

综合安全分析文档

2014 年 4 月 11 日

目录

综合安全分析文档.....	1
目录	2
1. 文档版本跟踪.....	3
2. 网络流量审计.....	3
2.1. 流量监控频道.....	3
2.7.1 网络总体状态监控图.....	4
2.7.2 端口协议分析监控图.....	4
2.7.3 Top 网络流量监控图.....	5
2.7.4 Top 网络数据包监控图.....	6
2.7.5 网络扫描活动监控图.....	6
2.2. 流量搜索频道??	7
2.3. 入侵监控频道.....	8
2.3.1 IDS 事件分布监控图	8
2.3.2 IDS 事件类型监控图	9
2.3.3 IDS 事件严重性级别	10
2.3.4 Top 攻击事件监控图	10
2.3.5 IDS 时间线监控图	11
2.3.6 IDS 扫描事件监控图	11
2.3.7 首次攻击事件监控图.....	12
2.4. 弱点监控中心.....	12
2.4.1 弱点概况监控图.....	13
2.4.2 Top 弱点监控图.....	13
2.4.3 Top 弱点资产.....	13
2.4.4 弱点存活时间.....	13
2.4.5 首次弱点发现.....	14
2.4.6 弱点中断.....	14
2.5. 弱点分析频道.....	14
2.6. 网络配置监控.....	15
2.6.1 根据配置改变动作.....	15
2.6.2 根据配置改变设备.....	15
2.7. 端口协议监控.....	16
2.7.1 端口活动.....	16
3. 资产账户审计.....	16
3.1. 资产审计频道.....	16
3.1.1 根据优先级.....	17
3.1.2 根据业务区域.....	17
3.1.3 根据功能分类.....	17
3.1.4 根据具体信息.....	18
3.2. 账户审计频道.....	18
3.2.1 根据优先级.....	18
3.2.2 根据账户权限.....	19

3.2.3	根据业务区域.....	19
3.2.4	根据具体信息.....	20
3.3	会话审计频道.....	20
3.3.1	长会话连接.....	20
3.3.2	会话时间分布.....	21
3.3.3	最频繁会话.....	21
4.	地理资源审计（low priority）.....	21
4.1.	地理事件监控.....	21
5.	用户操作审计（pending）.....	23
5.1.	事件复核审计.....	23
5.1.1	根据每个用户.....	23
5.1.2	根据事件重要程度.....	23
5.1.3	Top 贡献用户.....	23
5.1.4	最近复核事件.....	23
5.2.	当前取消事件.....	24
5.3.	事件转发审计.....	24
5.3.1	无日志接入监控.....	24
5.3.2	日志接入性能监控.....	24
5.4.	数据完整性审计.....	24

1. 文档版本跟踪

版本	完成时间	作者	备注
V1	2014.4.11	Ario	V1 初稿。
V2		Ario	

2. 网络流量审计

概述：网络流量审计主要用于网络以及网络设备的监控，包括路由器，交换机，防火墙和 IDS 入侵检测等设备。所有的网络传输流量都将通过这个频道进行审计，审计内容包含总流量，特殊网络传输模式，流量产生的来源，端口流量，网络弱点扫描结果等。

2.1. 流量监控频道

概述：显示网络状态的总体审计结果，帮助检测网络动态趋势和流量变化，同时关联设备或者来源，用于判定当前或是历史网络状态是否有安全问题。

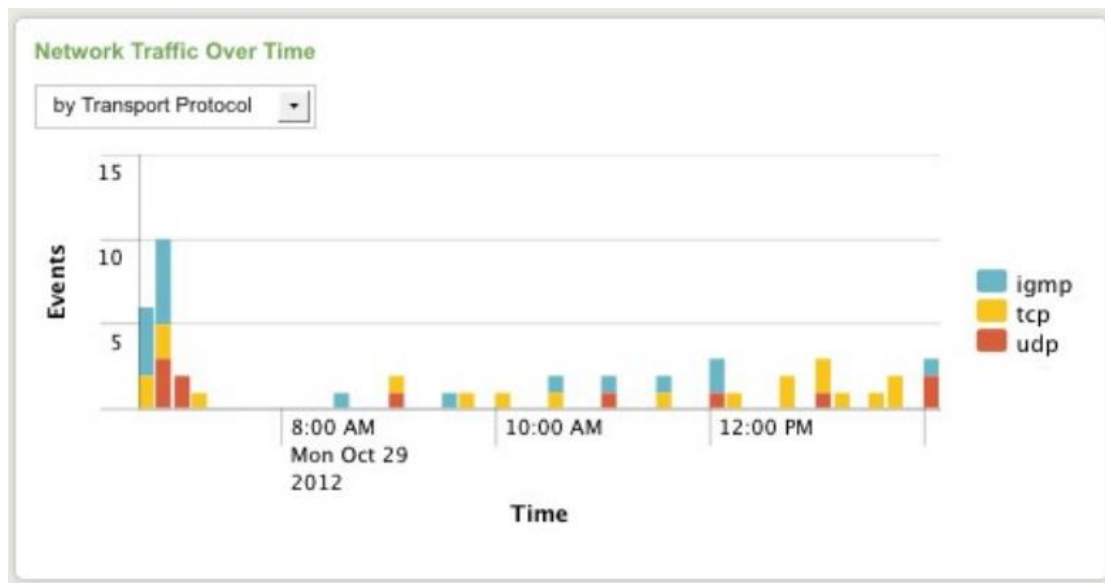
数据：路由器，交换机，防火墙，IDS 日志

2.7.1 网络总体状态监控图

功能：用于查看网络流量的异常增加和减少或者是网络数据包发送个数异常增加或者减少。

字段：开始时间，结束时间，源 ip，目的 ip，源端口，目的端口，协议类型，输入包个数，输出包个数，输入字节数，输出字节数

展现：累积柱状图。



细分：流量分布异常（源地址分散度异常，目的地址分散度异常、端口分散度异常等）；各类 P2P 流量等。

最好可以联动到地理资源监控频道，可以直观看到地址的分散情况。

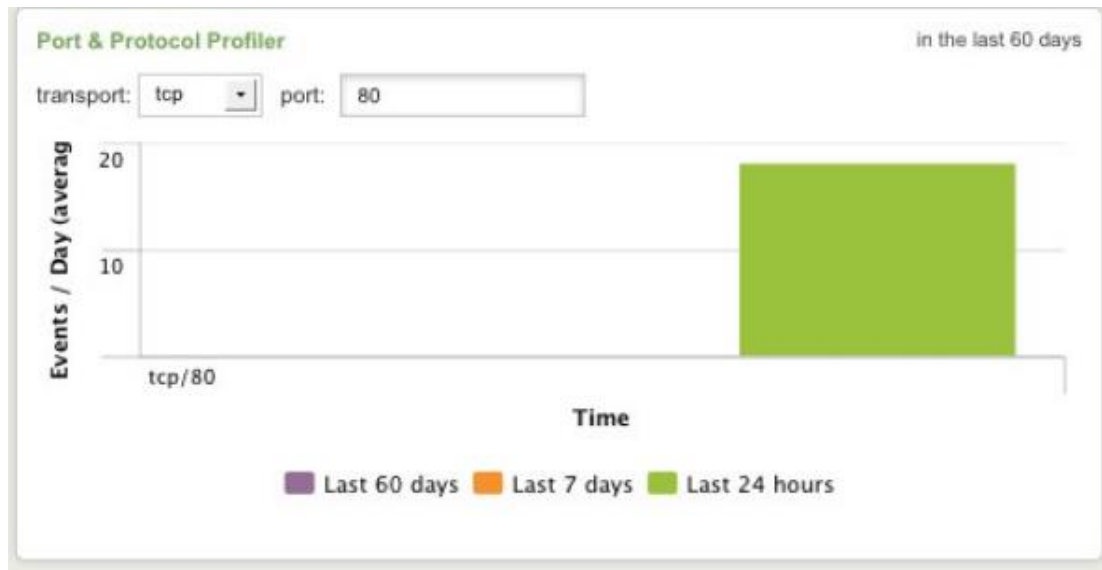
同时计算分散度置信区间，对置信区间外情况报警。

2.7.2 端口协议分析监控图

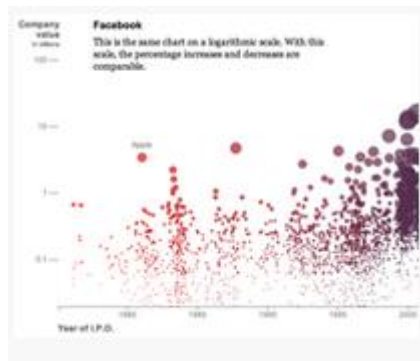
功能：查看针对某个端口及协议每日的平均事件数量，用于检测是否有异常多的事件发生，或者协议比例（机器学习能力，能够统计并记录平时的比例的参数）异常。

字段：传输协议，端口号，时间线

展现：柱状图。选择端口号(0-65535)和协议(TCP, UDP, or ICMP)，可以展现过去 24 小时，过去 7 天，过去 60 天的数据。



或者是离散图

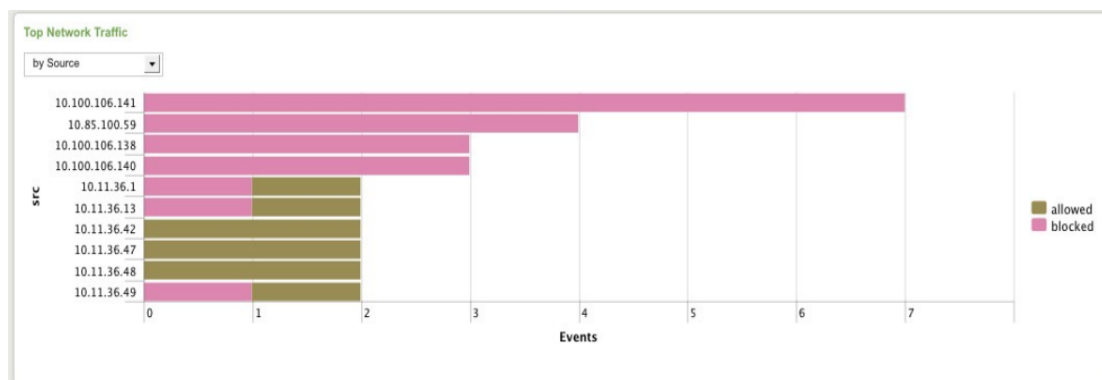


2.7.3 Top 网络流量监控图

功能：展现在某一时间段内网络 top 流量事件。

字段：资产设备，传输协议，来源 ip，来源端口，目标 ip，目标端口，事件

展现：横向柱状图或者是圆形关联图。可以根据数据选择过滤展现的维度。



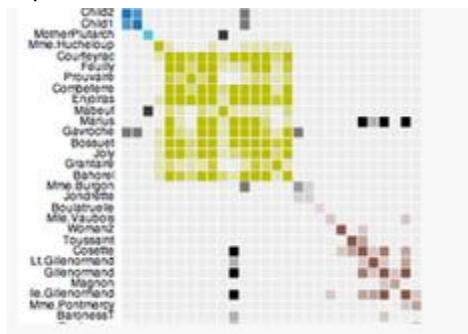
2.7.4 Top 网络数据包监控图

功能：计算并且展现某一时间段内资产收发数据包频率

字段：资产设备，传输协议，来源 ip，来源端口，目标 ip，目标端口，数据包收发频率

展现：柱状图。可以根据数据选择过滤展现的维度。

Top 的流量和数据包想要做成一种热点图的形式。

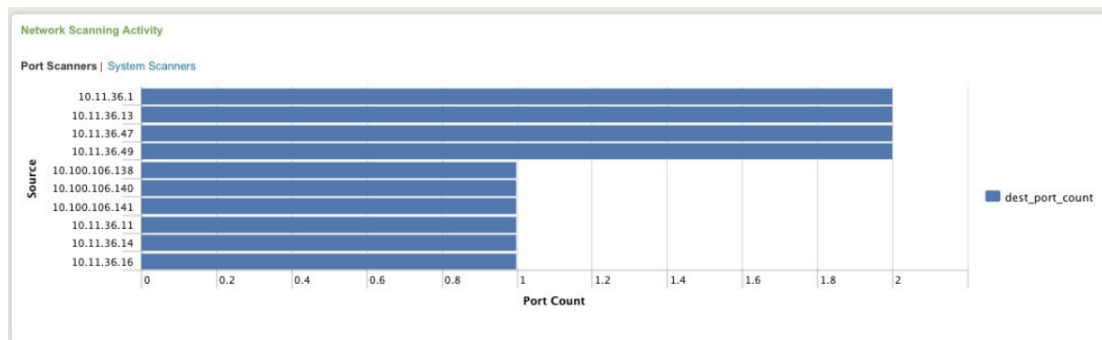


2.7.5 网络扫描活动监控图

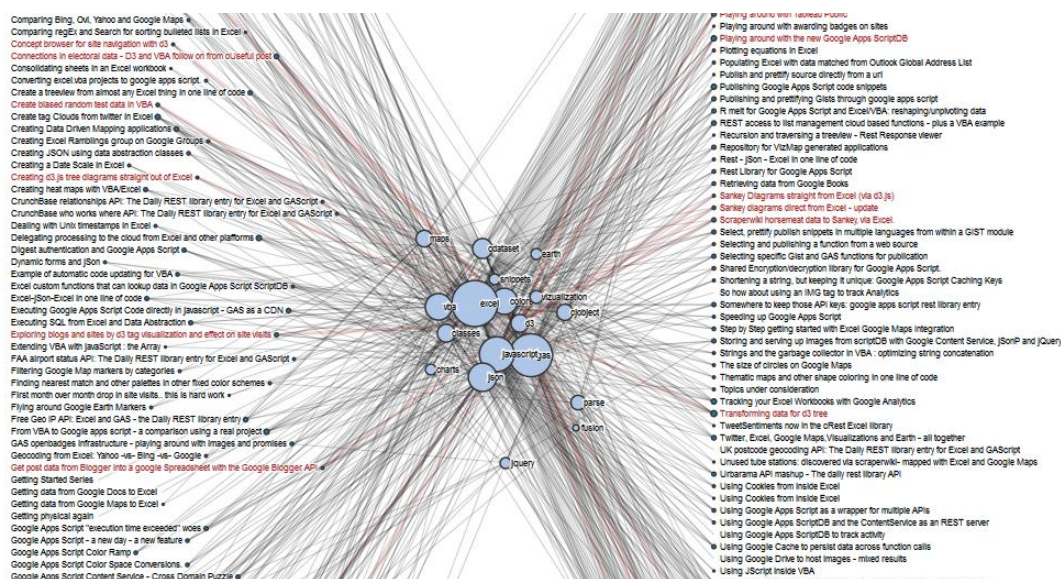
功能：显示对资产设备的扫描活动，预警和检测未经授权的潜在恶意扫描

字段：来源 ip，目标端口，目标 ip。

展现：同一设备，大量端口被扫描定义为端口扫描。同一端口，大量资产被扫描定义为系统扫描。



左边来源 ip，中间端口，右边目标 ip，

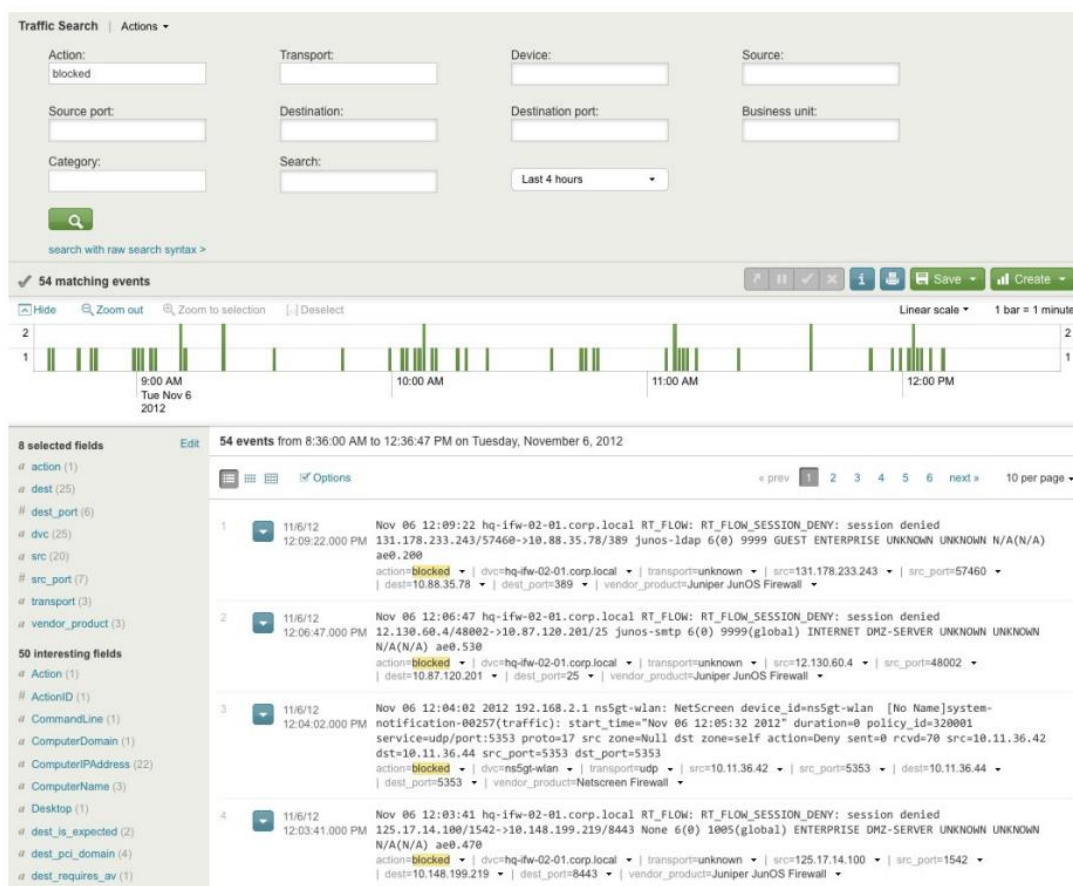


2.2. 流量搜索频道??

概述：显示所有防火墙事件的总体情况。比如查看某一资产的所有防火墙日志，哪些端口被访问过，端口涉及的系统服务有哪些。

数据：防火墙日志。

字段：资产设备，来源 ip，来源端口，目标 ip，目标端口，动作行为，时间区间
展现：



2.3. 入侵监控频道

概述：入侵监控频道显示所有网络入侵事件的总体概况。监控 IDS 事件，评估资产安全趋势状态。

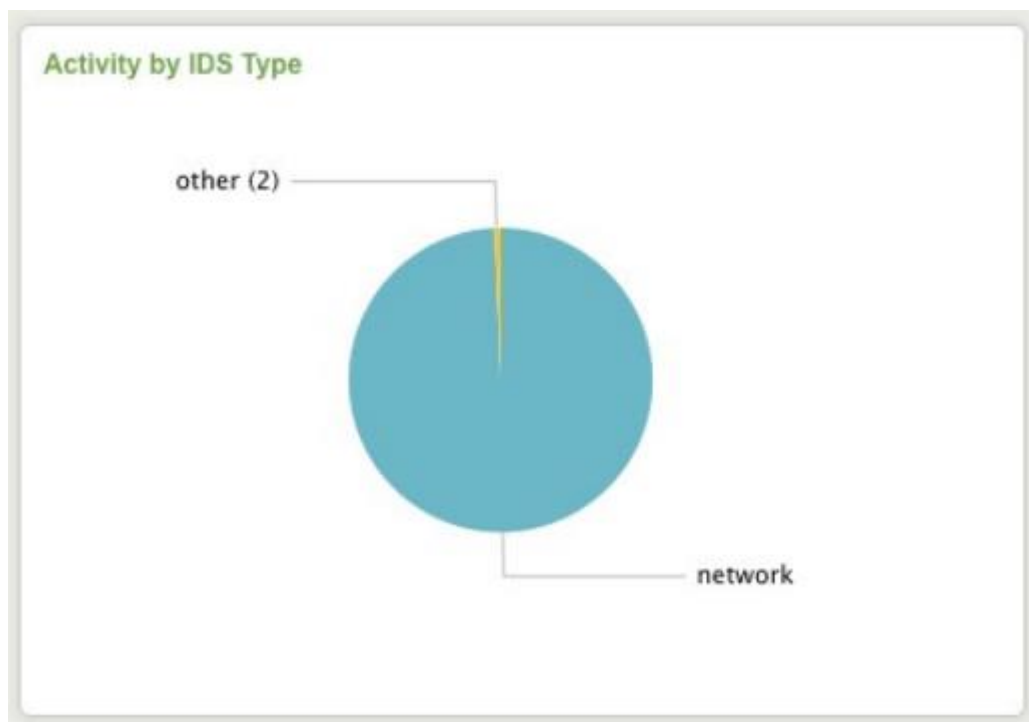
数据：IDS, IPS, waf, web 日志。

2.3.1 IDS 事件分布监控图

功能：显示 IDS 事件的分布情况

字段：应用（web, 数据库, ftp, 邮件服务器等），主机，网络（交换机, 路由器, 防火墙），无线

展现：饼状图

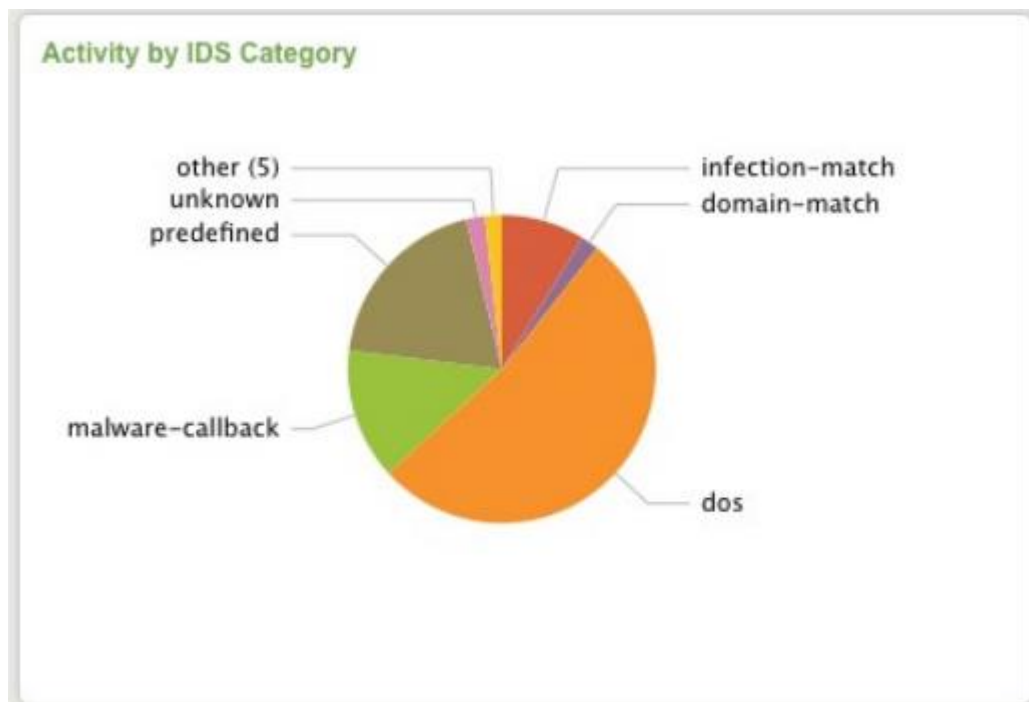


2.3.2 IDS 事件类型监控图

功能：显示入侵类型

字段：DOS 攻击事件，恶意软件攻击事件，预定义事件，感染事件，未知事件等

展现：饼状图



2.3.5 IDS 时间线监控图

功能：显示 IDS 事件的总体数量，检测突然增长的事件

字段：IDS 事件数，资产设备，攻击事件类型，时间线

展现：

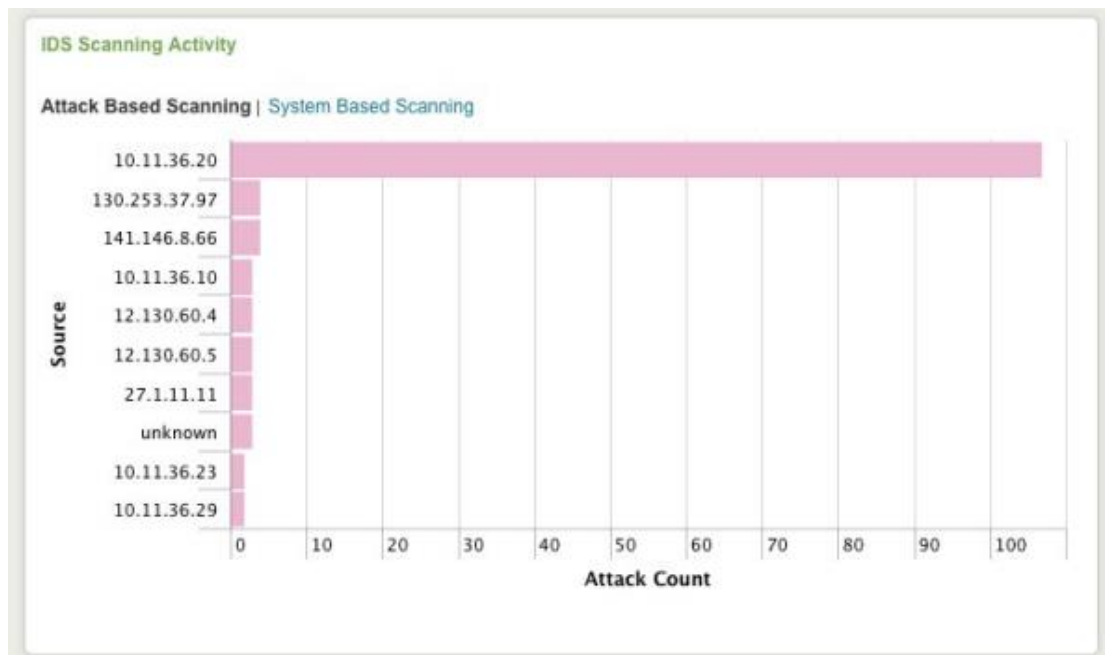


2.3.6 IDS 扫描事件监控图

功能：从系统和攻击两个维度显示 IDS 扫描事件

字段：攻击次数，来源 ip，资产

展现：



2.3.7 首次攻击事件监控图

功能：显示第一次被捕获到的攻击事件。新的攻击向量表明可能有新型的安全威胁，优先级比多年经常出现的高。

字段：时间，攻击特征，严重性程度，目标地址数量

展现：

firstTime	signature	severity	dest_count
11/06/2012 12:10:35	dns:wpadreg	medium	1
11/06/2012 12:09:35	dns:audit.type-all	medium	1
11/06/2012 12:09:21	dns:overflow.txtrecord	medium	1
11/06/2012 12:08:49	im: msn (.net) messenger alive	low	1
11/06/2012 12:05:46	dns:too-many-errors	medium	1
11/06/2012 12:05:13	db:mysql:select-sub-dos	medium	1
11/06/2012 11:11:01	dos:netdev:d-link-dns-320	medium	2
11/06/2012 11:10:49	dos:netdev:hp-lcd-mod-9100	medium	1
11/06/2012 11:10:19	login session opened	informational	1
11/06/2012 11:10:11	dns:audit.type-unknown	medium	1

2.4. 弱点监控中心

概述：提供展现弱点扫描事件概况。主要被管理员用于检测解决系统弱点，以及预警新型安

全漏洞威胁

数据：弱点扫描器报告

2.4.1 弱点概况监控图

功能：以时间线显示弱点在资产的总体分布。

数据：弱点数，时间戳，资产 ip

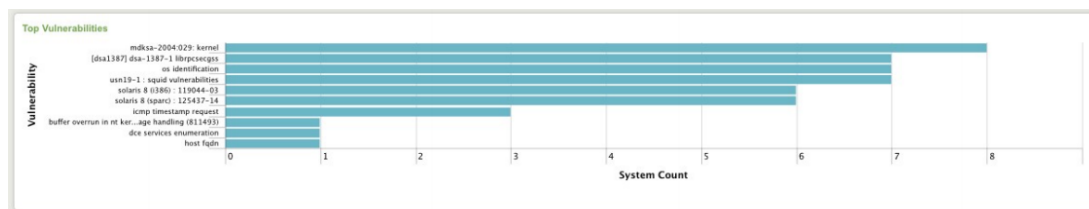
展现：横向折线图

2.4.2 Top 弱点监控图

功能：显示弱点扫描器报告的最常见漏洞。

字段：弱点，有弱点资产

展现：

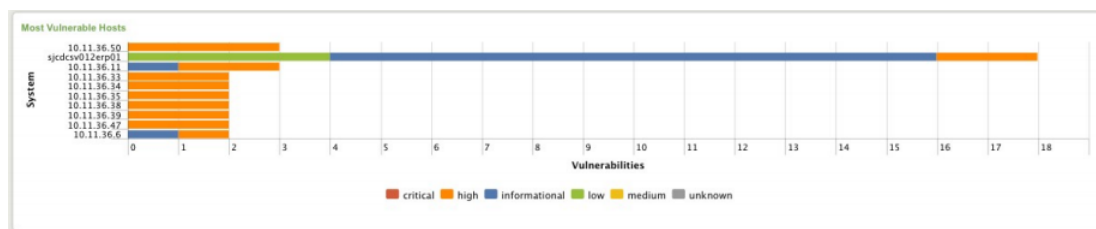


2.4.3 Top 弱点资产

功能：显示弱点最多的资产。

字段：资产 ip，弱点分级。弱点数。

展现：



2.4.4 弱点存活时间

功能：显示存在时间比较久的弱点。

字段：弱点，时间

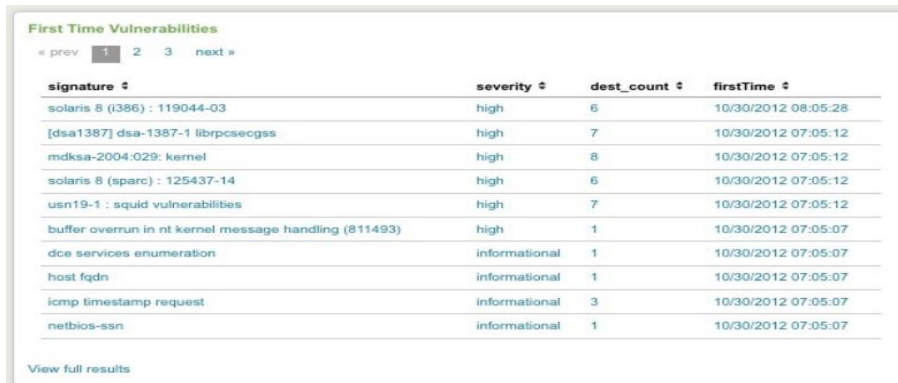
展现：横向柱状图

2.4.5 首次弱点发现

功能：显示第一次被检测到的弱点

字段：弱点，严重性，目标资产数，首次发现时间

展现：



signature	severity	dest_count	firstTime
solaris 8 (386) : 119044-03	high	6	10/30/2012 08:05:28
[dsa1387] dsa-1387-1 libpcsecgss	high	7	10/30/2012 07:05:12
mdksa-2004-029: kernel	high	8	10/30/2012 07:05:12
solaris 8 (sparc) : 125437-14	high	6	10/30/2012 07:05:12
usn19-1 : squid vulnerabilities	high	7	10/30/2012 07:05:12
buffer overrun in nt kernel message handling (811493)	high	1	10/30/2012 07:05:07
dce services enumeration	informational	1	10/30/2012 07:05:07
host fqdn	informational	1	10/30/2012 07:05:07
icmp timestamp request	informational	3	10/30/2012 07:05:07
netbios-ssn	informational	1	10/30/2012 07:05:07

2.4.6 弱点中断

功能：显示弱点扫描中断的资产设备，帮助检测是否因硬件环境或者是配置问题导致弱点扫描失败。

字段：资产，首次扫描时间，最后一次扫描时间，终止时间。

展现：



dest	firstTime	lastTime	dayDiff
10.11.36.32	10/30/2012 07:05:12	10/30/2012 07:05:12	0.25
10.11.36.5	10/30/2012 07:05:30	10/30/2012 07:05:30	0.25
10.11.36.23	10/30/2012 08:05:28	10/30/2012 08:05:28	0.21
10.11.36.31	10/30/2012 08:05:28	10/30/2012 08:05:28	0.21
10.11.36.41	10/30/2012 08:05:28	10/30/2012 08:05:28	0.21
10.11.36.8	10/30/2012 08:05:28	10/30/2012 08:05:28	0.21
10.11.36.1	10/30/2012 09:05:34	10/30/2012 09:05:34	0.17
10.11.36.26	10/30/2012 09:05:34	10/30/2012 09:05:34	0.17
10.11.36.43	10/30/2012 09:05:34	10/30/2012 09:05:34	0.17
10.11.36.6	10/30/2012 09:05:34	10/30/2012 09:05:34	0.17

2.5. 弱点分析频道

概述：显示所有弱点相关事件列表及细节信息。

数据：弱点扫描器报告

字段：弱点类型，严重性，弱点特征，CVE，资产ip，时间戳，资产类型。

展现：

Vulnerability Profiler | Actions ▾

Vuln. category: Severity: Signature: CVE:

Destination: Business unit: Category: Last 30 days ▾

firstTime ▾	lastTime ▾	category ▾	severity ▾	signature ▾	cve ▾	dest ▾
10/24/2012 13:05:50	10/24/2012 13:05:50	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.23
10/24/2012 13:05:50	10/24/2012 13:05:50	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.2
10/24/2012 12:05:39	10/24/2012 12:05:39	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.32
10/24/2012 12:05:39	10/24/2012 12:05:39	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.38
10/24/2012 11:05:32	10/24/2012 11:05:32	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.45
10/24/2012 11:05:32	10/24/2012 11:05:32	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.16
10/24/2012 10:05:26	10/24/2012 10:05:26	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.38
10/24/2012 10:05:26	10/24/2012 10:05:26	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.19
10/24/2012 09:05:19	10/24/2012 09:05:19	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.50
10/24/2012 09:05:19	10/24/2012 09:05:19	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.1
10/24/2012 08:05:07	10/24/2012 08:05:07	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.18
10/24/2012 08:05:07	10/24/2012 08:05:07	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.6
10/24/2012 07:05:00	10/24/2012 07:05:00	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.14
10/24/2012 07:05:00	10/24/2012 07:05:00	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.48
10/24/2012 07:04:20	10/24/2012 07:04:46	unknown	high	solaris 8 (j386) : 119044-03		10.11.36.48
10/24/2012 07:04:20	10/24/2012 07:04:46	unknown	high	solaris 8 (sparc) : 125437-14		10.11.36.41

2.6. 网络配置监控

概述：用于追踪防火墙以及其他网络设备的配置修改情况，帮助检测网络设备因为配置导致的安全问题。

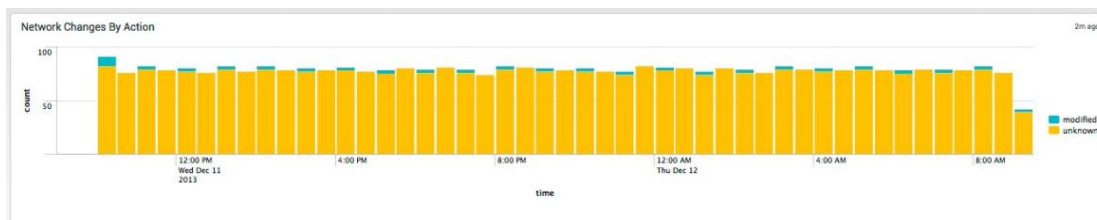
数据：网络设备日志

2.6.1 根据配置改变动作

功能：显示配置修改动作分布

字段：时间，改变行为（修改，增加，删除，未知）事件数量

展示：

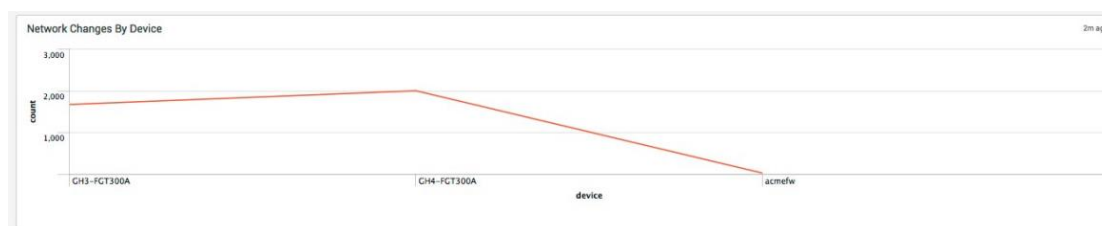


2.6.2 根据配置改变设备

功能：显示设备配置改动分布

字段：时间，资产设备，事件数量

展示：



2.7. 端口协议监控

概述：基于平台规则，监控授权和未经授权的端口及协议访问事件，检测不合规的网络传输事件。

数据：路由器，交换机，防火墙日志

2.7.1 端口活动

功能：显示最近使用的网络端口情况。如果检测到有未曾使用过的端口突然被使用，可能表示有安全威胁，很多木马或是恶意程序会自发打开一个生僻的端口用于和外界通信，或是远程控制。

字段：协议，端口，端口状态（approved,unapproved,pending,Any）,首次活动时间，最后一次活动时间。

展现：

First Time Port Activity					
Show first time port activity within the last <input type="text" value="7"/> days					
transport	dest_port	dest_port_status	firstTime	lastTime	
1	tcp	9997	approved	11/06/2012 11:01:45	11/06/2012 14:02:43
2	tcp	80	approved	11/06/2012 04:19:47	11/06/2012 14:07:14
3	unknown	137	approved	11/06/2012 04:08:17	11/06/2012 14:13:03
4	unknown	123	approved	11/06/2012 04:07:05	11/06/2012 14:08:20
5	unknown	139	approved	11/06/2012 04:04:30	11/06/2012 14:06:34
6	unknown	53	approved	11/06/2012 04:04:09	11/06/2012 14:12:21
7	udp	53	approved	11/06/2012 04:04:06	11/06/2012 14:10:20
8	http	80	approved	11/06/2012 04:02:49	11/06/2012 14:07:15
9	unknown	80	approved	11/06/2012 04:02:47	11/06/2012 14:07:30
10	dns	53	approved	11/06/2012 04:02:43	11/06/2012 14:09:52

3. 资产账户审计

3.1. 资产审计频道

概要：提供接入资产信息的审计状态

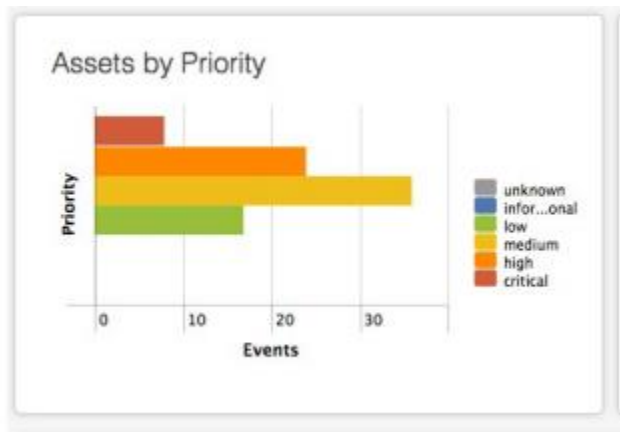
数据：数据库

3.1.1 根据优先级

功能：显示资产优先级分布

字段：优先级，资产数

展示：横向柱状图

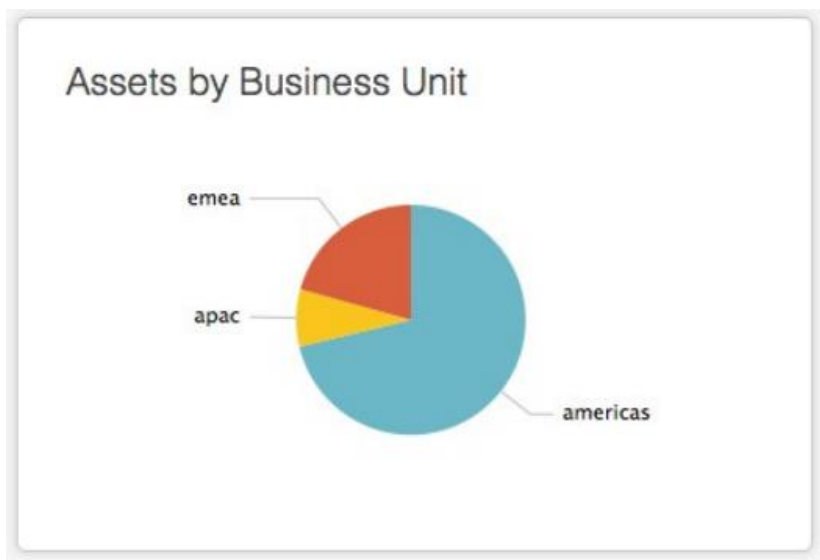


3.1.2 根据业务区域

功能：根据业务区域显示分布

字段：业务区域

展现：饼图

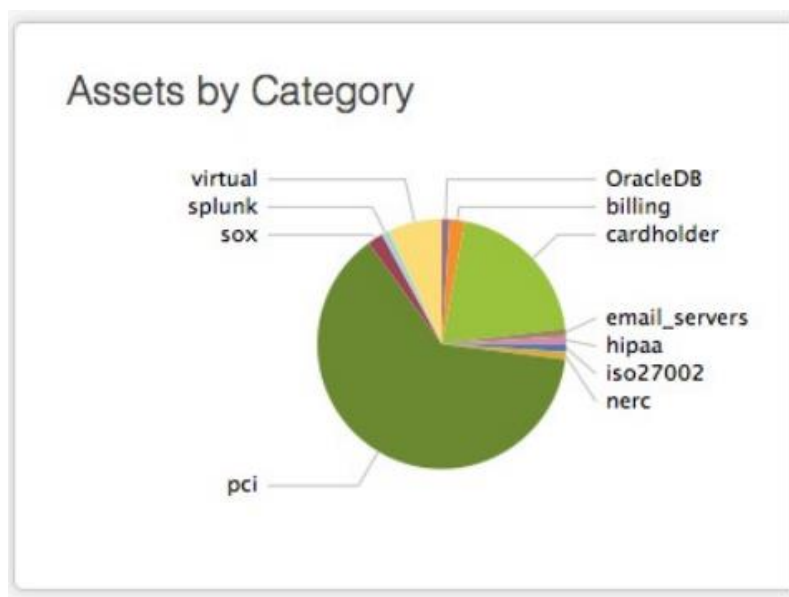


3.1.3 根据功能分类

功能：根据资产类别显示

字段：资产类别

展现：饼图



3.1.4 根据具体信息

功能：显示资产的具体信息

字段：ip, host, mac, 所有人, 地址, 类别

Asset Information												
dns	nt_host	ip	mac	owner	priority	city	country	lat	long	bunit	category	pci_domain
		6.0.0.1-9.0.0.0			low	Istanbul	TR	41.040855	28.986183	apac		untrust
		1.2.3.4	00:15:70:91:df:6c		medium	Washington D.C.	USA	38.959405	-77.04	americas		untrust
CORP1.acmetech.com					high	Pleasanton	USA	37.694452	-121.894461	americas	pci	trust
	storefront	192.168.12.9-192.168.12.9			critical	Dallas	USA	32.931277	-96.818167	americas	pci	trust
		2.0.0.0/8			low	Havant	UK	50.84436	-0.98451	emea	pci	dmz
		192.168.15.8-192.168.15.10			medium	Washington D.C.	USA	38.959405	-77.04	americas	pci	trust
		192.168.0.0/16			high	Pleasanton	USA	37.694452	-121.894461	americas	iso27002	untrust
	millenium-falcon	5.6.7.8	00:12:c7:30:27:b5		critical	Dallas	USA	32.931277	-96.818167	americas	nerc	untrust
	acmefileserv	192.168.15.9-192.168.15.9			low	Havant	UK	50.84436	-0.98451	emea	pci	trust
		192.168.15.9-192.168.15.27			medium	Washington D.C.	USA	38.959405	-77.04	americas		untrust

3.2. 账户审计频道

概要：提供所有平台相关人员的审计信息

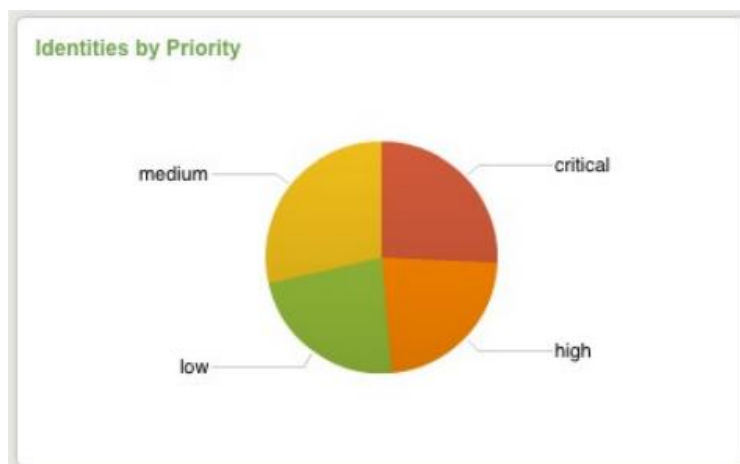
数据：数据库

3.2.1 根据优先级

功能：根据账户优先级显示分布

字段：优先级（低，中，高，严重）

展现：饼图

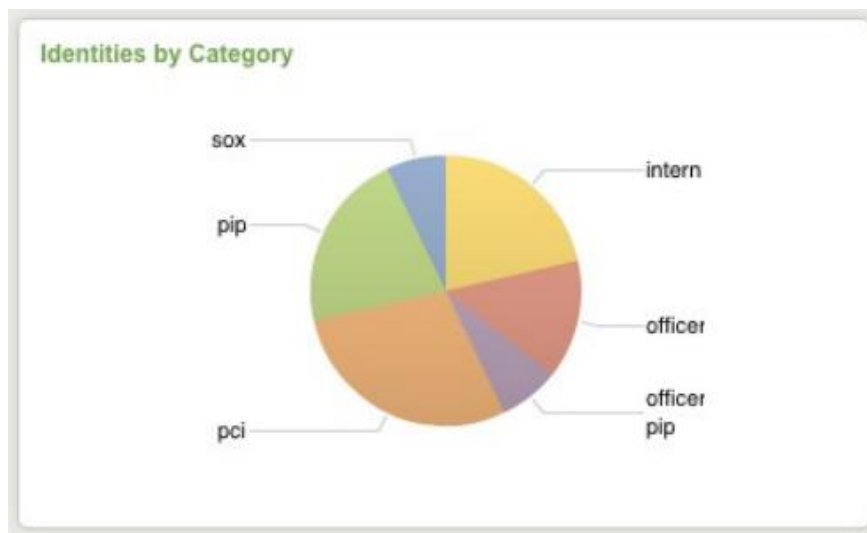


3.2.2 根据账户权限

功能：显示账户权限分布

字段：权限

展现：饼图

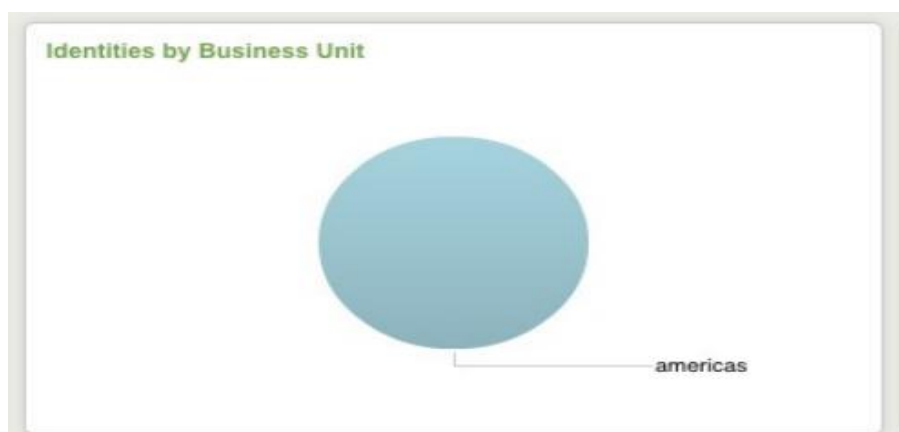


3.2.3 根据业务区域

功能：根据业务区域显示分布

字段：业务区域

展现：饼图



3.2.4 根据具体信息

功能：显示账户的具体信息。

字段：账户 ID，昵称，姓名，邮箱，汇报对象，电话，业务区域，账户生效时间，账户注销时间。

展现：

identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category	watchlist	startDate	endDate
1 mawe mawe@acmetech.com	Mr.		Martin	Awe		mawe@acmetech.com	+1 (800)555-1562	+1 (800)555-3327		critical	americas			5/1/03 0:17	
2 rmajcher rmajcher@acmetech.com		Nene	Ranee	Majcher		rmajcher@acmetech.com	+1 (800)555-8762	+1 (800)555-8549			americas			9/15/96 1:55	
3 ejennifer ejennifer@acmetech.com	Ms.		Elouise	Jennifer		ejennifer@acmetech.com	+1 (800)555-7388	+1 (800)555-2669			americas			3/13/74 6:31	
4 lkerst lkerst@acmetech.com	Mrs.		Larisa	Kerst		lkerst@acmetech.com	+1 (800)555-4897	+1 (800)555-4311	pepper	low	americas			12/12/04 17:31	
5 mpickle mpickle@acmetech.com	Miss		Miki	Pickle		mpickle@acmetech.com	+1 (800)555-5501	+1 (800)555-7321		medium	americas	pci		8/29/99 2:51	
6 aseykoski pepper a.koski aseykoski@acmetech.com	Dr.	Al	Allen	Seykoski		aseykoski@acmetech.com	+1 (800)555-2111	+1 (800)555-9996		high	americas			7/12/03 15:30	7/12/08 19:49
7 rmckitrick rmckitrick@acmetech.com			Renda	Mckitrick		rmckitrick@acmetech.com	+1 (800)555-8072	+1 (800)555-2031		critical	americas			10/28/83 0:27	
8 kwillets kwillets@acmetech.com	Ms.		Katharine	Willetts		kwillets@acmetech.com	+1 (800)555-7596	+1 (800)555-4546			americas	intern		2/13/77 23:14	

3.3. 会话审计频道

概要：提供网络会话概要。网络会话经常被用于通过 DHCP 或是 VPN 服务连接某资产或用户。通过这个监控可以查看用户或是资产连接某 ip 的会话状态。

数据：会话连接日志

3.3.1 长会话连接

功能：列出过分长的网络会话事件。会话时间很长可能表明有不安全的网络连接，增加潜在的安全风险。

字段：ip, mac 地址, host, dns, user, 开始时间, 结束时间, 持续时间

展现：横向柱状图

3.3.2 会话时间分布

功能：显示各个会话在各个时间段的分布情况。异常时间的会话表明可能有异常的安全威胁活动。

字段：ip, mac 地址, host, dns, user, 开始时间, 结束时间, 持续时间

展现：点状分布图

3.3.3 最频繁会话

功能：显示最近最频繁会话。

字段：ip, mac 地址, host, dns, user, 开始时间, 结束时间, 持续时间

展现：

ip	mac	nt_host	dns	user	startTime	endTime	duration(hours)
10.168.30.195	unknown	dmc_1420	unknown	latingirlswaag	11/06/2012 15:18:12		
10.178.198.97	unknown	steve_macbook	unknown	tripem74	11/06/2012 15:17:35		
172.168.15.13	03:00:00:00:00:00	bugsbunny	unknown	unknown	11/06/2012 15:15:55		
172.168.15.10	01:00:00:00:00:00	winfish	unknown	unknown	11/06/2012 15:15:49		
172.168.15.12	02:00:00:00:00:00	storefront	unknown	unknown	11/06/2012 15:14:29		
10.186.204.29	unknown	steve_macbook	unknown	laurentw1d	11/06/2012 15:13:04		
172.168.15.13	03:00:00:00:00:00	bugsbunny	unknown	unknown	11/06/2012 15:11:45	11/06/2012 15:15:54	0.07
172.168.15.12	02:00:00:00:00:00	storefront	unknown	unknown	11/06/2012 15:10:23	11/06/2012 15:14:28	0.07
10.151.191.20	unknown	adam_computer	unknown	vestel86	11/06/2012 15:09:50		
10.169.199.125	unknown	adam_computer	unknown	xxrossanneee	11/06/2012 15:08:52		

4. 地理资源审计 (low priority)

概述：提供额外的信息，关联外部安全资源

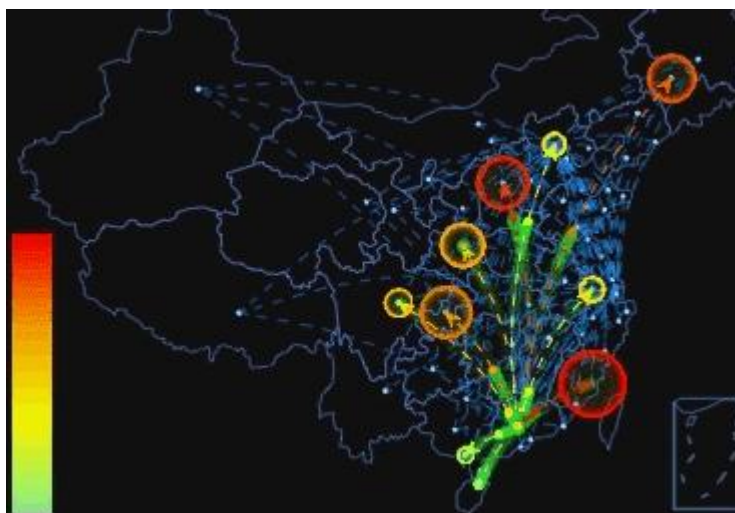
数据：地理日志信息

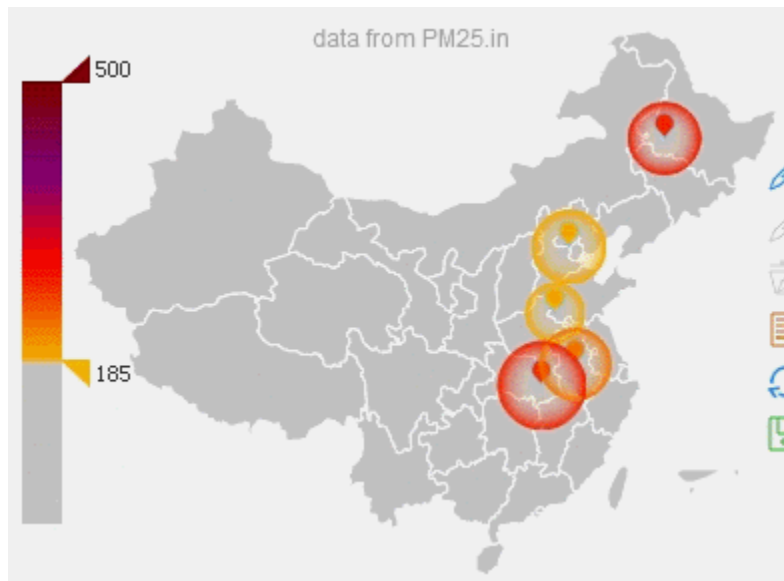
4.1. 地理事件监控

功能：聚集域内所有有地理信息的安全事件，以地图的形式展现。用户可以直观的看到某地的安全事件状态。

字段：来源地址, 目标地址, 安全事件, 流量

展现：





5. 用户操作审计（pending）

5.1. 事件复核审计

功能：对各个事件的复核情况进行统计。需要工单系统等组建支持

5.1.1 根据每个用户

功能：统计每个用户复核事件量。

5.1.2 根据事件重要程度

功能：统计重要事件的复核率

5.1.3 Top 贡献用户

功能：统计经常在操作的用户

5.1.4 最近复核事件

功能：统计最近被复核的事件

5.2. 当前取消事件

功能：对误报的事件，用户可以设置标记进行过滤。需要新组件。

5.3. 事件转发审计

概要：统计和显示资产日志是否正常接入

数据：资产日志状态

5.3.1 无日志接入监控

功能：显示哪些资产没有日志传到 soc

字段：资产，开始时间

展现：列表

5.3.2 日志接入性能监控

功能：监控每个资产日志传送的性能

字段：资产，性能指标，时间

展现：折线图

5.4. 数据完整性审计