OKSEC
非凡安全

基于攻击演译与攻击树的威胁感知方法与实践

让安全变得更简单

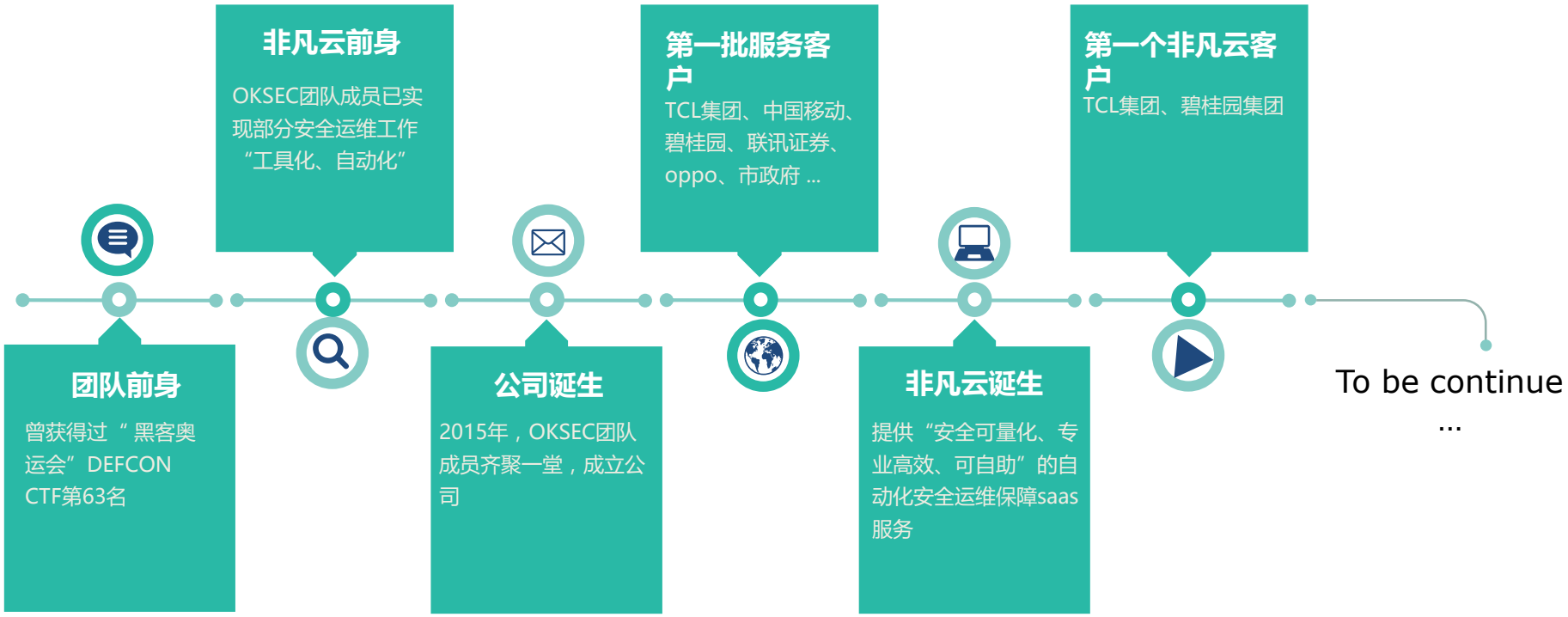
非凡安全 林旭滨

CCIE CISSP CISA PMP

发展历程

非凡安全 OKSEC.CN

广州非凡信息安全技术有限公司，成立于2015年，注册资金1100万元，总部设在广州，**基于自主研发的非凡云安全运维服务平台，为企业提供安全服务。**



OKSEC

1个疑问？

IPS/IDS在1G流量的环境下，一天内会产生多少条告警？

OKSEC

答案

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

2-7层黑客攻击

- 溢出攻击
- 蠕虫病毒
- 木马后门
- DDoS攻击
- 网络嗅探
- VOIP攻击
- WEB攻击
- 混合型攻击
- …

IPS/IDS规则匹配

- 基于攻击特征规则告警，绿盟科技IPS/IDS规则库拥有6400条规则约6400条规则

1G流量下约匹配120万次攻击

日志归并告警

- 基于同规则事件的归并

约12万条告警

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

OKSEC

真实的故事-某单位门户网站被篡改事件

某单位门户网站上启用了FTP用于管理网站文件，但某天该FTP服务被黑客成功暴力破解，并上传了网马，获取了该企业的机密信息以及篡改了网站文件。

该单位IDS运维现状

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	.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	.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	.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	.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	.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	.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	.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

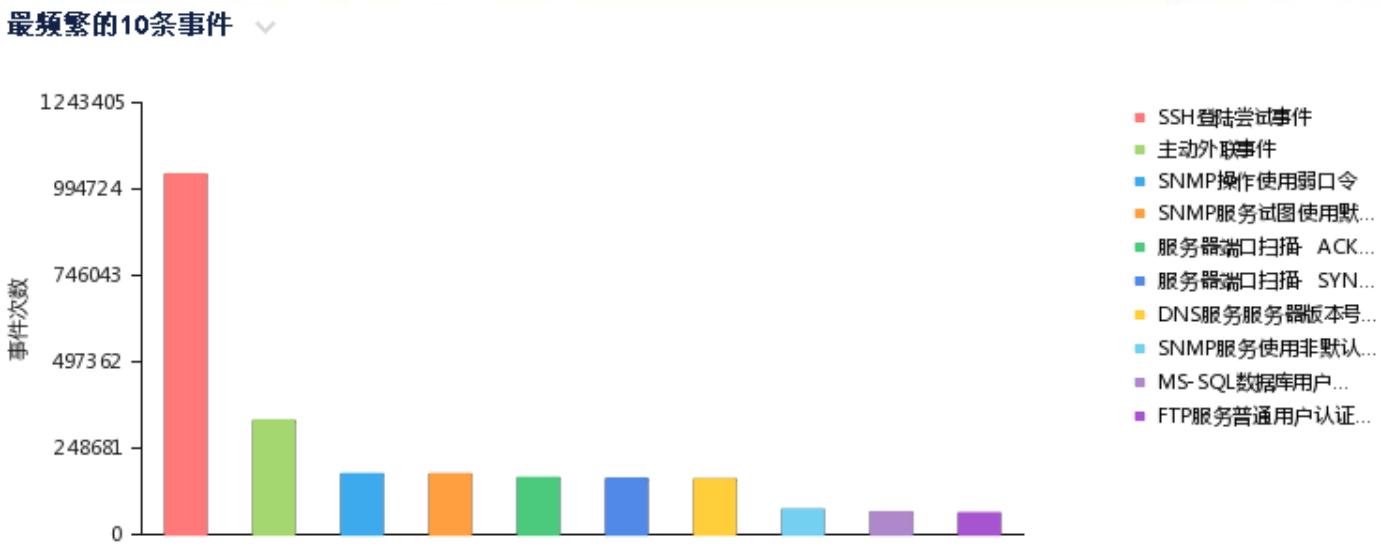
序号	源IP	源端口	目的IP	目标端口	攻击名称	风险类别	攻击时间	累计攻击数
1	183.29.90.173	48794	.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:28:05	1
2	183.29.90.173	57165	.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:15:47	1

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**，却忽略了“FTP认证失败事件”、“FTP服务认证成功事件”的**高价值的“低风险”**告警。

传统的分析方法

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



只查看高中风险安全事件，可是，低风险事件也很重要！

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	.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	.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	.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	.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	.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	.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	.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	.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	.15.173	21	FTP服务普通用户认证成功	低风险	2015-03-24 11:15:47	1

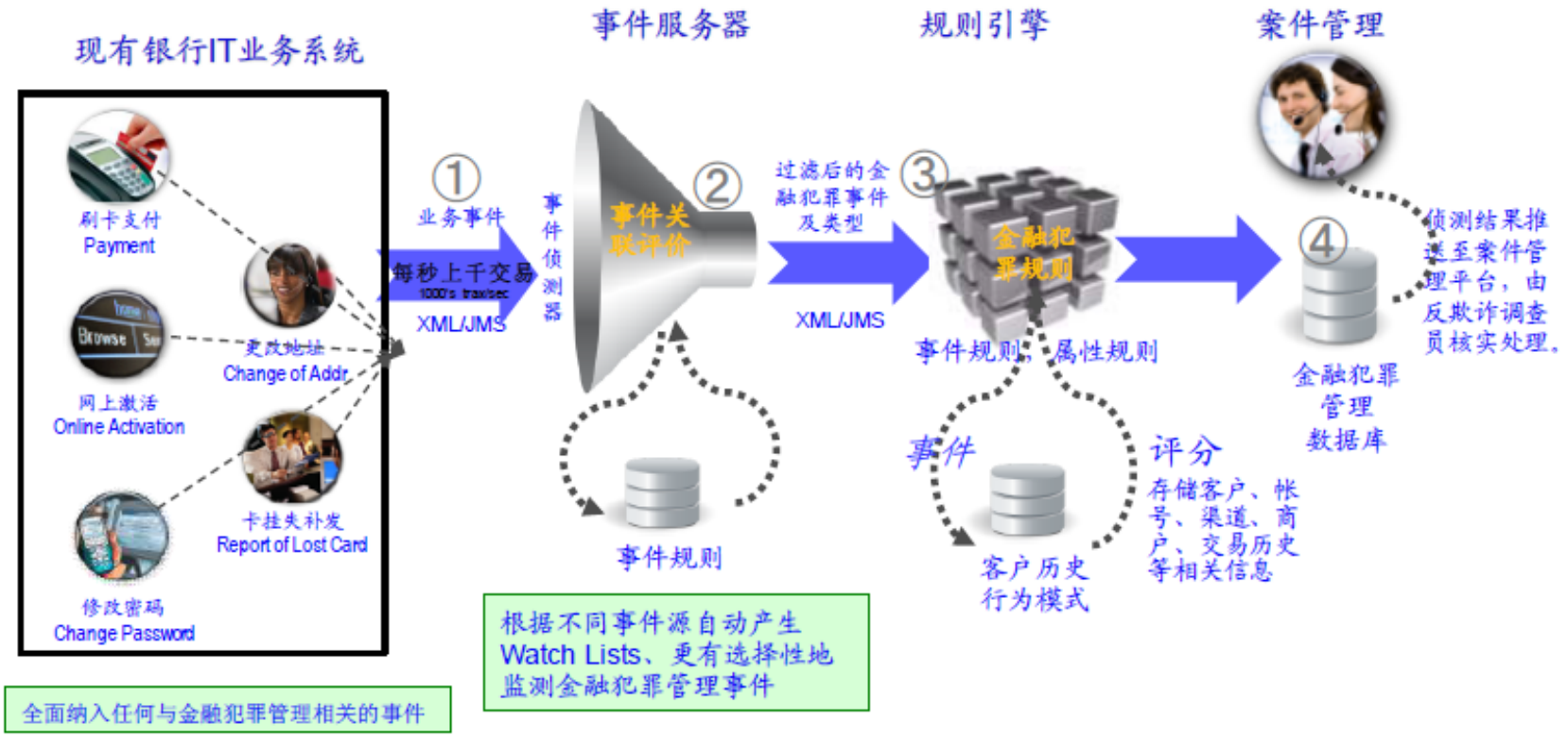
未能发现异常登陆事件

OKSEC

演译出行为模型-促进行为发现与理解

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



通过历史行为模式进行演译出异常行为规则，高效的发现交易欺诈行为

OKSEC

基于攻击演译的行为分析：理解攻击行为

过去

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

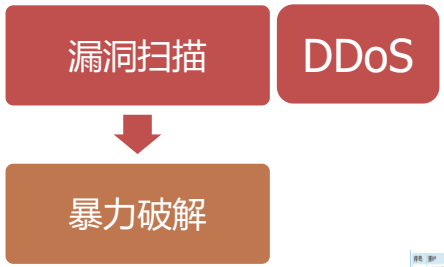
每页显示: 25 条，共54条记录 首页 上一页 下一页 末页 1/3 页，转到第 页

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	32175	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
125.227.80.221	38299	14.146.226.101	1433	MS-SQL服务用户暴力猜解口令攻击	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

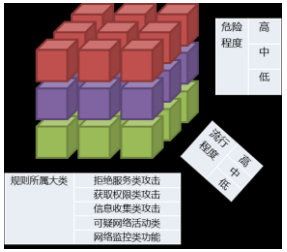
含专业术语告警，高水平的技术人员才能解读。

现在

黑客攻击过程



1、历史案例总结归纳：从历史案件中进行统计分析，找出规律。
2、模拟攻击场景：并设计**100多个攻击场景**，找出规律。
从而实现**攻击行为建模。**

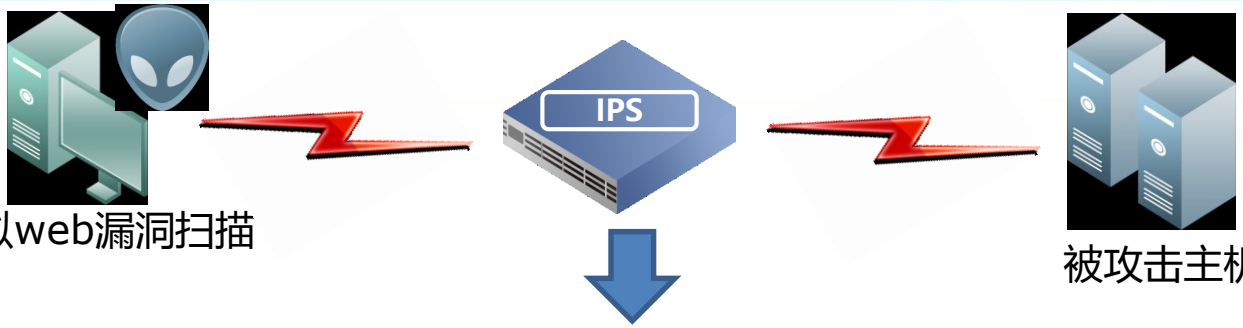


高效、准确识别黑客攻击行为，而且提高了告警可读性、可决策性。

普通的运维人员也能读懂。

OKSEC

举例-漏洞扫描



模拟web漏洞扫描

被攻击主机

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	10.82.70.165	35026	218.91.233.25	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	10.82.70.165	34917	218.91.233.25	8081	Microsoft FrontPage fp30reg.dll漏洞扫描探测	低风险	2014-11-03 23:36:21	1
3	10.82.70.165	34815	218.91.233.25	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	10.82.70.165	34780	218.91.233.25	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	10.82.70.165	34634	218.91.233.25	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

过去呈现情况：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	10.82.70.165	59.42.21.236	80	2014-11-04 13:18:08	2014-11-04 13:23:14	22 / 22	8	8	6	详情
2	10.82.70.165	218.91.233.25	8081	2014-11-03 23:30:46	2014-11-03 23:36:33	26 / 26	9	10	7	详情

现在呈现情况：直接研判出漏洞扫描行为

OKSEC

数据钻取-漏洞扫描事件发现

自动将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，高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
202.104.70.250	*.*.*.*	***	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...	低风险	详情
1	202.104.70.250	[redacted]15.109	主机漏洞扫描	2015-04-15 23:33:13	2015-0...	65	详情
2	202.104.70.250	[redacted].15.74	主机漏洞扫描	2015-04-15 23:10:06	2015-04-1...	55	详情
3	202.104.70.250	[redacted]15.97	主机漏洞扫描	2015-04-15 23:25:38	2015-04-15 23...	98	详情

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

再次数据下钻，查看该扫描行为的原

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	202.104.70.250	22893	[redacted].15.101	80	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	202.104.70.250	2906	[redacted].15.101	80	AWStats Totals multisort远程命令执行漏洞	高风险	2015-04-15 23:31:03	1
3	202.104.70.250	39921	[redacted].15.101	80	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	202.104.70.250	45852	[redacted].15.101	80	Apache Struts2开发模式命令执行漏洞	高风险	2015-04-15 23:30:37	1
5	202.104.70.250	53468	[redacted].15.101	80	WordPress plugin Foxypress uploadify.php任意代码执行漏洞	高风险	2015-04-15 23:30:36	1
6	202.104.70.250	65043	[redacted].15.101	80	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！

基于攻击树的事件推理：促进事后决策

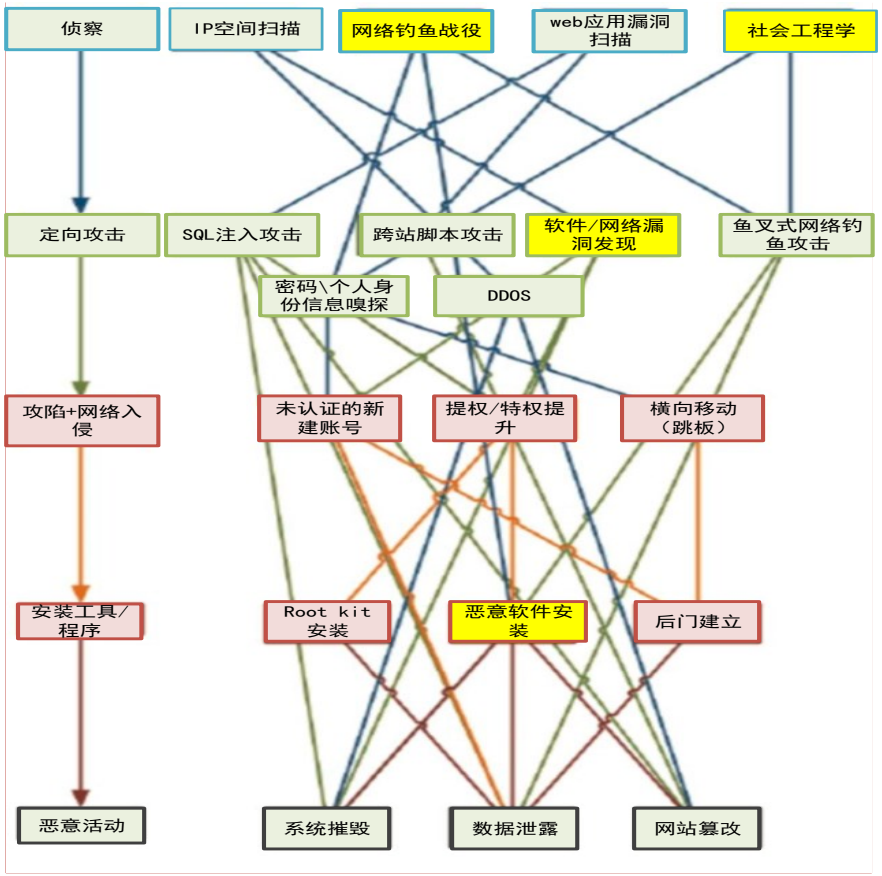
每页显示: 25 条，共54条记录 首页 上一页 下一页 末页 1/3 页，转到第 页

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	32175	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
125.227.80.221	38299	14.146.226.101	1433	MS-SQL服务用户暴力猜解口令攻击	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

攻击成功？不知道。。。

过去

现在



事件推理：通过事件推理研判攻击是否成功。

OKSEC

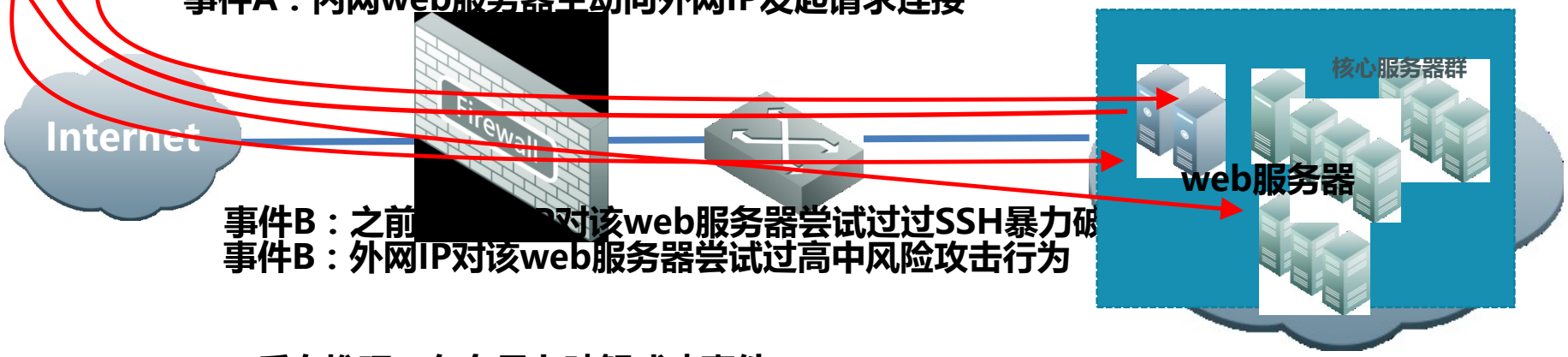
基于攻击树的反向推理：促进事后处置决策

通过反向推理，甚至可在一定程度上弥补IPS对于未知威胁的发现

黑客

事件A：外网IP成功通过SSH登陆web服务器

事件A：内网web服务器主动向外网IP发起请求连接



事件B：之前[illegible]对该web服务器尝试过过SSH暴力破

事件B：外网IP对该web服务器尝试过高中风险攻击行为

反向推理：存在暴力破解成功事件

反向推理：内网服务器IP地址中了反弹木马

攻击树推理-暴力破解成功事件发现

入侵威胁感知平台**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。**

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
1	14.151.52.4	60179	.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 14:28:57	15
2	14.151.52.4	43106	.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 14:26:53	19
3	14.151.52.4	43087	.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 14:24:48	5
4	14.151.52.4	43151	.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 14:21:32	10
5	14.151.52.4	45750	.15.173	21	FTP服务普通用户认证失败	低风险	2015-03-23 14:17:37	23

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	14.151.52.4	.15.173	21	FTP暴力破解	2015-03-23 11:21:16	2015-03-23 14:28:57

自动关联分析

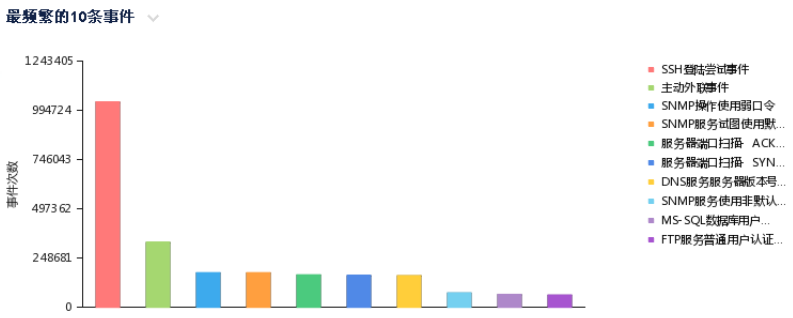
暴力破解的源IP突然登陆成功

14.151.52.4	48586	.15.173	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	14.151.52.4	.15.173	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

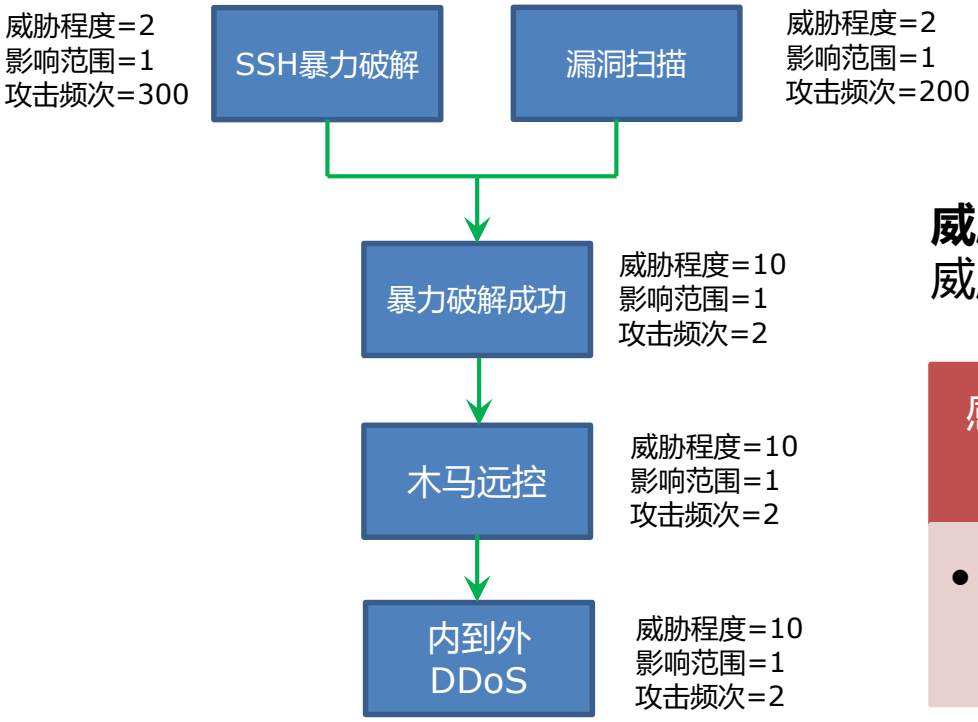
基于攻击树的威胁计分



哪些事件需要重点关注？
按攻击次数排序？
只看高风险？

过去

现在



威胁计分：评估每个IP在每个攻击节点产生的威胁程度、影响范围、攻击频次（烈度）

感知面临威胁较大的内网IP	感知攻击威胁较大的恶意IP
• 提前安内，避免资产被入侵成功	• 提前防外，避免黑客攻击成功

OKSEC

实现效果-威胁计分促进预警

预警威胁较大的攻击源，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	120.132.59.41	36	3064	5	详情
⊞	3	125.96.160.140	7	130	4	详情
⊞	4	120.132.59.43	26	2277		
⊞	5	120.132.59.42	22	1831		
⊞	6	180.150.177.71	27	1272		
⊞	7	60.12.31.70	11	239		
⊞	8	218.5.196.189	10	191		
⊞	9	218.202.225.74	19	1287		
⊞	10	122.49.14.84	106	4587		

被攻击目标威胁感知

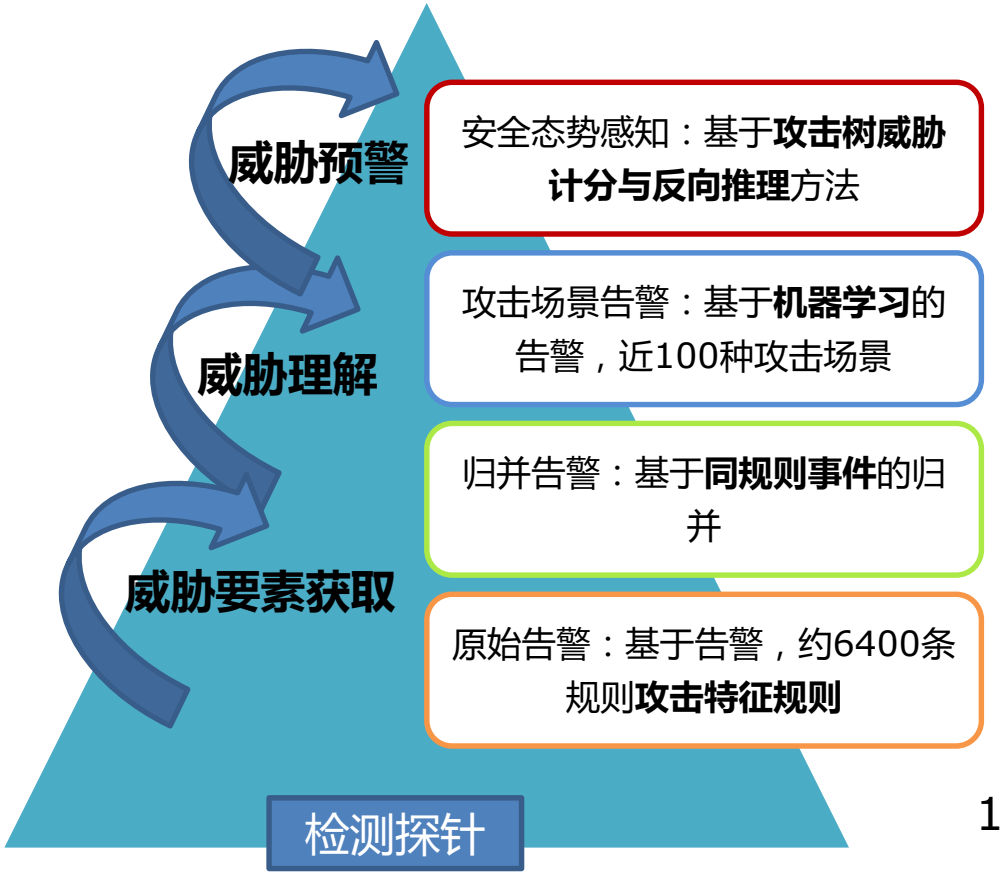
	序号	被攻击IP	攻击源IP地址数	被攻击次数	攻击种类	详情
⊟	1	[redacted].15.109	281603	357082	4	详情
	被攻击IP[redacted].15.109遭受281603个IP的攻击,共面临了4种攻击类型。 分别为： 1.FTP暴力破解；2.web攻击入侵行为；3.主机攻击入侵行为；4.主机漏洞扫描； 建议：对该主机进行漏洞扫描评估以及相应的加固工作，避免黑客入侵成功。					
⊞	2	[redacted].15.151	262457	312511	5	详情
⊞	3	[redacted]15.108	109043	121880	5	详情
⊞	4	[redacted]8.200.1	97744	100825	2	详情
⊞	5	[redacted]15.210	23041	2364433	4	详情
⊞	6	[redacted]15.114	19522	155216	4	详情
⊞	7	[redacted].15.17	19514	20450	4	详情
⊞	8	[redacted]5.115	19503	154540	1	详情
⊞	9	[redacted]15.113	19498	149330	4	详情
⊞	10	[redacted]5.221	19464	96599	4	详情

事件推理、威胁计分的结果可以直接转化为威胁情报进行分享。

预警面临威胁较大的资产，提供安全建议。

OKSEC

基于攻击演译与攻击树的威胁感知



安全态势感知：基于**攻击树威胁计分与反向推理**方法

攻击场景告警：基于**机器学习**的告警，近100种攻击场景

归并告警：基于**同规则事件**的归并

原始告警：基于告警，约6400条规则**攻击特征规则**

约20条威胁感知告警

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

OKSEC

OKSEC
非凡安全

谢谢

非凡安全● 让安全变得更简单

小广告

非凡云：自动化安全运维平台

资产管理

- ✓ 网站资产
- ✓ 域名资产
- ✓ 主机资产

安全预警

- ✓ 漏洞情报
- ✓ 安全周报
- ✓ 新高危漏洞检测

安全检测

- ✓ 网站漏洞扫描
- ✓ 主机漏洞扫描
- ✓ 基线配置核查

安全加固

- ✓ 加固跟踪
- ✓ 安全防护智囊
- ✓ 顾问咨询

安全响应

- ✓ 网站日志分析
- ✓ 主机日志分析
- ✓ 威胁情报分析
- ✓ 顾问咨询

OKSEC

分享一些国内外威胁情报网站

- http://www.nothink.org/honeypots.php
- http://www.blocklist.de/en/api.html#last
- http://botscout.com/
- http://malwareurls.joxeankoret.com/
- https://csirtg.io/
- https://www.blocklist.de/downloads/
- 烽火台：http://www.x-cti.org/
- 微步在线：https://x.threatbook.cn/