



SANGFOR
深信服科技



深信服智安全
SANGFOR SECURITY

深信服日志审计系统LAS

产品简介

深信服 智安全



SANGFOR
深信服科技



深信服智安全
SANGFOR SECURITY

目录

- 一. 需求背景与产品定位
- 二. 主要功能与产品优势
- 三. 应用场景与优势案例
- 四. 产品选型与操作演示



系统运维风险

日常操作导致系统的异常运行，服务中断。往往会事先在各类日志上有反映，如果缺乏有效的日志审计手段，就无法及时发现。

应用及数据风险

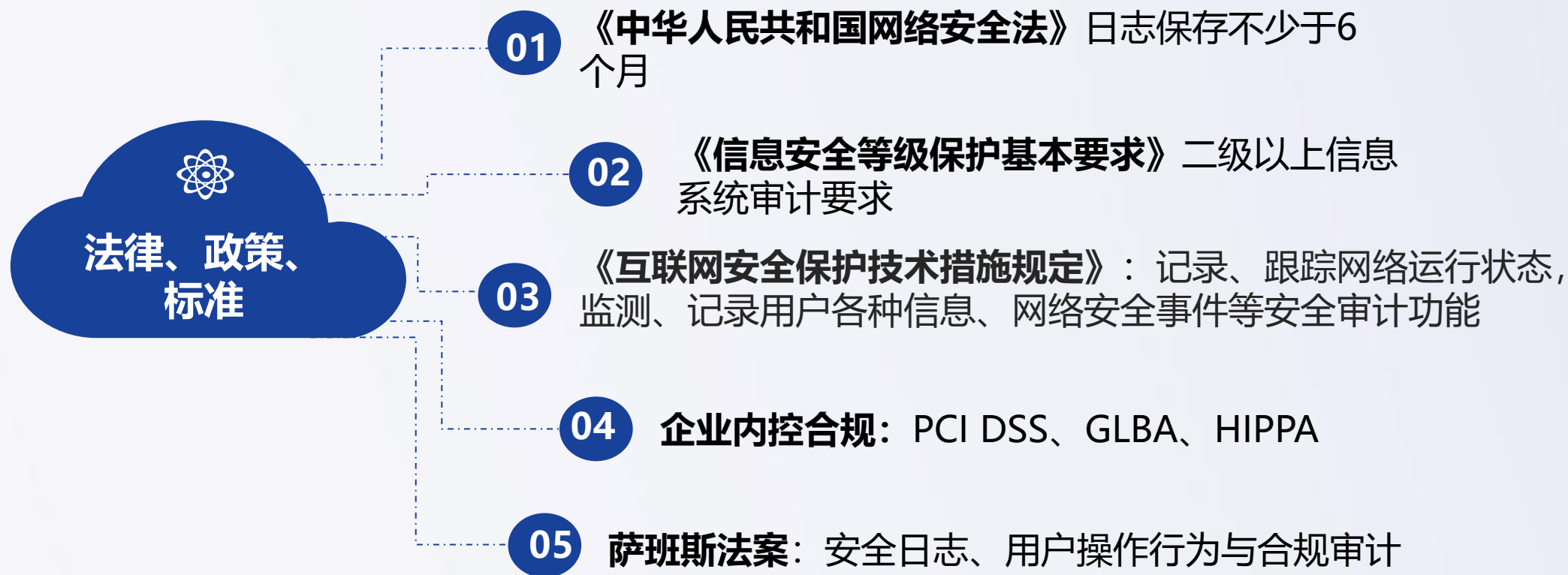
企业中各类应用系统在对外服务的同时也会面临各种用户访问行为造成的信息安全风险，必须实行有效的安全审计手段。

网络资源滥用

企业对员工的上网行为不直接控制，企业员工不当使用或滥用公司网络资源时，容易造成企业资料泄密等后果。

安全事件定位风险

由于目前的应用系统都是互相关联的，有时一个故障现象需要对数十台设备进行关联分析才能定位故障原因。



需求

等保合规建设

解决方案

结合等保网络和通信安全、设备和计算安全、应用与数据安全等的合规要求项

预期效果

满足等保合规项，增加等保评分

第三级网络安全等级保护基本要求		
层面	控制点	要求项
安全通用要求-安全区域边界	安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
安全通用要求-安全计算环境	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计；
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
		d)应对审计进程进行保护，防止未经授权的中断
安全通用要求-安全管理中心	集中管控	d)应对分散在各个设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求。
云计算安全拓展要求-安全区域边界	安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计,至少包括虚拟机删除、虚拟机重启
		b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计
云计算安全拓展要求-安全管理中心	集中管控	c)应根据云服务商和云服务客户的职责划分,收集各自控制部分的审计数据并实现各自的集中审计

- 信息化网络过程中部署了多种设备，产生了各种不同格式、不同语义的日志；
- 日志分散记录在各处，缺乏访问控制及完整性保护手段。

- 每日多达上千万的事件日志量，重复信息过多；
- 海量事件的处理与检索困难，手工处理难以从海量的日志中发现潜在的问题。



- 自动化程度低，缺乏对多种来源的日志进行关联分析的能力；
- 无法根据不同的审计目的区分一般审计和敏感审计。

- 多种设备、应用系统都提供了监控和审计控制台；
- 实时集中监控实施成本大，技术要求高。

深信服日志审计系统

提供了众多基于日志分析功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控及安全告警等，系统配备了全球IP归属及地理位置信息数据，为安全事件的分析、溯源提供了有力支撑，综合日志分析系统能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

系统能够实时不间断地采集汇聚企业中不同厂商不同种类的安全设备、网络设备、主机、操作系统、用户业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及审计违规。

记载着各类设备、系统、应用、网络访问等所有日志与访问信息



服务器



交换机



应用



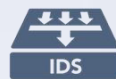
防火墙



防毒墙



IPS



IDS

监控

了解设备、系统的日常运行状态

排障

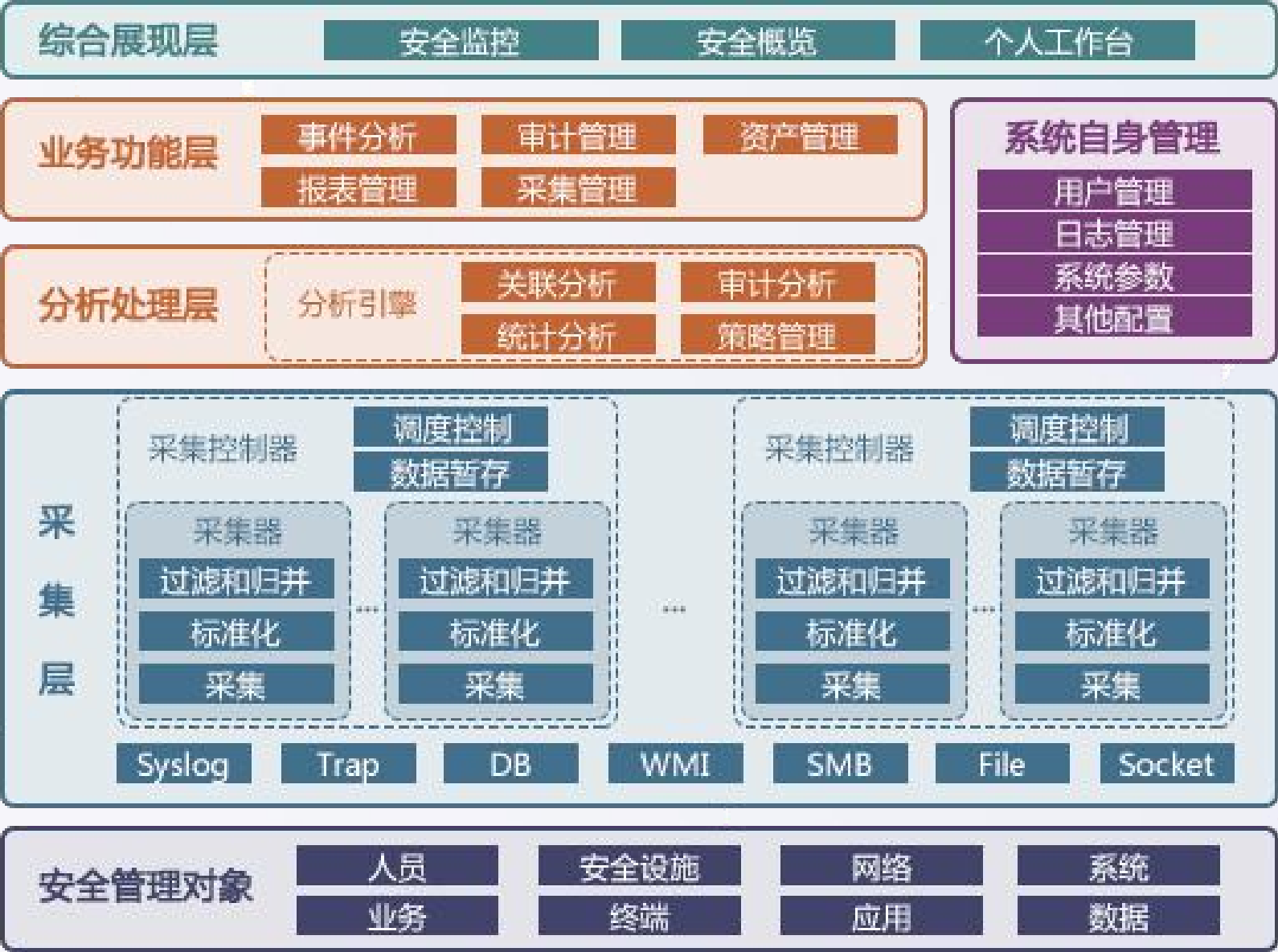
检查设备、系统运行错误的原因

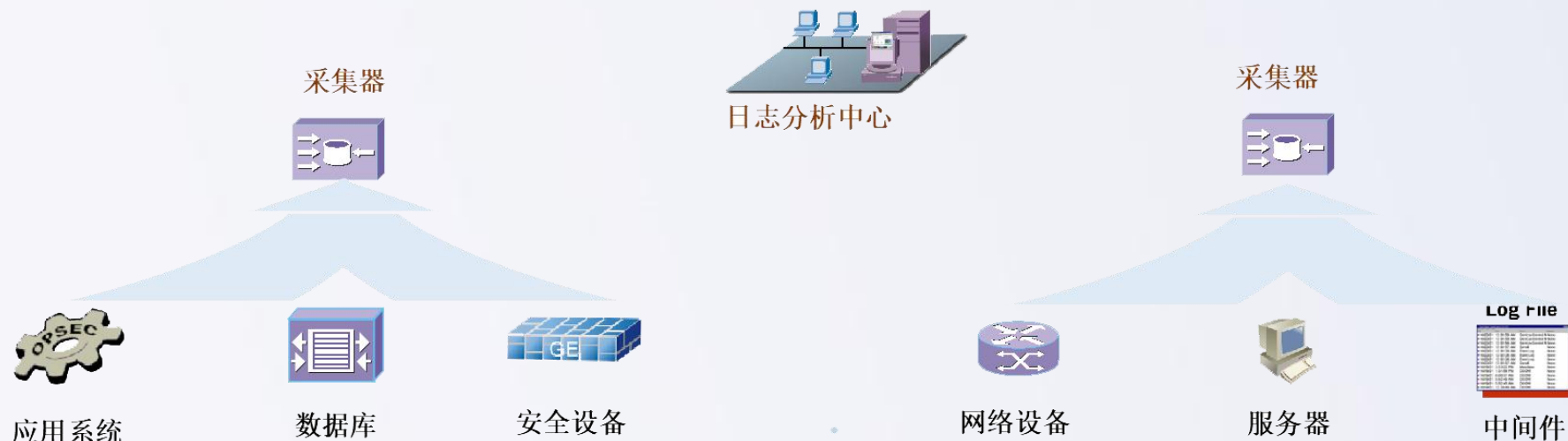
审计

追溯设备、系统被攻击时的痕迹

目录

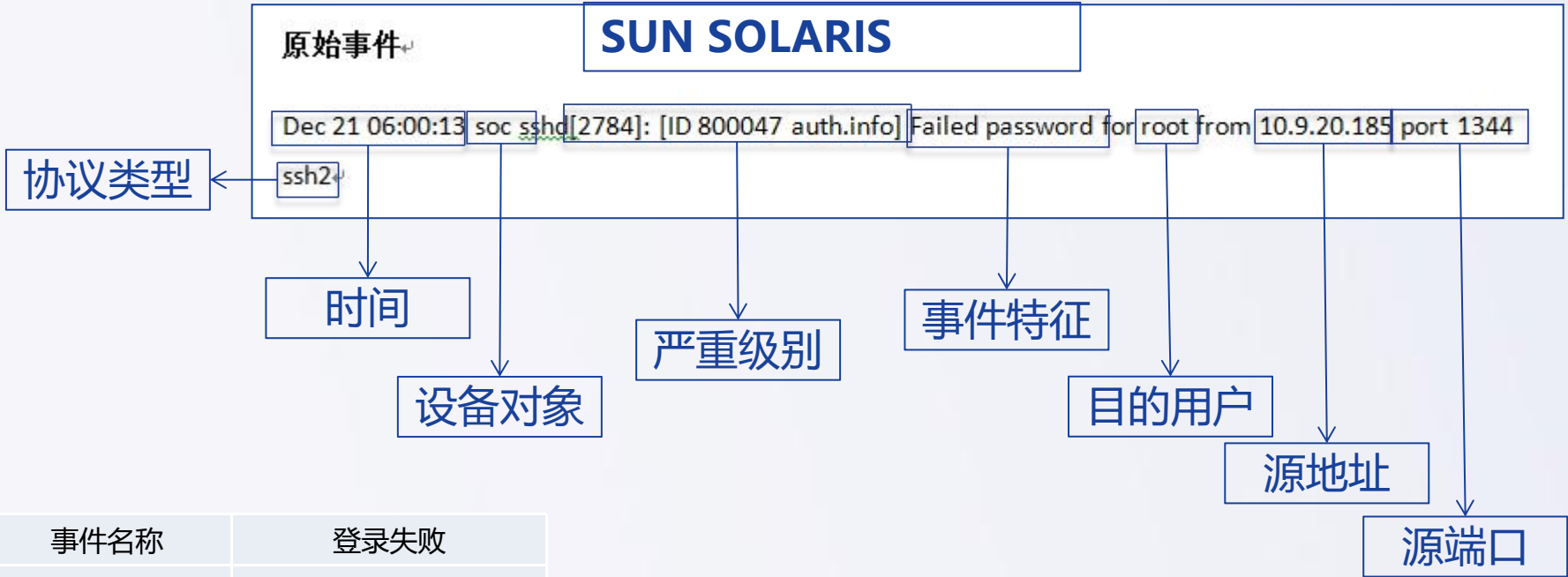
- 一. 需求背景与产品定位
- 二. 主要功能与产品优势**
- 三. 应用场景与优势案例
- 四. 产品选型与操作演示





支持各种主流的安全设备；非主流设备系统类型支持灵活的自定义扩充



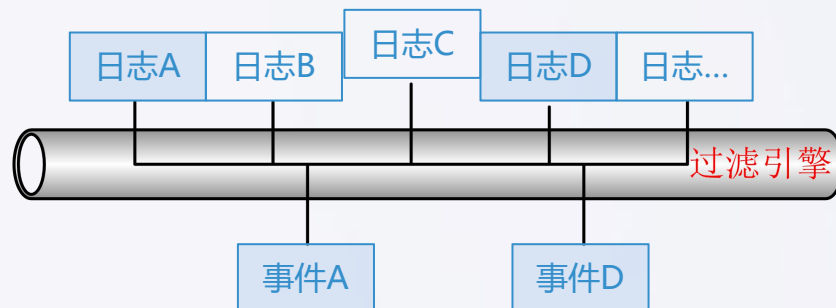


事件名称	登录失败
事件类型	访问控制类
发生时间	2013.12.21 06:00:13
源IP地址	10.9.20.185
源端口	1344
严重级别	信息级
主机名	SOC
目的用户	root
协议	SSH

由采集器根据解析脚本进行原始日志的解析，转换为统一的标准化格式

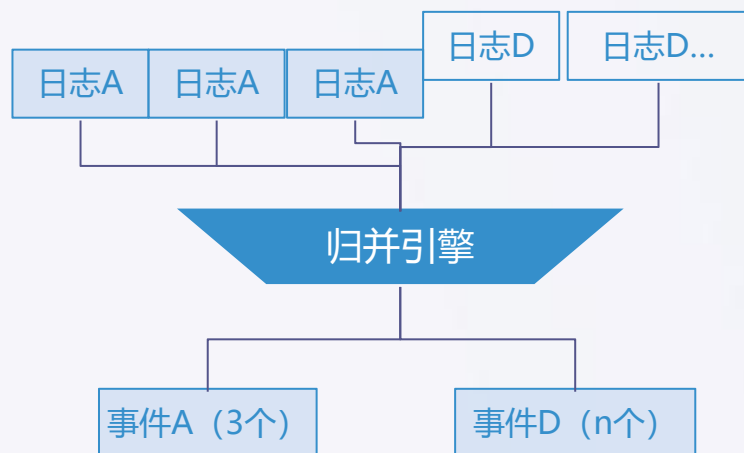
系统内置丰富的标准化策略，适配众多不同厂商不同设备的日志数据

对于小众的厂商或设备，具备良好的可扩展性，可通过界面导入配置文件



过滤

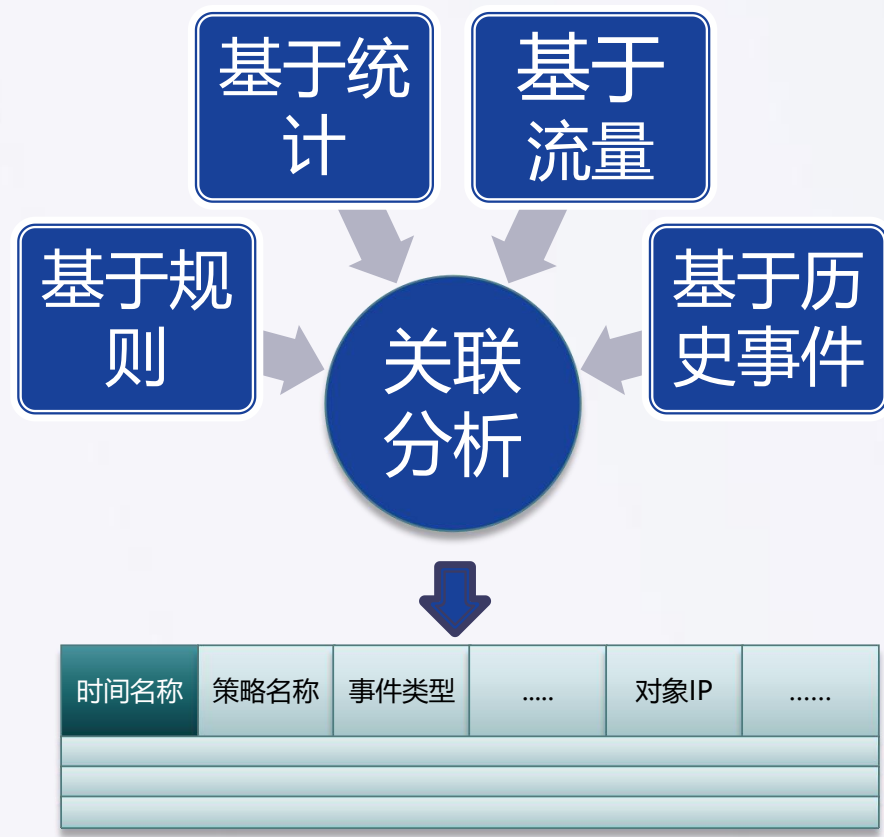
在众多杂乱的事件中，过滤出具备一定风险和价值事件



归并

如果多个事件满足归并的条件，如具备同样的目的和行为，可归类为一种事件

设定的不同的关联策略；配置可由关联策略产生审计事件，如时间、IP地址、方式等，对于相符合的结果，系统将在关联事件中呈现给用户



支持的数据采集方式

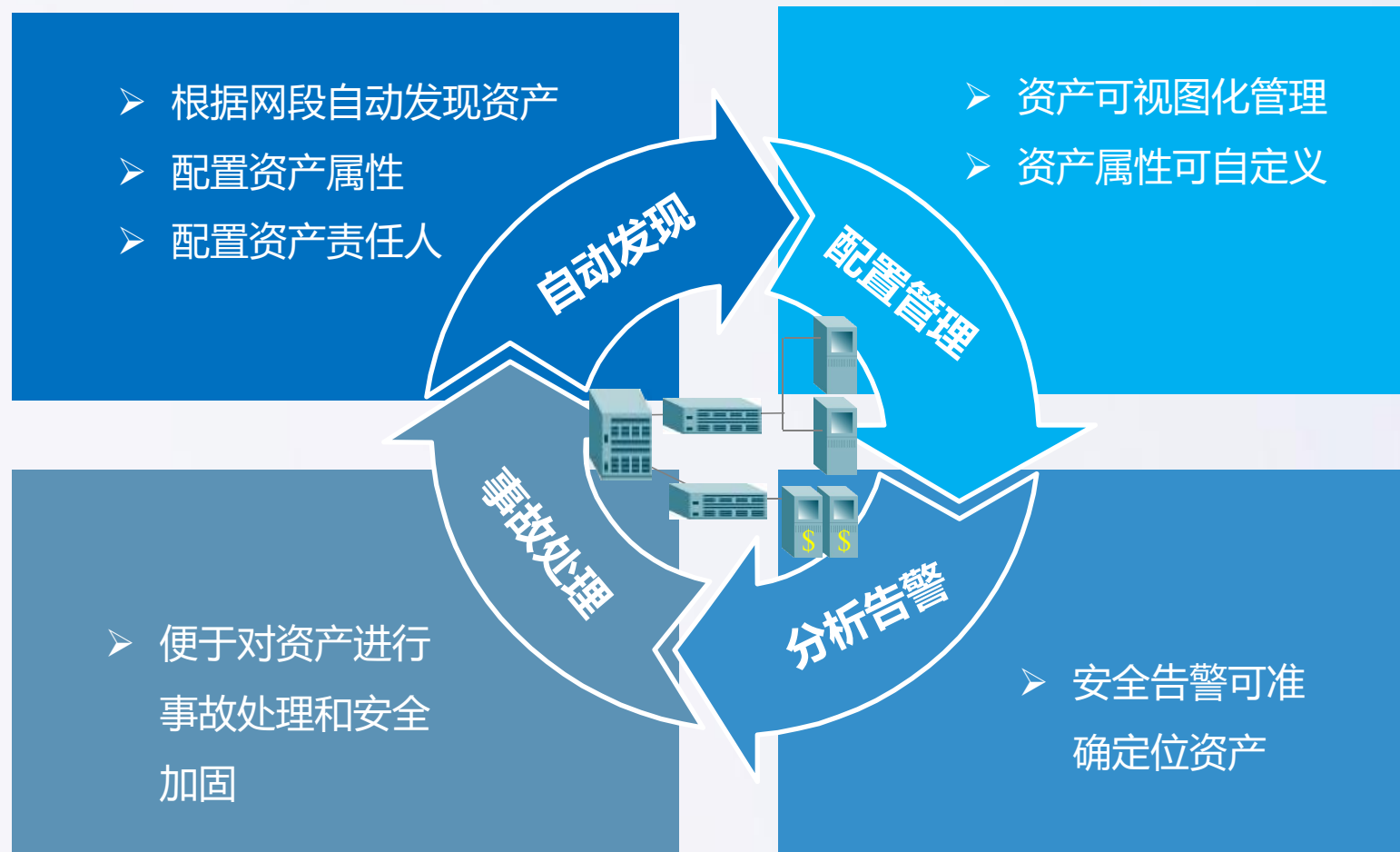
- SYSLOG
- SNMP Trap
- WMI
- SMB
- 数据库
- 文件
-

适用的场景

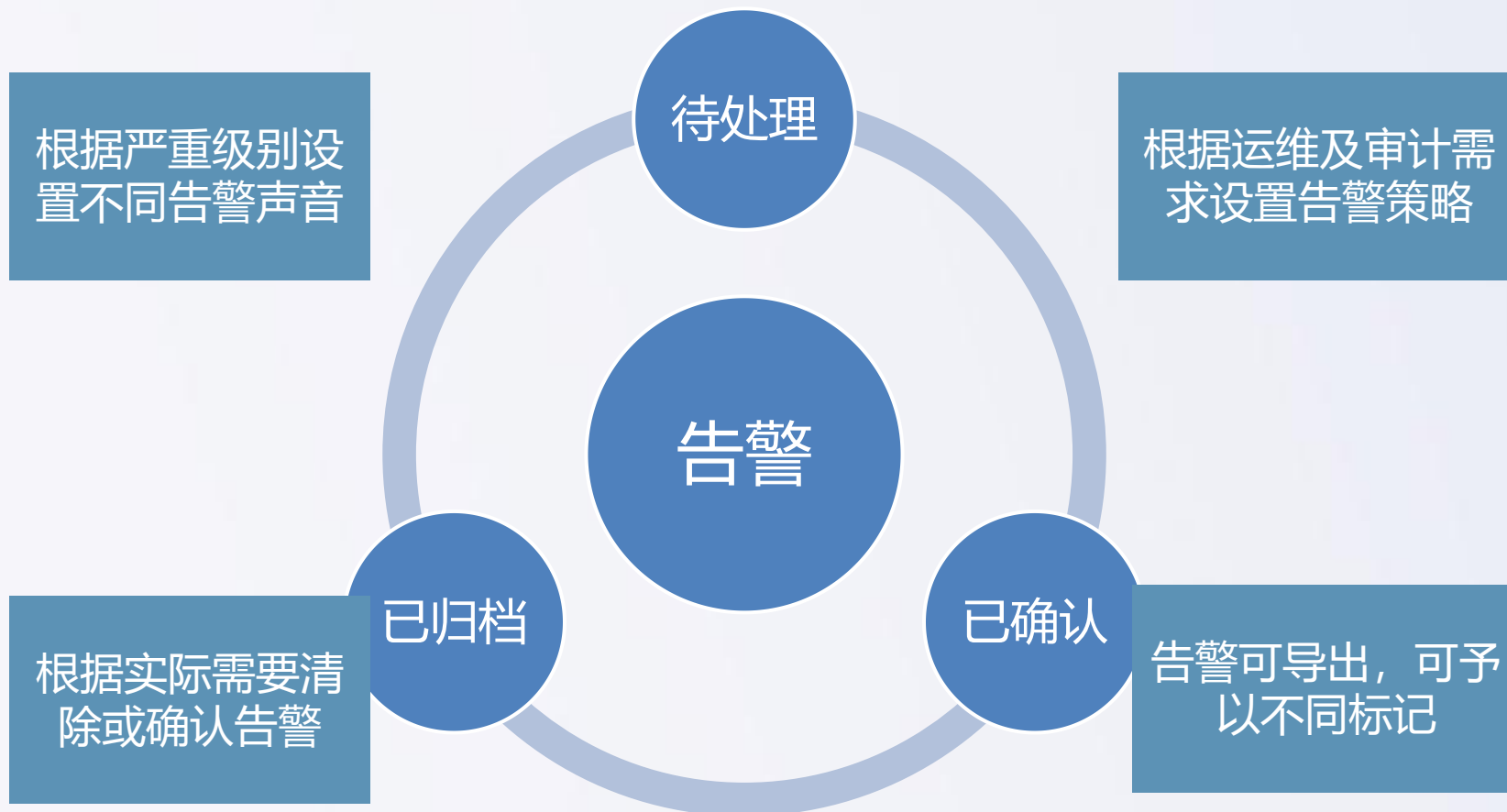
- 网站攻击
- 信息泄露
- 网页篡改
- 异常行为分析
- 带宽资源滥用
- Dos、DDos攻击
- 钓鱼欺诈
-

关联模型

- 弱口令扫描
- 非工作时间访问
- 异常登录
- 缓冲区溢出
- SQL注入
- Teardrop攻击
- 拒绝服务攻击
- 端口扫描
- 策略变更
- 可疑木马端口
- 发现病毒事件
- 异常流量
-









态势一目了然

信息快速浏览

自由定义界面

风险的集中展示区域，它支持以TAB页及微件（Widget）形式多角度展现，用户也可对仪表的布局和内容进行定义和调整。



- **高扩容：** 分布式架构，通过增加设备数量，能可靠地存储和处理PB数据。
- **低成本：** 通过普通机器组成的服务器群来分发以及处理数据。这些服务器群甚至可达数千个节点。
- **高效率：** 通过并行处理和内存运算方式，处理非常的快速。
- **高可靠：** 自动地维护数据的多份复制，并且在任务失败后能自动地重新部署计算任务。
- **高兼容：** 通过强大的采集系统，能兼容任意格式的结构化和非结构化数据。
- **高智能：** 通过智能策略库和关联模型，及外在专家库、数据库接口，智能化处理事件。

目录

- 一. 需求背景与产品定位
- 二. 主要功能与产品优势
- 三. 应用场景与优势案例
- 四. 产品选型与操作演示

《网络安全法》中明确规定网络日志留存不少于六个月

第三章 网络运行安全

第二十一条

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其它义务。

等保二级以上均要求应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等

交换机、防火墙等网络设备均为无硬盘架构，无法长期存放日志
需要日志审计系统做统一的日志收集与存储，满足相关法律法规要求





- 监控设备、系统、应用运行日志;
- 降低运维巡检成本;
- 查找设备、系统故障原因;
- 追溯攻击源头与攻击行为。



国网四川省电力公司 甘孜供电公司



需求场景

内网IT基础资源的集中日志审计，提升运维效率，满足等保和安全法要求。



建设效果

部署在数据安全II管理区，实现对基础IT设备日志收集及分析。

河北省民政厅



需求场景

日志统一收集和集中管理，要求具备超大日志量环境支撑能力，且因项目分批建设必须满足对众多厂商日志收集兼容性。



建设效果

收集各类主机、网络设备、安全日志，并通过存储压缩等特性大幅降低硬件需求。



甘肃省武威肿瘤医院



需求场景

安全运维，满足等保日志审计的要求；
日志统一收集和集中管理，要求具备超大日志量环境支撑能力。



建设效果

部署在医院内网，实现对内网全网日志采集及分析，对安全事件实现实时监控，发现安全事件及时告警。



中国电信集团 北京电信有限公司



需求场景

等保和安全法要求，满足全网日志统一收集和集中审计。



建设效果

收集全网出口、安全、交换、服务器等设备日志，对海量日志实现高速存储、查询，实现集中日志审计，满足安全法要求。



四川理工大学白酒学院



需求场景

学校全网日志收集和高速查询，满足安全法要求；

全网日志安全分析，及时有效的定位核心风险。



建设效果

收集全网出口、安全、交换、服务器等设备日志，对海量日志实现高速存储、查询，实现集中日志审计，满足安全法要求

河北省公安厅



需求场景

实现全网网络设备、安全设备、主机的日志统计存储、统一监控；满足企业内控安全要求。



建设效果

全网设备的日志收集，包括网络设备，服务器，安全设备等，集中管理、统计监控。

目录

- 一. 需求背景与产品定位
- 二. 主要功能与产品优势
- 三. 应用场景与优势案例
- 四. 产品选型与操作演示



型号	LAS-1000-A600	LAS-1000-C600	LAS-1000-E600
功能描述	包含流量采集、日志的采集、过滤、归并、关联分析、展现、告警监控、实时监控、报表等		
许可	包含50台设备的接入授权（可扩展到150个主机审计许可）	包含200台设备的接入授权（可扩展到450个主机审计许可）	包含400台设备的接入授权（可扩展到1500个主机审计许可）
EPS	1200	2000	4000
硬盘	1T	1T	4T
电源	单电源，250W	单电源，250W	冗余电源，350W
机型	2U	2U	2U
标配网口	6电	6电	6电
管理接口	1 Console，2 USB	1 Console，2 USB	1 Console，2 USB

STEP 01

根据设备数初步选定型号

一般情况下，根据客户需要采集分析的设备数量，选购基础平台产品就可以了，比如客户有185个设备需要采集，那选购LAS-1000-C600就可以了

STEP 02

根据EPS确定最终型号

根据客户环境内需要采集的设备日志量，评估LAS的EPS是否能满足客户需求。

STEP 03

需要选购采集机场景

存在区域划分：一个单位有2个或以上的不同地理位置的办公场所都需要采集数据，那可以在总部放一台设备，其它地点放采集机。

存在网络划分：可以在一个安全域部署一台深信服LAS，其它安全域部署一台采集机，多个安全域相互不能访问采集机，采集机与LAS之间通过防火墙开通一个访问策略

STEP 04

什么情况下，需要增加采集设备许可

LAS-1000-C600自带200个采集许可，对于客户需要略超出这个数量的，可以增加一定数量的许可，增加的数量最多为该型号允许范围内，详见产品型号表

序号	设备	单设备EPS数量参照
网络设备		
1	路由器/交换机	5
2	流量检测	100
3	Wireless AP (w/ 802.1x)	5
4	负载均衡	5
5	打印机	1
服务器设备		
1	Unix/Linux服务器	20
2	Windows	200
3	Windows域控	300
4	邮件服务器	10
5	代理服务器	1
6	DNS服务器	1
7	WEB服务器	50
8	应用服务器	1
9	数据库服务器	30
11	其它	10

序号	设备	单设备EPS数量参照
安全设备		
1	外部防火墙	150
2	内部防火墙	50
3	DMZ区IDS	20
4	内网IDS	1
5	IDS管理服务器 (10个传感器)	20
6	IPS	40
7	准入设备	20
8	主机IDS	1
9	防病毒服务器	1
10	员工卡读卡器	1
11	VPN	1
12	上网行为管理	20
13	WEB应用防火墙	200
14	密钥管理系统	10

系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)

Q 全文检索

 系统管理员

日志列表

详细信息

基本信息

名称: SQL注入

标准事件编号:

事件编号: f8d57767-196e-538a-8dd1-a69e1e634134

详细信息: Nov 14 03:34:34 WAF-T3-51e4183c0cca5 100491 | 175.2.97.244 | 门户 | SQL注入 | webauditlog | critical | attack.injection.sql.by,175.2.97.244,门户,www.gxu.edu.cn,///plus/mytag_js.php?aid=9191 | 2016-11-14 03:34:34

类型: 网络攻击

子类: 漏洞攻击

级别: 严重

原始级别: critical

设备类型: 防火墙

设备地址: 192.168.100.122

设备名称: WAF-T3-51e4183c0cca5

产品名称: TitanSec WAF

产品版本:

接收时间: 2019-06-23 03:58:34

原始时间: 2016-11-14 03:34:34

可信度: 50

源

源地址: 175.2.97.244

源主机名:

对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义

**SANGFOR**

LAS 3.0.4

当前事件速率(0eps)

全文检索

系统管理员

导航菜单

安全概览

安全监控

事件分析

报表管理

策略管理

审计策略

关联策略

采集策略

知识库

审计管理

资产管理

系统管理

采集策略

新增策略

友情提示: "※" 标注为必填项, 转发syslog适用于转发少量重点关注事件, 转发事件量过大会影响采集器性能

※ 策略名称

※ 过滤器

※ 动作

☐ 丢弃

☐ 转发syslog

☐ 转发syslog并继续处理

☒ 设置属性并继续处理

事件名称

严重级别

请选择

事件类别

请选择

事件子类

请选择

严重

高级

中级

低级

信息

描述

支持不同设备相同IP的日志识别

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)


Q 全文检索

 系统管理员

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)


Q 全文检索

 系统管理员

导航菜单

安全概览

安全监控

事件分析

日志列表

关联事件

审计事件

网络会话

导出任务管理

报表管理

策略管理

审计管理

资产管理

系统管理

日志列表

友情提示: 请输入至少一个筛选条件,否则系统无法返回任何数据。

普通模式

专家模式

查询条件

请选择

时间段类型: 自定义

日期范围: 2019-06-23 00:00:00 - 2019-06-23 23:59:59

采集器: 请选择

名称:

严重级别: 请选择

设备IP: 192.168.100.111

源IP:

目的IP:

设备类型: Web中间件

执行动作账号:

动作对象名称:

动作对象类型:

高级查询

查询

清空

保存查询条件

导出

配置列表默认字段

离线分析

标准化优化建议

序号		名称	类型	子类	严重级别	设备IP	时间	源IP	目的IP
1	<input type="checkbox"/>	未找到页面	连接	连接拒绝	信息	192.168.100.111	2019-06-23 03:59:12	218.203.188.166	
2	<input type="checkbox"/>	未找到页面	连接	连接拒绝	信息	192.168.100.111	2019-06-23 03:59:12	218.203.188.166	
3	<input type="checkbox"/>	未找到页面	连接	连接拒绝	信息	192.168.100.111	2019-06-23 03:59:12	218.203.188.166	

显示 10 条记录

显示 1 到 10 共 460 条记录 (实际查询到 460 条)

<<

<

1

2

3

4

5


>

>>

javascript:void(0);

测试许可, 截止2019-08-07

支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计

 SANGFOR | LAS 3.0.4

当前事件速率(0eps)

全文检索

系统管理员

导航菜单

安全概览

安全监控

事件分析

日志列表

关联事件

审计事件

网络会话

导出任务管理

报表管理

策略管理

审计管理

资产管理

系统管理

日志列表

概览

查询

设备日志量排名列表

日期选择: 2019-06-23

重建索引

设备类型

- Unix/Linux主机(1)
- Windows主机(0)
- 网络设备(0)
- 防火墙(2)
- 统一威胁管理(0)
- 入侵检测系统(0)
- 入侵防御系统(0)
- 扫描器(0)
- VPN (0)
- 防病毒(0)
- 数据库(0)
- Web中间件(1)
- 堡垒机(0)
- 应用系统(1)
- 其它(3)

序号	IP地址	设备名称	严重	高级	中级	低级	信息	总数
1	192.168.100.111	192.168.100.111	0	0	725419	4175341	32650765	37551525
2	192.168.100.191	192.168.100.191	0	0	0	0	4885	4885
3	192.168.100.122	192.168.100.122	2138	1040	1030	12	0	4220
4	192.168.100.121	192.168.100.121	0	0	0	432	864	1296
5	192.168.100.235	192.168.100.235	0	151	16	6	0	173

显示 10 条记录

显示 1 到 5 共 5 条记录

« < 1 > »

操作演示-日志查询



SANGFOR
深信服科技



深信服智安全
SANGFOR SECURITY

支持更加精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。

SANGFOR | LAS 3.0.4

当前事件速率(0eps)

Q 全文检索

系统管理员

导航菜单

安全概览

安全监控

事件分析

日志列表

关联事件

审计事件

网络会话

导出任务管理

报表管理

策略管理

审计管理

资产管理

系统管理

日志列表

友情提示: 请尽量输入精确查询条件,查询时系统将返回前10,000条记录。

普通模式

专家模式

查询条件

请选择

时间段类型

最近12小时

表达式:

eventName:"SQL"

提示

eg. reliability: [50 TO 100]

3、可以设置权重来显示优先搜索结果 (设置越大, 越优先显示, 建议设置在1~2之间);
eg. eventname: complication^1.6

4、与 (AND)、或 (OR) 和非 (NOT) 的联合查询;
eg. eventname: "complication" AND devicetype: "FireWall"

查询

清空

保存查询条件

导出

标准化优化建议

序号	<input type="checkbox"/>	名称	类型	子类	严重级别	设备IP	时间	源IP	目的IP
1	<input type="checkbox"/>	SQL注入	网络攻击	漏洞攻击	严重	192.168.100.122	2019-06-23 03:58:34	175.2.97.244	
2	<input type="checkbox"/>	SQL注入	网络攻击	漏洞攻击	严重	192.168.100.122	2019-06-23 03:58:34	175.2.97.244	

显示 10 条记录

显示 1 到 10 共 2,133 条记录 (实际查询到 2,133 条)

<<

<

1

2

3


4


5

>


>>

支持全球地理位置库

 **SANGFOR** | LAS 3.0.4

当前事件速率(1395eps)


Q 全文检索

 系统管理员

+ 流量

+ 审计

- 地理信息

源国家编号: cn

源国家: China

源省份: 湖南

源城市: Loudi

源经度: 111.99444

源纬度: 27.73444

源IP地址:

目的IP地址:

目的国家编号:

目的国家:

目的省份:

目的城市:

目的经度:

目的纬度:

源组织: China Telecom

源组织归属地: Chinanet

目的组织:

目的组织归属地:

+ 其它

+ 保留字段

为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了GUI方式的关联规则设置功能，关联的类型包括基于规则和基于统计的

 SANGFOR | LAS 3.0.4

当前事件速率(967eps)

全文检索

系统管理员

导航菜单

安全概览

安全监控

日志查询

报表管理

策略管理

审计策略

关联策略

采集策略

知识库

资产管理

日志采集

系统管理

关联策略

新增关联策略

策略名称

基于规则

基于统计

基于流量

基于历史事件

过滤器

关联条件

新增关联状态

响应方式

产生告警

转发外系统

执行程序

关联事件名称



支持基于因果式状态关联分析

SANGFOR | LAS 3.0.4

当前事件速率(1791eps)

全文检索

系统管理员

导航菜单

- 安全概览
- 安全监控
- 事件分析
- 报表管理
- 策略管理
 - 审计策略
 - 关联策略
 - 采集策略
 - 知识库
- 审计管理
- 资产管理
- 系统管理

过滤器:

与

事件类型 等于 访问控制

关联条件:

状态1

在 60 秒内发生 3 次

归并字段: 源地址, 目的地址

与

事件子类 等于 用户登录(访问控制)

动作结果 属于 (失败,fail)


状态1 之后 发生 状态2


与

状态1.源地址 等于 状态2.源地址

状态1.目的地址 等于 状态2.目的地址

支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)

全文检索

系统管理员

安全概览

安全监控

事件分析

报表管理

策略管理

审计策略

关联策略

采集策略

知识库

★ 审计管理

资产管理

系统管理

审计事件

审计事件列表

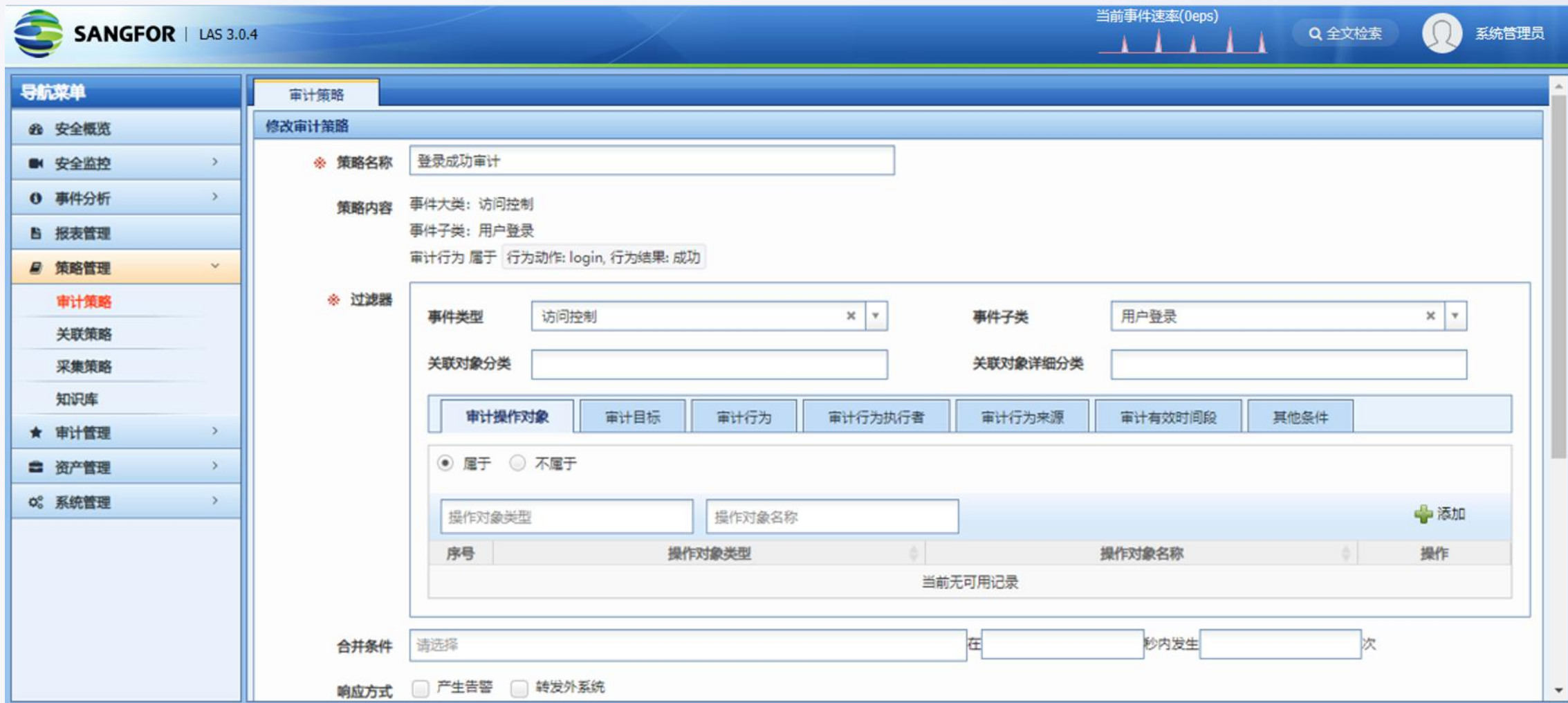
导出

序号	事件名称	对象IP	事件级别	产生时间	更新时间	总次
当前无可用记录						


显示 10 条记录

显示 0 到 0 共 0 条记录

提供可视化方式进行策略制定



支持TLS会话、数据库会话、工控会话、邮件会话、FTP会话、Telnet会话，即时通讯会话的展现

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)

Q 全文检索

系统管理员

网络会话

网络会话


日期: 2019-06-23 时间段: 00:00:00 - 23:59:59 会话类别: TLS会话 网络会话 HTTP会话 DNS会话 TLS会话 数据库会话 工控会话 邮件会话 即时会话 会话查询


客户端地址: 服务器地址: 服务器端口: 查询 重置

序号	服务器证书通用名	服务器名称	客户端地址	服务器地址	服务器端口	访问时长	操作
1	edge.skype.com	config.edge.skype.com	192.168.6.58	13.107.3.128	443	2019-06-23 02:09:10	1ms 查看
2	smartscreen.microsoft.com	c.urs.microsoft.com	12.8.201.200	104.40.17.139	443	2019-06-23 02:09:17	1ms 查看
3	smartscreen.microsoft.com	c.urs.microsoft.com	12.8.201.200	104.40.17.139	443	2019-06-23 02:09:17	1ms 查看
4	Microsoft IT SSL SHA2	cdn.onenote.net	12.8.201.200	2.17.52.161	443	2019-06-23 02:09:17	1ms 查看
5	smartscreen.microsoft.com	c.urs.microsoft.com	12.8.201.200	104.40.17.139	443	2019-06-23 02:09:17	11ms 查看
6	settings-win.data.microsoft.com	settings-win.data.microsoft.com	12.8.201.200	23.99.125.126	443	2019-06-23 02:09:17	11ms 查看
7	Microsoft IT SSL SHA2	cdn.onenote.net	12.8.201.200	104.71.152.102	443	2019-06-23 02:09:17	11ms 查看
8	settings-win.data.microsoft.com	settings-win.data.microsoft.com	12.8.201.200	111.221.29.253	443	2019-06-23 02:09:17	11ms 查看
9	www.bing.com	cn.bing.com	12.8.201.200	202.89.233.103	443	2019-06-23 02:09:17	11ms 查看
10	smartscreen.microsoft.com	c.urs.microsoft.com	12.8.201.200	104.40.17.139	443	2019-06-23 02:09:17	11ms 查看

显示 10 条记录 显示 1 到 10 共 42 条记录 (实际查询到 42 条)

包括报表内置实例管理和报表任务管理

 **SANGFOR** | LAS 3.0.4

当前事件速率(0eps)

全文检索

系统管理员

导航菜单

安全概览

安全监控

事件分析

报表管理

策略管理

审计管理

资产管理

系统管理





















报表管理

报表实例

报表任务

报表实例列表

新增 删除 启用 停用

序号		实例名称	报表时间	更新时间	操作
1	<input type="checkbox"/>	Unix类主机日志分布日报	时间范围: 每日	2019-05-07 19:36:13	 
2	<input type="checkbox"/>	Windows类主机日志分布日报	时间范围: 每日	2019-05-07 19:36:13	 
3	<input type="checkbox"/>	主机访问控制分布日报-Linux	时间范围: 每日	2019-05-07 19:36:13	 
4	<input type="checkbox"/>	主机访问控制分布日报-Windows	时间范围: 每日	2019-05-07 19:36:13	 
5	<input type="checkbox"/>	其它类日志分布日报	时间范围: 每日	2019-05-07 19:36:13	 
6	<input type="checkbox"/>	安全告警分布情况日报	时间范围: 每日	2019-05-07 19:36:13	 
7	<input type="checkbox"/>	应用类日志分布日报	时间范围: 每日	2019-05-07 19:36:13	 
8	<input type="checkbox"/>	应用访问控制分布日报	时间范围: 每日	2019-05-07 19:36:13	 
9	<input type="checkbox"/>	数据库类日志分布日报	时间范围: 每日	2019-05-07 19:36:13	 
10	<input type="checkbox"/>	数据库访问控制分布日报	时间范围: 每日	2019-05-07 19:36:13	 

显示 10 条记录

显示 1 到 10 共 44 条记录

<<

<

1

2

3

4

5

>

>>

业务管理配置，可以导出系统内报表、策略、采集器、资产等业务数据，供新设备导入配置，实现快速切换设备

**SANGFOR** | LAS 3.0.4

当前事件速率(0eps)


Q 全文检索

 系统管理员

导航菜单

安全概览

安全监控 >

事件分析 >

报表管理

策略管理 >

审计管理 >

资产管理 >

系统管理 >

用户管理

日志管理

系统参数

内置对象

升级管理

许可证管理

采集器管理

云端配置

云端升级

业务配置管理

业务配置管理

导入业务配置

配置文件

请选择文件

选择文件



导入配置

导出业务配置

全选

报表

策略

资产

采集器

知识库

导出配置



THANK YOU

深信服 智安全