

基于机器学习与攻击树的威胁感知方法与实践



充分发挥IPS/IDS价值 提高攻击对抗能力

CCIE CISSP CISA PMP

密级：限制分发

1 IDS/IPS安全运维现状

2 基于机器学习与攻击树的威胁感知

3 实践案例-某企业云平台部署案例



IPS/IDS在1G流量的环境下，一天内会产生多少条告警？

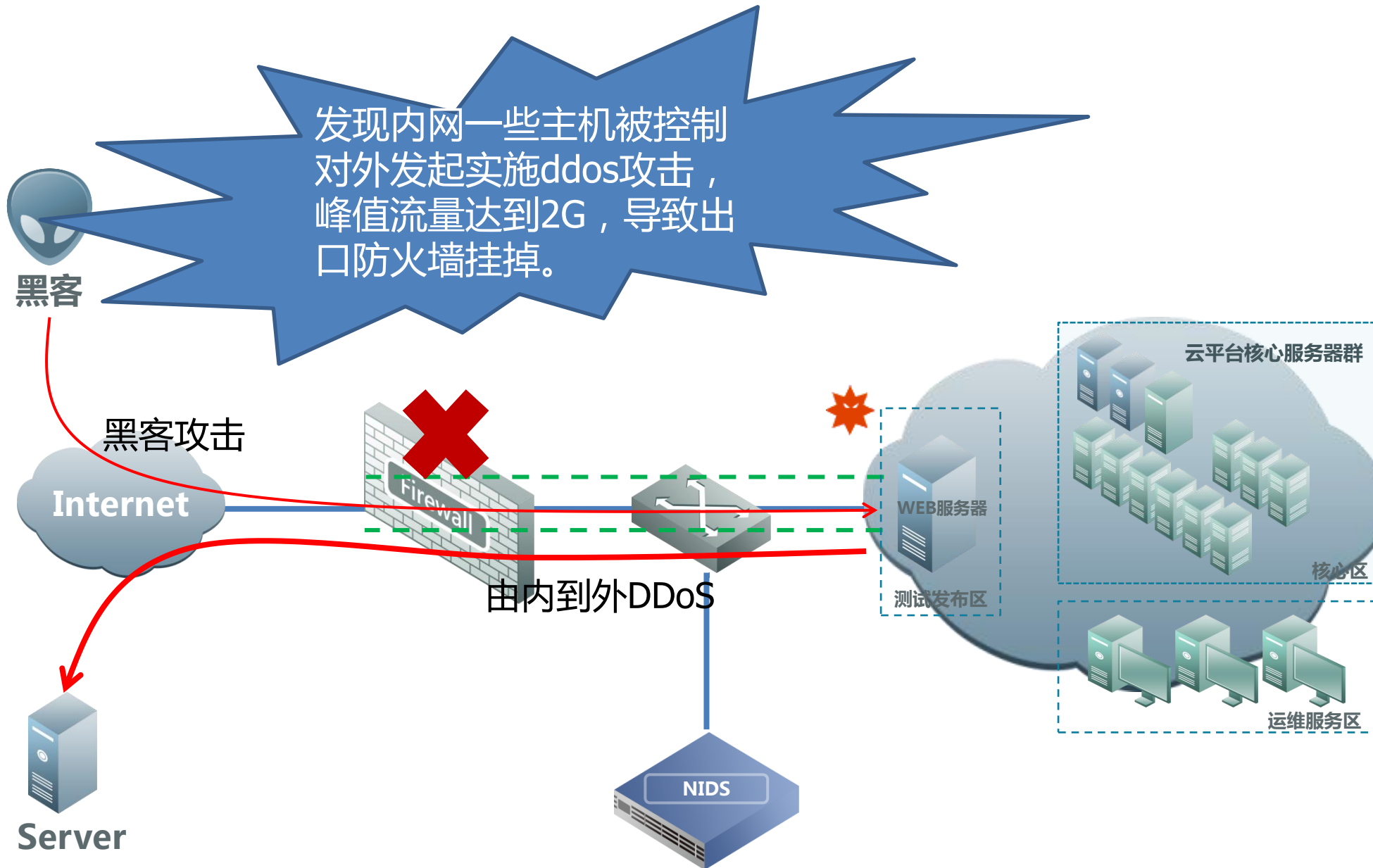
意味着归并后运维人员还需要面对**12万条告警日志**！

近年来随着企业的网络应用越来越复杂、开放，黑客攻击也趋向频繁，造成IPS/IDS此类检测2-7层攻击的安全设备的日志量越来越大

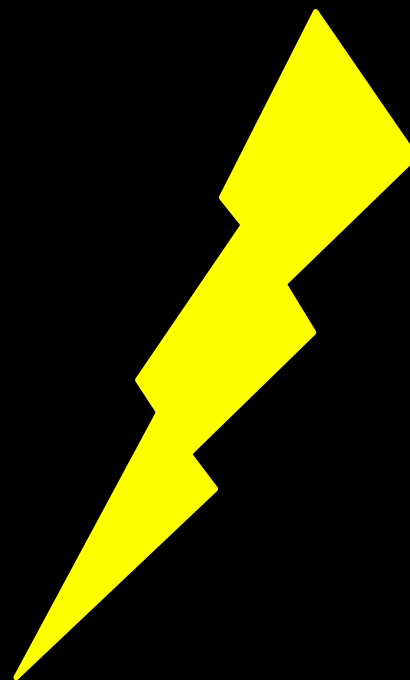


告警举例：

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	60095	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 12:02:49	11



- 一个看似平静的一天，突然整个云平台断网！



实际上在此期间IDS已经检测到黑客攻击主机（主控端）与云平台主机（被控端）之间的恶意通讯指令，如下图的告警信息。

	<input type="checkbox"/>		时间	上报设备	攻击手段	事件名称	事件次数	源IP	目的IP
<input type="checkbox"/>	<input checked="" type="checkbox"/>		2015-04-04 15:13:40	172.40.10.185 (IPS_185)	可疑网络活动	DDOS工具Trinoo客户端向主控端发送默认口令	1	202.104.70.250(广东省)	183.59.9.165(广东省)

由于IDS告警量非常多（1G带宽下，IPS/IDS一天可产生12万条日志），**运维人员平时只关注事件次数排在前十的告警事件**，如下图所示，该重要的告警信息淹没在IDS海量的告警日志中，未能及时发现。

排名	规则编号	事件	事件次数
1	88000	SSH登陆尝试事件	904494
2	88001	主动外联事件	351198
3	50450	SNMP操作使用弱口令	156215
4	40301	SNMP服务试图使用默认public口令访问	156212
5	30522	服务器端口扫描- SYNACK扫描	153622
6	30520	服务器端口扫描- ACK扫描	151438
7	30061	DNS服务服务器版本号请求操作	90075
8	50462	SNMP服务使用非默认的端口	87446
9	40401	MS-SQL数据库用户登录SQL服务器 失败	58067
10	50031	FTP服务普通用户认证成功	24852

某企业门户网站上启用了FTP文件传输服务，用于管理网站文件，但某天该网站上的FTP服务被黑客成功暴力破解，并上传了网马，控制了该企业门户网站，最终获取了该企业的机密信息以及篡改了网站文件。



实际上，IDS已经检测出大量的FTP认证失败事件，属于黑客在FTP暴力破解过程中的行为特征，后续IDS还检测出FTP登陆成功事件，证明黑客已经成功破解出FTP账号密码！

每页显示: 25 条，共37条记录 [首页](#) [上一页](#) [下一页](#) [末页](#) 1/2 页，转到第 页

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	60095	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 12:02:49	11
2	183.29.90.173	42246	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 12:00:47	23
3	183.29.90.173	42214	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:58:42	9
4	183.29.90.173	42205	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:56:33	18
5	183.29.90.173	40588	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:54:33	11
6	183.29.90.173	40569	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:52:21	1
7	183.29.90.173	53410	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:50:04	9

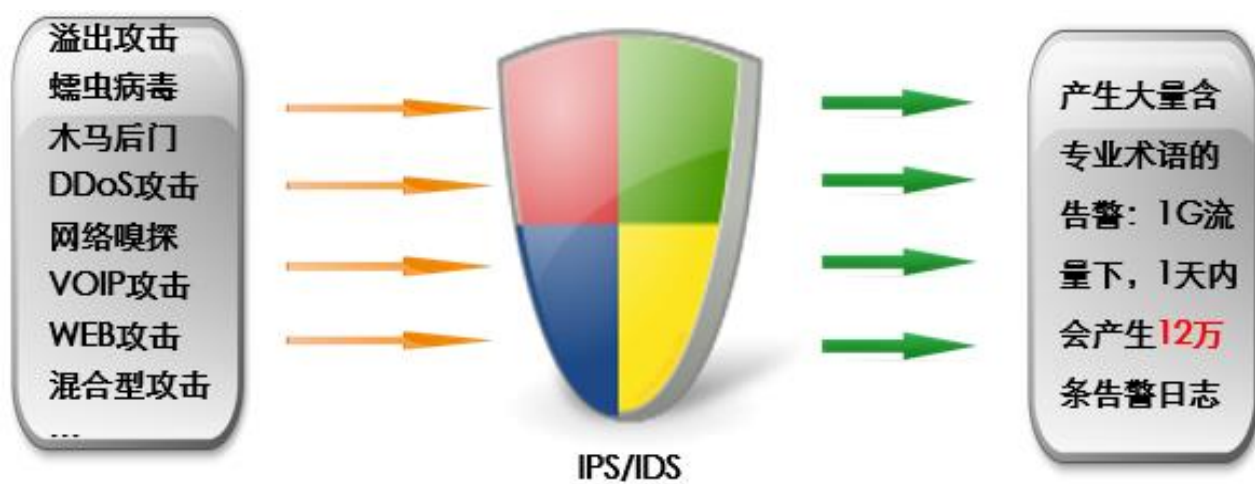
FTP认证失败告警：低风险

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	48794	14.31.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:28:05	1
2	183.29.90.173	57165	14.31.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:15:47	1

FTP认证成功告警：低风险

因为IDS告警量太大，运维人员习惯只关注高风险事件的告警，而对于“FTP认证失败事件”、“FTP服务认证成功事件”，IDS一般会判定为低风险事件。

只有建立在良好的运维环境下，才能确保信息安全，但现状是企业花费不菲的价格购买了**IPS/IDS**却难以充分地发挥出**IPS/IDS**的价值



1. 运维人员可能由于**没有足够的日志分析经验**对大量含有专业术语的告警日志进行关联分析
2. 运维人员可能由于**没有足够的精力**（往往是人手不足）对所有**IDS**告警日志进行分析，有价值的告警容易淹没在海量日志中。

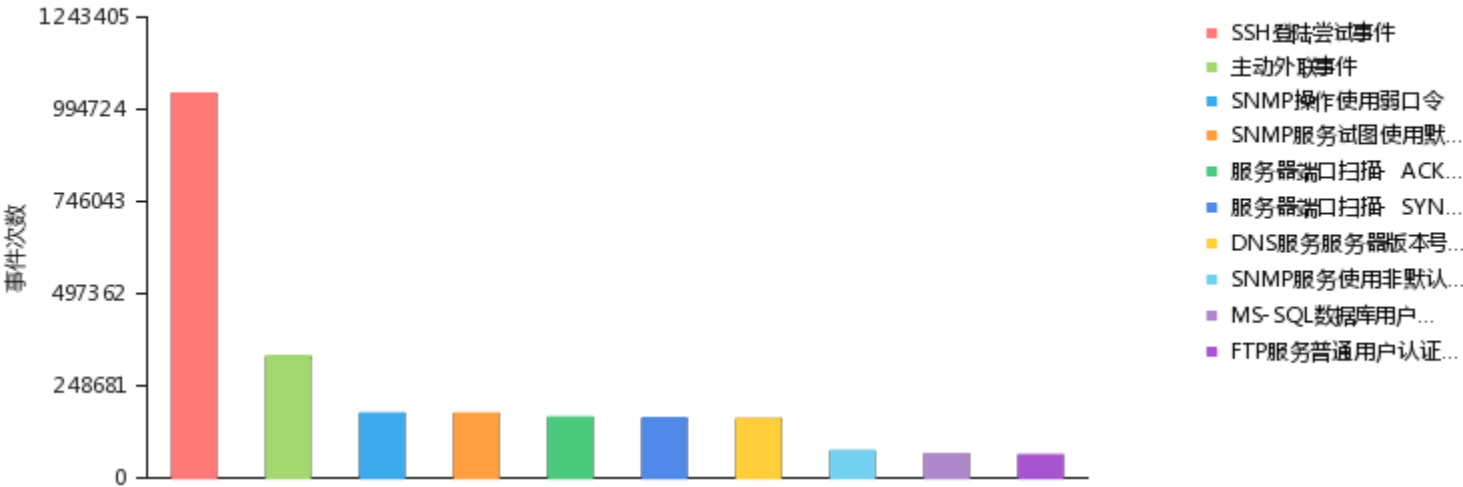
1 IDS/IPS安全运维现状

2 基于机器学习与攻击树的威胁感知

3 实践案例-某企业云平台部署案例

按事件次数排序，只看前十，大部都是一些信息探测事件，会忽略高风险事件

最频繁的10条事件



只查看高中风险安全事件，可是，低风险事件也很重要！

每页显示: 25 条，共37条记录

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	60095	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 12:02:49	11
2	183.29.90.173	42246	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 12:00:47	23
3	183.29.90.173	42214	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:58:42	9
4	183.29.90.173	42205	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:56:33	18
5	183.29.90.173	40588	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:54:33	11
6	183.29.90.173	40569	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:52:21	1
7	183.29.90.173	53410	14.31.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 11:50:04	9

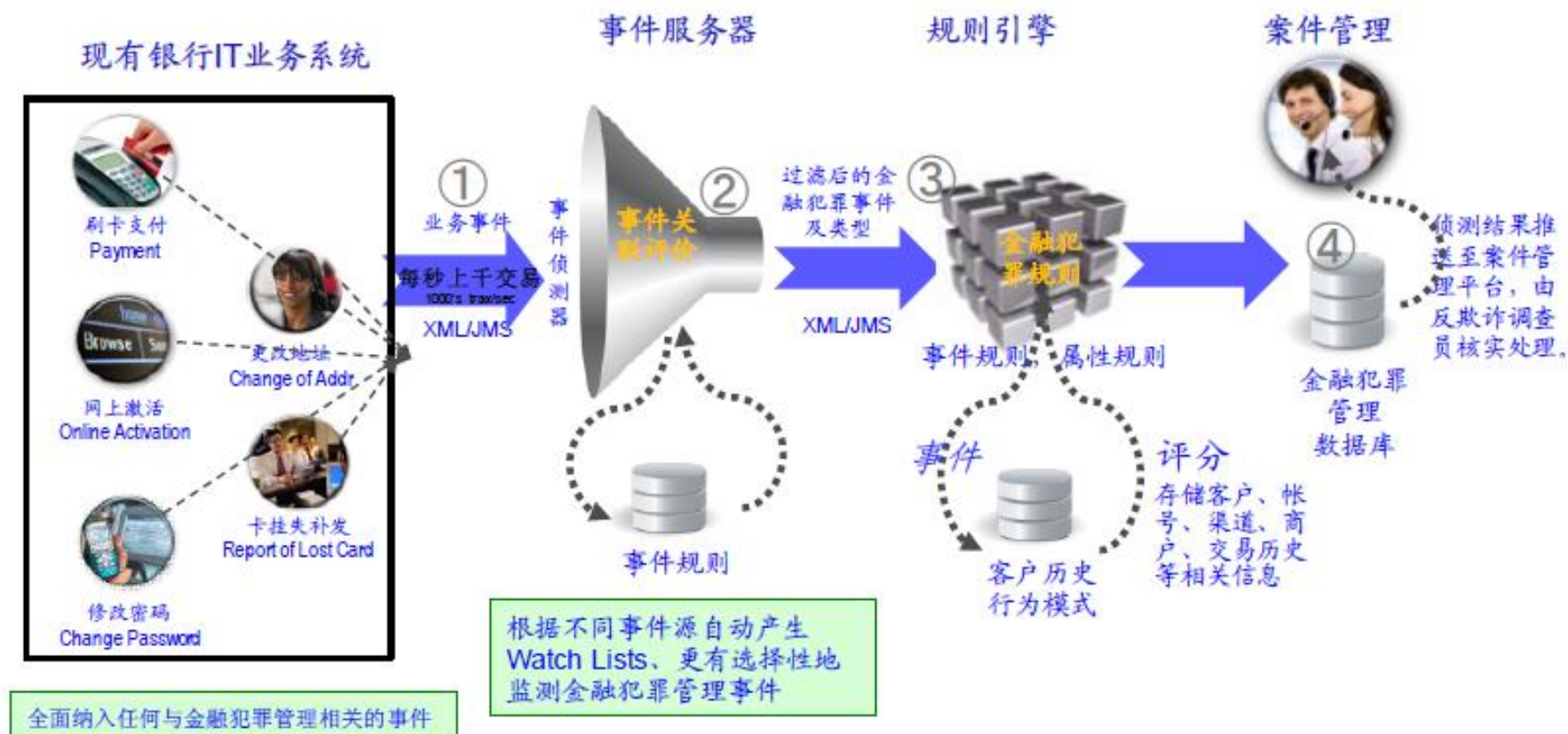
未能发现暴力破解事件

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	48794	14.31.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:28:05	1
2	183.29.90.173	57165	14.31.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:15:47	1

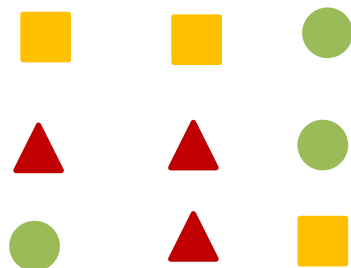
未能发现异常登陆事件

银行面对每秒上千交易量的日志，如何发现交易欺诈行为？

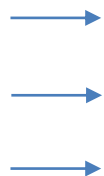
IBM ODM/BPM帮助银行利用大数据实现实时交易反欺诈



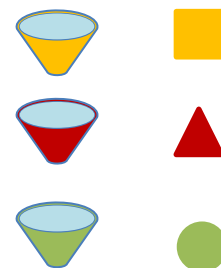
通过机器学习，建立行为规则，高效的发现交易欺诈行为



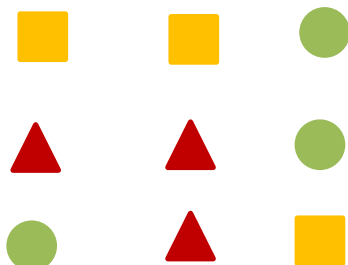
测试数据/历史数据



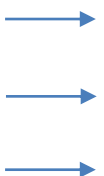
归纳演绎



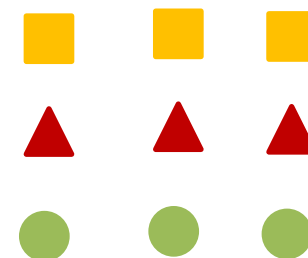
建立模型



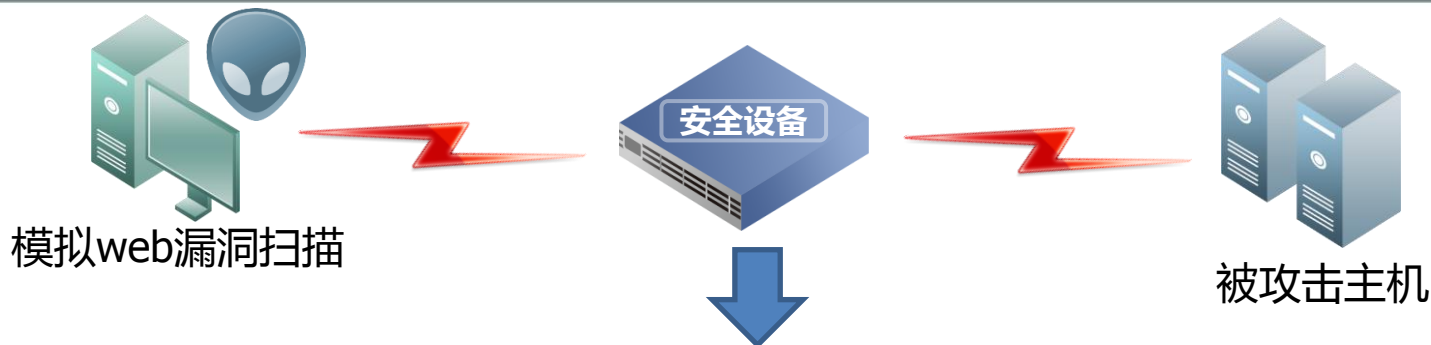
测试数据/历史数据



模型匹配
机器学习



自动分类



web漏洞扫描-原始日志

每页显示: 25 条, 共26条记录 首页 上一页 下一页 末页 1/2 页, 转到第 页

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1		35026		8081	Windows Apache服务器请求路径处理遍历目录攻击	中风险	2014-11-03 23:36:33	1
2		34917		8081	Microsoft FrontPage fp30reg.dll漏洞扫描探测	低风险	2014-11-03 23:36:21	1
3		34815		8081	Web服务远程SQL注入攻击可疑行为	高风险	2014-11-03 23:36:08	1
4		34780		8081	TinyBrowser Plugin for Joomla! upload.php folder参数任意文件上传漏洞	高风险	2014-11-03 23:36:06	1
5		34634		8081	Microsoft IIS 4.0 showcode.asp脚本漏洞扫描探测	低风险	2014-11-03 23:35:58	1

漏洞扫描过程触发一堆专业告警

web漏洞扫描行为告警

每页显示: 25 条, 共122条记录 首页 上一页 下一页 末页 1/5 页, 转到第 页

序号	源IP	目标IP	目标端口	首次时间	最近时间	总攻击次数 / 种类	高风险	中风险	低风险	详情
1			80	2014-11-04 13:18:08	2014-11-04 13:23:14	22 / 22	8	8	6	详情
2			8081	2014-11-03 23:30:46	2014-11-03 23:36:33	26 / 26	9	10	7	详情

可研判为扫描事件, 过程中尝试过多少次高、中、低风险攻击

web漏洞扫描行为告警										
每页显示: 25 条, 共122条记录		首页	上一页	下一页	末页	1/5 页, 转到第 页				
序号	源IP	目标IP	目标端口	首次时间	最近时间	总攻击次数 / 种类	高风险	中风险	低风险	详情
1			80	2014-11-04 13:18:08	2014-11-04 13:23:14	22 / 22	8	8	6	详情
2		2	8081	2014-11-03 23:30:46	2014-11-03 23:36:33	26 / 26	9	10	7	详情

10.82.70.165扫描了122个主机



源IP	目标IP	目标端口	事件描述	首次时间	最近时间	总攻击次数	高风险	中风险	低风险	详情
	,,*,*	***	共扫描了122个IP地址(web扫描)	2014-10-27 19:25:05	2014-11-04 13:23:14	23872	5481	17914	477	详情

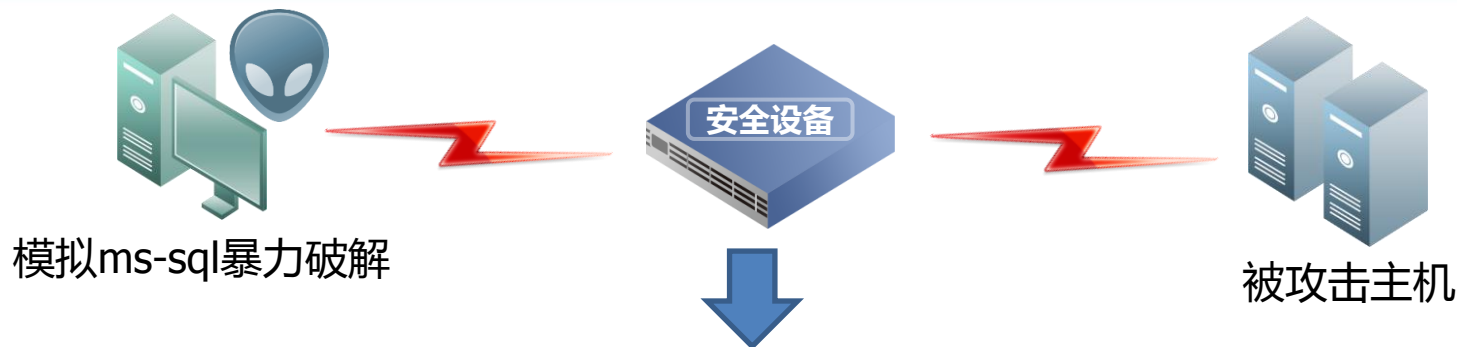
可研判为：一对多的漏洞扫描

高度压缩告警日志

23872条原始日志

122漏洞扫描行为日志

1条正向推理日志



MSSQL暴力破解过程触发一堆专业告警

每页显示: 25 条, 共54条记录 首页 < 上一页 下一页 > 末页 1/3 页, 转到第 页

源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
14.146.226.101	1433	125.227.80.221	12681	服务器端口扫描- SYNACK扫描	中风险	2015-03-26 15:16:39	1
125.227.80.221	22175	14.146.226.101	1433	MS-SQL 数据库用户登录SQL服务器失败	中风险	2015-03-26 15:15:18	211
14.146.226.101	1433	125.227.80.221	12681	服务器端口扫描- SYNACK扫描	中风险	2015-03-26 15:14:13	1
14.146.226.101	1433	125.227.80.221	12681	服务器端口扫描- SYNACK扫描	中风险	2015-03-26 15:14:12	1
125.227.80.221	7738	14.146.226.101	1433	Microsoft SQL 客户端SA用户默认空口令连接	中风险	2015-03-26 15:13:17	1

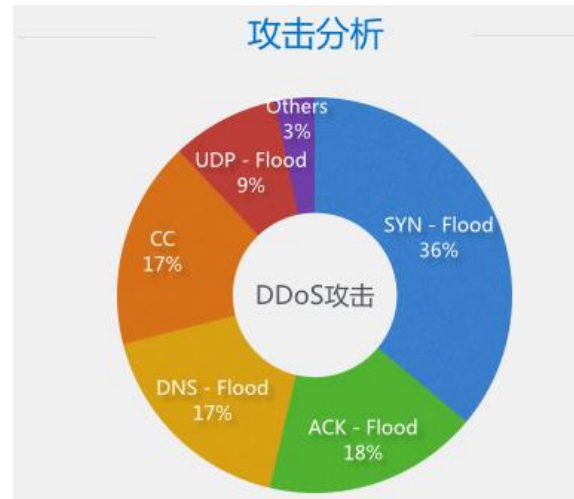
实践是检验真理的唯一标准

可研判为MS-SQL暴力破解事件, 记录首次时间、最近时间、累计次数

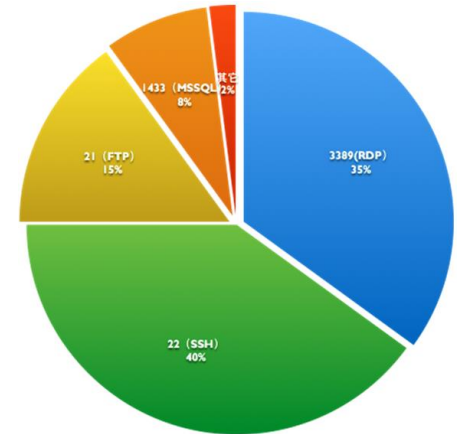
源IP	目标IP	目标端口	攻击名称	首次时间	最近时间	累计攻击数
125.227.80.221	14.146.226.101	1433	MS-SQL暴力破解	2015-03-26 00:45:31	2015-03-26 23:55:46	2509



DDoS与暴力破解趋势



DDoS类型攻击比例



暴力破解类型攻击比例

阿里云安全运营周报关注点

[事件] 一个基于IRC的Botnet僵尸网络
在上周，我们在流量中发现一个异常的情况，根据我们的分析，判断这是一个基于IRC的Botnet流量。

通过域名 **Denver.CO.US.Undernet.Org** 的反查，我们发现，这是一个专门用于僵尸网络控制的恶意域名，用于包括记录并上传用户键盘输入等恶意目的的僵尸网络。通过数据分析，我们获得了控制台和僵尸主机的列表。

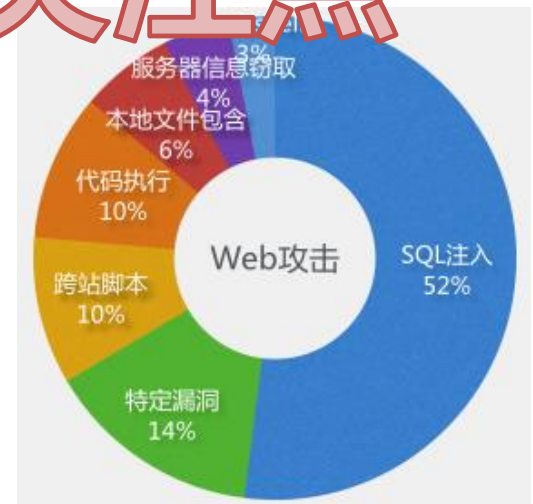
木马、病毒事件

阿里云安全运营团队提醒各位阿里云用户，请您及时做好漏洞修复和安全防范。

更多：<http://bbs.aliyun.com/read/179684.html?spm=5176.7189909.3.11.POpK7E>

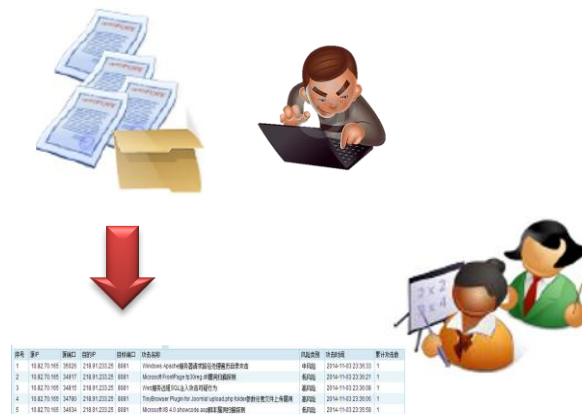
TrueType字体分析特权提升0day漏洞（CVE-2014-4148）和Win32k.sys 特权提权0day漏洞（CVE-2014-4113）

主机漏洞攻击事件



Web攻击事件

黑客攻击过程



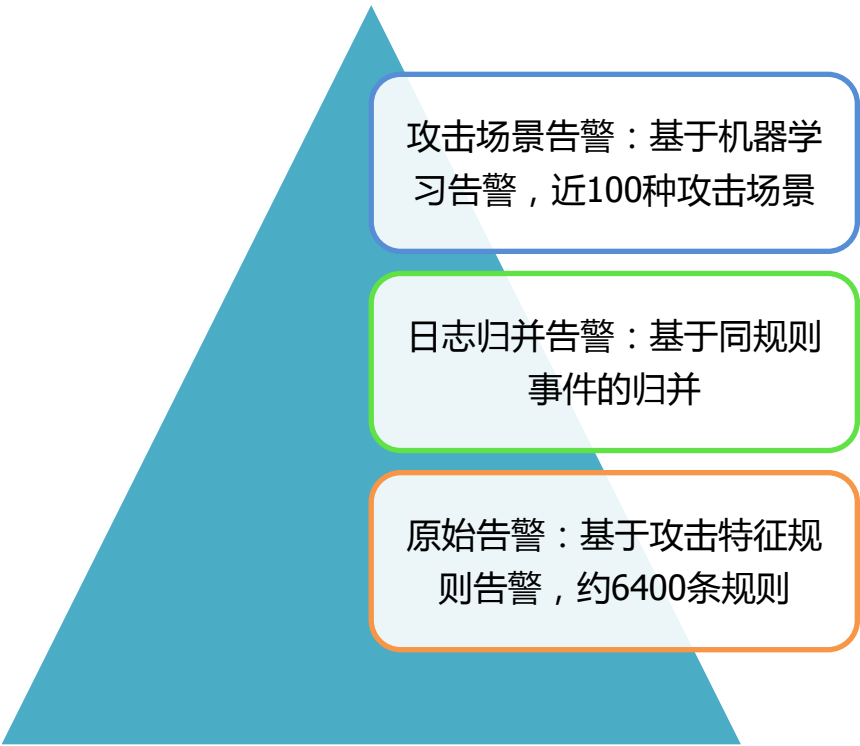
- 1、绿盟安全分析师从历史案件中进行统计分析，找出规律。
- 2、绿盟攻防人员设计**100多个攻击场景**，进行攻击行为建模，找出规律。



将发现的规律转化为行为规则模型和特征规则模型。部署在**入侵威胁感知引擎**中，在海量事件发现可疑事件。

入侵威胁感知系统 ▸ 威胁监控 ▸ 全局视角

监控项	当前	最近1小时	最近24小时	最近7天	最近1月
暴力破解	0	0	108	496	2053
漏洞扫描	0	0	6	19	66
DDoS攻击	0	0	4	22	85
手工入侵	0	0	365	766	2947
异常登陆与远控	0	0	0	0	5
危害与影响	0	0	0	0	1



攻击场景告警：基于机器学习告警，近100种攻击场景

日志归并告警：基于同规则事件的归并

原始告警：基于攻击特征规则告警，约6400条规则

约500条攻击行为告警

约12万条规则告警

约120万次攻击

1G流量下，不同分析层面产生的告警



我们知道了有哪些攻击行为，就可以了？



如何能够进一步促进安全运维决策，提高对抗能力？

能看得懂告警日志 基于机器学习的威胁理解

- 现在网络中存在哪些攻击行为

能够事前预警 基于攻击树的威胁计分

- 安内：哪些资产面临较大攻击威胁，提前加固，防止入侵成功
- 攘外：哪些攻击源威胁较大，提前阻断，防止入侵成功

能够促进事后决策 基于攻击树的反向推理

- 哪些攻击行为已对资产造成影响，黑客如何入侵成功

基于机器学习与攻击树的威胁感知

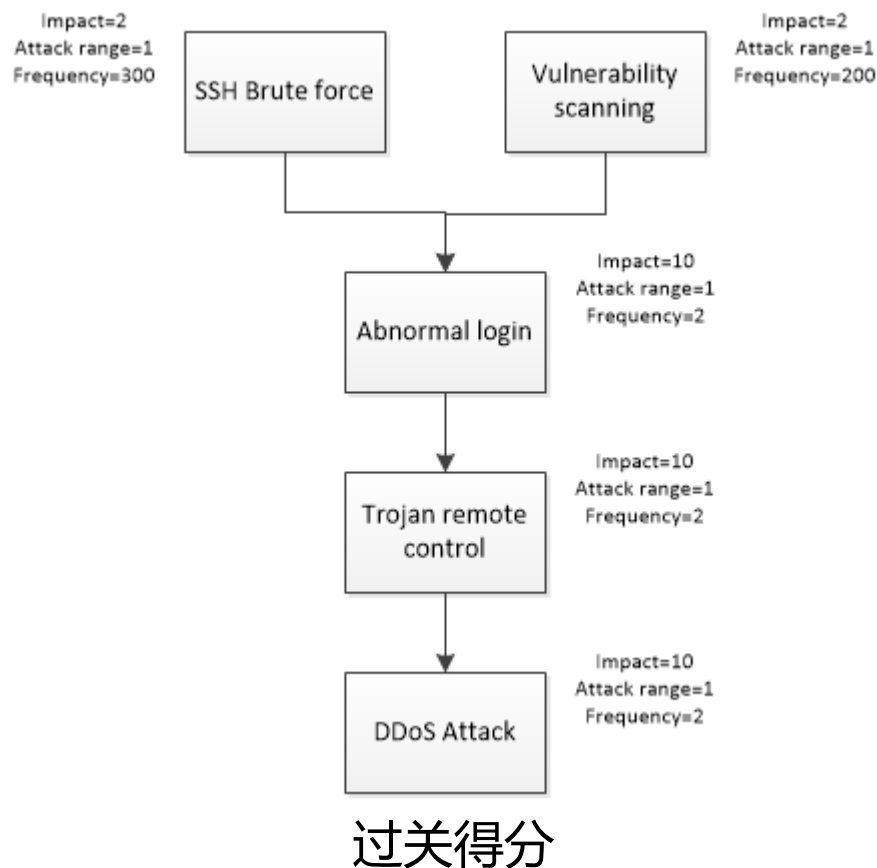
促进对威胁的预警

基于机器学习的威胁理解

基于攻击树的威胁计分

基于攻击树的反向推理

再回首



感知面临威胁较大的
内网IP

- 提前安内，避免
资产被入侵成功

感知攻击威胁较大的
恶意IP

- 提前防外，避免
黑客攻击成功

基于攻击树的威胁计分：在攻击视角情况下，通过分析每个IP的攻击树路径，评估每个IP在攻击树节点产生的攻击危害、攻击烈度、攻击范围评价**攻击IP地址的威胁程度**；被攻击视角用于评价**被攻击IP地址的面临威胁的程度**。

预警威胁较大的攻击源，关联专家知识库，提供安全建议。

攻击源威胁感知

序号	攻击源IP	影响IP数	攻击次数	攻击种类	详情
1	202.104.70.250	706	22503	10	详情
攻击源IP202.104.70.250攻击了706个IP,尝试了10种攻击类型。 分别为：1.FTP暴力破解；2.MS-SQL暴力破解；3.SSH暴力破解；4.http基本认证暴力破解；5.mysql暴力破解；6.telnet暴力破解；7.web攻击入侵行为；8.web漏洞扫描；9.主机攻击入侵行为；10.主机漏洞扫描； 建议：将该源IP列入黑名单，近7天内禁止该源IP地址的访问					
2	192.168.1.1	36	3064	5	详情
3	192.168.1.1	7	130	4	详情
4	192.168.1.1	26	2277		
5	192.168.1.1	22	1831		
6	192.168.1.1	27	1272		
7	192.168.1.1	11	239		
8	192.168.1.1	10	191		
9	192.168.1.1	19	1287		
10	192.168.1.1	106	4587		

被攻击目标威胁感知

序号	被攻击IP	攻击源IP地址数	被攻击次数	攻击种类	详情
1	14.31.15.109	281603	357082	4	详情
被攻击IP14.31.15.109遭受281603个IP的攻击,共面临了4种攻击类型。 分别为：1.FTP暴力破解；2.web攻击入侵行为；3.主机攻击入侵行为；4.主机漏洞扫描； 建议：对该主机进行漏洞扫描评估以及相应的加固工作，避免黑客入侵成功。					
2	192.168.1.1	262457	312511	5	详情
3	192.168.1.1	109043	121880	5	详情
4	192.168.1.1	97744	100825	2	详情
5	192.168.1.1	23041	2364433	4	详情
6	192.168.1.1	19522	155216	4	详情
7	192.168.1.1	19514	20450	4	详情
8	192.168.1.1	19503	154540	1	详情
9	192.168.1.1	19498	149330	4	详情
10	192.168.1.1	19464	96599	4	详情

预警面临威胁较的资产，关联专家知识库，提供安全建议。

基于机器学习与攻击树的威胁感知

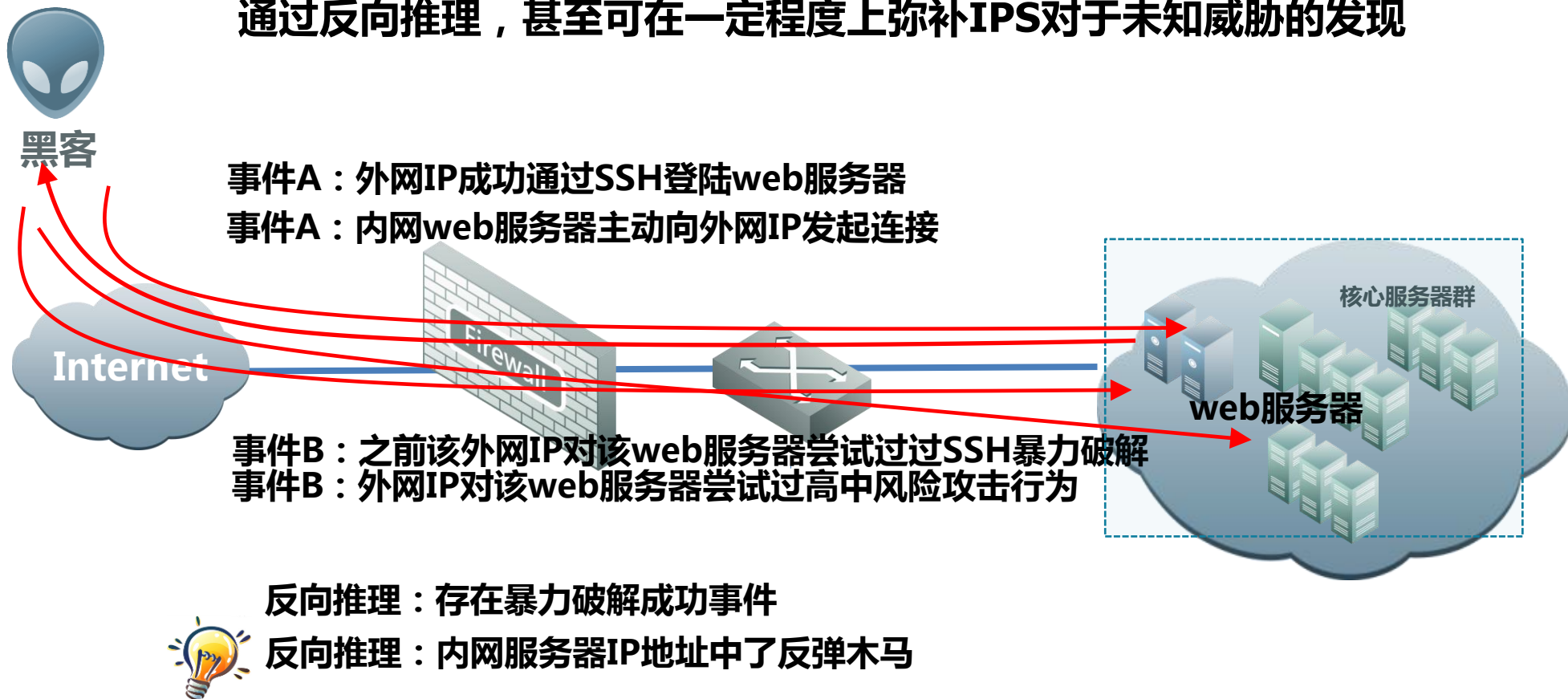
促进对威胁的预警

基于机器学习的威胁理解

基于攻击树的威胁计分

基于攻击树的反向推理

再回首



挖掘出入侵成功的行为

序号	源IP	目标IP	目标端口	攻击描述	首次时间	最近时间	攻击次数	详情
1			***	非法外联事件 目标IP对源IP尝试过高风险攻击	2014-11-13 11:01:52	2014-11-13 11:01:52	11	详情
2			22	ssh异常登陆事件, 登陆用户:root	2014-11-11 17:59:08	2014-11-12 20:40:27	2	详情
3			21	FTP暴力破解成功, 被破解账号:administrator	2014-11-12 10:51:57	2014-11-12 10:51:57	1	详情
4			3389	RDP异常登陆事件, 登陆用户:Administrator	2014-11-11 17:12:02	2014-11-12 10:50:50	2	详情
5			22	SSH暴力破解成功, 被破解账号:test	2014-11-11 18:01:56	2014-11-11 21:33:49	3	详情
6		*.*.*.*	80	正连僵尸网络 (控制了2个IP)	2014-11-10 18:48:10	2014-11-10 18:51:52	2	详情

异常登陆与远控事件

挖掘出入侵成功后造成的危害与影响行为

序号	源IP	目标IP	攻击描述	首次时间	最近时间	总攻击次数	高风险	中风险	低风险	详情
1	*.*.*.*		溢出攻击成功后添加用户 system用户创建了新用户:dreamklin	2014-11-13 11:03:32	2014-11-13 11:03:32	1	1	0	0	详情
2			内到外攻击行为	2014-11-13 11:01:51	2014-11-13 11:01:52	3	2	1	0	详情

危害与影响事件

基于机器学习与攻击树的威胁感知

促进对威胁的预警

基于机器学习的威胁理解

基于攻击树的威胁计分

基于攻击树的反向推理

再回首

威胁感知（web平台展示）

基于攻击推理树的
威胁预警



可决策的专家研判日志

数据挖掘（机器学习）

基于机器学习的
威胁理解



易理解的行为日志

数据仓库（分布式数据采集）

威胁检测

威胁要素获取



海量含专业术语的原始日志

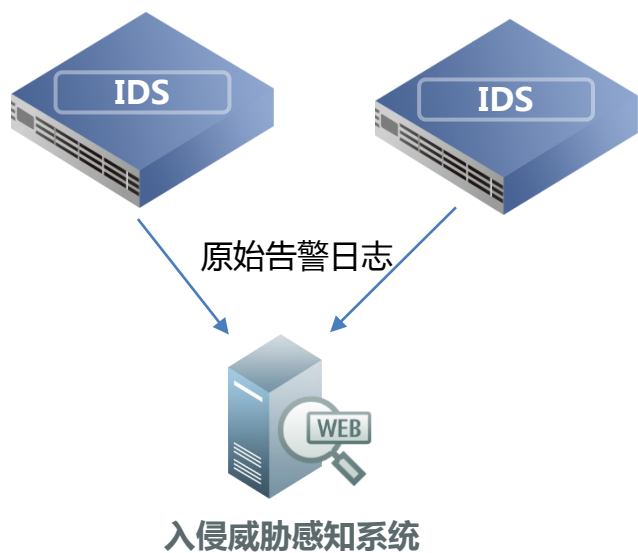
入侵威胁防御系统

IPS

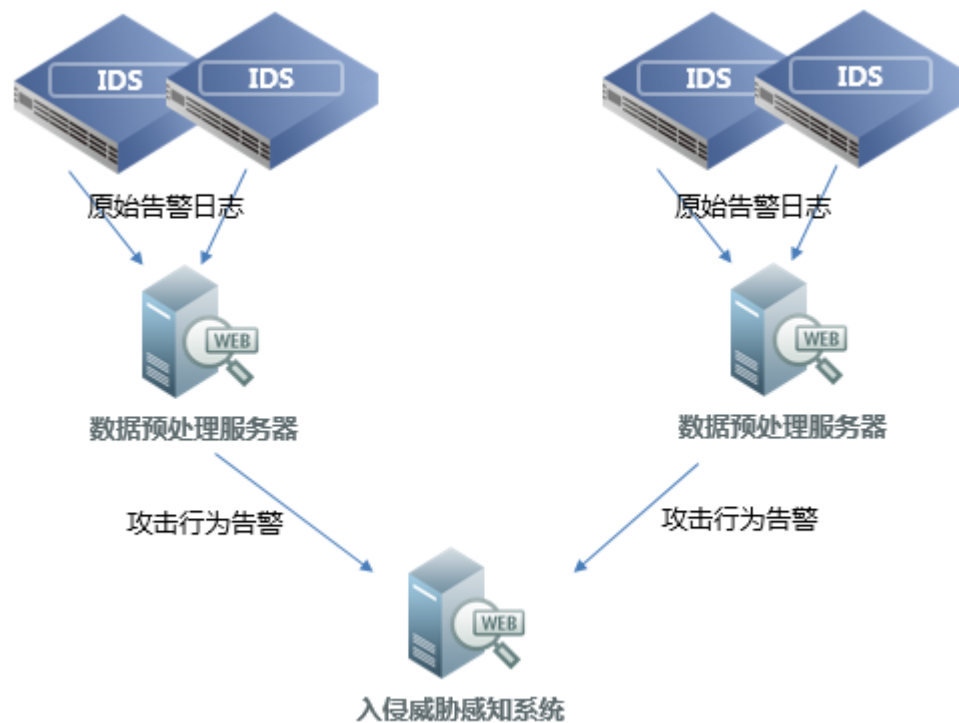
入侵威胁检测系统

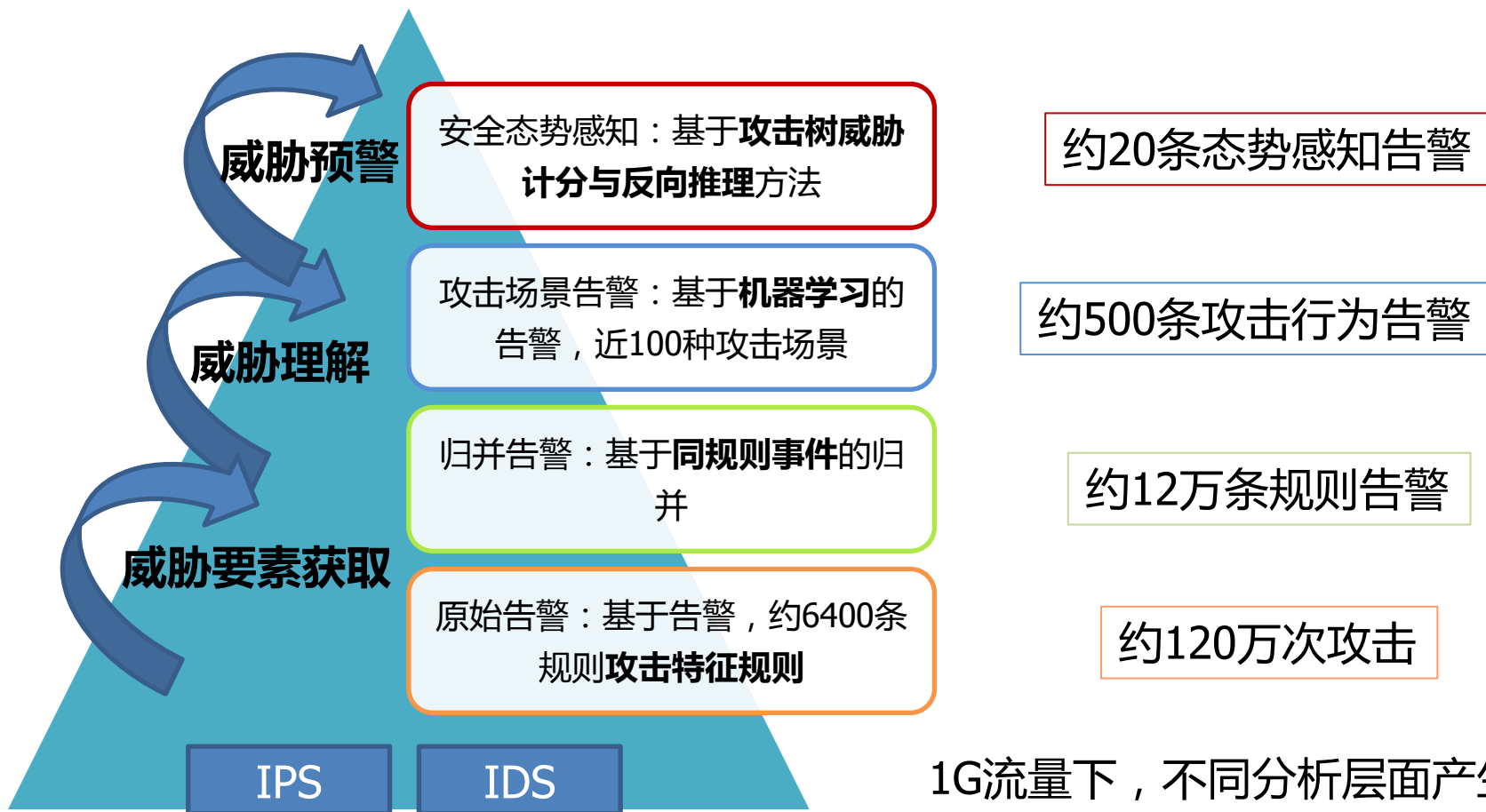
IDS

分布式部署-提高日志处理能力



分布式部署-提高日志处理能力





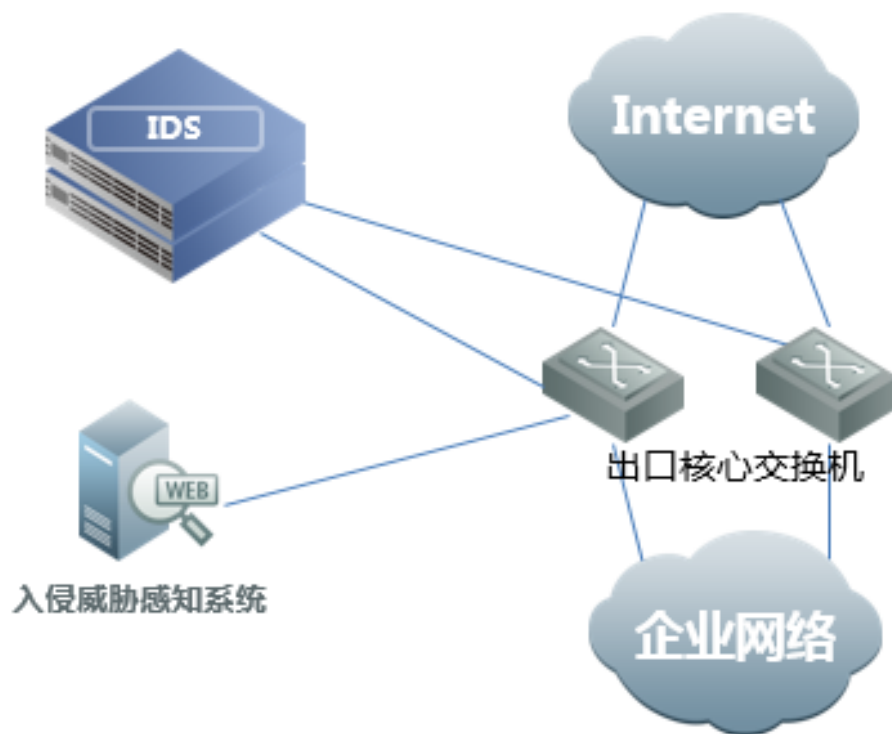
1G流量下，不同分析层面产生的告警

1 IDS/IPS安全运维现状

2 基于机器学习与攻击树的威胁感知

3 实践案例-某企业云平台部署案例

某企业云平台部署拓扑示意图如下，旁路部署两台万兆IDS，并将云平台出口的流量镜像到IDS进行2-7层的攻击检测。



入侵威胁感知系统安装在企业网络的服务器中，收集IDS产生的告警日志，帮助客户自动化输出可决策告警，促进IPS/IDS的安全运维。

➤ 真实检测某IP扫描事件：

入侵威胁感知系统自动研判出黑客的漏洞扫描行为，将此次漏洞扫描攻击过程中产生的**1万多条告警日志高度压缩为一条日志**，最终呈现在运维人员只有一条告警，可以及时对该攻击IP进行阻断等防护工作，**有效促进运维人员进行决策。**

源IP	目标IP	目标端口	攻击描述	首次时间	最近时间	总攻击次数	高风险	中风险	低风险	详情
2[REDACTED]	****	***	扫描了124个目标IP地址(主机扫描)	2015-04-15 22:47:26	2015-04-15 23:59:56	12181	198	1087	10896	详情

点击详情，进行数据下钻，可以看到具体扫描哪124个IP地址

每页显示: 25 条, 共124条记录 [首页](#) [上一页](#) [下一页](#) [末页](#) 1/5 页, 转到第 页

序号	源IP	目标IP	攻击描述	首次时间	最近时间	总攻击次数
1	2[REDACTED]	[REDACTED]	主机漏洞扫描	2015-04-15 23:33:13	2015-04-15 23:39:56	75
2	2[REDACTED]	[REDACTED]	主机漏洞扫描	2015-04-15 23:10:06	2015-04-15 23:17:17	66
3	2[REDACTED]	[REDACTED]	主机漏洞扫描	2015-04-15 23:25:38	2015-04-15 23:28:22	112

再次数据下钻，查看该扫描行为的原始告警

每页显示: 25 条, 共11条记录 [首页](#) [上一页](#) [下一页](#) [末页](#) 1/1 页, 转到第 页

序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	[REDACTED]	22893	[REDACTED]	0	Symantec Web Gateway 5.0.2.8 Arbitrary PHP文件上传漏洞	高风险	2015-04-15 23:31:37	1
2	[REDACTED]	2906	[REDACTED]	0	AWStats Totals multisort远程命令执行漏洞	高风险	2015-04-15 23:31:03	1
3	[REDACTED]	39921	[REDACTED]	0	Web服务远程SQL注入攻击可疑行为	高风险	2015-04-15 23:30:56	1
4	[REDACTED]	45852	[REDACTED]	0	Apache Struts2开发模式命令执行漏洞	高风险	2015-04-15 23:30:37	1
5	[REDACTED]	53468	[REDACTED]	0	WordPress plugin FoxyPress uploadify.php任意代码执行漏洞	高风险	2015-04-15 23:30:36	1
6	[REDACTED]	65043	[REDACTED]	0	AjaXplorer checkInstall.php 远程命令执行	高风险	2015-04-15 23:30:09	1

只呈现与该攻击行为相关的告警！

高度压缩告警日志

12181条原始日志

124条扫描
行为日志

1条最终
研判日志

➤ 真实检测FTP暴力破解事件：

入侵威胁感知系统**自动研判出FTP黑客暴力破解成功事件**。运维人员根据被破解的IP地址、被破解账号，**可以及时进行事后响应工作，有效促进运维人员进行决策。**

FTP暴力破解-原始日志									
每页显示: 25 条, 共25条记录 首页 上一页 下一页 末页 1/1 页, 转到第 页									
序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数	协议摘要
1		60179		21	FTP服务普通用户认证失败	低风险	2015-03-23 14:28:57	15	TCP.FTP S USER=apadmin PASSWD=*****
2		43106		21	FTP服务普通用户认证失败	低风险	2015-03-23 14:26:53	19	TCP.FTP S USER=apadmin PASSWD=*****
3		43087		21	FTP服务普通用户认证失败	低风险	2015-03-23 14:24:48	5	TCP.FTP S USER=apadmin PASSWD=*****
4		43151		21	FTP服务普通用户认证失败	低风险	2015-03-23 14:21:32	10	TCP.FTP S USER=apadmin PASSWD=*****
5		45750		21	FTP服务普通用户认证失败	低风险	2015-03-23 14:17:37	23	TCP.FTP S USER=apadmin PASSWD=*****

大量认证失败事件，自动研判为暴力破解事件

序号	源IP	目标IP	目标端口	攻击名称	首次时间	最近时间
1			21	FTP暴力破解	2015-03-23 11:21:16	2015-03-23 14:28:57

自动关联分析










暴力破解的源IP突然登陆成功

	48586		21	FTP服务普通用户认证成功	低风险	2015-03-23 14:42:17
--	-------	--	----	---------------	-----	---------------------












最终自动化输出暴力破解成功事件

序号	源IP	目标IP	目标端口	攻击名称	首次时间	最近时间	累计攻击数	详情
1			21	FTP暴力破解成功，被破解账号:apadmin	2015-03-23 14:42:17	2015-03-23 16:14:27	68	详情

攻击源威胁感知

序号	攻击源IP	影响IP数	攻击次数	攻击种类	详情
1		706	22503	10	详情
攻击源IP 202.104.70.250 攻击了 706 个 IP, 尝试了 10 种攻击类型。 分别为: 1.FTP暴力破解; 2.MS-SQL暴力破解; 3.SSH暴力破解; 4.http基本力破解; 6.telnet暴力破解; 7.web攻击入侵行为; 8.web漏洞扫描; 9.主机攻击; 建议: 将该源IP列入黑名单, 近7天内禁止该源IP地址的访问					
2		36	3064		
3		7	130		
4		26	2277		
5		22	1831		
6		27	1272		
7		11	239		
8		10	191		
9		19	1287		
10		106	4587		

被攻击目标威胁感知

序号	被攻击IP	攻击源IP地址数	被攻击次数	攻击种类	详情
1			357082	4	详情
被攻击IP 14.31.15.109 遭受 281603 个 IP 的攻击, 共面临了 4 种攻击类型。 分别为: 1.FTP暴力破解; 2.web攻击入侵行为; 3.主机攻击入侵行为; 4.主机漏洞扫描; 建议: 对该主机进行漏洞扫描评估以及相应的加固工作, 避免黑客入侵成功。					
2		262457	312511	5	详情
3		109043	121880	5	详情
4		97744	100825	2	详情
5		23041	2364433	4	详情
6		19522	155216	4	详情
7		19514	20450	4	详情
8		19503	154540	1	详情
9		19498	149330	4	详情
10		19464	96599	4	详情

可疑入侵成功事件

每页显示: 25 条, 共5条记录 首页 上一页 下一页 末页 1/1 页, 转到第 <input type="text"/> 页								
序号	源IP	目标IP	目标端口	攻击描述	首次时间	最近时间	攻击次数	详情
1			8000	木马后门程序SRAT通信	2015-04-07 01:34:48	2015-04-07 01:34:48	1	详情
2			21	FTP暴力破解成功, 被破解账号: apadmin	2015-03-24 01:45:43	2015-03-24 11:28:05	623	详情
3			21	FTP暴力破解成功, 被破解账号: apadmin	2015-03-23 14:42:17	2015-03-23 16:14:27	68	详情
4			23	telnet异常登录事件, 登陆用户: Administrator	2015-03-23 01:22:45	2015-03-23 14:07:29	41	详情
5			23	telnet异常登录事件, 登陆用户: Administrator	2015-03-22 14:17:38	2015-03-22 23:57:44	31	详情

威胁监控采用“攻击行为+时间轴”二维呈现方式



入侵威胁感知系统 ▸ 威胁监控 ▸ 全局视角

监控项	当前	最近1小时	最近24小时	最近7天	最近1月
暴力破解	0	0	108	496	2053
漏洞扫描	0	0	6	19	66
DDoS攻击	0	0	4	22	85
手工入侵	0	0	365	766	2947
异常登陆与远控	0	0	0	0	5
危害与影响	0	0	0	0	1

查看异常登陆与远控事件
查看漏洞扫描事件
查看手工入侵事件
查看DDoS事件

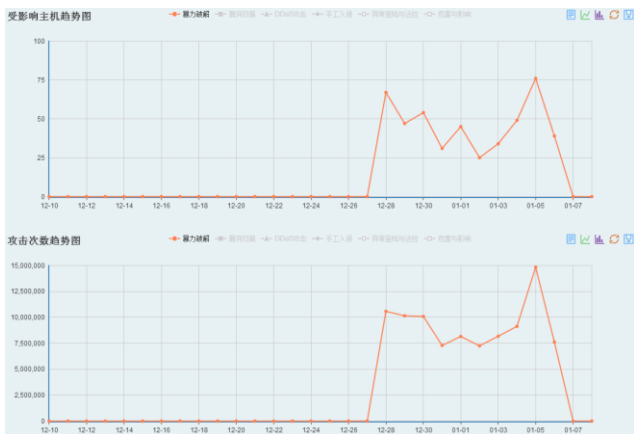
1/1 页，转到第 页

每页显示: 25 条，共4条记录 首页 上一页 下一页 末页 1/1 页，转到第 页

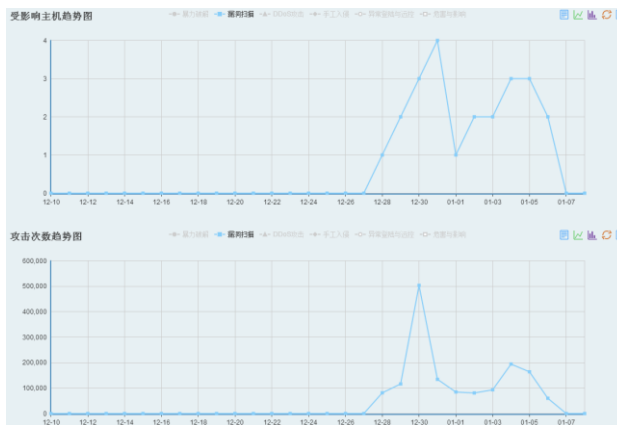
序号	源IP	目标IP	攻击描述	首次时间	最近时间	攻击次数	详情			
1			遭受 3856 个源IP地址的多源DDoS攻击	2015-04-16 00:00:04	2015-04-16 17:04:52	3997	详情			
2			SYN-Flood半开TCP连接淹没拒绝服务攻击	2015-04-16 04:30:02	2015-04-16 04:30:02	1	详情			
3			SYN-Flood半开TCP连接淹没拒绝服务攻击	2015-04-16 01:24:54	2015-04-16 01:24:54	1	详情			
4			SYN-Flood半开TCP连接淹没拒绝服务攻击	2015-04-16 01:24:34	2015-04-16 01:24:34	1	详情			
5			遭受 5341 个源IP地址的多源DDoS攻击	2015-04-15 00:00:07	2015-04-15 23:59:44	5632	详情			
5	...	1	度手工入侵 共遭受 143 源个IP地址的攻击	2015-04-16 00:20:05	2015-04-16 16:59:58	270	265	1	4	详情



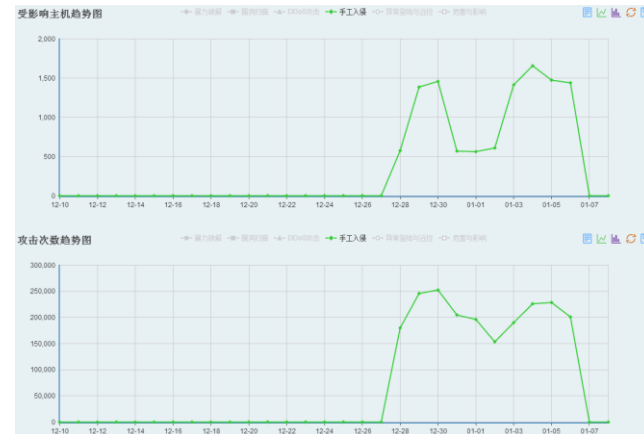
攻击类型比例



暴力破解攻击趋势分析



漏洞扫描攻击趋势分析



手工入侵攻击趋势分析

地图可视化呈现攻击威胁情况。





谢谢！