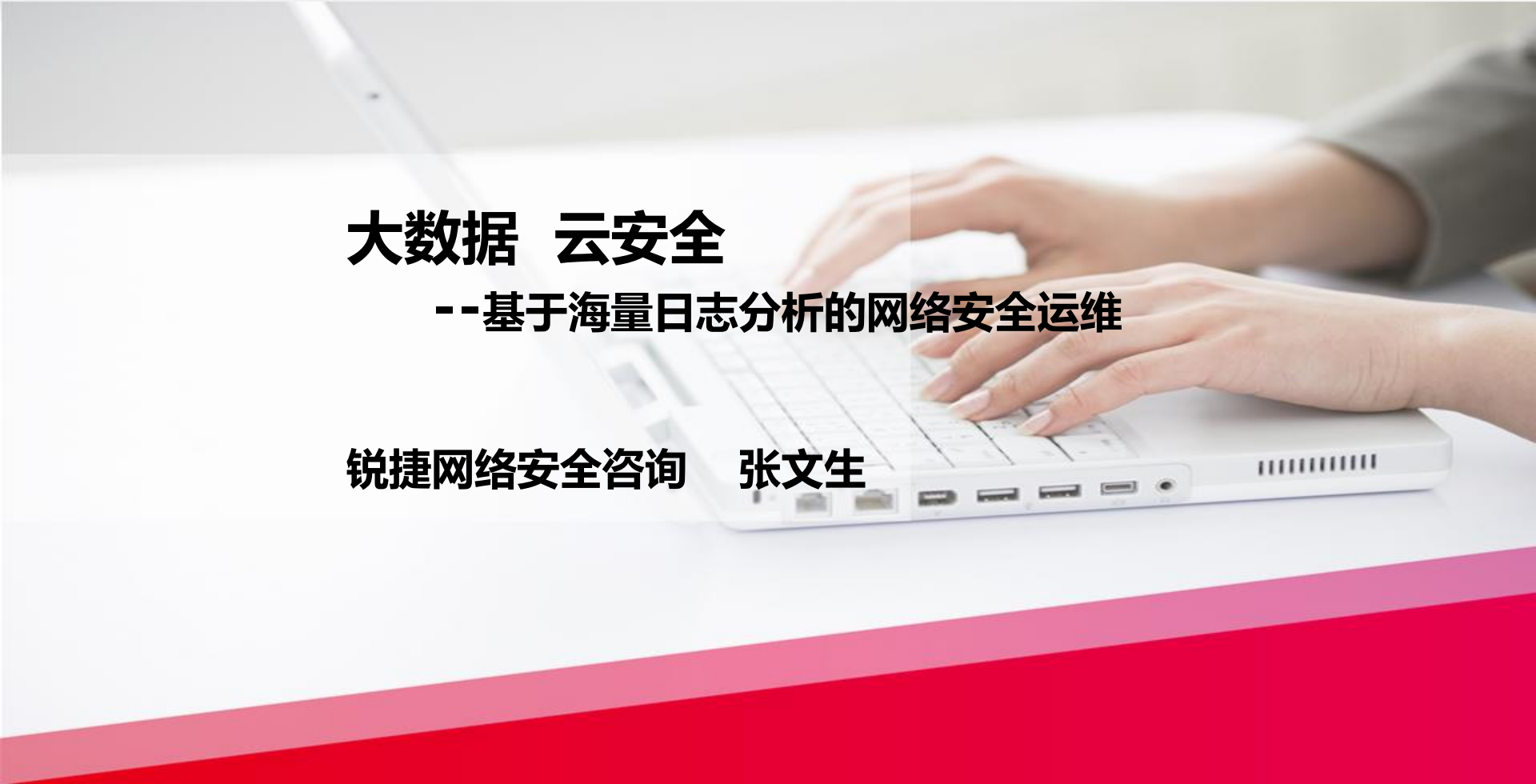


大数据 云安全

--基于海量日志分析的网络安全运维

锐捷网络安全咨询 张文生

数据中心的发展

计算中心

- 大型机
- 数据计算和存储

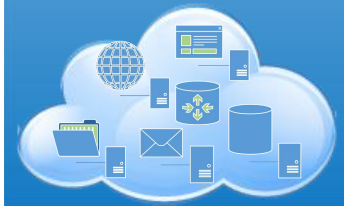
传统数据中心

- 机架式服务器
- 面向C/S架构

虚拟化数据中心

- 虚拟化集群
- 灵活高可用

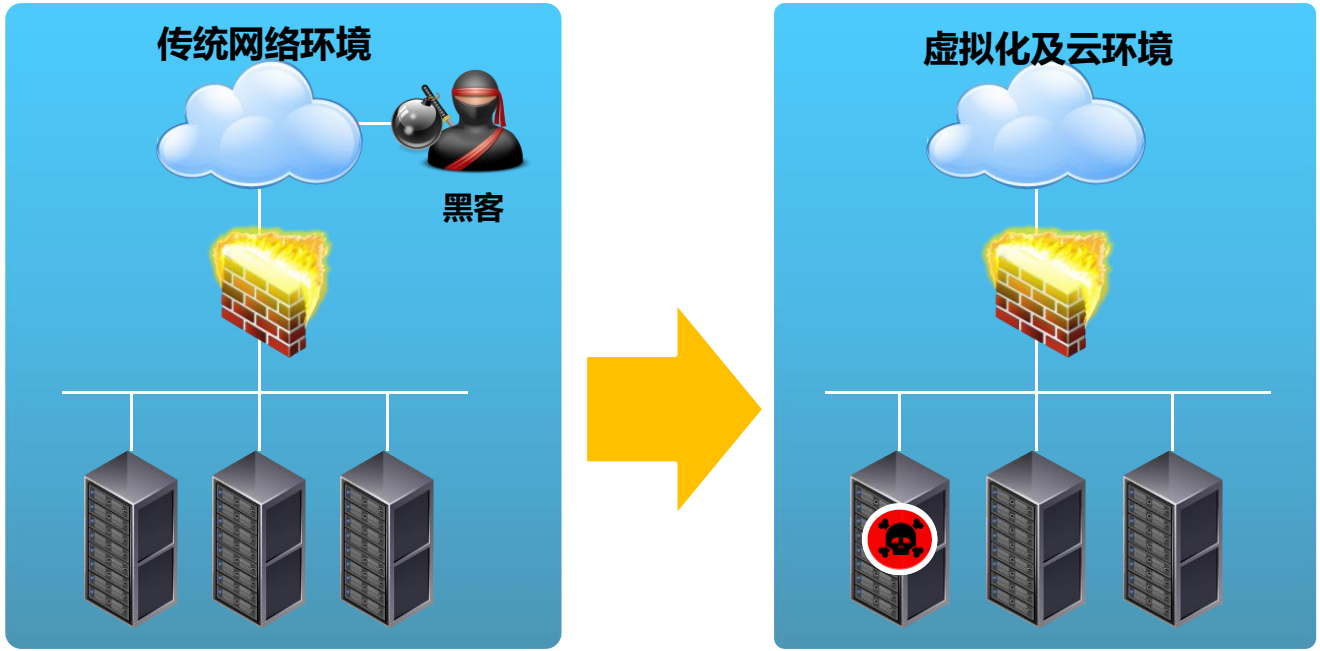
云数据中心



- 软件定义
- 面向服务

70年代　90年代　2000年　2010至今

安全问题的演进



南北向安全威胁

东西向安全威胁

政务云建设模式及面临的问题

私有云

私有云

私有云为用户单独使用而构建，其特点是资源专有。

主要安全问题在与如何对东西向通信进行安全防护

公有云

公有云

公有云为第三方提供商向用户提供的云服务，用户并不拥有计算资源

云服务提供商关注的是如何为每个用户提供其专有的安全防护机制

混合云

混合云

混合云融合了公有云和私有云，是当前云计算的主要模式及发展方向

除公有云和私有云的问题，混合云还面临着公有云、私有云之间的传输安全问题

云模式带来的安全问题

- 虚拟化导致物理边界模糊化，传统的网络边界防护措施失效。传统的以物理服务器为单元划分安全域的防护手段已不适用
- 虚拟化基础架构与管理端的安全性成为集中风险点
- 虚机系统数量爆炸式增长，虚拟化失控会带来安全盲区
- 虚拟安全域的隔离和防护成了云数据中心的核心问题之一
- 在虚拟化环境中，虚拟机成为网元的最小单元，而对于传统的硬件防火墙，以及基于行为特征分析的IDS/IPS等网络安全设备，根本无法感知到同一物理机上各VM 之间通信流量

如何对云进行安全防护

如何整体安全设计：

东西流量通过云虚拟化FW

南北流量经过数据中心物理防御设备

公有云与私有云间安全传输

如何控制东西流量：

主机0信任（每主机防护）

多租户安全隔离（部门防护）

如何管理虚拟FW：

云平台集中管理和下发策略

可自由定义每个虚拟机的哪些流量经过虚拟FW

虚拟防火墙

云虚拟防火墙配合常用的安全设备，对整网安全进行整体防护

案例分析

中X院

ARP系统是对全院人力、资金、科研基础条件等资源配置及相关管理流程进行整合与优化形成统一平台，这个系统构建在整个云中心系统上，外链几十个ARP子业务系统，全国隶属于中X院的单位均会访问；由于业务系统比较重要，用户对这个系统进行了比较全面的安全防范；

本次通过安全分析设备，接入虚拟机以及安全设备，并制定了漏扫计划，经过15天收集到3478万条日志信息，经过安全分析设备分析后发现2个疑似安全攻击：

1、接收到同源同目的利用BASH漏洞的XSS跨站攻击，共计5047次，通过漏扫日志发现目的服务器有BASH漏洞，黑客进行攻击可执行网站挂马，窃取企业数据等，且是成功的

2、检测到7213次针对XX院的SQL注入，由于XX院邮箱登陆页面在主页面，所以黑客可通过注入数据库进行拖库的行为，窃取科研人员的帐号数据信息；

案例分析

某政府机构

有10多个业务系统提供给下属100多家单位访问，安全防范难度大，**因此采购了大量安全设备，去年依然出现了2类安全攻击的高频入侵，存在数据泄露的严重风险，并且自己并不知情。**

部署安全设备 ≠ 安全

部署安全单位47%依然被入侵，81%第三方先发现

政务云建设的安全困惑

不论安全设备在不在那里，安全风险都在那里

- 不知道网络上的安全现在发生什么？
- 不知道网络上的安全即将发生什么？
- 不知道目前系统的安全性如何？脆弱性在哪？

安全建设面临最大的痛是什么？

——有安全的壳，没安全的魂，“看不到”安全

“看见” 安全是我们针对性地进行解决和规避安全风险的前提

所有的攻击行为都会留下痕迹或变化，利用数据分析挖掘我们能“看见”安全攻击

“日志” 是最高优先级首先要被利用的有价值数据

通过日志“看见”安全的两大核心障碍

海量日志

巨大的时间人力成本

整网信息化设备日志为千万级条目/天

技术门槛

较高的安全技术能力

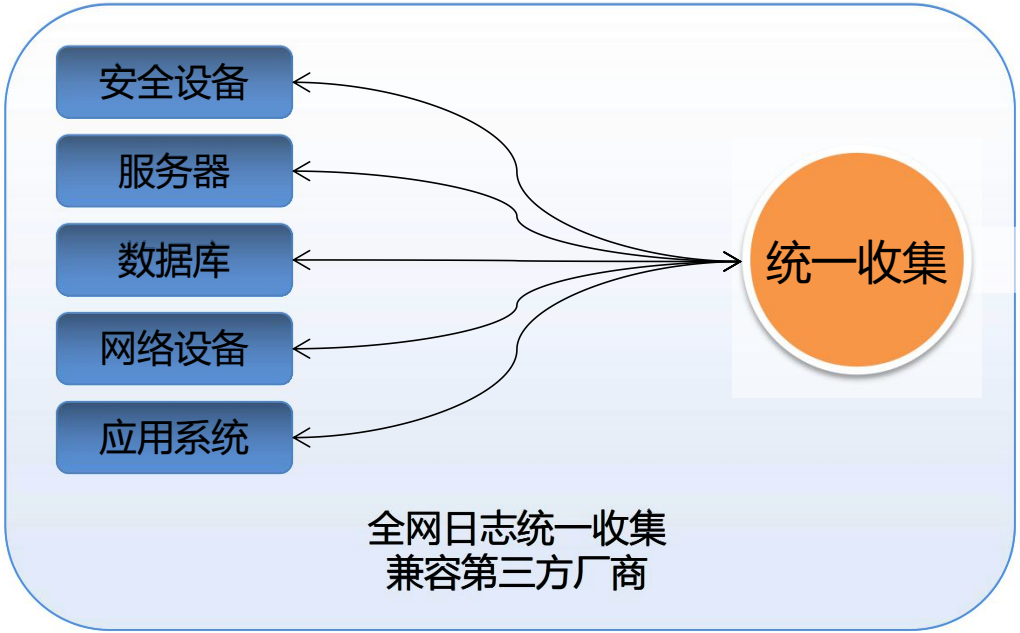
多种设备综合分析才能准确定位攻击

《中华人民共和国网络安全法》强化“看见”安全

- 日志留存：“出口日志60天” 变为“整网日志6个月”
- 安全防护：强调风险评估、风险监测、风险预测

RG-BDS大数据安全平台

锐捷大数据安全平台解决之道——快速构建数据仓库

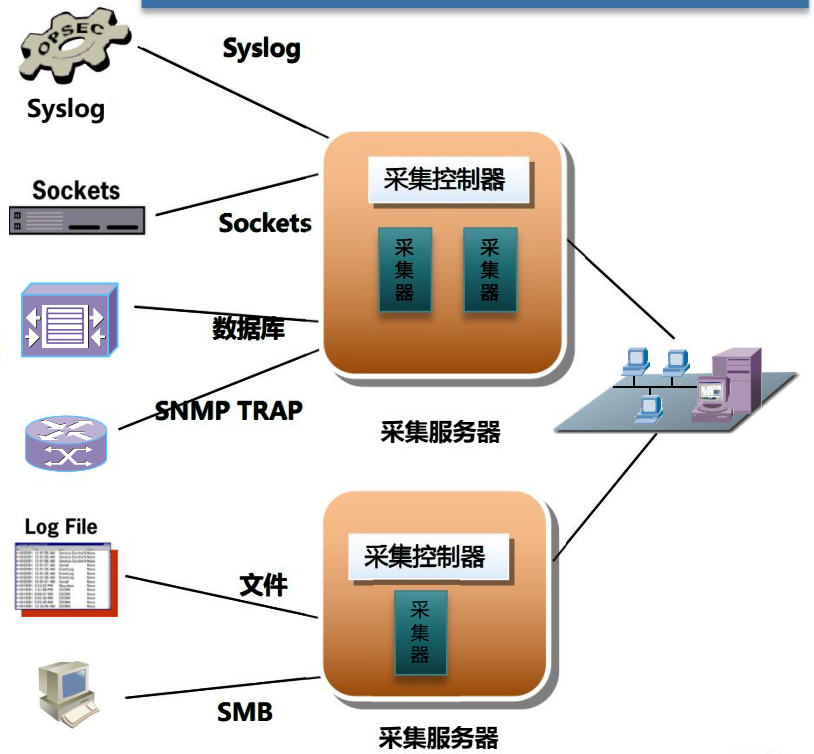


- **STEP 1 统一收集并标准化海量数据，构建安全大数据仓库**

锐捷大数据安全平台解决之道——快速构建数据仓库
——日志接入方式

支持各类主流的设备

支持多种日志采集方式：Syslog、SNMP trap、数据库、本地文件、控制台标准输出、TCP Socket等



采集控制器可分布部署、多级部署

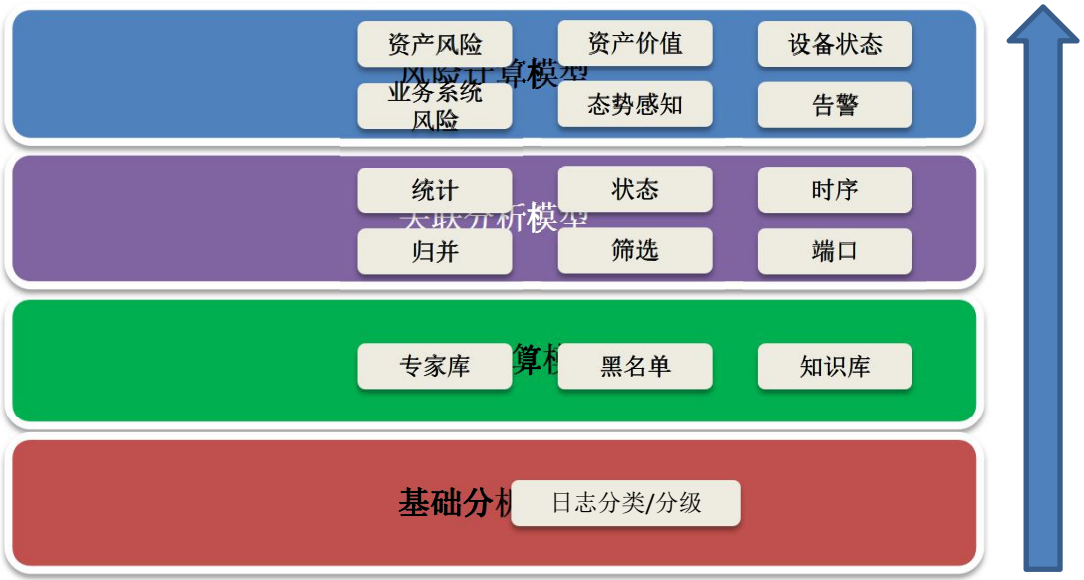
锐捷大数据安全平台解决之道——大数据分析精准定位核心风险

海量原始事件

准确定位关键风险

- STEP 2 结合日志、资产、漏洞进行大数据关联分析，直击要害问题

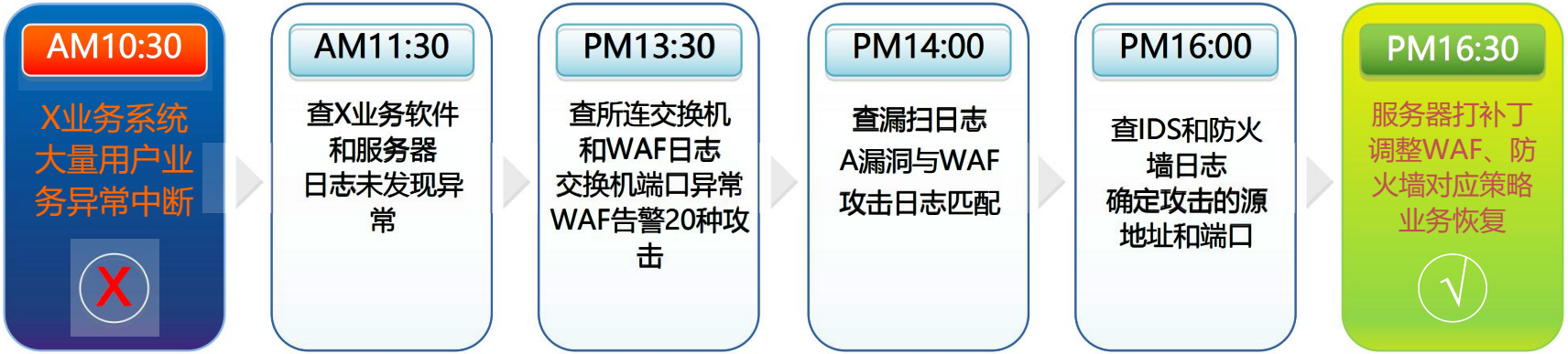
锐捷大数据安全平台解决之道——大数据分析精准定位核心风险
——四层分析模型



锐捷大数据安全平台解决之道——大数据分析精准定位核心风险
——基于关联的分析

状态	每条日志都是一个状态，基于一个或多个状态的情况来做分析，比如登陆失败这个状态短时间内大量发生它就可能是密码猜测，如果再出现登陆成功可能就是入侵成功，这就是两个状态的关联。
时序	按照时间先后顺序来做分析，比如先登陆成功后又新建了一个用户，这种情况可能存在很大的风险。
归并	将相同字段的日志进行次数叠加，比如root用户登陆，一天可能有上千次，只产生一条告警，后面显示次数。
筛选	基于字段进行匹配选择，比如用“删除用户”这个字段进行筛选，出现包含这个字段的事件就会进行告警。
端口	基于端口进行选择，出现这个端口的日志都会进行告警，比如一台服务器只开了80端口，可以设置成这台服务器只有80端口的日志才进行告警。
活动列表	将系统的某种状态或者属性记录下来和系统进行关联，出现利用该系统的这种状态或属性的攻击，就会触发告警。比如说系统有struct2漏洞没有处理，将这种状态保存在活动列表中，以后只要发生利用这种漏洞的攻击都会产生告警。

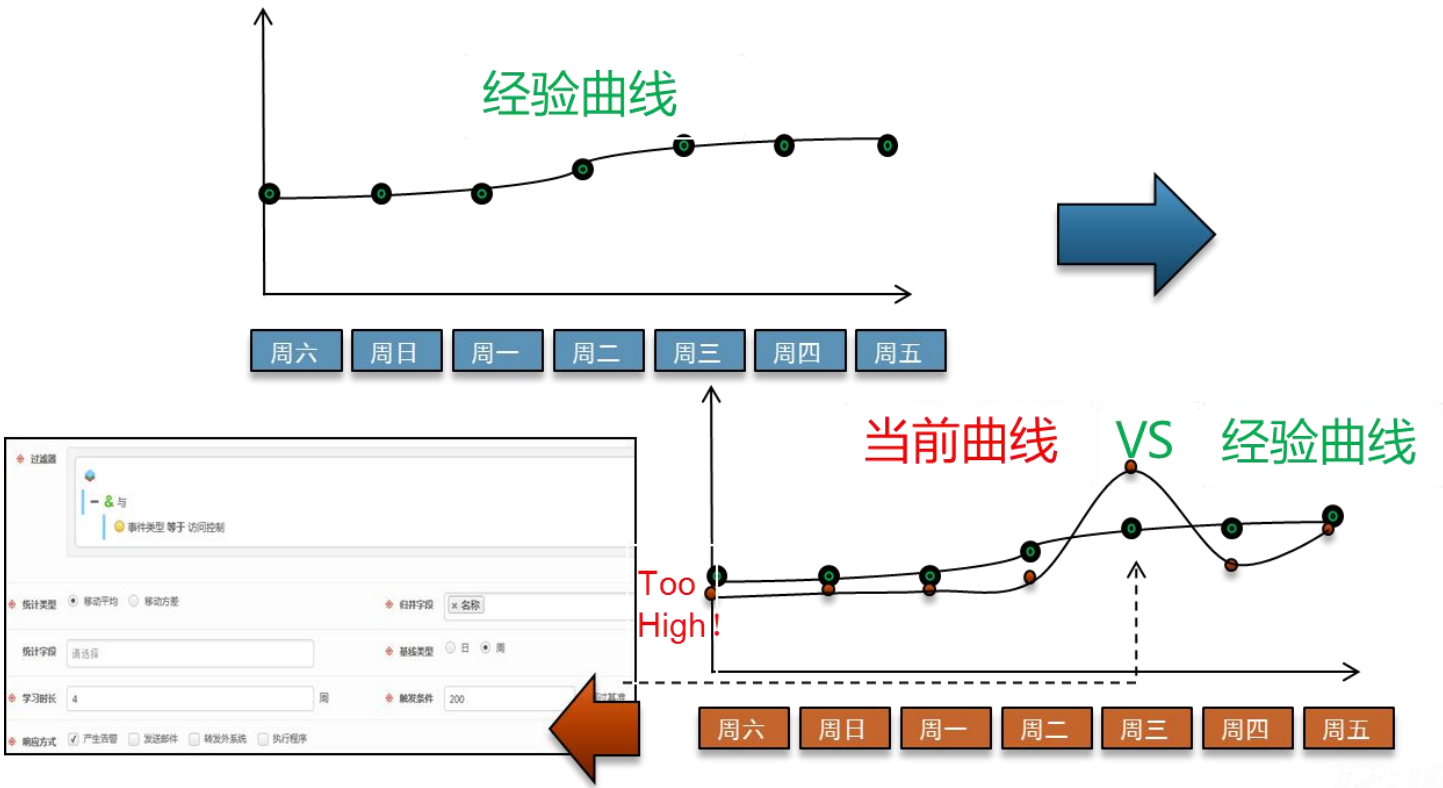
举一个关联分析的例子


AM10:30
X业务系统大量用户业务异常中断
X
AM11:30
查X业务软件和服务器日志未发现异常
PM13:30
查所连交换机和WAF日志
交换机端口异常
WAF告警20种攻击
PM14:00
查漏扫日志
A漏洞与WAF攻击日志匹配
PM16:00
查IDS和防火墙日志
确定攻击的源地址和端口
PM16:30
服务器打补丁
调整WAF、防火墙对应策略
业务恢复
√

举一个关联分析的例子


IDS告警日志
针对X漏洞的攻击
目标包含A的网段
主机漏扫数据
扫描出A主机
发现X漏洞
交换机日志
A主机连接交换机
端口流量异常
业务系统日志
A主机业务系
统访问异常
少量用户异常
中断链接
关联分析结论
高危告警
A主机的X漏
洞在被攻击
X

锐捷大数据安全平台解决之道——大数据分析精准定位核心风险
——经验曲线



云安全预警

针对KVM、XEN、VMware、Vmware、Citrix虚拟化平台及OpenStack、vCloud等云计算平台集成漏扫插件，提供针对云环境安全预警发现功能

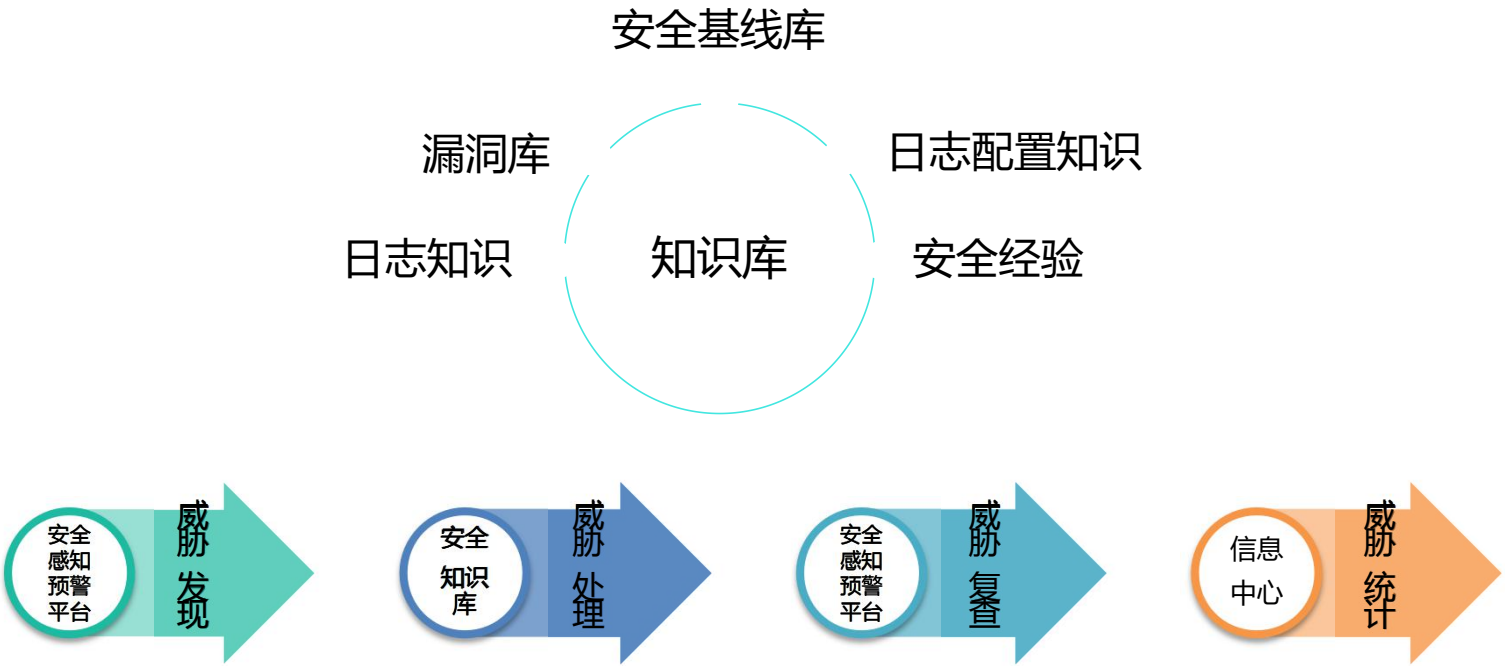
序号	插件名称	插件编号	插件族
1	Puppet 安全绕过漏洞|Puppet 远程代码执行漏…	1.3.6.1.4.1.25623.1.0.121012	Gentoo本地安全检查
2	OpenStack Ironic |		
3	OpenStack Objec		
4	OpenStack Dashb		
5	OpenStack Comp		
6	OpenStack Comp		
7	OpenStack Dashb		
8	OpenStack Comp		
9	OpenStack Nova		
10	OpenStack Comp		

序号	插件名称	插件编号	插件族
1	Linux kernel KVM和Xen 资源管理错误漏洞	1.3.6.1.4.1.25623.1.0.105465	思杰虚拟化服务器本地安全检查
2	Linux kernel KVM和Xen 资源管理错误漏洞|Linux…	1.3.6.1.4.1.25623.1.0.105517	F5本地安全检查
3	Xen 信息泄露漏洞|X		
4	Linux Kernel ‘requ		
5	Linux kernel KVM实		
6	Linux Kernel KVM L		
7	Linux Kernel KVM 'k		
8	Linux kernel KVM和		
9	Linux kernel KVM和		
10	Linux kernel KVM和		

显示 10 条记录

序号	插件名称	插件编号	插件族
1	VMware产品目录遍历漏洞	1.3.6.1.4.1.25623.1.0.100502	远程文件访问
2	VMware ESX探测(SNMP)	1.3.6.1.4.1.25623.1.0.103417	产品探测
3	VMware ESX探测 (Web)	1.3.6.1.4.1.25623.1.0.103418	产品探测
4	MIT Kerberos 5设计权限提升漏洞|VMware ESXi…	1.3.6.1.4.1.25623.1.0.103450	虚拟机本地安全检查
5	VMware Server VI Web Access操作系统命令注…	1.3.6.1.4.1.25623.1.0.103456	虚拟机本地安全检查
6	VMware ESXi/ESX/View 拒绝服务漏洞|VMware…	1.3.6.1.4.1.25623.1.0.103457	虚拟机本地安全检查
7	Linux Kernel ‘CIFSFindNext’ 函数整数符号错…	1.3.6.1.4.1.25623.1.0.103458	虚拟机本地安全检查
8	VMware 多个产品本地权限提升漏洞	1.3.6.1.4.1.25623.1.0.103466	虚拟机本地安全检查
9	Libpng库1位隔行图形信息泄露漏洞|VMware US…	1.3.6.1.4.1.25623.1.0.103467	虚拟机本地安全检查
10	VMware ESXi/ESX ‘VMX’ 进程拒绝服务漏洞|…	1.3.6.1.4.1.25623.1.0.103481	虚拟机本地安全检查

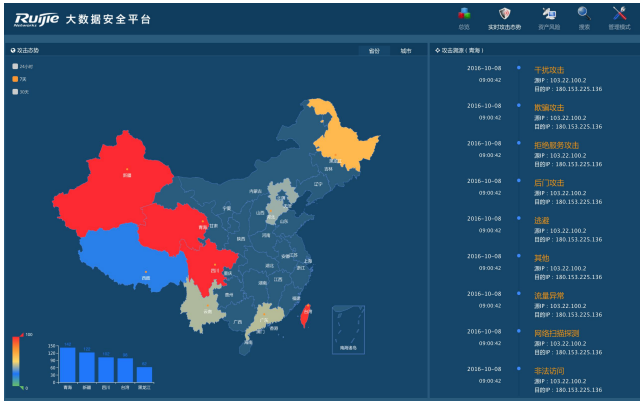
锐捷大数据安全平台解决之道——简单闭环安全问题



- **STEP 3 工单系统+知识库，闭环安全问题**

锐捷大数据安全平台解决之道——安全建设业绩直观体现

掌握整体安全态势
量化安全建设业绩



实时掌握攻击路径
简单做到攻击溯源

- **STEP 4** 量化呈现安全业绩，实时跟踪安全态势

总结——让安全设备物尽其用！

STEP 1　收集并标准化海量数据，构建安全大数据仓库

STEP 2　日志、资产、漏洞关联分析，直击要害问题

STEP 3　工单系统+知识库，闭环安全问题

STEP 4　量化呈现安全业绩，实时跟踪安全态势

THANKS

星网锐捷网络有限公司

地址：北京海淀区复兴路29号中意鹏奥大厦东塔A座11层　邮编：100036

Office Tel: 010-51715999　　Fax: 010-51413399

www.ruijie.com.cn