

相关样本

样本HASH	最早看到	恶意类型	关联信息
1E7A54EFA1F26B23FC228F73E792697	2019/04/19	Storify	Parite
B85C0ACCF1E768AAE41664525F982785	2019/04/13	Storify	Yisut
094A7221D09B934CB5A317CB6870909	2019/01/19	Trojan	Symal
85E94973837E5C00E561A8CF16F7871	2019/01/17	Botnet	FakeLPC
AEBDCD5CEC55603F56E7A117A0B923FF	2019/01/08	Trojan	Zbot

关联URL 没有数据

rat2.100geili.com

标签: 远控, Zegost远控, Nitel后门程序

用户标签: 远控服务器(0), 恶意网站(0), 正常网站(0), 钓鱼网站(0)

历史IP数量: 44 | 域名上的URL: 0 | 注册时间: 2012-02-11 08:32:25 | 域名服务商: GoDaddy.com, LLC

与该域名关联样本: 18 | 子域名数量: 10 | 过期时间: 2022-02-11 08:32:25 | 域名注册商: Select Contact Domain Holder link at http://www.godaddy.com/whois/results.aspx?domain=100geili.com

API查询 | 加入监控 | 本地API | 流量监测

情报聚合: 55 | 域名解析: 57 | 子域名: 10 | WHOIS: 45 | 可视化 | 数字签名: 0 | 用户标签: 0

威胁情报

情报来源	时间	情报内容	状态
ThreatBook Labs	2016-09-28 20:30:10	远控	有效

域名服务商: GoDaddy.com, LLC

域名服务器: ns03.domaincontrol.com;ns04.domaincontrol.com;

主域名: 100geili.com

更新时间: 2018-04-25

Tags: 远控木马, Nitel, cve-2017-8759

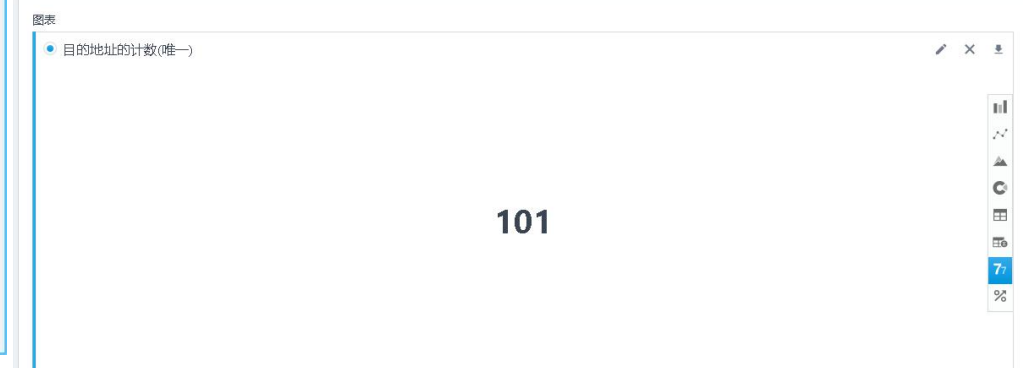
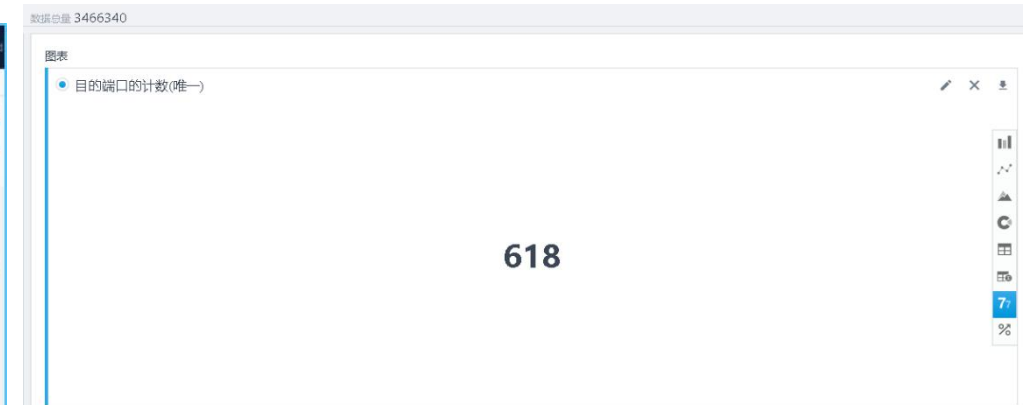
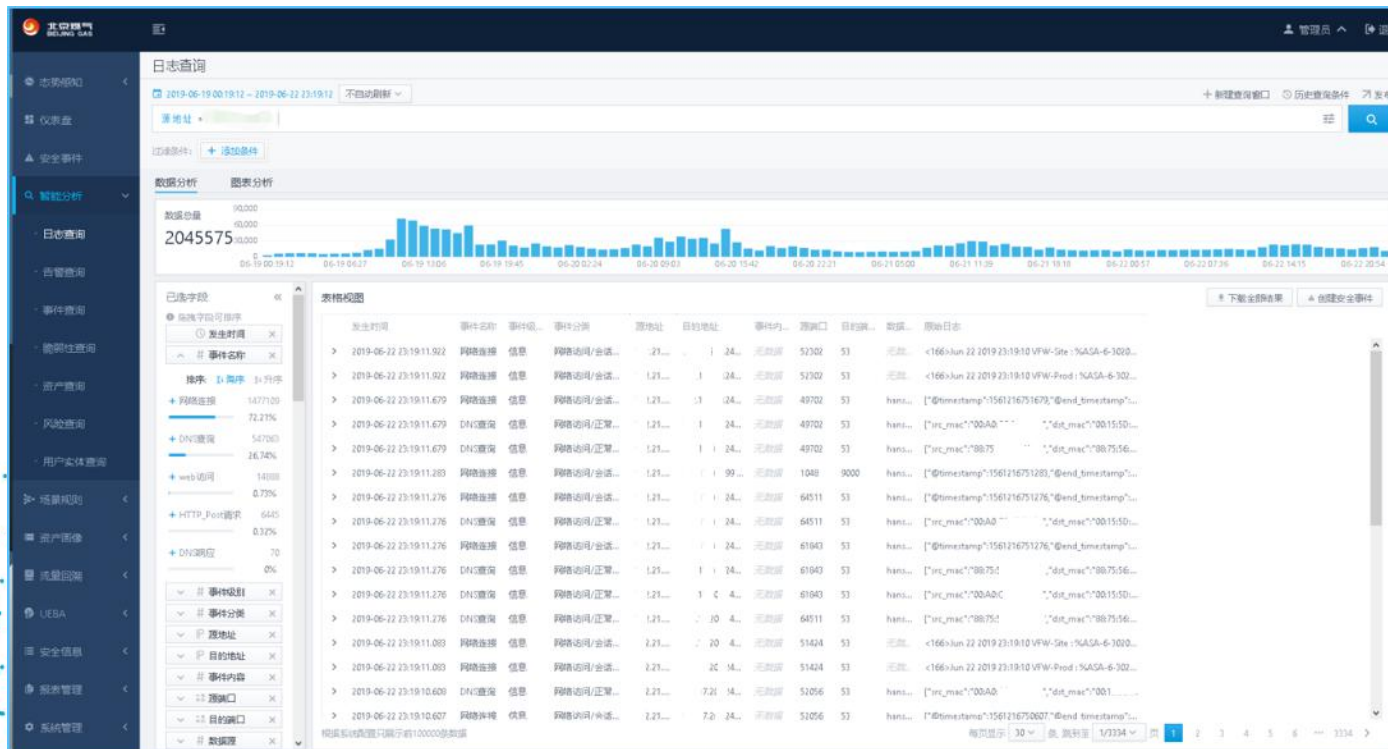
威胁情报

IOC信息

分类	家族	组织
开源情报(723) 更新时间: 2018-11-15	恶意软件	
云沙箱(532) 更新时间: 2018-11-09	恶意软件	Nitel
云沙箱(532) 更新时间: 2018-04-25	漏洞利用	cve-2017-8759
开源情报(493) 更新时间: 2018-03-27	可疑	
金睛团队(510) 更新时间: 2017-12-16	远控木马	Nitel
开源情报(27)	恶意网站	

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。

TRUCS 2019

TRUSTED CLOUD SUMMIT

可信云大会

中国·北京 2019.7.2-3

THANKS

