管家式安全服务

- 安全挑战
- 服务类型
- 服务项目
- 场景分享
- 服务支撑

LAN Yun Networks

A Solution and Service Company

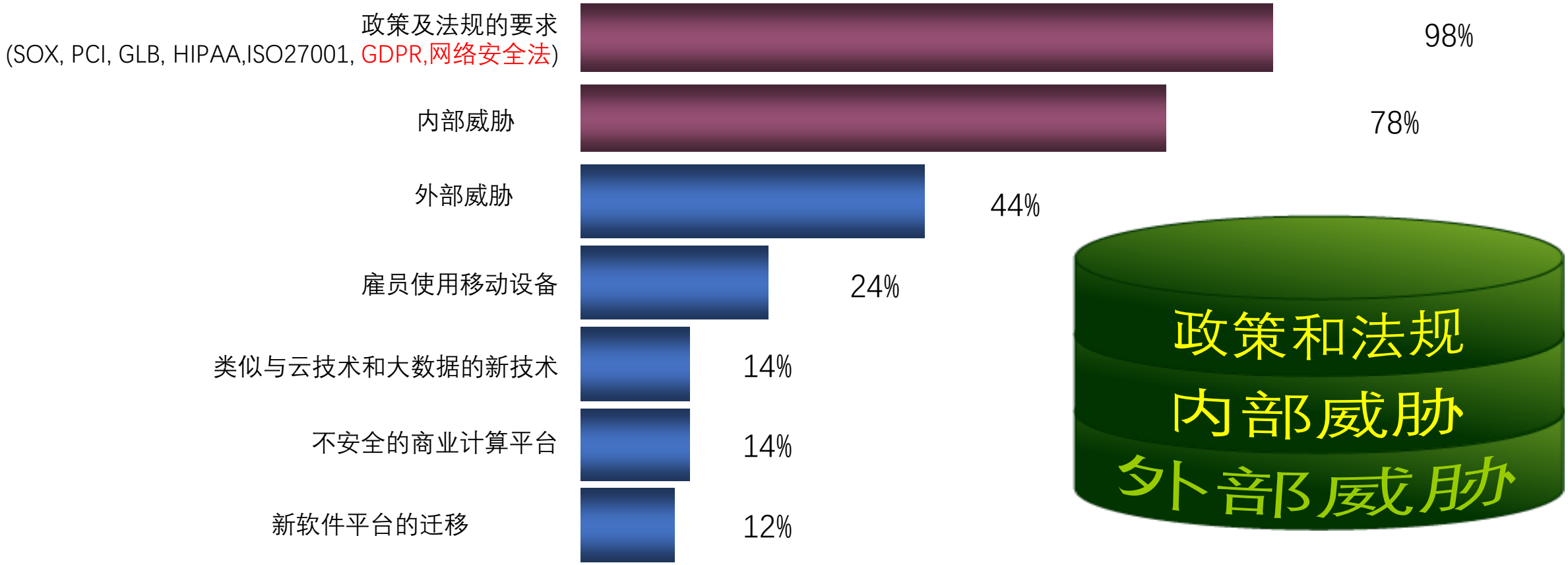
蓝云网络

一家专业服务与解决方案公司

安全挑战

企业如何应付新的挑战 – 新法规和内部威胁

对于 Fortune1000 CIOs/CSOs 的问卷调查:
什么是目前在IT安全支出上最大的驱动力?



Source: Goldman Sachs Security Spending Survey, 2/13/15

“管家式”安全外包服务需求

- 大多数客户没有足够的资源独立完成企业的可用性和安全管理，同时对网络和安全管理专业技术人才和设备的投入大大增加了企业的运营成本。
- 随着互联网环境和客户信息化环境的日益庞大和复杂，IT部门面对层出不穷的安全问题束手无策，不能保证免受内部和外部的威胁并避免可能导致的重大损失。
- 对法律、法规的遵从要求企业安全治理实现高度的制度化、专业化，对于绝大部分企业用户来说，很难从技术手段和专业团队自行搭建完整的合规体系。
- 急需7*24全天候的主动、实时、可托管的管家式安全外包管理服务的支持。

为什么需要“管家式”安全外包服务?

企业面临的困境:

- 安全专家团队
  - 聘请并留住真正的安全专家非常困难
- 平衡开支及服务级别
  - 雇用大量专业员工来实现高级别的维护是非常昂贵的，特别是高要求的7*24的监控和及时故障响应
- 各种安全解决方案投入成本高
  - 采用业界最先进安全方案成本高
  - 采用物廉价美解决方案解决不了真正问题
- 集中优势，节省开支
  - 企业将IT安全服务外包，能够集中有限的资源投入到核心业务中

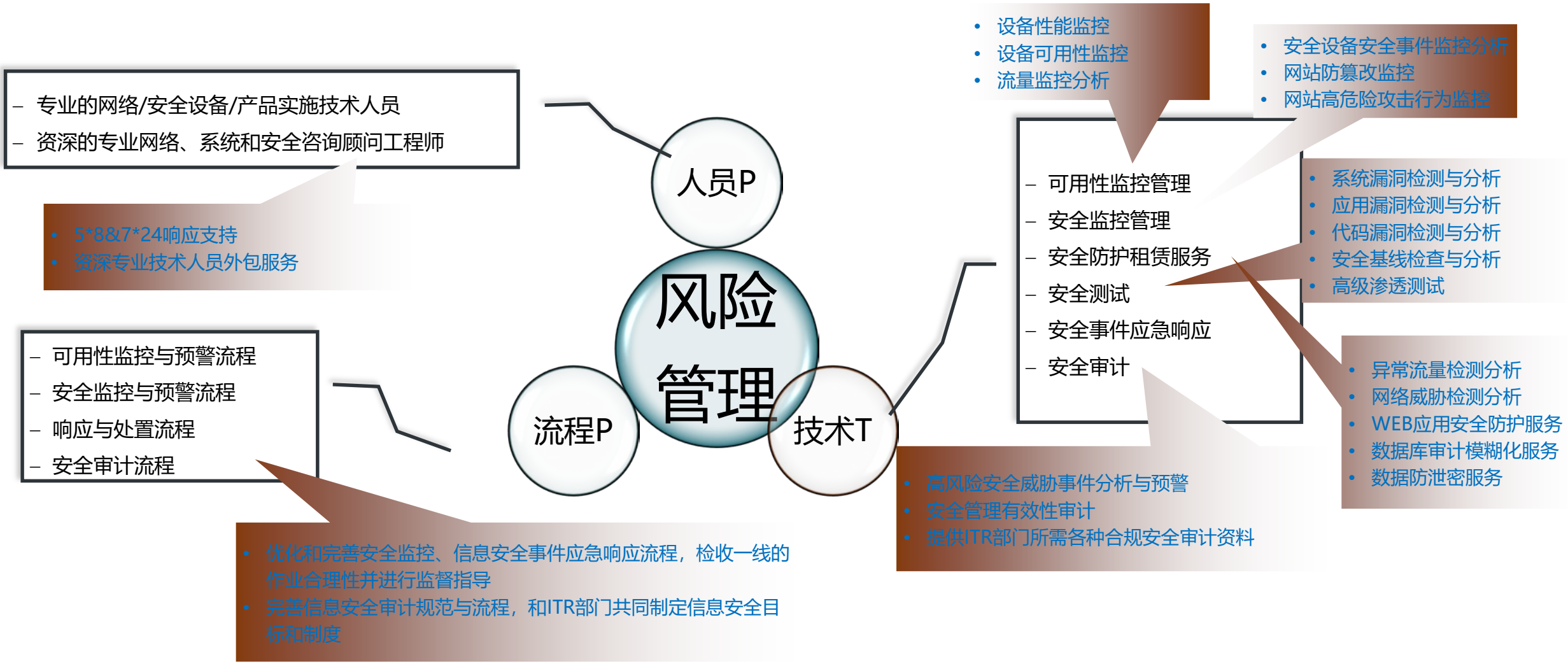
服务类型

专业综合信息安全管理服务

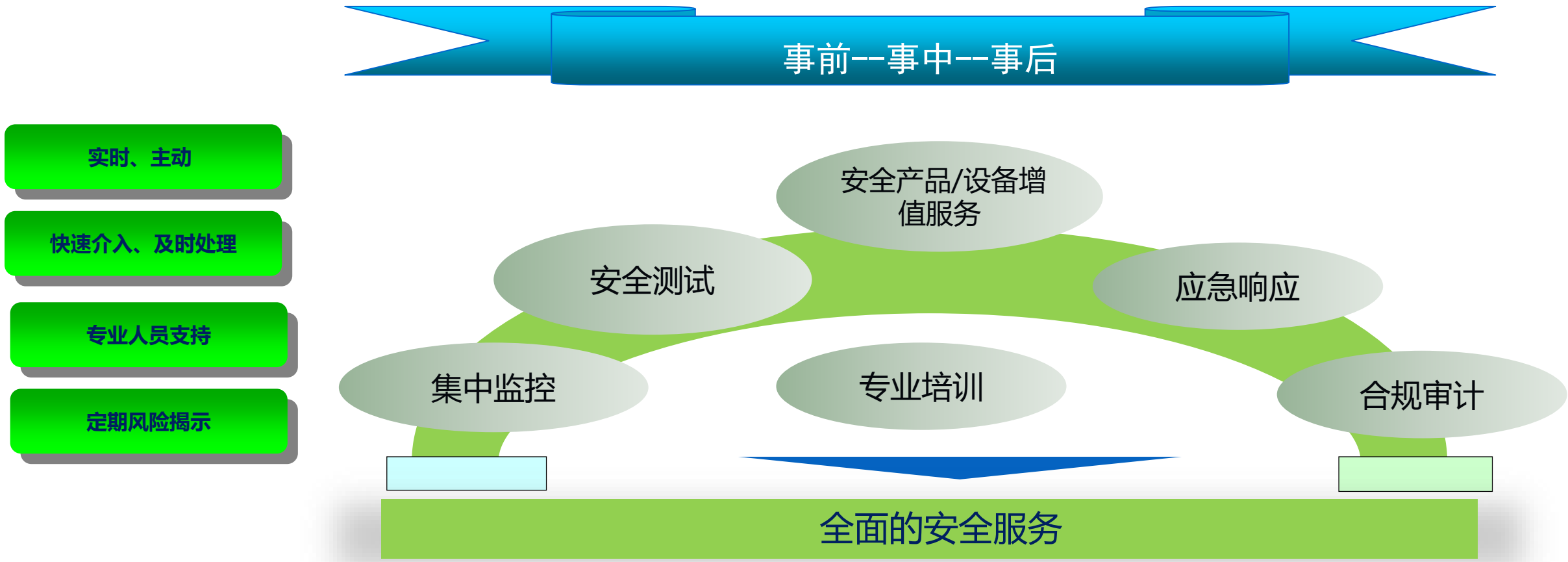
- 专业提供远程网络和安全监控管理、安全业务的运维管理咨询、远程/现场安全风险评估和弱点分析、远程/现场渗透攻击和代码审计、现场紧急事件响应、安全培训和安全合规等外包服务
- 服务内容包括监控管理、网络设备租赁和安全防御分析解决方案租赁服务等
- 帮您有效降低雇用专业网络和安全管理人员的运维成本

“管家式”安全外包服务

提供专业人员和技术服务，帮助客户建立以IT风险管理为核心，建议可持续改进的信息安全管理和技术体系



“一站式”无忧的安全服务


事前--事中--事后
实时、主动
快速介入、及时处理
专业人员支持
定期风险揭示
安全产品/设备增值服务
安全测试
应急响应
集中监控
专业培训
合规审计
全面的安全服务

服务模式

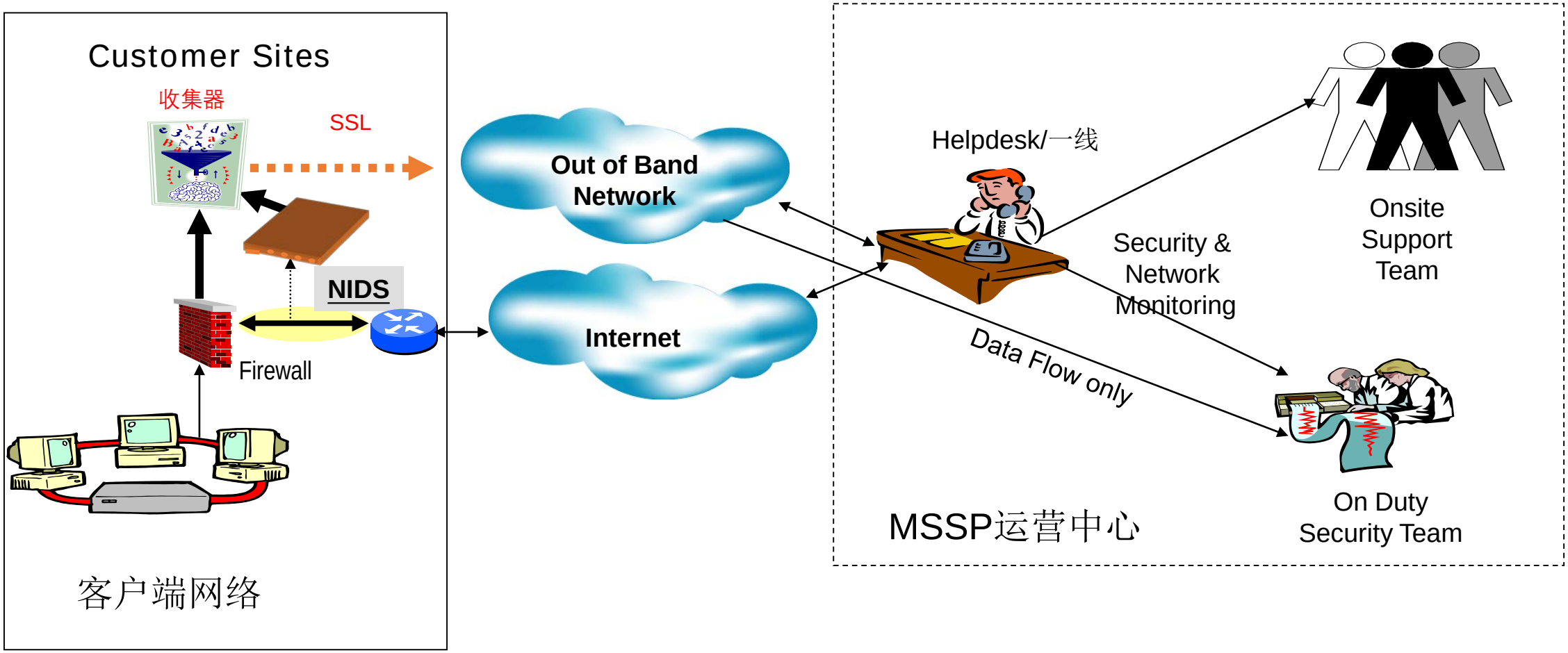
第一种模式：SaaS模式的标准服务

- 建立基于数据中心或云端的VNOC/SOC运营中心，提供专业人员进行设备接入协助以及相关咨询服务，支持用户端自助式登录Web Portal以查看设备状态。由监控人员（一线）或平台通过专业技术手段自动处理网络故障、安全事件日志信息，提供自动告警服务、自动定期报表/报告服务。

第二种模式：“管家式”金牌服务

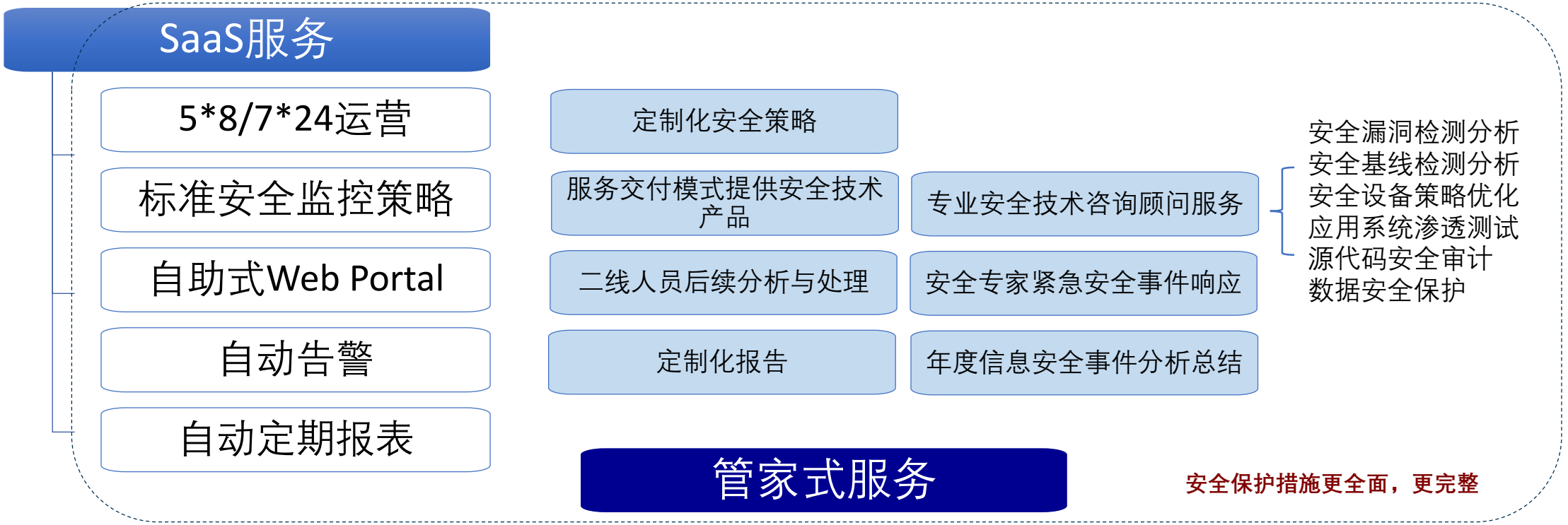
- 在通过VNOC/SOC平台提供7*24的信息安全事件监控与告警服务基础上，由监控人员（一线），安全事件分析与处理人员（二线），专家/资深安全顾问（三线）组成由专业的服务支撑团队，提供安全外包服务，主要包括安全设备运维管理、应急响应，以及安全漏洞检测分析、安全基线检测分析、安全解决方案咨询顾问等增值服务。

客户接入示意



*说明：无代理模式，客户端部署1台收集器设备通过SSL Internet加密单向方式传到数据中心/云端 MSSP服务器

Saas 标准模式与“管家式”金牌服务的区别



服务项目

我们提供的监控管理服务

一、监控告警
- 设备可用性和性能监控
- 安全事件监控告警
- 安全通告
- 跨设备的关联安全事件告警（金牌）

二、安全事件响应
- 安全事件一线处理
- 安全事件升级，二线三线协同处理（金牌）
- 专家级技术支持（金牌）

三、分析总结及报表
- 安全事件标准报表（周报/月报）
- 合规性报表-ISO27001/PCI DSS/SOX/等保（金牌）
- 安全事件处理的安全专家报告（金牌）
- 年度安全审计及风险评估报告（金牌）

四、可选的安全服务
- 漏洞扫描分析及加固
- 安全基线分析及加固
- 渗透测试
- 代码审计
- 安全紧急事件响应与处理

Feature	Standard（5*8）	Standard（7*24）	Golden（7*24）
监控告警			
设备可用性和性能监控	●	●	●
安全事件监控告警	●	●	●
安全通告	●	●	●
跨设备的关联安全事件告警			●
安全事件响应			
安全事件一线处理	●	●	●
安全事件升级（二线三线协同处理）			●
专家级技术支持			●
分析总结及报表			
安全事件标准报表	●	●	●
合规性报表-ISO27001、PCI DSS、SOX、等保			●
安全事件处理的安全专家报告			●
年度安全审计及风险评估报告			●
可选的安全服务			
漏洞扫描分析及加固			●
安全基线分析及加固			●
关键资产调研和安全策略优化设计			●
渗透测试	●	●	●
代码审计	●	●	●
安全紧急事件响应与处理	●	●	●

定制化安全解决方案租赁服务

Feature	Standard（5*8）	Standard（7*24）	Golden（7*24）
异常流量分析和威胁检测			
设备租赁与安全运维服务	●	●	●
重要应用调研（部署前）/监控策略设计	●	●	●
安全策略定期优化/知识转移与培训	可选	可选	●
WEB应用安全防护（WAF）			
设备租赁与安全运维服务	●	●	●
部署前-漏洞检测分析服务	●	●	●
部署前-人工渗透测试服务	可选	可选	可选
设备安全策略定制化部署	●	●	●
知识转移与培训、WAF设备策略定期优化	可选	可选	●
定期漏洞检测分析和人工渗透测试	可选	可选	可选
数据库安全审计及防护			
设备租赁与安全运维服务	●	●	●
重要应用调研（部署前）/监控策略设计	●	●	●
安全策略定期优化/知识转移与培训	可选	可选	●
敏感数据防泄密（DLP）			
设备租赁与安全运维服务	●	●	●
部署前-评估分析服务&方案整体设计服务	●	●	●
安装部署实施服务	●	●	●
知识转移培训服务、安全运维分析服务、策略定期优化	可选	可选	●
数据模糊化（SDS）			
设备租赁与安全运维服务	●	●	●
部署前-评估分析服务&方案整体设计服务	●	●	●
安装部署实施服务	●	●	●
知识转移培训服务、安全运维分析服务、策略定期优化	可选	可选	●
安全漏洞检测分析平台（黑盒/白盒）			
设备租赁标准服务	●	NA	NA
评估、设计、安装部署和策略调优服务	可选	NA	NA

场景– 可用性管理

一、实时告警

- 内存利用率
- CPU利用率
- 硬盘利用率
- 缓存问题
- 链路拥塞
- 链路故障
- 网络拥塞
- 网络过载
- 广播风暴
- 网络配置的最新信息
- QoS 审计

二、定期报表 or Dashboard

- 每月和实时的报告，包括高峰和平均使用率数据、带宽利用率、带宽使用最多的用户、网络事件和活动等

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固

场景–防火墙监控管理

一、实时报警

- 可用性和性能管理
- 非法扫描（port scan ）：需要把防火墙流量信息deny、all、permit发送至SOC（对SOC系统负担比较大）
- 非法扫描（sweep scan）：多个源头对同一目标端口进行扫描
- 数据异常外部传输：关键服务器向互联网主动发起连接（22/80/8080/443/3389/8000）
- 非授权访问-非正常时间的访问
- 非授权访问-非正常IP的访问
- 对防火墙的暴力破解

二、定期报表 or Dashboard

- TOP 10 Source IP/Destination IP/port/Application

三、等保/ISO27001合规性要求

- 登录事件
- 配置/策略变更

四、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固、关键资产调研、数据流和业务流分析、安全防护策略的定制优化

场景– IDS/IPS监控管理

一、实时报警

- 可用性和性能管理
- OWASP TOP 10（业务逻辑与敏感信息除外）
- Shellcode
- 缓冲区溢出
- DOS/DDoS攻击
- 非法扫描
- 设备产生的、非以上的高危事件（注：定义对象范围）

二、报表 or Dashboard

- TOP 10 Source IP/Destination IP与每个IP的攻击事件名称
- 攻击趋势

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固、关键资产调研分析、安全防护策略的定制优化

场景– 防DDoS设备监控管理

一、实时报警

- 设备可用性和性能管理
- 是否有DoS/DDoS攻击事件产生
- DoS/DDoS自身设备被攻击

二、报表 or Dashboard

- 攻击目标IP TOP 10与每个IP的攻击类型名称
- 攻击趋势

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固、安全防护策略的定制优化

场景- 杀毒网关设备监控管理

一、实时报警

- 设备可用性和性能管理
- 病毒爆发
- 蠕虫监控

二、合规性审计报表

- 病毒库更新失败：过长时间未更新（暂定：超过1周）
- 扫描策略执行失败

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固、安全防护策略的定制优化

场景– Web应用安全监控管理

一、实时报警

- 设备可用性和性能管理
- 注入攻击
- 跨站脚本攻击XSS
- CSRF攻击
- 不安全的直接对象引用
- 安全配置错误
- 敏感信息泄露
- 功能级访问控制缺失
- 使用含有已知漏洞的组件
- 未验证的重定向和转发
- 失效的身份认证和会话管理
- 敏感URL监控

二、合规性报表 or Dashboard

- TOP 10 Source IP/Destination IP
- 每个URL的攻击事件名称

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固、关键资产调研分析、数据流和业务流分析、安全防护策略的定制优化

场景-VPN监控

一、实时监控

- 设备可用性和性能管理
- 对VPN设备的攻击（例：暴力破解）
- 非正常工作时间访问
- VPN特权账户的访问

二、报表

- 登录事件：对VPN设备的攻击（例：暴力破解）

三、等保/ISO27001的合规性要求

- 登录事件:时间、时长、账户
- 配置/策略变更

四、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固

场景-系统威胁监控管理

* 前提：需要采集server（windows，Linux）日志

一、实时监控

- 设备可用性和性能管理
- 普通帐号权限提升
- 频繁的切换root权限
- 暴力破解尝试（点对点模式）
- 内部异常行为--新建账号
- 短时间内的帐号添加和删除操作
- 非授权时间系统异常登录
- 非授权IP系统异常登录

二、合规性审计报表 or Dashboard

- 新建账号（不实时报警，仅提供报表，客户自行审计）
- 非授权时间系统异常登录（不实时报警，仅提供报表，客户自行审计）
- 非授权IP系统异常登录（不实时报警，仅提供报表，客户自行审计）

三、增值特色服务（金牌）

- 设备漏洞分析及加固，安全基线分析及加固

增值服务-互联网安全威胁分析

一、实时报警

- 非法扫描&登录成功
- 暴力破解&登录成功
- IPS/IDS入侵痕迹检测&登录成功
- 外网非法扫描&帐号异常
- 暴力破解&账号异常
- IPS/IDS入侵痕迹检测&帐号异常
- 外网非法扫描&提升权限
- 暴力破解&提升权限
- 入侵痕迹检测&提升权限
- 其他关联分析事件（OWASP漏洞检测、Hacker Tool Website Access）

二、报表

- 攻击可视化报表（流量分析、端口扫描）
- TOP10 Users with VPN Successful Logins

增值服务-安全合规性审计

- ISO27001报表（周报/月报）
- PCI DSS报表 （周报/月报）
- 等保报表（周报/月报）
- SOX报表（周报/月报）

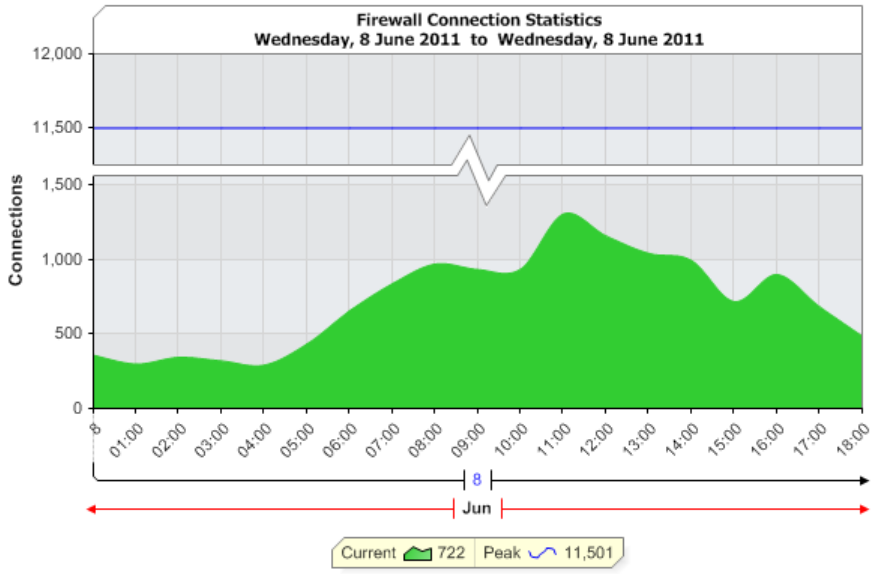
- 服务的两种模式：
    1. 统一收集日志上传到数据中心的MSSP平台
    2. 在客户本地部署日志分析管理平台，产生相应的合规报表

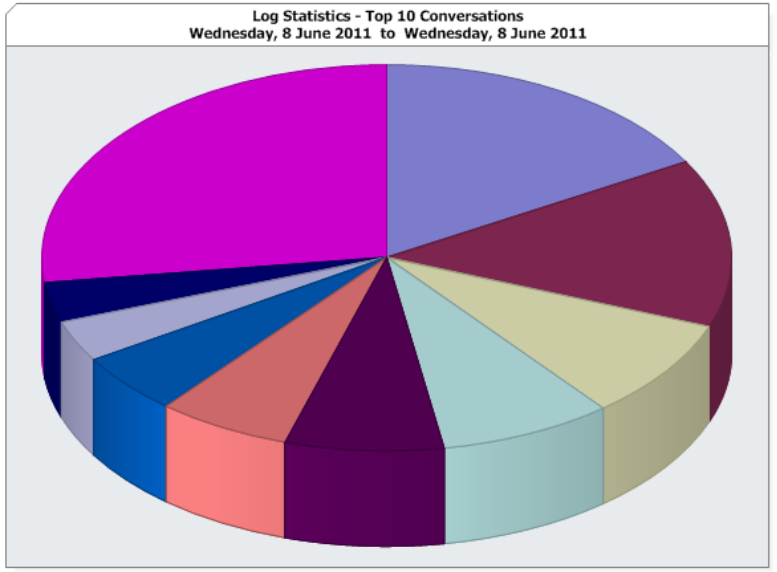
场景分享

安全设备可用性

安全设备状态监控

1. **流程触发**（一线监控or报告）
   - 监控界面实时显示安全设备状态。**示例**：防火墙CPU使用率过高，开事件处理工单
2. **事件处理**（二线）
   - 查看事件详细信息，查看检测到防火墙目前运行状况，连线数目过多。并查看大量连线内容并判断属于异常行为。
   - 通知设备运维人员处理：防火墙策略调整，设定来源连线数目限制以减少连线数量进行防护。
3. **结果反馈**
   - 一线确认事件处理完成，工单结束
   - 安全经理/安全审计员确认违规事件处理完成





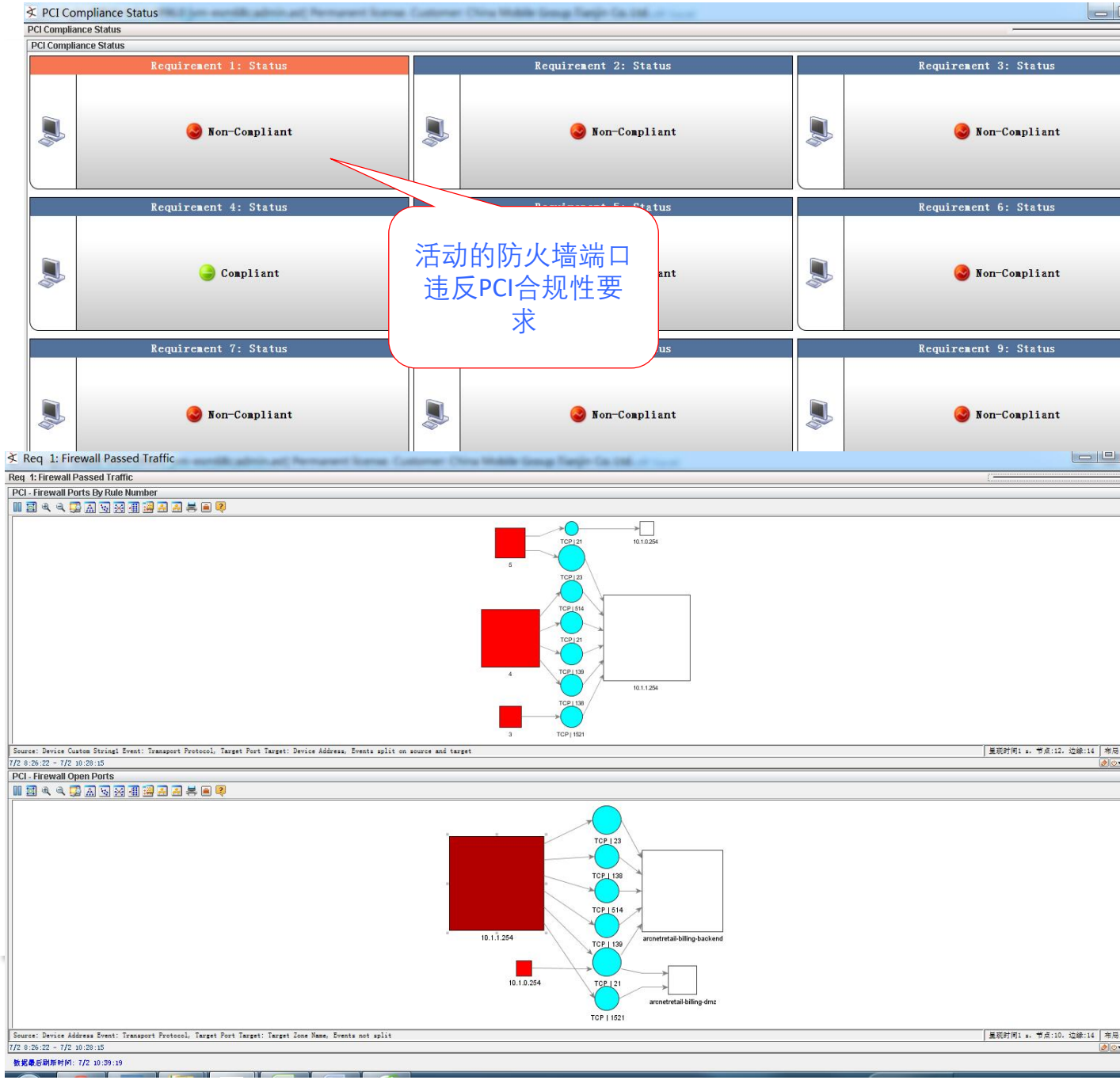
合规性审计

PCI DSS

1. **流程触发**（一线监控or报告）
   - 定期自动生成符合性审计报告，发送给安全经理/安全审计员。**示例1**：信用卡号码明文显示
   - 监控界面实时显示违规/疑似事件。**示例2**：防火墙开放端口不合规，开事件处理工单

2. **事件处理**（二线）
   - 查看事件详细信息，查看检测到防火墙开发了哪些违规端口
   - 通知运维人员处理：防火墙策略，关闭违规开放的端口服务

3. **结果反馈**
   - 一线确认事件处理完成，工单结束
   - 安全经理/安全审计员确认违规事件处理完成



安全管理

网络安全事件实时告警

1 **流程触发**（一线监控）

示例1：DoS攻击事件告警

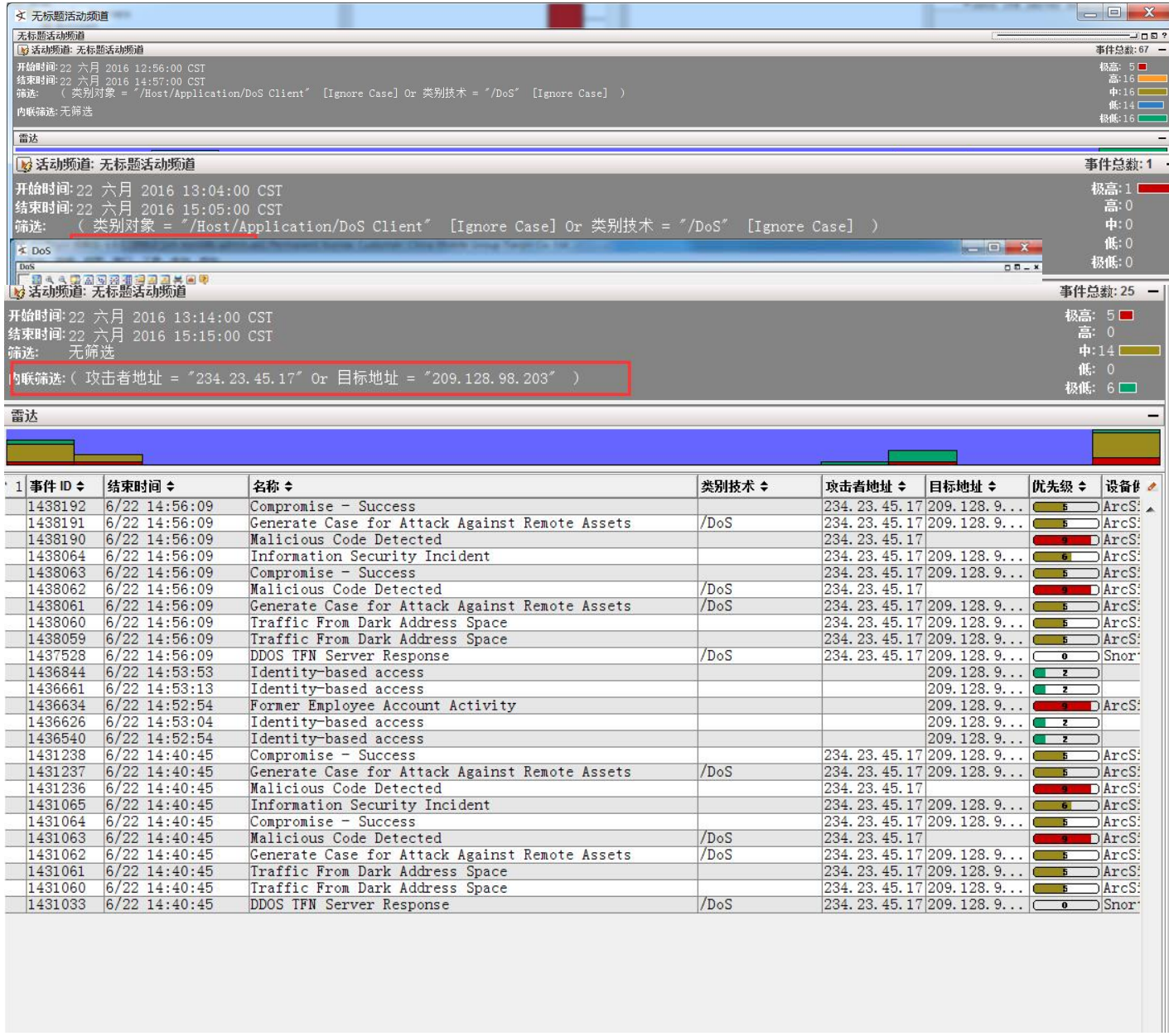
- 监控平台的“活动频道”发现高风险安全事件，自动告警
- 查看事件详细信息，记录事件ID，事件类型，源/目标地址，开工单通知二线处理

2 **事件处理**（二线）

- 检索对应事件ID，分析攻击者行为，评估可能造成的影响
- 以攻击源/目标IP为参考，进一步检索其它相关联事件，分析是否对网络内其它主机造成影响
- 通知运维人员处理：更新网络边界安全设备防护策略和访问控制策略，阻断攻击源

3 **结果反馈**

- 一线确认事件处理完成，工单结束



事件 ID	结束时间	名称	类别技术	攻击者地址	目标地址	优先级	设备
1438192	6/22 14:56:09	Compromise - Success		234.23.45.17	209.128.9...	5	ArcS
1438191	6/22 14:56:09	Generate Case for Attack Against Remote Assets	/DoS	234.23.45.17	209.128.9...	5	ArcS
1438190	6/22 14:56:09	Malicious Code Detected		234.23.45.17		9	ArcS
1438064	6/22 14:56:09	Information Security Incident		234.23.45.17	209.128.9...	6	ArcS
1438063	6/22 14:56:09	Compromise - Success		234.23.45.17	209.128.9...	5	ArcS
1438062	6/22 14:56:09	Malicious Code Detected	/DoS	234.23.45.17		9	ArcS
1438061	6/22 14:56:09	Generate Case for Attack Against Remote Assets	/DoS	234.23.45.17	209.128.9...	5	ArcS
1438060	6/22 14:56:09	Traffic From Dark Address Space		234.23.45.17	209.128.9...	5	ArcS
1438059	6/22 14:56:09	Traffic From Dark Address Space		234.23.45.17	209.128.9...	5	ArcS
1437528	6/22 14:56:09	DDOS TFN Server Response	/DoS	234.23.45.17	209.128.9...	0	Snor
1436844	6/22 14:53:53	Identity-based access			209.128.9...	2	
1436661	6/22 14:53:13	Identity-based access			209.128.9...	2	
1436634	6/22 14:52:54	Former Employee Account Activity			209.128.9...	4	ArcS
1436626	6/22 14:53:04	Identity-based access			209.128.9...	2	
1436540	6/22 14:52:54	Identity-based access			209.128.9...	2	
1431238	6/22 14:40:45	Compromise - Success		234.23.45.17	209.128.9...	5	ArcS
1431237	6/22 14:40:45	Generate Case for Attack Against Remote Assets	/DoS	234.23.45.17	209.128.9...	5	ArcS
1431236	6/22 14:40:45	Malicious Code Detected		234.23.45.17		9	ArcS
1431065	6/22 14:40:45	Information Security Incident		234.23.45.17	209.128.9...	6	ArcS
1431064	6/22 14:40:45	Compromise - Success		234.23.45.17	209.128.9...	5	ArcS
1431063	6/22 14:40:45	Malicious Code Detected	/DoS	234.23.45.17		9	ArcS
1431062	6/22 14:40:45	Generate Case for Attack Against Remote Assets	/DoS	234.23.45.17	209.128.9...	5	ArcS
1431061	6/22 14:40:45	Traffic From Dark Address Space		234.23.45.17	209.128.9...	5	ArcS
1431060	6/22 14:40:45	Traffic From Dark Address Space		234.23.45.17	209.128.9...	5	ArcS
1431033	6/22 14:40:45	DDOS TFN Server Response	/DoS	234.23.45.17	209.128.9...	0	Snor

安全管理

应急响应：网络安全

1 **流程触发**（用户报告）

示例1：网络异常访问活动

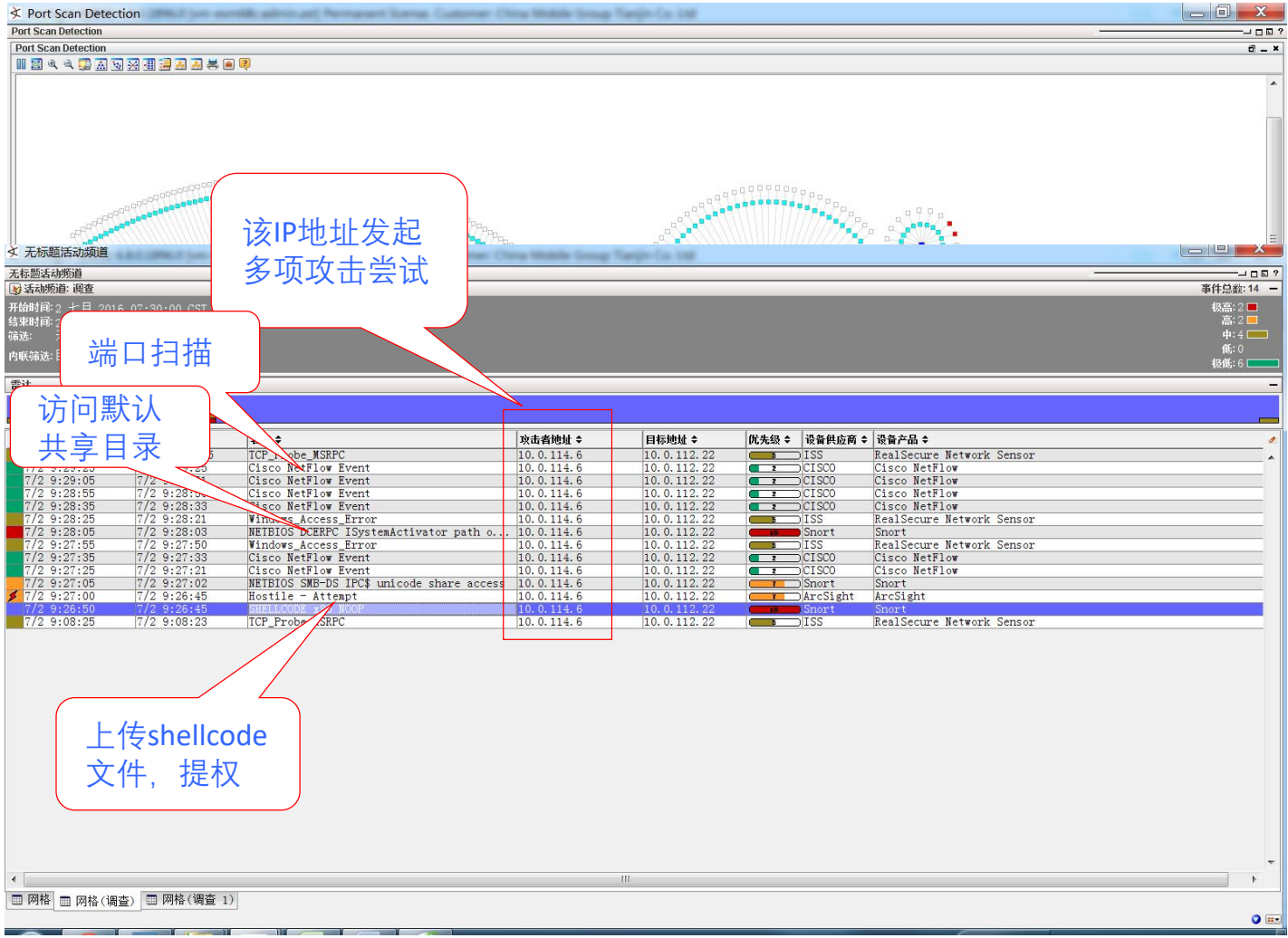
- 员工向helpdesk人员反映，办公网络速度慢，影响正常办公
- Helpdesk通知一线人员查看网络事件日志信息
- 一线人员在平台中检索到一个内网IP地址有大量向互联网访问活动，开工单通知二线处理

2 **事件处理**（二线）

- 查看该内网IP网络访问记录，判断该有另一台内网主机对该主机进行入侵攻击，提权，成功后利用此主机执行大量端口扫描
- 通知运维人员处理：检查主机入侵痕迹，清除后门、木马等程序，检查安全配置，更新补丁等

3 **结果反馈**

- 一线确认事件处理完成，工单结束



服务流程说明

- 流程触发
  - 透过部署在用户端的设备连接器，将不同安全设备的日志集中进行专来化处理，并将处理后的结果送至GNC监控平台。
  - 监控平台会进行信息内容与监控策略的匹配，发出告警给一线人员。
- 事件处理
  - 一线人员进行告警内容检视，如果告警属于一般性通知事件，依据流程开启工单并通知客户的安全人员。
  - 一线人员进行告警内容检视，如果告警事件安全等级较高，依据流程开启工单并提升事件到二线进行威胁验证。
  - 二线人员进行告警内容检视，进行安全事件的威胁验证。如果是属于误报事件的话，依据流程更新工单。并由一线人员通知客户的安全人员并就此结束并关闭工单。
  - 二线人员进行告警内容检视，进行安全事件的威胁验证。如果是属于真实威胁事件，进一步进行事件后续检测与追踪。二线人员处理完成后依据流程更新工单并且准备安全事件处理报告交给过一线人员。并由一线人员通知客户的安全人员并交付报告后关闭工单。
  - 二线人员进行告警内容检视，进行安全事件的威胁验证。如果是属于真实威胁事件，进一步进行事件后续检测与追踪。二线人员处理后发现无法解决，依据流程更新工单并通知三线的专家进行应急处理。同时间通知客户IT安全负责人。
  - 三线人员透过远程或是现场支持进行事件处理完成后，通知客户IT安全负责人员问题已解决。依据流程更新工单并且准备应急响应事件处理报告交给过一线人员。并由一线人员通知客户的安全人员并交付报告后关闭工单。
- 结果反馈
  - 所有工单关闭后，一线人员依工单内容通知客户安全人员处理内容。如有提升至二三线人员的事件，同时提交安全事件处理报告或应急响应处理报告。
  - 定期提交周报与月报给客户安全人员。

服务支撑

服务组成

NOC&SOC主要由3部分组成:

1. 人员
2. 技术
3. 流程

NOC&SOC *基础架构: IDC数据中心*

- GNC监控中心
- 基础设施管理
- 网络运行管理
- 网络安全架构
- 攻击及漏洞管理
- 安全事件分析管理

人员 :

- 专业认证的安全分析师和操作员
- 专业认证的安全顾问和工程师
- NOC&SOC经理
- 专业培训及知识更新

技术 : 网络和信息安全管理

- 集中的实时安全事件关联分析
- 真实威胁模型分析
- 高可用性
- 基于策略的安全事件汇总
- 图形化告警及报表

流程 : 24x7 运行

- 设立应急相应中心团队
- 实时事件通知、响应及处理
- 事件升级流程
- 呼叫中心及CASE系统
- ISO9001等专业化认证

服务系统的特色

- 提供了一体的解决方案，包括监控平台，监控流程和SLA的管理，专业的网络，服务器，系统和安全的服务团队；
- 有三部分组成**下一代监控平台，基于ITIL的管理流程，专业的管理团队；**
- 为客户提供了一站式的服务，无需担心实施的复杂度，系统的维护和升级，管理设备的增加和减少，故障的处理和日常等；
- 作为IT管理的天然的延伸，每月，每周，甚至每天和客户的交流沟通预防并解决客户的问题。解决了IT部门人力资源，技术能力的缺乏导致的IT基础架构高可用性直接的矛盾；
- 系统的高可视性可以让整个服务完整的，实时的呈现在客户的面前，不在是黑盒子服务；

下一代的监控管理平台

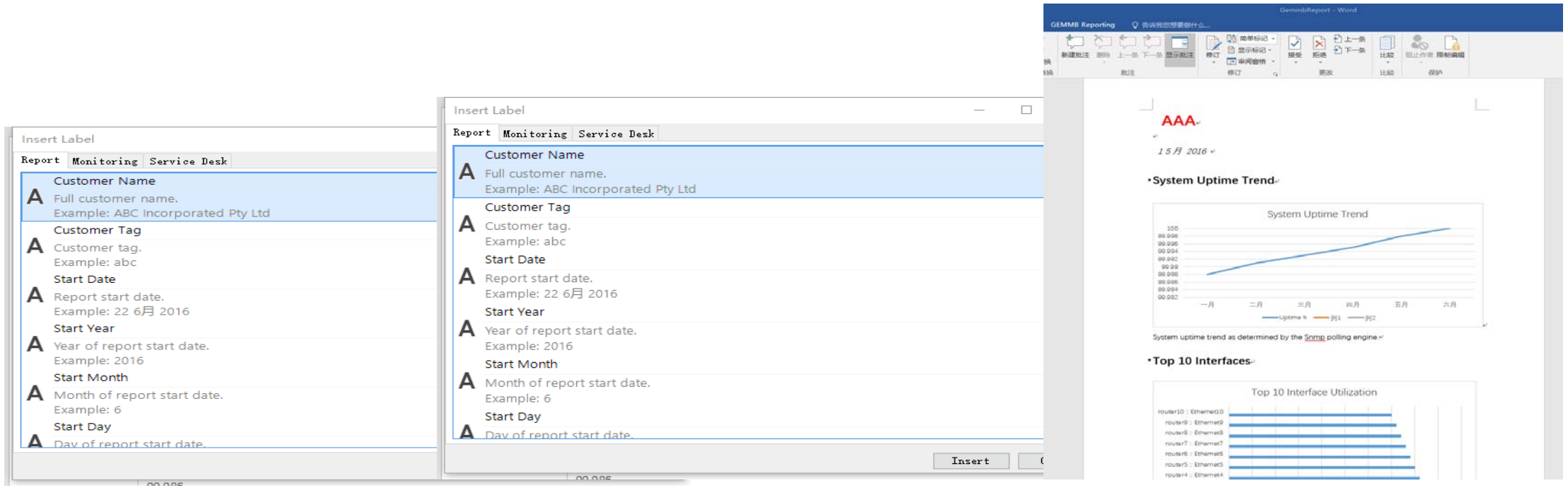
- All-In-One的企业级网络和安全监控管理系统;
- 基于云，同时可以服务于传统的IT基础架构和新兴云平台;
- 全面的安全管理子系统可以满足大中型企业对于管理权限的要求;
- 从100台到10000台被管理设备，只需要增加计算资源，存储空间和采集器的数量，无需重新安装系统;
- 系统提供完整的Web API，为客户提供了广泛定制化的可能，包括支持移动设备，Web页面的定制化，Widget的支持和现有通讯工具的支持，包括短信，微信和邮件;
- 管理包和更新包同时支持人工和自动的更新，系统的大部分更新无需重新启动，大大提升了系统的可用性和安全性。
- Ticket系统支持IT管理中最重要的三个管理流程：故障管理流程，问题管理流程和变更管理流程，为了方便IT人员的管理，对三个系统进行了有机的整合，形成自动的上报流程;

采集系统

- 高可扩展和高可用的采集系统（Poller/Connector）
  - 可根据客户的网络的不断扩展而部署相应的采集服务器;
  - 可根据地理上的需求部署采集服务器;
  - 多采集服务可以支持Load-Balance, HA 等备份方式，达到高可用的监控部署;
  - 每台轮训服务器可以支持1000台标准监控设备，平台可扩展至监控1万台设备。
- 采集系统连接性
  - 配置信息以推送的方式传递给采集服务器。
  - 为转询服务器与后端系统开放“outbound”连接通道。
  - 使用SSL加密方式。
  - 不需要为采集服务器提供专用的IP地址，并且完全支持NAT和PAT。
  - 采集系统可用布置在客户网络中（无需改变防火墙的任何配置），也可用布置在后台（需要使用到专线或者VPN系统）；
- 协议支持
  - SNMP v1,v2c，v3, SNMP trap;
  - Syslog,
  - telnet, SSH,RDP(Windows 远程桌面系统）
  - ODBC/JDBC
  - FTP
  - Script 脚本监控模式
  - ….

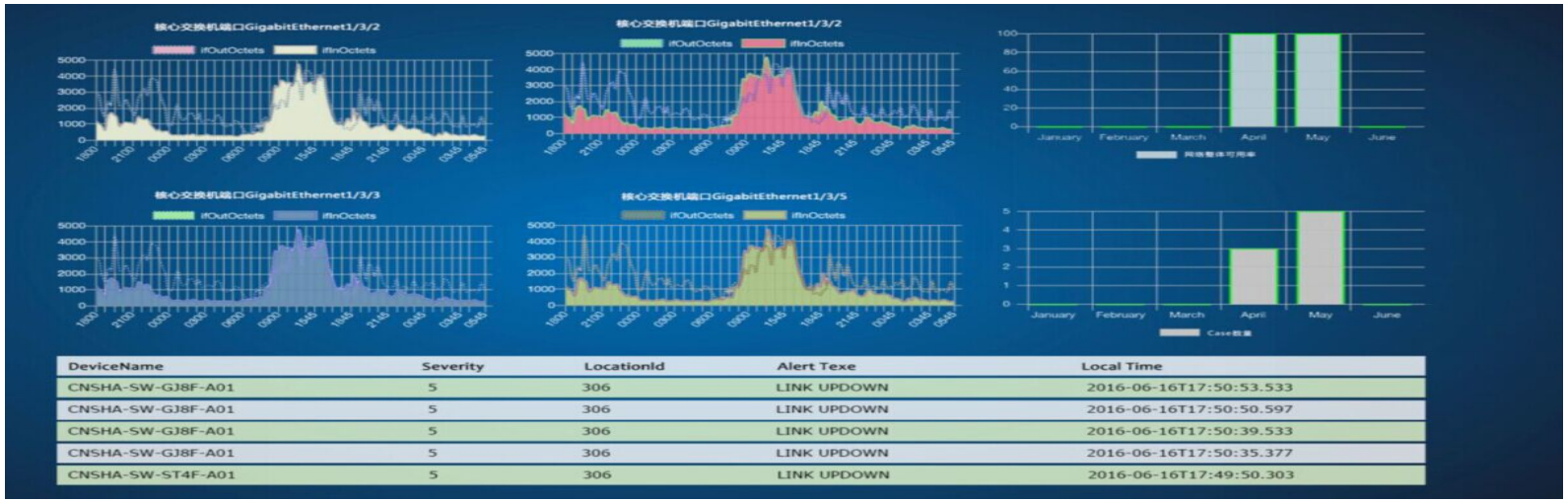
报表系统

- 独特的报表系统，结合了Word和API开发而成的Report plugin for Word，让报表的制作简单并且有个性化；
- Word 强大的报告展示功能和广泛的使用性；
- API可以直接允许Word 读取管理数据；
- 通过Word支持广泛的报告格式，包括html，pdf，doc，docx等



个性化的仪表盘

- 基于API，平台系统为客户在展示方面提供了空前的灵活性
- 基于HTML5的单页或者多页(自动滚动)的展示,直观的显示网路的允许状况；
- 适合客户不同角色的，个性化的仪表盘;
- 自适应大小的仪表盘，可以支持投影仪和电视等大屏幕，也支持PC机等标准屏幕和手持式设备等小屏幕

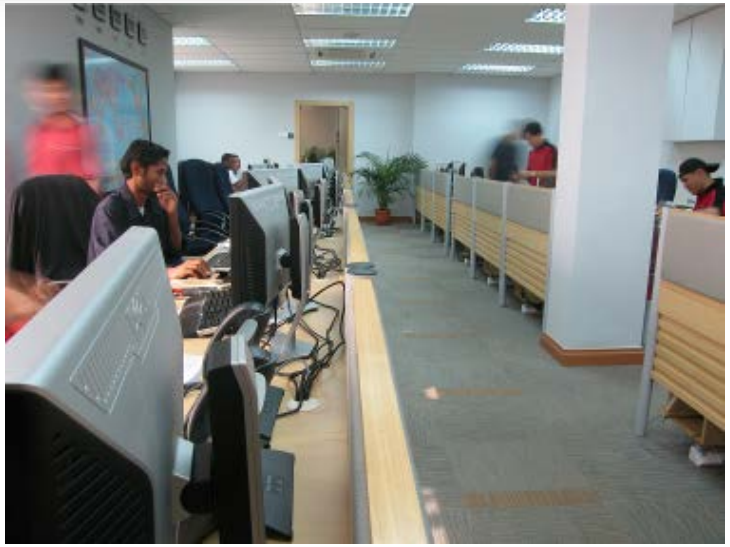


DeviceName	Severity	LocationId	Alert Texe	Local Time
CNSHA-SW-GJ8F-A01	5	306	LINK UPDOWN	2016-06-16T17:50:53.533
CNSHA-SW-GJ8F-A01	5	306	LINK UPDOWN	2016-06-16T17:50:50.597
CNSHA-SW-GJ8F-A01	5	306	LINK UPDOWN	2016-06-16T17:50:39.533
CNSHA-SW-GJ8F-A01	5	306	LINK UPDOWN	2016-06-16T17:50:35.377
CNSHA-SW-ST4F-A01	5	306	LINK UPDOWN	2016-06-16T17:49:50.303

安全功能

- Password Vault功能
- 集中保存系统，被管理设备，包括网络设备，服务器等设备的密码，并且和平台的用户进行绑定
- 和平台系统用户绑定，操作人员无需记忆相应的密码，降低了密码泄露的可能性
- 方便第三方公司和员工访问相关设备，并且无需提供设备的访问权限
- 支持一次性和有时限的Password，并纪录登录时间。

数据中心和监控中心



服务团队

NOC&SOC Manager

- 平台安全规则的制定与审核交付物质量
- 控制安全事件处理的过程
- 客户化的策略及报告定制
- 整个平台维护、日常管理、技术优化、场地管理
- SOC人员的管理和岗位职责的优化
- 安全事件流程的设计和优化

NOC&SOC运维负责人

NOC&SOC支撑负责人

一线

- 负责监控安全事件
- 安全趋势的跟踪
- 监控事件的初步分析
- 在线客户问题的答疑
- 安全事件的分配
- 安全问题的发现与告知
- Case进行跟踪

二线

- 在线客户问题的答疑
- 安全事件的分析与解决
- 客户服务初始化和注销
- 代理的安装与配置
- 一线监控组的技术支持

三线

- 紧急安全事件的现场响应
- 客户紧急故障的现场处理
- 客户安全事件跟踪
- 应急响应报告
- 部分安全研究的工作

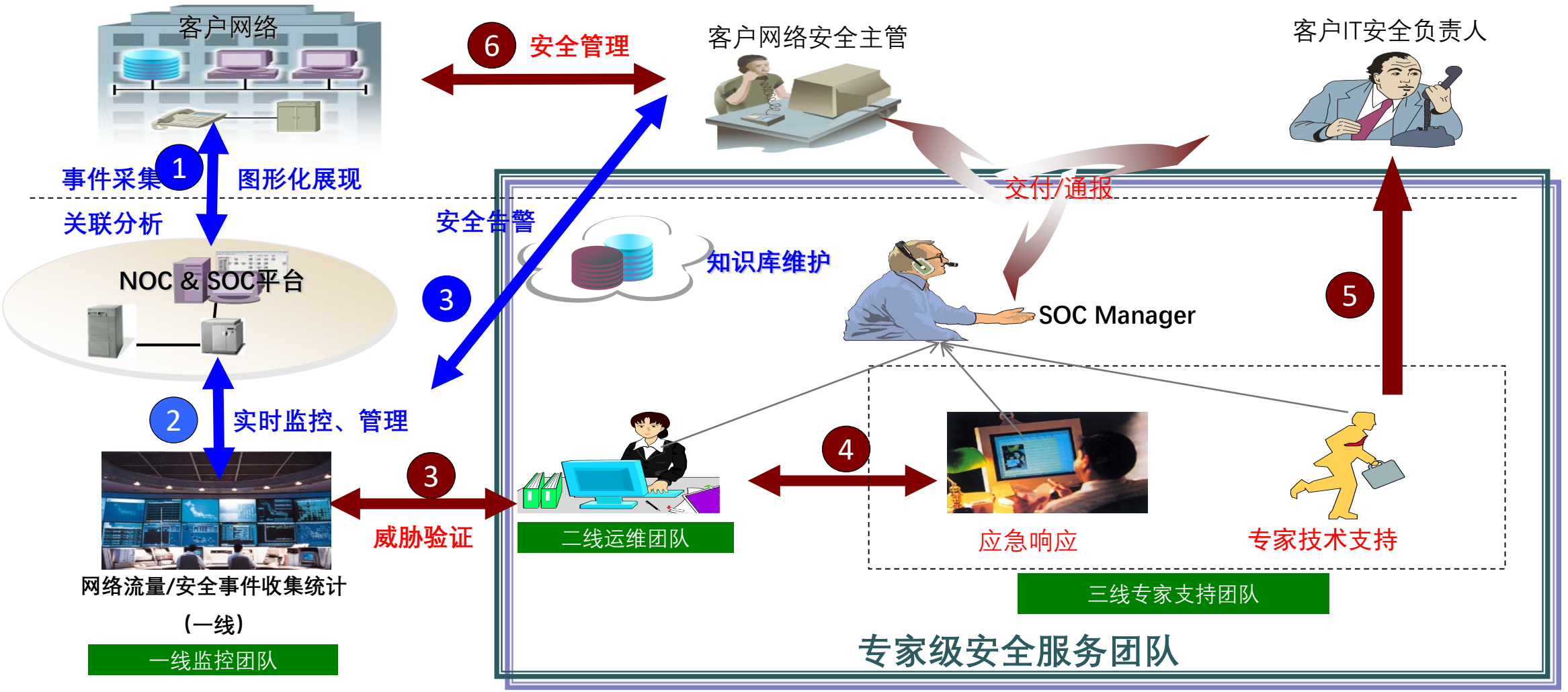
技术专家

- 重大的安全事件应急
- 新漏洞、新问题等的安全研究工作
- 系统、应用、设备等的安全问题研究

服务流程

SaaS服务

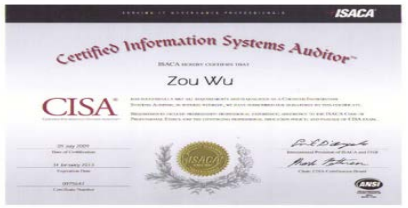
管家式服务

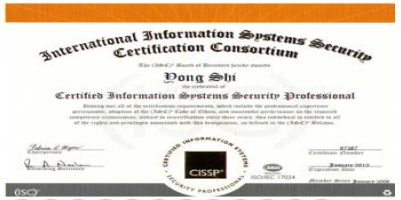


人员资质

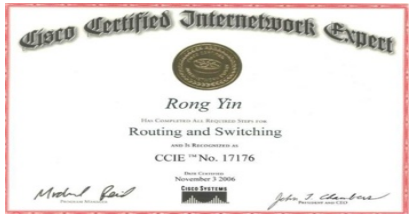
优秀的技术团队

PMP项目经理





安全咨询顾问：PCI-DSS QSA、ISO27001LA、CISA、COBIT、CISSP、CISP以及等保测评师认证人员



安全技术工程师：网络（CCIE）、主机（RHCE）、数据库、存储认证专家

公司有100多名专业的：

1. 安全技术顾问
2. 网络技术专家
3. 安全咨询顾问
4. 安全事件处理专家

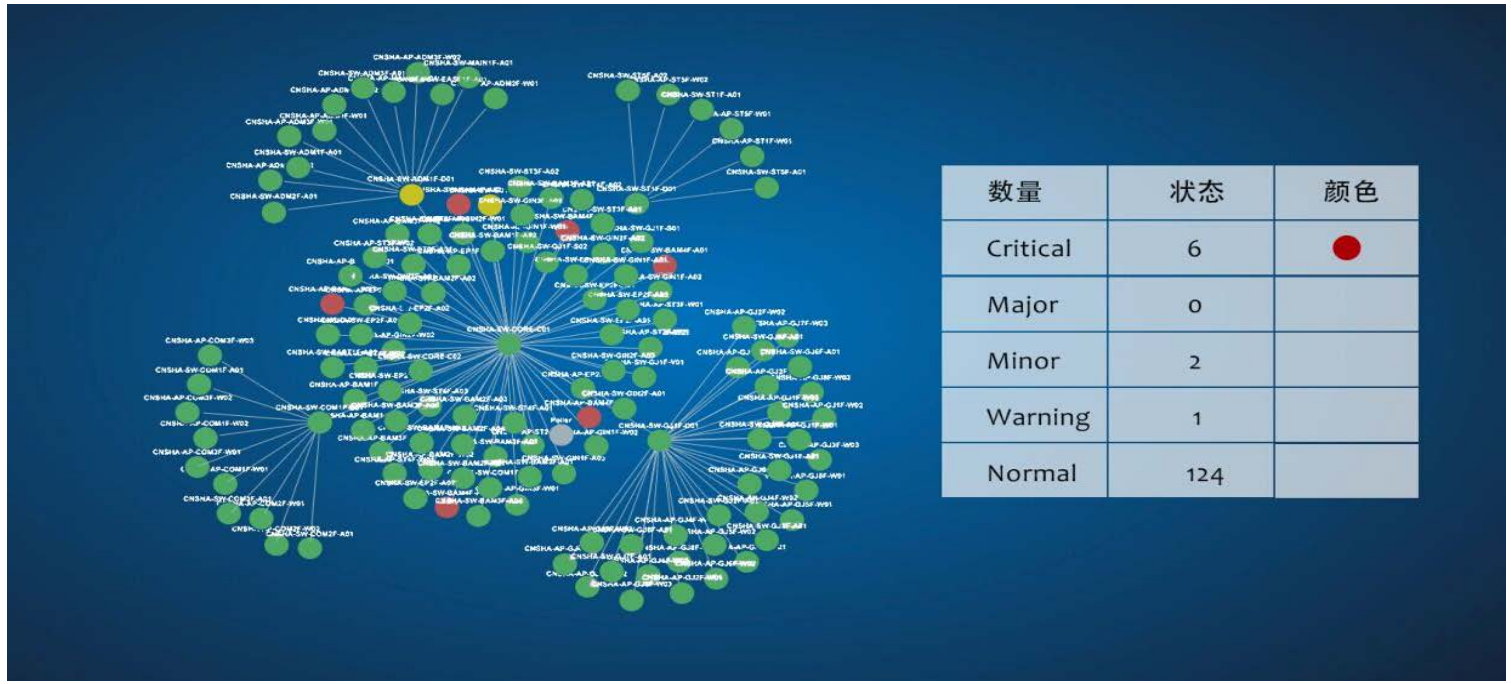
服务工程师

安全咨询顾问

安全事件处理专家

服务形式

- 7*24的GNC运营中心;
- 多数据中心的负载;
- 400 统一热线;
- 基于流程的工单支撑系统;
- 按需在线周报/月报
- 按需定制实时更Dashboard
- 多种方式的即时通知:
  - 邮件
  - 短信
  - 电话
  - 微信



数量	状态	颜色
Critical	6	
Major	0	
Minor	2	
Warning	1	
Normal	124	

服务价值

“管家式安全服务外包”到底能给客户带来什么好处?

省心	➢ 提供7*24小时实时监控 ➢ 网络、安全专家全程支持，安全无忧
省力	➢ 功能齐全，全程无忧 ➢ 完善服务体系，保证及时开通业务，提供优质服务
省时	➢ 实时监控、主动服务，及时发现故障、缩短处理时间 ➢ 定期提供网站安全报告，第一时间提供故障分析报告
省钱	➢ 专家级的方案能力 ➢ 平民级的财务投入

客户得益

·安全保障

·专业服务

·节约时间

·降低成本

服务总结

- 通过NOC&SOC的专业人员、核心技术和规范流程，我们的安全外包服务能为您提供完整的安全解决方案，包括:
  - 最适合您的网络解决方案及建议
  - 最合适您的安全解决方案及建议
  - 网络、安全领域的专家意见
  - 最新、最及时的安全通告信息
  - 7*24小时的监控和管理
  - 政策及法规的咨询
  - 稳定和可预见的IT安全开支

Thank You!