HUAWEI ENTERPRISE A BETTER WAY

华为 iSOC 统一安全管控解决方案

——全面、智慧、高效

enterprise.huawei.com

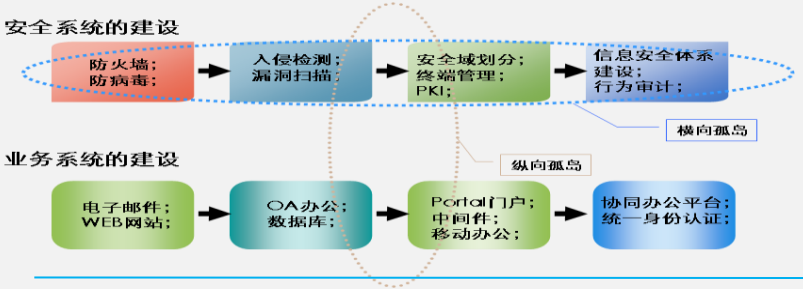
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

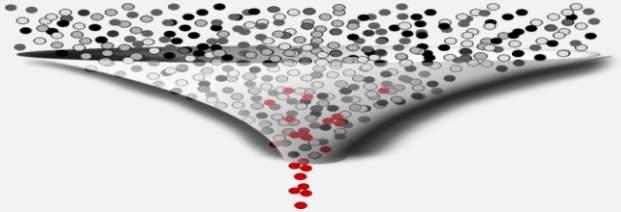
Content

云时代，IT运维面临的挑战

挑战1：审计孤岛的尴尬
分散监控，单点审计，人力浪费

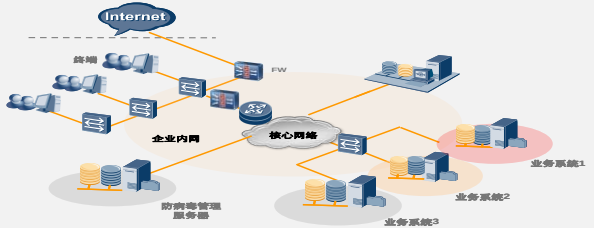


挑战2：数字洪水产生海量日志
发现价值信息有如大海捞针



挑战3：如何保证合规性

挑战4:内控措施缺乏，核心数据泄露
监控困难



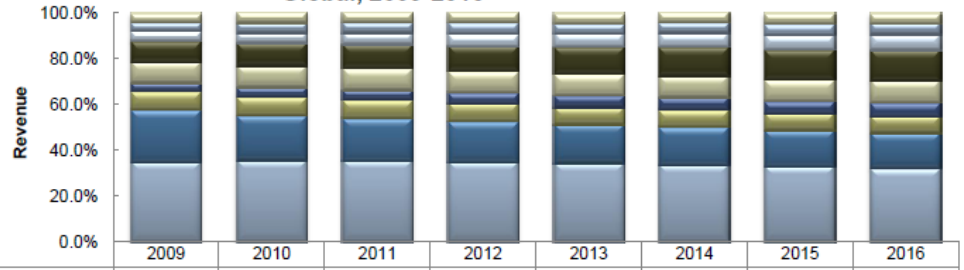
HUAWEI

安全管控日益紧迫

安全信息和日志管理日益成为企业应对网络威胁的重要一环。

Key Takeaway: SIEM and log management are becoming widely adopted services for many organizations.

Managed/Monitoring (CPE) Services Segment: Percent Revenue Forecast by Service, Global, 2009-2016



	2009	2010	2011	2012	2013	2014	2015	2016
Others*	4.0	4.3	4.2	4.2	4.6	4.2	4.7	4.6
End-point security	3.9	4.4	4.5	4.8	4.4	4.4	4.7	4.8
UTM	4.2	4.5	5.1	5.4	5.9	6.2	6.6	6.8
SIEM and log management	9.2	9.8	10.4	11.0	11.8	12.6	13.0	13.3
Identity access and management	9.2	9.5	9.5	9.3	9.3	9.5	9.4	9.7
DLP	3.7	4.1	4.3	4.7	5.2	5.3	5.5	5.8
Content filtering	8.0	8.2	7.9	7.8	7.5	7.5	7.3	7.6
IDS/IPS	22.8	19.5	18.7	17.8	17.0	16.6	15.9	15.4
Firewall IPSec	35.0	35.7	35.4	35.0	34.3	33.7	32.9	32.0

Year

Note: *A list of "Others" can be found in the appendix.

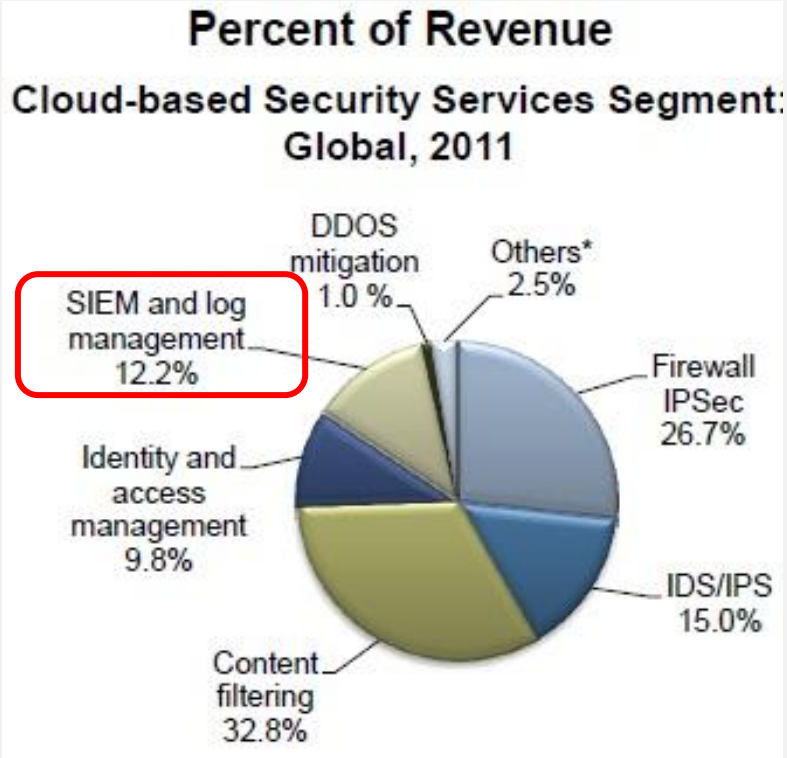
Note: All figures rounded. The base year is 2011. Source: Frost & Sullivan analysis.

Source: Frost & Sullivan analysis.

HUAWEI

安全管控日益紧迫

云时代的到来，安全是一切的前提。
调查发现，安全信息和日志管理已经成为云安全平台建设中的重要组成部分。



Source: Frost & Sullivan analysis.

HUAWEI

如何应对

统一管控平台

事前

- 查看设备漏洞信息，通过将漏洞与资产相关联，及时发现问题，防范问题；
- 通过原始事件、资产信息，动态比对历史数据，提前预警高危资产和高危业务系统。

事中

- 通过实时关联分析及时发出告警；
- 通过工单管理，实现安全告警事件的建立、跟踪、处理、审核的闭环管理，并提供问题回溯机制，提高运维水平。

事后

- 提供多种组合条件的日志查找，实现法规遵从要求；
- 行为审计软件提供快速的安全职责定位。

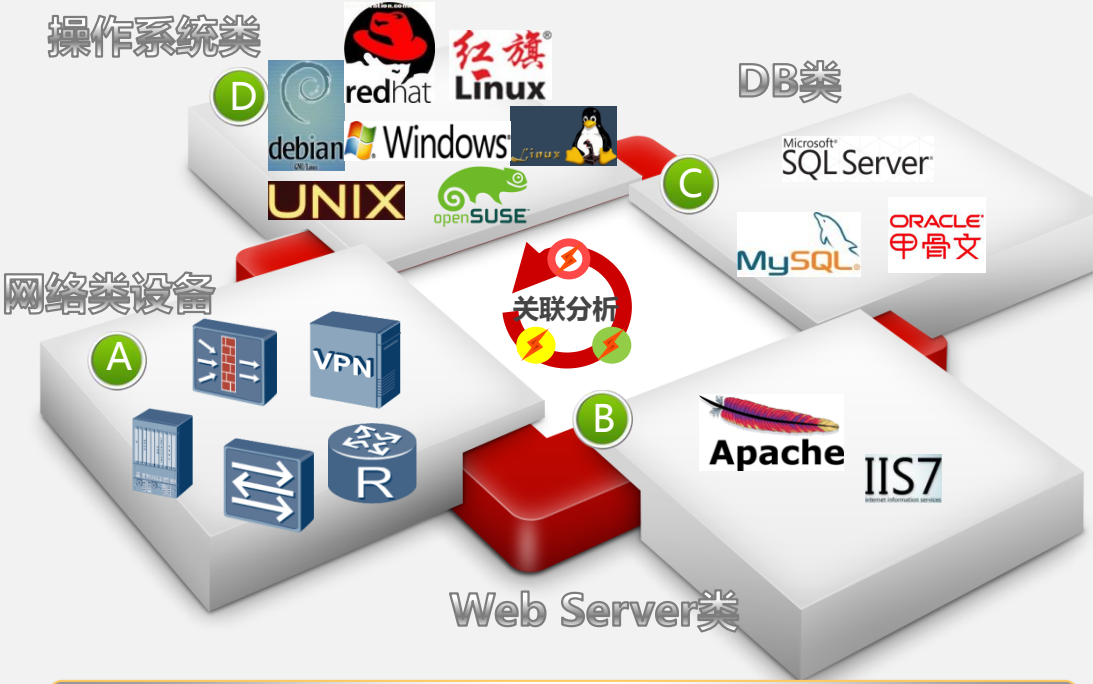
Content

iSOC安全管控设计思路

- 整体安全状态
- 等级保护水平
- 安全投资回报率

- 建立全局安全策略
- 等级保护自评测
- 报表报告

- 网络可用性监控
- 安全事件监控分析
- 预警与应急响应



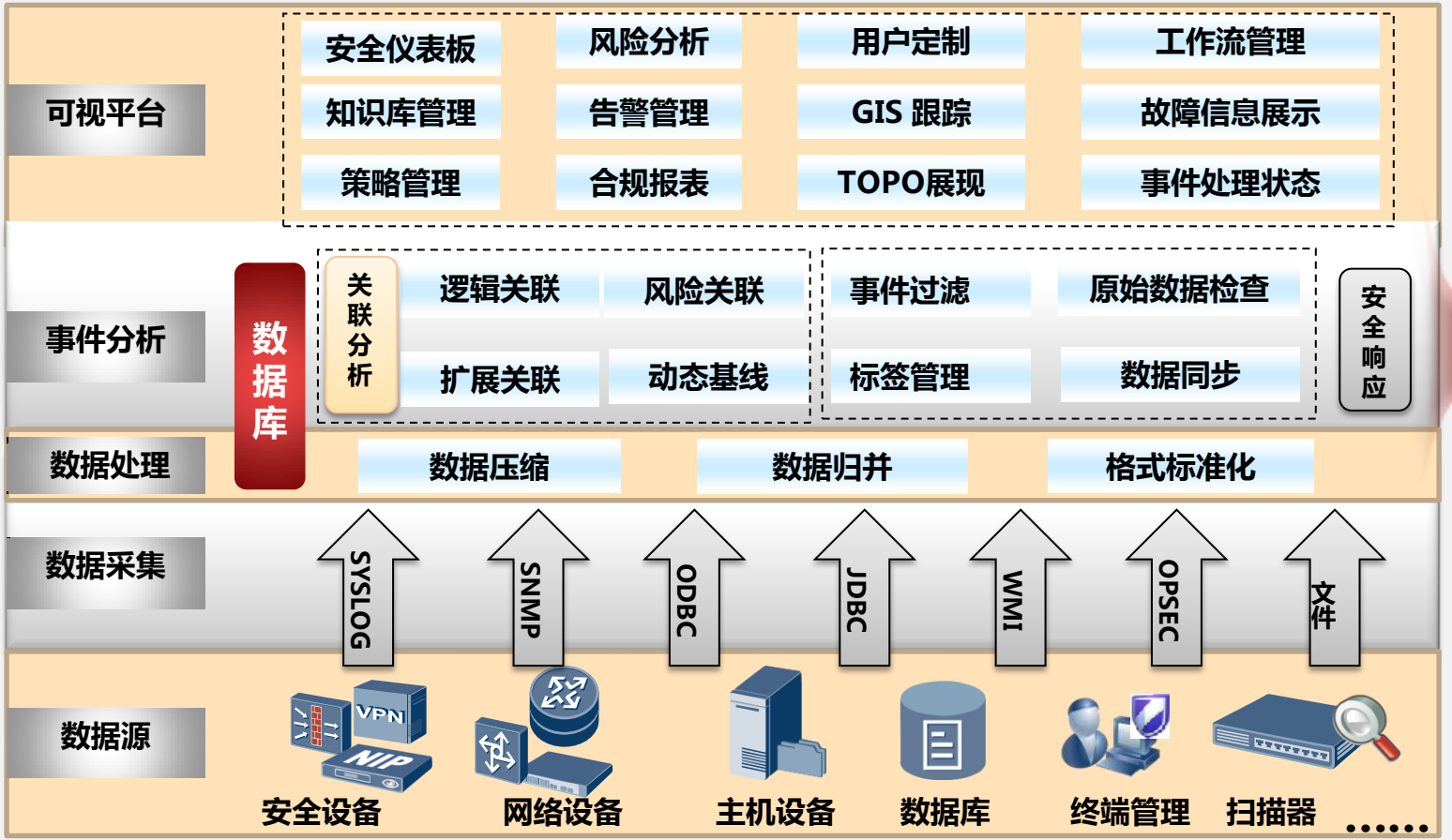
客户需求

日志采集，关联分析，合规匹配

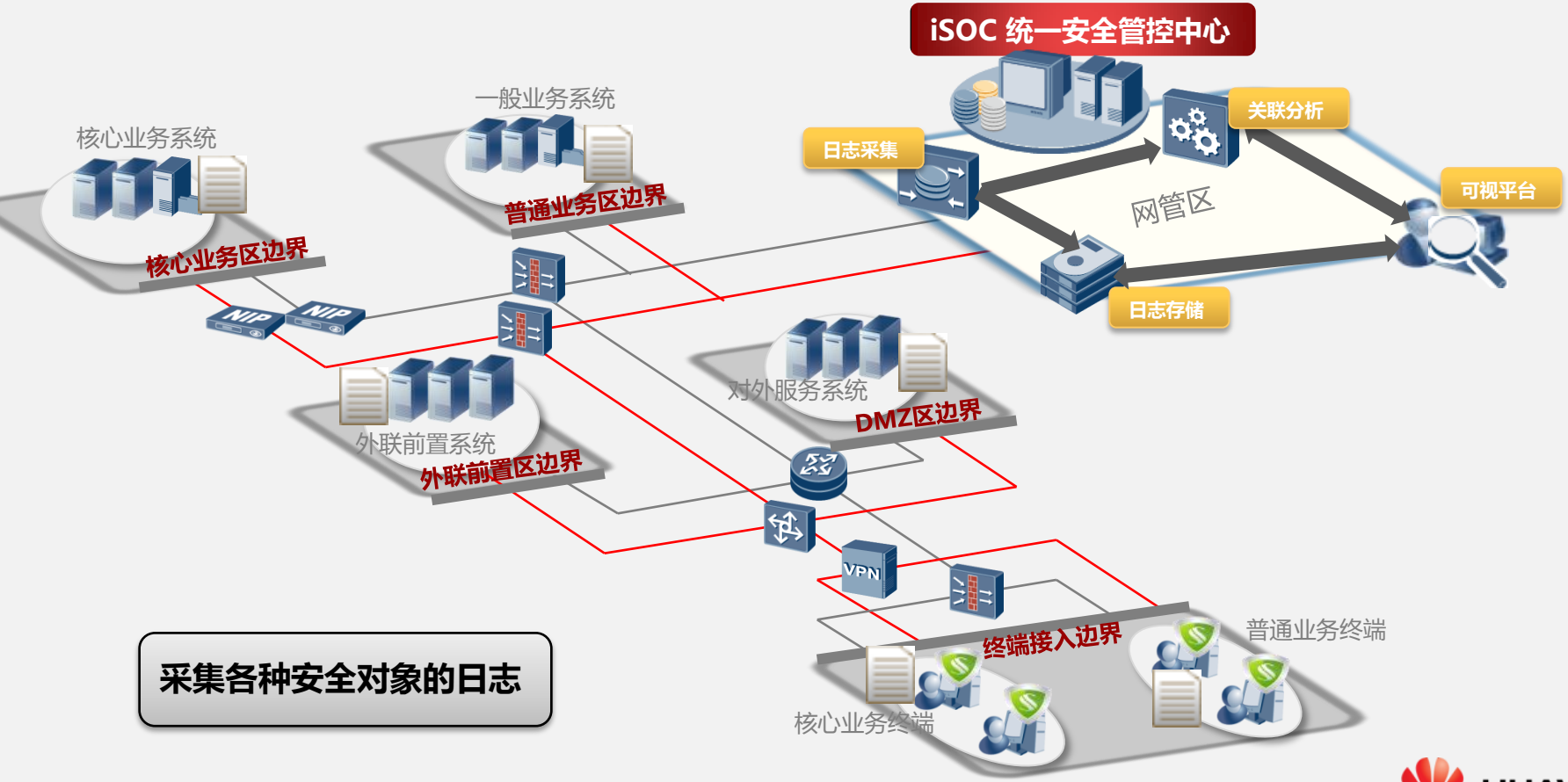
安全管理可视化

HUAWEI

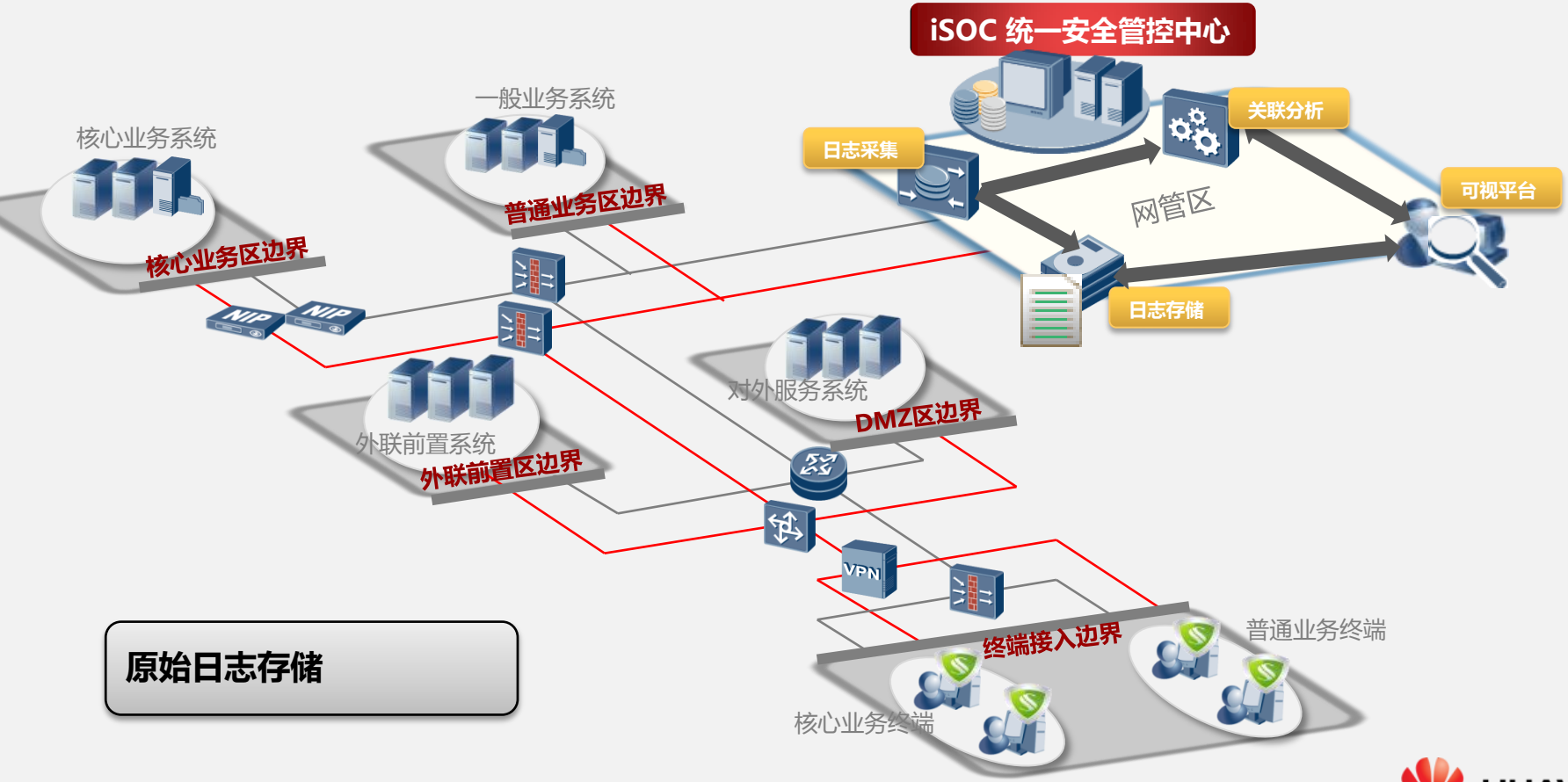
iSOC安全管控功能架构



iSOC系统工作流程

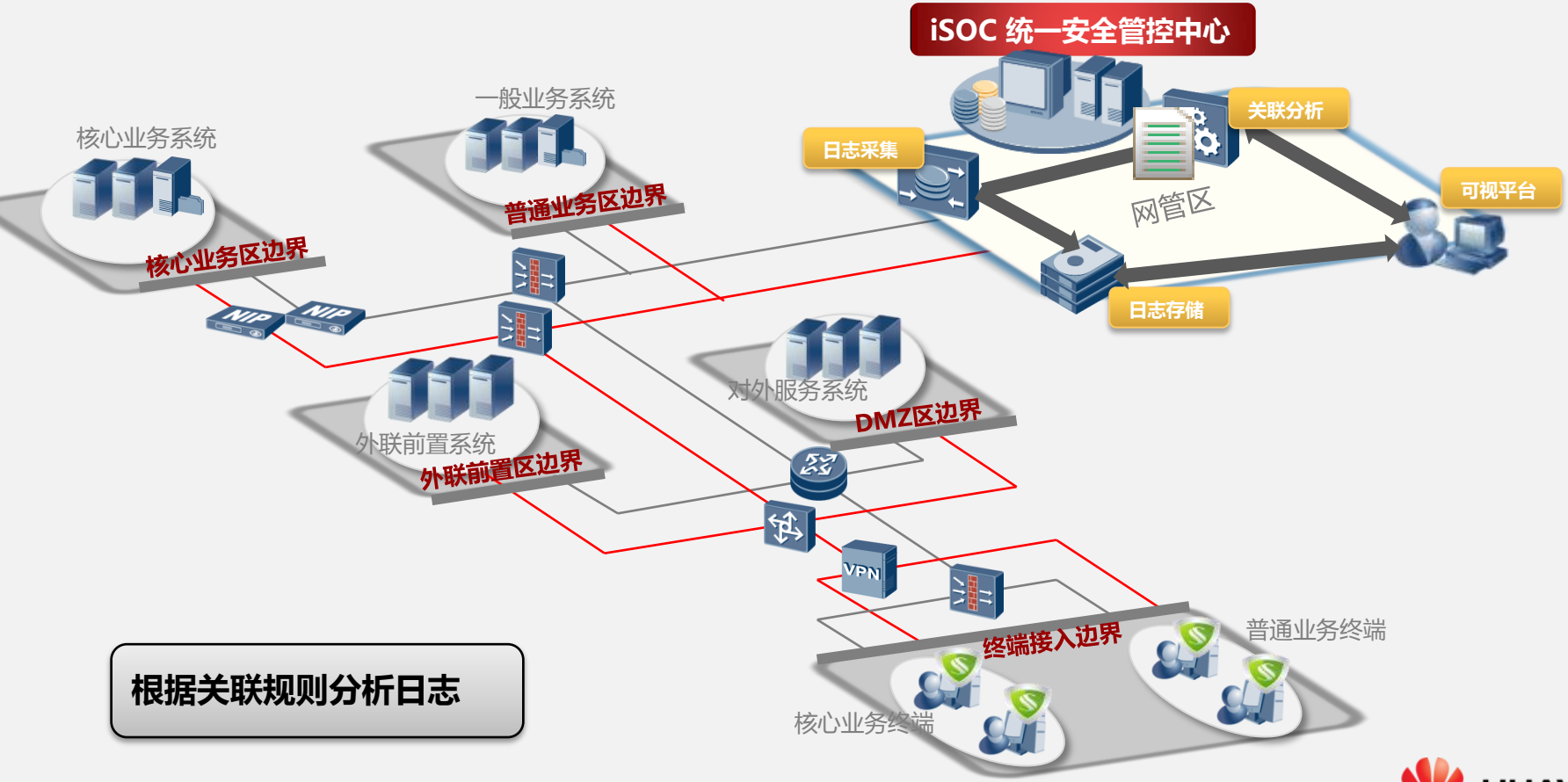


iSOC系统工作流程



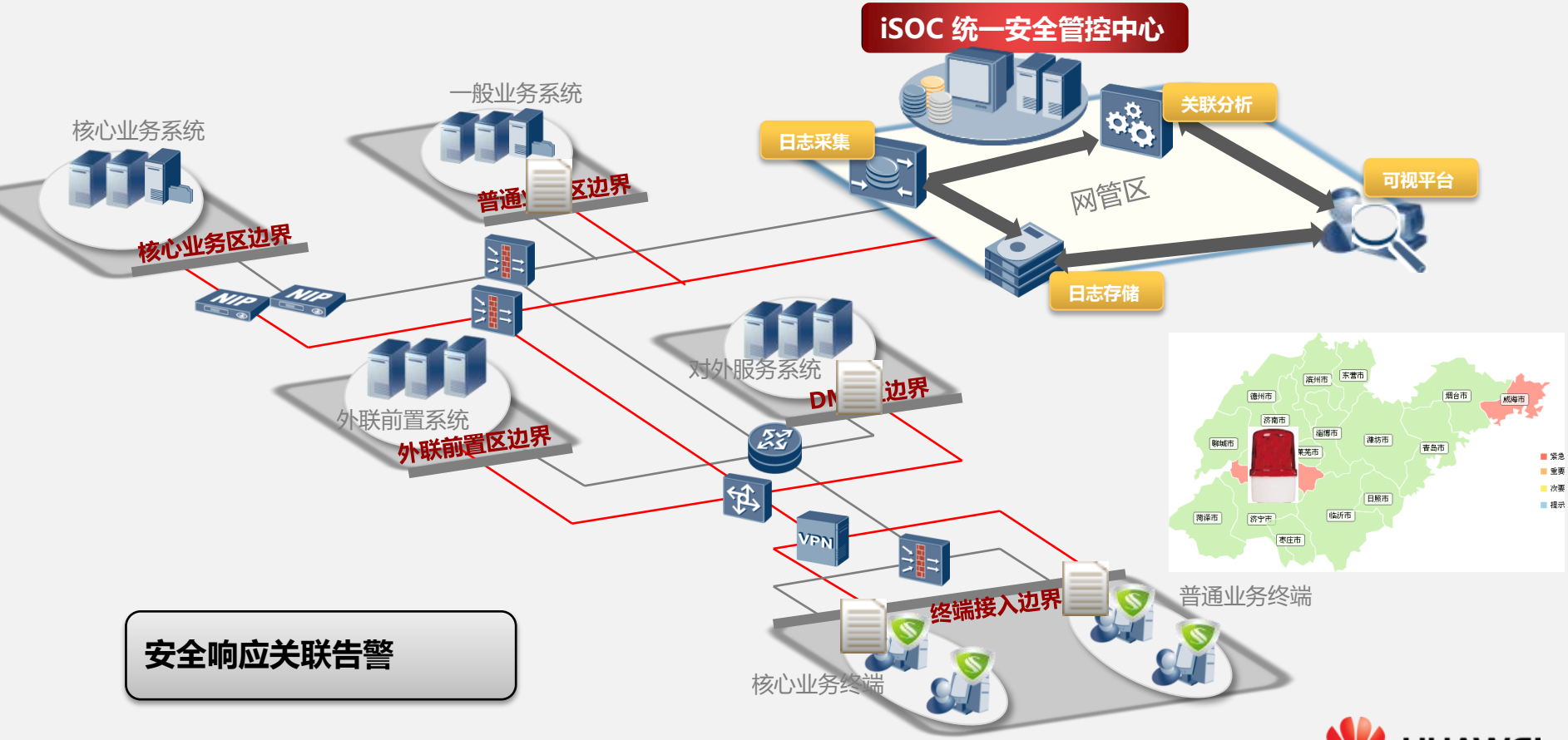
原始日志存储

iSOC系统工作流程



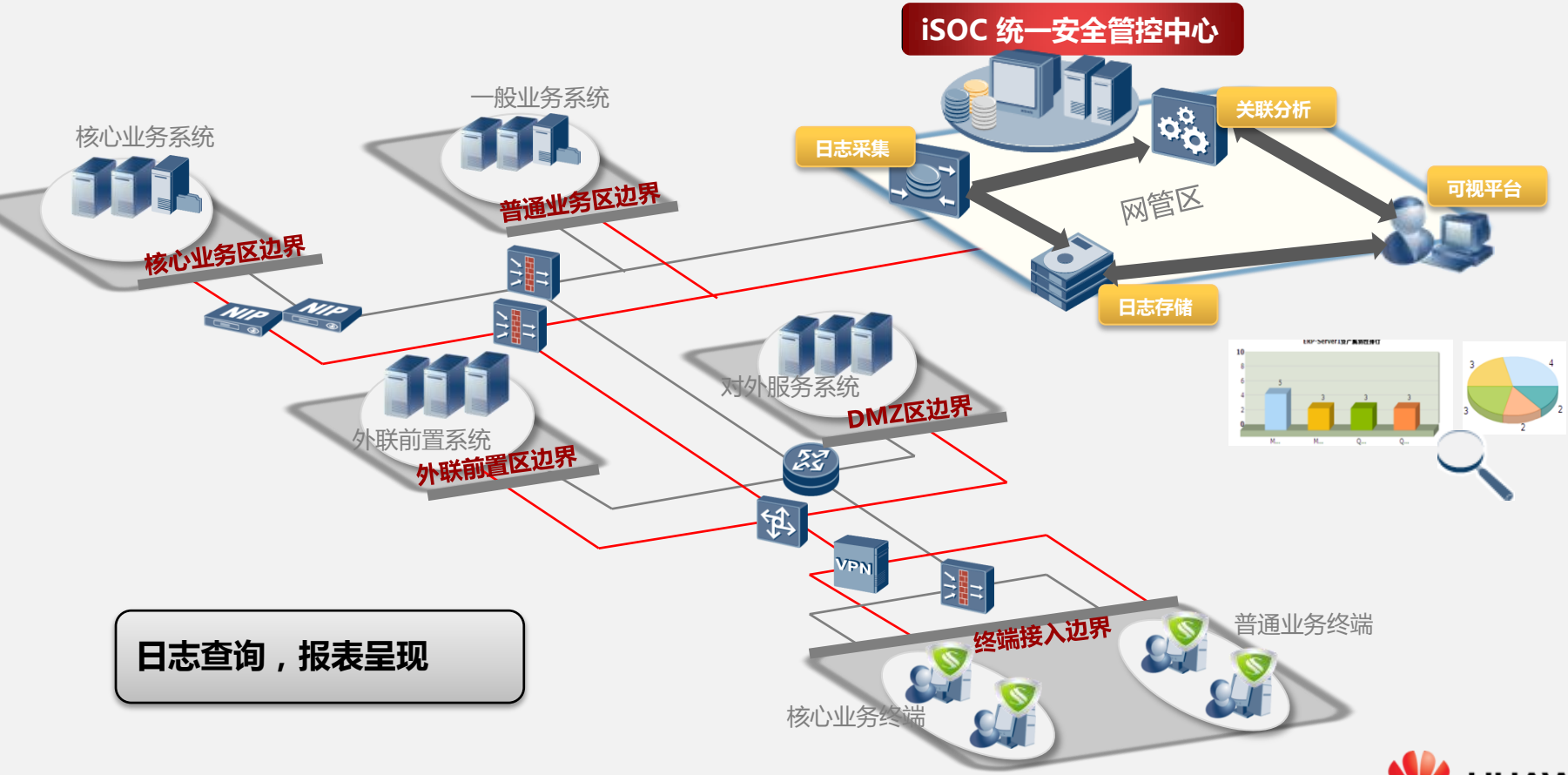
根据关联规则分析日志

iSOC系统工作流程



HUAWEI

iSOC系统工作流程



日志查询，报表呈现

HUAWEI

全面的信息事件采集

- iSOC支持160多类设备的日志采集和识别，包括主流的主机系统、数据库、网络设备、安全设备和存储设备等
- 对于非主流设备的日志提供快速定制接入，实现日志集中管理。

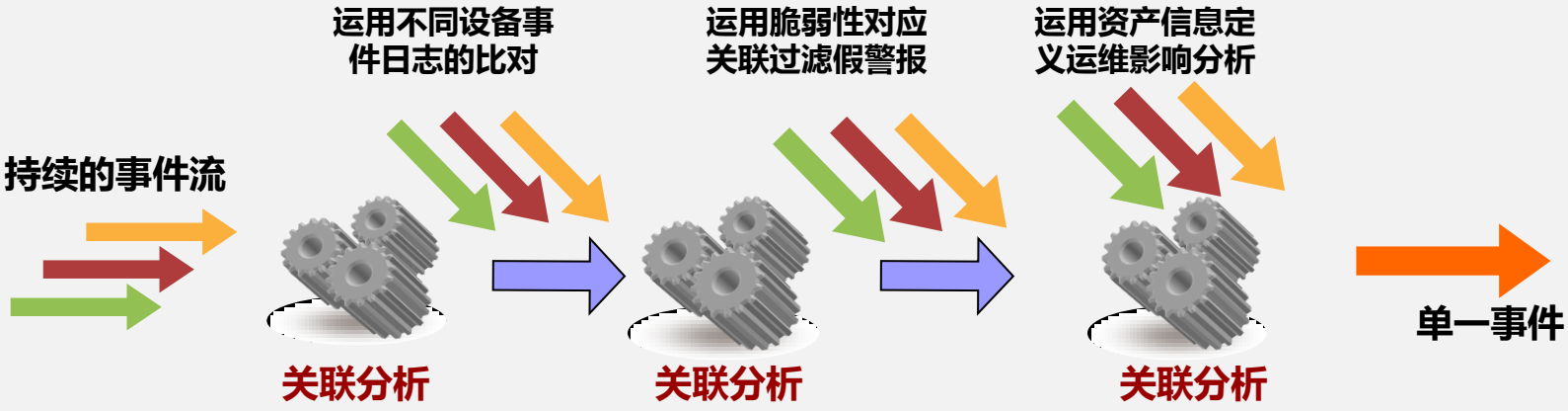
HUAWEI

高速、智能的关联分析引擎

- 通过跨物理、虚拟和云环境同步数据，将所有孤立的 IT 数据捆绑到单一智能仪表板，从而将安全事件数据实时转换成有用信息，在复杂的网络环境中，帮助客户快速定位安全异常。
- 内置100多条关联规则模板，帮助客户精确洞察IT漏洞。
- 提供现场定制客户化的关联规则，满足客户特定业务场景的安全需求。

HUAWEI

关联分析的三个维度



	IDS	FW	资产价值	脆弱性信息	严重等级
事件1	Attack	Deny	Low	-	0
事件 2	Attack	Accept	Low	-	2
事件 3	Attack	Accept	Medium	-	3
事件 4	Attack	Accept	Medium	Yes	4
事件 5	Attack	Accept	High	Yes	5

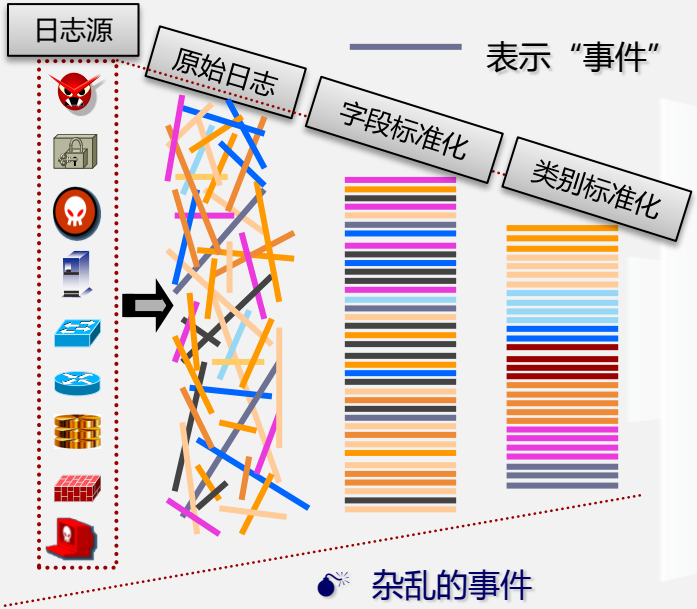
基本判断内容　　扩充判断内容

提高判断，精确定义安全事件等级。

HUAWEI

数据格式标准化

标准化=字段标准化+系统自动richer处理+用户自定义richer处理



脆弱性
- 基本配置
- 安全策略
- 安全漏洞
- 风险记录

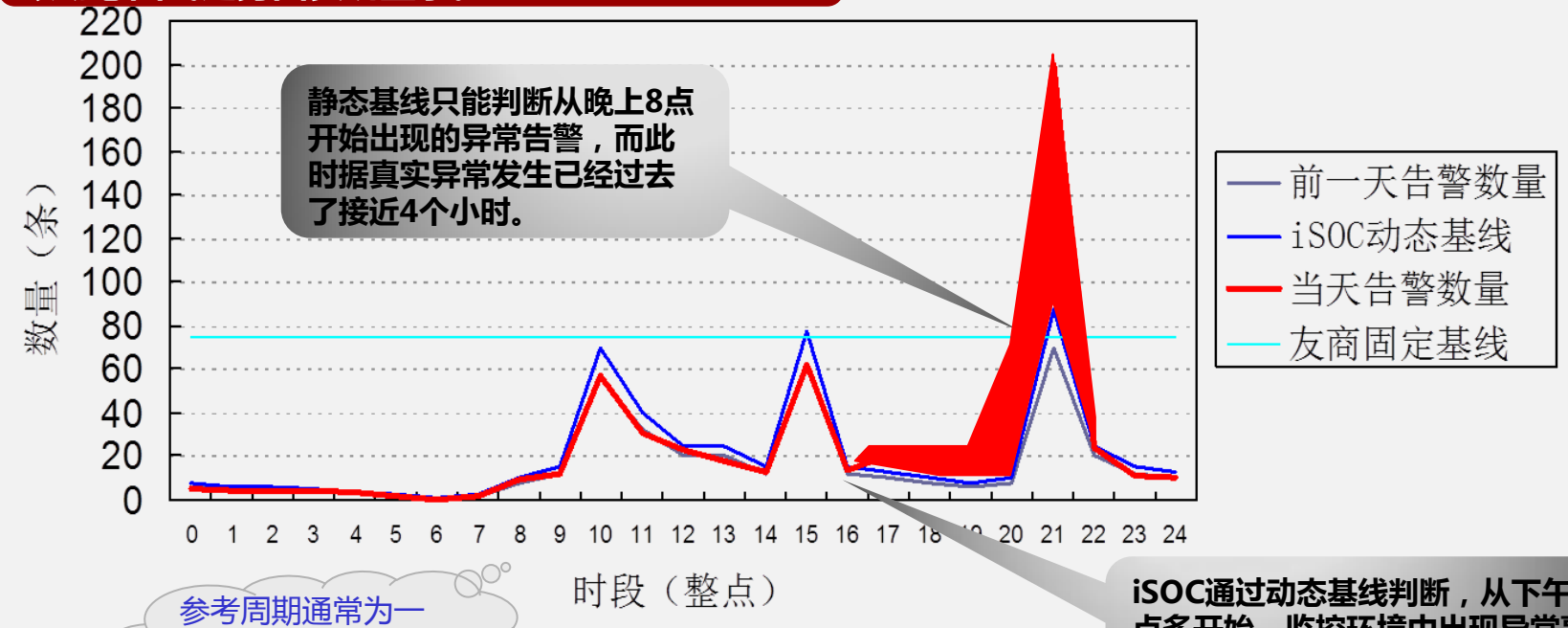
威胁活动
- 传统日志
- 活动状态
- 告警信息

资产价值
- 资产标识
- 资产角色
- 资产价值
- 资产机密

关联分析引擎

统计分析智能化

当前时段与历史段的事件频率自动比对和建模；以动态曲线趋势图实现显示。



静态基线只能判断从晚上8点开始出现的异常告警，而此时据真实异常发生已经过去了接近4个小时。

参考周期通常为一周；时间帧可细化到分钟！

iSOC通过动态基线判断，从下午4点多开始，监控环境中出现异常事件告警，异常从下午4点多一直持续到10点。

HUAWEI

分角色用户视图

不同角色的审计人员和领导具有自己的用户视图

Administrator

- 整体安全态势
- 等级保护水平
- 人员分权管理

Operator

- 建立全局安全策略
- 日常管理
- 问题分析

Auditor

- 用户操作审计
- 制定审计规则
- 定期日志审计

Security & Director

- 监控安全事件
- 审核安全员上报风险
- 协调问题处理

全网IT资源

iSOC统一安全管控平台

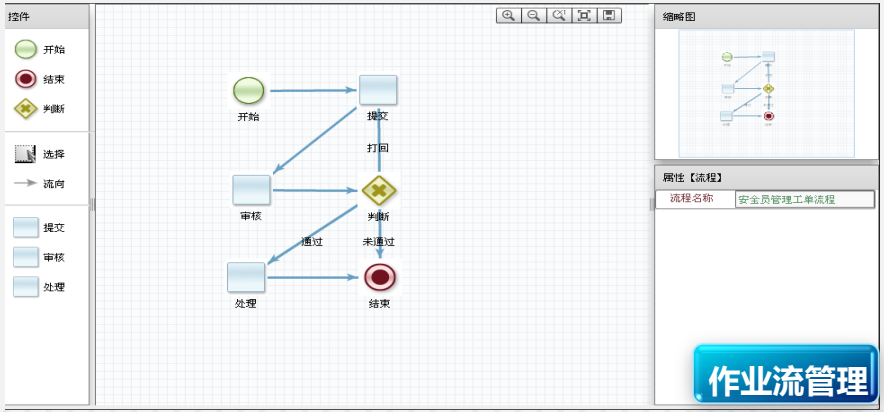
角色管理

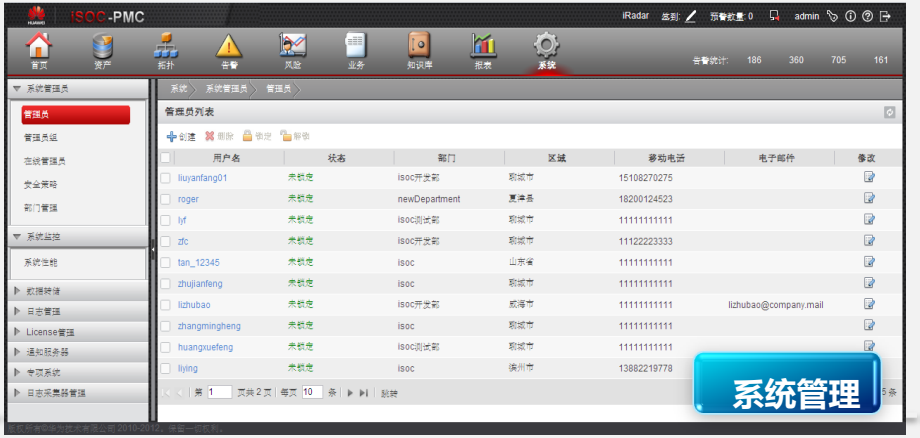
HUAWEI

运维管理可视化

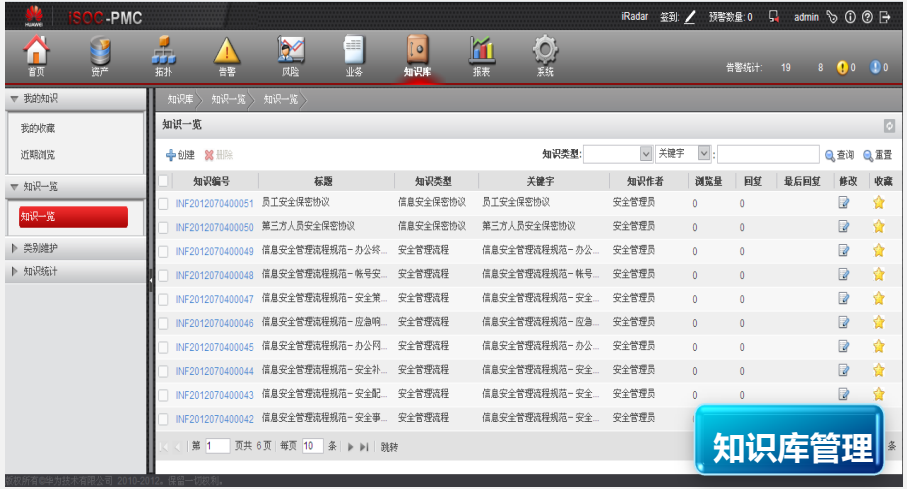
HUAWEI

运维管理可视化


控件
开始
结束
判断
选择
流向
提交
审核
处理
缩略图
开始
提交
打回
审核
判断
通过
未通过
处理
结束
属性【流程】
流程名称
安全员管理工单流程
作业流管理

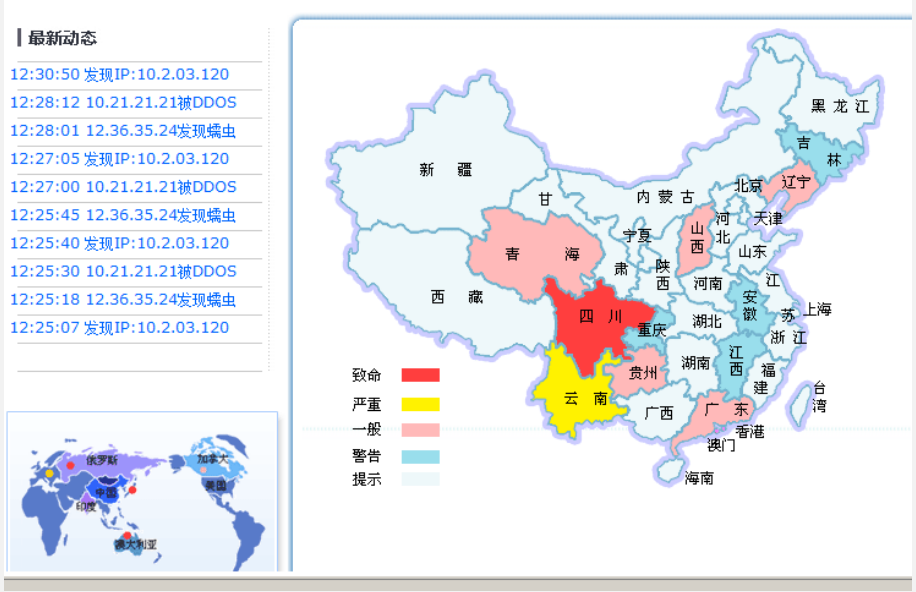

iSOC-PMC
管理员列表
系统管理


iSOC-PMC
资产统计图
查询条件
报表管理


iSOC-PMC
知识一览
知识库管理

安全态势可视化

- GIS快速定位
- 动态基线智能识别
- 攻击轨迹
- 追踪溯源

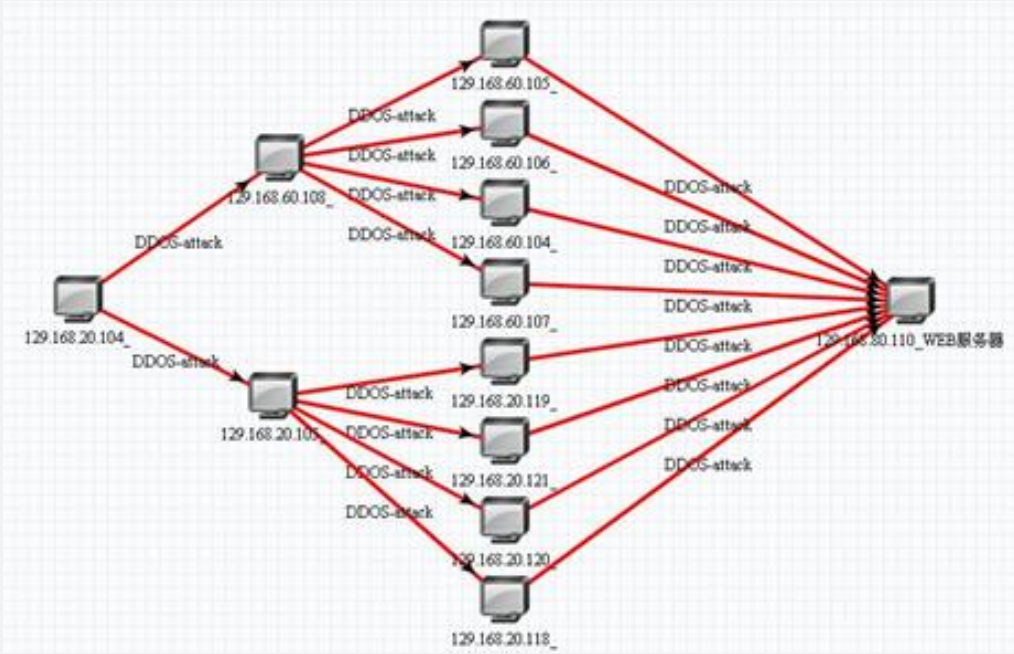


安全态势可视化

- GIS快速定位
- 动态基线智能识别
- 攻击轨迹
- 追踪溯源

安全态势可视化

- GIS快速定位
- 动态基线智能识别
- 攻击轨迹
- 追踪溯源



安全态势可视化

- GIS快速定位
- 动态基线智能识别
- 攻击轨迹
- 追踪溯源

合规报表展现

预置了大量的合规报表模板，包括Sarbanes-Oxley（SOX）、ISO27002、 BASEL II； PCI-DSS等。

Huawei iRadar 报表 在 2012年08月21日 下午 06时25分05秒运行

ISO 27002 Control of Operational Software：报告 2

操作软件
2012年08月
此报表列出了
作软件和数据

ImportPlugin
12-8-21 18:24
UpdatePlugin
12-8-21 18:24

EventSearch
12-8-21 18:23

ImportPlugin
12-8-21 18:23

enterpri

Huawei iRadar 报表 在 2012年08月22日 下午 04时00分56秒运行

Sarbanes Oxley Control of System Audit Data：报告 1

系统审计数据管理：当天
2012
此报表
备组，

Correla
12-8-2

Correla
12-8-2

Correla
12-8-2

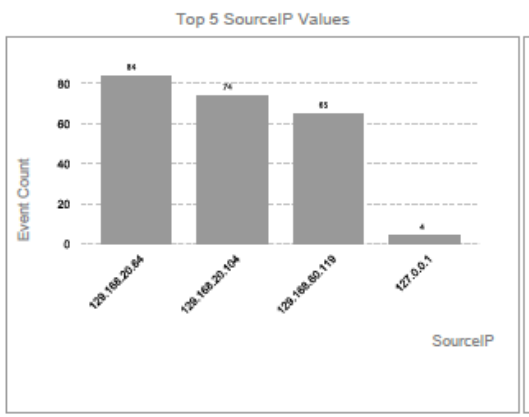
Correla
12-8-2

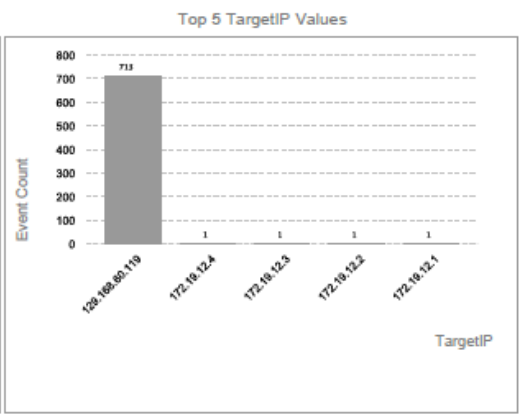
Huawei iRadar 报表 在 2012年09月04日 下午 05时08分51秒运行

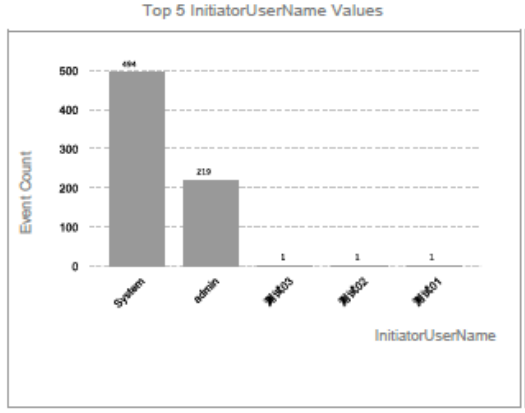
Basel II Control of System Audit Data：系统配置日

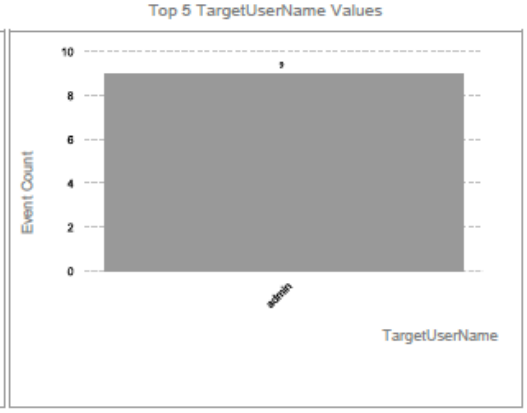
系统审计数据管理
2012年07月03日 下午 05时06分36秒 至 2012年09月04日
此报表列出了对软件和用于执行系统操作的数据的访问、修改事件。此
备组，并且包含这些数据的目录的审核级别是激活的。

事件名	源用户名
时间	
ImportPlugin 12-9-4 17:06:20	System Import plugin 报告 2 (ID 7DC
UpdatePlugin 12-9-4 17:06:20	System '报告 2' (ID 7DCEC9D6-D89 file 报告_21_17DCEC9D6D8 _21_17DCEC9D6D89D102F WJqjEijTqHSfViTfpjqV2g==)
EventSearch	admin

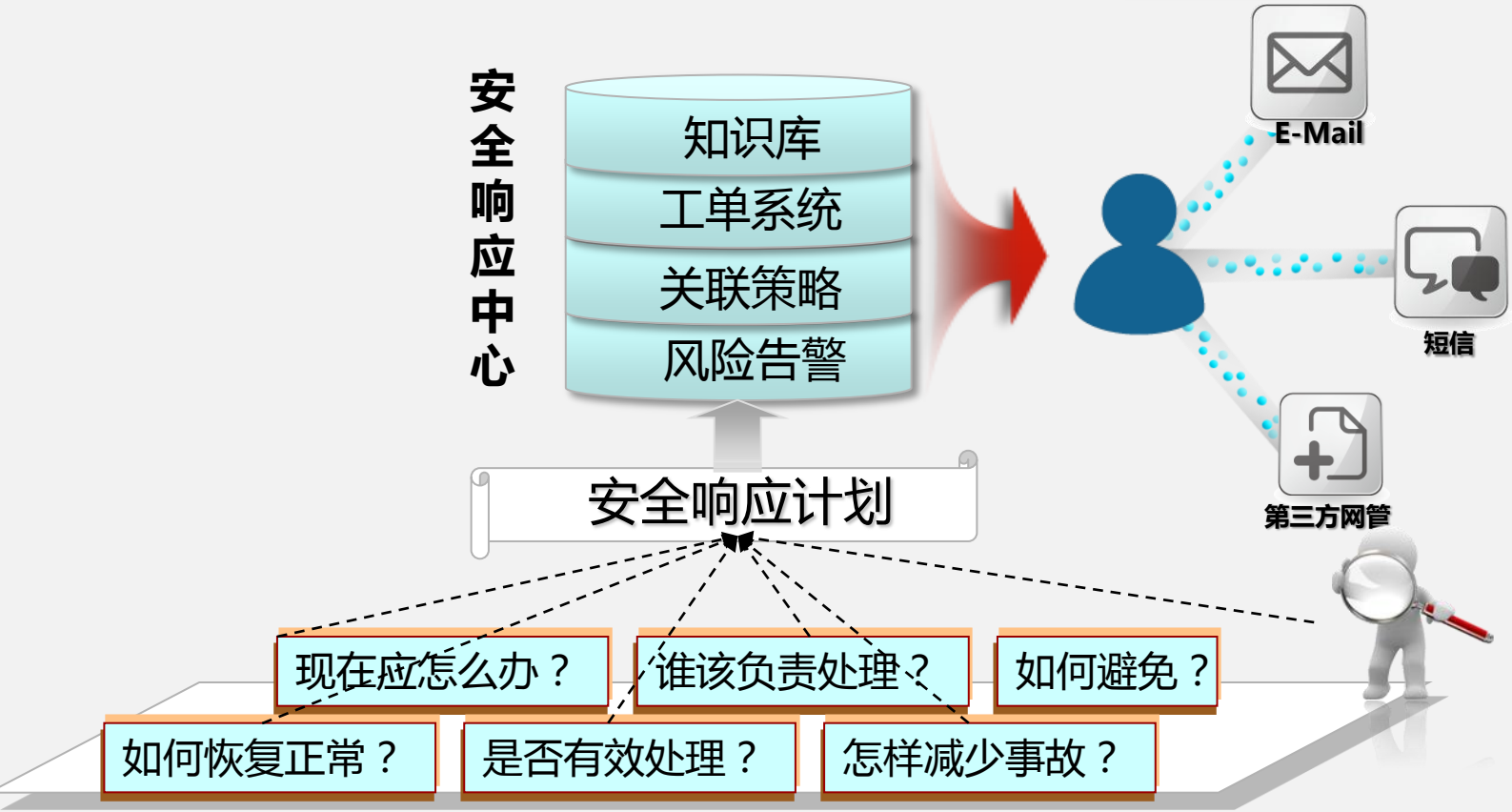




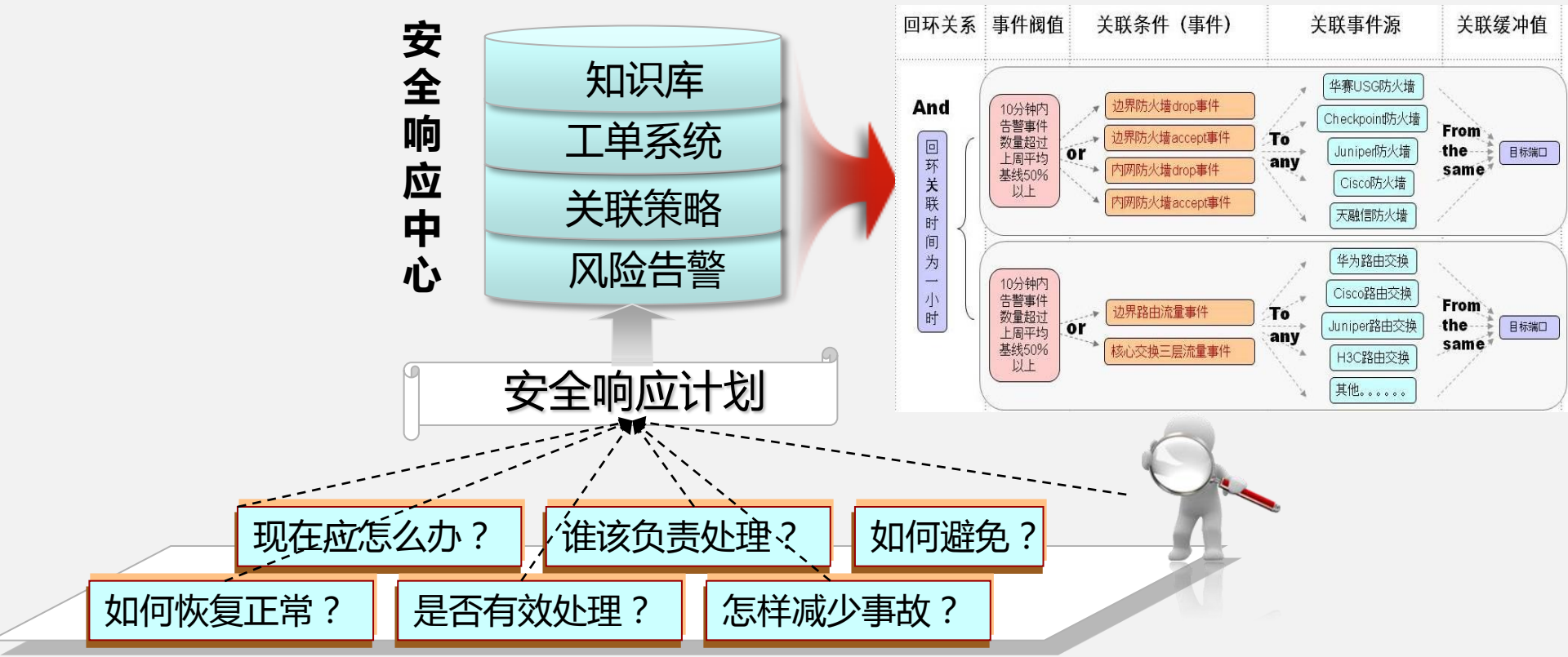




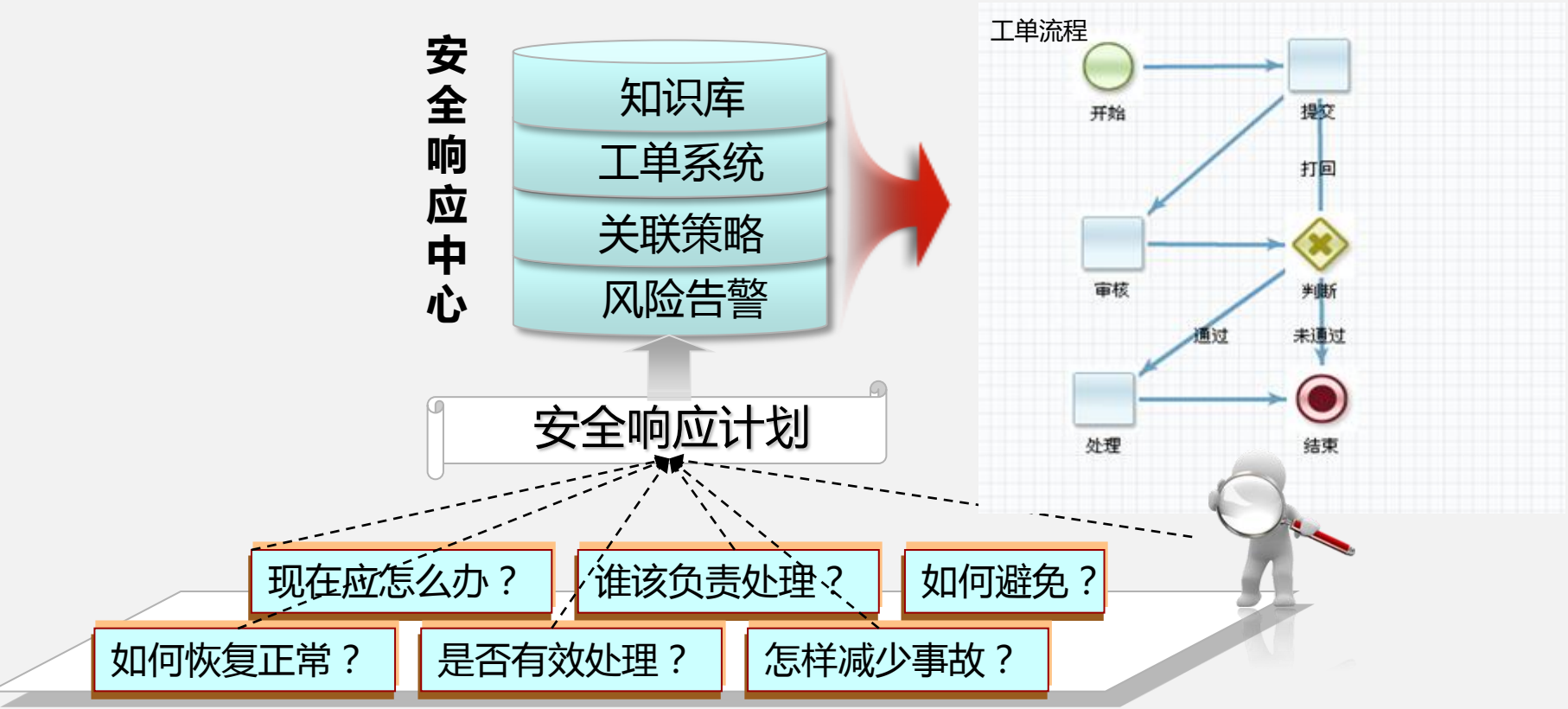
快速响应


安全响应中心
知识库
工单系统
关联策略
风险告警
E-Mail
短信
第三方网管
安全响应计划
现在应怎么办？
谁该负责处理？
如何避免？
如何恢复正常？
是否有效处理？
怎样减少事故？

快速响应


安全响应中心
知识库
工单系统
关联策略
风险告警
安全响应计划
回环关系
事件阀值
关联条件（事件）
关联事件源
关联缓冲值
And
回环关联时间为一小时
10分钟内告警事件数量超过上周平均基线50%以上
or
边界防火墙drop事件
边界防火墙accept事件
内网防火墙drop事件
内网防火墙accept事件
To any
华赛USG防火墙
Checkpoint防火墙
Juniper防火墙
Cisco防火墙
天融信防火墙
From the same
目标端口
10分钟内告警事件数量超过上周平均基线50%以上
or
边界路由流量事件
核心交换三层流量事件
To any
华为路由交换
Cisco路由交换
Juniper路由交换
H3C路由交换
其他。。。。。
From the same
目标端口
现在应怎么办？
谁该负责处理？
如何避免？
如何恢复正常？
是否有效处理？
怎样减少事故？

快速响应


安全响应中心
知识库
工单系统
关联策略
风险告警
安全响应计划
工单流程
开始
提交
打回
审核
判断
通过
未通过
处理
结束
现在应怎么办？
谁该负责处理？
如何避免？
如何恢复正常？
是否有效处理？
怎样减少事故？

快速响应

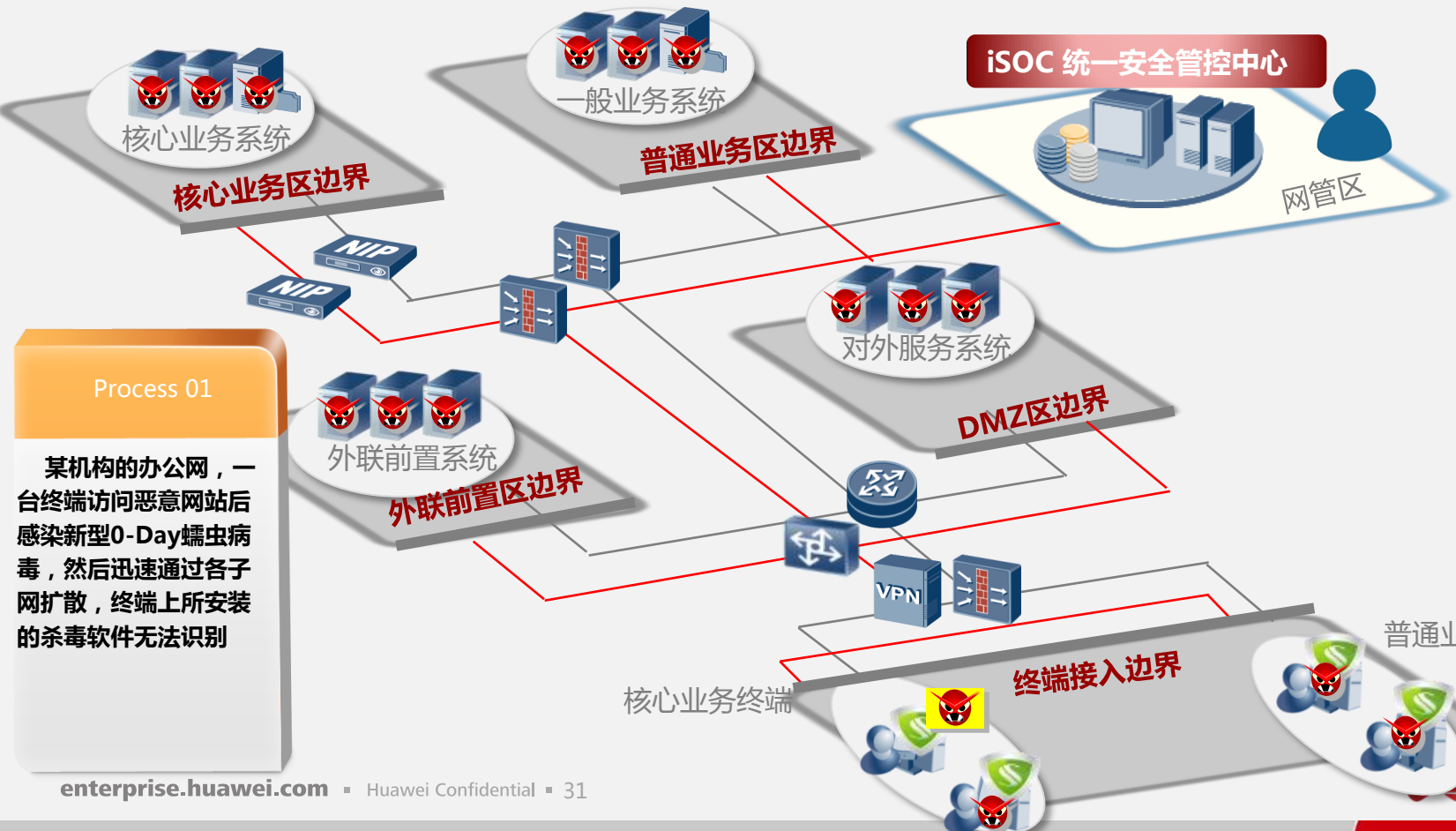
安全响应中心

知识库
工单系统
关联策略
风险告警

安全响应计划

现在应怎么办？
谁该负责处理？
如何避免？
如何恢复正常？
是否有效处理？
怎样减少事故？

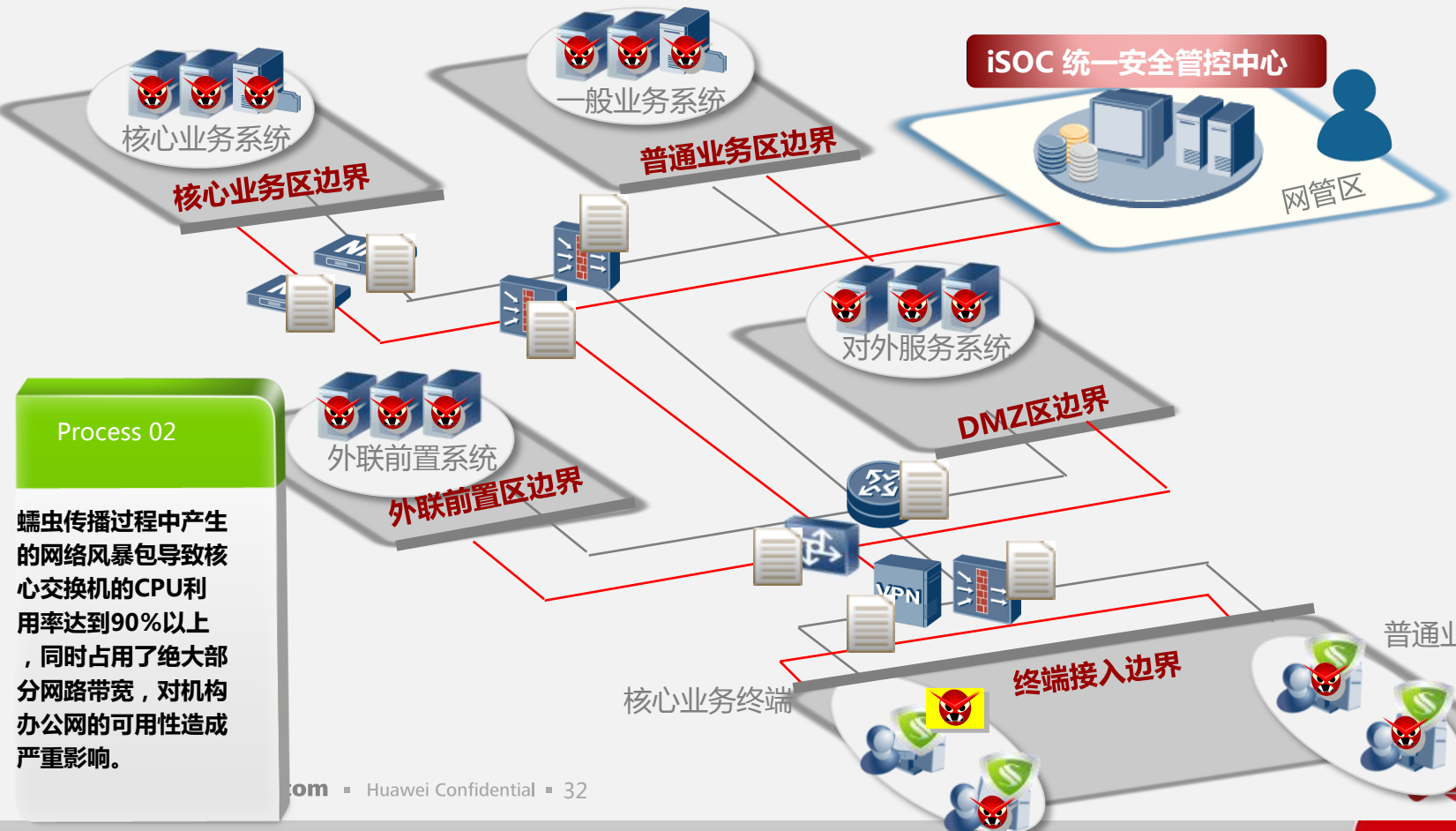
客户化安全场景一：蠕虫病毒爆发



Process 01

某机构的办公网，一台终端访问恶意网站后感染新型0-Day蠕虫病毒，然后迅速通过各子网扩散，终端上所安装的杀毒软件无法识别

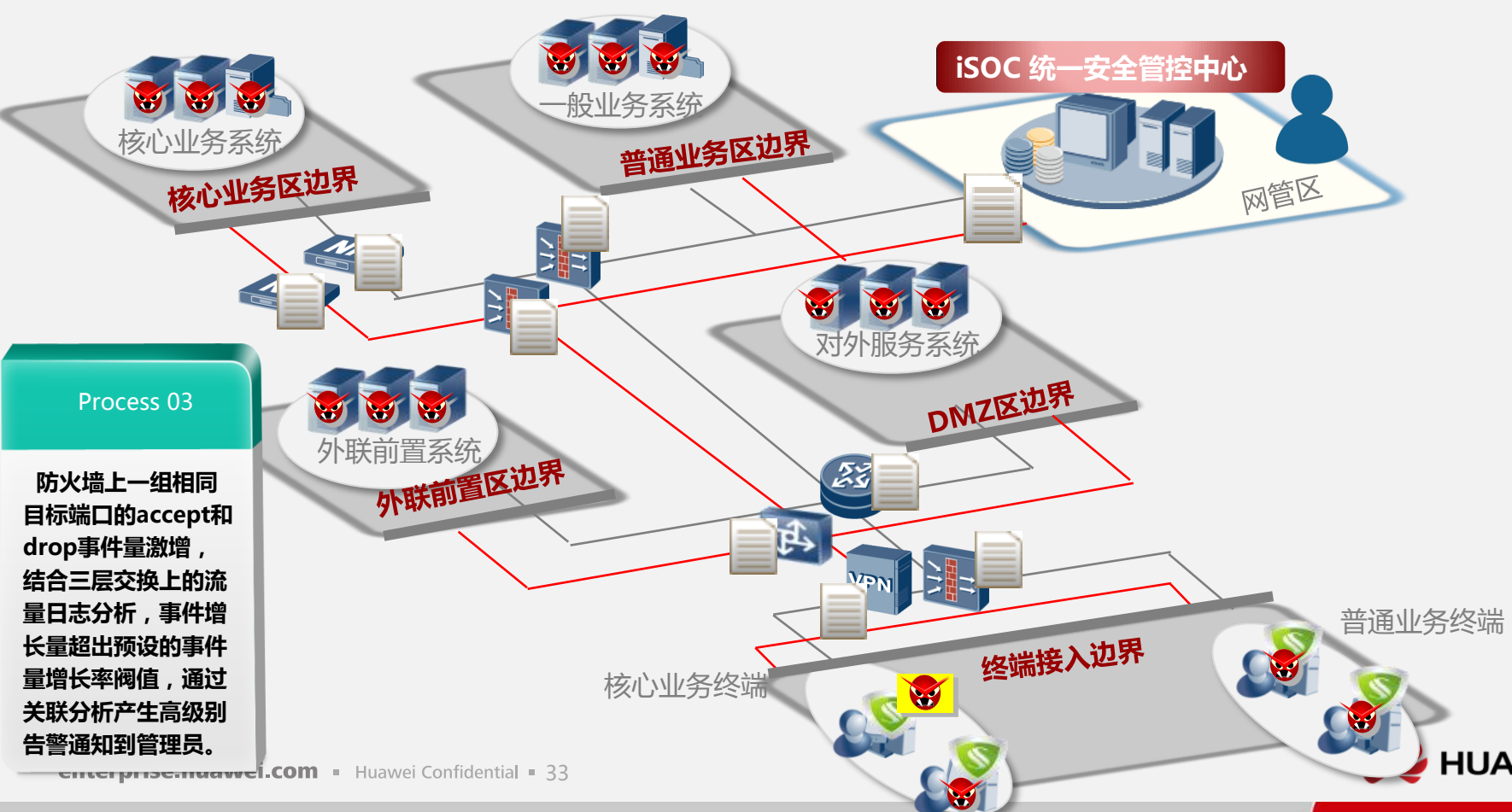
客户化安全场景一：蠕虫病毒爆发



Process 02

蠕虫传播过程中产生的网络风暴包导致核心交换机的CPU利用率达到90%以上，同时占用了绝大部分网路带宽，对机构办公网的可用性造成严重影响。

客户化安全场景一：蠕虫病毒爆发

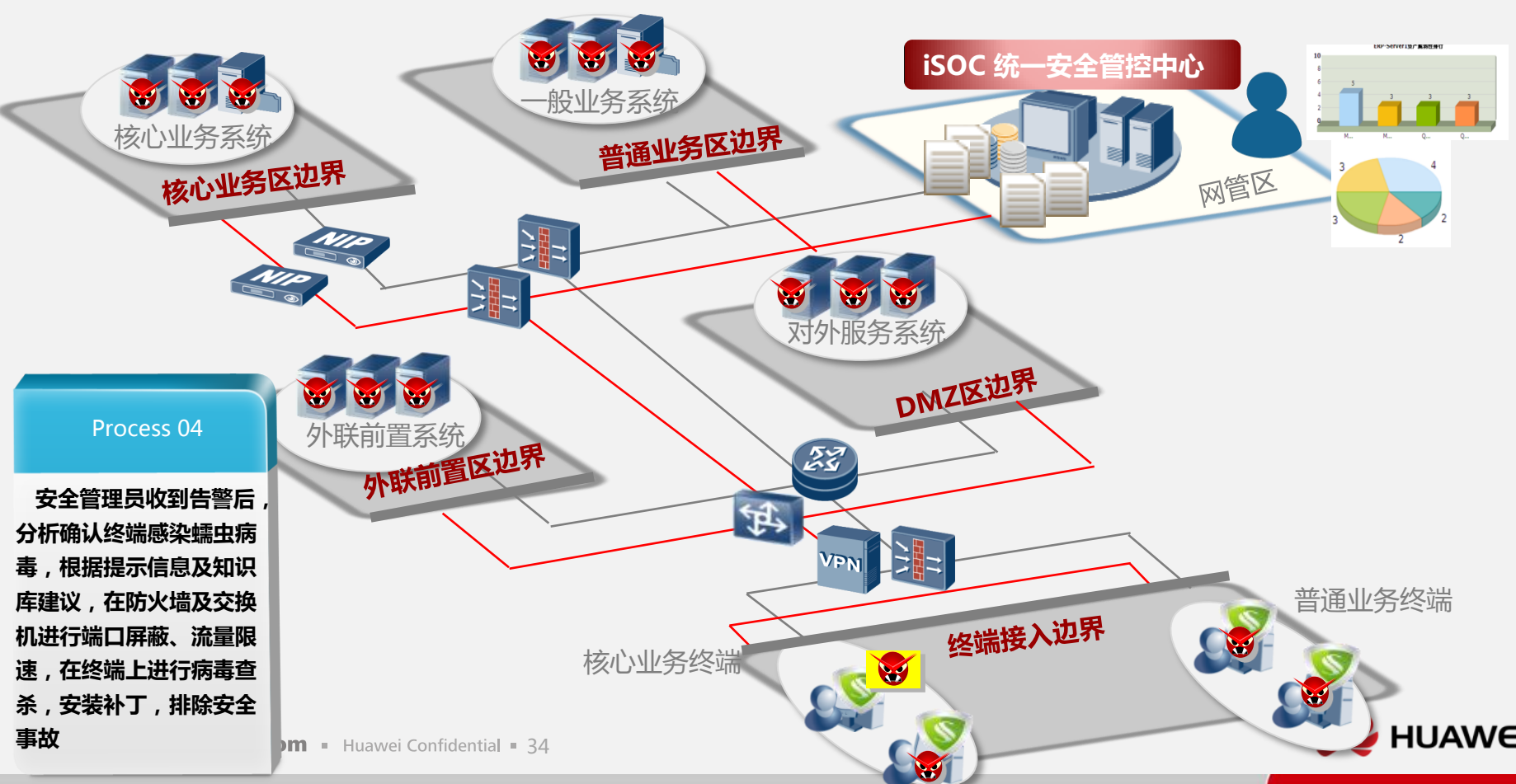


Process 03

防火墙上一组相同目标端口的accept和drop事件量激增，结合三层交换上的流量日志分析，事件增长量超出预设的事件量增长率阀值，通过关联分析产生高级别告警通知到管理员。

HUAWEI

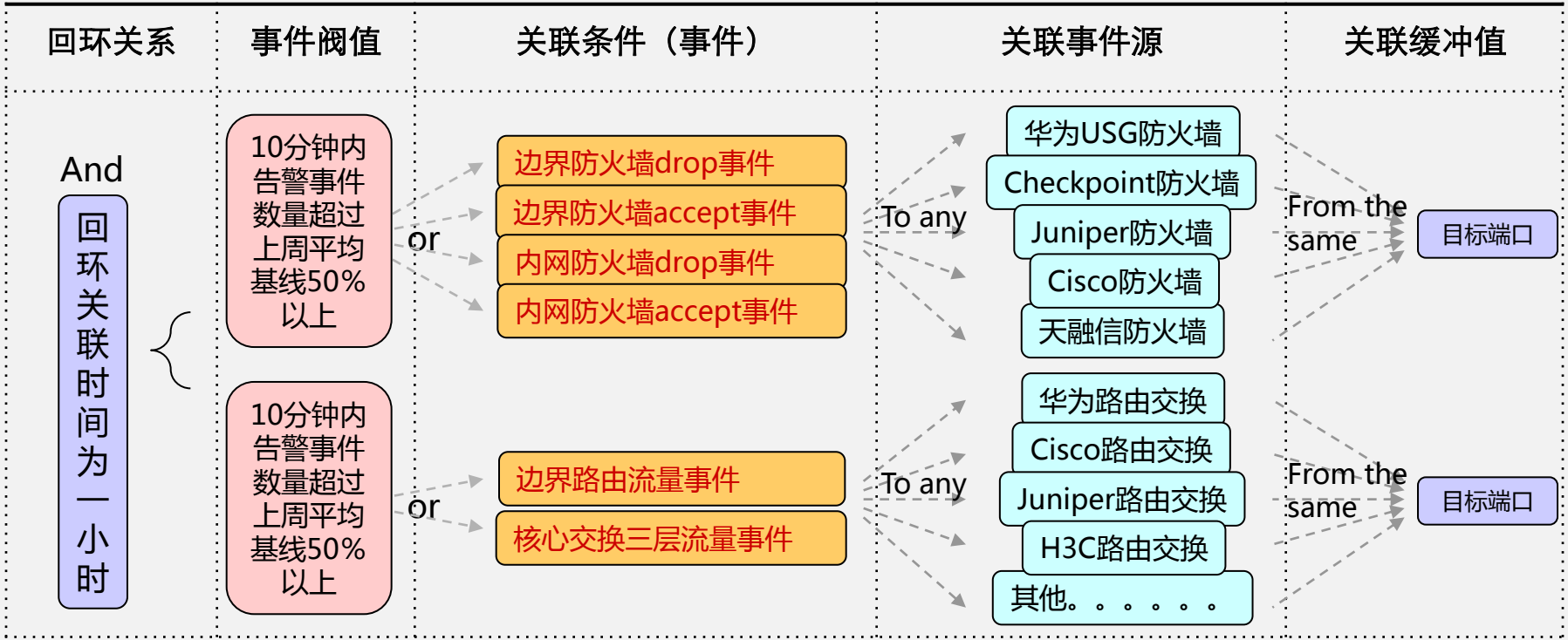
客户化安全场景一：蠕虫病毒爆发



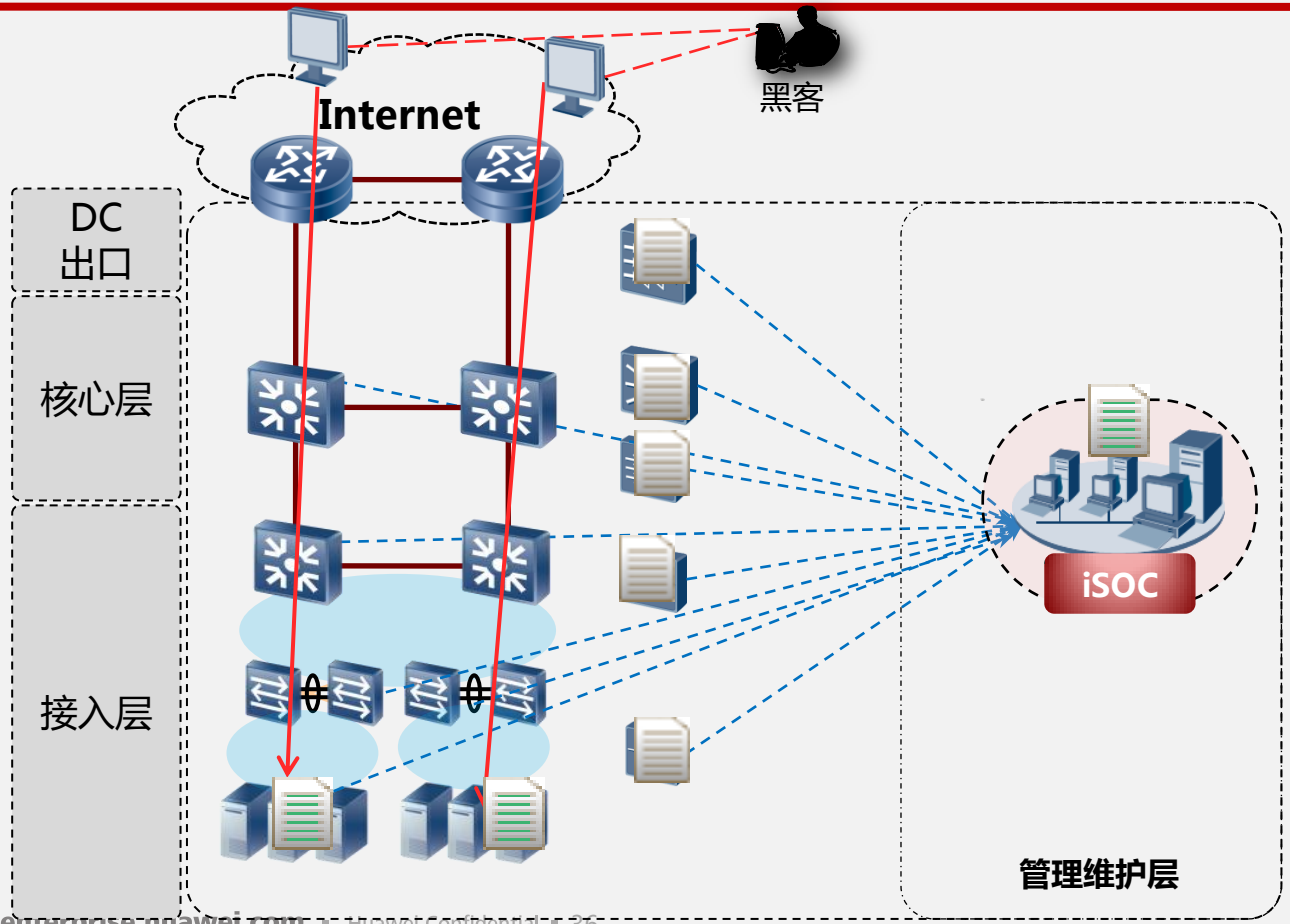
Process 04

安全管理员收到告警后，分析确认终端感染蠕虫病毒，根据提示信息及知识库建议，在防火墙及交换机进行端口屏蔽、流量限速，在终端上进行病毒查杀，安装补丁，排除安全事故

逻辑分析：蠕虫爆发预警关联规则



客户化安全场景二：DDoS攻击

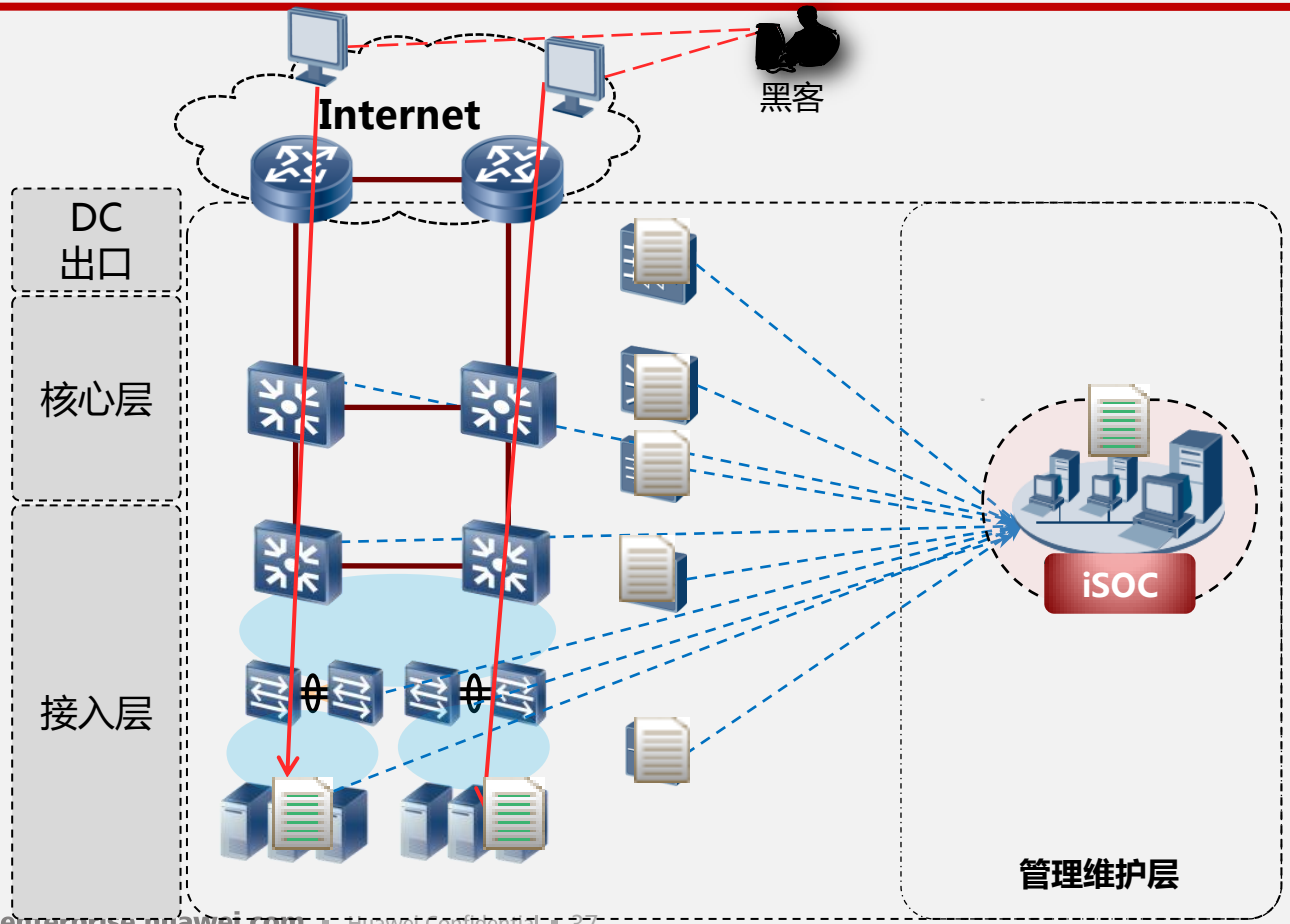


<场景说明>

黑客通过控制肉机，对关键服务器进行拒绝服务DoS攻击，导致正常访问请求被拒绝，业务访问中断。

HUAWEI

客户化安全场景二：DDoS攻击

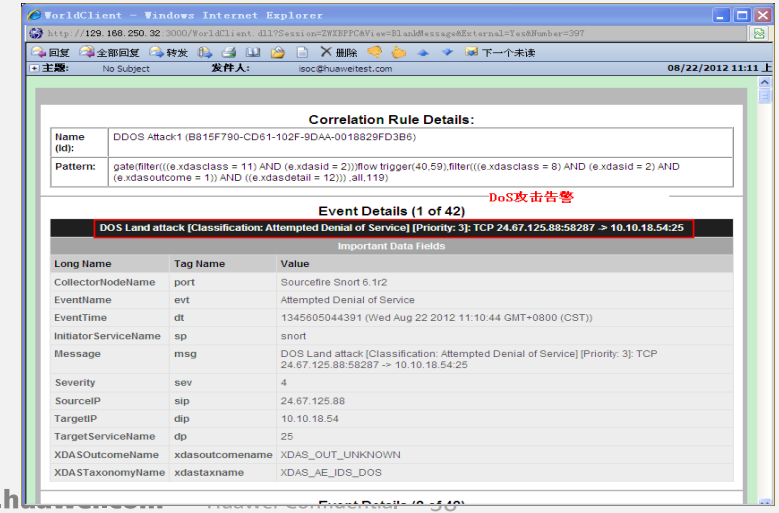


<侦测过程>

【1】边界设备FW/IDS检测到大量DoS事件
【2】边界设备SW、路由器资源利用率明显升高
【3】 被攻击对象资源利用率明显升高，正常的访问请求发生错误
【4】iSOC根据各类日志，进行关联分析。

HUAWEI

客户化安全场景二：DDoS攻击

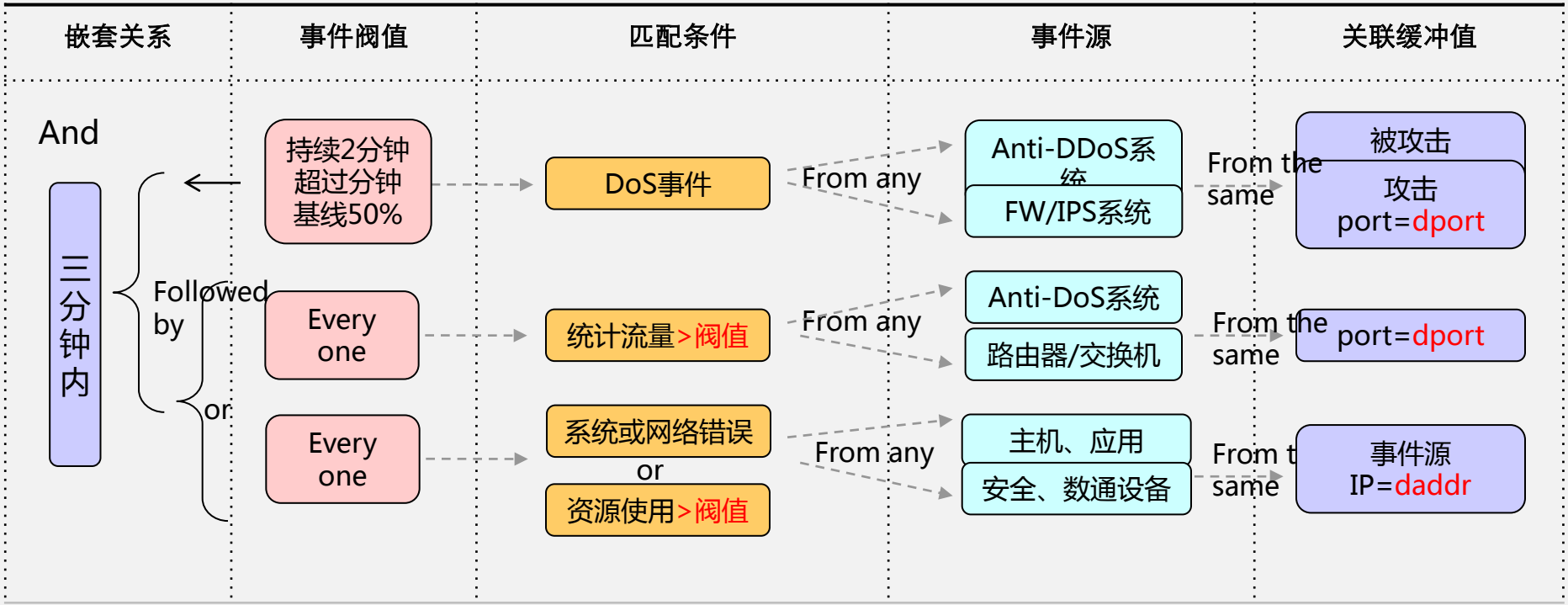


<溯源检查>

【1】管理员收到DDoS告警短信和邮件通知。
【2】进入关联分析引擎，查看事件详情
【3】查看触发器，追踪事件源头，找到攻击源。
【4】管理员在防火墙上制定ACL策略，限制攻击源访问关键服务器。

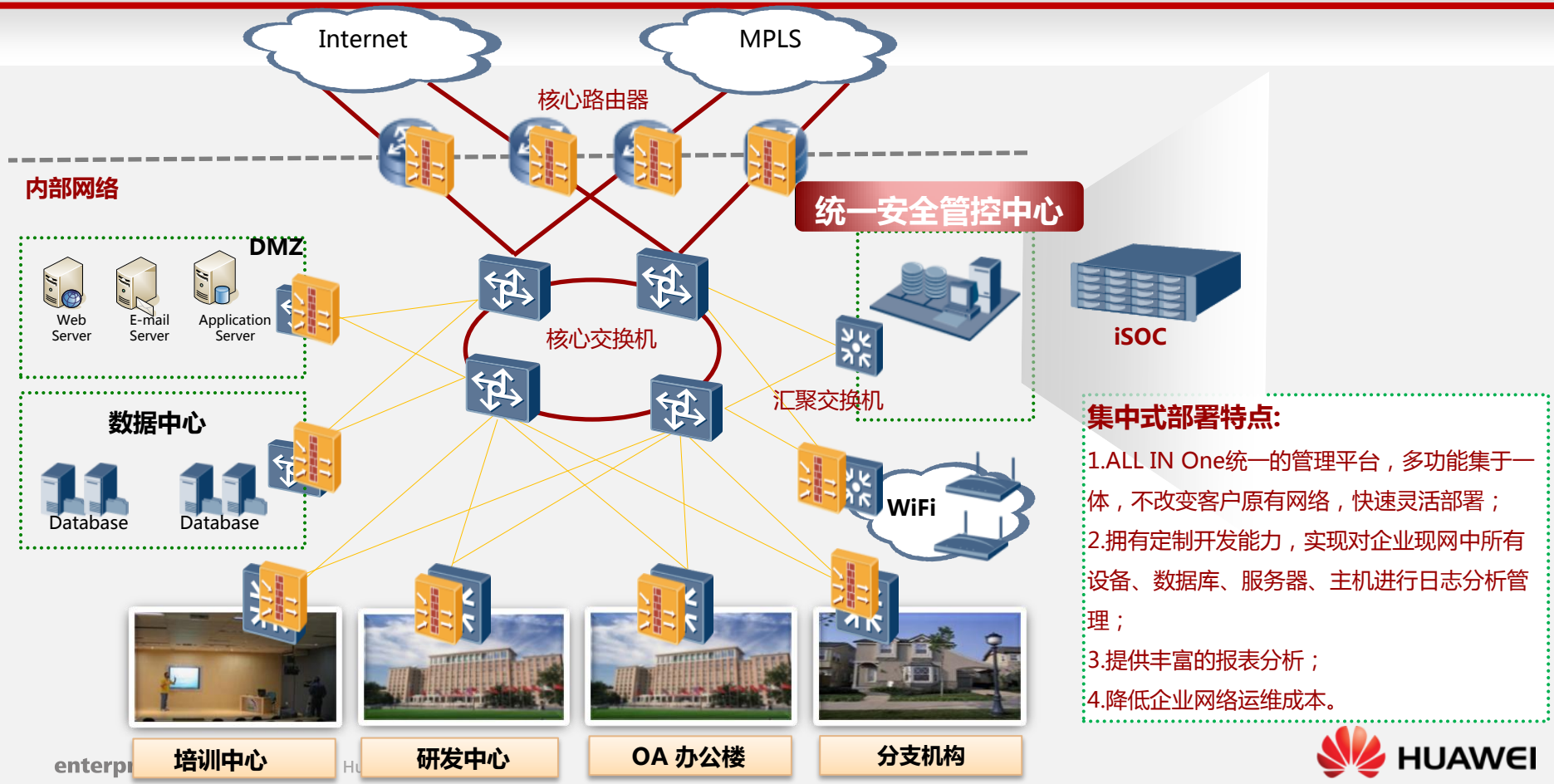
HUAWEI

逻辑分析： DDoS攻击预警关联规则



HUAWEI

iSOC典型组网：集中式部署



集中式部署特点:

1.ALL IN One统一的管理平台，多功能集于一体，不改变客户原有网络，快速灵活部署；

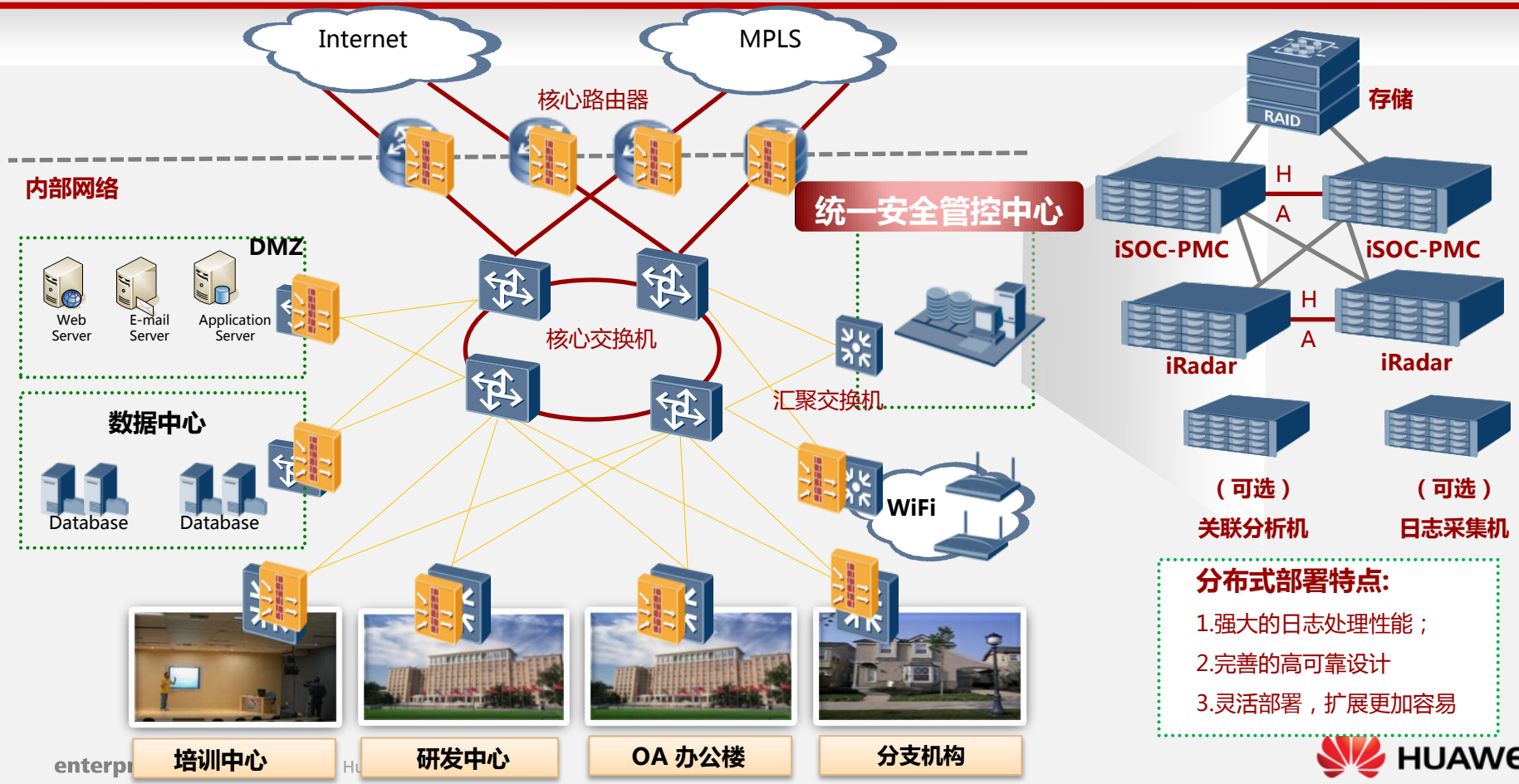
2.拥有定制开发能力，实现对企业现网中所有设备、数据库、服务器、主机进行日志分析管理；

3.提供丰富的报表分析；

4.降低企业网络运维成本。

HUAWEI

iSOC典型组网：分布式部署



分布式部署特点:

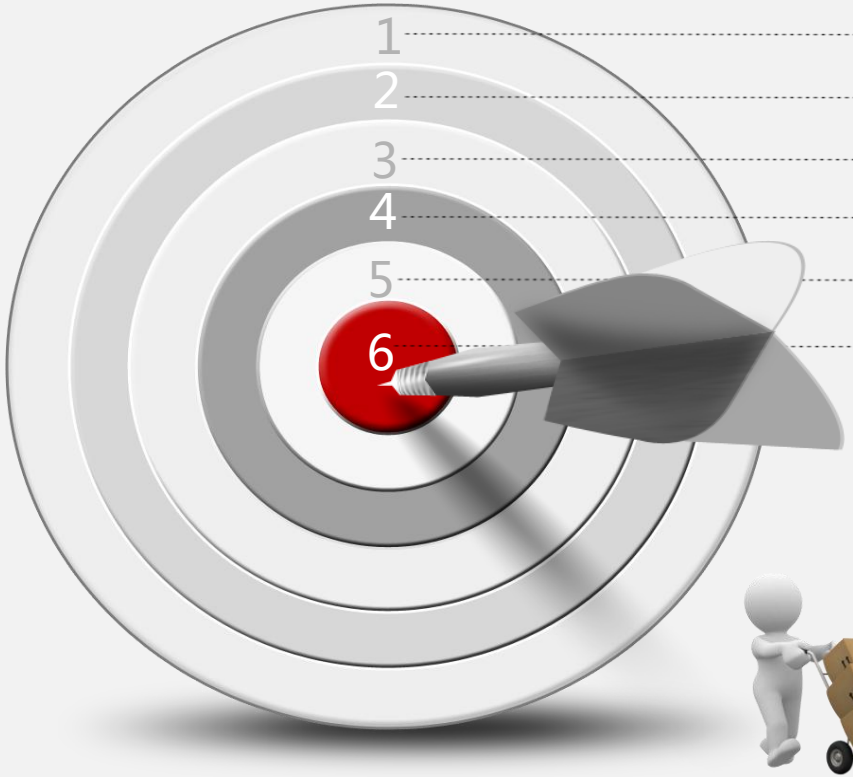
1.强大的日志处理性能；

2.完善的高可靠设计

3.灵活部署，扩展更加容易

HUAWEI

iSOC客户价值总结



1. 全面完备的设备日志管理，避免重复投资
2. 超强的智能关联分析引擎，帮助客户快速定位安全异常
3. 海量日志存储和快速查询能力，实现快速追踪和取证
4. 完备的报表和监控告警功能，主动提供决策数据
5. 灵活的组网部署方式，满足客户多样性网络需求
6. 电信级高可靠性，一次部署高枕无忧

高效

智慧

全面

HUAWEI

Content

国家超级计算深圳中心案例

- **客户挑战：**

  深圳国家超级计算机中心是国内领先的云计算平台和云服务模式的典范。其作为面向社会的公共服务平台，体现国家和地方创新资源的互动融合，为公共信息、企业创新、产业发展、科学普及服务，在对外提供服务的同时，也面临诸多安全挑战，如非授权访问、误操作、滥操作、第三方运维人员的管理等，同时等保合规性也明确要求对核心设备的访问需要监控和审计。

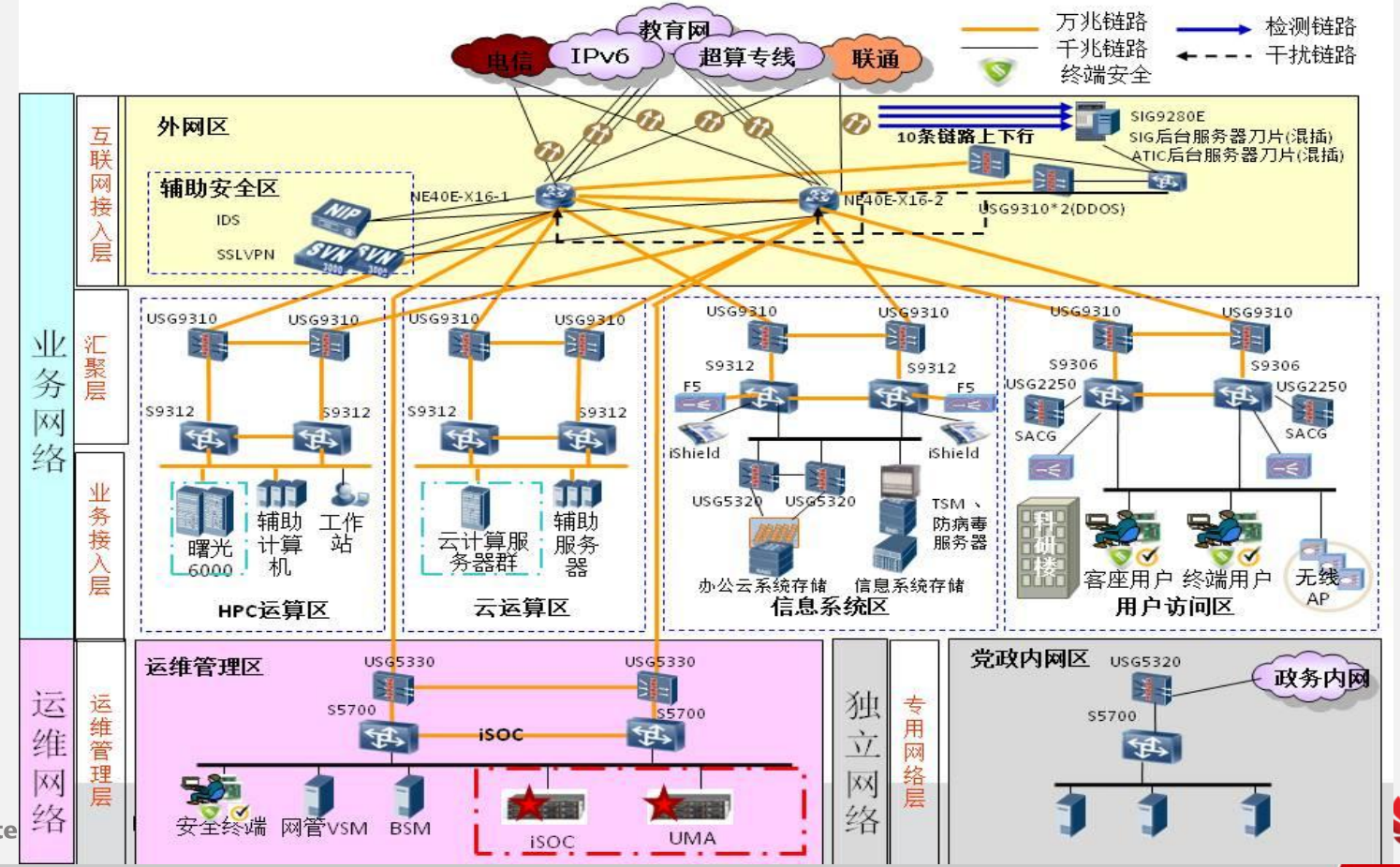
- **解决方案：**

  华为针对超算中心的运维业务特点，部署一套iSOC统一安全管控中心，对全网设备动态监控；同时部署统一运维审计系统UMA，对内部运维人员的操作进行集中的管理和控制，建立起自动化、流程化的安全运维体系。

- **客户获得的利益：**

  建立起统一运维接入平台，实现超算中心安全运维的统一身份认证、统一授权和统一审计管理，规范运维操作，提高运维管理水平，同时满足合规性的需求。

解决方案拓扑



HUAWEI

闸北卫生局区域医疗安全管理项目

- **客户挑战：**

上海市闸北区卫生局及下属各医院、医疗机构，无法监管内部运维人员和医疗人员对核心业务系统如HIS系统的维护和使用，他们能够轻易从数据库系统导出病人信息、药单数据等保密信息，而无法追踪到操作人员和搜集到证据。造成的影响：一方面这些数据被非法卖到药商那里，成为不法分子获利的工具，给医院的正常运营管理造成影响，另一方面核心数据的外泄，给医患关系紧张埋下隐患。

- **解决方案：**

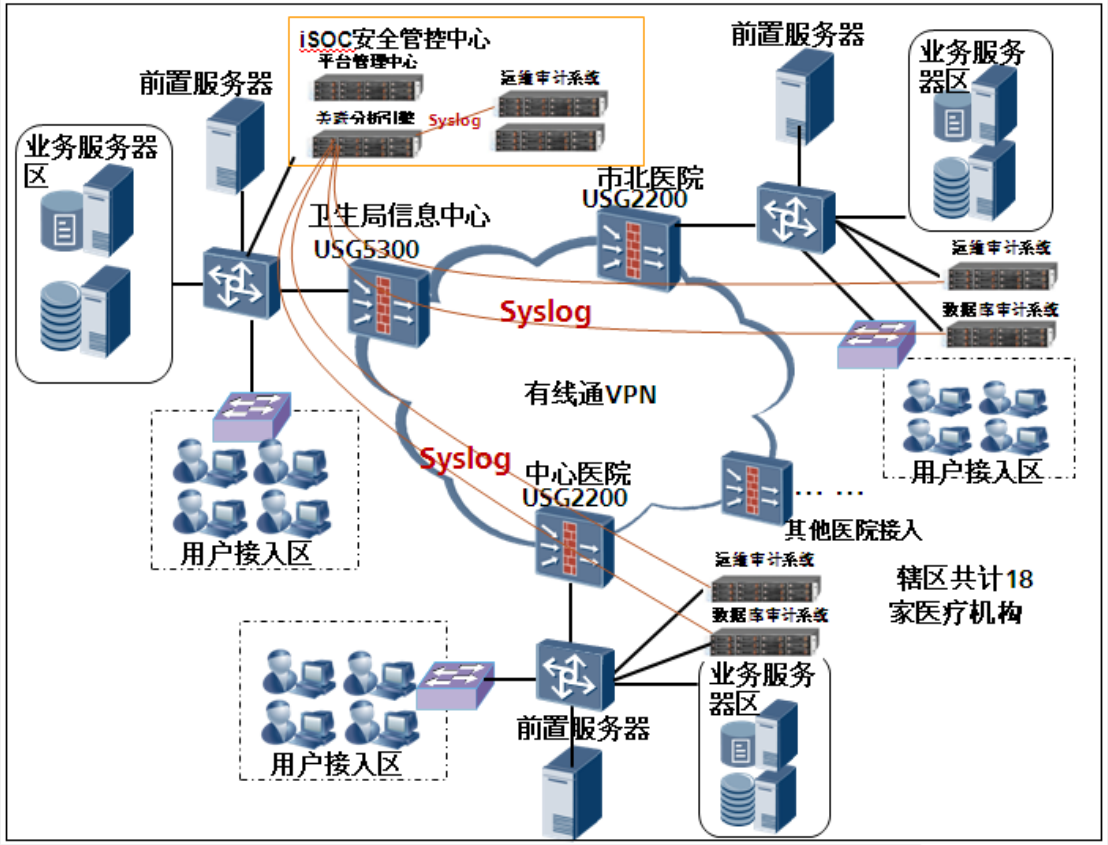
在市卫生局云数据中心部署一套iSOC统一安全管控中心，实现对卫生局和辖区医院业务系统的事件关联分析；对市卫生局和下属机构的IT设备和业务系统的日志进行集中采集、分类存储和关联分析，从海量安全事件中产生精确告警、定位安全问题。

定制客户化模板，对多次数据库的存取日志进行分析，提取可疑日志及时上报告警信息，在源头预防潜在的非法行为。做到事前告警、事中监控、事后审计和跟踪。

- **客户获得的利益：**

提高系统运维管理水平，满足相关标准要求，降低运维风 险，实现了医院业务操作的规范化管理，有效的解决了医院核心业务数据外泄问题。

解决方案拓扑



HUAWEI

首都高速案例

- **客户挑战：**

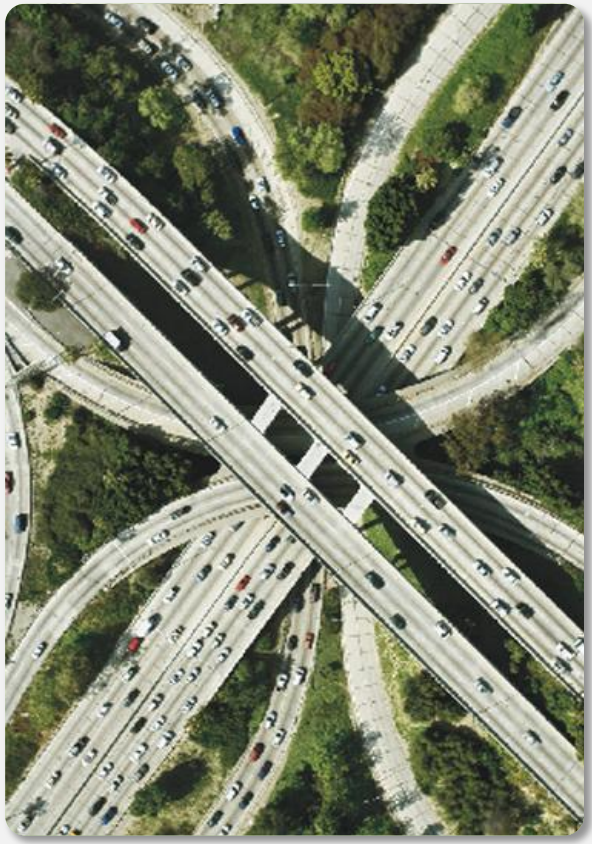
  首都高速网络规模比较庞大，在核心网络支撑下并行连接8套重要的业务应用子网，各子网之间主要通过VLAN方式进行隔离，但没有采取严格的访问控制措施，仅有部分相对比较重要的子网和关键部位部署了防火墙和IDS设备，以及防病毒软件，总体上缺乏全面的安全隔离和有效的安全防护体系，据等级保护三级要求仍存在较大差距。

- **解决方案：**

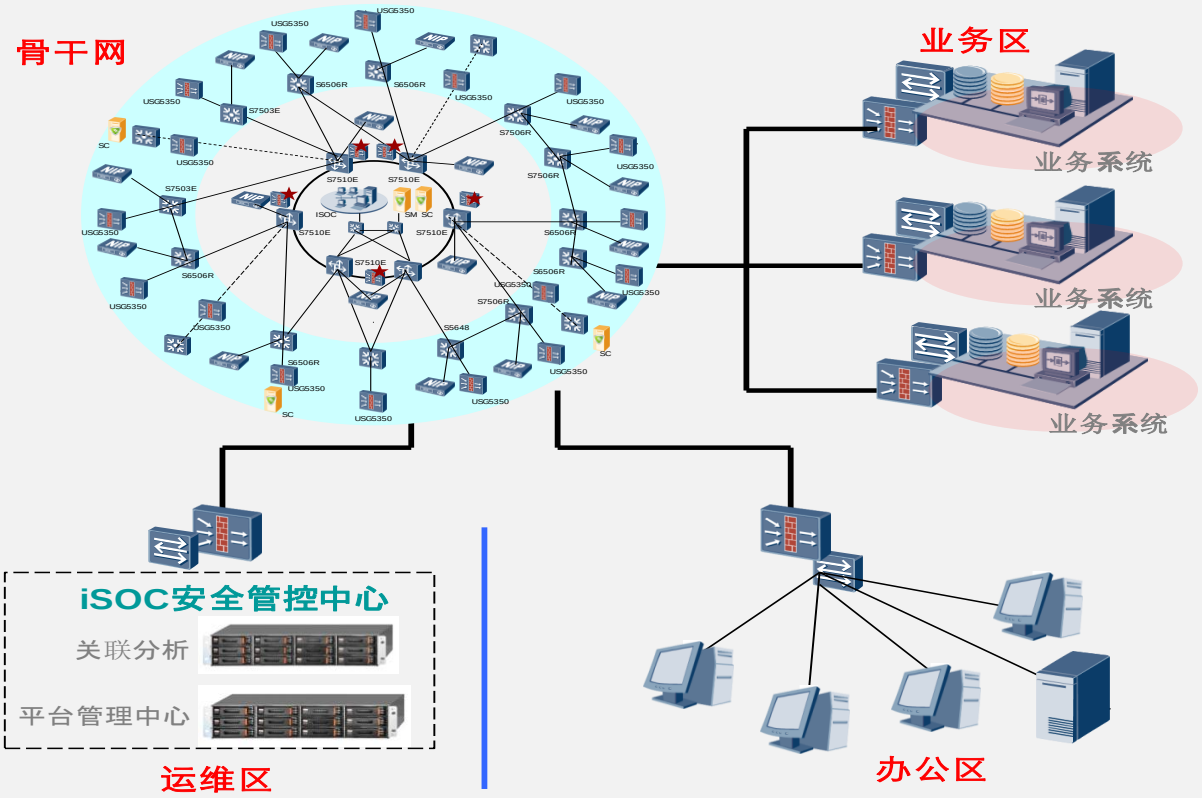
  针对首都高速的特点，在数据中心部署一套iSOC，对网元进行全面监控，端到端跟踪风险和漏洞，建立了统一防控体系。

- **客户获得的利益：**

  通过iSOC的部署，客户能实时监测通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等，并通过关联规则分析后发出报警；通过iSOC定制报表功能，根据自身的需求选择不同的字段、不同的报告模板进行智能分析，生成等保审计报表，方便查看和审计；利用iSOC内置漏洞扫描工具，可定期对网络系统进行漏洞扫描，做到了漏洞风险的可视化管理。



解决方案拓扑



福建省联通安全管理项目

- **客户挑战：**

  1、信息安全法规要求日志永久保存；2、计费中心大部分设备的运维外包，存在较大安全隐患；3、网络故障及安全异常，不能及时发现；出现故障或异常后需要很长时间来分析和排查，且对运维人员技能要求较高。

- **解决方案：**

  通过iSOC集中采集网络、主机、数据库、安全设备的日志，进行分类存储和关联分析，从海量安全事件中产生精确告警、定位安全问题，提升安全运维管理效率，并满足相关安全合规的要求。

- **客户获得的利益：**

  1、设备日志被长期保存、不可篡改，满足ISO、ITIL、等保等法规对日志管理的法规要求，同时通过运维日志的事后审计对日常运维操作起到了很好的监控和规范作用。

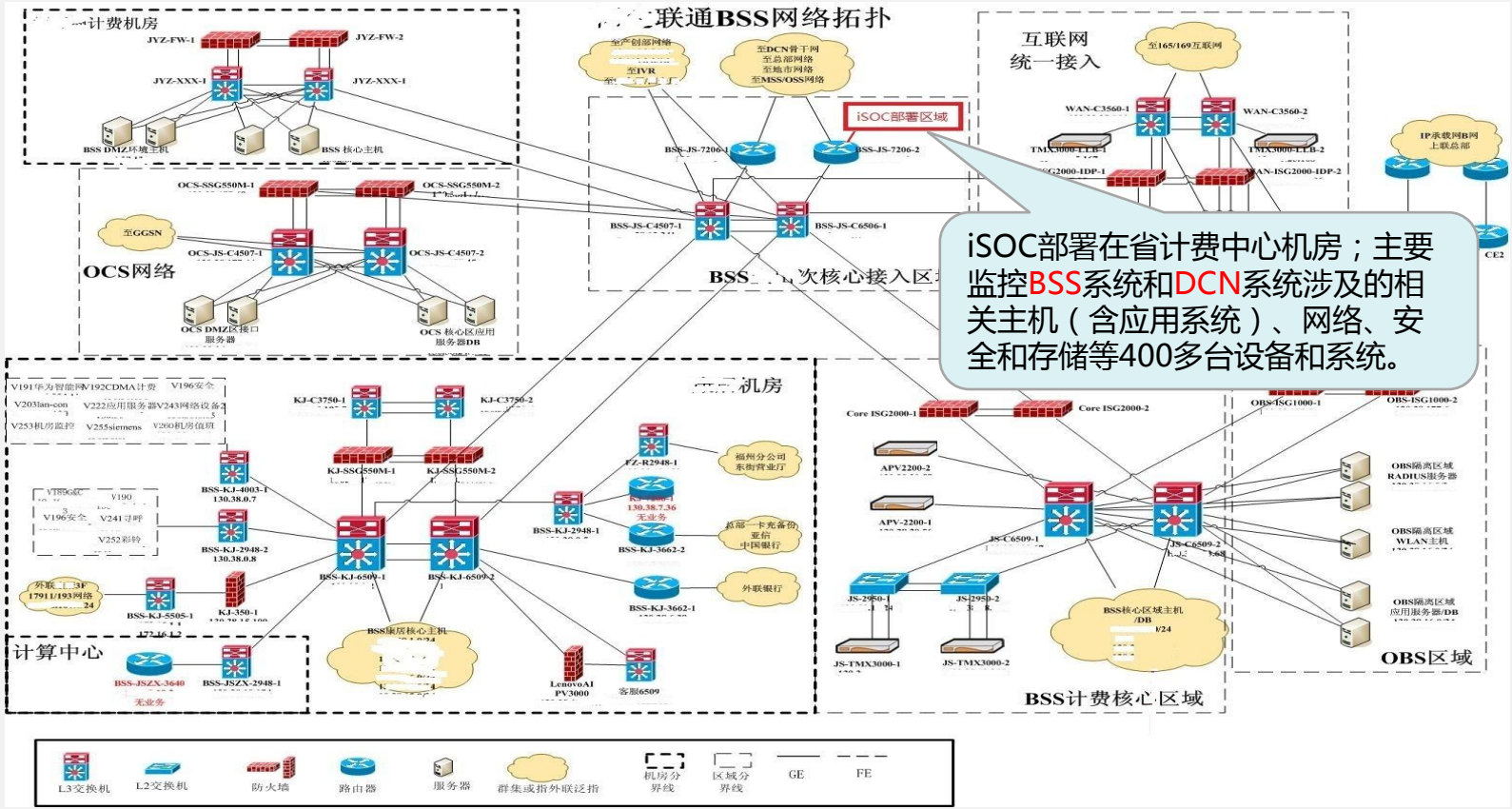
  2、监控设备和应用的性能、故障和运维操作等可用性信息，准确定位安全故障，协助分析故障原因。

  3、对恶意攻击、数据窃取、网络欺诈等信息安全异常事件进行检测和分析，并及时预警，或阻断。

  4、监控和统计业务和网络数据，分析网络安全现状和趋势，为未来IT建设策略的决 策提供参考依据。

HUAWEI

解决方案拓扑



iSOC部署在省计费中心机房；主要监控BSS系统和DCN系统涉及的相关主机（含应用系统）、网络、安全和存储等400多台设备和系统。

Hutchison 3G UK（英国和记3G）安全管理优化项目

- **客户挑战：**

  H3G拥有大量的外包人员，如何降低运维成本，提升运维效率是亟待解决的问题。同时，英文法律规定运营商网络必须满足PCI DSS相关合规要求，

- **解决方案：**

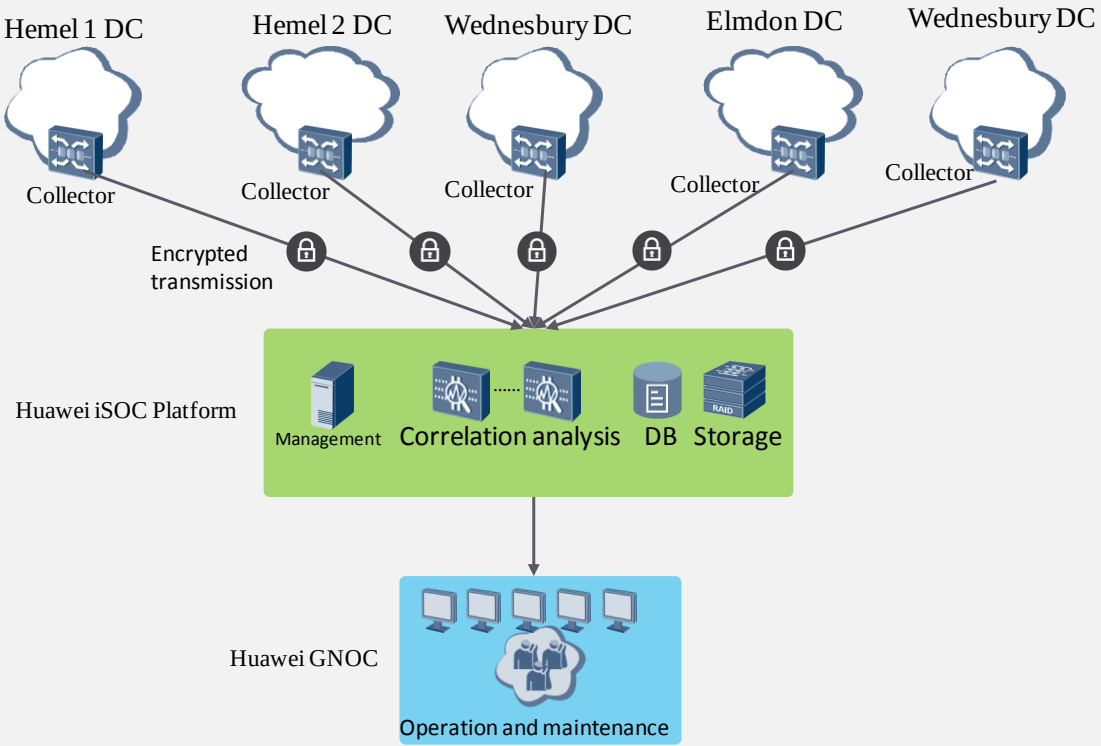
  围绕iSOC建立一套安全运维管理平台SMP（operational security management platform），提供3到5级专业服务，针对PCI DSS提供顾问服务，帮助客户满足合规要求。

- **客户获得的利益：**

  提供了完备的安全管理平台，降低了安全响应时间，减少了TCO，强化了业务过程的安全管理，同时满足法律规定的PCI DSS规范要求。

HUAWEI

解决方案拓扑



HUAWEI ENTERPRISE A BETTER WAY