



星冕——守护这片星空

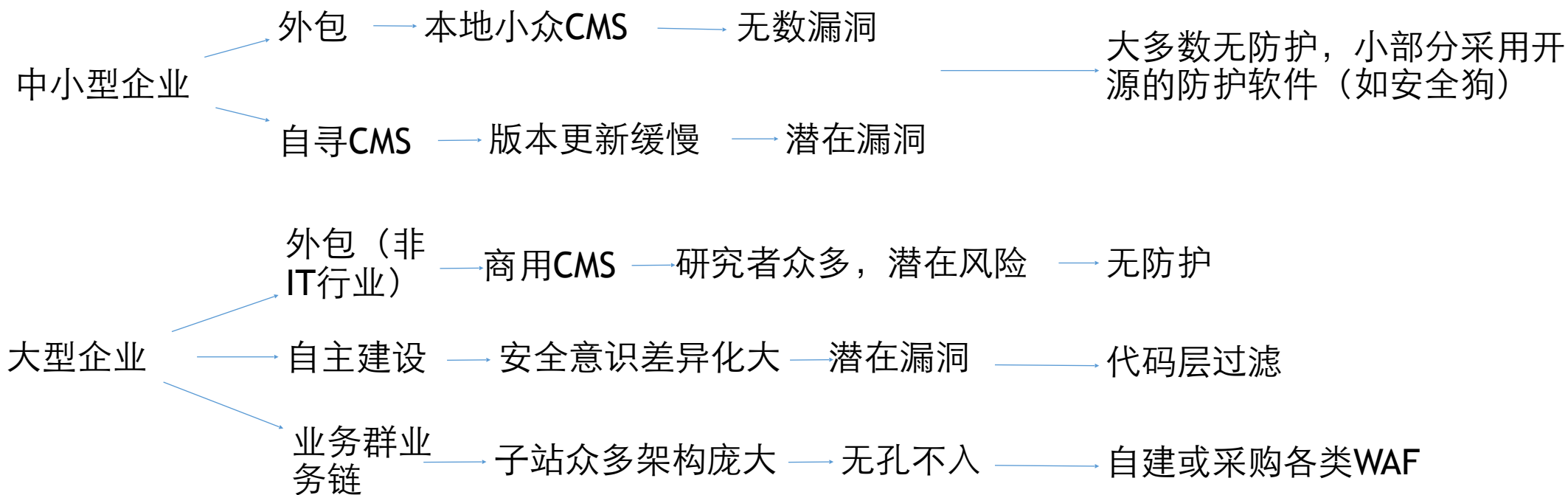
主讲人——PKAV何鹏程(蘑菇)

各类型企业面临的安全风险

企业类型

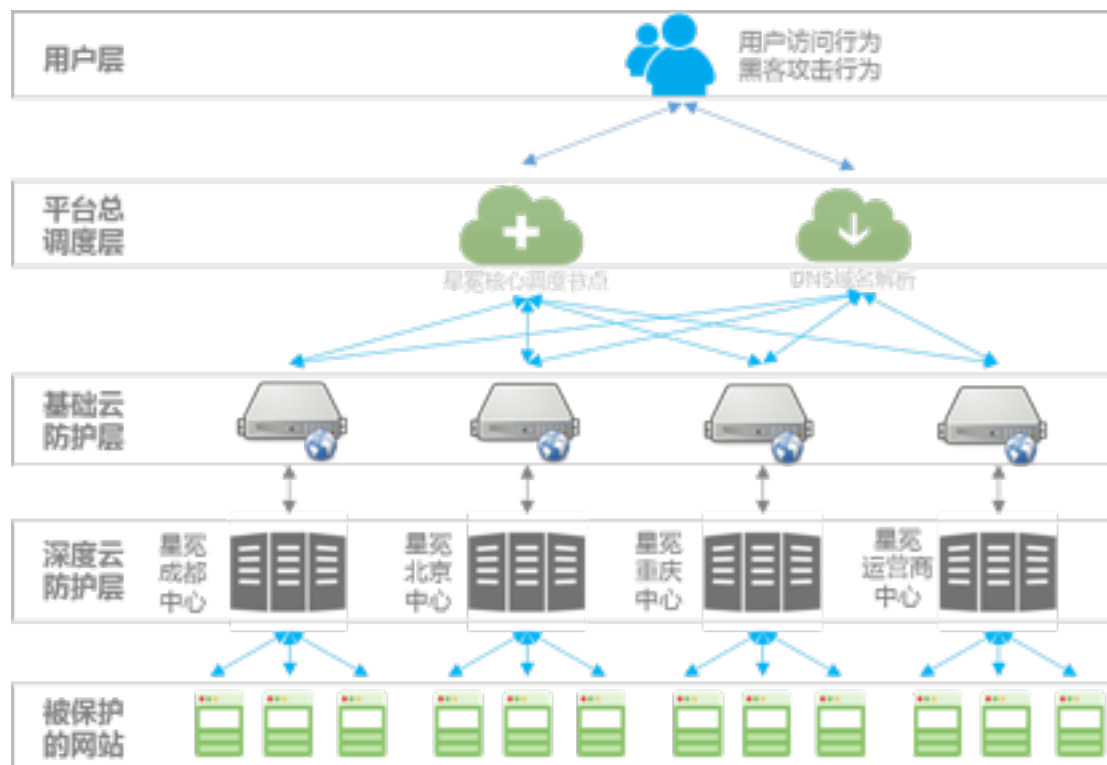
建站架构及风险

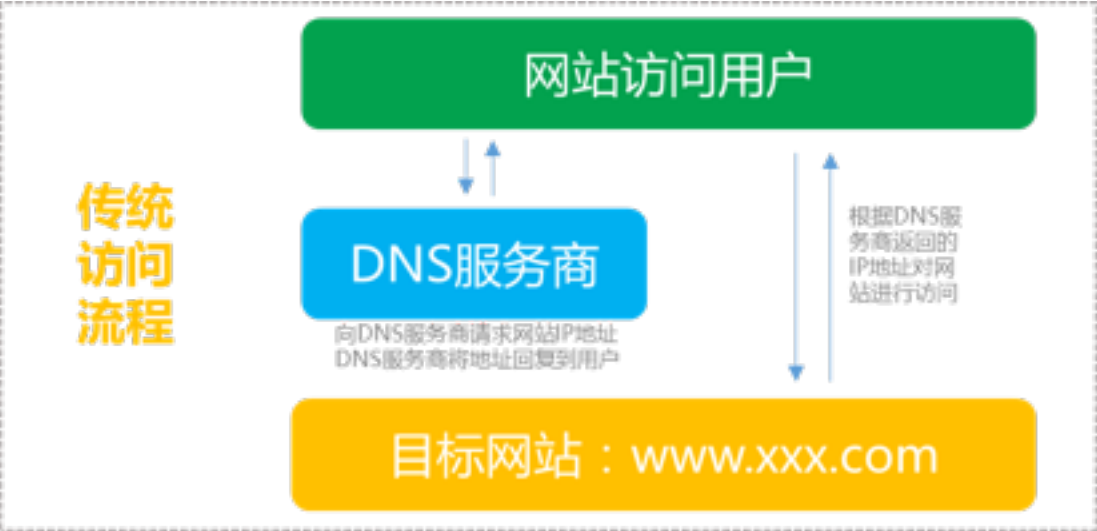
安全防护



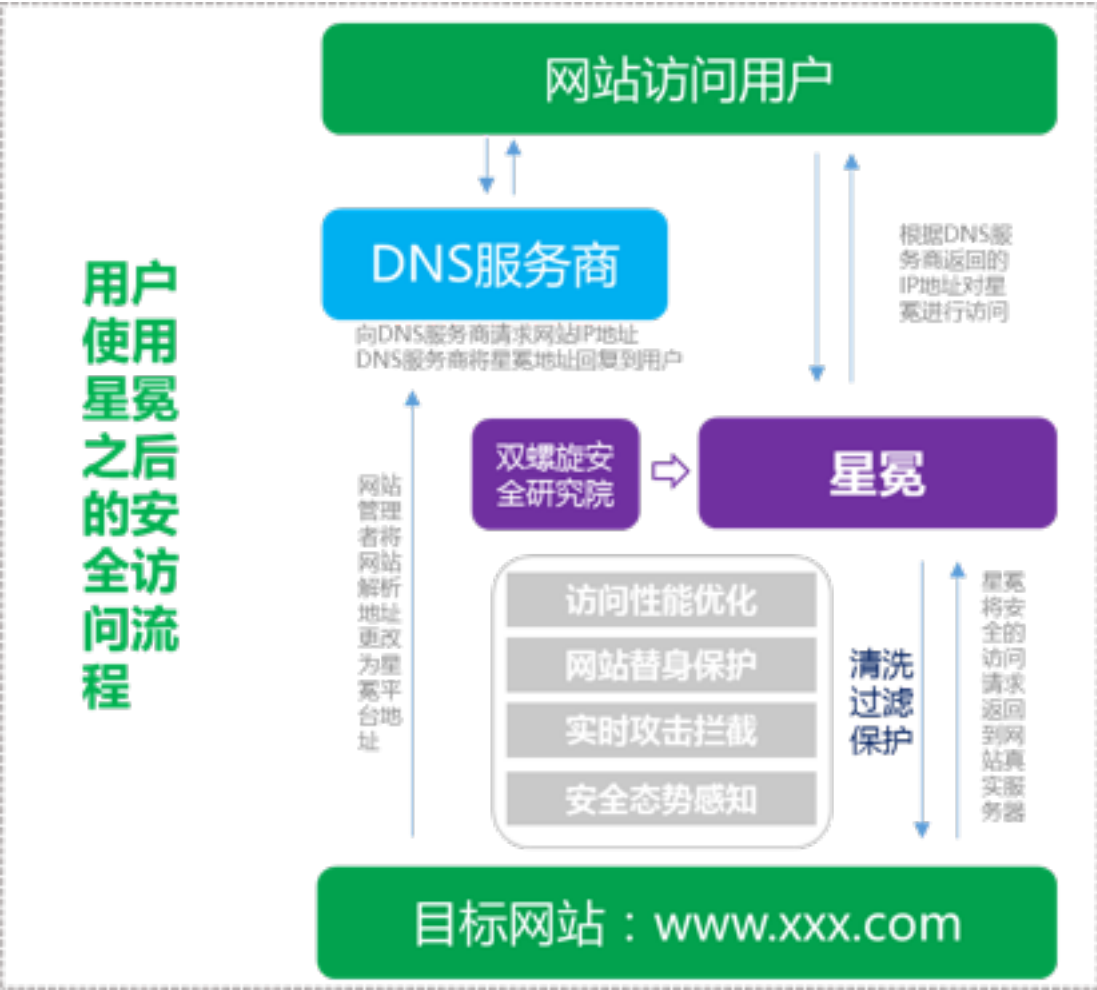
如何在不改变系统原有架构的前提下统一规避风险？

PKAV团队自研的集网站监控、防护与态势感知为一体的系统——星冕

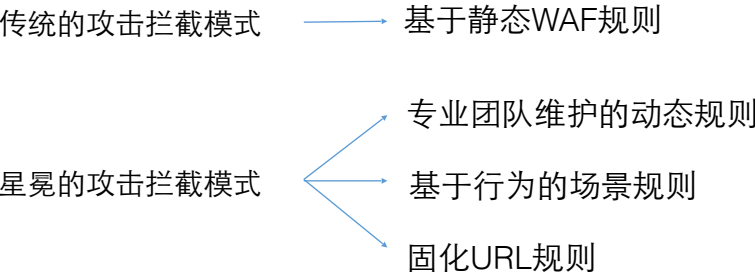




平台功能	功能说明
网站访问加速	对接入设备的网站实现反向代理，反向代理能够帮助用户智能选路并通过静态缓存实现访问加速的功能，与此同时，反向代理能够帮助用户拦截各类攻击请求。
网站日志审计	记录和分析网站的威胁情报日志，以小时为单位对权限范围内的管辖网站进行多维度的日志分析，通过点击日志还可以查看所有网站的安全状态详情，并通过链接定位到安全细节。
全站流量分析	提供实时以及非实时的流量分析统计，用户可以根据自己的需求查看网站的流量负荷并从中提取和发现出异常流量和攻击行为。
多维攻击检测	提供三种维度的攻击检测和积分机制，包括WAF积分、场景积分和固化URL积分三类，用户可以通过该模块来查看网站的安全状态，同时该模块也会智能地拦截非法用户的访问请求。
访问行为还原	当用户选择了指定时间段的指定IP后，可以将该时间段的IP访问行为进行多维度的还原以识别这段时间的用户访问。特别是当确定了攻击者后可以通过该模块来完成入侵行为的还原，并且具有良好的展示效果。
网站篡改检测	通过大数据的手段来识别网站是否遭到了恶意篡改，包括进行网站的源码相似度、图片相似度、词云相似度等多维的数学检测，从而判断网站目前的安全状况。
网站后门检测	通过整站后门检查，检测网站是否被植入后门。
反向落地追踪	提供JS回执功能，对于可疑IP选择性的开启JS回执功能，该模块可以配合指纹系统定位攻击者的虚拟身份信息。
黑白名单添加	提供黑白名单添加的接口，包括IP黑名单、IP白名单以及URL白名单三类，管理员可以自行调节该接口来对特殊页面和特殊IP进行管理。



攻击拦截方式



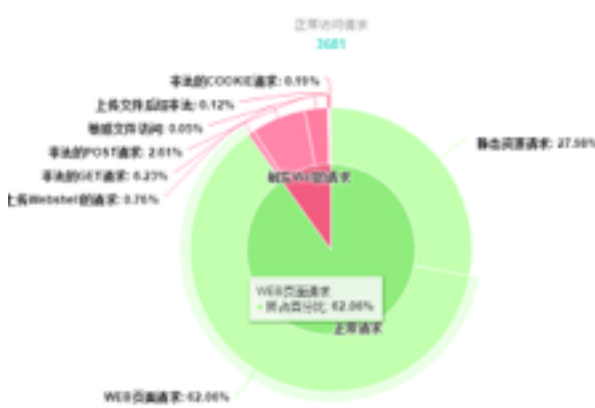
威胁情报日志记录



威胁得分与评级



基于规则的访问详情



固化URL监测信息

固化URL监测信息			
COUNT	REQUEST_METHOD	PARAMETER	REQUEST_URI
4704	get	id	*
435	get	lanmuid	*
366	get	sublanmuid	*
1	post	aid	/dede/money/

场景监测信息

场景监测信息	
名称	IP地址
某网站被访问1000次	15
某网站被访问1000次以上	1
某网站被访问1000次到2000次	44
用户登录失败进行多次尝试（上传图片）	3
敏感数据、操作和命令被请求	2
敏感后台目录被访问请求	7
敏感后台目录被访问5次以上	3
某网站被访问5000次到10000次	4
敏感后台目录被访问（上传）	2

行为还原方式

传统的行为还原方式

日志分析

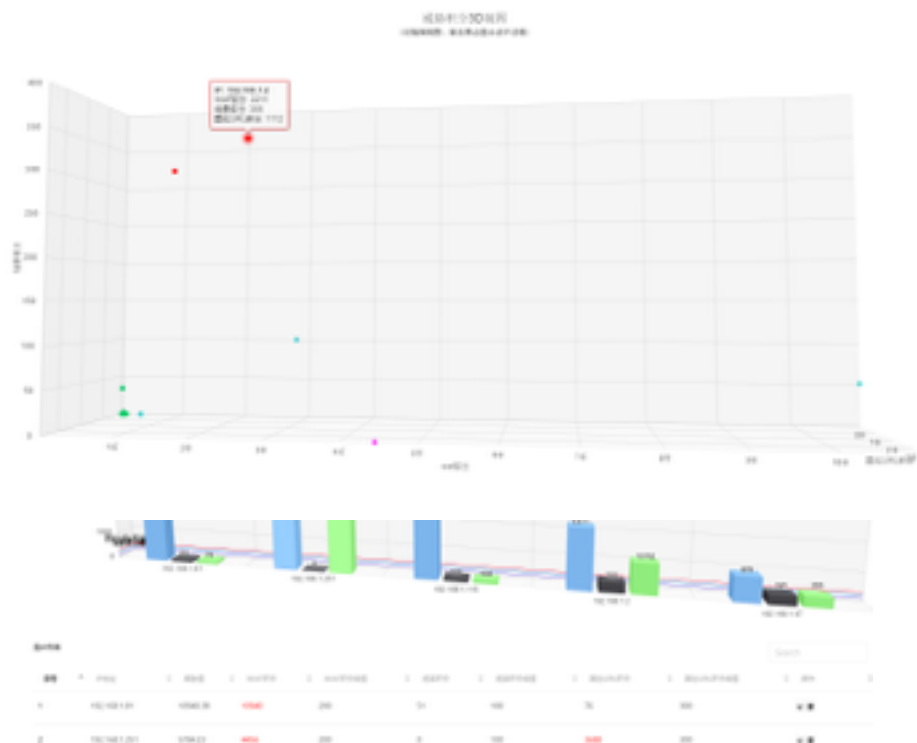
星冕的行为还原方式

可视化的访问记录显示

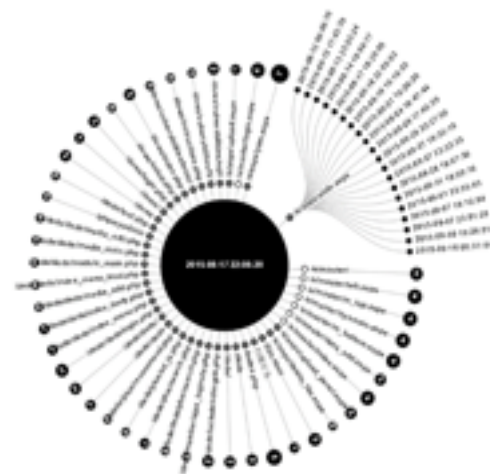
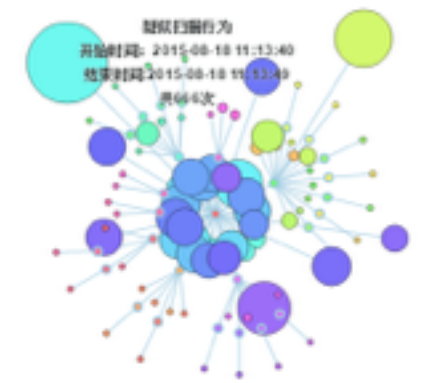
可视化的访问时段还原

基于算法的扫描行为识别

定向的行为还原接口

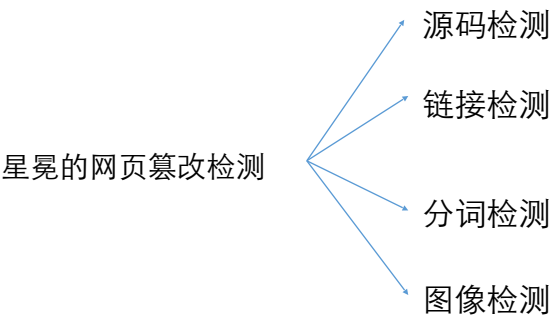


自定义的行为还原接口



网页篡改检测

传统的网页篡改检测 源码检测



页面基本信息

记录所属环境名称	
URL地址	http://www.10000.com
当前页面URL地址	www.10000.com/001/01
最新一次检测时间	2018-05-27 09:38:37
页面是否被篡改过	否

页面截图

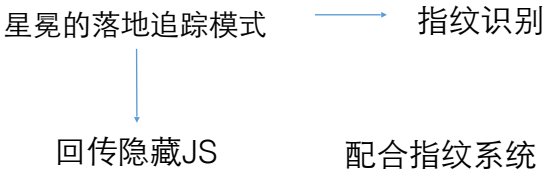
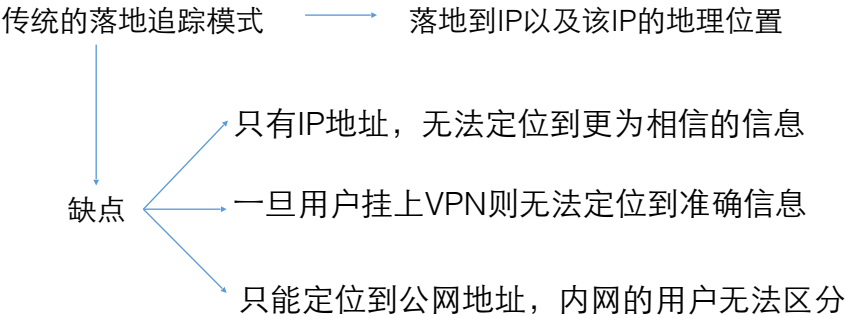
网站词云分布



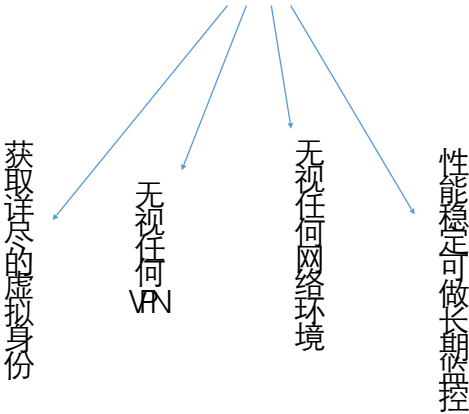
网站安全得分

源码检测得分: 100	⊙
利用网页安全的历史版本数据,依据网页源码的标签结构和语义进行了相似度检测和恶意代码检测,得分越高安全性越高。	
链接检测得分: 100	⊙
分词检测得分: 100	⊙
图像检测得分: 100	⊙
综合检测得分: 100	⊙

反向落地追踪



获取访客的唯一网络标识，以及该标识所对应的网络身份（包括ID、用户名、昵称等）



指纹系统总体技术架构->纯粹依靠漏洞，很难被模仿和被超越



除此之外用户也可以自定义返回JS信息（例如用作推广）



我们能获取到的网站指纹



详细监测信息

传统的监测信息记录 \longrightarrow 数据库 \rightarrow 表格的单一展示

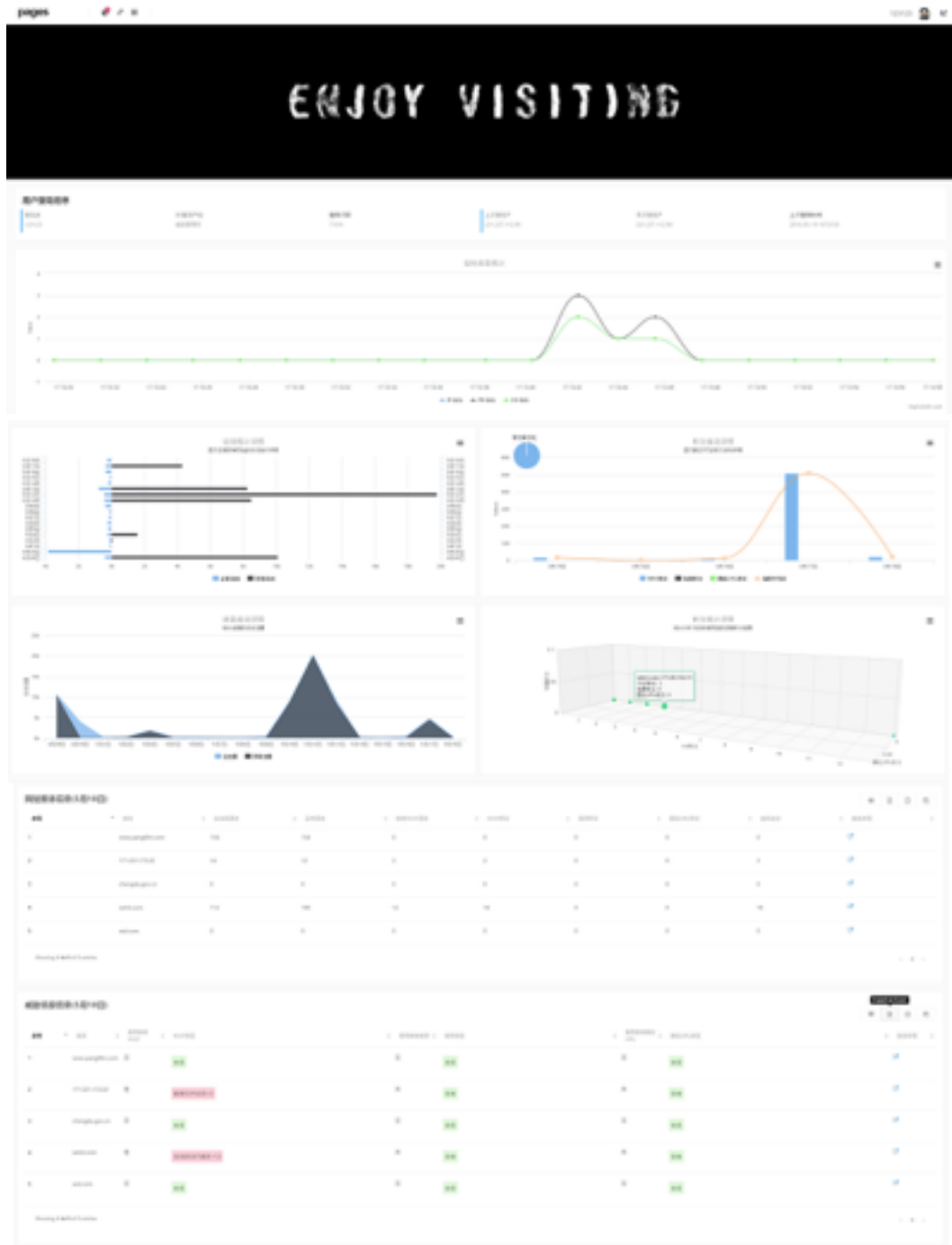
星冕的监测信息记录

图、文、表相结合

完善的报告生成体系

自定义的攻击预警提示

直观的实时监控信息

[illegible]

	地址: shangsha.gov.cn 起止时间: 2016/1/29 下午2:38-15至2016/3/29 下午2:38-12 最低押金: CC零卡请求(超1000g)	
	地址: shangsha.gov.cn 起止时间: 2016/1/29 下午2:38-12至2016/3/29 下午2:38-14 最低押金: CC零卡请求(超1000g)	
	地址: shangsha.gov.cn 起止时间: 2016/1/29 下午2:38-14至2016/3/29 下午2:38-16 最低押金: CC零卡请求(超1000g)	
	地址: shangsha.gov.cn 起止时间: 2016/1/29 下午2:38-16至2016/3/29 下午2:38-18 最低押金: CC零卡请求(超1000g)	
	地址: shangsha.gov.cn 起止时间: 2016/1/29 下午2:38-18至2016/3/29 下午2:38-20 最低押金: CC零卡请求(超1000g)	



Date	Attacker	Target	Attack
06-48:28 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:32 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:34 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:40 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:45 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:47 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:48 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:49 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:50 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User
06-48:51 19.03.2015	78.179.212.100 Linux	193.140.100.100 N/A	Not Suspicious Traffic ET POLICY GmailLinux APT User

除此之外

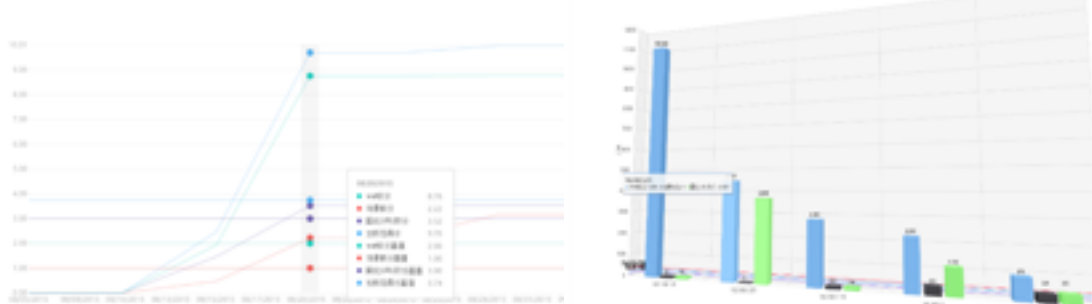
流量分析



黑白名单添加

The screenshot shows a blacklist/whitelist management interface. It includes a table with columns for '序号' (Serial Number), 'IP地址' (IP Address), '域名' (Domain), 'URL地址' (URL Address), '操作' (Action), and '备注' (Remarks). The table lists several entries, including domains like 'www.pangolin.com' and 'www.ahnews.com.cn'. A '添加' (Add) button is visible at the top right.

威胁信息管理



域名及用户管理

The screenshot shows a domain and user management interface. It includes a table with columns for '序号' (Serial Number), '域名' (Domain), '用户' (User), '操作' (Action), and '备注' (Remarks). A modal dialog is open, showing a form for adding a new entry, with fields for '域名' (Domain), '用户' (User), and '备注' (Remarks).

操作日志管理

The screenshot displays an operation log management interface. It includes a table with columns for '序号' (Serial Number), '操作' (Action), '时间' (Time), and '备注' (Remarks). The table lists several entries, including actions like '添加' (Add), '删除' (Delete), and '修改' (Modify).

后门检测

The screenshot shows a backdoor detection interface. It includes a table with columns for '序号' (Serial Number), '域名' (Domain), '用户' (User), '操作' (Action), and '备注' (Remarks). The table lists several entries, including domains like 'www.pangolin.com' and 'www.ahnews.com.cn'.

The screenshot displays a backdoor detection interface. It includes a table with columns for '序号' (Serial Number), '域名' (Domain), '用户' (User), '操作' (Action), and '备注' (Remarks). The table lists several entries, including domains like 'www.pangolin.com' and 'www.ahnews.com.cn'.

细节决定成败



品质铸就辉煌

