





本文中出现的任何文字描述、文字格式、插图、照片、方法等内容,除另有特别注明,版权均属杭州安恒信息技术股份有限公司(简称"安恒信息")所有,受到有关产权及版权法保护。任何个人、机构未经安恒信息的书面授权许可,不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的的单位或个人,应在授权范围内使用,并注明"来源:安恒信息"。违反上述声明者,安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外,本手册中出现的其他商标、产品标识及商品名称,由各自权 利人拥有。



目 录

前	言	I
1.	快速入门	1
]	.1 产品特点	. 1
	1.1.1 部署特点	. 1
	1.1.2 检测功能	. 1
]	.2 产品功能	. 1
1	.3 角色与权限说明	3
]	.4 登录系统	. 4
]	.5 产品形态	. 5
1	.6 设备身份	. 5
2.	导航	8
4	2.1 导航页面	. 8
	2.1.1 统计信息	. 8
	2.1.2 风险趋势	9
	2.1.3 流量分析	10
	2.1.4 攻击展示	.11



	2.1.5	高危风险类别	.11
	2.1.6	攻击源区域排名	12
	2.1.7	紧急事件/高危事件	13
	2.1.8	语音告警	14
2	.2 失陥	<u> </u>	15
	2.2.1	风险类别排名	16
	2.2.2	回连区域排名	17
	2.2.3	风险事件	18
	2.2.4	失陷主机 IP/黑客组织	19
	2.2.5	失陷主机事件	21
	2.2.6	最新事件	22
	2.2.7	失陷主机数	23
2	.3 攻击	- 溯源页面	23
	2.3.1	攻击主机个数最多的情报事件 TOP10	24
	2.3.2	威胁情报告警类型分布	25
	2.3.3	IP 查询	26
	2.3.4	威胁活动	28



	2.3.5 3D 展示	29
2	2.4 主页 admin 菜单介绍	35
3.	探测器	37
3	3.1 查看管理口 IP	37
3	3.2 探测器配置	37
	3.2.1 新增探测器	38
	3.2.2 修改/删除探测器	38
	3.2.3 升级探测器	39
	3.2.4 同步验证	39
	3.2.5 配置同步	39
3	3.3 流量代理 (Agent 代理模式支持)	40
	3.3.1 打开 Agent 配置开关	40
	3.3.2 配置其他端口	41
	3.3.3 测试链路	41
	3.3.4 启动/停止/删除网口	42
	3.3.5 编辑网口	42
	3.3.6 端口修改	42



4.	配置	44
	4.1 常规配置	44
	4.1.1 基本配置	44
	4.1.2 地理位置	48
	4.1.3 客户网络	50
	4.1.4 语音告警	51
	4.1.5 NAT 地址解析	52
	4.1.6 资产识别配置	53
	4.2 检测配置	53
	4.2.1 引擎管理	53
	4.2.2 文件检测	54
	4.2.3 IP 检测配置	62
	4.2.4 黑 IP 黑域名	65
	4.2.5 白名单	66
	4.2.6 Web 特征	75
	4.2.7 Web 登录	76
	4.2.8 IDS 规则	78



	4.2.9 邮箱防护	. 79
	4.2.10 ARP 检测	79
	4.2.11 弱口令配置	. 80
	4.2.12 自定义规则	82
	4.2.13 特权账户配置	85
	4.2.14 智能语义分析	85
	4.2.15 SSL 流量检测	. 86
	4.2.16 UDP 端口过滤	87
	4.2.17 暴力破解模型	. 88
	4.2.18 扫描行为模型	89
	4.2.19 拒绝服务攻击模型	90
4.	3 联动配置	90
	4.3.1 EDR 联动	90
	4.3.2 WAF 联动	91
	4.3.3 防火墙联动	93
4.	4 数据外送	95
	4.4.1 服务器配置	95



4.4.2	发送字段配置	102
4.4.3	安全域配置	103
4.4.4	协议审计	103
5. 系统…		105
5.1 权刚	艮管理	105
5.1.1	角色管理	105
5.1.2	用户管理	106
5.1.3	用户安全设置	108
5.1.4	IP 访问控制	109
5.1.5	动态令牌管理	110
5.1.6	敏感信息管理	110
5.2 数排	居维护	111
5.2.1	自动备份	111
5.2.2	自动恢复	113
5.2.3	手工备份	115
5.2.4	手工恢复	116
5.2.5	自动清理	116



	5.2.6 出厂设置	117
	5.3 系统资源	118
	5.4 升级管理	118
	5.4.1 手动升级	118
	5.4.2 在线升级	121
	5.4.3 云端配置	122
	5.4.4 托管配置	123
	5.5 许可证	124
	5.6 日志管理	125
	5.6.1 系统日志	125
	5.6.2 操作日志	125
	5.6.3 升级日志	126
	5.7 其他	126
	5.7.1 SNMP 配置	127
	5.7.2 网络配置	128
6.	分析	130
	6.1 分析	130



	6.1.1 紧急事件分析	. 130
	6.1.2 主机威胁分析	. 130
	6.1.3 失陷主机分析	. 133
	6.1.4 情报事件分析	. 134
	6.1.5 攻击者视角分析	. 136
	6.1.6 受害者视角分析	. 138
	6.1.7 脆弱性分析	. 139
	6.1.8 流量统计	. 140
	6.1.9 登录行为分析	. 141
	6.1.10 抓包分析	. 143
	6.1.11 PCAP 文件上传	. 144
	6.1.12 威胁情报检索	. 145
6	5.2 文件分析	. 146
	6.2.1 文件威胁分析	. 146
	6.2.2 回连域名/IP	. 149
	6.2.3 文件审计	. 149
	6.2.4 文件上传	. 150



	6.3	域名分析 1	52
	6.	3.1 受感染主机 1	52
	6.	3.2 C&C 服务器1	53
	6.	3.3 高频访问同一域名1	55
7.	风降	<u>ھ</u> 1	.57
	7.1	查询和处理风险 1	57
	7.2	应用举例 1	60
8.	资产	≿1	.65
	8.1	资产概况 1	.65
	8.2	非标端口1	.67
	8.3	分组标签 1	.67
	8.4	识别区域1	.68
9.	报	度 1	.70
	9.1	报表分类 1	70
	9.2	报表查询1	71
	9.3	报表导出 1	.72
	9.4	报表订阅1	73



9.5 报表设置	
9.6 邮箱设置	
10. 登录故障排查平台	
11. 术语&缩略语	





概述

感谢您选择安恒信息的网络安全产品。明御[®]APT 攻击预警平台(简称"APT"或"平台")通过对网络中的流量进行解析,发现其中的攻击事件。利用网络流量分析技术、异常访问定位技术、基于 Web 的攻击检测技术、恶意文件分析技术及云端的高级分析技术来综合分析检测发现 APT 攻击,大大提高了 APT 攻击的成功检测率和减少了误报情况。

本手册描述明御[®]APT 攻击预警平台产品用户使用过程中常用的操作和配置。

手册所提供的内容仅具备一般性的指导意义,并不确保涵盖所有型号产品的所有使用场景。因版本升级、 设备型号、配置文件不同等原因,手册中所提供的内容与用户使用的实际设备界面可能不一致,请以用户 设备界面的实际信息为准,手册中不再针对前述情况造成的差异——说明。

出于功能介绍及配置示例的需要,手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为 示意,不指代任何实际意义。

预期读者

本文档主要适用于期望了解明御[®]APT 攻击预警平台的读者,包括服务工程师、系统管理员、网络管理员 等。本文假设读者对以下领域的知识有一定了解:

- ◆ 网络安全相关知识,包括 APT、DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- ◆ 安全防护策略、NAT 地址转换、VPN、各类路由协议的基本工作原理和配置。

格式约定



本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的菜单、页签、页面名称、窗口名称、对话框名称,例如:"在菜单栏中选择 系 统状态进入系统状态页面,选择接口状态页签。"
<>	Web 界面上的按钮名称、复选框名称、文本框名称、选项名称等。例如:"微信认证失败, 点击< 我要上网 >不弹出微信认证界面"。
*	介绍 Web 界面的操作步骤时,用于隔离点击对象(菜单项、子菜单、按钮以及链接等),例如:"在菜单栏选择' 策略配置>认证管理>认证策略 '查看是否开启了认证策略"。
斜体字	可变参数,必须使用实际值进行替代。例如:"在浏览器地址中输入'http:// <i>管理 IP</i> ',回车后进入系统 Web 管理平台登录页面"。

本手册图标格式约定如下。

图标	说明
-œ́	提示,操作小窍门,方便用户解决问题。
	说明,对正文内容的补充和说明。
⚠	注意,提醒操作中的注意事项,不当的操作可能会导致设备损坏或者数据丢失。
À	警告,该图标后的内容需引起格外重视,否则可能导致人身伤害。

获得帮助



使用过程中如遇任何问题,请致电服务热线 400-6059-110。

请访问安恒社区 <u>https://bbs.dbappsecurity.com.cn/</u>获取更多文档。

联系信息

- 地址:浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦
- 邮编: 310052
- 电话: 0571-88380999
- 传真: 0571-28863666
- 官网: <u>http://www.dbappsecurity.com.cn</u>
- 邮箱: <u>400-doc@dbappsecurity.com.cn</u>



1. **快速入门**

APT 攻击(Advanced Persistent Threat),即高级可持续威胁攻击,其危害及隐蔽性越来越高,一些涉密部 门是被攻击的重点目标。当前的检测工具如杀毒软件、防毒墙、IPS、IDS、防火墙等设备的检测大多基于 已知安全漏洞及恶意代码特征的部分攻击行为,无法检测利用 0day 漏洞进行渗透的攻击。

明御[®]APT 攻击预警平台通过对网络中的流量进行解析,发现其中的攻击事件。利用网络流量分析技术, 异常访问定位技术、基于 Web 的攻击检测技术、恶意文件分析技术及云端的高级分析技术来综合分析检测 发现 APT 攻击,提高 APT 攻击的检测成功率并减少误报。

1.1 产品特点

1.1.1 部署特点

- ◆ 系统使用旁路部署方式,不影响被检测网络的和服务器的正常运行。
- ◆ 可进行集群部署,方便系统性能提升。
- ◆ B/S 管理架构,使用简单。

1.1.2 检测功能

- ◆ 使用包括沙箱、智能分析引擎、威胁情报等检测技术多维度预警 APT 攻击。
- ◆ 使用综合行为分析关联并呈现更深层次的攻击行为。
- ◆ 支持 Web 等协议的快速解析。
- ◆ 内置大量安全检测策略,全方位满足不同用户的使用需求,安装调试简单便捷。
- ◆ 云端大数据分析,基于机器学习和深度挖掘等技术,实时共享最新安全威胁情报,快速预警新型恶意
 威胁。

1.2 产品功能

明御®APT 攻击预警平台具有以下八大功能模块。



一、导航

分为导航、失陷主机、攻击溯源三个页面,用于展示各类告警信息。

- ◆ 导航包括: 攻击展示图、紧急事件总数、24 小时紧急事件、各阶段风险等级的统计、攻击源区域排名、
 高危风险类别和恶意文件总量。
- ◆ 失陷主机是对失陷主机事件、回连区域进行统计、最新事件等,并且通过图形化界面展示。
- ◆ 攻击溯源对攻击主机个数最多的情报事件、情报事件类型分布、威胁活动、情报事件攻击进行展示。

二、分析

主要包括分析(紧急事件分析、主机威胁分析、失陷主机分析、情报事件分析、攻击者视角分析、受害者 视角分析、脆弱性分析、流量统计、统计分析、登录行为分析、抓包分析、PCAP 文件上传、威胁情报检 索)、文件分析(文件威胁分析、回连域名/IP、文件审计、文件上传)、域名分析(受感染主机、C&C 服 务器、高频访问同一域名)等功能以及文件审计和规则配置功能。

三、风险

对不同类型、级别的风险进行查询和处理。

四、资产

通过对流量中的 IP 地址、端口等进行统计,对网络资产进行主动发现并快速识别未登记资产,可基于特定应用或服务对内部资产进行梳理(系统类型、IP、域名、端口等),查看资产端口暴露情况,特别是以非标端口提供的服务情况。

五、报表

提供综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类型的报表,支 持报表导出功能(导出格式分为 HTML、PDF、Word 三种),可定时发送天、周、月报表。



六、探测器

探测器主要用于监听各种类型的业务操作,完成数据采集和分析任务。

数据中心可以对子探测器进行同步验证。

七、配置

配置功能包括常规配置(设备自身运行相关的基本配置)、检测配置、联动配置、数据外送(NTP 模式) 等功能。

八、系统

系统菜单功能主要包括权限管理(用户安全设置、IP 访问控制等)、数据维护(出厂设置)、系统资源、升级管理(手动升级、云端配置等)、许可证、日志管理及其他功能配置(SNMP 配置、网络配置等)。

1.3 角色与权限说明

系统缺省的四种角色和用户如下所示。

用户	角色	对应菜单权限	初始密码
admin	超级管理员	系统所有权限	Dbapp@2014
analyzer	风险查看员	具有首页、分析、风险、报表等菜单权限	Dbapp@2014
config	配置管理员	具有探测器和配置等菜单权限,包括配置引擎、	Dbapp@2014
		策略、探测器、风险通知等	
system	系统管理员	具有系统菜单权限,拥有系统级别的配置、权	Dbapp@2014



用户	角色	对应菜单权限	初始密码
		限管理等操作权限	

1.4 登录系统

操作前提

- ◆ 用户已经获取 APT 的访问网址。
- ◆ 用户已经获取系统登录账号以及账号密码。系统默认的用户名和密码为 admin 和 Dbapp@2014。

操作步骤

Q

步骤1. 打开浏览器, 输入 APT 访问地址 (APT 设备的网络主机 IP) 并回车。

为实现最佳浏览效果,建议使用最新版 Chrome 浏览器或者火狐浏览器。

步骤2. 进入登录页面,输入用户名、密码、验证码进行登录。

	_			1	
		首次登录重置密码			
	· 8~8	1000			i i
	() veen		18		
	- ###	2011/0101			
	* 通过新闻的	Baran (Ball)			
		*0 EA			
			*	8266	
	20周点查打药,煎提	2, 20 K 10	0.2		L. 1 ()
研研	直击新型网络攻击	nuiz	67761 William	naid	



初次登录后参考界面提示进行修改密码操作,且密码不能设置为初始密码。



步骤3. 配置当前位置所在城市,添加方式请参考地理位置设置。

当前位置所在	城市		×	
▲ 设备部 网IP地址	警位置为单位出口或内网时, 止,以保证检测功能正常运行	需在 【地理位置设置】 中完 了	整配置内	A.
* 省份	-选择省	Ý		S. Ç
*城市 [选择市	~		-27
设备部署位置: (▶ 单位出口或内网 🛛 🔵	城域网		ST.
	多前往配置の	确定 じ取消		
	Y3		443	1

1.5 产品形态

APT 有三种产品形态: APT 模式、独立沙箱模式和 PTS 模式。独立沙箱模式和 PTS 模式产品形态见对应 产品的*用户手册*。

登录成功后,默认进入导航页面,显示 APT 检测到攻击事件的统计和大致分布情况,如下图所示。

1.6 设备身份



部署单台 APT 设备,系统默认设备身份是数据中心(探测器)。

分布式部署场景下,需要用户使用串口方式设置设备身份。具体操作请参考《明御[®]APT 攻击预警平台 V2.0.67 快速部署手册》。

设备身份主要有三类:

- ◆ 数据中心:在新增探测器时,会把对应的探测器进行出厂设置,然后将数据中心全局配置同步到探测器上。
- ◆ 探测器:负责采集数据信息,采集到数据信息后,会把对应的风险信息、报表信息等都上传到数据中心。
- ◆ 数据中心 (探测器) : 具有数据中心和探测器的双重功能。

用户在不同身份的设备上可见的功能页面及操作权限不同,请参考下表。

设备身份	权限说明	菜单功能分配						
数据中心 (探测	拥有所有系统的操作权限且	日前 公托 风险 次立 捉主 探测器 配罢 乏法						
器)	自身会采集数据	马加、刀竹、八陋、页厂、放衣、休冽品、癿直、厼尓						
粉提中心	拥有所有系统的操作权限但	日前 公托 风险 次立 捉主 探测器 配罢 乏法						
数据中心	自身不采集数据	- 守刚、刀竹、八陋、页广、 扳衣、 休 冽 品、 出 直、杀统						
探测器	仅有采集数据权限	导航、分析、风险、资产、报表、探测器(仅查看)、系统						

查看当前设备身份

点击 APT Web 界面右上角 "admin" 图标, 在弹出的菜单中选择 "当前设备身份" 查看当前设备的身份信

息。







2. 导航

2.1 导航页面

用户登录系统后,默认进入导航页面。该页面主要对各种类型的告警数据进行统计分析,并通过图形化方 式展现。

导航页面主要分为以下 8 个区域: 1.统计信息、2.风险趋势、3.流量分析、4.攻击展示、5.高危风险识别、 6.攻击源区域排名、7.紧急事件/高危事件、8.语音告警。



2.1.1 统计信息

导航页面左侧的统计信息(区域 1)显示统计周期内发现的紧急事件数,包括紧急事件总数和未处理事件 总数;以及恶意文件数,包括恶意文件总数和已扫描文件总数。

统计周期默认为 24 小时, 鼠标移到 "最近 24 小时"可切换不同的统计周期。





如果统计信息中显示的紧急事件数或恶意文件数不为 0, 表示用户网络环境中存在紧急安全事件或恶意文

- 件,应尽快对感染主机进行安全防护。
- ◆ 点击**紧急事件数**/总数下方数据列出全部紧急事件,或点击**恶意文件数**/扫描总数下方数据列出全部恶意文件。
- ◆ 点击单条紧急事件或恶意文件查看详情。
- ◆ 如果确认已经处理完毕,在弹出窗口中点击<处理>关闭选中的紧急事件或恶意文件,如下图所示。

- BBBIAPTICA	445 - 11						test (shie)
30 预算平台 ann.trainin		State of Landau					1
	Lation of the second se		approximit, arrests	hisparter.			
	ALISIDA: - BOLA						
50/6.0575	an merenne. Hunk (2.17)	8215. 88542 (1021,01181096).	BC		And the local data and the start		
	1000-12-17-1 (0.270)	AATTI TAPUPUNTAN			Million In Charles and Artest		
11.11	40.71 (000-12-17)	44107 1021212010000	REPRINTED TO A		Million and a product segment of the		
	1.20 1.20 2000-12-12 2000-12-12	Addit INCLUSION	STREET FRANCISCO	n completents.	Marine Ar paragonation Million Ar paragonation		
	1000-12-17-1 1000-12-17-1	eetos toszczelentemo.	1000111415-0 W		MERCUN STOCKS AND STOCK		
	1000 10 10 10 10 10 10 10 10 10 10 10 10	1420309 1420309 1000	selection of the select		REPORT OF CONTRACTOR		
	1000 10.17 T	bielle therease	10000 (110 (5.00) (5.00)		Harrison C. (1999) and a spin print Harrison C. St. (1999) and the spin print Harrison C. St. (1999) and the spin print		
ena enamelo							
The second second	AND TRACE	1007 Jos 1	A A A A A A A A A A A A A A A A A A A	it storiae	Sciences Sciences 10 House	0.0000 2000-12-07 (See 10	Activati 2004-10-17 No.IM dt
THE LOOMAN DESIGN	Tana Sana Column		1. • 10050 6540 6100		REAL CONTRACTOR		NUMBER OF STREET

2.1.2 风险趋势

导航页面左边风险趋势(区域 2)显示统计周期内各阶段风险的总数和走势图,方便用户了解风险告警的

走势情况。

折线图中蓝色表示低风险,橙色表示中风险、红色表示高风险,如下图所示。





点击各阶段风险下方的数据可以展示全部风险信息,点击单条风险信息查看详情并进行处理。

Racento - HOUD		#80±45	RADE CARE				
	8015						
2020-06-24 11486-45		110		Et al.	1000		305
2620-06-241146-80		10000-000	4 11572-01		200	1917 http://16.50.22.21/IBRD/hers/scheduleCenter/spilatelebMe.	
2020-06-26 11289.29		2523-08-2	411/08/42			POST http://10.30.22.21.0003/hers/scheduleCenter/cyclateIoMite	
ALL9-08-24 13:07.36							
2020-06-26 11477.14							
2000-04-24-1147.81							
adde-seller 1940Ale							
7879-06-24110707							
2028-06-24 1147/86							
2020-08-28 1147/68		AL-4-0548					
2020-00-0411406-09		10.12	2002240107110000100				
211.05-08-24 11:06-81			THE DESIGN TO A COMPANY OF LA PARTY	20 C			
			L'INFERTATION CONTRACTOR				
		(Inclusion)	ense				
2020-00-24 1146-06			POST Help/U/10/90/22/21 # #00/	hereite beier anne jegelete beiete ageste			
1003-08-2411-05-89		WICH.	Here: 10.51.17.21.0000				
2025-06-2411-05-56			fibenetlens korp aftre				
			Accept 12				
2128-09-241145112			X-Requested With: XVLHop40	ingest			
1010-06-2411-0511			Con Agent Martia/Ld (Mach	Handli, West Mac OL X 10, 15, 41 Applettisted 3/517	Migorial, the Getter Over	eq/843.0147.115 hats/\$517.36	
			Origin http://10.10.20.214am				
			Referent Http://10.30222.21.888	O/huma/hickenderkeConder:			

2.1.3 流量分析

流量分析 (区域 3) 从吞吐量、HTTP、DNS 三方面显示当前实时流量情况。





2.1.4 攻击展示

攻击展示(区域 4)通过分析 APT 捕获到的攻击行为,结合相关坐标信息,以图形化方式展示最新的攻击行为,包括攻击源与攻击目标等信息。点击攻击路线可展示统计周期内该攻击路线发生的高风险事件。

攻击展示图每隔 5 分钟刷新一次,只显示高风险的攻击行为。



点击单条风险事件查看详情并进行处理。

IT MAYOR			100.115						1 - 11 - 11
2010			Dente:						
200512-121546.07	tiel		10.00		RUNT	ing is			816
200112112194220				7 1542.22			2051 (vite-	10064/	8.8
2020 12:16 18:85:07									
2020-12-16-1622-0									
2010/12/14 18/21/84		100							
2020.12 15 15 (140.00)		100							
2610-12-15 18/25/81									THE COMPANY OF
			11 100 11 11 11 11 11 11 11 11 11 11 11 11	And Annual States of the State	ALL CONTRACTOR OF A DESCRIPTION OF A DES	ny foot arrite Final Augusta Angela Angela Chanacour (1400 Augusta)	112 رطبت المع		11490004/114000

2.1.5 高危风险类别

高危风险类别 (区域 5) 展示统计周期内的高危风险攻击的所有类别,点击风险类别名称展示统计周期内



该风险类别的所有统计事件。



点击单条事件查看详情并进行处理。

SHUMBER - WIND	utani.	1P±180	A SHE SHORE				
121		BUSE					
2020 12:17 1657:50	218.75.109.58	0.000		100 million	and the		(15.57)
2020-12 12 16:56:26	218.75.106.18	12020-12-	17 165736	218/75/105/28	100	POIT http://www.hirtunice/inflig/Terriny/18/00-12-11/v4/	RIDER-7140-4- 2 0
2009-12-17 16:52:50	208.75.106.38						
3939-12-17 1658-49							
3839-13-1716-4836							
2029 12 17 10 28:54	210.75.100.38						
3529-13-17 1619-36							
3129-13-17 1642/14							ويعاندريكا ومعمد
2829-12-12-19-660							
2829/12/17 154640		11+43.0					
2000-10-17.15-46(19	118.25.25.29	1946	201212105258000000				
2020-13-17 15 44-41		-	ADD WEREHELD DWELLST TRUEL AND				
2020-12-17 15:42:04			the state of the state of the state of the state	A REAL PROPERTY AND INCOME.			
2000-12-17 15:55:21		00102	GACTER .				
3339-13-17 15-35-19		12.7	PDSI http://wphthc.jctuFilsTeent	2020-12-17,64793987-2645-4414-abolt-0910-baselasT	fan mere		
3829-12/17 15:35:16		HEF.	Hestryphytogen.				
0009-12-17 15:85:11			Control Longto 262				
0101-12-17 15-55-10			Original Interactions Party of an				
3939-13 17 19:19:09			Uppede wordere dispertent				
3000-12-17 15:35:00			UKB.1				
			Utar Agent Mitchig/Lil (Macintonia Accept test/Med.application/simile	Trind Max CIS X TO, 15, 4) AppleWebbb/527 36 (RHD) enviloppilization/endig=0.00/energiev/Unioge/webb.2	8, The Gedu) Drive negations,"/")s:03	ny (15.6,400), 102-5a (arg 17.50) a gain (artiste (Signed Sector percent) (19.9), 10.0	

2.1.6 **攻击源区域排名**

攻击源区域排名(区域 6)展示统计周期内风险事件最多的 6个攻击源区域(国外数据大于 3条时会显示

国内3条+国外3条)。点击攻击源区域名称会显示指定攻击源区域在统计周期内的全部风险数据。





点击单条事件查看详情并进行处理。

收出期区域种名一标用			AG89注44. 米3239 143.00					
	-	P.1.(1)	Part O.					
2020-04-28 17:15:15		2.198	IHE		100 Pt 40		● 使用 使文	BICS.
2020-04-29 17-1614		10200	2020-04-20	17.15.14				12.0
2020-04-36 17:18/14		(a.217	1020-04-25	12:18:10				-3.05
2000-04-35 17:15:13		5-492.703	2020-0=-20	17.18.15				2.0
2020-04-28 17:16:13		10.242,46	2020-04-20	a traterte				12.40
2020-04-28 17:15:13			2020-04-20	12:18:16				2.45
2008-04-08 17:15:11		22020						
2020-04-38 17:16:10		\$2,291,129						
2008-64-28 17:15:00			AUG E C	vett: 200428171				
2020-04-28 17:15:03		1.6.69	基本信息					
2020-04-28 17-15-03		37.8.89		plant ar ven				
2020-04-28 17:16:00			IN PROPERTY.	aucodate.				
2000-04-28 17:16:02		3.6.65		THE OWNER WATCHING THE PARTY OF				
20012-04-05 17:15:02			ST BEATTERS	201420111140200	16853_1.pre#F			
2003-04-28 17-16:02		5.6,11	电击机线	wid				
2020-04-28 17:18:02			12290	23900003				
2000-04-35 17:15:00		5.6.13	In starting					
2020-04-38 17:15:00		200.500	Annual of part of	an and any set of a lot of the	72 00 00 00 00 10 10			
2020-04-28 17:14:59			10010 : 00 P	00 00 00 00 00 00 00 00	90 90 00 00 00 00 FF	FE		
2020-04-08 17:14:59		8.4.141	10020 1 00 0	AO DOO BEU III AIZ AO2 112	50 43 70 4E 45 54 57	4F		

2.1.7 **紧急事件/高危事件**

如果在统计周期内没有发生紧急事件,紧急事件/高危事件窗 (区域 7) 会显示最新 12 条聚合高危事件数

据,手动刷新页面更新数据。

和時			
8 <u>-3 #158</u>	收击时间	Vにまま10月	埃击时间
2020-12-17 19:31:38	2020-12-17 19:15:11	2020-12-17 18:34:33	2020-12-17 17:01:28
原記主約	歴史主約	使业主机	/經驗主机
192,168,30,169	10-20-28-217	10.20.165.250	10.20.57.84
ECHI	SDBH	EAM	EDIH
MANAGESTE SILMA	MERINAGER, MANN.	Millionations, and the	MEMANINELIM (MAN)

点击单条紧急事件或高危事件查看详情并进行处理。



No.			MARKE FOR			(1000) (*1
WHEEL THE			(Bred)			
84	MERCENT IN	energian antipart	HAND AND AN AVER STOCKNOW	PRATORNAL DEF.	ACTIN BOX 11 Control respect, service relay	180.52 2.11
	111					
KRGB						
## 2 % PT						
3810-12-10		HALTERLILIET				
2000-12-14						
			ans)()/156/000000			
			an mentalise liveness	BANK) WAREPERFORMENT INCOME		
			DIRE BAD			
			BT kandrepart, ensuring			
			and the expected specification of	Internet and the same case for pressent		
			#2011/17/17/00000000000000000000000000000			
			ar-isite			

2.1.8 语音告警

默认关闭,可在配置页面语音告警打开。

语音播报在导航页面中心处,实时展示符合语音告警的信息。点击语音告警实时列表,可查看该风险的原始风险数据。

点击 美闭按钮可在导航处不展示实时播报的情况,点击右下角的 可恢复展示语音实时播报情况。



点击右下角的告警播报 (1),显示统计周期内所产生的语音告警,展示了语音告警的发生时间、风险类型 及风险等级、探测器名称、播报状态。点击风险名称可查看该风险的详细信息



5-1046GPril				
3341R	TUR EVA -	2000 LIN	#BIRE	
#1018-12-17 12 2848	\$1513.545 L \$1644 W/D \$2	WILLIAM BORT THE	2382	
3009-13-17 13-2529	HINKALD-HINKE	APTROX MIRE * YO	2008	
2000-12-17 17/27/24	X RITE FOR DEPARTMENT	AVIDABIT	EWN	
ward 10/11 thunse	N.X.LADOLING HARMOND	and the Bill Tur-	in the second	
2008-10-07-0728-201	SCH JEZZEL J VILL BON (DTB)	APTINA WEITER	1284	
2009-12-1717/2189	WHEN PROVIDED AND A REAL PROVIDA REAL PROVIDA AND A REAL	AV160182710	12010	
1000-10-17-17-24-50	SCHOOL STORE STORE STORE	APT 100 100 100 100	201	
and that realize	Ministration and a second	ACTION ADDRESS OF	1983	
2000-12-17 that is	BORDER PRODUCED AND THE REAL PROPERTY AND A DESCRIPTION OF A DESCRIPTION O	AVI TION BEET FOR	1988	
2009-12-11125ce	SHILPOLP-THE COLD	HARD BEFORE		
3005-12-17112454	#8343001=C100000	人口な出版明平田	2388	
3003-10-11 11(443)	SELECTION	Annual Hotel or	2002	
auto-12:17 13:24:17	2.514.7421.229 Hot (5.2	W/T tout Mills File	0.040	
2003-10-111121:54	SCHOOL WEAK STORE	ATTILL BETTE	1100.0	
3005-12-17-2044	HERE FOR DESCRIPTION OF THE PARTY OF THE PAR	AV1303 MINT N	1988	
800010.17174109	XRINGCOMPANY	APPENDENT		
(010-14-11 11um/10	STREET, DOOR HALF	AV100x000000000	1984	
3000-10-17 1101108	SIN- DEPOSITOR	AV10.000010	1283	
1008-12-17 1729-21	#162475421=C24.0.00#	Add 185 C MINE THE	1200	
ann is ir itaane		APTROX MODE NO.	CHE	

2.2 失陷主机页面

在系统菜单栏点击"导航"菜单下拉框,选择"失陷主机"切换到失陷主机页面。



失陷主机页面对失陷主机事件、回连区域进行统计,通过图形化界面展现最新安全事件。页面默认 5 分钟 刷新一次。

失陷主机页面主要分为以下 7 个区域: 1.风险类别排名、2.回连区域排名、3.风险事件、4.失陷主机 IP/黑客 组织、5.失陷主机事件、6.最新事件、7.失陷主机数。





2.2.1 风险类别排名

风险类别排名 (区域1) 展示统计周期内失陷主机相关的风险类别排名。

① 远程控制	
2 121	

点击各类风险排名柱状图展示统计周期内指定类别风险的事件总数、趋势图以及最新的8条事件信息。

点击单条风险事件查看详情并进行处理。

_ 阳御∆PT1⁄2圭	导航 分析		风险 航产		<u></u> 成产	服装	設調業
の 预警平台 展時度 単位	*####		allezet a	905.			
NEWRICK		autility	1988 18 () 8 ± 5 ()				
()	16491990	790	1948	2012172006410	000040		
4 🕾				STATES (SIVI)	BIDERINE Skoryald]		
O Constant		\sim	8495	头描注机			
4 105.00			1877	WIRONSES H	10.20.120.150] #HEEELW	D-mostomory.ww	
a decession			-	0 (1876)			
			DNS#0019	0+104.27.128.22 0+172.67.219.29 0+104.27,129.22	前在他にLDUDFLAKE.COM 所在他の間、TTL34 所在他CLDUDFLAKE.COM	A, TTL::34 A, TTL::34	
			Billigan.	2012172005410	000060.map; 8		
	10.20.25.225		北田田田	5.85			
			10.43	MAN (REF			
			404615	Unor#B#B. 1	C-2/TEX/1/I (HEDDOS/RA		
		1111	10000	Skeeysh			
			RADEXS E	弟出 Skoryah			
			和产物内积				
	(*R±	(atto	(PtRA)	10.11.34.67:5215	D de		
I REEMES	16 26						

2.2.2 回连区域排名

回连区域排名 (区域 2) 统计 DNS 流量下对恶意域名进行回连的区域排名。

回连	区域相	洺			
杭州	-	日本	•	美国	-
31		14		12	
韩国		乌鲁木 齐	-	广州	-
8		7		5	

点击回连地区可展示统计周期内该地区发生的回连事件列表,点击单条回连事件查看详情并进行处理。

🟹 安恒信息



网络区域神名 - 北京		MERV:±H1	未处理 [] 秋田 [100
100	HERE AL							
2129-12-17 20/01/03	10.11.41.249	and the second		副古田 中	100265	-82		操作组
2020-12-17 19:56.06	10.11.28.176	2028-12-1	7 20-01-01	114,112,54,14		STONSENS (0.20120.1501 Million or	nadz 2 49
2020-12-17 19:40:19	10.11.41.57							
2020-12-17 18:28:57	10.11.28.2							
2020-12:17 16:24:54	10:11:42:247							
2020-12-17 18:52 14	10,11,41,57							
	10:11:35.104							
2020-12-17 17:24:55	10.11.34.237							
2020-12-17 17:24:17	10.20.20.48	M-1-0101						
2020-12-17 17:18:43	10.11.44.30	.1942	201217200103000340					
2020-12-17 17:07:54	10.11.37.134		- marrie rivelloweath	ME CACIL				
2020-12-17 17:05:34	10.20.5.5		100	all control of				
2020-12-17 17:08:27	10.11.4E201	BITRO	则用主机					
2020-12-17 16:59:11	10:11.36202	通知	法用DNS和目標[10.20.1	120.150 WWWS: unrad.echements.co	a Cl			
2020-12-17 16:58:96	10.11.32.96	10.5751	0.04230					
2020-12-17 10:54:55	10.20.00.233	APRIL CHIEFE	10-11-11-11-1-1-10-00	6.00 TL 4TL				
2020-12-17 10:53.04	10.11.37.149	8	ULTI4,11234.13. INTER					
2020-12-17 16:49:39	10.20.5.142		BUTIAL112.54.11, HEER					
01000.10.17 16-68-04			CHOICE AND ADDRESS					

2.2.3 风险事件

左侧圆环(区域3)外环以**失陷主机**为视角,展示以失陷主机为事件类型的风险事件,其中外圈展示威胁 情报事件,内圈展示非威胁情报事件。

失陷主机分布在亚洲、美洲、非洲、欧洲四个大洲对应的 1/4 圆环中。如果一个失陷主机多次受同一大洲 地区 (如日本、韩国)的攻击,默认展示最后一次发起攻击地区;如果一个失陷主机多次受不同大洲地区 (如韩国、法国)的攻击,则分别在亚洲、欧洲两个地区中展示对应的信息。

圆环内每个矩形方块代表一个事件, 鼠标悬停在矩形方块上会显示失陷主机的 IP 和攻击源区域。





左侧圆环 (区域 3) 内环以**横向攻击**为视角,展示以横向威胁为事件类型的风险事件。横向攻击视角外圈 展示攻击状态为"尝试"的 IP,内圈展示攻击状态为"成功/失陷"的 IP;圆环中心的数字表示统计周期 内横向攻击事件的攻击者 IP 总数。

圆环内每个矩形方块代表一个事件, 鼠标悬停在矩形方块上会显示攻击状态和攻击者 IP。该 IP 在攻击状 态相同时默认只展示 1 次。



2.2.4 失陷主机 IP/黑客组织

右侧圆环 (区域 4) 左半部分默认展示遭受攻击最多前五位的失陷主机 IP, IP 地址下面的数字表示统计周期内失陷主机 IP 数量。

右侧圆环 (区域 4) 右半部分展示失陷主机事件的名称,默认展示攻击事件前五位的黑客组织名称。名称 下面的数字表示统计周期内失陷主机事件原始数据的总数。





鼠标点击左半部分的 IP, 在滑出窗口展示以下信息:

- ◆ 左上角展示失陷主机的 IP、被攻击源地区、被攻击总次数等。
- ◆ 下方展示失陷主机的被攻击关系图,关系图上的节点表示攻击者,节点之间的数字表示攻击次数。
- ◆ 鼠标悬浮在攻击源的节点上显示攻击源的 IP、地区,如下图所示。



鼠标点击右部分的黑客组织事件,在滑出窗口展示以下信息:

- ◆ 左上角展示失陷主机的黑客组织/病毒家族名称、攻击事件总数。
- ◆ 下方展示失陷主机事件的攻击关系图,关系图上的节点表示被攻击者,节点之间的数字表示攻击次数。
- ◆ 鼠标悬浮在节点上显示攻击源的 IP、地区,如下图所示。



2.2.5 **失陷主机事件**

失陷主机事件(区域5)以柱状图形式展示统计周期内各阶段失陷主机聚合事件的次数。



点击柱状图或柱状图上的数字展示该时间段的所有失陷主机事件列表,点击单条事件查看详情并进行处理。



杭州安恒信息技术股份有限公司

了安恒信息


2.2.6 最新事件

最新事件(区域 6)展示最近 9 条失陷主机事件。左侧的竖线表示风险等级:蓝色表示低危,黄色表示中危,红色表示高危。

事件部分展示风险详情、事件名称、发生时间。

最新事件	
192.168.10.201发生隐蔽	信道通信事件
	16:02:55
安生	远程控制事件
威胁情报——普通远控木平	马事件 16:01:59
性远程的	制事件
威胁情报——恶意软件	16:01:59
192.168.10.201发生隐蔽	信道通信事件
	13:42:55
	控制事件
威胁情报—普通流氓推广	「事件 13:33:43
发生	远程控制事件
威胁情报——普通远控木马	骑车 13:33:42
生远程的	制事件
威胁情报—恶意软件	13:33:42
10.20.28.119发生隐蔽信	道通信事件
	13:33:39
发生挖矿	事件
BLACKLIST DNS reque	st f. 13 33 37

点击单条事件展示风险名称、域名、攻击者 IP、攻击源地区、受攻击者 IP、发生时间等详细信息。





2.2.7 **失陷主机数**

失陷主机数 (区域 7) 以柱状图形式展示统计周期内各时间段的失陷主机数量。

失陷主机数

鼠标悬浮在柱状图上显示具体时间段和该时间段内的失陷主机数量。

2.3 攻击溯源页面

在系统菜单栏点击"导航"菜单下拉框,选择"攻击溯源"切换到攻击溯源页面。



攻击溯源界面展示 APT 攻击的溯源信息,主要分为以下 5 个区域:1.攻击主机个数最多的情报事件 TOP10、

2.威胁情报告警类型分布、3.IP 查询、4.威胁活动、5.3D 展示。



2.3.1 攻击主机个数最多的情报事件 TOP10

攻击溯源页面左上角(区域1)展示统计周期内发起攻击次数最多的情报事件,最多展示10条。

	攻击主机个数最多的情报事件 TOP10
	JSClicker点击默诈事件
2	bitter
3	
4	普通流氓推广事件 ■
5	普通远控木马事件 ■
6	隐蔽信道通信 1
7	1994° I
8	TrickBot窃密木马事件
9	APT-C-35
10	C&C

点击柱状图展示统计周期内该情报事件聚合的 IP 风险信息,点击 IP 展示该 IP 相关的风险详情列表,点击

单条风险查看详细信息并进行处理。

● 预警平台	FURITMET 10.11.43	ris .	-	x12-0	
HOLESHIT		IN NEW YORK			
			12.8.638		
STATES AND SHARPING IS IN	2509-12-17 1455-08			and the state and second second	
	202012-17 1855-08	THE CO			
the second se	2520-12-17 14-55-00	- in the		Bandra Liversteinsburger Constituenty	
12			91.22	milletsh,	
States and			187	BEINSBUR	
Concession of the local distance of the loca					
Contraction of the local data	2939-12-17 14:12:07				
a (11)			自動的公司	201113/00000001ecent 🗑	
	2020-12-17 14:52:37		地生物生	th.	
6.HEN2			2012	#Tr05	
In TRANSLER			-	Analysis and the distance of the second second second	
a thread			CT AS	CohMise	
a francis	2011-12-17 1653-06		THE OWNER.	RED CutoMater	
and the second s					
D GUERREN D	2601-12-17 1411.00		REWER		
			2.6614		
	2001-12-17 14:51:25			and the second se	
	20201-12-12 14-11-28		600 L	Electricities/e	

2.3.2 威胁情报告警类型分布

威胁情报告警类型分布(区域 2)从事件角度展示失陷主机各情报事件的占比。左侧数字为统计周期内各 类情报事件的总数,圆环中间展示各类情报事件在统计周期内发生的总数、名称、占比。

默认展示情报事件统计周期内发生次数前 9 位情报事件类型,低于前 9 位的事件类型将全部统计为"其 他"。



点击情报事件对应的圆环展示统计周期内该类型情报事件的风险信息列表(基于 IP 地址),点击 IP 展示

该 IP 在统计周期内的情报事件信息,点击单条事件查看风险详情并进行处理。

杭州安恒信息技术股份有限公司

安恒信息



RECENTION	10.0	·····································	
	単中:11時		
2020-12-17 20.00.47	10.7	基本供用	
2025-12-17 20:03:40		2113 21 7 21 MBA (750 0000)	
2029-12-17 19-5M-18			
2020-12-17 39:56(45	1194	AR (Inferites) (Infertes) (Infertes)	
2020-12-17 19-51-05		NITES STREET	
2020-12-17 154617		ar growing Elsens 1	
2020-12-17 19-45:50		###### 0 (0210)	
2009-12 17 19:39:19		OVEREIN	
2020-12-17 19-34(12)		a .	
2020-12-17 1630-21		15 (F1,5.9) 201217200147000020.0cm H	
2020-12-17 19:24:04			
2020-12-17 19:27 47			
2020-12-17 19:24:50		REAR WRAN	
2009-12-17 14:1922		CaleMont®-##[1992]1094/00104-5, \$40,000#8405168.	
2220-12-17 Turris		district CoolMiner	
2020 12:10 19:10:02		Marchelle BD Combiner	
2020-12-17 10-03-57			
2020-12-17 1902-00		#Fwith	
2020-12-17 (6:58:10	Yax		
		Has I	
		MALUEE 35 254	
		2010/01 WAY 6281720344001 HBE30299995	
		NET GALLER	
		FRM	
		MACESE AA. OT	
		HDE28M DNS	
		1111100 前兰 Hittin A. Mos 711 Hittin S.2. A 14 odds	
		分析与微致	

如果统计周期内记录的情报事件类型超过 9 类,点击饼图下方<其他>展示统计周期内所有情报事件的名

称、发生次数以及占比,默认保留1位小数。

No. of Concession, Name		成的情報告望的		
	17842			
	100		25.79	
	DOMES			
	2024		12.4%	
	Inclusion and Billion			
	HADDA/BIC		1.7%	
	NACES:			
	DIC		3.7%	
	BALLO SILGHT			
	Liber		10.000	
	10-MER WE			
	Management and warpilling			
	Toolor@W.#1580			
	Wattalline			
	Completion			
	10-15 00:00			
	Harrist A GBH			
	Distances faired ChCEH			
	Deportikitek %			
	71			
	Easter			

2.3.3 IP 查询

攻击溯源页面右上角(区域3)展示 IP 查询框和时间范围。查询时间范围默认为最近24小时,可选择最



近7天、最近1个月、最近2个月。



在 IP 搜索栏输入 IP 或者在下拉框中选择 IP 进行搜索。左侧搜索结果关系拓扑图中蓝色外圈表示被攻击

者,红色外圈表示攻击者,半蓝半红表示既是攻击者又是被攻击者,IP之间的数字表示攻击次数。



右侧列表显示所有匹配的搜索结果(基于攻击过程的时间倒序),点击查看每个攻击过程的相关风险列表,

点击单条风险查看风险详情并进行处理。



100,010		dit i f	ANT DES					
		Press of						
THE OWNER	THE P				100			
		and the	C				- 400	
			menter (record) in	THE .				
		BACTURE .						
					interest Pite.			
			 How equilation of the light of					

2.3.4 威胁活动

威胁活动(区域 4)以攻击链的形式,基于弱点探测、渗透入侵、获取权限、命令与控制、数据盗取 5 个 节点对攻击事件进行归纳汇总。

鼠标悬浮在威胁活动的柱状图上,显示不同攻击阶段名称和该阶段在统计周期范围内发生的告警总数。

l wei	1665 AD	and a second		to)
603493	istari				
ipiń	入僚				
EENK	धरमन	渗透入	æ:397		
ŵ\$	191278 11				
	is in the second				

鼠标点击威胁活动的柱状图,显示选中攻击阶段的所有风险类别名称;鼠标悬停在风险类别名称柱状图上,



显示该风险类别名称和统计周期范围内该风险类别下发生的告警总数。



点击风险类别名称的柱状图显示统计周期范围内该风险类别下产生的所有风险信息列表,点击单条风险信

息查看详情并进行处理。

MINISTER - WITTON		apprent.	NAME AND ADDRESS OF				Depit Set	184		
		and the second second								
				20.0 million				equa	BUE2AD4T	
			10.00010.000			FIRST NAME				
0001-12110-0010-14										
0002-0118-08-05:00	110									
									6	
		approximit.							Statute 1	
			101110-000-004							
			INCOMES INCOME.	trievetHith.						
								Western .		
			Bernine.							
								TRanking.		
			darright treasfing store					and the second second		
			Contact Dright Tree							
								and the second second		
			Henry Provident	Contraction of the second	U. Ji Agentingen, U.	nder Beerg (minister Ar Kenne antigeren Inderen) Manuel () Manuel ()				
			- 454/111 aller (Anfrach Committe Dispositions In Exercises: Types Sealights fault - 454/111 aller, (Anfrach	iabbellitten er den bereitten in darenten dit arbeiterten						
		0.116								

2.3.5 **3D 展示**

失陷主机页面中间的 3D 图形 (区域 5) 展示统计周期内 IP 间的攻击关系。上方紫黑色小球表示外网 IP, 中间的图形表示服务器 IP、下方橙色小球表示内网 IP。默认展示攻击/被攻击次数最多、攻击方式最多或 威胁等级最高的 IP 地址。外网 IP 最多展示 12 个,服务器 IP 最多展示 6 个,内网 IP 最多展示 10 个。





IP 之间的连线表示攻击者与被攻击者的关系,实线表示直接攻击,虚线表示间接攻击。

点击 IP 图标展示该 IP 相关攻击事件详情,包括攻击/被攻击事件关系拓展图、攻击者/被攻击者信息、攻击 过程等。

一 预警平台	titlet +			with the	194	16,7523	H.
A COLUMN A							
Anterest in the second		16(11.32 16(11.32.70) 16(11.22.3) 16(11.22.3) 17(1)) 17(1) 17(1) 17(1)) 17(1) 17(1) 17(1)) 17(1) 17(1) 17(1)	87 S 1925	Real Provide P	HIGHER	10000 1000000	x
S							

2.3.5.1 **攻击/被攻击关系拓扑图**

拓扑图展示攻击者和被攻击的基本信息,图中蓝色外圈表示被攻击者,红色外圈表示攻击者,半蓝半红表



示既是攻击者又是被攻击者, IP 之间的数字表示攻击次数。

点击攻击路线显示"攻击者 IP>被攻击者 IP",同时左侧展示对应攻击者和被攻击者基本信息,右侧展示 这两个 IP 间的攻击事件。



IP 存在扩展攻击行为时, IP 外圈的右上角会编辑有❶图标。双击❶可向下扩展一层, 同时图标变为■, 最

多可以扩展两层;点击-图标隐藏扩展的攻击路线,同时右上角变成-展示之前的拓扑图。



杭州安恒信息技术股份有限公司



2.3.5.2 **攻击者基本信息**

攻击者基本信息展示攻击者 IP、影响的内网主机数、攻击产生的风险事件、风险类别、地理位置、经纬度、 匹配到的情报信息、处理建议等。内容超长时,会显示为下拉框形式,如下图展示。



点击右上角的■图标展示统计周期内攻击者 IP 相关的攻击事件列表。

● 預警平台	04675	inter in the second sec					
A CONTRACTOR OF A CONTRACT	11299			8,7967			
			RENAL CONTRACTORS (1941)			WE REPORTED IN CASE 1/00 WHITE IN LAST ADDRESS OF	
			ROMAN DEPENDENCIER SHALL			HERE AND ADDRESS OF A DESCRIPTION OF A D	
			BANK DINDER OF STREET			IN PROCEEDINGS IN LAN 1993 IN PROPERTY AND INCOMENTATION.	
			DENN CORTANIA (S.C.)	15,78,48,211		APPONDED BOTH LOLING BETWEEN THE ADDRESS OF	
		ASSN 12-18 (Britten)	BURNEL DIVERSION AND DR. LINCO			BOTOMORNER DOLLAR AND AND ADDRESS CONTRACTORS	
		Jaco to change by	SHORN DISTRICTION COCT	1424(017)		HERIOGRAPHIC COURSESS BETWEEN COLDENSING AND	
ALCONDUCT IN CONTRACTOR		2020-12-18-0941-51	STRAIN CONTINUED IN COL	10114540		BEFORE BERTHER DOLLAR DATE FOR BERTHER THE AND INCOMENTATION	
senitat -		VERSION VERSION	EDDALE LETTING AND STREET			WITCH SHE WITCH LITE FOR WITCH AND ADDRESS OF	
		AGE 11 18:08:01:24	STREET, CONTRACTOR STREET, CARCIN.			ALTONOMIA IN 199, 19, 199, 199, 199, MINING THE ALCOHOM STREET	
		2009-10-17-26-0017	STORE CERTIFICATION AND THE CARLS			HERENGER BURGER, SALAR AND AN AND AN	
Sector 1		2525 17.1T 254141	OTHER DISTURBANCE CONTR			BUTCHOUSE THE PROPERTY AND ADDRESS OF A DECEMBER OF A DECE	
Contraction of the Contract			CHARLE CONTRACTOR COLL			BURGHONDER DOUGLASS 1200 WHERE THE ARCHITECTUCK	
			ROMA DEPENDENCE CACT			ADDERVERING COLOR FASTIVE REPORT COLOR ADDRESS	
		and of the leaderst	Retain patron all die Chain		04.0023414	WHEN WERE WORKED AND AND AND AND AND AND AND AND AND AN	
£			Berner pittimetoender mitti			SPECIAL STRUCTURE STRUCTURE STRUCTURE AND ADDRESS AND	
			BRAN DATION (20/22 (201)			ALTERNATION (NO.) 100 RESIDENT ADDRESS (
attentions Off, 1219104044			HOME COTOMERSE LINCE			STREAM STATISTICS IN THE STREAM AND	
NUMBER 2 COMMENSARY			REMARK COMPANYING THE CONCUL			ALL DESCRIPTION OF A PARTICIPATION OF A PARTICIPATIONO OF A PARTICIPATION OF A PARTICIPATIONO OF A PARTI	
HITE-CONTECTIVE RELIGIEST			DUMPS CONTRACTOR STATES	10,15.00.202		OPENING THE PARTY OF STREET, S	
PROTECTION OF THE ADDRESS			RANG DIRITRO AND A 19471			HEPOWORNER DOUBLING THE REPORT OF A COMPANY OF	
NALINGTON AND AND AND AND AND AND AND AND AND AN							

点击单条事件查看详情并进行处理。



REALENCE		#590±51、求处理			
	「読み主新」	(Invested)			
2001-12-18 10:5422	10.1	18250	103196-1	186311 1812	MACE 1
2000-12-18 09:27.19	10.1	2020-12-18 10:34:22		0 MMONSERIER	d Methesu III.O.
2020-12-10 09:11:29					
2020-12-10 09-10:50					
2020-12-10 09:00:04					
2021-12-18 09:02:56	10.2				
2020-12-10.09:01:51					
2020-12-18 00:29:13	10.1				
2021-12-10 00:27:29		用料: 単子(+単) 201710105423020113			
2000-12-17 20:54 17		844019			
2000-12-17 20:01:01		30 2012101014228000110			
2009 12:17 19:40:19		tim minist purchased a	201		
2820-13-17 19/24/54		Dirate Shinki			
2020-12-17 18:58:12			4441592		
2020-12-17 10:57:14		APP WARDPORTUNE I	without the		
2000-12-17 17:28-00	10.45	MATERIA DI CATALONI			
		DALASSAN IN: RECEIPTING			
2020 12:17 17:07:54		B P1 - (Helling)	FTL159		
		Pri Prévaille, 1	murse.		
2020-12-17 10-53-04		11100-11-11 20121110114220000146Lasses	A		
		100000 100			

2.3.5.3 被攻击者信息

被攻击者基本信息展示被攻击者的 IP、被攻击的事件数、被攻击产生的风险类型等。



点击右上角的 展示统计周期内被攻击者 IP 相关的攻击事件列表。

nikim a namh-th		N 114	36	10.1	10.0	1.11.00	KR HH	100 (at 10
の日本の日本	Witness	20						
- Scale showing the	Tarms.				10.7967			west.
I I I I I I I I I I I I I I I I I I I			- BRIER DEPENDENCE CHILI				STOCKED BUILD, OR OF STATE IN ADDRESS TO	
Contract of the Owner of the Ow			STREET DATABASE CALLS				BROKERON (11,20,221,55) WE MILL IN ALTOHNOOD	
			ments (service and the courts)				BETCHCHER 110.21 CA 150 MR MEL TH AT HOUSE AND	
and the second second			where press and the second				Automatical and an and all the second and an	
14			stress nationed the cards				CONTRACTOR (14.2) UN THE MARKET IN AN ADDRESS	
FERENCE STREET								
110-0012972393000007								
The set								
95								
1. BERAMOR THE STONESS								
ALL REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY AND A REAL PROPERTY AND A REAL P								
HIL OTHER CONTRACTOR								
dertuden handlichen								
An American P. H Construction								
TAL FERRIT AND A DOWN AND THE PAST								
ARCHINETHER, BLUCKER, C. LANSING, M. L.								
and a second sec								
AN IT STATES								
C TRACTICATION C								

50								
Contract of the local division of the local								
						DATE OF STREET, STREET		



点击单条事件查看详情并进行处理。

输攻石者详细的原		400141 A-020 1000			
14195	単和主称	Burney .			
2020-12-10 10:34:22		19(10)	SCHOOL 1	100.00 (NEC)	
2020-13 18 01:54:00	inti	2020-12-10 10:34:22		0 WHOWAENE	49168. U. C.
2003-12-18 09:48:34					
2020.13.17 17:07:54					
2020 12-17 10-42547					
		10121010142300000/0-			
		ER	N OK1		
		WINE SHEEK			
		87.06052	allender, S		
		and (state			
		PETAT RESER	08, 77,2199 28, 17,2199 29, 17,2199 29, 17,2199		
		10005ER1 _2012101034220001140.pv	00 B		
		WENT IN			
		M2M3N BLASH			

2.3.5.4 攻击过程

右侧默认展示攻击全过程,包括事件发生时间、攻击者 IP、被攻击者 IP、攻击链阶段。

2020-12-18 10:34:22	114,112,34,14	10.11.37.134	Antes
			and states
2020-12-18 09:27:39	114,112,34,14	10.111.33.106	00 月按3
2020-12-18	114,112,34,14	10.11.39.35	00564
2020-12-18 09:10:50	114,112,34,14	10.20.40.171	aosita
2020-12-18	114.112.34,14	10.11.11.213	· 승수 도단의
2020-12-18 09:02:56	114,112,34,14	10.20.92.71	- - - -
2020-12-18	114,112,34,14	10,11,42,41	6 44158
2020-12-18	114.112.54.14	10.11.13.91	00588
2020-12-18	114.112.34.14	10.11.34.189	
2020-12-17 20:56:17	114.112.34.14	10.11.40.199	-

点击左侧 扩展攻击过程展示区,展示风险标签、攻击次数、攻击状态等更多详细风险信息。



HIE	被击击	Hersteiner	13210406749	20168	政由決議	時度後点
2020-12-18	114.112.34.14	10.11.37.134	前中与15日	1969.5H		9.MR
2020-12-10 09:27:39	114,112,34,14	10,11,33,186	自中社官部	Long 2021		25.95
2020-12-18 09:13:29	114.112.34.14	10.11.39.35	WHERE	LOADER HI		失拒
2020-12-18 09:10:50	114,11234,14	10.20.40.171	09555	DREEM		头脂.
2020-12-18	114.11234314	10.11.33.219	#958M	interio		关后
2020-12-18 09:02:56	114.112.34.14	10.20.92.71	002250	UNTROS		关府
2020-12-18 09:01:51	114.112.34.14	10.11.42.43		10421214		关缩
2020-12-18 08-29:13	114.112.34.14	10.51.33.91	14555	15493244		失間
2020-12-18 08:27:29	114,112,34,14	10.11.34.189	自令与后期	interests		失柄
2020-12-17 20:56:17	114.112.34.14	10.11.40.199	807369	15192961		沃格

点击右上角的<**自定义筛选**>筛选在攻击过程中显示的攻击链阶段。

	自定义筛选
\checkmark	弱点探测
\checkmark	渗透入侵
\sim	获取权限
\sim	命令与控制
\checkmark	数据盗取

2.4 主页 admin 菜单介绍

点击 APT Web 界面右上角<admin>(或其他登录用户名),弹出对应的功能菜单,如下图所示。





将鼠标悬停在"系统时间"、"设备身份"上显示相关信息,或点击"关机/重启"、"修改密码"、"故 障排查" "关于"、"退出"执行相关操作。支持点击"故障排查"前往拍错页面。

菜单	功能描述
系统时间	可查看 NTA 服务器的系统时间。
设备身份	显示当前设备的身份。
关机/重启	关机或重启设备。
修改密码	修改当前用户的密码。
故障排除	进入故障排查登录页面。
关于	查看当前版本信息。
退出	退出系统。



3. 探测器

3.1 查看管理口 IP

管理口配置一般在 APT 快速部署的时候,通过串口程序 1->1 菜单完成,选择管理口设备及修改管理口 IP 地址。详细配置信息请参考对应版本的*快速部署手册*。



此外,可以通过 Web 界面配置管理口,详细请参考 Web 界面配置管理口。

在主菜单选择"探测器",可以查看管理口 IP。

如下图所示,管理口为 eth0,管理口 IP 为 192.168.33.236。

CONTRACTOR	影響平台	1165	116	244	47° NA	102848	878	80%	CONTRACT.
-	out of the local of	and Dess							-
WIELD WEAR	19231982 102.198303								
-									
86	19954	48	antimice (S. M.	annual dist	West-to-	822++450	et. MAR	相应一间和此; 包枯草	976
WOMPETH	(10104333296	Ξœ	Example 1 and 1	200403003001216	14.116/0.1012-68	59		£0	
								N18 1 1	102.0012

3.2 探测器配置



探测器配置功能用于管理属于该数据中心的探测器,包括新增探测器、修改探测器及删除探测器。

3.2.1 新增探测器

在探测器页面,点击<新增>,在弹出的页面输入探测器名称、IP、端口,点击<确定>进行保存。

THE ACCORD		125.00							
200 HH 2	INCOME, MILINAL	1m				22			
-				01000338					
200	MARK.	MD)		BAD DE	1941, REALINGT AND ADDRESS OF	#d-22.4	Annestering state	AN HEREIMAN	Desc
ADDRESS	110.08.04.05	48))	10000000000	- 668	394-3998-194		0	10 M	
				10000	04-0301			- 10 M (1)	345 (M) () 8
				- WARKS	210-101-012122	-			
				· excitera	Al Mari	_			
				180AUE	1949-bend				
				1.0000000	0000 3 0000				
					100				
					1 A 4 4 4	_			

参数说明

参数	参数解释	是否必选
名称	输入探测器的名称。	是
探测器 IP	输入探测器设备的 IP。	是
探测器端口	输入探测器的端口。	是
发送最大速率	配置探测器的发送最大速率。一般使用缺省值。	是
发送主目录	配置探测器的发送主目录。一般使用缺省值。	是
发送时间段	配置探测器的发送时间段。一般使用缺省值。	是



新增探测器必须保证探测器的 sensor 版本和数据中心的 server 版本一致,否则会添加失败。

3.2.2 修改/删除探测器



在探测器页面,点击新增探测器右边的²⁰图标编辑探测器配置项;点击新增探测器右边的¹⁰图标删除探测器。

3.2.3 **升级探测器**

在探测器页面,点击新增探测器右边的 ^(A) 图标,可以升级探测器,即升级版本升级包、策略升级包、排 错升级包。

10.101	PRC 22-941 192 192 192 193 1	134						
-	15.e							
ue .	arren a	48	10010-TE-R	arrorfild .	TEMPOLY.	RET24-HERMET SOLW	MIST-HOMINE SOLID	Atra.
TRAFETA	weite die eine steller	0.0	3 8 4 8 10 7 10 10 10 10	3 (10) 227 33 30-342	16/08720-248			
CHICK AND A	1982 188 No. 207	2#	A CONTRACTOR AND A DECIDE	3.3146.33768.301331	Anatopian	ů.	4	1 1 4 1
							A28	1 24 7.41

若不进行手动升级,版本升级包和策略升级包会隔10分钟从数据中心自动同步版本和策略升

级包, 排错升级包不会自动升级。

3.2.4 同步验证

在探测器页面,点击新增探测器右边的 [《]图标,将数据中心设备配置同步到各个子探测器,实现分布式部署。

ET 9690 E	NECKARD 102.446,193	136						
-	ini i							
659	+124	MB	arrest Dill	arvetit	MALE	WIC2++HFREE MAR	101-10101-010	18411A
ALCOHOL: N	782.04830-258	EW.	2.848.22549.201717	210306.22846.201217	2022665261216.0			
10100	162.165.21.217	2.9	34/64/2007 20125	10.05.71907.001024	10310263010250	140	0	11 1 4 -

3.2.5 配置同步

在探测器页面,点击<配置同步>按钮,可以查看探测器使用的模板;点击 按钮,可以切换探测器使用的同步模板,探测器会按照模板勾选的内容同步相关配置。

17. HINE WALLER HALING	रक्ष:	No. of Concession, Name		10	
and along		222-119			
	85 28 28	A PRIME REPORT AND A PRIME	HILL, DERIGHT S. ABRONNERS Distance, ADRIANES MUNIMA	an entre suit-bein	RA-CONCERN DES 1 D. S. C.
					818 - 🖬 - 1883 - 88 1
		iviwa	107.004	ana	
		/129208	ATU JEN T		

点击<**同步模板**>,进入模板管理页面,可以新增、编辑模板,用户可以根据自己的实际使用需要,勾选需 要同步的配置项。

-		ing ing			
		£39.	ARTIN	NTENTION .	
10 975000999 107000	1788. 1967. Stat Al 200 1967. Stat Bit 1977	88. 23		NE NE <td></td>	

3.3 流量代理 (Agent 代理模式支持)

当 APT 使用 Agent 代理部署方式的时候,请参考本章配置。

3.3.1 **打开 Agent 配置开关**

Agent 配置开关在 APT 设备界面 "探测器>流量代理"上, 默认不会打开, 需要登录 APT 排错平台修改数 据库配置才能打开。

操作步骤

步骤1. 使用 root 账户登录排错平台,登录方法参考登录故障排查平台。

安恒信息



步骤2. 在左侧导航树选择"**服务设置≻数据库管理"**,在该页面下方"**执行** SQL"区域输入执行下方语句。

UPDATE wdd_sysconfig SET val = 2 WHERE FIELD='system' AND item = 'EngVirtualRecvWork';

- 步骤3. 在左侧导航树选择"检测项目>3: 服务器状态检查"。
- 步骤4. 点击 "探测器主引擎"操作列的<重启>。
- 步骤5. 在弹出的提示框点击<确定>,完成探测器主引擎重启。

3.3.2 **配置其他端口**

点击操作项的编辑 图标, 配置探测器接收端口。

编辑探测器接	收端口	×
1.修改探测	器的流量接收端口后,所有正在发送到该探测器的网口都将会重启; 修改接收端口后会重启流量接收引擎,测试链路不能马上成功,建议 §测。	
* 端口:	54321	
	取消 确定	

默认 Agent 发送流量端口与探测器接收端口为 54321,修改端口后会重启 Agent 抓取流量任务以及探测器 接收流量引擎。

3.3.3 测试链路

编辑网口信息,其中 IP 地址必须填写跟管理口非同网段的业务口 IP 地址。点击<测试链路>,测试 Agent 与探测器之间是否连通。

成流量的端口为54321。 开吸端口为54323,如果3	如果竭口被占用,请 配置其他竭口 如何被占用,请 配置其他竭口	
eth0(192.168.33.110)		
APT攻击预警平台		
192.168.33.86		
测试链络	确定	
	 2)法量の第日为54321, 中の信日为54323, 如果 eth0(192.168.33.110) APT攻击棟響平台 192.168.33.86 夏試貨幣 	 送流量的端口为54321、如果编口被占用、简 配置其他鐵口 件切端口均54323、如果端口細占用、適 配置其他鐵口 eth0(192.168.33.110) APT攻击探響平台 192.168.33.86 創試路路 御定

3.3.4 启动/停止/删除网口

网口信息	操作项
停止 eth0 (192.168.33.237) APT攻击预警平台	0 🛛 🗖
◆ 启动:添加完成后默认停止,如需开启则点击对应的 [●] < 启动 >。	
◆ 停止:如需停止网口则点击 [◎] < 停止 >即可。	
◆ 删除: 删除网口会停止 Agent 上相应网口的获取流量任务。	

3.3.5 编辑网口

修改网口将停止原网口的流量获取任务以及启动新网口的流量获取任务。

网口信息	操作项
停止 eth0 (192.168.33.237) APT攻击预警平台	▶ 🗹 💼

3.3.6 端口修改

默认 Agent 过滤端口为 APT 设备配置的端口。

点击 APT Web 界面 "配置>常规配置>基本配置"菜单,下拉到"当前配置 Web 端口"区域可以查看并 且新增或者删除相关端口。

安恒信息



🕘 明朗APT攻击预整3	昭台	96	9.6	93,82	317	新茶	致激展	10.9K	新植	admin vr
DA B	÷ MARCHEWEBIRES	nn:x) (en	•]						
• 2795	Р напасарорзансі (на)									
C HOLE	F BARRENSMIPPED									
	F MERCHIMAPIRCI									





配置部分由**常规配置、检测配置、联动配置、数据外送**四部分组成。

4.1 常规配置

4.1.1 **基本配置**

在主菜单选择"配置>常规配置>基本配置"菜单,进入基本配置页面。

4.1.1.1 风险查询参数

风险查询参数用来配置风险查询信息,配置界面如下。

- 风险查询参数		
查询结果每页显示:	20 🗸	
查询结果记录数:	600 🗸	
查询缺省时间范围:	最近12小时 🗸	
查询结果导出最大记录数:	100000 🗸	
报文最大显示长度:	2000 🗸	
	保存	

配置完成后,在主菜单选择"风险"将按照上述配置显示风险查询结果。

4.1.1.2 时钟同步

配置 NTP 时钟同步服务器,此后 APT 设备就可以通过配置的 NTP 服务器进行时钟同步,包括 APT 设备的系统时间和硬件时间。



分布式部署场景下,数据中心从时钟同步服务器同步时钟,探测器则从数据中心同步时钟。

• 时钟同步			
	*服务器IP:	127.0.0.1	
		保存	

4.1.1.3 连网设置

选择<是>或<否>, 允许或禁止 APT 设备访问互联网。

- 连网设置			
	可访问因特网:	〇是	● 否
		保存	

4.1.1.4 Web 规则配置

针对不同的网络部署环境, APT 提供两套 Web 规则供用户选择。

- ◆ 当 APT 部署在 Web 服务器或邮件服务器等,可选择<外网规则>。
- ◆ 当 APT 部署在企业或单位出口交换机时, 会有大量内网 IP 访问外网, 这些访问容易产生包括 XSS 在 内的一些误报, 为减少误报可选择<内网规则>。

Web 规则配置的界面如下所示,默认为内网规则,切换实时生效。

- WEB规则配置				
	可访问因特网:	•	内网规则	(在监控单位进出口流量时适用)
			外网规则	(在监控WEB服务器进出口流量时适用)
			保存	



4.1.1.5 **会话释放策略配置**

配置会话的 DNS 策略,包括超时释放和实时释放两种。选择实时释放时,系统收到响应后立即释放会话, 会导致会话应用流量统计信息日志量增多,外送时建议关闭 DNS 协议的会话应用流量统计信息。

DNS 超时释放需要等待 30s 会释放会话。

DNS莆略:	超时释放	۲	实时释放	٢
	保存			

4.1.1.6 Web/邮件端口配置

根据自身的网络环境配置审计端口。系统支持 Web 端口、POP3 端口、SMTP 端口、IMAP 端口等配置。

一般情况下,系统会审计这些协议默认的端口。如果用到非默认端口,需要手动增加或者开启对应的协议 自动识别。增加非默认端口或开启协议自动识别后,系统才会对这些非默认端口进行审计。

APT 设备默认会对 Web 非标端口(如 8899 端口)进行审计,但默认不审计邮件协议的非标端 口。



Web/邮件端口配置界面如下。

F INANACIO BO X	EWEB4861	8080 ×	443 (SSL1087)	468 (SSL30E)	+新語	
P 当的配置 110	⊈POP3编口 + 新唱					
F 39629	\$SMTP端口					
25 F 当前配定	+ 新想 創MAP端口					
143	+新環					

默认端口不能删除, 其中 Web 类型默认端口是 80, POP3 类型默认端口是 110, SMTP 类型的 默认端口是 25。

对于加密传输端口,需要在 SSL 流量检测菜单上传证书,并配置端口才能生效。例如:Web 的 443 端口, POP3 的 995 端口以及 SMTP 的 465 端口,具体请参考 <u>SSL 流量检测</u>。

4.1.1.7 **协议自动识别**

对 FTP、HTTP、IMAP、POP3 等 9 种协议进行自动识别,可识别这 9 种协议的非标端口并进行审计检测。

默认开启 HTTP、SSH、SSL 协议。

	• 协议自动说	只别									
		FTP	HTTP	IMAP	POP3	RDP	SMB	SMTP	SSH	SSL	
保存											



4.1.1.8 **功能配置开关**

配置登录行为分析的开关,默认关闭状态。

登录行为分析:	● 是	() 否
	保存	
	登录行为分析:	登录行为分析: • 是 保存

登录行为分析主要针对流量中登录行为进行分析。若关闭登录行为分析,不会对流量中的登录行为进行分 析;开启登录行为分析,可在"**分析>分析>登录行为分析**"中查看具体的登录信息。

4.1.2 地理位置

4.1.2.1 **配置地理位置**

第一次登录系统后,需要设置地理位置,如未设置,用户登录成功时会重新提示,默认添加内网 IP (例如 192.168.0.0/16 等 IP),如下图所示。

EMPAPTING						
(2) 冠盤平台 MGL Burnert					-	
			20	Statistics (
		and a local second		i anti-	- T	
				1000	- 32	
		14 BB		1.20	S. 67	
				1 ×	View.	
		V		7 I	-	
118 - 1996.		-				
		1000				

设备部署位置为单位出口或内网时,需在地理位置设置中完整配置内网 IP 地址,以保证检测功能正常运

行,且需要确认内网地址已经完整配置,否则该弹窗提示将一直会显示,如下图所示。



如需对此配置做出调整,选择"配置>常规配置>地理位置"菜单,点击<新增>,如下图所示。

* 国家:	中国	
城市造際	3形工 / 杭州	· 支持印刷印刷
* IP地址	192.168 1.1/100	例如:单个甲: 192.168.1.10 甲地球目: 192.168.1.100/24(支持位数: 24- 成192.168.1.1-192.168.1.255(C段) 甲状始转: -1
单位地址:	经遗为的-1288段	IPV6版社家: :1/124(支)体位数: 120-128)
内网地址	a 0 8	
	R /8 M ±	

配置完成后,新增地理信息将添加到地理位置设置列表中。勾选当前所在城市所在行,点击 2 按钮可以修改当前城市。

0.0									
T VALUE		-	Contraction, Georgenters	Design and the later	NAME AND ADDRESS OF	LEVEL BAL			
* A*5H		1-300002001 Q 707 00000	HOR 1000						
		ENVIRONMENT N							
5 67108									
- 0900		主动的复数形式							
- MATERIA		10 BA 100 BA	44						
101008		0. 6/2624	PRIS.	104	1948	*0*4	everes.	45	Inhis
(i) FEMILIA		848(12.55.809)	18.0,1460.8-02/16	100.144800	80.204418			/ 💶 :	9(T
C DANCE		R00元十年3月2月2月	teacam	197.144591	Represent			•	1.1
E mana	1	80048-0144	1124645-1121120248	125.144899	scannis			•	0.2
	1	B4R+# 014th	10(0-218	120.144007	W2eeeee			•	1 2
		() (0.000)+(0.001-(0.0))	PRC(6;210)	(20)14420//	30309915				812
								265	at the

4.1.2.2 **导入/导出地理位置信息**

安恒信息



系统支持增量导入和全量导入两种方法导入地理位置。

- ◆ 增量导入是导入与当前列表 IP 地址不同的信息。
- ◆ 全量导入会将系统原有的数据清除,导入表格内的 IP 地址信息,请谨慎操作。
 如果需要导入地理位置配置信息,建议先点击<下载模板>,按照模板内容填写完成后保存,点击<导
 入>。
- ◆ 点击<全部导出>, 以 xlsx 格式导出全部数据。

导入	$ \times $
 ▲ 导入文件暂只支持Excel格式 下载模板 ● 全量导入将覆盖原有数据,请谨慎操作! 	
类型: ● 増量导入 ○ 全量导入	
文件: 选取文件	
取消 确定	

📑 当城市对应的 IP 地址为局域网地址时,国家一栏填写"局域网"即可。

4.1.3 客户网络

对客户网络进行网段划分,标注网络等级、所属区域、责任人、描述配置等,便于用户细化客户网络等级、

区域等。

10 HOLE										
- 8185		- 29	anat	88	10070	ministr	2000. A	847	ROB -	1670 M
- 10012		11 Hert	0.1140.110.1140.239	4	14	121	.0	127125		10 I II
F BORE		g mu.	102.5983-1,702.008.1.2	11						B. (B)
+ 8405		ier@	itanae	1	16					10 II
(i) CHEB	~	and .	0.0111.0.01	- a	16.					10 I
E NARA								A18	65 1 1	80.1.8

操作入口



选择"配置>常规配置>客户网络"菜单,点击<新增>,填写名称、IP/IP段、网络等级、所属区域、责任 人、描述等信息,然后点击<确定>,完成客户网络添加。

 ▶ M ▲ IP/ 	组守软有 1~10 级,数值越入表小重安性越高。 IP 段的地址格式需按照右侧的要求填写。	
	a: 😸 1014 🔢 1014	
* e	ni) Authoritat	
-+ (P)(P	8	2) (2) (2) (2) (2) (2) (2) (2) (2) (
1010	a and	#VX89800 = 1/124(8)94280 120-120
1000	e maileren, min, su, an, final intro-top	
#4	AL BRANDA WAR, MR. THINK, MISPIN	
	B MAXANE, HEAVING	
	40H (MG)	

相关操作

- ◆ 选中多个添加的客户网络, 点击<删除>按钮可以批量删除已经添加的客户网络。
- ◆ 选中单个添加的客户网络, 点击该客户网络对应的 🛄 可以删除已经添加的客户网络。

4.1.4 语音告警

用来控制**导航-语音告警**的开启和关闭,可配置语音告警的风险级别、风险类别、攻击状态、客户网络。开 启语音告警后,可在导航页面查看实时语音告警和历史语音告警。默认语音告警关闭状态。

数据中心可以对探测器进行配置管理,如图所示。

10								
S week			Contractory of the local sectory of the local secto	100.000		and a local sector	100	100
- 314825			- Magin	- Personal	- MARE	81-7401	V-	917.0
- 100018		ALCONG. 1	東井里	18	81	10	00	10.0
- 6770315		1310500				10	.00	R.C.8
							#18 I	383 183 13
- NATIONAL								
+ 10-41582								
@ NINKS	100							
K2 HURR	-							
Et material								



◆ APT 攻击预警平台这一行是数据中心和探测器对自身的语音告警配置;对探测器的语音告警进行配置,语音告警会上传到数据中心进行语音告警。

点击 / 按钮,可以进行配置修改。

编编百音音整		
ti de		
同胞级型	5 2# 5 # 6 # 5 #	
问题类别:	STEAM O WERE TARE O	
取曲状型:	bi⊞ 0 508 0 82≘®	
書/中阿相:	1en2_10 @ 1ec2_102 @	ane sal
	8294 main	

◆ 探测器语音告警页面只能对自身进行配置管理,如图所示。

its:		
风险保护	0 10 0 R 0 P 0 E	
和如果計	全部	
攻击状态	● 全章 ○ 成功 ○ 至成	
袁 户同绩:	±#	1891
	192.47	

4.1.5 NAT 地址解析

针对通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段,

可进行配置字段名读取首次或末次的 IP 地址从而获取真实的 IP 地址。

操作入口

在菜单栏选择"配置>常规配置>NAT 地址解析"进入 NAT 地址解析配置页面。



5 mm						
- 11-12	87.8	9000	+045	#2	0.3,8809	851
- 10100-00	10.14	a forwarded for		•		
+ 0.7294						
- Rene						
· National Address						
- 37-138/B						
E simon -						
C oues -						

点击<新增>可以增加 NAT 地址解析配置。

NAT地址		
状态:		
* 字段名;	xii	
字段位置;	 第次 ○ 末次 ○ 第一个非内部地址 ○ 最后一个非内部地址 	
	取消 神生	

4.1.6 资产识别配置

资产识别配置主要用于资产识别,勾选完成该类资产,将在资产概况中展示该类资产数据。

5.99 E	3		
第 常規配置 ・ 第二型第	ŝ.	▶ 例本原制配置 由产的配配量: VPN和VPN协议类 □ 聊天泉乐美 □ 下数工具类	后程直接供
• 地理位置		6777	
 查戶間径 须复告袋 			
• NAT地址解析			
• mr-inman			
Administrative Admin	2		
C ROCH	~		
巴 数据外送	1.1		

4.2 检测配置

4.2.1 引擎管理

用来控制各种风险检测机制的停止和运行。



操作入口

选择"**配置>检测配置>引擎管理**"菜单进入**引擎管理**页面。

默认行为分析、ARP 欺骗、扫描行为和邮件社工攻击这5个引擎为禁用,其他引擎默认开启。

• WEB攻击		+ 9812\$		3824941041	
恶意文件攻击) 胆绝服务攻击) 翻件社工攻击	
> 远程控制	•	 35-806(2) 		ARPTXN	
★ WEB后门结问		+ #15636	•	+ REMINSO +	
• 行为分析		1297		無他	
DGA域名请求		思敏工具利用)	-		
SMB远腔溢出攻击		• 扫描行为			

点击 Web 攻击下的》图标,展示智能语义分析、WEB 特征、IDS 规则、可疑爬虫或扫描 4 个子引擎。

智能语义分析是把人类自然语言,转化为机器能读懂的代码。即对检测内容进行语法分析,提高规则模型 的适用性。

WEB 特征、IDS 规则是通过内部规则进行匹配产生告警的。

WEB攻击	
智能语义分析	
WEB特征	
IDS规则	
可疑爬虫或扫描	

4.2.2 文件检测

文件检测包含了安全文件大小、沙箱检测配置、压缩文件中子文件真实格式识别、沙箱操作系统设置、分



离文件后缀、恶意文件 MD5 等。

4.2.2.1 检测配置

设置文件检测的相关配置。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>文件检测>检测配置"。

1) 安全文件大小

安全文件大小设置用来设定系统对用户发送或接收文件大小检测的门限。假如文件大小超过设定的门限大

小,系统将不检测该文件。配置界面如下。

安全文件大小		
* 安全文件大小:	10	M (范围1-1024)
	保存	

2) 文件访问过滤

文件访问过滤,是根据客户端到服务端的访问方向对分离文件进行过滤,过滤掉文件不进行安全检测。

• 文件访问过滤	① 根据客户端到服务	务端的访问方向对分离 文	(件进行过滤,过滤的文	件不进行安全检测。
	夕下网->夕下网	◎ 外网->内网	□ 内网->外网	内网->内网
		保存		

3) 文件威胁情报

设置文件威胁情报是否开启。开启文件威胁情报之后可以在情报事件分析界面查询到相关的文件威胁情报

数据。

		As-scourty the dat
- 文件威胁情报		
文件威	或胁情报: 💿 是	
	() 否	
	保存	

4) 沙箱检测配置

沙箱检测配置有两种选项: "检测所有文件"和 "仅检测恶意文件"。两种配置的不同导致检测效率不同。 检测所有文件,会对流量中识别到的所有文件进行检测,检测结果更具全面性,但是这样会花费大量的系 统资源;仅检测恶意文件,只检测流量中病毒木马扫描和静态分析结果判定为为恶意文件的文件,可提升 沙箱检测性能。如果性能不足,建议选择 "仅检测恶意文件"。

于沙斯检测能置					
	沙箱检测配置	0	检题所有文件 仅检测恶意文件	(仅检测病毒术运应图和静态分析检测判定为恶意文件。	可提升20種性現性能)
			保存		

5) 监测结果复用

设置是否复用监测结果。

■检测结果复用		
	检测结果复用:	 是(文件MD5值相同时,不重复检测,复用检测结果) 否(不复用检测结果,重新检测)
		保存

6) 压缩文件中子文件真实格式识别

开启之后,可以检测压缩包中文件格式非真实,或无后缀的情况。

て安恒信息

压缩文件中子文件真实格式识别	
压缩文件中子文件真实格式识别: 💿 是	
保存	

7) 沙箱网络行为

沙箱检测文件时的沙箱行为,包含"API解析"和"数据包保存"两种。用户选择"数据包保存"时,会 在风险查询界面提供保存的数据包下载链接。

- 沙箱网络行为			
	沙箱网络行为:	•	API解析
			数据包保存
			保存

8) 沙箱操作系统配置

当沙箱有多种操作系统时,用户可以选择使用某种操作系统镜像类型沙箱。

2	沙腊镇像名称	沙箱能像类型	沙箱起时时间(秒)	沙箱检测文件类型	描述
	winseven	Windows 7	37 🕅	dii,doc.docm.docx.dot.dotm.dp.,, 🔗	标准winT
	winsp_a	Windows XP	30 🗹	dli.doc.docm.docu.dot.dotm.dp., 🗵	相比/的建winxpt間/Dwps85803

4.2.2.2 **分离文件后缀**

分离文件后缀功能用来配置系统对哪些后缀类型的文件以及哪些协议类型中包含的文件后缀进行分离操作。协议类型主要有HTTP(GET、POST)、SMTP、POP3、IMAP、FTP、SMB、NFS、TFTP。

🟹 安恒信息


操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>文件检测>分离文件后缀"。

14 3 5 1000	- HERRER - LEWISHING			
- ====	5 1989/168			
- 10012				
- 67598	5 和业水对¥问			
- 22/10				
- 1983	2316/18	Nex5	#0	interna.
CONTRACT OF	- n	WTWS2C002LWTW25C002LUMTERCHUW44 PW SHEAPLINTE	•	wiz.
- PERMIT	S 44	UTING THE OFTEN OF THE MET AND AND THE DESIGNATION	•	8.2
- #29522	8.4	HTTP://ITY/SHUHTP/FOUT/SHUBHTP/FOF2/MAP/TP/SAM/MISTTIP		HILE
- 2010	C 14	HTPOHTSSENTRPOYTER, WITHORS, WARKING AND NEED TO		用注意。(
- wranke	A 140	www.enable	•	ar 11
- WIRME	hrd	HEROTETERS HEROTETERS WITH REPORT AND A DESCRIPTION OF THE AND A DESCRIPTION		10.10
- 01008	U initia	HTH GET BALLINT REPORTS WORKTER CONSIGNER THE GAR AND THE	0	14 10
- 1990	(C 1000)	HTHEST SEALHTHPICSTRY MARTINE AND THE MANAGETTIC		MS#10
- 812-180	R #	WINNERTSSQUATERPORTSDUCKERS/WATERCHUMAN FEEDWARASSTEEP		(中)
- 1000BHDN /		HTTP:///TEXELHTTP:///TEXELINTE.POP/JAME/119.344(AP), 1919	•	
- NINWEIDE	0 80	INTERESTIMATING CONTRACTOR SHOP AND	•	10 2
	(C acc)	HTH GETTING HTTRHOST/SIG, SHITE YOR'S WARPER, SHITE YOR YOR YOR WARPER, SHITE YOR YOR WARPER, SHITE YOR YOR YOR YOR WARPER, SHITE YOR YOR WARPER, SHITE YOR YOR YOR YOR WARPER, SHITE YOR	C	11 P 20 (
- marked	11 144	INTERCET/NUMPTREPOSIT/NUMPTREPORTMENT/INDURSTITIE	•	H (A)

配置选项包括<**分离所有文件**>和<**分离指定后缀文件**>两种。在**分离文件后缀**页面点击<**编辑**>选择分离文件类型。

- ◆ 分离所有文件会对所有的文件后缀报文进行分离,包括没有后缀的文件。
- ◆ 如果选择了<分离指定后缀文件>,在下方列表查看文件后缀列表并确保需要启用条目状态列下的
 开关处于打开状态。如需要新增待处理文件的后缀类型,点击<新增>增加文件后缀。

新增文件分离后	錣	$ \times$
* 文件后缀:	请输入文件后缀	
* 协议类型:	HTTP	
	FTP	
	SMTP	
	POP3	
	□ IMAP	
	SMB	
	NFS	
	□ TFTP	
* HTTP协议方法:	GET POST	
	取消 确定	

输入文件后缀,选择协议类型,点击<确定>即可添加成功。保存成功后会在列表中显示新增的后缀类型以及协议类型。

4.2.2.3 恶意文件 MD5

恶意文件 MD5 支持自定义恶意文件信息、新增导入恶意文件信息以及根据 MD5 查询对应的 MD5 文件,

可以让设置的样本经过系统检测产生恶意文件风险告警。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>文件检测>恶意文件 MD5"。

2.9 2.9863	anter anterna anternati				
2 CHEE				(au	
1 2140	янирі	#1012.HIELH	e-trad	10.00	87116
+ PURC	NGC 123 DELETION AND A STREET AND A STREET	田田大村			10
· MOMME				#±9 1 🚺	2007 00 1 2
- 1000m					
+ working					
+ MIDER					

点击<新增>按钮, 输入文件 MD5 值、恶意信息描述, 添加恶意文件 MD5。

杭州安恒信息技术股份有限公司

安恒信息

87.5%		
*文件MD5:	IGM 化无关系	
"高度信息描述	明城人王政信奉指述,长贤用限14年回位	
萨考德德	1010 A 47-1010-10	

支持增量导入、全量导入两种导入方式。



4.2.2.4 压缩文件密码

可自定义设置加密压缩文件的解压密码(若 APT 设备分离出加密压缩文件后没有在本功能中匹配到相应 解压密码,则设备对该文件会解压失败而导致沙箱无法进行检测)。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>文件检测>压缩文件密码"。

2.4E	-	service convictor	E Revents Harvers	VARIANCE		
i anali	1	STREET THE STREET	a sarvinaro marvinitat	Toron(dia		
i) elimitati	121	828				
 (1単同種) 	_	895		*11	¥.5.	941510
 - 33946881 		121		用户标准		0
 IPROMOTE 		Igidževis		利用制度		
 907983630 		machael		AC1010	•	
· 089		1000444		21-15-15		P 1
· WEBISH	1	national		m=wa		
 verzegene iczsami 		yltest		All the last		
• 8070000		D infected		miegel)		
· ARPIER		nopairwind		SHEED.	•	
· 00000608		iii vina		wiezłu,		
 BEX380 					R95 1 1	205-22 812 1
· 03080-028						

杭州安恒信息技术股份有限公司

🟹 安恒信息



 ◆ 点击<新增>按钮, 输入密码添加解压密码, 最多允许十个有效密码, 如果想继续添加, 需删除或手动 关闭某条密码, 系统默认三条密码不可删除。

4.2.2.5 YARA 规则

YARA 的每一条描述或规则都由一系列字符串和一个布尔型表达式构成。YARA 规则可以提交给文件或正在运行的进程,帮助用户识别其是否属于某个已进行规则描述的恶意软件。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>文件检测>YARA规则"进入 YARA 规则配置页面。

東岸	10	*****	areed	at the second	TOP OF BUILD	VARAME			
TO WIRKER	1.00	(LINGEL	1 //PLAITE	at 1975, K († 1910)	CENEXCH-NEW				
 ・		8648	-				Juni Xeen		
 助理位置 		TR-	展现关注	文件名	规则等级	ANDINALE	波加时间	秋西	接性 项
• 藍戸同西			转态规则	CVE-2010-0805	E	cve_rule	2021-05-23-16-0211		A 12 (
• #859			林本规则	CVE-2010-0887	46	cve_nule	2021-05-21 16	•	10 (R) (m)
NATIELEWH			192104	CVE-2013-0074	Æ	cve_rule	2021-05-21 16c		9 B)
(a) 10 10 10 10 10 10 10 10 10 10 10 10 10			静态规则	CVE-2013-0422	Œ	cre_rule	2021-05-21 16		B (B)
· 31222			MORDI	CVE-2015-1701	iii.	cor_nile	2021-05-21 16		≅ 8
+-2440M			#0901	CVE-2015-2426	Æ	cve_rule	2021-05-21 16		国 (图)
Promacat			■衣掘列	CVE-2015-2545	9E.	cvit_rule	2021-05-21 16:		M 1 81.1+5
· RPRMS			60.00N	CVE-2015-5119	Æ	cve_nile	2021-05-21 16:		- (B)
 約22年 			84/05/021	CVE-2016-5195	Œ	cve_rute	2021-05-21 16:		N B (m.)
 WEBIBIE 			INCERT IN	CVE-2017-1188	٤.	cve_nile	2021-05-21 16		≥ 8 …
• WEEE22			新在规则	CVE-2018-4878	£	cve_rule	2027-05-21 16:		10 12
 IDSMBN 			静态探测	Android_adwar	100	deprecated	2021-05-21 16		10 (B) (m)

点击<新增>,在弹出的新增对话框设置相关参数,可以新增 YARA 规则。

新增YARA规	el	
状态		
规则美型	● ● ● 市長期間 ○ 内容規則 ○	
规则等级	○低●中○賞	
* 规则描述:	静态规则	
* RERI	1882# ()	
	取消 構定	

4.2.3 IP 检测配置

IP 检测配置包含 IP 过滤和指定 IP 检测,对应页签括号内数字表示启用该规则的数目。

4.2.3.1 IP 过滤

IP 过滤的作用是不审计在 IP 过滤表中配置的相应 IP 报文。可以通过新增和导入两种方式添加 IP 过滤。

操作步骤

步骤1. 登录系统 Web 界面,选择"配置>检测配置>IP 检测配置"菜单。

步骤2. 点击"IP 过滤"页签。

- 步骤3. 点击<新增>,添加IP地址过滤;或者点击<**导入**>批量添加IP地址过滤。可选择<按单个IP地址 过滤>或<按一对IP地址过滤>。
- ◆ 按单个 IP 地址过滤: 输入 IP 后,点击<保存>即可。当目的 IP 或源 IP 匹配该 IP 后,系统对其报文均不会产生审计行为。

🕜 安恒信息



(円式)建築際:	• EM-T-PROLED # 0 EM-201PROLED #
« IÞ	152,168.3.3
第日:	8080

◆ 按一对 IP 地址过滤:添加的时候, IP1 必填 (支持网段), IP2 (不支持网段) 和端口可以选填。

新增IP过滤		18
Przistetta:	1644-1-Patalisia 💿 16-951Patalisia	
* 1P1:	192,168,8,5 = 192,168,1,1/24 ×	
* IP2;	10.20.13.25	
(P2\$8)	8080	
	電波 電空	

◆ 导入 IP 地址过滤

点击<导入>,导入指定的 IP 过滤规则。导入的方式有增量导入、全量导入两种。建议点击<下载模板>, 然后根据模板格式填写好后导入。

增量导入是导入与列表 IP 地址不同的信息,全量导入是会将当前列表的所有 IP 地址的信息清除,导入表格内的 IP 地址信息。

导入	\sim
△ · 帶入文件支持excell反式 下式模板 • 全國与入活團無限有效感,這邊國際作1	
笑型: ④ 東重导入 ① 全重导入	
文件: 语取文件	
हरूम क्रम्स	

◆ 点击<全部导出>, 以 xlsx 格式导出列表所有内容。



4.2.3.2 指定 IP 检测

启用后, APT 只审计在指定 IP 检测中配置的相应 IP 的报文。

操作步骤

步骤1. 登录系统 Web 界面,选择"配置>检测配置>IP 检测配置"菜单。

步骤2. 点击"指定 IP 检测"页签。

步骤3. 点击<新增>, 添加 IP。支持 IPv4 和 IPv6 格式的单个 IP 地址或 IP 地址段。

新增指定IP检	39	$ \mathbf{x} $
+ Apphylip;	ang A strengt	
描述	举制·加州社会、中部14月2	
	「東海」「西金」	

◆ 导入 IP 检测

点击<**导入**>, 导入指定的 IP 检测规则。导入方式有增量导入、全量导入两种。增量导入是导入与列表 IP 地址不同的信息, 全量导入将列表的所有 IP 地址的信息清除, 导入表格内的 IP 地址信息。 建议下载模板根据模板格式填写完成后, 点击<**导入**>。

◆ 点击<全部导出>, 以 xlsx 格式导出列表中全部 IP 检测配置信息。

导出完成		
	② 导出成功!	
	关闭	

4.2.4 黑 IP 黑域名

手动添加黑 IP 黑域名后,当攻击者访问用户配置的黑 IP 黑域名时,系统就会产生远程控制(用户配置数据)告警。

操作步骤

步骤1. 登录系统 Web 界面,选择"配置>检测配置>黑 IP 黑域名"菜单。

步骤2. 点击"黑IP"或"黑域名"页签,点击<新增>手动添加黑IP或黑域名。

* 篇IP	请给入照开	
•风险等级:	0 # 0 #	
描述:	insi-3035	

或点击<导入>批量导入黑 IP 或黑域名。目前只支持增量导入,即导入与列表 IP 地址或域名不同的信息。

导入支持明文或密文方式, 密文方式采用的是 MD5 加密, 导入的界面如下。

🟹 安恒信息



目前仅支持导出明文数据,即未加密的数据。

步骤3. 点击<导入记录>,可按导入批次查看导入数据的导入类型、导入数量和加密类型等信息。

MP Migs 0.53	-			
9387	10 A 17 19	10.5.85%	10.00	85.5
#1073ED1	NUT.	1	16.2	π
			R18	TT 1 200-70 000 1 17

4.2.5 白名单

添加和启用/禁用白名单,包括文件白名单、域名白名单、黑 IP 白名单、黑域名白名单、客户端 IP 白名单、

服务端 IP 白名单、IDS 规则白名单、Web 特征风险白名单、发件人邮箱白名单和发件人域名白名单等。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>白名单",进入白名单相关界面。

除了 WEB 特征白名单,其他类型的白名单都支持导入、导出操作。

4.2.5.1 文件白名单

文件白名单启用后, 该文件在非手动上传场景下检测结果为安全。

添加方式有两种。

🕜 安恒信息



◆ 在"**文件白名单**"页面,点击<新增>,输入文件 MD5 值,界面如下。

网络国家和	2 10	-						
NAMES AND ADDRESS OF	ALC:	新增文件白衫	5单	×				
Margan M.						100		No. of Co.
mainten w		* MD5	0000,0000					HALFT ME
MARKAGE AND INCOME.		39.6	1230-1420 K.R.S LOUI		FB / I			
and the second				-2		C698 1	1000	-
INSIATURE			(松田) (新田)					
WARRANGES AND	1		1.1					
100 A 100 FT 100								
NINAMHINA								

或点击<导入>批量导入白名单。目前支持增量导入和全量导入两种类型,导入的界面如下。

◆ 在主菜单选择 "风险" 进入风险查询页面, 在列表中点击单条风险展开详情, 在风险详情的文件 MD5

部分(如果有)点击<添加文件白名单>,如下图所示。

201 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	11.12 Press (Annual Second Sec
2100 0CM00	87.958 (P192) (P82) (17
	California and an
	PART 1802 VOID of a second RADIN WOLD ACTIVE
4110D	1624
1.87	AP http://www.inspire.com/angivening/riferation/riferation/angivening/riferation/rifer
815	High: Stored, All-single State.com Alexandr (4
HITYGER	30
#(34	30 50
	30798
2014	w2
1980	Rest Conception of the second s
	Automatical Sector Sect
	Annual and Annual Annual Annual
ww.m	8-HTELER HERVERTRANS/S278/HERVERTRANS/
01625408	Authorithment Attack Get Swall Philippe Control (Control Control Contr
THERE .	3020 42, 44 114-0.01



4.2.5.2 **域名白名单**

配置域名白名单后,不再产生该域名的审计和告警。域名白名单的添加方式有两种:

SHEE#							
福西日后年		0.00	新增域名白	名单			
SPECK*							
3441618#			* HOST	WHILE A HOUSE	HLLE.	108	1017-10.
REWIGEN	×		描述	· 建银石振动: 和波行10月	n lat.		
#SEPERA					 共和	a s anaim	and in the
ANALISA				40.34 Mag			
WINNERPEN							
201/200228							
THUM STORE							

◆ 在"**域名白名单**"界面,点击<新增>,输入域名手动添加,如下图所示。

◆ 在主菜单选择"风险"进入风险查询页面,查询可能涉及域名访问的风险告警(例如恶意文件攻击),

在风险列表的操作项列下点击 📮 按钮添加,如下图所示。

		COMPANY AND				
		NE DECEMBENT (NAME) Alexan Contractor Contractor Contractor Annale (NE)	4.2001/fra	1	Martine (4.200 and	
	- 23''	AT DESCRIPTION OF A DES	NAMES AND	-	NUTTER OF CONTRACTOR	
	-		Langestenson Sociones and Montes		Marcolaster (and marcolast	
			namin'ar	**	1000 (august 1 augustana)	
-	-	take general constitution management	-	**	$\frac{1}{2}$. The same matrix formula to the same till introduce the τ	D.
				1.041		***

4.2.5.3 黑 IP 白名单

配置黑 IP 白名单后, IP 地址为该 IP 的攻击事件不再产生远程控制告警。黑 IP 白名单的添加方式有两种:

◆ 在 "黑 IP 白名单"界面, 点击<新增>, 输入 IPv4 或 IPv6 地址手动添加, 如下图所示。

	1. 1219	-	and the second se				
	-	新增量iPEH	SM	1 × 1			
		+.jąpp	conversement.		1014	#.R	19 M 16
x		描述	HALLES, 120-105	-			
				-	共行第 111	2048-035	RE: 11/1

◆ 在主菜单选择"风险"进入风险查询页面,查询远程控制告警(例如 IDS 规则告警)。如果用户想把 某个黑 IP 列为白名单(即之后不对访问该 IP 的行为产生"远程控制"告警),可以通过风险查询页 面风险列表操作项列下的按钮 □ 添加黑 IP 白名单,如下图所示。

Real Property lies				ALC: NO.
		micate.	-	
THE OWNER OF		MPT INCLUDED		
	1	Autority and the second second		Profession in concerning in co
	and a second sec	(100) (100)		1000
3100 . STATE	Made orati of		A:	
41	22421041408294			
5.0	2 AMERICAN MIRE #11			
8+4X	Mart			
	IT NOT THE REAL PROPERTY.			

4.2.5.4 **黑域名白名单**

配置黑域名白名单后, 该域名不再产生远程控制告警。黑域名白名单的添加方式有两种:

◆ 在"黑域名白名单"界面,点击<新增>,输入域名手动添加,如下图所示。

	A state works	and the second se				
MEETEW	新增速域名:	88#	1.0			
1016211383.W	' HOST			- MITH	460	MG M
	and the	48.000.000	101			
			-	2.18	316-22	PT 1 2
		10 in				
		_				

◆ 用户可以通过风险页面查询远程控制告警 (例如威胁情报告警)。如果用户需要把某个黑域名列为白

名单(即之后不对访问该域名的行为产生远程控制告警),可以通过风险查询页面风险列表操作项列

杭州安恒信息技术股份有限公司

守恒信



下的按钮 📮 来添加黑域名白名单,如下图所示。

	-	-			dense.	RADR	Shar	-	84	878
1	15.001	sense of party	(and shares (b.C.)		Inclusion of the	-		14	sectors and the sector sector and	
1.0					1000 F	-	201208-0-0	1.00	MATCHEMIN IN CALCULATION INFORMATION AND INVESTIGATION	
126			International Address		and the second		and the second second	1.0	APOLISER ULLER - A - O MARK - AND BOOM	
1.00	2.0	1000 (1000) (1000)	1000 modane 2000 0.0000	THERE HAD			- A.		metrophene management of the second	
	(4)	3054100064	The second s	 mentionAt 	Hagfatore -	-		. 201	where an array of the local sector of the	
1	1.8		producers and provide the impre- demonstration		81				of many states and the states of the states	
24	1582	SERVICE OF COMM	And the second s		NAME OF	-	Manager of	. 341	OF MALER COLD STREET, INC.	
	1.0	State of Longian			miletan Cal	-) det	and engineed into its international states	

4.2.5.5 客户端 IP 白名单

配置客户端 IP 白名单后, 该客户端 IP 不再产生的审计和告警。仅支持单个 IP, 添加方式有两种:

◆ 在 "客户端 IP 白名单"界面, 点击<新增>, 输入 IPv4 或 IPv6 地址手动添加, 如下图所示。

×(IEEK平		-	CHARME				
HADRA		新增客户端)	P日名单				
2010.00		1994				100	1000
menne		· Shallib	1110-410-600t	0.55	1000	14.0	10010-40
WPOMPCHEM	4	1014	233.458, 439-000	0:15			
and and provide the local sector				 839			
and the second second		10 ·		1:37			
NUCLEAR AND		10.00	-取消: 研定:	4.21			
WEERLEAST				 parts -			
NOT X ADDING TO					31.4 B	200	第0. 1. 页
RR.040007							

◆ 用户可以通过风险页面查询可能涉及到客户端操作的告警(例如 Web 攻击告警)。如果用户需要把某 个客户端 IP 列为白名单(即之后不对来自该客户端 IP 的行为产生告警),可以通过风险查询页面风

险列表操作项列下的 📴 按钮来添加客户端 IP 白名单, 如下图所示。

- 2	States in succession	SUSARCHA/REPRODE	-		
1.04	makely of parallel		11.18.0	spinster and the second states	
1.8		CONTRACTOR AND A CONTRA	1.000	And in case of the local division of the loc	
	POPULATION AND ADDRESS	#IR44F-152.005.0078-88	1. 100	and the other list of the state of the	
1.4	Internation of States of	BURKENPERSONAL REMOVEMENTATION	1.000	THE PERSON NEW YORK OF TAXABLE PARTY.	
1.0	Internation Contact	ME FELSALTS	1.00	off shares for the lot between some	
14			1.000	out to be readed in the second on	
1.18.1	Internation of Concession,	1 M 1 M 1	1.1.20	THE PARTY NEWSFRIDE	
		The second se	1000	DECEMBER OF STREET, ST	
	and in strends	Included over Include	10 Tapes	The reaction of the ball of the reaction	
- 18	2010.00.0040	State	3 28	STREET GRADE CONTRACTOR	

4.2.5.6 服务端 IP 白名单

配置服务端 IP 白名单后,该 "服务端 IP+端口"不再产生审计和告警。服务端 IP 白名单添加方式有两种:

杭州安恒信息技术股份有限公司



◆ 在"服务端 IP 白名单"界面,点击<新增>,输入 IPv4 或 IPv6 地址手动添加,如下图所示。

SHORN (- 10 M	A NEW YORK AND		24			
M22354		100	新增服务端IPE	3名单				
MITTER AN			a month a sector			-	100	index to
101621210395		-	·服务部P	为如Py460Py6倍元		-1012	.400	WUNE .
With Street of the	1		*服务编唱口	2019/1-00/2010/02/02/201	er.			
Marken PERSON			100 F	WILLIA, EXPLOID		. M.O.W. 1	208-71	8H 1 8
058060309			100000					
WEINING				10次 前定				
2191.002232				and a second sec				
Metro Americania					af -			

用户可以通过风险页面查询可能涉及到服务端操作的告警(例如 Web 攻击告警)。如果用户需要把某个服务端 IP 列为白名单(即之后不对来自该服务端 IP+端口的行为产生告警),可以通过风险查询页面风险列表操作项列下的 定 按钮来添加服务端 IP 白名单,如下图所示。

	BRENS STREET	Treasure and period with the		OTTAX DOLLARS	montest	41.8	And instant source of a	
1.1.8	THE OWNER WHEN		20188-005-005/	LPARES AN		80 B.		
	STREET, STREET, ST.	Management (Act)	in the second			- 1	and where proves only makes were driven on	
	3624 mi 35 84 14 22	(Dense here) for the second	BPAR 112	HAREN RINKING	are done and	-	CETTER, WHEN WE AT REPORT OF	and a
· · · · · · · · · · · · · · · · · · ·	and in strength	(Processing (states and states))	· Mittauer, 112	Hell 28,7600		-	STITES/SCOLUTIONS AND	1) -
	Distant in states	(respectively) is not the other .	ALCONG.	NUMBER BRATH	are an end	25	OF PROVIDE NO. 10 PUBLIC OF	
A.K.	200102 05 041430		2041. 112.118 2014/2017/14/1	MM menTura	- E	20	OUT WANTED DO NOT THE PARTY OF THE PARTY OF	
	302210-05-0414-0	And Distance in the second		-		20	CONTRACTOR AND ADDRESS OF	
1.1.1	3031 10 25 25 14 20			1.1		-	STITES///BLINE.ITTR/seeming	
1	STATISTICS.	(press and) income the later	14	TRACTOR AND INCOME.	The second second	-	OFT THE AT A DESCRIPTION OF THE OWNER	
	Income in called	Press and Inclusion.		10.000	Increases	20	OFT THE ATTLE AND PARTY AND	
	2000-00-00.0414,2	(Without Section Provide Section 1997)		101-101-041-0		240	OUTSIAN IN AN ADDRESS OF	

4.2.5.7 IDS 规则白名单

配置 IDS 规则白名单后,满足配置的"规则 ID+客户端 IP+服务端 IP+资源路径+有效期"的风险数据将不再产生 IDS 规则告警。

添加方式有两种:

◆ 在 "IDS 规则白名单"页面,点击<新增>,在界面上输入规则 ID、客户端 IP、服务端 IP、该条规则 的资源路径、IDS 规则白名单有效日期,如下图所示。

	A TROOMER	TRACK OF	a:					
	新增IDS规则白	名单						
	-			1000	an and a second	-	10.01	
	O Hamida	(出)开带体制	95. Marine		and and the second s		(MSD III	
	* MERID	1000.0000	t didne	2006-12-13 23:50/58	2021-03-38 14/17/16			
			gover.	2099/32 (1/2358/59)	2021-08-01140300			
DIMINISKI	能行動的		guest.	2099-12-31 22:59:59	3021-03-11 14:02:02			
	REPHINP	2.50 Postar Aller	guesti	2009-12-11 23:50:54	2021-03-11 1402:07			
	城名	1998-X-NEE	quest.	2099-12-11 235555	2021-03-31 1402:02			=
	社務地 段	1992 - 1993 (1992)			2.412		1 7	
	* #xXXHB	2099-12-31 23:59:59						
	1221.05	and other, when the						

◆ 在主菜单选择"风险"进入风险查询页面,查询可能涉及 IDS 检测的风险(例如策略来源选择"IDS 规则"),在风险列表的操作项列下点击 ^② 按钮添加。风险查询界面添加 IDS 规则白名单有四种组合类型,分别是为规则名称、规则名称+客户端 IP、规则名称+服务端 IP 和规则名称+客户端 IP+服务端 IP 等,如下图所示。

- H	1811	Married Street, or other	(Ballines or on the Science	and an and an an an and the second se	-
1.000				ROOMINGER X REALIZING COMPANY	
8.2.1		succession.		REAL RACET Lie Agent stree values out an all start 10 March 10 and 10	
				Ballindensen, abundarren 40 W Witherstrandstate	
100	(8)	inter a letter	((remains) reactions) (re-	man, armet in ACRIST the Agent and back with a back wath some star	
1.0	48.0	-		The second	
10.0	100	2010.2-2010		and spirit results. I find while the second se	
	(#)			and any start for a second and a second and a second	
	1.0	PP-LANCE		And and a set owner, we as will be an an and a set of the set of t	
	18)	-		a too an installation and	
1.00	1.011	April 2 March		AN AND A DR. OF CALLER & CONTRACTOR	
1.1	1.811	COLUMN TRAVEL		3 0.0 00 - 10 00 00 00 00 00 00 00 00 00 00 00 00	
	141	THE OWNER.		idiacein - constant an artesintella.comman	
	1.80	-		Minister Thinking you of partment forwards	

在风险查询页面,可通过设置 Web 攻击的 IDS 规则来源、远程控制 (IDS 规则)、隧道通信 (IDS 规则)、挖矿、恶意工具利用、其他等风险条件过滤出涉及到 IDS 检测的风险。

4.2.5.8 Web 特征白名单

配置 Web 特征风险白名单后,满足配置的 "客户端 IP+域名+Web 特征类别+Web 特征规则+HTTP 方法"

🗸 安恒信息



条件的风险数据将不再产生 Web 特征风险告警。

添加方式有两种:

◆ 在 "Web 特征白名单"页面,点击<新增>,输入客户端IP+域名+Web 特征类别+Web 特征规则+HTTP,

如下图所示。

文州口田华		C. Stawington I						
		新增WEB特征的	3名单					
		客户课户		1.00	- 非常利用) MOR	WS.	1015.50
		*城谷	1444人和約1	ta the	2021-01-55 39/12			
generality		WEB##EE#/IZI	28		(0.10) (S	X 2010	10-12 王	HE (* 10
WEBSHID SH	1	WEB#\$HEARDS	安期					
		HTTP方法	全部					
		nue.	·····································					
			- 10 詩					

◆ 在主菜单选择"风险"进入风险查询页面,查询可能涉及 Web 特征的风险 (如策略来源选择"Web 特征规则"),在风险列表的操作项列下点击 [□]按钮添加。Web 特征风险白名单有三种组合类型,分别是为客户端 IP+域名、客户端 IP+域名+规则名称、域名+规则名称,如下图 所示。

-								
2	-	-			-	**	uest.	
	1.4	TRANSFER P.	International Accession of the	#307770017700009204823E34	-	all shares and have share provide the second states of the second states		
	ji.	anna in Hàine	Personal advantage over	Proof State State State State Reads State State Reads State State Reads State State Reads State State Reads State	A.	42 Marco and a second account of the second seco		
	108	HERE .	Detailing [1] Mail Area of Agentic Street which allows	6/*94*, 942; 10,214-038; 10,00,0434-02585 0.000107087-0.028		GP 1992 TER DI ULBR papping pass anti-himotoxia nge Magneseniger 19.34 anticipaty	-	
100	14	-	and the second second	WARF, MC. REISH: 10204140, 10204141	8	17 412 11 11 11 11 11 11 11 11 11 11 11 11 1		
8	÷.		(1000)	MELANNEL CONTRACTOR MELANNEL TELEVISIONEL and a 200400 CONTRACTOR DEPENDENT		Let experie be an experimental transformation of the statement of the sta		
	-	ALL DE LE CALLER	1999041-0009-001-00041907-001110	2.0	## 3	10 11:10:00 (00 (00 (00 (00 (00 (00 (00 (00 (00		



4.2.5.9 **发件人邮箱白名单**

配置发件人邮箱白名单后,此发件人发出的邮件不再产生审计和告警。

添加方式有两种:

◆ 在"发件人邮箱白名单"界面,点击<新增>,输入发件人邮箱,界面如下。

APRODA I	A THE ADDRESS THREE						
	新编发件人都和	白名单	X				
					1 MARY		1000
	* 发件人創稿	1000-53195-53100				10.25	AUT IN
RCHIGHE	 1918	INS.5885. 929-040		500 (
					关48 1	200/35	1000 100 1000
REAL PROPERTY.		-82.85 00.3 2					
NO.AMMERSON.							

◆ 在主菜单选择"风险"进入风险查询页面,查询可能涉及邮件发送的风险(如邮件社工攻击),在风险列表的操作项列下点击[□]按钮添加,如下图所示。

	340.00	-	28	Real Contract	BARN BRIDT	And	8. C	- MARE
4 ()		puntin in Debar	2000,0000 (2001,000)	ELLENG A MILANESSE			(2016) - A (2016) BR(2016) 2017 (FROM CORDS 1011) 10 10 20 A 2017 (State of the state of the s	
				BRANKER DER BRANKER	Lemun mania		 Construction (1997) And the training of the second state of the second st	
			10-000 (pro-222)	Internet in the second se			28 Execution performance part (Here, Property America, New York, Star 1993), Self (Self-Senser), and (Here, Property America, Senser), and Property (Fig. 2004) Sectors and Self-Sector parts (Self-Sectors and Self-Sector parts (Self-Sectors and Sectors)). Sectors (Self-Sector), Sectors (Fig. 2004), and Sectors and Sectors (Sectors). Sectors (Self-Sector), Sectors (Sectors). Sectors (Sectors). Sectors (Sectors). Sectors (Sectors). Sectors).	

4.2.5.10 **发件人域名白名单**

配置发件人域名白名单后,在该列表中的发件人域名不再产生审计和告警。添加方式有两种:

◆ 在"发件人域名白名单"界面,点击<新增>,输入发件人邮箱域名来手动添加,界面如下。

201664	C THAT BERNE	THEN DEPTT					
	新增发件人域名白	名单	lix)				
	* 對件人創業総名				mir.	¥.a	19/7 39
	而述	WENGE, Site out:		i iz			
					30 O 34	208422	
		10.15					
	1						
新祥人编制的书中							

◆ 在主菜单选择"风险"进入风险查询页面,查询可能涉及邮件发送的风险(如邮件社工攻击),在风险列表的操作项列下点击[□]按钮添加,如下图所示。

	-		Army REAM SHART	-	-	ATE
14	201-12-04 12-04	Alemantas (area 2004)	法加加支入部署の第三部第一部第一 第三部第一部第一部第一部第一部第一部第一部第一部第一部第一部第一部第一部第一部第一部	2. al	and another plant approximate and approximate products that an approximate app	
14	##:13.M 11690	and the second second			COMPARENT CONTRACTOR VIEW AND COMPARENT CONTRACTOR THE COMPARENT CONTRACTOR CONTRACTOR Sector Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor Contractor	

4.2.6 Web 特征

对 Web 特征规则进行启用和禁用管理,特征管理的攻击类型有: SQL 注入、命令注入、跨站脚本、远程代码执行、文件上传、路径遍历、信息泄露、越权访问及其他。

操作入口

选择"**配置**"主菜单,在左侧导航树选择"检测配置>Web 特征"。点击页签进入不同类型的 Web 特征管理页面。

安恒信息

100						
e18.	107					A.8 21
**						1.1.2
NO.	STREET,	100.1				
645	area.					
_	Profess.	10	10	5.8	-	815
942	antersteel (100	1001	and or 2004-000	1.1.1.22×11	•
10	27.15	120	1003	ekittirid#	winet frime_DP	•
	WORD.	. 11	1206	Levelant and the P.	earliest sett2.5	
	16.012	14	1807	mins front2.5.	Andrea Property 2.	•
42.	ANDERST	- (4)	Tess	ettab./w	9-12000-140	•
100	100.1	124	40	47(E)8121(6);E	10.740.0000 (0.0.9.0.	
198			4813	一小小市市市	my load \$5.00000	
10.200			7874		ryoy Killer	•
8-14			ists	17744 (\$123.0)	Property Malitania	

◆ 在 Web 特征列表下,点击状态列下 图标可以切换禁用、启用状态;点击<全部禁用>或<全部开启> 禁用或开启全部规则,如下图所示。

SOLEA	36				
04633	- 04	and a second second			
11081	- 31	ID.	2.00	me	80
0.000000000	34	1001	and or 200408	and or Balletin	
出种主领	- A	1000	asked Worws210	search topologia	
mont.		1006	update setEA.	azzdadu aetiliji.X.	0
in the second	- 14.	1007	deleter transletz,	delete frantEJ.	
100101	- 1	100m	中行#dikter	#BHSinw	
110	- 1	1012	中日政治市际有关量	单位的最高级 建定量	
		1018	mptal Killi W	mylamim	
		1018	mpiel Witten	myse Linter	
		1019.	的复数形式	ついた単語書	
		tóte.	oracle(E).#989	maciaEA.###	
		101 7	maghing #	muthilt #	•

4.2.7 Web 登录

设置 Web 登录相关的配置,包括用户名、密码和用户名来源、登录状态码及返回值内容等配置。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>Web 登录"。点击页签进入不同类型的 Web 登录配置页面。

4.2.7.1 **用户名密码管理**

新增用户名/密码关键字,提高对WEB登录行为,弱口令、弱密码进行精确匹配。

安恒信息



可以单击状态栏按钮启用/禁用该关键字。

@ einetzi	and the second second			
1.1988				
- 11408			990-797 ⁴	
- 1100MER	887	*2	viz:	101.0
	- and former	A-410		10 m
+ 200 M	anat	E-BU	•	
+ WISH12	#12.75%**	8.000 L	•	
esworige.	acture	8.000 0		
-	ectrane	84208 V.		
· ARTINE	-	many is	•	
· 001+908	1 1 mil	84021	e	
· 3000.000	Ant	Restru.		
+ 10000079030	a second of	RateST11.		
- Weikcow	8.09	entri.	•	
A STUDENTS	A postflame	sizestu.	•	

4.2.7.2 配置

用户名来源用于配置用户登录行为用户名获取方式,例如请求 url 状态开启,用户名可以从请求 URL 中去

解析获取。

于用户其来源	
者求知道 💿 开篇	C ME
RAURL 🛞 开 🛱	0- MH
postbody是西支持-管道输行 📀 并属	() 关闭
poetbody使用完计 ISON概念 ④ 开露	0 MR
■序5cockle: ④ 井田	13 ** #
R tte	

系统默认请求头认证、请求 URL、postbody 普通格式均开启, postbody -JOSN 格式、请求头 cookie 需手动开启。

状态码配置主要用于配置用户登录行为登录状态的判断,用户登录行为满足配置的状态码,则该次登录状态即为成功;用户登录行为返回内容中满足返回内容配置,即可判断该登录行为成功或者失败。

And the second second			
THE IS AND AND			
(mith links			
MON .	wo		anna.
201			H (B
383	•		16 m
		878	2007 00 1 2
			and the second state of the second
Xikw	Q.W.A.M	112	an-a
haugen (fallind - Falsen	· 502:		NO IEI
tagin_accounting	* 500		10.00
lagin_Nalissi mas	• 28		¥ 8
topin, suscered filter	• **	•	18 T

4.2.8 IDS 规则

IDS 规则管理可通过页面对 IDS 规则进行启用、禁用的管理, IDS 规则主要有 WEB 攻击、远程控制、WEB 后门访问、拒绝服务攻击、隧道通信、挖矿、恶意工具利用、漏洞利用、其他等 9 个风险。

操作入口

在菜单栏选择"配置>检测配置>IDS 规则"进入 IDS 规则页面。

◆ 点击状态列 ■ 图标来切换禁用、启用状态来对规则进行管理。也可以点击<全部禁用>来禁用全部规则,点击<全部开启>开启全部规则。还可以通过勾选"只看紧急事件"来筛选紧急事件。

• INTERNAL	387 200						**	2.2
@ ###### -								
+ E1923512	WEIRVA.	4109	MH CHINA	###### 目前成在計算件				
• 37050	6820546	-10	10	8.0	URBANIES .	81.0	医热带 药	
 PERADE 	CONTRACT OF	950	4555557	Shette Romerniberlike Sir/#Plit22018 M.1	2021-01-25 12:16:50	•	(35)	
• #PP#040	WORK INFE	(319)	8886608	Shirp Rememberive EUNDREAD M2	2021-01-25 12:16:30			
· 88#	(18030	500	1556587	Shiru Rememberhte Ertsteitellin Mit	2021-01-25 12:16:50		100	
+ WEB512	and the second second	E	1000000	Thrue Remember Market States Market	2001-01-25 12:16:50			
• WEIR2	SPERIC	12	(00000)	Shirp Rememberishe HIPPING III MS	2021-25-17 14:12:59	•	100	
11058291	\$1.50	- 6	1000004	Thinkadowno @ P. #P. # Phone Of CVE-2008-2	2021-05-10 155533			
• 8080879*	300.	- 105	400006	Thinkadatana (ERIA BURNELSCOC VE-2000-2	2021-05-10 15:53:23		128	
APPER	1000000	1111	11300004	Rhf1630www.ced140	2021-05-10 1553:03		1.00	
· BLOOMER	3690/00	392.5	11300007	04+他去亲任属范围访问部站	2021-05-10 13:53:33			
· MATRICE	828743	122	11100009	製成で中心の形式(Aphadityphy)	JDJ1-05-10 155533			
and a second second	3118	1797	11100012	nt Methoda A and Market Market	2021-05-10 15:5111	•	(CD)	

◆ IDS 规则配置,目前系统支持精简规则和全量规则两种规则模式。

ኛ 安恒信息



- 精简规则: 是经过安恒威胁分析团队筛选的, 比较常见且重要的规则。
- 全量规则:为了提高检出率,加入了更加复杂多样的规则库,匹配性增多,系统资源占用率高, 建议在设备流量吞吐相对较大的场合慎重开启。
- ◆ 系统支持精简、平衡、增强三种置信度,置信度是基于规则的匹配内容是否可信,危害范围进行综合 评判。
 - 精准: 该模式规则数量较少, 但告警准确度高、误报可能性较低。
 - 平衡:模式在保证告警准确度的前提下,选择适当重要的规则。
 - 增强: 该模式规则数量较多、检测范围广, 但出现误报的可能性增大。
- ◆ 支持导出 IDS 规则管理的规则 ID、IDS 规则名称、启用/禁用状态、风险名称等内容。

4.2.9 邮箱防护

在邮箱防护模块,可以点击<新增>,添加域名及邮箱服务器 IP 地址,添加后的邮箱才会有发件人欺骗检测,及在引擎管理下邮件社工检测中的针对发件人欺骗的检测才会生效。

操作入口

在菜单栏选择"配置>检测配置>邮箱防护"进入邮箱防护页面。

2 9969	The same want to make the same			
0 mm	estitutes	912 · · ·	NK:	-
· man		· weather all Party. The Indone at	***	
- 104				
(+				

4.2.10 ARP 检测

ARP 检测功能可将 IP 地址与 MAC 地址绑定,便于识别解析 ARP 欺骗,提高检测精度。

操作入口

在菜单栏选择"配置>检测配置>ARP 检测"进入 ARP 检测配置页面。



③ 明EAPT这正明图平台			116	0.0	1.000	R.C.	.M.W.	NMM	6.8	3.05			
- 1808 PA	-												
- 2008		193.	916										
- PRIME	- 10.04				AAACIESE						:80	4	
+ INTERNAL							10.00 C						
1 × 155.00							10.000						
- 1422003									717.8	182	1.18		÷.
- WINDY													
- 1148													
+ #2000 P													
<													
- VALMENT													
- 107002008													
- ANNER													
· SCHOOL													
C DAME													
CT ALCEN													

◆ 点击<新增>可以进行单个 IP 地址与 MAC 地址的绑定。

新増IP和MAC绑定										
* IP地 <u>北</u> :	10.10.144									
* MAC地址:	00:50:56:8f:98:ad									
	取消 确定									

- ◆ 点击<**导入**>可以进行批量增加数据,点击<**导出**>可以进行批量导出数据。
- ◆ 支持增量导入、全量导入两种导入方式。
- 全量导入会覆盖原有数据,请谨慎操作!

导入	ĺ.x.
△ • 短入又件支持exce描述。 下較機較 • 全量与入井憲盖版有数据。 清逢這慢作!	
类型: • 增量导入 () 全量导入	
文件: 医取文件	
- 現直	

4.2.11 弱口令配置

通过对常见应用的用户名、口令进行提取,并进行复杂度判断,以识别应用中存在的弱口令的情况,减除



企业应用中潜在的风险隐患。

操作入口

在菜单栏选择"配置>检测配置>弱口令配置"进入弱口令配置页面。

- ◆ 点击**弱口令规则**进行规则配置,本项是弱口令判定依据,凡是符合设定条件的即为弱口令。满足规则
 字符类型≤2,口令长度≤6或者 字符类型≤1,口令长度≤8 即被判断为弱口令。
- ◆ 可以点击 + 进行增添规则或者点击 🏛 进行删除规则,单击 🗹 进行规则修改。

系统最多保存4条弱口令规则。

atun ilat
100

◆ 点击弱密码,可以增添自定义明文密码以及 MD5 密码,支持单个增添以及批量导入。关闭状态则禁 用该条密码检测。

IHWAPT攻击F	贝警平台	ł	9.6	946	34.62	窗/**	###:	18.81.01	6C W	1145	altar
• COMEN		9612\$4500 1003 4									
 IPADKE IRPEKE 		THE DAY	maj								
+ 0.6M		#13.92H	2	AD/Selectory			3.9			85,6	partia.
· WEREIG		1234%(dom:	30	DOCO-RAINING	HAADCS/17/25	6538) A	Antes .				
· writiger		(SED:00	ä	2110607045	EA7EBAC1F2051	##005#	EV.D			()	
+ 105,800		erririn .	1	†An252AD910	47A4Deres Trics	ADDRESS	10.00				
• BAREAR	1.6	1000000	1	techil-kinka	Persenautati-4	10000	815.0				
+ 2012/0/000		12,066	k	10400394984	SAAble Solds Tra	stanie	811.01				
 NSORBEDB 		90123456	1	NECEPTER LAN	STEPHNALESS	42810291	810.0				
< 0.09988210208		413345		FILIPOPYASDA	ZÖFUC Jellin at Gas	Ascent	81025				
 Alifesti 		12345		UNIC BORDARS	106C4C34A1029	17 6 45 78	41100				
CONDUCTION IN		†W12145		SHIRAAR TANK	02548A472548A4	4424CN	8142.01				
42 BA1928		16123459	1	Di IEFSZIRMF	1084670793031	ERSDAN	\$15.00				
to solution		g123454	4	415499CPDIT#	contricm sea	7288.18	810.0				



4.2.12 **自定义规则**

根据用户需要,自定义特征检测规则。当规则状态为<**启用**>时,如果流量中有满足配置的内容,风险页面 就会产生自定义特征检测告警。

操作入口

选择"**配置**"主菜单,在左侧导航树选择"**检测配置>自定义规则>新增**",根据规则类型选择特征匹配类 或周期统计类填写各项规则匹配条件,如下图所示。

◆ 默认选择特征匹配类,根据规则内容和 Flowbits 进行匹配。Flowbits 会进行标记流,匹配时告警更加的精准。

1100	PER S all BR	10110 TE2
1008.R		
CONT.	and a street and a	
104	Henry Conversion of	TRAD. BONN/MIL
1000		
ervite .	Advant. 1 1 / 1 / 1 / 1 / 1	libed. A V + e & A
2-1001		- there a rad faces shall been along along adapt
Call of the local data	THE R LT LTT CATT	
rrek (TO B DESK MAN WAS
KOHRE	(and the)	
NEX 1881	1000	and the state of the
10.42	196.1	Name and TAX
C2.2.1.0	All a set 1 for	
CORPORT OF STREET, STR		- Silling - Bar Marchent-Hall
0100200	- 2010 1011	
	- Area V Area	
OR CHARGE		
10011100		B41 B2

 ◆ 选择规则类型为 "周期统计类" 时需要设置阈值,在周期内统计来源满足次数要求并符合规则内容和 Flowbits 才会触发告警。



#= # ## Fat	ABON NEW .
	1944 - 1948
dine	Patrick Right 700
R162, [125-10]	ANNE = + × =
	Allen a fam mann walls worth success process
960. (0. 529 // (OF	
184 (04400 0 FER SD 200 FR 700
-BK2 111	
	THE REPORT
500 (B and) 2022	area and
	the pro-
NNO INI	from an TEE

◆ 点击<添加>添加规则内容,即特征中需具体匹配的流量内容。

1 1000 1 1000 1 1000 1 1000 1 1000 1 1000 1 1000 1 1000	2月17日月、第三人間1月17日月(日本日本日本日本日 2月17日月、岡本市町1月1日(日本日本日本日本日本日 2月17日月、岡本市町1月1日(日本日本日本日本日本日 2月17日月、日本町一日日本日本日本日本日 2月17日月、日本町一日日本日本日本日本日 2月17日月、日本町一日日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本	
内容器	· TOB _ OF INCOMPANY	
16春	Pacial/(1005Fart)	
154	(d)	
1000	÷4	
「尾鹿」	d	
• 97 B	-1 -	
大小石板市生	8 am 🗇 Aan	
24	④ 〒転営 □ UR: ○ 御芋豆吉 ○ Cooler ○ 御芋头	#782
	1.0	

添加规则界面参数说明如下。



参数名称	参数说明	默认值	
山空酒	设置规则内容来源。	◆ 不配置	
内台源	可以选择不配置或者来自文件。	◆ 文件	
内容	设置规则内容。	手动输入。	
	距离是一个配合规则内容使用的参数。距离参数设置了内容模	手动输入。	
距离	式匹配函数从它搜索的区域的起始位置后的某一距离开始搜	距离参数和范围参数一般	
	索。	配合使用。	
	范围是一个配合规则内容使用的参数。范围参数设置了内容模	手动输入。	
范围	式匹配函数从它搜索的区域的起始位置开始的搜索最大范围。	距离参数和范围参数一般	
	范围要比规则内容包含的字符数目多,才能进行匹配。	配合使用。	
	深度是一个配合规则内容使用的参数。深度参数设置了内容模	手动输入。	
深度	式匹配函数从他搜索的区域的起始位置开始搜索多少个字符。	深度参数和偏移量参数一	
	深度要比规则内容包含的字符数目多,才能进行匹配。	般配合使用。	
	偏移量是一个配合规则内容使用的参数。偏移量参数设置了内	手动输入	
偏移量	容模式匹配函数从他搜索的区域的起始位置偏移多少个字节	深度参数和偏移量参数一	
	开始搜索。	般配合使用。	
大小写敏	配罢湘麦时内突抑则由的今姓且不需再变换匹配十小军今舟	◆ 忽略	
感性		◆ 不忽略	
区评	设罢湘李区博、即和则匹命湘李的英国	不配置、URL、请求方法、	
	以且这杀凶战,叫观则也能该杀心也固。	Cookie、请求头、请求报文	

杭州安恒信息技术股份有限公司



4.2.13 **特权账户配置**

涉及登录行为相关的应用场景,例如特权账号登录、弱口令、脆弱性分析等,需要对特权账户进行标识, 因此需对应增加配置界面进行区分。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>特权账户配置",当有登录的账号满足状态开启的 账号名称和登录协议,即可被标注为特权账号。

1.1083	100 C				
1.25588	969.0	RANK	and the	800	sna
· PERMIT	11 alter.	HITP	NGN/*	(1)	814
				#18 J 🖬	201 00 1 5
· without				-	
+ WITHON					
+ K70808					
- 80000					
+ 607m8					
+ BEDERE	6				
· BERLINS					
· ####225#					

◆ 点击<新增>按钮,新增特权账户,输入特权账号,选择登录协议,界面如下。

新谱特校账号		
0.5		
* 141236/P:	3890.5.10523575	
* 整要纳权:	aiten o	
SEct	-Rin/Mat. 9.89-1202	
		4
	双川 西京	

4.2.14 **智能语义分析**

智能语义分析是把人类自然语言转化为机器能读懂的代码。即对检测内容进行语法分析,提高规则模型的

适用性。



为了防止现场智能语义分析误报过多, 该模块可以针对单个智能语义分析 (例如: 智能语义分析 XSS 攻击 等) 进行引擎的关闭。

操作入口

选择"配置"主菜单,在左侧导航树选择"检测配置>智能语义分析",主要控制智能语义分析功能的开

启状态。

- 1988					
- 12/4428	MMR239900200	WW983(399007428)(814)		WHEN CONTRACTOR STATE	C
+ 210 Million					
· attants	Maritz, HWH2112, Alice	\$P\$10.0000-0000-0000-0000-0000-0000-0000-0	C		
- mim.					
+ WORKE					
· 2012/000					
+-1010800					
- 3080211					
- 237420					
· HOURS	2 C				
- 80823991					
+ 1009-7402					
+ REALIZING					
- 11108404					
- UTFORDED					

4.2.15 SSL 流量检测

SSL 流量检测是对当前用户网络环境中出现的加密协议流量(HTTPS、SMTP、POP、IMAP)进行检测。 该检测需要上传相对应证书,即该加密协议流量中网站的私钥(目前只支持 RSA 私钥解密)。

证书上传操作方法

- 步骤1. 登录系统 Web 界面,选择"配置"页签。
- 步骤2. 在左侧导航树选择"检测配置>SSL流量检测"。
- 步骤3. 点击<**上传证书**>, 在弹出的界面上配置私钥别名、私钥密码、服务器 IP 地址、对应的协议以及加密端口、上传服务器私钥文件。完成后,满足该配置的加密协议流量就能被审计并检测。
 - ◆ 点击左侧的[⊕]增加协议及对应端口,一个 IP 地址最多输入 4 个端口。



◆ 点击右侧的 ^④ 新增 IP 地址记录, IP 地址只允许输入单个 IP。

	出物繁平的						NOTE:		A CONTRACT OF
24		Concession of the	10						-
TI NIGER		Come and	上接证书				14		20.000
@ NAME		s.imt.	- States				- 1	94.64	TRY 10
10002			A	SPIMEE, MPULSA	AND ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	11.00000000			
 S2000000 							- 1		a star water
- insummer			WERE				-	10.8 218-5	1 100 1 10
- 300 miles			everenis						
* 258VB			Contraction of		and the second				
- 26.000			ACRON.		= 1000				
- WEITER			* IEEE 254//01/2314	BIT231					
1.101000				10					
1.0000011					a detailed		_		
• 1888/2009									
+ 1512081038									
 consideration 									

- ◆ 证书编码格式为 PEM 文件格式, 如 PKCS#8 加密格式、PKCS#8 非加密格式、Openssl ASN 格式等。
- ◆ 证书名称由数字、字母、-、_、.组成,长度:1~255。
- ◆ 此处配置不需要再在端口配置中新增 ssl 加密端口

4.2.16 UDP 端口过滤

自定义对 UDP 协议(传输层)进行端口过滤,过滤掉无需检测的协议端口。

操作入口

B

选择"配置>检测配置>UDP端口过滤配置"菜单进入 UDP端口过滤配置页面。

- ◆ 过滤类型可选择"过滤以下端口"(即端口黑名单形式)或"过滤以下端口外的其他端口"(即端口
 白名单形式)。
- ◆ 如果不需要过滤 UDP 协议端口,选择<禁用>。



المعالية 🌔	的新聞的		9.6	នត	风险	课户	服務	原湖田	起軍	新柏	atten -
2019日	3								2 2		
FE WINNER	196	100	6 en 0 #	1							
entrement	1.4	and a state of the	inter i								
+ 100 EU		10 00 00 00 00 00 00 00 00 00 00 00 00 0									
• 交织相關		iciante: 1	EDADGETRACE (11100011	F44CDH的地名 编						
· PRIMA		1440	PARTY PROPERTY	Paterian							
- 10071034/L			103 - 100 -								
+ 618/W			GUTS								
 WOMENT 	-										
 WEIRGH 											
- 105858											
- analysis											
· 000000											
- 1112084030											
+ UDPARTIESS											
- 20700W											

4.2.17 暴力破解模型

对暴力破解模型的触发机制进行设置,适应用户的实际使用环境,主要涉及**时间范围、登录次数、检测机** 制等关键指标进行配置,满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择"配置>检测配置>暴力破解模型"进入暴力破解模型页面。

点击 开启该类型风险检测 (启用模型需要在"**配置>检测配置>引擎管理**"页面确认**暴力破解**及其子模型开关已开启);点击 [☑]可以编辑该模型,更改配置内容。

100								
Here a	10010	#232	100	1052200.00	0%2B	epimert.mi	#8	87.0
real		Aminida	(D4P	-	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	いため、2011-10201-2011 102-008、120-0 102-008、120-0 102-008-01-102-102-102-000-000	•	914
2990) 2980)	ICTR/MR	urtilis	107	-81	References 14 Brancost, 1 Brancost, 1 Bran	ran ne-sur Span 784 Brandia nasiet	•	30
	1-81164	untions	35m	10	第編集平行2台(18):0 第四平行2台(第十四):0 第四平行2日(第十四):000 回知約:10 回知約:10	enne: 200-11207 Reven: This Revenuental network		8.0
isite i	2018-08-030-38	#90m/89	and with		18.08.0	PRE BRARD ALL REALT TRA REALT RAD	•	1010
ikani Kalimi	410-090230188	REALIZED	10	30	SACTR: 10	学生学、西洋・日本51-1月1日 第二年度:工業上 初に日本50月後、月に日 - 2月3日	•	363
NECOSE	****	anticity.	WISD.	.00	400.000-14	988.864.804.801 84488.788 620488.8784-478488	•	(8)
	und weight an		SHEALE		48.18 H	19年間1日月1日-1月1日 月1-4月1日 - 月日日 10月日日日日 - 月日日 - 1月1日日日 11月1日日日 - 月日日 - 1月1日日日	•	
	********************	#10108	Misig	40	A20.00.10	Part Br-Brotac	-	(10)

4.2.18 **扫描行为模型**

对扫描行为模型、爬虫扫描模型的触发机制进行设置,适应用户的实际使用环境,主要涉及**统计周期、访问IP、访问端口、访问次数**等关键指标进行配置,满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择"**配置>检测配置>扫描行为模型**"进入扫描行为模型页面。

点击 开启该类型风险检测(启用模型需要在"**配置≻检测配置≻引擎管理**"页面确认**扫描行为**及其子模型开关已开启);点击 [☑]可以编辑该模型,更改配置内容。

(and a second s	18558	(0.11000/01)	8181.01	0294	wawa	80	94110
	#_SCAN	-	WHER WALFARE - REMARKER AND A	67.2	#16.	(38	(1) - 40 (1)
(288)	1210,1220	10	NTRON MULTIPATION AND AND AND AND AND AND AND AND AND AN	16742	*12	100	10.00
Labor	Hom scan	- M	NUMBER BUILDING AND A COMPANY	6574	100.0	120	h(sin)
1710M	MOMN_SCAN		NAMES IN ADDRESS OF AD	e38	816		10.00
AURY -	SAR_SCAR		NAMES BATTONESSERVICE	1078	mit		8.4
01100	HIP SCHN	0.00	office exclusions and an an	618	+(c.)	0.00	1(10)
ullinen	TRANSPROTED, SEAN	100	HTML PARTICIPATION PROVIDED IN THE RESIDENCE OF THE RESID	658	work	00	1.1
ITHEODIX.						10 a 🗧 🚺 🤉	2082 82 1

杭州安恒信息技术股份有限公司

₹ 安恒信息



4.2.19 **拒绝服务攻击模型**

对拒绝服务攻击模型的触发机制进行配置,适应用户的实际使用环境,主要涉及**统计周期、单包长度阈值、统计周期内访问阈值、统计周期内总流量阈值**等关键指标进行配置,满足设置的触发机制的风险才会产生告警信息

操作入口

在菜单栏选择"**配置>检测配置>拒绝服务攻击模型**"进入**拒绝服务攻击模型**页面。

点击 开启该类型风险检测(启用模型需要在"配置>检测配置>引擎管理"页面确认拒绝服务攻击及其 子模型开关已开启);点击 [☑] 可以编辑该模型,更改配置内容。

- 1996	MAD #	Dard Ballin data	activities	10.00 % (KINHD	was.	erra
· PERMIT	006,009,51000		#11:5051 X00 mr/Whitehild 1000	+100	we	CBF	11.10
- 2020	201,009,046		851-865 105 81+9855528682 101	+728	84	- 120	10.00
- wrang	action/why		HET REPAYATION DE LE CONTRACTOR DE LE CONT	+700	-	09	8 M.
- WARR	dol.jdf.okkish	4	HERE XE MITERAL	+10	wit	CBF	1.1
- states	205,007,0809		#SHIRES VI WHRETHERMER (F	174	84	0.00	10.00
- ADVER	DOCTONINGHOUD	10	BURREN W	+72		00	10 M
- 842.000	101,009,009	(0)	INTERVISION AND TO CO.	+208	310	.00	(0)(0)
- 1000/108	000,307,599		SUMMOUSEE 000	+700	#16	.08	2018 ·
+ 80008323/W	105,707,057	4	WITHMAN BAB 100	+122	wit	08	- 41 (M
< vitualitade	205,00,00	14.1	ectebrostate and	+122	*10	- 128	10.14
+ 201462039 C	201,109,408	1917	INTERNOTERS INT	1.000	815	(19)	(80)(87)
+ W1/W/W012	100,000,001	1.1	AHEADOREER N	+704	84		10.00
	300,00P,R000	(94)	●私兴田建築、1780 例刊開発性的教育等: 二	+12	wat	- 39	(10) (2)
C wota P	DOLLICANT FLICO	1.00	HOTERPARTER NON	+722	410	138	-16 M
Ei mitra						48 - 🚺 1 185	

4.3 联动配置

4.3.1 EDR 联动

APT 检测到恶意文件投递行为, 且接收恶意文件的主机 IP 为内网 IP 时, 同步该恶意文件 MD5 值和内网 IP 地址给 EDR 管控平台, 由 EDR 管控平台返回该 MD5 值对应恶意文件的执行状态, 如果样本还在该 IP 主机上, 也返回该样本的路径。同时 EDR 会扫描该内网主机近期活跃文件, 检测是否存在其他恶意文件。

杭州安恒信息技术股份有限公司



操作入口

在左侧导航树选择"配置>联动配置>EDR 联动"进入 EDR 联动配置页面,选择 EDR 管控中心页签添加 联动 EDR 设备信息。

- 服务器配置	
状态	
* IP1\$2;	192.168.3.6
****	443
• 顺符扫描时经	90 Binders 2 + 5 Prost States - America

◆ 选择联动信息页签可以查看样本投递时间、被投递病毒的 IP、样本文件 MD5、联动状态、样本执行结果、样本路径、EDR 病毒木马扫描结果。在操作项列下点击 ◎ 图标查看选中样本的详细信息。

EDRTEPHO Million	•						
样本提進的问	植现态将希的中	样本文件MD5	國家政治	释本执行结果	样本题经	的時時本這台級結果	BH155
2020-05-25 11:30-48	192 168 10 230	1c8++455071+31808cd1720	订松结单共物	执行状态未知		記録 102.168.10.230 (年	10
2020-05-25 11:30:48	192,168.30.15	Obe624bToc19a3178ccd6.	获取结果失败	执行优态未知		②蜀[102.148.30.15]美安。	e.
2020-05-25 11:28:49	192,168.38.73	19a423c59093e67417a7a	研究信息失效	医疗状态手知		前者[192,168,30,78]未安。	10
2020-05-21 15:32:27	192,168,30,15	Obe524b1cc19a3178ccd6.	供取纳原共和	网行动态单短		彩新 192.168.30.15]丰富。	12
2020-05-21 15:30:10	192 168 10 220	1c8ee455071e31808cd1720.	民歌組織共和	的行动因素和		6266(192.168.10.2003#	la:
2020-05-21 15:30:10	192.168.30.73	10#423c50095#67817#7#	安观结婚关政	执行状态未知		· 企業 102 166 30 73 決安。	8

4.3.2 WAF 联动

APT 支持与 Web 应用防火墙进行联动, 阻断针对 Web 服务器的恶意攻击, 从而达到更好的安全防护效果。

实现原理

WAF 联动的阻断类别分为两种,一种是基于源 IP 的阻断,一种是基于服务端 URL 的阻断。



当 APT 检测到流量中有上传 Webshell 且攻击状态为成功的行为、下载 Webshell 行为或某个源 IP 上传了恶意文件, 会生成联动策略并通知 WAF 对 Webshell 页面或该 IP 的任何访问进行阻断。其中对于 Webshell 页面永久阻断, 对上传恶意文件的源 IP 的阻断时间为 1 小时, 阻断时间过后如再次上传恶意文件, 则再次阻断 1 小时。

操作步骤

步骤1. 在菜单栏选择"配置>联动配置>WAF 联动"进入 WAF 联动配置页面。

步骤2. 选择 WAF 设备页签,点击<新增>,添加待联动的 WAF 设备。

备	$ $ \times
支持IPv4和IPv6格式	
支持1-65535间的数字	
取消 确定	
	 登持IPv4和IPv6格式 支持1-65535间的数字 取消 确定

步骤3. 选择联动策略页签, 查看该策略相关联的阻断事件。

点击策略溯源事件次数列的数字,查看策略溯源详细信息,也可对策略进行启用和禁止操作。

IN 28 BICTUR IEXEN				
				(T) (
0.0245046	00.01	183 WAR	NIM (0020 00-19 (1998)	9.5
100038110	34		<u>it</u> ,	
	Sector Sector S		10	1.000

步骤4. 选择阻断事件页签, 查看阻断事件详情。

页面展示所有 WAF 回送的阻断事件,包括发生时间、源 IP、目的 IP、域名、报文和触发策略等, 如下图所示。点击列表中的触发策略,可查看关联的原始风险。



WAFIER TRAIN	· 印新本件				
京府学校 -					
*****	前中	ERF.	城东	叔文	相次策略
Could a real					

▶ 对于 Webshell 攻击, WAF 阻断这个 Webshell 页面, 所有 IP 都不能访问。返回给客户端的

阻断页面如下所示。

÷	÷	0	不安全	192.168.30.88/apt/compx.aspx
1.90		× 1790	College and	service and and a service proceeding

403 Forbidden

 对于恶意文件攻击,WAF 阻断客户端 IP 的访问,上传恶意文件的客户端 IP 对保护站点的 所有 URL 都不能访问,其他 IP 对保护站点的访问正常。返回给客户端的阻断页面如下所所 示。

← → C (D #@# 192.168.30.88\upflim.htm) 403 Forbidden

Request forbidden by administrative rules.

4.3.3 防火墙联动

APT 支持与明御[®]安全网关(DAS-Gateway)进行联动。检测到风险信息后,触发 DAS-Gateway 对指定源 IP 列表进行阻断。其中阻断时长可统一在 APT 产品的防火墙联动页面中进行设定,默认为 10 分钟。

当攻击者(符合 APT 所定义的 Web 特征检测、扫描行为、web 后门访问、隐蔽信道、暴力破解、挖矿、

远控工具利用等风险)是外网 IP 时, APT 会生成联动策略并通知 DAS-Gateway 对该攻击者进行阻断。

操作步骤

步骤1. 在菜单栏选择"配置>联动配置>防火墙联动"进入防火墙联动页面。

杭州安恒信息技术股份有限公司

Request forbidden by administrative rules.


步骤2. 选择防火墙服务器页签配置联动防火墙,输入服务器 IP、端口 (默认 80 端口)、阻断时长等。

10 5 10005	n.comme	Reits Armene	
****	105563		
-	1970		
(i) comm	1-000	arianities .	
C sues	246	NARIO	
	1ect.	41	
- managed	Merch	1018	
Emme	 ambatto		
	TARGET.	and as as to make	
		inter :	

步骤3. 点击阻断信息页签可查看阻断 IP、阻断开始时间、阻断结束时间、阻断状态。如果阻断过程中又

NAMESH DIFFE	ter de la com			
				¥204
19912	10(0)(21 (salar))	RENVERIN	B30:0542	9210
12166293	2028-03-30 00.38.01	2020-05-38-1648-31	Ec.ue.	161.81
Taninana'	2023-03-30 00;38:39	2020-03-30 (00-48.00	114.08	(44) (#)
			#1# (1	288 88 4

有对应新的风险产生, 会重新计算阻断结束时间, 如下图所示:

◆ 点击<阻断 IP>可跳转页面展示该阻断 IP 的风险列表。

h maxima									
-	ant.	10	Brief.	Rahm	anar.	1000	mail	4.0	and.
18	2223 85-50 10.0001	(1997) MARAWAN CAN AND TARA MARAWAN TARAKAN MARAWAN Al Makamat Marawan Kan	*120.2%5	-	12105253	200	100	101 100/0772 100.532/equippinion_association-405401390	

◆ 点击操作项下的¹¹图标,可查看该阻断 IP 的风险详情信息。

FOR A DAMAGE	and the state of t
+m=08	
*6	January Carl Container
4.10	Table 1 MAR (MAR), CAN WA TA Sale Allowing High and Market and American Street State
wing	10xett
	(a) http://www.intextee.com/www.journation.com/anticipity
825.	Not HERREN Nes des Conserve Nes des Taue des Charles II and Auge Mercenter II and Auge Mercenter II and Mercenter II and Auge Mercenter III and Auge Mercenter IIII and Auge Mercenter III and Auge Mercenter IIII and Auge Mercenter IIII and Auge Mercenter III and Auge Mercenter IIII and Auge Mercenter III and Auge Mercenter IIII and Auge Mercenter IIIII and Auge Mercenter IIIII and Auge Mercenter IIIII and Auge Mercenter IIII and Auge Mercenter IIII and Auge Mercenter IIII and Auge Mercenter IIIII and Auge Mercenter IIIII and Auge Mercenter IIIII and Auge Mercenter IIIIIIII and Auge Mercenter IIIII Auge Mercenter IIIII Auge Mercenter IIIIII Auge Mercenter IIIIII Auge Mercenter IIIIIIIIII Auge Mercenter IIIIII Auge Mercenter IIIIII Auge Mercenter IIIIII Auge Mercenter IIIIIIIII Auge Mercenter IIIIIIIIII Auge Mercenter IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
	anti- and a second seco
17798-0	44
	m 200
101-8	1 when
-	
1010	- MA
	Linear,
F#ITWS#	
1982	(0,0/283,0mm)



- ◆ 点击操作项下的[□]图标加入防火墙白名单,加入防火墙白名单后防火墙不再对该 IP 进行阻断,该 IP 仍能正常产生告警。
- 步骤4. 点击防火墙白名单页签,可以新增、启用、禁用和删除防火墙白名单。点击状态栏下的 🤍 图标

切换阻断 IP 的状态,灰色时表示不会阻断该 IP。

@-emm	and an interiment			
C sures	Restored.	Etersi	atta	
	0.168.203	2020-89-20 (11921	•	
- EXAMPLE			218 I 🛄 I I	282 82 1.2
E want				

4.4 数据外送

数据外送指 APT 以网络流量综合探针形态运行时,采集到数据信息后把对应的风险信息、审计信息等上传 到数据中心(如安恒信息的 AiLPHA 大数据平台),或以邮件、钉钉等方式发出通知。

使用须知

- ◆ 当 APT 平台从 V2.0.62 版本升级到 V2.0.63 及以上版本时,禁用的配置会被删掉,如需继续用此配置, 请在升级前启用该配置。
- ◆ 服务器类型有 7 种: 分别为 SYSLOG、KAFKA、邮件、FTP、短信、钉钉、上传恶意文件。

4.4.1 **服务器配置**

用户首先需完成服务器配置才能够开始数据外送。

操作步骤

步骤1. 登录 APT Web 系统, 在菜单栏选择 "配置>数据外送"进入数据外送页面, 选择服务器信息页签, 点击<新增>, 选择服务器类型、发送格式、数据加密等, 点击<下一步>, 直到完成配置。



ine X venue	(!) BRERTON	- (1) anima	2.66
- 2782 - 1010000	Terrer a sais	Ref 116 KW 200 TellW20	
() mante El monte El monte	1000 8 8 8		

相关配置项请参照下表:

参数名称	参数说明	参数取值
服务器类型	数据外送服务器类型。	SYSLOG\KAFKA\邮件\FTP\短信\钉钉\上传恶意文件共7种。
		默认选择 APT 风险通知。
发送格式	服务器发送的格式。	KAFKA 服务器对接大数据产品可选择"安恒 AILPHA 大数
汉还旧式		据平台 3.4 及以下版本接口规范(JSON 格式)或者安恒
		AILPHA 大数据平台 3.5 及以上版本接口规范(JSON 格式) "。
数据加密	数据是否加密。	是、否。
ᄟᅇᆇᅷ	选择数据加密方式 加密密钥。	AES、SM4
加密力式		当" 数据加密 "参数选择"是"的时候,该参数可配。
密钥		默认或者自定义。
		当" 数据加密 "参数选择"是"的时候,该参数可配。

步骤2. 点击<下一步>,在弹出的界面完成服务器配置。根据上一步勾选的服务器类型不同,界面参数也

不同。详细参数配置可以参考下表。

参数名称	参数说明	参数取值
SYSLOG 服务器配置		



参数名称	参数说明	参数取值	
服务协议	配置 SYSLOG 服务器传输协议。	UDP、TCP。	
编码格式	配置 SYSLOG 服务器使用的编 码格式。	 GBK: 汉字编码字符集。 UTF-8:针对 Unicode 的可变长度字符编码。 	
IP	配置 SYSLOG 服务器 IP 地址。	输入 IP 地址。	
发送者	配置风险消息发送者。	缺省值: dbapp。	
端口	配置服务器使用端口。	缺省值: 514。	
接收设置(当 SYSLO	G服务器的"发送格式"选择"	APT 风险通知"时,该参数可配)	
华兴米型	配置风险通知消息的发送类	◆ 发送统计消息	
反达尖尘	型。	◆ 发送单条	
类型	配置接收风险消息的类型。	点击下拉框选择。	
等级	配置接收风险消息的级别。	点击下拉框选择。	
KAFKA 服务器配置			
主题	设置 KAFKA 服务器的发送消息主题。	手动输入。	
服务器版本	设置 KAFKA 服务器版本。	◆ 0.8.0◆ 0.9.0 及以上	
	设置 KAFKA 服务器列表。可		
服务器列表	以输入多个服务器,以	例如: 192.168.1.1:9092。	
	IP:HOST 端口 方式填写。		



参数名称	参数说明	参数取值
是否需要压缩	配置 KAFKA 消息是否压缩传输。	是、否。
发送者	配置风险消息发送者。	缺省值: dbapp。
编码格式	配置服务器使用的编码格式。	 GBK: 汉字编码字符集。 UTF-8:针对 Unicode 的可变长度字符编码。
服务器响应	配置是否需要等待 KAFKA 服 务器响应再发送数据。	 不等待:发送方不等待 KAFKA 服务器接收响应,直接发送数据。延迟最低,数据仅仅发送一次,可靠性低。 等待 leader 应答:发送方等待 KAFKA 服务器器写入 leader 消息后发送数据。延迟较低,可靠性稍高,但仍然有丢失数据可能。 等待所有应答:发送方等待 KAFKA 服务器写入全部消息后发送数据。延迟较高,可靠性高,发送效率最低。
协议类型	选择协议类型	 ● 明文 ◆ SSL ◆ SASL 认证+明文 ◆ SASL 认证+SSL
邮件服务器配置		
发送邮件服务器	配置发送邮件服务器的域名或 者 IP 地址。	手动输入。
发送者	配置风险消息发送者。	缺省值: dbapp。
DNS 服务器配置	配置邮件服务器的 DNS 服务器 IP。	



参数名称	参数说明	参数取值				
发送者邮箱	配置发送者邮箱。	手动输入。				
		◆ 不需要验证:默认配置。				
SMTP 验证	配置是否使用邮件服务验证。	◆ 需要验证:选择该参数,需要配置验证密码				
		和加密类型(不加密、TLS 或 SSL 加密)。				
	配置邮件传输服务使用的端					
「「」	Π.	默认 ^远 口 23。				
接收设置(邮件服务器	器)					
每类事件显示前	配置接收邮件的显示数目。	默认 100条。可以手动输入。				
接收邮箱地址	配置接收邮箱地址。	手动输入。可以配置多个接收邮箱。				
FTP 服务器配置						
IP	配置 FTP 服务器的 IP 地址。	手动输入。				
上传目录	配置 FTP 主目录的相对路径。	手动输入。默认主目录则填写"/"				
端口	配置 FTP 服务器端口。	默认端口 21。				
田中名德田	配置 FTP 服务器登录用户名和					
用广名/密码	密码。	于动物八。				
伯田板士	可要吧夕照住口的炉刀按卡	◆ GBK: 汉字编码字符集。				
9冊1月16日1	化直服方态化用的编码俗工。	◆ UTF-8:针对 Unicode 的可变长度字符编码。				
接收设置 (FTP 服务器	接收设置 (FTP 服务器)					
举入 立供目夕曰一 立	配置单个接收文件最多显示的					
甲1`乂件	数目。	私以則 100 余。可以于动铜八。				



参数名称	参数说明	参数取值				
接收统计信息	配置是否接收邮件统计信息。	是、否。				
短信服务器配置						
服务器 IP	配置短信服务器 IP 地址。	手动输入,支持 IPv4 和 IPv6。				
格式	短信服务器格式。	默认。				
端口	配置短信服务器使用的端口。	手动输入。				
编码格式	配置服务器使用的编码格式。	◆ GBK: 汉字编码字符集。◆ UTF-8:针对 Unicode 的可变长度字符编码。				
请求参数	配置短信服务器的请求参数。 包括手机号码和短信,其中手	手动输入手机号码。 短信不需要配置,默认为告警信息。				
请求方式	配置短信服务器请求方式。	◆ GET:从服务器获取数据,安全性低。◆ POST:向服务器传送数据,安全性高。				
URL	配置短信服务器的 URL 地址。	手动输入。				
钉钉群机器人服务器设	段置					
机器人 URL	配置钉钉群机器人服务器URL 地址。	手动输入。				
上传恶意文件配置						
上传恶意文件的服务 器 IP	配置上传恶意文件的服务器 IP。	手动输入。				
上传风险相关恶意文	配置是否上传风险相关恶意文	◆ 上传。				
件	件。	◆ 不上传,默认值。				

1		信	È
2	DASIS		尼

参数名称	参数说明	参数取值	
上传风险相关沙箱报	配置是否上传风险相关沙箱报	◆ 上传。	
告	告。	◆ 不上传, 默认值。	
发送风险内容(当服务	S器类型选择"发送格式"选择'	"APT 风险通知"时,该参数需单独配)	
风险级剧	配置发送特定级别的风险消	今郊 宣 由 任	
/^いい23又力リ	息。	土叩、同、十、瓜。	
	配置发送特定攻击状态的风险	今郊 成功 学试 生際	
	消息。	王即、成功、云风、大阳。	
风险米到	配置发送特定类型的风险消	占土下拉框进场	
	息。		
		点击下拉框选择。	
客户网络	1110000000000000000000000000000000000	点击< 编辑 >, 可跳转到 " 配置>客户网络 "页面	
	2日。	进行配置。	
数据发送配置(当服务	S器类型选择"发送格式"选择'	"安恒 AILPHA 大数据平台"时,该参数可配)	
宙计信自	勾选是否发送审计信息及选择	相捉守际重再进行勿进	
甲口侣总	相关协议类型。	恨茄头 附而安近11 马匹。	
风险信息	请参考"发送风险内容"。	请参考"发送风险内容"。	
今迁应田辺別信自	勾选是否发送会话应用识别信	相捉实际重要进行勾进	
云山四田広が旧尽	息。	¹¹ 区加大附而女匹11 马匹。	
会话应用流量统计信	勾选是否发送会话应用流量统	相捉实际重曲进行力进	
 息	计信息及选择相关协议类型。	1改插头附而安近11 马匹。	



参数名称	参数说明	参数取值	
佐 榆巨流量统计	勾选是否发送传输层流量统	根据实际需要进行勾选	
15期层流里统1	计.		
应田曰纮注信自	勾选是否发送应用层统计信	由招令厅會再进行方法	
应用层犹计信息	息。	们的历史时而安定门马边远。	
恣叶仁头体让信白	勾选是否发送登陆行为统计信	古石今月中日生命方法	
豆陆行为筑计信息	息。	恨据头际需安进行勾远。	
立从中心人们	勾选是否发送文件安全监测信	也很实际重要进行力进	
义件女王位测信总	息。	依据头际 带安 进行	

- ◆ 发送数据时默认数据不加密,当发送数据时选择数据加密,密钥可以选择默认或者自定义, 密钥加密方式是"base64"。
- ◆ 对于 KAFKA 服务器,系统支持安恒 AiLPHA 大数据平台 3.5 及以上版本接口规范(JSON 格式),并且支持审计信息配置白名单时是否外送、告警时是否外送、非告警时是否外送。
 - ◆ 勾选白名单时外送: 支持 HTTP 协议的客户端白名单、服务端白名单、HTTP 的 IDS 规则。
 - ◆ 勾选(非)告警时外送:支持 HTTP 协议和 DNS 协议的 IDS 规则。

4.4.2 发送字段配置

在主菜单选择"配置",然后在左侧导航树选择"数据外送>发送字段配置",配置发送服务器的设备

ID、设备名称和厂商代码。

字段信息的字段适只适用于自定义 json 格式 (对接安恒信息的 AiLPHA 大数据平台), 默认发送开启的 字段 (状态栏下开关设置为 □)。



12.W	з	Territory and the second		
TT WHERE	191			
(i) 10.000 (ii) 10.000 (iii)	-	∃ 協動信仰		
C UARE	1	- 2940 0		
Ex CLOTED	-	SEER devicemente		
		/78/56 1		
	4	● 字段信息		
		φn&#</td><td>8525</td><td></td></tr><tr><th></th><td></td><td>accessAgent</td><td></td><td></td></tr><tr><th></th><td></td><td>acctClashi</td><td>C</td><td></td></tr><tr><th></th><td></td><td>acitSessionid</td><td></td><td></td></tr><tr><th></th><td></td><td>acctitutus</td><td></td><td></td></tr><tr><th></th><td></td><td>attelProduct</td><td></td><td></td></tr></tbody></table>		

4.4.3 安全域配置

安全域配置用于从 AiLPHA 大数据平台上更新安全域、内网 IP、规则等, 该功能默认关闭。

在主菜单选择"配置",然后在左侧导航树选择"数据外送>安全域配置",配置 AiLPHA 大数据平台的 IP 以及端口并且启用该功能后,就可以从该平台上更新信息。

展開		1941-14-cm m	安洋海绵和雪 出合体和雪 执行审计	
部 米埃配置		as// mileo		
 () 检测配置 	~			
C. 形动配置	~	状态	: 〇 启用 ④ 数用	
		*.(P:	: IIINEADP	
		* (MC):	2 这号)465355间即国39	
		协议:	D HTTPS O HTTP	
		機型:	: 🗋 安全城 📃 内部(P 🛄 現明	
			- 21 7	

4.4.4 协议审计

协议审计用于控制服务器信息-审计信息部分, ICMP、NETFLOW 协议外送勾选按钮显示, 默认关闭。

在主菜单选择"配置",然后在左侧导航树选择"数据外送>协议审计",选择开启按钮,点击保存,就



可以在配置服务器信息-审计信息部分勾选这两个协议。

Ini	服务操作曲	发送	260表2個	安全场	5100	はいいます
~	axyo parimos	68.40.3	P.S.COLUM	3K 3E 448		U ASTER
~	F协议审计					
~		ICMP:	开启	 美国 	1	
	NET	FLOW:	开启	• 郑	(仅期	W10版本)
			1941			
	 × × 	SE 服务器信息 、 F 协议审计 、 NE	編 服务器信息 友送 ・ ・ ・ ・ ・ ・ ・ ・ か な 市 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	SE 服务器信息 发送字段配置 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	SE 服务器信息 发送字段配置 安全域 ・ ・ ・ ・ ・ 協议审计 ICMP: ○ 开启 ④ 关灯 NETFLOW: ○ 开启 ④ 关灯 保存	SE 服务器信息 发送字段配置 安全域配置 ・ ・ ・ ・ ・ ・ ・ 協议审计 ICMP: ○ 开启 ④ 关闭 NETFLOW: ○ 开启 ④ 关闭 (仅限 保存



5. 系统

登录数据中心 (探测器) Web 界面可以看到"系统"选项卡下所有菜单。

分布式部署场景下,登录单个探测器 Web 界面,进入"系统"选项卡只能看到部分菜单,不能对"系统" 配置进行修改。

系统菜单主要功能有**权限管理、数据维护、系统资源、升级管理、许可证、日志管理**和**其他。**系统配置功 能可以让管理员用户更好的管理系统权限、数据、资源、许可、升级和日志等重要系统功能,让设备更加 安全高效的运行。

采用	3	_									
() exercise	~	810			_						
+ 用户管理		用户名	角色	用户认证		Pddrouw.	矛机	filit	465	操作项	
· 角色管理		admin	川边查着员, 配度管理员	家份登录		Dog.c	155 396	Administrator		181 B	
·用户安全设置		analyzer	风险查看员	常研發展		mple.c		analyzer			
 IPutitizeni 		config	配置管理质	2002年		pla.com		config		2 P	
• 动态令牌整理		system	来续蒙瑞员	医颈壁袋		iple.co		system		B	
· 0.955922		test1	test_role	市研設業						10 1 2	12
ES REALEMENT		cenig	风险查费员、 配面管理员	图码+动态		om				2.0	1
昌 系統資源	-	ji .	刘治去举点, 纪宫堂理师	密詞+読む						(a) (2	1
国 升级管理		wangf	风险要要员 , 配度管理员	密码整象						121 8	8
四 許可证		analyzer1	用這些要要出	常研設業		D99.5				IN D	1
日本常課	- 10	config1	配置管理师	主动教育		Deg.				2 8	1
皇旨 純信	÷	system1	系统管理员	医铜酸素		Dqq.c.				LE I R	12
		number_1	风险查察员、 配置管理员	市行登录						818	8
		look	风险查费员、配置管理员	市行整象						2 8	2

5.1 权限管理

5.1.1 角色管理

系统内置四个角色为风险查看员、配置管理员、系统管理员和超级管理员。详细情况请参考系统自带用户

<u>和角色</u>。



操作入口

在菜单栏选择"**系统>权限管理>角色管理**"进入**角色管理**页面。

点击<新增>添加角色并且赋予新角色对应权限。

新增角色		×
*角色名称:	请输入角色名称	
* 权限:	☑ 导航 □ 分析 □ 风险 □ 报表	
	□ 探测器 □ 配置 □ 系统	
描述:	请输入描述信息,长度为0-128位	li li
	取消 确定	

5.1.2 **用户管理**

系统自带四个用户。对应系统缺省的四种角色,支持编辑但无法删除。

用户	角色	对应权限	初始密码
analyzer	风险查看员	查看导航、分析、风险记录、报表等	Dbapp@2014
config	配置管理员	配置引擎、策略、探测器、告警外送等	Dbapp@2014
system	系统管理员	拥有系统级别的配置、权限管理权限	Dbapp@2014
admin	超级管理员	系统所有权限	Dbapp@2014

操作入口

在菜单栏选择"系统>权限管理>用户管理"进入用户管理页面,点击<新增>创建新用户。支持对非系统



自带用户进行编辑和删除操作。

新建用户界面包括基本信息、联系方式、角色类型等,根据界面提示信息直接填写即可。点击 <</td>用或禁用该用户名。

登录认证方式可选择密码登录、密码+动态口令登录。动态令牌需要在"系统>权限管理>动态令牌管理" 中导入对应的 xml 文件, 具体配置请参考动态 令 牌 管 理。

005-	THAT U BAT
+ 1914-342	lest
新选	潮流用户
- 1973	
* #\$U.85%	
- BERIFIC	
* Email,	test@qq.com
<i>∓4</i> %	3034 February an Edit Southern Consultant
- 角色类型	
READ	S Flands. S finites. S sierrich
- 教堂法语	
+ WERE	
+ 143-5-18-6-512	060000000000000000000000000000000000000

认证方式为密码+动态口令登录的用户登录系统输入正确的用户名密码后还需要输入动态口令方可登录成

功。



如果时间不一致,导致口令校验错误,可点击输入框中的同步按钮。进行同步,同步完成后输入当前口令

即可。当前动态口令输入当前显示的口令,下一条动态口令输入当前口令改变后的下一条口令。

100 明	将令牌显示的动态口令 0 的口令改变后,将新的	输入 "当前动态口令" 框中,待令牌显示 动态口令输入 "下一条动态口令" 框中。	
	*当前动态口令:	清姫入	
	*下一条动态口令:	诸编入	

新增用户或修改用户密码后,系统暂不做强制性退出,需单独退出重新登录才能生效。

5.1.3 用户安全设置

在菜单栏选择"系统>权限管理>用户安全设置"进入用户安全设置页面。

配置安全相关选项,包括登录安全设置、密码长度设置、密码过期设置、超时设置等。

ኛ 安恒信息

三日	3	
() ermann	1	于 塑像安全设置
• 用户整理		60 彩之内,用户型试量是的关系次数通过 3 次,数据该用户 60 彩。
 加合管理 		
 личения 		产 电彩长度设置
• 伊尔河动制		最短度码长度 8
+ 3654時間提		
· ###0.0222		▶ 場例計測设置
C: REMP		世界に明辺第 〇 二月 ③ 第月
昌 新庆庆道		常用/DBBH用 7 天
日 升级管理	6	
• 平动升级		807
 · · ·		
 〒時配用 		
1991年		÷ 机时间均分别
E 日本智速	8	00 50件运无操作。用户需要重新型款
显音 神线	×.	
		9077

5.1.4 IP 访问控制

在菜单栏选择"系统>权限管理>IP 访问控制"进入 IP 访问控制页面。

◆ 启用该功能时,可以新增、修改、删除、导入访问该设备的 IP 地址或者 IP 地址段。开启后,只有当前列表中的 IP 地址可以访问 APT 设备。

若列表中无数据或所有 IP 都被禁用, IP 访问控制无效, 所有 IP 都可以访问。

◆ 禁用该功能时,不容许新增、导入、全部导出、删除 IP 访问控制列表等操作。所有 IP 都可以访问 APT

设备。



🕜 安恒信息



5.1.5 动态令牌管理

导入对应的 xml 文件,列表上会显示动态口令的序列号、生产时间、失效时间。

14 1	C and a second			
O HARMY	A A A			
1.0100	8.91E	1.995	3000004	uera.
+ 80.00	20207026400130	2020-01-14 Hete25	2014-02-05 10-05-25	0
- N*****				ATA DAT - I - MALE - I
* TOOLN	-			
alter mette				
S new				

5.1.6 **敏感信息管理**

操作入口

在菜单栏选择"系统>权限管理>敏感信息管理"进入敏感信息管理页面。

系统用户查**弱密码、暴力破解、密码明文传输**类型风险详情时,需输入**敏感信息管理密码**才能够查看告警 中含有的密码信息、下载或者在线预览数据包。

系统分为三类用户:无权限用户、需要验证密码用户、无需验证密码用户。

管理密码可以默认同 admin 账号密码,也可以新建管理密码。

雪的	 愛用admin账号(验证偿码同admin账号) 新建管理 	王宗 马
查看案研范围		
查看他妈边跑	2 第三百 18 金方如新 10 五日和文形式10 1	
查看來得权限		
• 权限派遣	- 元素始正就以豊示電码。关联用户:	U
	NAME AND ADDRESS OF ADDRESS ADDRES	WARD DOWN OF THE OWNER

无需验证用户,密码直接显示,数据包可以下载和在线预览;

无权限用户查看相应风险详情时,密码隐藏,无查看按钮,无法下载预览数据包,如图所示。



数据包名称	2012181648030000760.pcap	
攻击状态	要議	
风险相关信 息	admin20账户发现弱口令隐患【密码长度为7,密码字符类型单一,密码为r*****6】	

需要验证密码用户查看相应风险详情时,密码隐藏,查看按钮显示;点击弹出敏感信息密码输入弹框,如

图所示。

RIUUSAN - BULL	dbird, and and		
14.00			
2020-12-10-10-00-01			
Statement In Seattle	社 正教 新 唐朝 聖 理 把 50	1.00	
2010/12/19 14:46:02	DOMESTIC CONTRACTOR		
2010/10/10 10 16 46:01	NAME AND ADDRESS OF ADDRESS		
2015-12 10 10-00022	(1)日本1: 本町11年4回(1)日日本1:		
2010 (2.18 14 48 45	A PERSONAL PROPERTY.		
2010-12-19 14-40-08	analysis of the second endedth as a statement of	and the second s	
pere la la Manuel			
2010/10/10 10:0648/00	* 800 () () () () () () () () () (
2010/12/18 16:40:00	C TASH - TO CONTRACT	1.1.1.1	
2025 12:10 26:4025	1034 (F 1010)	073988	
2020 12 18 24-0000		Sector Street	
2008-12-18 1548-55			
2810 12 18 164600	2.0		
3079 (2.1876-800)			
250 CONTRACTOR			
2009-1018-1648-00			
2010/12/10 14:46:41			
2010/12/18 14:44019			
100000			

5.2 数据维护

数据维护配置包括备份与恢复、自动清理和出厂设置等相关配置。

备份和恢复只能在每台机器上面单独完成,数据中心不能控制探测器的备份和恢复。

5.2.1 自动备份

@

自动备份采用备份前一天的告警数据方式完成,并且提供 FTP 自定义时间点外送到备份服务器上以及上传 备份文件的功能。

无论是否配置 FTP 服务器及发送配置,数据都会在本地自动备份。为了确保备份数据安全性,建议配置 FTP 服务器并且开启备份数据自动外送功能。



备份选项卡配置功能点包括:备份文件存放目录、占用所属分区最大比例、FTP 服务器及发送配置以及历 史备份记录等。

应用举例

使用场景:每天0点时开始备份,上传到备份服务器192.168.33.196的目录为/data/recv/backup。

操作步骤

- 步骤1. 登录 APT Web 界面,在菜单栏选择"系统>数据维护>备份和恢复"进入备份与恢复页面,选择 自动备份及恢复页签。
- 步骤2. 选择"备份"页签,设置自动备份参数。
 - 1) 设置备份占用所属分区最大比例为 20%。
 - 2) 配置 FTP 服务器,备份文件产生后将自动上传到 FTP 服务器。需要确保 FTP 服务器可
 - 用,配置完成后,点击<测试连接>测试 FTP 服务器是否可用。

新创配器						
份文件存放目录		古比斯麗分区最大比	89 20 16			
FTP服务器及分词最	e cia					
10.070						
开窗外送	(3)	在一点发送		后的备使	zebfiP@68. D Mendelmanstr	
1118/02						
* FTP图例翻护:	3150,5			* 98(2)-	21	
* 闸户条:	300A			(数码)	1986.A	
1上市日景;	1710.1					

步骤3. 点击<保存>。



步骤4. 当时间到次日0点时,备份文件生成后,可以在历史备份记录列表中查看备份文件。备份文件会

自动上传到 FTP 服务器。

Partial and NERLARD				
1000	CROME	Ref.	208.64	PTONEDIRE .
interaction in the constant of 1	1 2010-06-29 2606-54 11	104.000	100	84(44339443-538301-788101+
				218 I I 385 85 - 1

5.2.2 自动恢复

点击<恢复向导>进行数据恢复操作。

2010年7月,1月1日日前 1月1日日前				
NHR	Remain	敗匪実型	秋志	绿竹油
192.168.33.225(APT放击振鳌平台)	2020-12-15 17:25:22 2020-12-22 17:25:22	Eatis	处理成功! 最份依赖结果:依赖文件[0]个	в

操作步骤

步骤1. 在菜单栏选择 "系统>数据维护>备份和恢复"进入备份与恢复页面,选择自动备份及恢复页签。

步骤2. 选择恢复页签。

步骤3. 点击<恢复向导>,选择备份文件存在的位置。

有两个位置供选择:一个是本地目录: /data/recv/backup, 一个是 FTP 服务器。本地目录为必选,



如选择 FTP 服务器,系统会通过 FTP 服务器上的备份文件进行恢复。

恢复内待		×
第1/2步: 请向您	御祭夏始文件在慮望?	
10. # 10 C H 10 4 4	they/lineterp	
ETF服务部		
* FTP程格翻P;	10.20.28.119	
* 18171	32	
* RPE:	admin	
* 1939.	and and a second se	
1上作巨致;	1	
	RMARE	
	和2月 — 不一步	

- 步骤4. 点击<下一步>,选择数据的发生时间段进行恢复。
 - 1) 选择要恢复的探测器。

NUMBER OF					
第2/2步:请问总想恢复的内	宿却什么?				
FREE MALMALITYS	International o				
14H188 0 2020-12-	io 16 30 29 - 2020-12 17	16 20 29			
· MER SALANS		Real west	CINEW		
FMB.	已為初始家	λR.	文件大小	+8	
102.148.11.75 [APTINES].	2020-07-21 = 2020	143 💷 📾	65.7M		
	共主席	21675	C ED	80.5	C)

2) 选择要还原的时间范围和数据类型,然后点击<完成>。





步骤5. 在弹出的提示框点击<确定>,提交自动恢复任务。

步骤6. 等待几分钟,在恢复列表中查数据恢复情况。

anarthia rasylica				
40 88				
NAMES OF BERMAN				
WHEN	and distantia	and we have a second	855	9910
NATIONAL SERVICES (REPORT MORPHIC	* 3030-03-30 00.5700 + 3030-01-07 00.5700	Hauton		- 5
			stin 🚺 2000	42 × 5

5.2.3 手工备份

操作步骤

步骤1. 在菜单栏选择 "系统>数据维护>备份和恢复"进入备份与恢复页面,选择手动备份及恢复页签。

- 步骤2. 选择备份页签。
- 步骤3. 点击<备份当前配置>,备份系统当前的配置信息。

备份完成后,在备份文件列表点击该备份文件可以下载到本地。

en var					
MIN NORMALINE					
路份文件召用	完成期间	文件大小	8303-4	115	接作词
names chi 2020122217282	2020-12-22 17:29:45	2146	20.66.22728.201222	 1235 	

5.2.4 **手工恢复**

操作步骤

步骤1. 登录系统 Web 管理界面, 点击"系统"主菜单, 在备份和恢复页面, 选择手动备份及恢复页签。

步骤2. 选择恢复页签,上传备份文件进行手动恢复数据。



该操作会导致原有配置被覆盖,使用时请谨慎操作。

5.2.5 自动清理

开启自动清理配置后,可以防止在线数据占满系统存储空间。

在菜单栏选择"系统>数据维护>自动清理"进入自动清理配置页面, 启用或禁用该功能。

当存储空间达到系统配置阈值上限 (如下图配置的 80%) 就会清理业务数据及文件系统中的部分文件, 直

到占用空间低于配置阈值下限(如下图中配置的 70%)。

系统默认不配置数据保存时限,用户可以根据自己需要进行配置,界面如下所示。

守恒信息



-	1.00	+ economica	7-64000020	52
() contra				
E sum		DOUGHE & RM MIN	2925-11-29-10.09-18	
+ 9400nm	_	entification of the	2002 2019 1444 2017 2019 2010 111 111 2016 2017 10	
- Record		The second se	U 2820-11-29 18 AB-AN	
+ 01" 10 B	_	- STARETYNNAMOLEN IN N	MME259 3448. #HEADBR 2020-11.10	
B annu		ADDATES & AND CONTRACT MIL	40 871.1s	
		Comment of the second sec	1000 1010 1448, 10095100 2020-11-00	
13 milii			U 2020-11-29-18-48-88	
E Sient			##2019.1448	
107 and			46 42 (h	
			0 2930-17-29 19 49 19	
			- 100時代1月11-1043 - 100時日1月11-1041 - 1010日 - 1011 - 1011-1011 - 1011-1011	

- ◆ 清理动作门限可配置。默认 80%, 即当数据分区的磁盘空间被占用超过 80%后, 系统会自动清理数据 直到空间占用小于 70% (默认值, 可配置), 由最老的数据开始清理。
- ◆ 在线数据文件保存目录默认使用数据分区"/data"。
- ◆ 清理数据前会先进行数据备份,除非备份目录也达到清理上限。

5.2.6 出厂设置

出厂设置包含两个功能,一个是清理业务数据,一个是恢复出厂设置。

1 第一次设备出厂时做清空测试业务数据。此功能会清空系统内部数据,请谨慎操作。

在主菜单选择"系统",然后在左侧导航树选择"数据维护>出厂设置"。



清理业务数据

删除全系统所有业务相关的数据,包括风险、审计、报表、日志信息等 (配置信息不会删除)。

请慎重执行!

恢复出厂设置

删除系统所有数据及配置信息,恢复到出厂状态,请慎重执行!



恢复出厂设置后, admin 密码会恢复为初始密码 Dbapp@2014。

5.3 系统资源

在菜单栏选择选择"系统>系统资源"查看系统自身或各个探测器运行状态,包括 CPU 使用率、内存使用

玆	莝	
Ŧ	Ŧ	۰

20年	31	· production			
① 权限管理	~	F 赤斑斑潭			
白 松照维护	~	1938	APT攻击损警平台		
		内在	(73%	#31.26 (rost-in-tr incodition)
① 升级管理	2	支援空间	(1738	关32.0G()304-68-67()686-69()87()
国 许可证		CPUE	229		(2017-0)-37 19月0-(3)時前
日本管理	~	原明分区:	-	70%	共31.4G could as it thousanting
185 其他	~	截截分图:	C 119		共1.77 (2017-05-1) 1920-000m
	=	1000000	129		共49.1G coor in it in addation
		人產種中分配	¢1%		共968M courses of subscription

5.4 升级管理

5.4.1 **手动升级**

5.4.1.1 **系统版本/排错版本升级**

前提条件

已经获取版本升级包文件且文件版本比系统当前版本新。

◆ 系统版本升级包示例:

GoldenEyeIPv6_B9A2C_sen2.0.66.22621.201216_ser2.0.66.22620.201216_r23146.encrypt.tar.gz

◆ 排错版本升级包示例:

GoldenEyeIPv6_1F350_maintain2.0.66.22457.201210_r23158.encrypt.tar.gz



系统版本升级和排错版本升级操作方法相同。

升级步骤



步骤1. 在菜单栏选择"系统>升级管理>手动升级"进入手动升级页面,选择版本升级页签。

步骤2. 点击<选择文件>,选择版本升级文件点击上传。

英称	8				
③ 校開業用	~	版本计组	重略成升级		
• HP#8					
• 用的管理					
• 用户安全设置			E	<u>,</u>	版本升级 1 82760/28+715
 (P切)可能如 					1. MANDINISTED 1014. EMPATION. DD-19814. E-1702ALL. 8:47-7.
• 动态分钟管理		1.000	2.0.66		
· #1810.01274	1				1011.3.11
Es manne	~				
• 黃衍与印题					
+ stanoopta		≑備近—次升级	- 90M		
• 出厂设施		新國制作	2020-12-31 10:07:46		
圖 系统资源		-	新日期版中从 2.0.65.225	989.201230 升极型 2.	0.66.23611.201230;
តា សារាមាធ	e l	710252544	回日國版平从20166.225 該博特意加平光支化、当	903-2012-30 并现金 2. (南版本: 2.0.65,21030.	0.00,21012,2012.10; 201012;

步骤3. 确认升级成功。

- 1) 上传成功后,等待一段时间完成升级。
 - ◆ 对于系统版本升级,一般需要等待 10~20 分钟左右的时间。若升级版本跨度较大,需
 多等待一段时间。
 - ◆ 对于排错版本升级,一般等待5分钟左右就可以。
- 2) 点击上图的<刷新>按钮。
- 重新登录 APT 系统,再次进入上图页面查看右下方的升级信息。如果升级时间信息和升级
 结果信息显示与本次升级操作时间以及版本号一致,则表明本次升级成功。

相关操作

当有添加探测器的情况下,可以在数据中心设备的"探测器"菜单下点击 ^(~) 按钮对探测器进行手动升级, 若不进行手动升级,探测器也能从数据中心自动同步版本并升级。



1803 #104 1	ERCPRE: 10.148.33.14						
100							
en al	1000	#.5		eerver SLB	REA++MINAL INCO	WOR-HEREING MINUT	36710
的行动者的展开的	102168.10.161	3*	2030.10150.00000	20461993030000	1	8	
Nitala?	102.188.1120	正常	20.65 THYNG, 200 BOY	2045/19142.200819		4	X 3 4 4
						278 1 1 28	11 ALC - 1

5.4.1.2 策略版本升级

完成系统版本升级和排错版本升级后,检查策略库版本信息,如果获取的策略包比当前系统显示的版本新,

则执行策略库版本升级操作。否则无需升级策略库版本。

前提条件

已经获取策略库升级包文件且文件版本比系统当前版本新。

策略版本升级包示例: GoldenEyeIPv6_17DEC_strategy2.0.22505.201212.1.encrypt.tar.gz

升级步骤

步骤1. 在手动升级页面,选择策略库升级页签。

步骤2. 点击<选择文件>按钮,选择版本升级文件点击上传。

演曲				
③ 松和田田	-	居本升级	角色年升组	
S mmmp	181			
国 升级管理	14		ASA	第略库升级
• #25HB			58082	2. 00007401024000015-000
+ 0359-9			2.0	(BURSON)
+ 元時秋度			Senten Contract	
🗈 গণ্যৱ				
图 日本市理	19			
95 Mm	18.0	F藏統一次升銀	6R 😳	
		19/80496	2020-12-15 01:30:34	
		开始热潮	第86年8月年已开始第12.0.22505.201212.1	

步骤3. 确认升级成功。



- 1) 上传成功后,等待5分钟左右的时间。若升级版本软件包较大,需多等待一段时间。
- 2) 点击上图的<刷新>按钮。
- 重新登录 APT 系统,再次进入上图页面查看右下方的升级信息。如果升级时间信息和升级
 结果信息显示与本次升级操作时间以及版本号一致,则表明本次升级成功。

5.4.2 在线升级

除了本地手动升级外,还可以通过在线升级方式对产品进行升级。

操作前提

- ◆ APT 设备具有外网访问权限,可以连接 APT 云端服务器。
- 当云端服务器的版本升级包、排错升级包、策略升级包比当前设备的版本要新的时候,在线升级界面 就会显示有最新版本可以更新,点击实时升级按钮即可升级。

操作方法

步骤1. 登录 APT Web 管理页面,在菜单栏选择 "系统>升级管理>在线升级"进入在线升级页面。

步骤2. 点击<在线升级>按钮进行升级。

◆ 有多个更新时,需要一个升级完成后再进行下一个升级。

▶ 策略升级需要在版本升级完成后进行。



步骤3. 升级验证。

等待升级完成后,重新进入"在线升级"页面,查看当前版本是否为最新版本。

5.4.3 云端配置

开启云端配置后, APT 可以引入安恒信息的云端威胁情报等资源, 提升检测能力及对新发安全事件的响应

速度。云端配置功能包括云端配置和云端功能配置。

使用前提

APT 设备可以访问云端服务器。

操作入口

在菜单栏选择"系统>升级管理>云端配置"进入云端配置页面,点击云端配置开关 [●]开启或关闭云端配置功能。可使用默认的云端地址或者手动配置云端地址和端口。

可使用默认的云端地址或者手动配置云端地址和端口。

安恒信息

F 五端記載 CO NGRE Epison - REALER - RENER -			
* #94932; aproxid d5appsecurity com cn	+ pe(1)	445	10.14
* HORE A 400	* 98[];	1)114000000000	
N.使用户名: 000.3	从证券的	8987	

编辑云端地址时可选择<代理服务>,需填写代理服务地址、端口、认证用户名和认证密码。

代理服务器 (Proxy Server) 可以代理网络用户访问网络信息。增加代理服务功能,便于内网用户通过代理服务访问云端内容,进行云端功能配置。

配置完成后点击<保存>。点击<在线验证>查看云端配置是否可以正常使用。

云端功能配置

配置是否使用各种云端功能。包括策略库自动更新、上传恶意样本到云端、紧急事件云端同步、威胁情报 更新、版本自动更新、排错平台自动更新等。

▶ 运输功能能器					
alatin = ≘somµ.	•	Range Baller		MALLINER CONT	
43/8E29	•	810357	•	ALB = Whate	•

5.4.4 托管配置

托管配置是将本地设备托管到大数据平台,可以由大数据平台进行统一管理,对设备版本升级、许可证更 新进行同步等操作,本地设备无法再对这些功能进行操作。

配置成功后, APT 产品可以从大数据平台同步关闭 IDS 规则, 对 IDS 规则进行管理; 独立沙箱产品可以从 大数据平台同步文件检测配置。

操作入口

💦 安恒信息



◆ 当状态开关打开时,可以编辑托管服务器地址,须填写 IP 域名和端口号,点击<保存>即刻生效。

服务器配置	
状态;	
IP域名:	80.000 C
* 端口:	
	保存取消托管

◆ 点击<**取消托管**>,可关闭该功能。

÷

5.5 许可证

查看当前系统许可证的使用期及维护期。

操作入口

在菜单栏选择"系统>许可证"进入许可证页面。

点击<上传许可>上传并更新许可证。

0		- anne
- In the		
< and a second		
- Investors		
Basse -		
B seed	- MARKED -	
Ш нене -	松井根用片半 2	
az ene		
E HARR	difficit APT broughts but	
22 + 19 -	0/1903)1 2021-01-04 23 10 28	
	annual ()	

申请许可时需注意产品形态,请选择用户需要的"许可类型"。

杭州安恒信息技术股份有限公司



5.6 日志管理

5.6.1 系统日志

记录系统运行相关日志信息,包括异常日志、通讯日志和其他日志等。

操作入口

在菜单栏选择"系统>日志管理>系统日志"进入系统日志页面。

查看所有系统日志,点击 🖩 输入筛选条件查询日志;点击日志对应的 🗎 查看日志详细信息、处理日志。

系统支持系统日志的导出。

±#		-						
· RIMER	121	TALL						19.15
E mump	121	. 2010 HB	DOM:0	実現し	統治工	単件側32	entre :	1877-18
5 FILES		3021-05-17 99:4630	AFTSZMWFS	神業日本	+ 不此權	110.002	土机加制等的全体使用单位。	10
E HORE	120	2021-05-17 09:36:00	APTERMENT	90.00118	+ ###B	11.679.25	ER.METHAS/ERHEL.	2
112 年初期		2021-01-17 09:26:00	APTELEPH	semilar.	+ 722	10.000	ERNETHING BAD	18
E nome	14	3023-05-17 09(16:59	APTRISADERIA	科学日本	+ 10.0	PERMAN.	这些目的是这些问题中间。	12
· BRIDE		3021-05-17 (9605-54	APTRIAMETH	宗常日命	+ + = = =	RAMPA	11.1.4年5分26世中年(14
+ ###Gitt	14	2071-05-17 08:55-54	APTERBERT	新新日田	+ 31010	marray	355567599999	10
+ #463m		2021-05-17.0006535	AFTROMWED	种植日生	+ 754238	manag	上机台机关种空间来中间。	12
98 mm	1.00	2021-05-17-06:35:53	APTILIZERFW	90MD #	+ 1112	10.41925	28.NR2985/02968(. 10
		2021-05-17 (0:25:52	APTROCHERIN	99.80.0 E	+ 1100	10.41723	35.0851R20(#948)	120
		2021-05-17 08:15:52	APTRAMETED	於第日年	+ 41238	25.017.03	土机和机场经空间使用单门。	12
		2921-25-17-00/05/11	ATTREAMPTO	算用日间	+ H108	1000	ENARSESSIERE.	12
					2.122.5			

5.6.2 操作日志

记录用户对系统的操作信息,包括登录系统、退出系统及各种新增、修改、删除等信息。

操作入口

在菜单栏选择"**系统>日志管理>操作日志**"进入**操作日志**页面。

查看所有操作日志, 点击 🍹 输入筛选条件查询日志; 点击日志对应的 🖹 查看日志详细信息。



系统支持操作系统日志的导出。

20	- 18	-							
O ROWARD	-	4994							2.10
Et annone		BRINE _	605	(2) (\$1.0	1546-8	ANTE:	10.0	HIR.	121718
L SER		2021-05-17 09:51:34	andreine	10.20.00128	网络雷德	8423	* 450	管制成功	
国 舟橋龍田		2021-05-17 0908call	solimies	10.11.47.7	网络	65	* 4840	#2004直接	9
83 H-102		2021-05-17.0908-52	astrop	30,11.42.7	系统 计线管语 改管型	60	+ 40.0	机构和利用管	
E stim	1.0	2021-05-17.0948-29	astrop	10,11,47,0	彩线 计语言语 六等能。	46.0	+ 4020	机构和利用	
+ Minerson	_	2021-05-17 00:26:29	admin	10,11.15,200	1420	N0581	+ (00)	的地名达希尔托斯	
+ INTER		2021-05-17 00:32:24	admin	10,11,15,370	P100	N0284	+ (00)	IN SERVICE IN CONTRACT, INC.	а.
1 11932		2021-05-17.003022	altern	101113200	传机登进	1000	+ 1622	重要成功	1.1
10 月11	3	2021-05-17.00/2029	altern	101113-209	传动数据	1000	* 15	gath ROARSH.	
		2021-05-17.0927.04	40+0	1011.47.7	用纳量源	8422	+ 452	建原始结	12
		2021-05-15 161919	40110	10.20.90.128	84	RARE	* 4921	的现代结果所任用	12
		2021-05-11 161826	admin	10.00.00.00	715	NORM	+ (52)	#105016XILB	10.
									12
					31 201 8		1 4 - 1	> 208-51 W	a i a

5.6.3 升级日志

记录设备升级信息,便于用户查看版本、策略等升级记录和升级结果。

操作入口

在菜单栏选择"系统>日志管理>升级日志"进入升级日志页面。

查看所有升级日志,点击日志对应的 🖹 查看日志详细信息。系统支持升级日志的导出。

10.46		and the second se			
© execution	~	401H			
ES ASSESSE	9	Filmina	升级类型	FISHER	細作場
墨 和店商店		2021-05-75 16/92/04	展在开展	個別編集古王会伝, 由利田市: 206724573210513, -b//→保護部	4E
国 开编管理		2521-04-14-124906	双耳开病	副目標標本未完成, 店前加水: 20672457131051% +br/+例386	a. u
關 许可证		2321-05-14 09:43:01	旗串升幅	銀登編編本3A, 2:0.67.24572.210512 升级架; 2:0.67.24571.210513	(h.) 😫
〇〇日本市理	- 16	2321-05-14 01 30 43	推动对征	新闻的18-18-19-18-19-18-19-19-19-19-19-19-19-19-19-19-19-19-19-	
* 8883 S		2021-05-13 12:41:00	我不开祝	副原冊成本 後、2067-24571,210512 升級国: 20.67,24573,210513;	- <u>10</u>
· smBit	-	2021-05-12 19:27:06	微年/10	重要理睬本从.2007.24570.210511 升线型:20.67.24571.210512	<u> </u>
• 개월日 年		2021-05-12-09/28/28	推進計構	服務機能本以 2.0.07.24560.210511 升級型: 2.0.07.24570.210511:	- R
95 min	10	2021-05-11 14(30:31	版工计由	他用每回本从 2.0.67.34568.210510 升级世 2.0.67.34565210511;	44 M
		2021-05-10 16251/16	(6):E.7+60	新売機能なみ 2007-24567.310500 井城空 20.07.24568.210518	- B
		2021-05-08 19:22:12	施市开垦	※外機協力王幸保,何期回去: 2.567.241657.210508,+64/+探測器	6f., La
		2021-05-01 18-4711	版工计编	前用用版本从 2.0.67.24562.210507 升级至 2.0.67.24567.210508	- 8
		**** < 0. ** : : ***			
				共471歳 1 3 3 4 5 6 → 34 3 70株団	Mill 1 1

5.7 其他



5.7.1 SNMP 配置

简单网络管理协议 (SNMP) 是用于 IP 网络管理 (服务器、工作站、路由器、交换机等) 的一种标准协议, 属于应用层协议。

启用 SNMP 配置后, APT 设备作为 SNMP 服务器, 客户端可以通过 oid 向 APT 发送请求并建立联系。

操作入口

在菜单栏选择"系统>其他>SNMP 配置"进入 SNMP 配置页面。

滑动开关开启或关闭 SNMP 功能。

开启 SNMP 配置之前需要确认 APT 设备的防火墙中是否开启 SNMP 服务,可以在"系统≻系

统资源"菜单下按"Shift+I"组合键查看 SNMP 服务是否开启。

◆ SNMP 版本为 V1&V2C 时,配置 Community string 值。配置界面如下。

* 豪蘭組祚	apt.	
< INTERED	Stanow	
* Ernali	aph@douppecturity.com/cm	
SNMPER	initial initialinitia initial initial initial initial initial initial initial	
· Community string	ca_apt	

◆ SNMP 版本为 V3 时,认证方式有不认证不加密(noAuthNoPriv)、仅认证(authNoPriv)、认证及加密(authPriv)这3种,需要配置用户名、密码、密码加密方式(MD5、SHA1)、传输加密方式(DES、AES)、传输加密密码等,配置界面如下。

开关。	
* 溢番名称	apt
* 物理位置	Unknown
* Email	apt@dbappsecuity.com.cn
SNMP版丰	○ V1&V2c
认证加密方式	○ 不认证不加责 ○ 仅认证 ⑧ 认证及加密
* 用户客	ana).
2 密码	- 1892A
= 唐明加密方式	182M4 (V)
传输加密方式	
ANDRES	SINLS.
	97 7

5.7.2 网络配置

网络配置包括管理口配置(包括 IP 版本、管理口 IP、子网掩码、网关等)、DNS 配置以及业务口配置等。

操作入口

在菜单栏选择"**系统>其他>网络配置**"进入网络配置页面。

78.5	a na live		
1000	462030134		
	346 378 3540		
- 1146	10.0010		1
	-		
- 04001	[and]		1
	-		ы.
D DAMAGE			
o Davidezili - Enite			J.
- UNIS - UNIS - UNIS			2
DAGER -Dag -Dag			2
- (m) - (m) - 681.008		C CRAIN (1

业务口配置功能可以自定义选择不需采集流量的网口, 配置界面如下所示。

杭州安恒信息技术股份有限公司

🟹 安恒信息



业务口选择:	一 待选择	0/10	已选择	0/1
	eth0	1	C eth3	
	C eth1			
	eth11	1		
	C eth2			
	eth4			
	eth5			
	🔲 eth6			
	eth7			


6. 分析

6.1 分析

6.1.1 紧急事件分析

以列表形式展现当前用户网络环境中出现的必须紧急处理的安全事件(**默认显示未处理的紧急事件**),让

用户更直观、更客观、更准确地感知紧急事件,处理紧急事件。

操作入口

在菜单栏选择"分析>分析>紧急事件分析"进入紧急事件分析页面。

-		915	彩牌	H72HMF	le a	#**	200	96	-1046	「日午台	NATRONE
									and and a local diversion of the second s	191	
									Part of the second s	100	int E
8112	化物化的				2.0.047			49.44	DALTHEN .		-
1.1	0.000	perpetant	INTERNAL PROPERTY	2031001025404080	10001112		0+1903001823.00.019	16-25-007	0.12-1110/1646		- selanisti
410		to ingrange	ETHER BALLY (20,50-14/01120-05/000	00801152		VP 180001118.25.22.510	11525-013	0-12-17 145753		Restore
418	1.000		eensy off	Caralitication (www.	\$80,004.5			Takini arcia	thing of second		- 20030412100
14.1	0.000		1000 1995/7-0100	LESSE MADRIES	NUMBER OF T		12	141100.002	6.12-17 LADIU		Treatment .
414			estaton, mateix ()	20,5914094) \$1258.1.0000	1000 (1162)		PROBATTIBLIS, JOS W	11525-003	0-12-17133455		- STRAILADT
418	1.000		into trate (yes	mina editedite	Sindowings		81	10.11.000	on a contract of the		- and the real of
1.01	0.000		000-F20ME 1498	GUTE MOMONE	1000100		108	112104.00	632-77324100		· Ballinin
418			INTERNAL PARTY	sante methoday	entervision		•	16,2625,25	514-17 101462		- 208041
418	1000		int more than	mina entrange	Sindowings		£1.	TRATA I	DUANT TORON	- 1	CHILDREN .
	0.000		WOLDON HIM	IZTE MOMENT	10 Million March		55	1013-029	642-101010		NATHT
410			INTER CARLO STATE	CALLER MALERIN	entervision			10.11.575	0-12-171109453		- 401001731
418	1.400		invition of the	Inta sources	SHOWING T		81	. W. Hankin	etanie vruce		2,910
	0.000		000-000 Street	ISTE MOMENT	1000100		nt (10362511	632/17/00/011		1.10.11.11.11
. 10			man paker was		entervision			10.25 176.1	0-12-17 010121		
	1000		inst pair one	mina activizatio	SISSAND.		81	10.06.00.00	eine meinen die		
	0.000		1000 DALL 1000	CONTRACTOR INCOME.	NUMBER OF STREET		106	1626062	0.12/16/10/12/20		

- ◆ 点击页面右上角的[™], 输入筛选条件查询紧急事件; 点击[□] 查看紧急事件详细信息, 可以在跳转页面点击<处理>确认紧急事件; 点击[□] 直接确认紧急事件。
- ◆ 点击<导出>以表格形式导出当前紧急事件。

6.1.2 主机威胁分析

主机威胁分析基于不同风险事件对网络安全的威胁程度换算成一个可直观显示的数值,以便让用户更直观、

更客观、更准确地感知一个风险事件的威胁程度或者某个 IP 可能产生的风险影响范围。



操作入口

0.01110		1 28.4	40.00	438-046	0.02746304	0.2.0.000
tion of the second s		0.01110		-	2020-11-00 09:24:20	2010/10/17 10:04
121.79		-settinger tor		841	ACC0-11-0100/16-01	101001110-14 10141100
and the second		1.0201			ACCE 11 10 10-004	Canal Later Hadron
		0 (0.441-01-10)		1.000	6000.10.0010001010	count family contains
Contraction of the local distance of the loc		i matemati		2445	NUMERICAL PROPERTY AND	And in the same
The second s		0.000 (0.000)			(0.00.10) (0.11-05-00)	20020-1013-1014-0-0
117.04		10562048		-03	100.11.04 HISAR	UNDER THE REAL PROPERTY OF STREET, STR
Ne .	14	wire.00.401	*******	141	(4281-1-1-10.0000110-	3030-1017-002208
		i spinouti		Low 1	200-1-10 (Dece	and the second
ateria.		0.010.01		101	atom representation	mm0 (275 (0.000)
		10.00.004.000	******	Line,	and to second	print of O ministra
1.040		ing tag as and	*******	5, 844	(con-1) - (cons.c)	all all the the the street
		and and a		Ante	and the strength	and to the second
				1999	8508.71.00TT-0109	1040 () () () () () ()
		mattan ma	*******	Auto	and the probability	anan 19.11 2 00107
		0.00047		riots	instance of an Annal	10100 12110 municipa

在菜单栏选择"分析>分析>主机威胁分析"进入主机威胁分析页面。

查看主机威胁详细信息

点击主机威胁分析任意一条记录或者点击列表中 > 图标,可以展开查看主机 IP 的威胁指数、攻击溯源、攻 击过程、攻击溯源可视化选项卡等详细信息。

6.1.2.1 **主机威胁指数**

主机威胁指数选项卡展示主机IP在最近30天内的威胁活动和威胁性指数。如果主机存在相关的威胁活动,

包括被攻击行为或者主动攻击行为,则对应的威胁活动阶段会有一个绿色小图标。

例如,如果主机被渗透入侵或入侵他人,则威胁活动中的"渗透入侵"阶段会有一个绿色小图标

<u>渗透入侵9</u>, 图标上面的数字表示渗透入侵活动的次数。点击图标查看威胁详情。



A 284P	and line We will be	addecircle	10 (0.7792/0056)	Altochystophile Belleville
- 10.00.41.08		80	3020-11-18 D504-58	2020-12-17 13:35:47
teranam ma	an and analytic			
÷ 主机基本位用				
2504	10.20141.58			
##C#10 (121072)	HARRY - BANKY - BANK - BONDA - BEEK			
10701021030				
	\sim	$\wedge \wedge$	\sim	$\sim \sim$
-	V	\mathcal{N}	\Box	\sim

6.1.2.2 **攻击溯源、攻击过程和攻击溯源**

◆ 选择**攻击溯源**选项卡,页面展示攻击溯源时间轴,包括攻击类型、攻击次数和攻击状态等。如下图所示,点击**攻击次数**可查看具体攻击行为。

# ENIP	ality the second second	4639-0730	现品的被胡椒	20.2510.000
- isanaras		802	3020-YY-10 00:04:56	2020-17-17 13.31.4T
THERE NO. 20	ACT REAL PROPERTY AND			
0 2020-11-19 09-27-17 221-221-104-103 17正是符号接进行了 0 2020-11-19 11:06:24 47.91.170.222 17正是符号进行了	General and a second a second to the			
2020-11-20 02:10:31 47.245.57.170 2020日間回行了 ■1 2020-11-20 15:47:23	une and a same a same			
2020-11-22 13-42-34 2020-11-22 13-42-34 27.228.18.194 Hostinikali/17	netal les. Représ : ». attricte			

 ◆ 选择**攻击过程**选项卡,页面展示攻击过程图形化攻击阶段图。如下图所示,点击**攻击次数**可查看具体 攻击行为。

# 380P	4630-10143	wE391 07.95	观观界性影响	20.8.40.90.8000
··· 10.20.41.58	********	817/	2030-11-10 09:04:58	2020-12-17 11(15:47
25,609,682 33,828 53,8	2011 杂音描度空镜的。			
2020 11-10 0054:56 strattmans 10.20 120-150 (217) 2020 11-10 200534 strattmans 10.20 120-150 (217) 2020 11-10 10:13:07 strattmans 00 100.27.42 (317) 2020 11-10 10:23.42 strattmans 01 100.27.42 (317) 2020 11-10 10:32.38	8458 08. 05.78 207. 50.845 (0) 8459 08. 05.78 27. 50.845 (0) 8450 08. 05.78 (0. 50.85) 8450 08. 05.7 (0. 50.85) 7 4518 08. 05.70 (0. 50.85) 10.			
· 秋均田原門田市県 120.92.71.200 田行7	area as whom in automa			
Q 2620-11-18 10:40/14				

◆ 选择**攻击溯源可视化**选项卡,页面展示攻击溯源图形化攻击阶段图。





6.1.3 **失陷主机分析**

展示失陷主机被攻击情况,包括失陷主机 IP、MAC 地址、事件数量、最初时间、最后时间等。可快速发现所有失陷主机及相关取证信息。

操作入口

在菜单栏选择"分析>分析>失陷主机分析"进入失陷主机分析页面。

200.810	WACES!	84710-36	al-Color	and a set of the set o
31.01.01.126	10x100+075-15	4	2020.12.11.00.21.58	2020/01/17/14 04:64
ALTO ALT 11	many utility		and to ta teach.	3030-13-(P142330)
10.11.46.14	minutoson (a	¥.	ando-salint-removie	anan-no of excluse
00.11.16.00	10 stealid teel	3.C	2020-12-16 (act:0)	.10030-18-17 12-121-14-
10.20.00.20	Mide/Railwell	8	2020-12-10 10 1426-34	3838-18-17 (20033)
ALL MAILTING	ALL DAMAGE DAMA	4	mus-ul-m custos	10.2m-(1-1) (1.55%)m
30.11.46.75	instranstal	12	2025-12-011548:28	2020 10-10-00/1047
10.22(98.129	04505456a2m0	表:	1020-02-01 (0.47-28)	3030-12-14 (4.5650)
90.11.40.206	6-Restauth-tab m	1	2000 (Q-10 12-15-W)	2020 (2.12)4-0010
101125-10	(20De-Reflacion)	4	2025-12-10-17-ktol9	mm-14-11 (dom-a)
10111-02-01	M10000040pp	1	2020-12-00 19-18-47	anam-18/19 (3:15:00)
28.20.MLM	1044-54201	10 K	2105-12-10 2004 (5	2529-12-1719-Secim
10.11.04,211	10/01 em/(s10/4	1	3000-12-10 28:06-81	20220-18-17 13-90-000
11.20.53.00	Animaterio and Anim	8	AND ALL PROPERTY AND A	2020-16-17 TA-56-4E
11.11.25.44	e. A free-wateries to ba	1	p121.12-11106.06.09	2020-12/17 01/16/01
1010-0018	1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	E	-2010-10 11 08/M-04	2030-1411-0259124

查看失陷主机详细信息

◆ 选择任意一条数据,点击>图标查看失陷主机事件名称和访问次数等信息。



# AMER	MACHEN	100/140136	62/01/01/0	stavenni
- 10.20.41.126	50#168#4/95/13	*	2020-12/11 00.0158	3620-12-17 1456-54
9:0117/01E				
9.M.E.H.	BH1806	Webdite	MMNOR	ML Arriel Sec
10.00.41.126	王明和许	N)	2020-12-11 1856/53	2000-02-11-0705-077
10.25.41.120	DGAI電影響行提的	916	2020-12-11 00:55:10	2000-12-17 5458/54
10.23.41.126	DGA服業構成	241	2020-12-11 00:38:10	2020-12-17 1458643
10.30.41.12E	CBC	41	2020-12-11-00/11/SP	2020-52-17-07.81-55
				8.4.8 1 1 100-11 NO. 1 J

◆ 点击**失陷主机明细**列表中任一条数据 IP 位置可以跳转链接至风险页面查看详情。

	1016	891	- angan	B(*6.0	94/16	HINGP-	molt	82	189.15
	1.8.1	3030-13-11 17(1-07	Randin ((Amarika Bar Bartin))	1020-01 (UK ar	*	10000000	36	REDURNE (14)(4)(4)(4)(4) with the second distribution	- D.
	18	3030-12-11 1630-05	and four sector states	1004 (Inc.)	+	ann an	5	#7045888(0.2012)00 #6482	
	1.0	JUD-12-11 IGNESS	P248 (MINE 49/20 8/2011)	10.00.00	-	Jackson and Sol Soft a Second Party Soft	8	#705888(202)10030(\$P\$86;,	
		3090-12-11 16:56:54		1.000	-	And The Res 100		REPORTED LITTING SPHER, some framerikansk	
	14	.0000-(12-11)	Frank (Merch and All Property)	WARTEN OF	-	8.118.40 http:	QC 1	WTINGER ULLES WEEKL AND DEPART	

◆ 当事件名称为远程控制(威胁情报)类型的风险数据时,点击访问次数列对应的数字可以展示域名列表。

当列表		
序号	域名	次数
1		2
2		1

查询失陷主机

点击页面右上方的 🌾 , 根据风险类型、失陷主机名称、事件名称、时间范围等参数进行查询。

其中,事件名称可以输入部分内容进行模糊查询。

6.1.4 **情报事件分析**

情报事件分析是以事件角度查看失陷主机,将同一类事件合并展示,显示事件名称、失陷主机数,最初时



间、最后时间等。通过查看情报分析,可快速掌握同一风险事件有哪些失陷主机、访问次数以及最早发生 时间和最晚发生时间。

操作入口

在菜单栏选择"分析>分析>情报事件分析"进入情报事件分析页面。

(3) 450APTIC 31502FFF		94	1923	10°	inist.	a contraction of the second	100	.825	****
an (1)									
8 **									
- manual	* ##E200		89,2548		ARCEN			44 CT	
+ extension	1 dkt		-671			9 (% 120)		(000-0)-07 045860	
+ FREIDIN	9.885		19		(R)R (1	T Pyrisat			
+ MARKET	Distriction (107		2020-02-	1.000000		2003-12-17 (10/0000	
· neethor	10.000		18		100.10	e inakle		planting (7 General	
- statistic	0.000		17		7620 (3-	110/057		-C. IT debidor	
· Materia	Distanting		14		anim de	1002010		and or of the second	
· Millionitti	1 T-588		1001		1010-121	18394		00011017144001	
- 34860	1.48				2020-12-	0.164528		2020-0-07 (0-025)	
• KING141	Distant Australia Barra		à		2640-02-	2 million		anne sa ca ca ca ca	
+ ACVALENTIN	CREARING CONTRACT				1828-30	100001		3005-12.1714-4000	
· ADDRESS	1 DOUBLANDE		1.8		jada si-	CHARLES			
L XMMA	1.80		14		2001.01	e leator		design reaction transmission	
CT MINOR	Mitel227-870809		10		1000-02	4 (45257 -		0006-02-14 (#1232	
	CALLER OF THE COMP.		1		10.00-12	11000		anne specialization	
	0-004044		18		2010-12	0.000.0		page-12-18 (10)8425	
	1 8/00/10/2004584		ιũ.		10.00 (2)	111/947		4000-02-1410-0214	
								20.0 · · · · · · ·	ar 10 1

查看情报事件明细

◆ 选择任意一条数据,点击>图标查看失陷主机事件名称和访问次数等信息。

2854	18		2020-02-11 10:10:51	2020-12-17 (7254)
#39-101				
841/10	10.24	10422100	REACHING .	MADERA
DHD+	92.11.33.137	1	2020/12/12 10:49:49	2620 (12) (2) (2) (2) (2)
EBN/C	561131147	1	2020-12-11 1011658	2020-12-14 10:56:56
1000	10111-011-056	41	2010-02-15-0657-00	and the second second second
28404	40.11.00.00	40	2020-12-40103814	2020-12-16 1838016
2mm)+	00(1.05125)	<u>900</u>	JELE-12-17 05/5408	2000-12-17-09554.040
E#wiit	10.13.00.04	15	2039/12/11 11144-07	2000-12-11 17-44-39
1904	10.11.01.139	10	2020-12-12-12-11-11-02	2820-12-13 mmilia
Detrie	45.13.41.239		2020-12-16 11/04/24	2020-12-16 12:04:24
Emole .	1011-655	1	(828-12-14 14/19/95	2020-12-14 1475-05
EBICH .	90.11.07.347		30012-12-15 065a05	2020-12-15 00:54.05

- ◆ 点击**情报事件明细**列表中任一条数据可以跳转链接至风险页面查看详情。
- ◆ 当事件名称为远程控制 (威胁情报) 类型的风险数据时, 点击访问次数列对应的数字会展示域名列表。

域名列表		×
序号	域名	次数
1		5

查询情报事件

点击页面右上方的 ⁷/₆,根据风险类型、事件名称、时间范围查询参数进行查询。事件名称可以输入部分 内容进行模糊查询。

6.1.5 **攻击者视角分析**

攻击者视角分析从多方面展现攻击事件,包括攻击方向、攻击者 IP 数、被攻击者 IP 数和攻击成功事件数 目,便于用户清晰了解网络攻击情况,快速处理风险。

用户可以通过攻击方向、时间范围及攻击者 IP 查找相关攻击事件,快速获悉攻击者 IP、攻击手段、攻击 资源等信息。

攻击者视角分析列表展示当前时间范围内的攻击者事件,包括攻击者 IP、被攻击者数量、风险类型、攻击 方向、攻击次数、攻击状态、发生时间等。

操作入口

在菜单栏选择"**分析>分析>攻击者视角分析**"进入**攻击者视角分析**页面。

安恒信息

#.	- 10								
raente Statute	5	11682 9644	(1) Losses C. Invest (************************************	and passed of	- Hos	3000-6	20010012	ann (1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
		834		1,202			762		
CRAINING		the Coulom						mants and	
person.		110	4(1.5.0mm)	10(11)	84.08	RAND	81.0 To \$ 1000	600719-16-5944	操作指
millionan-	1	10114270	14		101-0.05	+ 927	\$1111-12-17 \aa4\ap	3505-13-11 1441.4P	$ \mathbf{x} =$
CARGINER ADVANCES		0.01.03		THE REAL CONTRACTOR OF	4 -1010	• 9412	3030-12-12 103938	3000-12-17 14:39:39	4.08
28.2% 47.9%	1	18.11.00.12	3		-	• dave.	2018-12-17 14-08-02	3000-12-17 14,99413	
		10.11.44.001	4	anistes.	101		3038-13-17 1438004	3000-13-12 (ik3654)	2.4

- ◆ 点击<导出>导出所有的攻击者 IP, 方便用户进行排查。
- ◆ 在攻击者列表的操作项列下,点击¹¹或列表中被攻击者数量列的数字可以展示该攻击者 IP 详细信息。

P.854	10.10.004	P 10.11.20.12 Magine R	4						×
1940	1981	建农力相	Marit	11.1.28	station .	100303.00F4	#16532:32.00%	WITTE	
10.1142.00	8-2720) 2019 1	114114114114	and the	100 - 100 -	• @bilt	2020-12-17 1438-11	2020-12-17 14-98-03	3	
a prosi in it vestor	Albands y Investigant	101.123.186.40	WIERE	10.00	• #dth	2000-12-07-1439/(T	2020-12-17 14:23:13		
10,11,22,155	900 F28 F F22 F88 F F35 800 F Briedlig F					m.2	•	85 85	i)a
	4451082 8257952 202622 106622								

◆ 继续在指定 IP 的风险详情页面点击¹²¹,跳转到风险页面显示风险详情。

5 200 Mg 10	N I	28	8798.0	8.6.514	Shar	thanks.	4688 BX	(Prints
- 18 - 19	85-12-17. 196-11	The party of the statement	-			62	<i>u</i>	
3103 BP	wae.	BRANK BATTONS 118	- N					
	-10	101217148810000148						
	- 18	NO DEBARI invite BENIN (hep-Columnian)						
	in and	8-30.						
	10.01	a ciliao						
6.00	READ.	and a second sec						
	are.	illar						
	Nite:	1101003						
		00000 500 272 911 00 000 00 000 001 00 000 00 000 007 70 007 000 000	oi contadar					

◆ 点击<处理>或 🗟 处理事件,完成对攻击事件的后续处理。确认处理后,此条攻击者 IP 将不会在界面 显示。

🗸 安恒信息

20.6 B	4612.02.02.02.02.00	网络莱尔	madm match	推动制度的同	BUDDA: LEWIS	1914 G
10.11.42.70	±0			2020-12-17 1441:47	2020-12-17 14441487	4.) R
10.11.01.1105	Ϊ¢.	WEINT	na -n an 🔶 Bata	2020-12-17 14:09:08	2020-12-17 14(19:19	in [3]
10.11.00.1z	8	WINE MOHAN	2 2011	2020-12-17 14:38:33	3020-12-17 14(38-13	8.0

6.1.6 受害者视角分析

受害者视角分析从受害者视角展示内部资产受攻击情况,包括攻击方向、攻击者 IP 数、受害者 IP 数和攻 击成功事件数目,便于用户清晰了解网络攻击情况,快速处理风险。

用户可以通过攻击类型、时间范围及受害者 IP 查找相关事件,快速获悉受害者 IP、受攻击手段、受攻击 资源等信息。受害者视角分析列表展示当前时间范围内的事件,包括受害者 IP、攻击者数量、风险类型、 攻击方向、受攻击次数、受攻击状态、发生时间等。

操作入口

在菜单栏选择"**分析>分析>受害者视角分析**"进入**受害者视角分析**页面。

E oe • Zhenni • stigzon	-	ELAR DECAS	en senera n Co senera s	ersnen vænsta e	(needed 10) (needer 10)	. ANTER	1000-i	5.00 H4 300.01	2003-02.24 14 30.04	
- NELTON - REPORT - REALIZED - REALIZED	-	(1) 2008 971			O 925			6 533		
- REPORT		Inter Streets							PATE A	e - 11
- HECTOR		-	ILLANDS.	NAME		20,000	HAND	BOOM MADE	BURESH	BIT.9
- 85598	1	10.00 101254	X	100		1 101		2020-11-21-14-2988	1010-12-21 942908	2.5
· AD-ADOUTS		214.05.204.8	r.			1 331-12.23 1.1.1.1		2020-13-29 (#2011)	jam (Jay Galata	2.6
3 48.05	-	18111125784	6	wenne		1 80 - 1 18	• 8017	4615.47 (J-D) 14,2146	80-12-21 14/2-46	4.8
		10.140.007.000	36	MR.		1 101.103.005 1.1.1	+ mattr	3000-13-31 (4,8540	303(-12-2) 542500	41.0

- ◆ 点击<导出>导出所有的受害者 IP, 方便用户进行排查。
- ◆ 在受害者列表的操作项列下,点击¹¹或列表中攻击者数量列的数字可以展示该受害者 IP 详细信息。

🔿 安恒信息



世活時	IS-SHIP	3 10.11.36.107 AUGUVIE	9-3 8					
99)	10E	RAR	NAME	8428	ikedGt.	#12/38-11-0944	0008:1094	####
• anno 10 pri 642044 I pros-12 pri 642044	nieros (nieros (nieros (165327732	TINICAL	4 80 ×0.65 1 0 4	• 7.55	2020-12-21 142152	2020-12-21 1421/52	.0
10.11.36.107	August	101/4531298	Inflation I	1 101	e Hh	3030-12-31 142254	2020-12-21 14:22:54	2
Lan ten innis	REEKS (<i>π.</i>	\$ 27	1 SIN - 20
111.229.243.238	Antonia di							
• .000-13-21 H40024 1 .005-13-21 H40024	(6.004)(0.1 10000000) 100000211							
10216633.118								

◆ 继续在指定 IP 的风险详情页面点击¹¹ ,跳转到风险页面显示风险详情。

HAME											
. 29	100	HERE AND									
10	1481	145.327.73.2									
8194	en el	3839-12-21-14	21-52								
81113	214	1929-12-21 M	8.42								
		- 18									
FRENE											
8	1446	-	10	87523	-	Sitcar	textents	man	81	BYTE	
11.6		3030-12-23 14:23-22	Email (Addamated) (1911	Watan Briss	-	105227732	10.1	2	#2014/2018/01/01/01/01/95/95/00/00/00/	-	
			1						A18	1007 40	

◆ 点击<处理>或 臺处理事件,完成对事件的后续处理。确认处理后,此条受害者 IP 将不会在界面显示。

90.11.36.107	i,	(2013)	1 an on an 1 0 1	2020-12-21-14:21-52	2020-12-21 142254	-
111,225,243,238	5	Ameri	1 10 10 10 10 10 10 10 10 10 10 10 10 10 1	3000-12-21-14:20:24	2020-12-21 14:20:24	
192.168.23.119	10	William Towns and	11 10.10.10. • Bighter. 1.1.1	3020-12-21 14:19:31	2020-12-21 14(23)23	10.00

6.1.7 脆弱性分析

脆弱性分析统计**弱口令、密码明文传输**类型风险受到影响的主机、账号信息,展示弱口令 TOP20、受影响 内部资产 TOP10,便于用户清晰了解自身密码相关的风险信息,快速处理风险

操作入口

在菜单栏选择"分析>分析>脆弱性分析"进入脆弱性分析页面。

- 186	HD + Batter Avtre							
Kanne	BALL OF COMMENTS OF				1000 No. 10 10 10		010.12.21.12.21.16	
	The second second second	Part /						
WEIGHT	Bran an an annual annual an	6.7		BOXD 1995				
NUMBER	Biren			2702 111				
the second second								
STREAM								
and the second s	O REAR INC. O RATER	A Maritian or						
Million .								
without 1	3 801370#28			3 SEARCH R.º 10 P14				
REAR	2			10.00100111				118
11 (mm) - #					1.0			44
		24.516		101.108.07.73				- 11
								12
silvening.		mState		1030442				
40-82118 30106 -		La Star		102104.00				. 7
4048233 3096 - 18876 -		Na star		1000642				2
alenten - Intera		T BASS		1000420 00 1021643020 00 1021643020 00 102048202010				2 4 4 4
alemente Series - Marent -		Up%er-		100040 102164,054 102164,054 102164,057 102164,057 102164,068				7 4 4 5
AD-RETER XHOA - HERME -	Dr. Autom	UB*		199944 192164-04 192168-04 192168-04 19216 19216-04 19210			average and	
AD-MICE - MILINE -	DE JUNER RANKE RUNIES	MREE ME	MD 6 Main	HERE	1983	#15.10H	anense nas Referenti	

- ◆ 点击<**导出**>导出主机信息,方便用户进行排查
- ◆ 在弱口令列表的操作项列下,点击 IP 下弱口令的详细信息。

Minour-	New	510.24156.102.002	traint and					14
98	- BRICH	drike/*	9011	designation.	NOTICE	#16323.00FF	Arr.u	
10.000000000		possi	1	· Storiet	2020-02-24 4348022	3000-(2-2) (Lab.0)		
•		Kiata	1.0	+ match	2005-12-25 1225-07	0028-12-21 12:3740		
1 000-43-31 440000						HIR I	and the	1.1
88.303.200								
part of a transit								
(62)(64:22.27								
and the property of								
10.20157.199								
- 2020-01.21 (Monthle 2020-01.21 (1920-01								
18.00196-182								
and the second second								

◆ 继续在指定 IP 的风险详情页面点击 📄 , 跳转到风险页面显示风险详情。

) Mante										
.01	Cart I	4,4110101								
27	-	paid -								
	100	mit 144114	66.01							
4010	NH .	-	akitu							
		110								
108na										
		**		214.0	-	-	-	nni	87	19716

6.1.8 流量统计

流量统计页面展示统计时间内 APT 采集的网络流量,并且实时更新,方便用户了解统计时间内 APT 流量

杭州安恒信息技术股份有限公司

🗸 安恒信息



采集情况。

操作入口

在菜单栏选择"**分析>分析>流量统计**"进入**流量统计**页面。

nangaran na n				•	
	O-AFTRANSPOR	COLUMN CO- NUMBER OF STREET			
150 kgis					
Cill for			/		
Million .					
00 tyli		~	/		
20 mm		$ \land $		1	
0.0				1	_

点击**流量统计折线图**右上方的时间按钮可以选择统计时间段;数据中心可以查看探测器的流量曲线,左上 方下拉框可以选择需要展示的探测器流量曲线。

6.1.9 **登录行为分析**

登录行为分析用于业务口流量的登录行为进行统计分析。当基本配置中的登录行为分析开关打开,此模块

才会显示,具体配置见<u>功能配置开关</u>。

操作入口

在菜单栏选择"**分析>分析>登录行为分析**"进入**登录行为分析**页面。

#					5
B-Rest	think the	89.*	History.*	8482	#0384
1025-12-17 1440-11	441	15.35.40.47	173/16.2.199	HTTP	200
2020-02-17 Shidon	44	10204130	172.16.2.196	wittp:	20
2020-12-17 1440-11	#210	10.11.23.47	10027548-505.02	HITE	2005
2820-12-17 14Ab11	kintigation mena	10.20.44.131	120.00136.04	HTTP.	300
2020-02-17 Samon	821	10.004.539	10.20.100.100	SITTE	200
2020-12-17.5440.00	6102312	10.11.42.20	18.216 St7-214	10110	200
2020-12-17 1440-00	6476-01	ana cart	10,504.07	HITP	220
2020-12-17 5440:00	autor-opport-2020-11-01	1811.86.208	16.8152.21	wittp:	20
2020-02-07 14462/0	я.	10.00.40.10	OTENTIA	i-ettal	200
2820-12-17 1448-0	4244	10.11.20.39	192166.36.82	HTTP.	100
3020-03-07 5840039	1706	10.10.40.06	171116-0123	siTTR-	200
2020-12-17.1448200	90.5	10.20.40.00	178,16.2.124	HALLS.	200
2020-12-17 1440-01	10 C	10-03-41-193	173/16.0.124	HITP	270
2020-12-17 1648-pv	40100	18.11.8639	192,168,38.42	WITE	82
2020-12-17 (Headual)	#210	10.11.20.54	1822108-30273	ierra.	200
2525-12-17 14-80-09	4240	12.11.25.04	192166.3671	107770-	200

◆ 登录行为分析支持的协议类型如下所示。

Telnet、FTP、Radmin、SMB、IMAP、POP、HTTP、Oracle、Mssql、Sybase、MySQL、DB2、PostgreSQL、LDAP、QQ 等。

- ◆ 不支持加密数据库。
- ◆ HTTP、SMTP、IMAP、POP3 这 4 种加密协议默认不解析。(如果需要审计,请先在 SSL 配置里上传对应的证书,具体操作请参考 <u>SSL 流量检测</u>)。

◆ 查看登录行为详细信息

B

选择登录行为分析列表中的任意一条数据,点击>图标展示登录行为的详细信息,包括基本信息、客 户端信息以及服务端信息,如下图所示。

= sustant		教堂地中有	12:0210	E540	8903.000	3425905
~ 2020-12.17	14:40.11	443			HTTP	200
2+00	seate Esate					
10.0	2012171440110034061					
\$15.45B	3025-12-17 144011					
2250-2	-44)					
0.0452	HITP					
809	- 300					
Runa						
URL	PDST / satisficijar po physio	internation ope				
NADE	CONTRACTOR OF THE OWNER	and the second				

◆ 查询登录行为信息

点击页面右上方的 证 , 根据登录 IP、协议类型、时间范围排查用户登录行为。

安恒信息



6.1.10 **抓包分析**

抓包是对业务口产生的流量进行抓包。

操作入口

在菜单栏选择"分析>分析>抓包分析"进入抓包分析页面。

点击<新增>,可以根据客户需求进行流量抓包。

新增抓包分析参数设置主要包括:协议类型、抓包时长、文件大小、IP1、IP1 端口、IP2、IP2 端口等。

当抓包时长和文件大小其中任意一项满足抓包分析参数设置,都会结束抓包。

16以用型:	8 20 O TCP	UD#	
· MANDARE:	10	8#	
(安保大小):	20		м
wi:	100.5		
HP108C1:	1998.0.0		
iP2:	1865		
H2mCl:	1998.1.8-1001		

在抓包过程中,点击对应的抓包分析项目操作列的 回 手动停止抓包。

抓包结束后,在界面上会显示文件名称、文件大小、状态、任务开始时间、任务结束时间、协议类型、IP1、 IP1 端口、IP2、IP2 端口、操作项(重新抓包、删除)。

点击已经抓取数据包的**文件名称**可以下载数据包;点击操作项 ³³ 按钮可以重新抓包;点击操作项 🗍 按 钮删除已抓到的数据包。

0.00											
2/F8#	立件术中	80,0	11875 March	(PANADIA	ncett	181	1913403	192	1925823	tirt	
nin statini j_	131.16	mand	2030-12-14 14/02/29	2020-12-14 170230	10F38P	10.11.37.37	122		- 22	U.	Ξ.
82801.82911011K.)_	21.56	stand.	2020-12-0111-01-08	2020-12-03 1102545	105.00	10.11.36.208		115,238,37,18	10	- 10	
maninia(5520).j_	1.28	राज्यत्वाचे.	2229-10-18 (5252-0)	2020-10-14 15:52:21	TOPUER	12.11.42.50		23	33	19	5
Manmathaney.	240	Rest.	2530-10-14 15:45:22	2020-10-14 1549(99	TOPUOP	1026,4230		0	1		E
RUMITAL SALES	200.094	manuel	2020-10-14 15-46-29	2020-10-14 15-86-50	10PsiDP			5		9	=
	1.96	mana	2020-10-1815-9841	2020-10-14 15:07:08	TCP/UDP	10.20.90,122		5		- 0	1
	117.0	Start.	2020-05-09 15:24:30	2020-09-09 19:3432	TOPUOP		65.505			.0	π

6.1.11 PCAP 文件上传

上传 PCAP 格式文件,系统会对该文件进行回放,如果含有风险事件,系统检测完成会产生相应的告警信

息,可在**风险**页面搜索查看。

操作入口

在菜单栏选择"分析>分析>PCAP 文件上传"进入 PCAP 文件上传页面。

支持本地 PCAP 包上传分析,点击<**文件上传**>,选择本地文件上传,即可对上传的 PCAP 转包文件检测并 且给出检测结果。

		and the second se				
E ##		29.20				
> ###555F		20PI而H	T-MONINE	#FileActivities	AZ MY A PROPERTY	4200M/B
- ±54800#		untrad-pet/21Lanaang	3020-03-03-00-30012	2008-13-11 dicks.10	3028-12-11 063014	Long
- season		animi-peri212praying	anas-ra-re imaeun	2020-12-0100a1010	2028-12-11 Institut	1,014
- 1009/001		sampler-ap-2000002115 00:41x4601ce9800 a/b04acf01064a7b5ccas	3020-09-22 15:44:58	2020-09-22 15-45:01	2020-98-02 15-95-03	1000
 33#SRIP; 		falled memory in the Datase	3020 49-21 141923	2020-09-21 1459-28	2020-09-21 1419-25	sited.
- BRADRON		2009141304050000045zcar	2525-89-14-13/21/29	2020-05-14 13:31-01	2525-05-14-13/01/21	unut
- MALLANS		200509111339800040.pc.ep	2520.45-01142447	200-05-01-40400	7520.45-09 142464	sind
- 158001		0000827104735_p1_003040134.map	8005-09-04 15-49-01	2030-05-04 1546-04	8000-09-04-16-49-04	onel
- 01000	1	delite grap	3020-86-13-1605-34	2020-08-13 1920-40	Joon da 13 Jaiotan	une .
		artes2,flamorealizing	ason de páris an le	2020-08-84 1942-40	anon on the institut	1992
		al attack reaction to	3039 47 31 15 23 48	2020-07-21 15-22-00	38.85-97-31 15-2346	19962
🖯 xmmi	242	superapl.	3030-87-31 (0.110)	2020-07-23 (0.1108	30385-825-321 (00.3) (200	1993

点击<选择文件>,上传文件进行检测。如下图所示。

🕜 安恒信息



6.1.12 **威胁情报检索**

威胁情报检索提供域名、IP 地址、SHA256 值向云端查询展示相关的威胁情报,用户需在"系统**>升级管** 理**>云端配置**"配置好云端信息,方可查询。

操作入口

在菜单栏选择"**分析>分析>威胁情报检索**"进入**威胁情报检索**页面。

1.4						
2 18			- the company of the second			
-			BIRD International	1) <u>(************************************</u>	internet.	
- amazone		7 MER: tau nanjingchwesi core				
- 168254141 - 18826441049		2016-07-16.1406-25	10040 10040	2005-00-10 15.63-40		
- 228/04/11		ACTING CARGES (1944) (19	ursa.			
- 318111000		> Fitterhoutett				
- 20.00	- 7	Fettal	100000	11294	1286.4	11-stians
· PEAPERLIN		3016-01-11.11/044	282(-0)(-0.103540)	Mining Cost Computing (Helping) (co. 181		
						ala 18 18 18 18 18
aune 🗧						
II 166/165	1	5-Asstations				
		17.636	A126	454		without .
		maceir.mine	unte de 18.8080.000	ani ani ani		10.119.54
		(status))	2015/05-19 904040	#(#E)*		-B-UMP mm
		1.198.219.10	10118-01-10-00-00400	A1407		NEARLA STR
						A18 - 🚺 - 24.0 - 80 - 3

风险详情页面,含有 IP 地址、域名、SHA256 值的地方点击搜索按钮,查看云端情报。

杭州安恒信息技术股份有限公司

🕜 安恒信息



		166683±9 🖸	
: 10'			×
成的等级	**		
威胁使型	WhiteList		
注意	29.868387		
经度	121.54979		
地理位置	中国-浙江县-杭州		
ASN	A54837		
MACIESE	00.0c2%1		
服务端伍印			
	\$619,73		

6.2 文件分析

6.2.1 **文件威胁分析**

文件威胁分析展示当前所有恶意文件信息,包括文件 MD5、威胁指数、传播次数、病毒检测、静态检测、 动态检测等信息。

操作入口

在菜单栏选择"分析>文件分析>文件威胁分析"进入文件威胁分析页面。

R41MD5	wEM-HUM	4410835388	纳马拉洲	种态和效率	WHERE WE
0xe624b1cr10x1178ccc54x078008 b2c)0xe624b1cc18x1578ccc64x07 6908b2c5.pdf	mann	1	Explicit.7LPdfkaarer	¥	<i>9</i> .
fcBee45507%30006c87700404c1 c[tcBee45507%30006c877004064c lcdbe]	III OULO	54.	Exploit MSExcel Agent ad	8	<i>x</i>
0daade94857/d2766177407Nc058 4tts[74.nat]	-	ă.	Trojas-Downloader/Win12.CodecPack.oz	±:	

查看文件威胁详细信息



点击某个文件样本信息,或点击左侧>图标,进一步展现该文件的详细信息:

◆ 受感染主机: 展示所有接收该文件的主机 IP。 若该 IP 是接收邮箱所对应的,则括号内显示接收邮箱。

点击传播次数列下数字查看该文件所感染其他主机的风险详情。

1	医感染主机 威胁情报 可视化分	析 沙嶺狼青			
100	E机P				
1	92.168.30.73				
	79cb65f7cd32d9f805238c1d6b8f13 ff [5.pif]		2	邮件附件为高危后缀文件	÷
3	412848b792d2207139996f857f2b2 516 [3.com]		2	邮件附件为高限后疆文件	3
5	4d52c9f2019fca4a43e5fcc6373402 31 [1.cpl]		2	邮件附件为高危后缀文件	÷
	fc8ee45507fe3f808cdf720bf0fc4c1 c [fc8ee45507fe3f808cdf720bf0fc4c1 c.doc]		4	Exploit.MSExcel.Agent.ad	ŝ.

◆ 威胁情报:显示文件 MD5、文件名称、沙箱报告、云端确认、威胁指数、传播协议(HTTP、SMTP)、
 传播次数、病毒检测、静态检测、动态检测等内容。



受感染主机	威胁情报 可视化分析 炒着报告
文件MD5	0daade94857fd276b177407f4c05f4fb
文件名称	[7s.rad] 下版
沙積报告	0daade94857fd276b177407f4c05f4fb.html 下数
云磷磷认	已确认
成的描述	******
传播协议	[FTP]
传播次数	25
肉毒检测	Trojan-Downloader.Win32.CodecPack.azwg
静态检察	
动你检测	適历系统中的进程 从资源或释放文件并运行 加载资源到内存 写入自启动注册表增加自启动1 梯改测完器代理 创建网络教授李连接 使用Get方式增发数据 使用Post方式增送数据

◆ 可视化分析:沙箱报告中的动态运行图。

					start
					[PID_1316]2243.ex
	Service	Malicious	Malicious	Malicious	Malicion Malicion

◆ 沙箱报告:威胁文件的沙箱报告。

安全评	* • • • • • • • • • • • • • • • • • • •		
\sim			
基本信息		##CR	•
B AGR		₩+@ <u>₩</u> ₩059	1
基本位度 文法条件	2343	8400 8039 61454	• • •
藤本位泉 文州名称 文成大小	1043. ese 1430 - (14704/berea)	8400 8039 61454 61454	



6.2.2 回连域名/IP

回连域名/IP 取自【沙箱报告—软件环境—尝试与 N 个域名/IP 通信】部分。目的是将恶意文件回连的域名和 IP 列表展示,并提供加入威胁情报功能。便于用户检测访问该部分域名/IP 的行为。

946				14. ÷	1845/5
18	WATER RESIDE	NURSENWAMOS	10.5 mill (\$10	IP TTU	83
n.altyyatuure	2020-12-22 09:06-11	5+421+90001512909152+645c52455447	CB		(100).
tal/solution	2020-12-22.00558.08	3486.7979076445454541447564754	0.0	40	8/12/00/0
wing fastion over	1020-12-32 (0058-28	3486-709925666-65843526754	CB	0.14	And the second
luppern Lilon :	2020-12-21 12:13:47	249(006)(1483)(006)(469)(01138)118	(CB)	11/11	#1/256(15+141/h
Auto Ofganalizer	2020-12-19.11:50:28	au166a01002a01002a000364629991(912	0	3.9	460.
wingingare.com	2020-12-19 12:50-26	au3 6448 http://20220885962399919912		2.0	8242,68988
iniuram	8020-12-18 (0208-51	Stablebook Scholastica: Weall2216	- CB -	4.0	
ww.jedue	30203-12-17 10(Mode	diersaliste Norte Houtenabilitet		10.00	adapt.
and gloch	2020-12-17 10:58:41	Www.Satistike?4c?1x3touter40x85x8	1	10	Land Land
unertanglissagi inn	3020-12-16 YOME/H	Average Average and a second s	0.00	a cite	81 88
pineloghestuis	2020-12-16 08688.33	de05c5404ecx(a0x121020104a2073)	0.00	a:0	
ortani-iom	2020-12-16-09/28.08	417a):845733xNaaah)64;37aV928	100		
will 167bit port	2020-12-19-0922299	417a2-545713s5aaa6254c7340903	00	011,17	
trado officient	2020-12-10-05/22:08	417a2c846713c0eaeeE364c7740903	CB	01.07	
www.izzztwahew.com	2020-12-16/01-62/27	148W11539140044560513575396462		- 9	

相关操作

- 加入威胁情报功能启用时,该域名/IP 加入威胁情报库;按钮禁用时,根据该域名/IP 不加入威胁情报,
 匹配的告警不生效。
- ◆ 点击操作栏中的 🖹 <查看>按钮, 跳转风险页面、展示产生该域名的恶意文件告警。
- ◆ 点击
 ◆ 点击
 < <不再关注>按钮,该域名归类为不再关注,列表中默认不展示;但启用的威胁情报生效,即
 修改域名/IP 是否关注并不影响该域名/IP 的启用/禁用状态。
- ◆ 点击 [™] < **筛选**>按钮,弹出筛选页面,搜索不关注的数据,可以点击 [№] < **重新关注**>按钮,该域名 归类为关注,列表中默认展示。
- ◆ 沙箱报告中新产生回连域名/IP 时,数据更新到列表中,默认关注,威胁情报默认不启用。

6.2.3 文件审计

文件审计显示当前被系统审计的所有文件列表。



操作入口

在菜单栏选择 "分析>文件分析>文件审计"进入文件审计页面。

		No. astrict	10111-0								
🔄 तमः		1.0	Passage	12000	10000	-2.502 N	152003	100000	1.200	Sector 1	ALC: NOT
- controlation	1	Ener Teratation	TIMES	200-0-0104897	inforts.	Withan 128	162.166.36.76	-019	NEX Development of Terreptor all regions	Rint131	in in
· Harris		*** (MESSAE) ; *	6	3999-12-17 14(8)(27)		seasonad.	+0.20110.25	111	POST (netchonstables otherwhite	9952	003
· TRIB		spin folia an	(Au))	anan ol 17 tamati	71	10.11,18.09	. 11120210100	90796	POST /variability/chail 11 gaty-withtime down't c-downer-Id8/eP/06.337 40 Revenue-T820-Encoder c-d8/Relet-1020-encoder c-d8/Relet-1020-encoder captor_Strosp 20 down-107 c-24/21/21/41 (2010) 134 15723564/2011	ubw#es	
		99,910		900-17-17 1405d7	*1	9111.0.00	11120210046	stra	PDNT nummarphiphot siggs veintime generi c desice information 50,07 400metri 1000000000000000 e000000000000000000000	sheres	×.
							19 ja 19		PGNT /varmadipmathol + tapy-settement generit 5-benine-tdby-1001.17 PROVEMENT (8-re-	are	

相关操作

- ◆ 点击 [™] 通过检测结果、文件类型、时间范围等过滤出符合相应检测结果的文件信息。
- ◆ 当用户确认某个文件或某些文件是绝对安全的,并且这些文件状态尚未检测处理,可以勾选文件,点击<
 批量不检测>进行手动处理。
- ◆ 手动处理过的文件系统会提示检测结束安全,点击操作项列的 📄 可以查看被审计文件详细信息。
- ◆ 检测结果确认安全的文件默认不保存沙箱报告。

6.2.4 **文件上传**

对上传文件进行检测。目前检测方法有三种:病毒木马扫描、静态分析、动态模拟分析。

😡 文件上传检测优先级高于文件审计检测。

操作入口

在菜单栏选择"分析>文件分析>文件上传"进入文件上传页面。

		2.0	10 D± 1	- 31110								
E-FE-Hell			anns.	*****	sinc.	ALCONTON.	-	1816	MOVE:	Lehensel	SERVICIONESI.	100.00
The second			A HORIZON	Anc.	1945	2.0	24	100	attiannilionetietet elaizoinit	2120-12-17 (119735)	200-12-17 (34130)	-
COMPANY.	_		(and the second second	100.1	1010	44	24	566	The OPENNEL OF THE PPIN AT A STATE OF T	2020-02-17 13:00:00	2020-12/07 13:38:16	(+)(#)
-			Saturty GALate	1997)	1045	Palacithillinger	+	39	HEEVISENAAMAANAANAA BARTAAN	2020-12-171831116	2085-92-07 1321-88	
				-	0.055	*1		-10	#####056##\$12#1#Z78##82 ##%26##117	4400 (2-1) (94 (14)	200-0-1063641	- 0
			(Lpin)	***	nitest		42	- 101	(Actual production provident) Rectific Table	2000-12-04 10:54:21	2020-12-04 (10:04:05	(8)
	1		rConsiOyNg		1815	HELR:Toje (Wirld)Ge Helt	+		66216491016668006680 367926475	2020-12-02110.52:54	2020-10-82 19:55/10	- 0
			Received and the	-	1.815	Topo-Famonathela Troodie gre	+	- 10	ATAINING ISBN 774786413. 711000aadat	200-12-81 (±1468)	2025-12-41 (1116-21	- 6
			10000	34471	1.015	Failed MilliDisgar	+	10	matemachterentisien soeimietste	2020-14-81 18:38-26	200-241 (140)	0.00
						WFRIGTS RC20+3084037 BR20+508-1-647 Million Mi						

◆ 点击<**文件上传**>,上传文件进行检测。如下图所示。

文件上传			
 上传文件不能大子 上传过程中。像不 可直接上标emi文 	200M,不完算 基础的支援。 中主机的副作用	·土壤OKB起文件 ·谢谢特。	
* 检测环路: 🛃	而南本马扫描	田本分析 日本分析 日本分析 日本分析 日本分析 日本分析 日本分析 日本分析 日本分析 日本分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析 日本の分析	3 动态情况分析
"动态模拟分析时间:	25	to to	
*文件:	上传文件】	师文件史	
	報調	West -	

 ◆ 当文件检测以动态模拟分析方式进行时,如果文件被检测出存在可疑的攻击行为,就会生成报告。点 击该文件操作项列下的 [◎] 按钮预览检测报告,点击 [□] 按钮下载检测报告。报告截图如下所示:

🕜 安恒信息



BEOM
85 PM
QAPT
被制力
交易行为
#0FN
2.45P

◆ 相关操作

在**文件上传**页面点击<**导出**>导出设定时间范围的上传文件结果,点击<**报告下载**>下载设定时间范围的检测报告。

6.3 域名分析

6.3.1 受感染主机

通过 DNS 流量检测 DGA 域名请求功能,自动识别流量中的 DGA 域名请求,从中发现受感染主机,确认

僵尸主机受感染的病毒木马类型。

操作入口

在菜单栏选择"**分析>域名分析>受感染主机**"进入**受感染主机**页面。

受感染主机菜单将捕获到的受感染主机 IP、MAC 地址、受感染的病毒木马类型以及触发时间等直观展现

出来。如下图所示。

_				
				Ė
× 2	52			同
1	DAS-S	eouri	ty er	0.0

	- 8					
益 nw		With				76.1
वित्रसम्बद्ध	1.0	* \$WE215	MACHIN	ANIA PETE	DGARIN	\$100 Million # \$104
EI 48791		102041126	Schule Bank (MILT)	25475iai	pplane, el condition is	10120-12-17 Vilaguag
-		10.20.4.97	aktitettiitteettee	198000		1510-12-19 ph/08-41
COCENSE.		10,11,28,100	16/1014433.dxd2	70905.5		20100-12-10/11/10-AU
- 20101-01		10.0.34(10)	8cm209013000	yeads		3000-12-16 VE10X0
		102.03.#AL195	pictitional facility	200		2020-0-111021210
		(0.11.41.34	an Gradomontal v	204		2410-13-17 10-18-81
		1.00128289	1248/9/9/00/01	31		2010-12-17.29(09-41
	- 2	10112348	8-21-30-w1/16-12	21		2020.12-13 1040.41
		1 M0.11.12.58	eeds/deHitTs7	22		2020-12-13 1802951

查看受感染主机详细信息

在受感染主机列表左侧, 点击 > 图标查看受感染主机详细信息。

选择受感染主机明细页签, 查看受感染主机 IP、佐证、DGA 家族、病毒类型及触发时间等。如下图所示:

~ 1811,23.49	8x285/981a4x76x82	23		2020-12-15 16:40:45
0.99524709	BACHINE			
18	61Z	DEARS	82.12	MIREDUK
15.11.23.49	1015年121020-13-151610-12型2020-13-151616-1381 GA(統領導所	No. 2007 10:00		2020-12-15 1604043
10.11.23.49	100年後10000-12-15-1429-11国20000-12-15-1429-1193 0.44時期週期	95, 267 1) 20		2020-12-15 1459048
				A28 0 1 0 160 80 1 2

选择回连 C&C 域名页签查看回连 C&C 域名详细信息。

···· 10.11.23.49	8c4590ai;7kd2		23		2020-12-15 16-0340
#SNT NAE	Enclosed B				
MR	MEMOCCIP	COPREM	DNSBILIPM	INFINE	MELETER
7nalpg.m	118.28.141.13	#3	Bilit paget-beine mizhaerba.com, TL,	2020-12-15 1645/14	2020-12-15 16/45/14
References 1	119128-141-10	-	BBarget-bella.etchaeba.com 71	2020-12-13.145623	2020-12-15 145623
=29/411000	1254.181.234	RIN .	劉英 aupited.numebright.com, TTLED.,	2020-12-15 1455;12	2020-12-15 14:55:12
					R18 (1 180 86 1 R

6.3.2 C&C 服务器

C&C 服务器指的是远程命令和控制服务器。目标机器可以接收来自服务器的命令,从而达到服务器控制目标机器的目的。该方法常用于病毒木马控制被感染的机器。

APT 通过 DNS 流量检测 DGA 域名请求功能,发现受感染主机后,并进一步通过 DGA 域名请求中成功解 析的 C&C 服务器的 IP 地址,结合 bot 受感染的病毒木马类型,最终确认被同一 C&C 服务器受控的僵尸



网络 (botnet)。

操作入口

在菜单栏选择"分析>域名分析>C&C 服务器"进入 C&C 服务器页面。

C&C 服务器菜单用来管理捕获的 C&C 服务器,并将 C&C 服务器 IP、感染 IP 数等展示出来。如下图所

示。

Camilia .	4 Chrankall	autorhei	STATE OF	69-52-58
-California	1 A0130-19338		24	
(dente)	15,184,812200	1	14	*0
and a second	 Istratacov 	i i		74
and the second se	544,201,185,175	()	4	**
there is a	1942/01/86.07	i i	u.	**
ANDE -	1542/0.180.198	<u>0</u>	4	
1000	1 IS#201100374	1	1	
	1542/0710.112	40	1	88
4204 -	1542/0.190.055	a di seconda	1	**
ine and	154200.000.048	1.	1	**
A CRIME	154,200,108,108	4.1	8	

点击<导出>将 C&C 服务器信息汇总导出,点击感染 IP 数对应的数字和域名数对应的数字可分别查看 IP 或域名详细数据。

查看 C&C 服务器详细信息

在 C&C 服务器列表左侧,点击 > 图标查看 C&C 服务器 IP 所对应的受感染主机 IP、MAC 地址、C&C 域 名、C&C 服务器 IP、佐证、访问时间、触发时间等信息。如下图所示。



CACERBILIP		164098		Mashelat	用在他	
154,94,304,111				1	8.4	
名称主动主的时间						
Silia 1 M	MACRIA	CACIER	CACEMBIP	64	(GRIMA)	autorise
0.30.41.126	Stanistad 95.75	Thyyytt cam.	11434-104113	第9年3031-12-11 04.1130至303 0-12-11 04.1330回時月、加加了1 2 00564編記編第	3630-13-11 0450.10	2026-12-13 84-5110
0.20.41.126	50amilia495/35	system	17454.104.113	00002000-12-11 84.0002002 0-12-11 04332005800, 9927 1 2-10064822066	2020-12-11 Dealers1	2020-12-11-04-63/10
0.20.41.126	58x658xa4.85x35	1279303.0000	154,54,154,113	WFRE2020-12-11:04:1453(型202 0-12-11:04:1453(型型用: 別紙ア) 4:10日GAM名音楽	2020 12-11 0438-33	2020.12-11:0438:52
0.20.41.125	Statistical IN-IN	fass/166.com	15434:104.111	00702000-12-11-0416350200 0-12-11-0416030878878790071 0.00004080888	2020-12-11-0x3638	2020-12-11 04-42/10
						108/7 818 1

6.3.3 **高频访问同一域名**

高频访问同一域名菜单用于管理被捕获和检测到的同一域名频繁被访问信息。

操作入口

在菜单栏选择"**分析>域名分析>高频访问同一域名**"进入**高频访问同一域名**页面。

- Maria			5 (o
E 168	204629-0192	MULTINE.	Allow An COL BY A
20peig.com	2	5250	3020-12-17 1105-48
nullirfian (1	2770	.8122-12-10.19:39-43
7 separations	2	2337	2020-12-17 10:00:63
			N.I.B. C 1 22805 102 1.2

查看高频访问域名详细信息

在域名列表左侧, 点击 > 图标查看 IP 在某个时间段内访问该域名以及子域名的明细, 从而确认其威胁程

度。

点击蓝色域名查看详细的域名及其子域名列表。如下图所示。



5 MB	10.0012/6-10-02	()()()()()()()()()()()()()()()()()()()	MI ## ## ## ## ## ## ## ## ## ## ## ## ##
angeogram .	2	5257	1000-13-17 1100-49
Rater H-MARIN			
	MACHIN	6ii	NUMBER OF BRIDE
10.11.18.35	ad 83 a / 4d at 0 (a	第19日2025-12-16 1941427至2025-12-16 1942-46999月 19月27-05 12月 17 pvg2xvx:電波構成	2520-12-56 19:45:48
10.11.35.19)		第四世2000-(3-17 11/041号型2000-(3-17 11/047号号の人) 当然(2574000) 22 goog com 地名美国	2020-12-57 110540
			228 2 10 1 100 M 1 1

城名刘贵		×
188		
	vg.com	
	g.com	
	g.com	
	vvg.com	
	121gvvg.com	
	gwg.tom	
	g.com	
	wg.com	
	a.com	
	twd.com	
	1125	#12 1 W



7. 风险

7.1 查询和处理风险

该功能用于查询特定风险类型告警,例如,通过勾选某一风险类别或其他一些附加条件(如:事件类型、风 险类别、攻击状态等)来查询相关风险告警。其中风险级别、事件类型、风险类别等可多选。

操作入口

在菜单栏选择"风险"进入风险查询页面。

默认查询条件展示风险级别、数据类型、事件类型、风险类别、攻击状态、处理状态、时间范围等。

默认时间范围可以通过"配置>常规配置>基本配置"菜单的风险查询参数部分的查询缺省时间范围设定。

点击<重置>将查询条件重置成默认查询条件。查询界面如下。

F 意识做/特				9 2 -
Reisting	48 X 9 5			
1.8.8.7.2	Rechman Water			
#H352	es name ware stars			
80.53	22 C			
12562	ure and and and			
北部代志	· · · · · · · · · · · · · · · · · · ·			
100728	2021-08-10 08:28 08 - 2321-05-17 10:01 13			
87,000	E Production most E Production most	12,010	10.51	
E-Hill	1000 - 28 Watel 100	40.0253		
(82	And an and the second			

查询结果

原始数据为单条风险记录;聚合数据将 30 分钟内相同源 IP、目的 IP 和相同规则的 Web 攻击风险、自定义 特征检测风险、挖矿等风险的原始数据集合为一条。其它类别的风险也可通过聚合数据查询,但实际查询 结果与原始数据相同。



风险类别选择<全选>,点击<查询>,列表默认展示风险等级、发生时间、风险名称、客户端 IP、攻击方向、 服务端 IP、响应码、报文等。

点击右上角^(②) 图标可以对列表进行隐藏或显示,刷新页面后展示默认列。查询结果界面如下。

	u =1 u	10010	ABJETH EM						
	10110	104		87907	**//1	Since .	. ++++	61	WTHE.
		3836-13116 1709/03	Distributi (Milling) wasa Distributi (Milling (Malani ang ang a	16.8.81.01.0		manutria	30	HOD Vega (17) (4.3) (Styles (18) - and over 10 12 (10) (10) (10) (10) (10) (10) (10) (10)	
	48	1100-11-16 1700-11	Entry (Distant States)	10113880	+	Manual Manual	9	REPORTED IN CONTRACTOR OF THE ADDRESS OF	4
	18	2025-12-18 1758-18	HERRICH SHEDRIGHT)	General L		THE RECEIPTION	э.	Realization of Realization of Section 10	
	18	(1125)-12-18 (1100015	Annual parameter per et and \$2 - galance	10.000.00	-	an marca	4		0
	1.8	2008-Cirk Treees	A DESCRIPTION OF A	0.0600.000			9		2
	18.	anie-sana. Tranes	Arrest parently year provide and the	TET: BOD at	-	winner			=
	1.8	100/00-12-18 17:07:58	waan janun (400 min aana	101134.002	-	00100000	14		
		2025-12-19 17(2549	angeline) (webba) musanifikasi ne inc	1611212-Day		-	-	WWW INTERACTION AND A CONTRACTOR	
	18	1008-02-08	And the local distance of the local distance of the	TRACE IN CO.			÷4		2

导出风险

点击<导出>,可以以 EXCEL 格式导出查询结果中的所有风险,包括时间、风险名称、IP、报文等信息。

处理风险

在风险列表中勾选多条记录,点击<处理>,可对风险进行批量处理。处理操作包括修改风险状态(处理中、

处理完成、延迟处理、拒绝处理和其他)及添加描述,如下图所示。

处理		
状态	请选择	
描述	处理中	
	处理完成	li
	延迟处理	
	拒绝处理	
	其他	

风险关联信息查询

在风险查询结果界面,点击"客户端IP"或"服务端IP"进行风险关联信息查询。例如点击"客户端IP",



指定客户端 IP、服务器端 IP、风险类别及时间范围等过滤条件,查询出指定 IP 在选择的时间范围产生的 攻击,如下图所示。

风险关联	言息查询	
茶户菜中	10.20.12.42	
服务端P	203.119.169.241	
风险类别		
预档来通	IDS/MAS	
时间范围	事前事后1小时	

查看风险详细信息

在风险列表区域左侧,点击>图标查看风险详细信息,包括基本信息、客户端信息、服务端信息、关联信

息、处理等,并可对该风险进行处理。

2-#WRIE							- 18
98	re szorre se						
8. C	68	BUTSUP	REAN	direase -	1968	#8	HENK
	(2) a manager (second over manager man and one of	10.000 a	-	ITA YA JIYA JIYA	300	PQDT mpp/173.11.20.114/second BET Law/yeer/BETBETBETPR/Society.com monocols indicates for the society particle of plagins, and place and particle of the society of the soc	
8145 B ⁻ 955	Route materies onlight lot						
**	pht/10/18030014#						
2.6	THEORY INSTALL MANY TRANSPORT						
2145	1442						
47	2017 http://12.16.0114/view/08-last/view/97.829.074@control-classes-value	e)/marijes/lip/lip/s/s	i an	(constraint) -	A State	y launa kirtaay kiriya kiriya	
825	Hear (1)2,14,201788 Committee hear alive Committee hear alive Committee hear alive Committee hear alive Committee hear alive hear alive Committee hear alive hear alive Committee hear alive hear alive hear alive Committee hear alive Committee hear alive Committee hear alive Committee hear alive Committee hear alive Alive Alive hear alive Ali	Geologi Chraney 17,040 Geologi Chraney 17,040 Galler Market Market M	ktor Galacita Genesialena 17:0yetskor	7.38 PLAPASSA Padra PSe (2549) Jacke	unuyaas	25.5540 faad oo ar ee yn te ferfal foedig as g	
POTINE	while throughout here						

若关联查询前的数据是原始数据或聚合数据,那么关联查询出来的数据对应为原始数据或聚合数据,查看 详细信息对应为原始数据或聚合数据的详细信息页面。



Web 特征检测、远程控制、SMB 远程溢出攻击、挖矿、自定义特征检测产生的聚合风险的详细信息中除以上信息外,还包括原始信息列表。



- ◆ Web 行为分析风险的详细信息中除以上信息外,还包括关联信息列表。
- ◆ 动态检测产生的风险的详细信息中除以上信息外,还包括文件下载和沙箱报告。
- ◆ 隐蔽信道通信的聚合风险详细信息中除以上信息外,还包括 DNS 详细信息。

7.2 应用举例

本章分别以 Web 后门访问和恶意文件攻击-动态检测产生的风险为例,展现查看风险详细信息及如何处理风险。

应用举例一: Web 后门访问风险处理举例

步骤1. 在风险查询结果页面中选择一条 Web 后门访问风险, 点击该条风险, 如下图所示, 点击每个选项

卡查看风险详细信息、参考分析与建议及对风险状态进行处理。

85 (meth.) 10	THE CONTRACTOR OF A DESCRIPTION OF A DESCRIPANTE A DESCRIPANTE A DESCRIPANTE A DESCRIPTION OF A DESCRIPTIONO				
* JANNE 104	1534	RITER	sahn Baar	wali KX	Xirtis
	NTA-100 Project and a state provide provide a second second	HARWOOK		gitant/mage/second/mage	
8**** #P958	seals matche organ cit				
	Jerzye vsztrazonnem				
4.0	New WIELENEL (NEWS 2014) and anticipal				
and a second	Muzzk				
	GRT Kitp.0.0500 gp.mit/changes/hojimpitgs				
#25	Dier-Agent Machael & Oliveises N° 6.1 (KDBAG Appellise Gel11) is 2015A, Historie Status Consister Keyl-Alex-	Ree Carrieri Chromer VI.A. 3497	100 (2019) 117-18		
455	(80.128)				
2016	162				
amow	- https://doily-cambro/formination-2007/1-caused have/plassorid/increa-	provide experimental	nit' search 6.8 " dirent close	www.filedyy-cyldal>	
125.41	HIS-STREET, N				
0.9912	303				
Web-witted	200100				

步骤2. 在风险查询结果页面中,还可以通过点击操作中的¹³按钮对该条 Web 后门访问记录进行**添加** IP/Host **白名单**的操作。添加 IP/Host 白名单后,符合刚刚添加的 IP 及 HOST 的数据将不再产生 告警。

添加 IP/Host 白名单操作的界面如下。



-										
	THE R. P. LEWIS CO., LANSING MICH.	244	-		MP-MP	sale a		-		Marca B
	-14	102101	And address of the second second	· · · · ·	10000	-	1.11 - 11.11		UT approved a particular star	
	1.00	BRIDGHT .	NAMES AND ADDRESS OF TAXABLE	2012/16/07/162	/水产编中日电单			367	and the second s	
	1.0		TRANSPORT DATABASE	APAPUN. (INSECTION)	1043.328 1999-1997, #1198	1000		10.1	Million and the second s	
	1.0	1000-02.14		ALLASTIC	CALINAL ANNA	· Laboratoria		-	and the strength of the state of the	
		-marite Three	PERMIT PROPERTY AND INCOME.	MAL SAME	antes, antes FR			10)	. 1011 (1000) (10.0120 (10.0010) (10.000)	
		-	The second s		20.	18 ·		-	Performance and an array of the	
	1.4	-	and interview in the second		HARDAGE (#)		A.A.M. M.	201	were some the second second second	
	100	AND LOT OF	No IN STREET, STREET,		interinte:		12.4.5	- 200	POST Internal Internal Distance in Contractory of State	

应用举例二:恶意文件攻击-动态检测产生的风险处理举例

步骤1. 在风险查询界面,选择并且查看恶意文件攻击告警查询出来的界面。

84	435.7.8	2478	NATATA IN						
۰.	10010	and .	0.8	8/16/	8824	REALF	-	RX.	8118
			CONTRACTOR STATEMENT OF A STATEMENT OF A DESCRIPTION OF A						
	44	202-13-16 3175-55	rificant anna amhrachta	isone a	-	101-01-02-00	28	(27) The contrast of the co	10.10
			r Altri (Ellistitis) ver a si saldi li Altria Mulli I. Adlippe						
	61	0025-12-08	BTL contract from BTL and BELLINE CONTRACT CONTRACT BELLINE D	100000-0		(TET EN AL ANTA	10	(27) https://www.integradia.com/active/package/mini- package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-package/mini-p	ilete
			Chim (Billioniki) of a second like one will have a						
	94	3925-13-14 17:14-08	Alterative Million Million Raymon (1.011	-	101.11.01.000	10	OD http://doise.Unipplimet.confur,htp/serren/00001/Http/Sets.Las. e	P 0
			WWH [BEEDWEE] for a second Otherway Well Mail Ages						
	14	3912-12-14 Homost		10.0010.014	-	122206-015	10	007 intercolour Darging front conduct redeners of 10.0,000 option Sec. 6	a 1

- 步骤2. 在上图中,勾选多条记录,批量下载沙箱报告和恶意文件,或者点击操作列 建 按钮下载单个恶意文件。
- 步骤3. 选择一条恶意文件攻击-动态检测风险,点击该条风险,处理风险。如下图所示。
 - ◆ 点击各选项卡查看风险基本信息、客户端信息、服务端信息、分析与建议、沙箱报告以及对
 风险状态进行处理。
 - ◆ 点击文件下载和报告下载按钮,下载恶意文件和沙箱运行报告。



◆ 点击<添加白名单>,将此文件 MD5 设置为白名单。当下次再次审计该文件的 MD5,不再进

行检测,直接报安全。

	1.1.1.17 F BERT (1997) F BERT
2-25 m ⁻ 1053	899888 H-5/20 H-6/8 -28
.40	anu (m stationaloua)
#R	LINER TERESHIP OF FAMILY REPAIRS AN INTERVISED
#n#S	1228
87	027 http://tougtop.com/rokd/packaga/typ/pu///0011/top/ta-Love
875	Hanget 12".
ACTION	1MG
MER	JIR IOC
8115	AGA19
aline	Ma
24059	MARINE COMPANY SACCIAL PAR
2948	Turbu Jaw
29601	NUMPERSON
54478	Nuclear Transford Automation
DALINE	O Licite and ASS Community of the Association Control of Control o
THEORY	2009-12-17 12:0:09
Sets	**

步骤4. (可选)当用户在"系统>升级管理>云端配置"菜单中开启云端配置的情况下,查询恶意文件 攻击风险数据,除了以上信息外,增加多 AV 引擎检测结果功能。通过全球知名 AV 检测引擎的 检测结果进行辅助判断。

点击<多引擎在线检测>,会连接到多 AV 引擎检测结果的页面,如下图所示。

- 01A - 1	AND THE PERSON DECEMBENCY OF A VALUE AND A	
	RANGE 1410 180 18	
+1	2020/02/05/06/04	
20	Pages (Margins) est-main Margins Marginger	
8145	HELD .	
	HT Max (Yang balance) with the second s	
875	Head tips a parameters Accept CP	
+00064		
ean .	200 (200	
40+#	and a	
8878	54	
1965	MULTIPLE AND ADDRESS AND ADDRESS ADDRES	
2+428	sandie	
294405	additional and a second and a	
040/18	palar (stat) (stat) (stat) (stat) (stat) (stat) (stat) (stat)	
044168	and the second	
100,000	muth 1 5 17 T MARKIN	1
1000	HA.	-

1 Date	Converting of the second								
CHRIST	403-11-34 (52750)								
SHUE .	Are 3								
1241210	(4)								
19443	Heldhull37/Geld/MinHelded/Actived/	4							
"IMA268	414353140528568968515531952446465	dasatzer/mittaattearne							
anna ITAB		1200.0	VERA	125544					
ETAB ITAB		Net Calence per (Med)	9264 21.0375-0	31276aanaa Joon 11 Jan Joonnaa					
anna Tan Tan Tan		aganian - Was (Schwarz gar (Mind) - Garris da Collia, 11 (100)	VELA JE DITAS Jacopit	912960000 2001-11-27-00000 2020-11-27-00000					
ETAB TAB S Aran S Aran		nganian - Was (Schwarz gar (Mind) - Garris (an Schwarz) (1980) - Annale Was (Schwarz) (1980)	VELA 20 DITAS Salasti 42	912293aaaa Joon 11-Jan Boonse Joods 11-Jan Kosking Joods 11-Jan Kosking					
alanta ISTAR ISTAR ISTAR ISTAR		aganian Mine Distances que y Mana Generales a Mana, in 1999 Manage Mine La Mana a La Manage Manage Mine La Manage de La Manage	UDEA 2010/100 2210/17 42 2210/1	91009000000 Jocoti 11- Jan Sourcean Jocoti - Jan Kondon Jocoti - La Brickandon Jocoti - La Brickandon Jocoti - La Brickandon					
NAME AND A CONTRACT OF CONTRACT.		ngahin Weldebook perjidad perjaketahan roma manya Weldeboltan Managementan atawa ya samilar Paganilika perjid	UDEA 2010/100 2210/10 42 2222 2222	712293aaaaa Joose 11-25 Alexandr Joose 11-25 Alexandr Joose 11-28 Alexandr Joose 11-28 Alexandr Joose 11-28 Alexandr Joose 11-28 Alexandr					
ERENTER INTERNET INTERNET INTERNET INTERNET		REMAIN We (Schwarz per (Med) General e (Schwarz (1990) Hannes Well (1991) (1990) Hannes Well (1991) (1990) Hannes (1990) (1990) Well (Schwarz (1990))	UELA ALUITAS SALAUT AL ULLA SALAUTA SULLA	912293aanai Joon 11-Jan Ananon Jooda 11-Jan Ananon					

点击数据包名称,可下载风险数据包,方便用户取证;点击数据包名称右边的按钮,可在线查看

数据包。

	NATE AND A DESCRIPTION OF A DESCRIPTION
\$108 \$PHER	BENKE DETAIL LE
87	(2017) Set Minute
	ILLUD, UNIDER J. BREED HURDEN HURDEN HURDEN HURDEN HURDEN DOOL
	1 Box (20)
	PERT House, VFIELD ULL TO TOTAL DESCRIPTION OF LOW PROVIDENCE OF
875	Constant-Type multi-animalyse Xermal-Constant-all # Wave dispertisons(FLBA House Fitz) and in the IFED Kernel Fitz) and in the IFED Constant-Kernel Fitz) Constant-Kernel Fitz Constant-Kernel Fitz)
POLINE	- Pointer C State "Line" (and "Line" (and "Line") and "Line" (and state and "Line") and "Line" (and "Line") (and "Line"
	58
10(15)	AN Protocol
alter	- M -
125.01	
3846	
6030	. Sansi
10.00	http://www.innegraphination/collidation/pr/son-principality/Station/Station/

了安恒信息



3 mmHz: 2012/07135450000068.pcagt

11120	teda - Salaar								
74	Yese .	Seco	Destantan	Nessee	Longit .	10h			
1	0.000000	18.01.01.00	10110516110	11.9	117	41/161-14 1/100 (1915) ACR (1916) 1 Actor / Miles RC Lines 2017 Trans 21/14470/17 (Trans 21/14470)/17 (Trans 21/14470/17 (Trans 21/14470)/17 (Trans 21/14			
1	8.008000	16.20.01.00	18210015-100	ermit.	107	2007 Antilogicity assert (UTTWA). Taxwee and Open Molecular and parts			
1	8.038008	1021081019109	18.3531.84	-	114	HTTP://I.Ref Marcower			

Franse 1. DV paper or new (2022 and, 2039 parts concerning 2020 press Orderwork, Sec. (#Conference) and disklandschenden (Entre Text Statistical Conference) 480: 25: Version (AN, Fellis, D. D. D. S. 216 marriero Permanen Version (S. S. 2020) 740: Con 2020, 740: 70, 740 Transmission Commit Paperson, S. V. Polse, KOGA, Der Part, 2020, San 1, Ann. 7, ann. 246



8. 3

8.1 资产概况

在菜单栏选择"资产>资产概况"进入资产概况页面。页面下方会列出用户已经扫描识别出的资产,更多 信息请参考识别区域。

APT 支持 IPv4 与 IPv6 地址解析资产,、

概况模块可以通过输入 IP/IPv4 段、域名、资产名称、系统类型、端口号、等级、应用类型、所属分组、标 签、服务类型等进行资产查询。

◆ 点击<**导出**>可以将所得信息导出为 Excel 格式。点击>键可以查看资产详情。

a wreat	3 10 20 001													
() etters	200	massie an			100	1001				1001				
	0.044	A				445		-	-					
	5/5×5				-	malali			10	-				
	871.00	(4)										•	**	
	-	1.0.14												
	1.0	8*10	100	-		825	103812-01	**		100	XXXXXXX	si.	10	
	1 1 20	981981917					*15.5			#85.	2020-12-14 1912-04	10		11
		42100353					*42			*45	2020-1216-1406.28		-	5
		012.03167.257					*12.2			##X	2826-12-10 0939-38		. 10	
		102140.111100					842.5			44,5	3020-12-16-0038431		-	1
		111110-014					*12.1			PES-	3829-12-14-09-19-40			76
		100.160.177.000					A10.11			4165	JUDDE-13-15 IDEALOR	10		

◆ 单击编辑按钮,可以对未定义的资产进行分配编辑。其中,所属分组和标签需要在主菜单选择"资产
 >分组标签"进入对应页签设置。

- Đel	1002210								
10	用户目标	516	6.1	Bits.	HUMOHUM	48	19.0	10000	10419.345
	192.168.191.2				***		*24	2020-12-16 16:12:24	M In AC
	192,168,55.2				+#5		+82	2020-12-16 1404-98	N = 6
	192.168.87.251				#12×		建筑业	2020-12-16 09:58:59	15、二、四、四
	192,168,152,140				892		*82	2020-12-16 09-2013	R. 6. B.
	192.168.28.40				A.5.2		半夜 以	2030-13 09v11u40	R = 0.
	192.466.137.225				*21		*22	3030-12-15 20-6664	8.4.8
	192.168.137.30				*955		#1912	2020-12-15 20/20/23	2.0.3
	192.1KE.2.II				単度の		果理论,	2020-12-15 14:0542	21.6.8
编辑资产			×						
-------	---------------	---	---						
资产IP:	192.168.151.2								
名称									
新鳳分祖:	清洗詳								
标题:	第 告师								
等级:	普通资产								
	版词 4	毒							

◆ 单击攻击溯源按钮,跳转导航-攻击溯源页面,查询该 IP 地址的相关信息

84	ARA C								
14.10	8846	5.0	store.	10.0	ALCONOMIC .	#8	**	1014010-F	1977.00
	192.165.157.2				*21		*22	3020-12-16 16(12:24	2 1 1
	19216855.2				*#3		****	2020-12-16 14:04:50	8.00.0
	102.160.07.251				122		*22	JT070-12-16 09:55:50	Rinin

◆ 单击主机威胁按钮,弹主机威胁详情页面,查看该资产的主机威胁详情。

946	4.834								
4,11	30.0-35W	816	病用	88	PEGLETHE	₩E	110	ACTION OF	aus.
	192,168,151,2				*822		141802	2020-12-16 16:12:24	F1 4 5
	102.105.35.2				#12.9		清理点	3020-13-16 16:06:18	21.0.18
	192.168.67.251				##2		*92	2020-12-16 29:59:50	2.4.2

包括主机威胁指数、攻击溯源、攻击过程和攻击溯源可视化等信息。

(安恒信息



aruenan ika	Sta mella memaneli
ANA CH	
250	162.168.15.204
amiku (1836%)	REAL - COLUMN - REAL - REAL - REAL
ministratio	******
00945-530	

8.2 非标端口

操作入口

在菜单栏选择"资产>非标准口"进入非标准口查询页面。

查询条件支持通过资产 IP/IP 段、协议类型、端口号等查询条件,方便用户对非标准口进行查询。

针对非标端口展示其端口、协议类型、资产名称(IP 地址)、所属分组、标签、等级、发现时间。可根据 非标端口查看资产的异常情况。

H RANKE	5 machin						
@ 100ml	are (10. · · · · · · · · · · · · · · · · · · ·	9482 8	-		No realization of	1911
13 states							
10.000 million							
	-	WREE	8468	NECH	**	**	8782495
	8357	HETT	addr.547ed.4519cd-428fe	9212		*22	2020-12-16 14:54:42
	810	14(19)	500-700+87(back40)	+82		*21	acon 42-He riscone
	12009	19.	3x0010k7320.033913a4d	824		.882	2020-12-19 1041:31
	11111	24	540-0-743-01291 MM	+81		*#1	3000-10/19 104101

8.3 分组标签

操作入口

在菜单栏选择"资产>分组标签"进入分组和标签设置页面。



◆ 选择**分组**页签,可以自定义增加分组名,可以在**资产概况**处依据分组对查询到的资产进行分类。

an a R area () searc								
		COMPANIE AND A DESCRIPTION OF A DESCRIPR						
The sector of	101F		10110					
		The second second						
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
	And A Contract of							
	diller.							
	anny .							

◆ 选择**标签**页签,可以自定义增加标签,可以在**资产概况**处依据资产标签对查询到的资产进行分类。

E RABR	8	SHE WE
@ #####I	_	○ 而于对资产进行将性分类。④如: 副祭職
D transa		
E ROMEN		APT = HERE + HEE

8.4 识别区域

操作入口

在菜单栏选择"资产>识别区域"进入识别区域设置界面。设置识别区域后,可以对满足条件的 IP/IP 地址 段进行扫描并识别其中资产,否则不进行扫描和识别。

点击<导入>进行批量新增,点击<全部导出>可以导出全部数据。

E ware		and a second	100		-		1.22	
6 mian	rea	and a second		-58	0.010.8	PPERM	1000	ars a
C 2198452	150 100 AU	具体内计算 水江 和 约	1011144067	35.209115			•	11:2
E 43464	10.002.00	AMPLIES (C. NY)	105144(9)	00,009111			•	1112
	172,9638-172,51294291	和4月二日月二月月	103.544047	10.200911		*		N 1 B
	2332-210	#1010-00-012-011	100.144307	30.209715			•	- 1.5
	MONINE	83460-48 IN1-626	00.74400	36,20903			0.00	11.12
	(96.966.25.22)	31	100.03(40)4	-6.1203			0	R 18

可以新增内部 ip 地址, 默认 ip 地址段由**配置>常规配置>地理位置**中的 ip 地址同步而来,更改地理位置中 ip 内容后,新增数据自动同步。

杭州安恒信息技术股份有限公司



*国家:	中国	
城市选择:	派工/杭州	
* iPtete:	EBPRE	
单位地址:	100050-12012	
内网地址:	* # 0 H	
	取消 前主	



9. 报表

9.1 报表分类

将报表类别归纳为综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类型。

- ◆ 综合威胁分析报告主要是从整体风险情况来进行事件类型的分析,包括风险总览、安全事件分析、失陷主机、外部威胁、横向威胁、对外攻击威胁、脆弱性分析、文件威胁分析、风险类型说明和处理建议。
- 主机威胁分析报告主要是以主机视角来分析发生的风险情况,包括风险总览、失陷主机、横向威胁、
 对外攻击威胁、脆弱性、风险类型说明和处理建议。
- ◆ 文件威胁分析报告主要是根据恶意文件来从风险趋势、投递情况、恶意文件进行分析,包括风险总览、
 恶意文件风险趋势、恶意文件投递风险、APT事件、恶意文件分析、恶意文件风险描述和处理建议。
- 外部威胁分析报告主要是以外部攻击视角根据攻击者和被攻击者来进行分析,包括风险总览、风险趋势、被攻击主机、外部攻击者、风险类型介绍和处理建议。

NVABONBI	-1452 - 17	W AR	87° MB	NUMB AND	#AB.		
ALC: NO.			武府一个田田来 世,开	chik			
1954)							
REDR							
### #			E.C.	himed	0.00		
NUT B	综合或防分析用性	主約	城的分析推告	父件或胎分析服性	外部间的分析机	外部國防分析提出	
	642-43		GEOWIN .		P P B P P B		
	-			E-second state	-		
	Restored and				Sector Sector		
6	New Jie						
	P IN ICON MICCON						
	1 a decembra i	information and an	Company of				
	1004	10.00 M	RPH10	HIRA,	的最大限的	87.0	
	10009	NAND	804828 * 2028-03-15-16(22)# 2028-16-16-16(22)#	BEEA.	NEARA NAMESARE STATE	898 	
	10004	NAX9 NAX9	89405 * 2008-03-05 5497254 1 2008-05-05 5497264 * 2008-05-27 754444	#88.4 2010	HEARN THEARTHEARN CANE.	878 + 1110	
	10000	NAXS HAADIIFSD MAADIIFSD	99-009 • 2006-05-56 (2006) • 2006-05-56 (2006) • 2006-07-27 (2006) • 2006-07-27 (2006) • 2006-07-20 (2006) • 2006-07-20 (2006) • 2006-07-20 (2006) • 2006-05-56 (2006) •	HBA anto attitu	HEARD Doubertainsteachara Doubertainsteachara	878 * 11:33 * 13:43	
	10004	NANT NAND-FER NAND-FER	99-0019 • 2008-03-05 Megrate • 2008-03-05 Megrate • 2008-07-02 USS-044 • 2008-07-02 USS-044 • 2008-07-02 USS-044 • 2008-07-02 USS-044 • 2008-07-02 USS-044 • 2008-07-02 USS-044 • 2008-07-02 USS-04 • 2008-05-05 Megrate • 2008-05-05-05 Megrate • 2008-05-05 Megrate • 2008-05-05-05 Megrate • 2008-05-05-05 Megrate • 2008-05-05-05-05-05-05-05-05-05-05-05-05-05-	HBA anno anno anno	HEANN INLARDARDULAND NARDARDULAND ANDREADDULAND	898 41213 41213 41213	
	1004	0482 0482=**** 0482=**** 0482=*****	99-1019 • 2008-10-55 Sett254 • 2008-10-55 Set2544 • 2008-11-21 Toback • 2008-11-21 Toback • 2008-11-21 Toback • 2008-11-21 Toback • 2008-11-21 Toback	ABH anno anno anno	HEANN INLANDART BLAND NAMES AND THE AND ARMEN AND THE AND	*** ***** *****	
	100000 10 2000-12-10 (400001 10 20 2000-14-00 100000 10 20 2000-14-00 100000 10 2000-14-00 1000000 10 2000-14-00 1000000	NANY NANDOFEN NANDOFEN NANDOFEN NANDOFEN	2020 - 12-15 - 10222 - 12-15 2020 - 12-15 - 10222 - 12-15 2020 - 12-15 - 12-17 - 12-16-16 2020 - 12-27 - 12-16-16 2020 - 12-27 - 12-16-16-1 2020 - 12-27 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1 2020 - 11-17 - 12-16-16-1	HEA advice advice advice advice	HEARN INLARGUERDUAND INLARGUERDUAND INLARGUERDUAND INLARGUERDUAND	878 41313 41313 41313 41313 41313	

9.2 报表查询

报表查询可以查询综合威胁分析报告、主机威胁分析报告、文件威胁分析报告和外部威胁分析报告四种类 型。

操作入口

在菜单栏选择"报表>报表查询"进入报表查询页面,点击<立即查询>后选择时间范围进行报告预览。报

告预览如下图所示。

🟹 安恒信息



综合威胁分析报告

项目条称	test
时间范围	2020-12-15 16:09:53器2020-12-16 16:09:53
分析时间	2020-12-16 16:09:54
资产范围	全部



一、风险总览

1.1 整体风险情况

本节是对蓝胸网络在探告期间发生的风险情况进行概述,如无单独说明,关于风险按照的统计均是针对假合风险。

> 在报告期间,总风险数量11445次、荒危风险16次、紧急事件18个。 > 发现已失端主机186台,被外部攻击成功主机0台,有描向攻击行为主机342台,对外攻击主机455台, 誘弱性风险主机120台。 > 发现已要放立件65个、其中宣传现象文件11个、原始文件共传播109次。

1	DCREED/2504.1TV/F11	Set Merchanter and Links	STATISTICS AND ADDRESS OF	

网险总数	失殖主机	恶意文件	素危恶意文件	深意事件	
11445	186	65	11	18	

历史查询记录记录历史报表详情,包括报表生成时间、报表类型、时间范围、创建人(登录用户)、创建

人角色等	₽.

) Kenn						
444						
11.14	E-MERICAL CONTRACTOR OF CONTRACTOR OFFICIAL OFFIC	建筑规划	ATFECT28	朝線人	前建人物的	ien a
	💷 2025-12-16 1609513	综合系统分析绘图	* 2020-12-15 16/9854 = 2020-12-16 16/9854	adontri	月秋春春九美雪堂诗风 彩竹莺…	*(B(0
	() 2020-12-16-1453891	94.429-017839	2020-12-15 14:53:54 2020-12-18 14:53:54	admin	A.比较很不是在WIRA,SHIF.	$= (\Xi) [0]$
	🗇 2020-11-22 (55314)	中央國際的性態家	* 2020-11-27 15:54:54 = 2020-11-25 11:54:34	autority.	风险会争先发展管理员系统管	0.010
	2020-11-28 1552-41	watering	* 2020-11-27 15:5441 - 2020-11-28 15:5441	attein	Abern Kerknad	* (B) B
	1 339-11-12 (538-14	经合成部分代码的	2020-11-11 15:81:53 2020-11-12 15:81:55	amin	NEERARGERSAME.	= (1)(0

在历史查询记录列表的操作项列下,点击 [@] 预览该时间范围内的报表,无需重新生成;点击 ^前 图标删除 选中的报表记录;点击 😳 将设定时间范围的报表以 RAR 压缩包格式导出。

如果报表预览时间过长可能会被清掉,页面上将不显示 [@] 预览、 []] 导出图标。

9.3 报表导出

在菜单栏选择"报表>报表导出"进入报表导出页面,可以选择时间范围、报表类型、报表格式 (HTML、

PDF、WORD) 三个参数导出报表。

杭州安恒信息技术股份有限公司



导出可选择全部报表类型,但格式只能选择一种。

0.00	FSWOM							
(2 KREN								
E same	SERVICE OF BEDEVES	\$ 2002-12-60 10.11.36						
E and a	- Desity of the second	water the contract	in network in a					
S warm	and an an an an and	Annestering Secondary	the company of the company					
E enus	Rent Int. To	WORD						
	5 Section 20							
	CT SIRNA	124,812	104018	NWB/C	HITE A	087.86	anu	
	2008-11-28 15/44-17	internation and	a and the read of states	404	1000	ALERARBER.K.	21.10	
	() 200 (0-0 (m4/s))	(6480-11180)	* 2020-10-14 10:44.23 - 2020-10-14 10:44.27	900		AventApentx.	31.8	
	2022-10-14 Mc5519	intamorram.	1 2010 10 14 00.6219 1 2020 10 10 12 5210	9090	-	INSTANTANTS.	1.1	
	202110-10104014	274011158	* 3528-08-14 YO-5514 C 0528-18:34 YO-5514	345933	-	AUGRACEMENTS.	21.12	

在历史导出记录列表的操作项列下,点击^前图标删除选中的报表记录;点击²将设定时间范围的报表以 RAR 压缩包格式导出。

9.4 报表订阅

报表订阅可按照用户需要定时自动生成并发送报表到配置好的邮箱。

在菜单栏选择"报表>报表订阅"进入报表订阅页面,勾选启用状态、配置发送周期、报表类型、报表格 式和收件人邮箱,点击<保存>完成报表订阅配置。

豪 配置报表订阅前先点击"报表>邮件服务器"配置邮件服务器。详细请参考邮件服务器设置。

2.888.899	
2. 报表导出	- 提出(100)
RADA	* 庭形状态:
5 报表设置	* 波送局期: 與天 尋問 喝酒
昱 邮件服务器设备	生成时间:每天 0.世 - 接收数据时间范围: 0.世 - 24.世 -
	* 重要类型: 全部 接合机动分析报告 主化机动分析报告 文件或初分析报告 外部风动分析报告
	· 細胞描述: HTML PDF WORD
	* 在外人創稿: 四月四人亦下各村人如何

◆ 用户可在**报表订阅历史**列表查看、编辑和删除历史订阅报表记录,如下图所示。

0	明御APT攻击预警平台 同時法律综合探讨		特赦	-9 Wi	15.M	R77 #12	服務部 配	11 Xi	焼		
(1)(4) (1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(日本市内	F 程业订成历史									
E	田本寺出	服務表型	最高的式	我这周期	EMINE	用的批用	收得人創始	例除人	相關人物色	ORIES	操作场
10 10 E		但且推荐计符程度,主 的减数计符程度,实计 增数计行用面计包相 取计符件面	HTML	63	50,651-10.5	- 推动一	-	admin	不能會新來。 記書等時代。 多代新現代		8 8
		伊自國際位所增加,本 約,410百名將國為文件 國際任所提為,內部國 動任所提為,內部國	WORD	47	8704	0 crit 24/3		Atlenies	间风度着色, 配着登场风, 来的建设的	•	N R
		增合成款公约增加,主 约,成款公约增加,又外 成款公约增加,外部成 款公约提加,外部成 款公约提加,	HTML	.92	107.524	i aut I 2440	in the second	admin	风险高着机 配度增加点 高速增速的	39	20 8)

◆ 点击历史发送记录选项卡,展示发送报表的生成时间、报表类型、时间范围、报表格式、发送周期、 发送结果等。用户可以重发或者删除历史报表订阅记录。

	6465	576	14.65	107	82		100	atm.	10.00	about -
See 3 E anns	-					<i>a</i>				
E sette										
E watch	T-MARKA	\$8.72	even		are c	10040	WHEA.	的收入的世	RISHE	954
12 wears	2020-12-16 00:00:00	manatolorithia, 17,420-orithia, 11022-orithia, 140422-orithia	* 2001-0-10 000000	W	90	ą.	-	706484.80 898		4.0
	(T 800-0-16 0000)	ROBERT HA 25 AD OFFICE TRADUCTION FEASTORN	1 2000, 12, 14 00000-00 1 2000 12 14 200400	w	oie	47		tarent eg gian	PRIVACE PROVIDE	
	820-12 va (wittel)	mash-insta 2fabortaa 1nabortaa 10abortaa	* 3000 (3-01 000000) 		ы,	4.1	and the	101.849.5.812 812.9	entities provide	

9.5 报表设置

在菜单栏选择"报表>报表设置"进入报表设置页面,可自定义报表的组织 Logo 和产品名称,可自定义报

杭州安恒信息技术股份有限公司

安恒信息



表的组织 Logo 和产品名称。

0	明即APT改击预整平台		11.85	3.85	26.89	1274	16.3K	303838	<u>к</u>	新档	atere -
24						_					
日間	82N	1000 . 01010-0	000 5	受範囲應	1882.060	+					
日期	648										
U1 80	NCH	Pasta 🔳 igawite	由田塘平市								
8 .		0.01									
E2 ##	848										

默认使用安恒信息的 Logo, 产品名称为"明御 APT 攻击预警平台"。如下图所示。



PDF、HTML 格式报表中不展示产品名称。

产品名称是非必选项,若不选产品名称,导出报表中 Word 页面不显示产品名称,如下图所示。

主机威胁分析报告	
一、风险总货	
主机威胁分析主要	
·	сколы чил оказаных нашениях, начажения с тарженият оказ, воены у Е.
小 [。] 事件,均需要重点关注 失陷主机	75 ±

9.6 邮箱设置

-

杭州安恒信息技术股份有限公司

1



报表发送功能需配置邮件服务器。

操作入口

在菜单栏选择"报表>邮箱设置"进入邮箱设置页面。

配置参数包括发送邮件服务器、发送者、DNS 服务器配置、发送者邮箱、端口、SMTP 验证等参数。其中 密码为发送者邮箱 SMTP 服务的授权码。

III.	 - water			
Di analare				
E RAUS	121627428	irrb diappoolarty cont in	1012-0	itapp:
(2 mmi10	· ONS語來語		*201401W	one or property and
S HARR				
ER WHIGH	SMIPHE		1 (MC)	15
	180	1010000 W.C.	100米位	8 764 0 145 0 544
		service we		

参数配置完成后,点击<发送测试邮件>,输入接收邮箱地址,确保邮件服务器可以正常工作。



10. 登录故障排查平台

APT 故障排查平台,简称"排错平台",有两种方式登录:

- ◆ 在任意 Web 管理页面按 "Shift+p" 组合键可弹出排错管理窗口, 点击<**故障排查平台**>, 输入账号密 码进入。
- ◆ 在浏览器地址栏输入:http://管理 IP:82/,输入账号和密码进入。

APT 排错平台的登录账号分 admin 和 root 两个, admin 账户对产品进行普通管理, root 账户属于产品本

身出现故障或者需要修改配置时才需要使用。

◆ admin 用户的密码是 Das@2014。

◆ root 密码每天变化,若需要 root 账户密码请联系产品组人员并说明问题情况,代理商请向
 区域渠道负责人联系获取。



11. 术语&缩略语

术语	解释
APT 攻击	APT 攻击(Advanced Persistent Threat),即高级可持续威胁攻击,也称为定向威胁攻击,指某组织 对特定对象展开的持续有效的攻击活动。这种攻击活动具有极强的隐蔽性和针对性,通常会运用 受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack,简称 DDoS)是指处于不同位置的多个 攻击者同时向一个或数个目标发动攻击,或者一个攻击者控制了位于不同位置的多台机器并利 用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的,这类攻击称为分 布式拒绝服务攻击,其中的攻击者可以有多个。
DHCP	动态主机配置协议 (Dynamic Host ConfigurationProtocol) 为网络中的主机动态分配 IP 地址、子 网掩码、网关等信息。
NAT	网络地址转换(Network Address Translation),可以把局域网内的多台计算机通过 NAT 转换后 共享一个或多个公网 IP 地址,接入 Internet,这种方式同时也可以屏蔽局域网用户,起到网络 安全的作用。通常共享上网的宽带路由器都使用这个技术。
SaaS	SaaS 是 Software-as-a-Service 的缩写名称, 意思为软件即服务, 即通过网络提供软件服务。SAAS 是云计算的一种服务模式。
认证	是一种信用保证形式。按照国际标准化组织 (ISO) 和国际电工委员会 (IEC) 的定义,是指由



	国家认可的认证机构证明一个组织的产品、服务、管理体系符合相关标准、技术规范 (TS) 或
	其强制性要求的合格评定活动。
	虚拟机 (Virtual Machine) 指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环
电空气	境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中
虚拟机	创建虚拟机时,需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟
	机都有独立的 CMOS、硬盘和操作系统,可以像使用实体机一样对虚拟机进行操作。