

TDP 用户手册 3.1.1

2021.4 TDP

微步在线科技有限公司 LEADER IN THREAT DETECTION AND RESPONSE

前言

TDP 通过分析网络镜像流量,基于规则检测、机器学习模型、大数据技术,可以实时感知用户系统的安全威胁,检测到外部攻击、内网渗透以及失陷破坏的威胁。同时支持对网络内部的资产进行梳理,帮助用户建立全局安全意识。

本文档介绍了微步在线威胁感知平台(Threat Detection Platform,以下简称"TDP")的使用方法。帮助安全运营工程师了解产品功能,熟悉产品用法,以满足实际使用需求。

本文档适用对象为普通用户、安全运营人员、实施工程师。本文档假设读者具备如 下相关网络和安全知识:

网络拓扑结构

网络协议 (DNS、HTTP、TCP、UDP、DHCP)

威胁情报

网络沙箱原理

如需获得更多信息,请联系我方支持团队(contactus@threatbook.cn)。

一、监控

TDP 监控功能包含"首页"、"大屏"和"系统运行状态"三个功能模块页面。

首页功能为用户提供基础的系统安全评级,展示整体的安全概况;

大屏页面,支持用户展示需求,友好的展示当前系统的攻防态势,以及威胁检出情况;

系统运行状态页面,支持用户进行系统运行状态诊断,并对当前系统的流量、处理 量、网口状态做了友好展示,帮助用户确认系统运行状态,排查问题。

1.1 首页

用户登录后, 默认来到首页页面, 首页时间段默认展示近 7 天, 用户可以自行调整 为 "24 小时" 或者 "近 30 天", 用户可通过切换业务组查看不同组下设备的告警总览。

页面路径:

从导航菜单进入监控页面 (登录系统默认来到此页面)

选择"监控-首页"子菜单项

系统首页为用户提供 TDP 检测到的安全概况, 分别从以下角度呈现:

TDP 微步在线 成形感知平台	监控 威胁	资产&风险 调	寶 <mark>一課</mark> 报告	处置 平台管理	175主节点 ▼ 微步在线内部测试 <mark>试用</mark>	s 🔹 🖡 😮
监控	首页				请选择业务组 > 24小时	7天 30天
🛛 大屏	📦 健康度: 检测中	当前每秒处理量: 0	I Ba	ള流量: 0路 │已接日志: 0路	已接入Agent: 0台 已开启检测功能: 03	Ω.
 論页 小,系統运行状态 供取供式 ④ 級联協控 	整体安全态势 ですういた。 存在風雨利用成功/存在。 存在均可能用成功/存在。 存在均可能明成初	▲ 音響主机: 52台 ■ 日共順主机: 37台 ● 已处理主机: 0台 以上数環从 883542 条件	 或助事件: 			総环: の 対外攻击:0 を た273 数据の取:0
	TOP協会理主机 金郎 デ重 192.168.100.12 振動器 第 ア重 10.10.10.4 振動器 第 ア重 10.10.10.9 振動器 10.10.22.10	服务器 ○ 共満 3) 外部攻击或投進) 型 共治 # APT 二 型 共治 # APT 二 型 共治 # APT 二	室看列1 系 攻击成功 º 失路 聋 APT 与远控编建立连接 与远控编建立连接			O-4/09 20:23 € 04/09 20:23

1.1.1 运行状态

TDP 在此展示系统的运行状态,包含以下信息:

【当前处理量】展示了系统的实时处理速度。

【已接流量】展示了系统接入的流量路数 , 鼠标浮动上去可以看到具体的接入信息。

【已接日志】展示 TDP 接入 syslog 的数量, 鼠标浮动上去可以看到具体的接入的日志信息。

【已接入 Agent】展示 TDP 接入 Agent 的数量,点击页面跳转进入终端取证页面,用户可以查看所有接入的 Agent。

【已开启检测功能】展示系统当前开启的检测功能数量,鼠标浮动上去可以看到具体开启的功能信息。

1.1.2 整体安全态势

TDP会对当前系统所选时间内的安全情况做一个评级,用户可以视情况修改评级, 修改后 24h 内生效。



关键指标如下:

【已失陷主机】展示了系统内部已经失陷的主机数量。

【告警主机】展示了受到威胁的主机数量。(告警主机中也展示了已处理主机数量)

【已处理主机】展示已处理的告警主机数量

【外部攻击成功】展示了所选事件范围内,系统遭受外部攻击的攻击种类数量

【针对性攻击】展示了系统遭受的针对性攻击的数量。

【Webshell】展示了遭受 Webshell 攻击的数量

【建立远程连接】展示了所选时间范围内,系统被黑客控制失陷的事件,以及被黑客操纵向外发起攻击进行破坏的事件。

【其他告警及风险】点击可查看所有告警数据及风险数据

【操作】以上核心指标,用户均可以点击,进入详情页面,详细了解相关的内容。

1.1.3 攻击链

TDP 为用户提供威胁告警的攻击链可视化展示。在威胁分类图中,用户首先应该 关注是否存在漏洞利用攻击成功的威胁种类,若存在攻击成功,则应该尽快处理攻击成 功事件。攻击链从两种威胁来源做了可视化,一种是渗透攻击,另一种是感染病毒木马 等。



渗透反映了互联网对系统内部的攻击情况,统计展示了外对内的攻击类型数量,包 括以下类型:

【侦查】来自外网的所有侦查扫描事件种类。

【漏洞利用事件】来自外网的所有漏洞利用攻击事件种类。

【漏洞利用成功的事件】会使用红色标签标志在漏洞利用类型数量之后。

【内网渗透】统计了系统内部的所有横向攻击类型种类。

感染的路径,可能包括以下类型

【恶意样本】系统下载或者传播恶意文件,以及系统尝试下载恶意文件行为 【命令与控制】包含以下恶意行为:

系统连接远控地址, 该连接通常由木马和病毒等恶意程序发起;

系统进行 DGA 地址连接, 意味着内网存在木马或者病毒等恶意程序;

内网主机发出符合木马特征的恶意流量;

内网主机对外流量中发现了远程管理工具相关的通信协议,可能正在使用远 程控制工具;

内网主机连接新发布域名,新发布域名(Newly Observed Domain,NOD)是 刚刚在全球 DNS 服务上注册和发布的域名。黑客经常使用 NOD 域名来发送垃圾 邮件,进行恶意软件传播,组建僵尸网络或者作为远控服务器地址;

发现僵尸网络行为,通常为机器被控后利用计算机资源进行其他非法操作,如 对外发起 DDoS、对外发送垃圾邮件等。

【挖矿】内网主机主动连接或查询了加密货币矿池地址,对应主机上可能正在执行 挖矿程序。

通过

【数据窃取】内网主机发现数据窃取行为。

【系统内部对外攻击】内网主机发现对外攻击行为,有可能已经成为黑客跳板机。

【操作】在威胁类型中,每一种威胁类型,都支持点击下钻,点击后会展示所选威胁类型的具体事件列表,用户可以继续追踪相应的事件详情。

TDP

1.1.4 待处理主机

TOP待处理	主机 ○ 全部 ○ 服务器 ○	○ 终端	查看列表 >
1 严重	192.168.100.175 终端	存在内网渗透〕发起对外攻击	
1 严重	192.168.100.171 终端		
1 严重	10.10.51.2 终端	存在内网渗透已被黑客控制	
1 严重	192.168.76.103 终端	- 已被黑客控制	
近 严重	10.10.10.11 终端	已被黑客控制	

【TOP 待处理主机】模块展示了所选时间范围内, 主机检测到告警, 并且安全运营 人员未处理的主机, 按照严重级别进行了排序, 用户应该首先关注严重级别较高的主机。

【待处理主机模块】展示内容包括主机的 IP, 主机的类型(服务器或者终端)、告 警严重级别、以及主机的状态。用户点击对应的主机 IP, 就可以跳转到此主机的主机详 情中, 从而详细查看主机的告警状况, 同时可以在主机详情页面进行告警处理。

【操作】此模块支持对服务器或者终端进行筛选,默认展示全部待处理主机,点击 右上角"查看列表"按钮后,页面跳转到所有待处理主机页面,用户可以在此页面查看 全部告警主机,然后进行处理。

1.1.5 威胁事件和趋势



【TOP 威胁趋势】模块展示了所选时间范围内的告警趋势,并展示了 TOP4 严重 程度的威胁事件。

【威胁事件】展示内容包括:告警时间、威胁类型(包括外部攻击、失陷破坏、内

网渗透)、攻击类型、攻击名称、严重程度以及涉及到的服务器和终端数量。

【操作】鼠标滑动到对应的服务器和终端数量上,可以看到具体的机器 IP。

1.1.6 资产与服务



【资产与服务】模块展示了用户系统检测到的资产和服务,系统通过一段时间的流 量监听和判断以后,会逐步的梳理以下内容:服务器 IP 资产、终端 IP 资产,全部服务 列表和最近 3 天新上线服务列表。

【操作】点击对应的标签,页面会跳转到对应的"资产&风险-资产和服务"页面, 详细展示具体信息。

1.1.7 登录风险

登录风险	登录接口 ■	弱密码 1 321/组	
	正常登陆 ////////////////////////////////////		97% 3%

【登录接口】TDP 自动识别系统内部的登录接口。

【弱密码】统计系统中用户使用的弱密码组数。

【正常登录/撞库比例】统计系统内所有登录接口正常登录与撞库的比例,从而体现了用户登录接口的安全状况。

点击【登录接口】、【正常登录或者撞库】,跳转到"风险-登录风险-登录接口"页面,支持查看系统内部所有登录接口,以及登录接口被撞库的情况;

TDP

点击【弱密码】标签, 跳转到"风险-登录风险-弱密码"页面, 用户可以查看系统 内有哪些用户使用了弱密码。

1.1.8 接口风险

API风险			
接口名称	PV数量	UV数量	API总数
192.168.100.175/lessonverview.mvc	1367665	1367665	137 /个
192.168.100.175/lessonverview.mvc	763454	737463	
192.168.100.175/lessonverview.mvc	5567	7865	
192.168.100.175/lessonverview.mvc	4345	3456	
192.168.100.175/lessonverview.mvc	344	737	

【API 风险】模块展示 TDP 监控到的系统内部的开放接口情况。

【API 总数】为监控到的接口总个数,点击可以查看具体的接口信息。

使用列表的形式展示了访问量 TOP5 的接口,包括以下内容:接口名称,接口的 PV 数量,接口的 UV 数量。

1.1.9 数据泄露风险

数据泄露风险 敏感信息接口		文件上传下载			
身份证 三副 <u>12</u>	银行卡 24	doc/docx:12	MP3:5		
手机号	邮箱		ZIP:2	txt	:3
33	₩ 54		tar:1	PDF:1	其他:1

数据泄露风险展示了 TDP 对系统内部敏感信息泄漏接口,以及文件上传下载的监控结果。

【敏感信息接口】展示了系统检测到的明文传输身份证号码、银行卡、手机号和邮箱这几类敏感信息的接口,用户点击可以看到对应的接口详情。能够帮助用户梳理系统内部敏感信息存在泄漏风险的点。

【文件上传下载】展示了系统内部被下载文件类型的分布,可以帮助用户发现异常的文件上传下载行为,点击后可以跳转到"文件风险"页面,进行文件上传下载行为的详细分析。

1.2 大屏



页面路径:

1.从导航菜单进入监控页面

2.选择"监控-大屏"子菜单项,页面自动全屏,同时展示大屏相关的内容。

TDP 大屏满足安全态势实时展示的需求,大屏展示以下内容:

【核心指标】包括告警主机数量、威胁事件数量、告警次数、已安装 Agent 数量, 用户可以根据这些指标直观的感受到当前的安全态势。

【自转地球】展示了用户自身的地理位置,通过攻击飞线展示了收到攻击的来源。

【内网关系图】展示了用户系统内部的告警分布情况。

【告警主机】列表展示了当前严重程度最高的 TOP5 告警主机,展示内容包括主机 IP 以及主机告警威胁类型。

【恶意访问地址】列表展示了当前系统内连接的恶意地址,展示了恶意地址的 URL、 所属地理位置、严重级别、告警次数的比例。

【TOP5 攻击来源】实时展示了攻击系统的来源 IP,展示内容包括攻击 IP、地理

位置、严重级别。

【实时攻击飞线】实时展示了互联网对系统内部的攻击,展示内容包括攻击名称、 受害主机数量、严重级别。

【攻击链】展示了攻击在攻击链各个阶段的分布情况。

【实时流量】滚动展示系统当前的处理的流量,展示内容包括:源 IP、目的 IP 或者恶意地址、以及协议。

【24 小时输入趋势】展示了系统 24 小时内, 接入的流量变化, 用户可以分析系统 流量是否正常。

【24 小时告警趋势】展示了 TDP 对系统镜像流量分析,产生的告警趋势。



1.3 系统运行状态

◎ 运行状态 📦 健康度: 100% 最近一次检测完成时间: 01月13日 16:19:34 ⑦ 系统启动 底层启动时间: 2020-01-09 15:19:52 S IOC更新 硬件状态 ♥ CPU正常 ⊘ 内存正常 ✓ 磁盘正常 输入模块状态 已开启1项 ⊘ 'unix_socket_input'正常 存储状态 S存储状态: yellow 服务状态 ✓ 核心服务:正常,服务启动时间 2020-01-09 15:19:52 重启服务 ☑ 后台服务:正常,服务启动时间 2019-12-25 16:44:12 重启服务 ◎ 流量分析服务:正常,服务启动时间 2019-12-25 11:23:27 重启服务 交存储服务:正常,服务启动时间2019-10-1516:30:25 重启服务 • 文件引擎: 启动中 重启服务 查看日志 ♥ web服务器:正常,服务启动时间 2019-12-25 11:41:11 重启服务 ⊘数据库:正常,服务启动时间 2019-10-15 16:30:19 重启服务 බ速缓存:正常,服务启动时间 2019-10-15 16:30:19 重启服务 云端连接 ⊘ https://static.threatbook.cn连接正常 ⊘ https://static-img.threatbook.cn连接正常

页面路径:

1.从导航菜单进入监控页面

2.选择"监控-系统运行状态"子菜单项

系统运行状态页面,为用户展示 TDP 当前的运行状态以及关键的系统指标,帮助 用户检测 TDP 运行情况,如有异常快速定位原因。

【运行状态】模块在用户进入此页面后, 自动进行系统诊断, 诊断后会告知用户诊

断结果,用户也可以手动点击"重新诊断"按钮重测。

运行状态页面会测试以下内容:

系统状态:检测系统状态,展示健康度

系统启动时间

IOC 是否更新

云端连接状态:是否连接正常

硬件状态: CPU、内存、磁盘

输入模块状态

存储状态: ES 存储状态

服务状态:如果遇到某些服务异常,可以尝试手动重启

【CPU 使用率】展示了 CPU 实时使用率以及近 72 小时内的 CPU 使用情况,用户 遇到异常可以查看 CPU 实时使用情况做异常排除,三天内故障可以通过 72 小时使用 率进行 CPU 异常状况排查。

【内存使用率】展示了内存实时使用率以及近 72 小时内的内存使用情况,用户遇 到异常可以查看内存实时使用情况做异常排除,三天内故障可以通过 72 小时使用率进 行内存异常状况排查。

【磁盘使用率】展示了磁盘实时使用率,用户遇到异常可以查看磁盘实时使用情况 做异常排除。

【实时网卡流量】展示了所有网口的 FLOW 和 PACKET 的实时流量状况,可以通过下拉菜单切换网卡查看。

【历史网卡流量】展示了所有网口的 FLOW 和 PACKET 的历史流量状况,可以通过下拉菜单切换网卡查看,时间范围可以通过时间控件进行调整。

【实时处理量】展示了 TDP 的实时处理量,用户查看此模块可以初步判断系统处理流程是否正常。

【历史处理量】展示了 TDP 近 3 天内, TDP 对各个协议的解析趋势。

【输入模块】展示了系统的主要输入模块状态,数据为每 24 小时累计值,每 10 分钟更新一次。

【检测模块】展示了系统的主要检测模块状态,数据为每 24 小时累计值,每 10 分钟更新一次。

【输出模块】展示了系统的主要输出模块状态,数据为每 24 小时累计值,每 10 分钟更新一次。

二、威胁

威胁模块在威胁的视角,为用户展示当前系统的威胁事件以及告警主机,同时提供 处置建议和处理流程。告警主机以主机的维度展示当前系统告警,并且提高主机处置功 能;威胁事件分为外部攻击、内部攻击、失陷破坏以及智能聚合。接下来做详细说明:

2.1 外部攻击

2.1.1 外部攻击列表

页面路径:

1.从导航菜单进入威胁页面(登录系统默认来到此页面)

2.选择"威胁-外部攻击"子菜单项 , 来到外部攻击页面

威胁 > 威胁事件 >	外部攻击						
 筛选:7天-全部	3			主机IP/名称/域名/	/告警名称/目标	示地址	搜索
严重性分布		攻击成功占比		TOP攻击者			
	17起	 严重:3 高:1 中:4 近:9 (孤息:0 	 ● 攻击成功: 0 ● 攻击失致: 0 ● 攻击未知: 0 	36.103.255.6 103.58.151.9 42.123.75.18 119.28.13.70 110.53.247.1	MyS NO SQL NO SQL NO SQL NO SQL NO SQL		405 304 304 301 300
时间	严重级别	威胁事件	告警主机	攻击IP	检出次数	攻击成功次数	操作
2019/09/23 10:11:29	▲ 产重	连接远控地址 :菜刀webshell列目录行为 连接菜刀webshell列目录行为远控地址192.168.100.171/909kk.php	all_list[共1台] 已处理	70.127.242.253	2	2	查看详情
2019/09/23 10:11:28	▲ 产重	连接远控地址 :菜刀webshell虚拟终端执行命令 连接菜刀webshell虚拟终端执行命令远控地址:192.168.100.171/909kk.php	all_list [共1台] 未处理	70.127.242.253	4	4	查看详情
2019/09/23 10:11:29	▲ 产重	连接运控地址 : 菜刀初始连接成功 连接菜刀初始连接成功远控地址:192.168.100.171/909kk.php	all_list[共1台] 未处理	70.127.242.253	2	2	查看详情
2019/09/23 11:56:33	高	漏洞利用: MySQL注入 针对192.168.100.175:9070/sqli-labs/less-5/的MySQL注入攻击行为	内部测试[共2台] 未处理	220.121.97.43[共70个]	2459	667	查看详情
2019/09/23 11:56:22	▲ 中	漏洞利用: 测试 SQL注入漏洞 针对192.168.100.175:9070/sqli-labs/less-5/的测试SQL注入漏洞攻击行为	内部测试[共2台] 未处理	186.215.89.210[共70 个]	726	0	童看详情
2019/09/23 11:55:32	▲ 中	漏洞利用: MSSQL注入 针对192.168.100.175:9070/sqli-labs/less-5/的MSSQL注入攻击行为	内部测试 [共1台] 未处理	220.121.97.43[共68个]	1710	0	查看详情

【严重性分布】TDP 对所选时间范围内的所有外部攻击事件,统计事件严重程度分布情况。

【攻击成功】TDP 对所选时间范围内的所有外部攻击事件,统计攻击成功、攻击结 果未知和攻击失败的比例。 【TOP 攻击者】TDP 将所选时间范围内,所有的外部攻击事件涉及到的攻击者, 根据告警次数做了排列,展示攻击最为频繁的攻击者。

【筛选功能】TDP 支持对外部攻击列表做多种筛选,包括以下条件:时间范围、严重级别、是否攻击成功。

【搜索功能】支持根据主机 IP、主机名称、域名、告警名称和目标地址进行搜索。

【外部攻击列表】列表中展示包括以下内容:事件中最近一次攻击的告警时间、严 重级别、攻击阶段、攻击名称、告警主机、攻击 IP、事件中告警检出次数、攻击成功次 数。

2.1.2 外部攻击详情页

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-外部攻击"子菜单项 , 点击对应的威胁事件列表中, 对应威胁的"查 看详情"按钮; 来到此威胁事件详情页面。

< 返回外部攻击												
高外部政	は 古 清 に 記 書: 22	<mark>洞利用: N</mark> 20.121.97.43	lySC §共72	2L注入 ?个攻击方 및 告讐主机	: 192.168.100.175		量早发现时间: 2019-09-19 15:16:08 最近发现时间: 2019-09-23 11:56:33	已处理:0台 未处理:4台				
威胁概况 威胁发现(70) 主机(4) 外部攻击IP 取证结果(28)												
内网主机: 所有4台主机 检出明细 翻		结果判 全部	定:	要攻击地3 ▼ 清输入	<u>#</u> :	筛选 导出						
攻击者(70)				时间	严重级别	检出	内网主机	目标地址				
搜索IP		Q	×	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				
103.233.156.168 印度尼西亚·印度尼西	攻击 38	成功 11	•	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				
103.233.156.58 印度尼西亚·印度尼西	攻击 37	成功 9	•	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				
103.58.151.45 泰国·泰国	攻击 33	成功 9	Þ	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				
103.58.151.90 泰国·泰国	攻击 39	成功 13	×	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqii-labs/less-5/				
107.183.23.82 美国·加利福尼亚州·淮	攻击 ⊪34	成功 7	Þ	2019/09/1915:58:15	▲ 中	MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				
110.53.247.101	攻击	成功		2019/09/1915:58:16	A	攻击成功 MySQL注入	192.168.100.175	192.168.100.175:9070/sqli-labs/less-5/				

在详情页开头,系统以卡片展示对应威胁事件的主要信息,包括:严重程度、威胁 名称、攻击者数量、受害者数量、告警最早发现时间、告警最近发现时间、已处理主机 个数、未处理主机个数。 在详情页面中,系统通过以下角度描述威胁事件:

威胁发现

点击"威胁发现"TAB,来到威胁发现模块:

在威胁发现模块,系统对所选的外部攻击事件,展示具体的告警信息,帮助用户溯 源追踪。包括以下功能:

【筛选与导出】可以根据内网主机、结果进行筛选,并且筛选后的结果进行导出。

【检出明细】点击"检出明细+"按钮可以展示此威胁事件的告警趋势图。

【攻击者列表】系统将次事件中涉及到的攻击者列出,用户点击具体的攻击者 IP,可以查看此攻击 IP 之下的具体告警。

【告警详情】用户点击攻击者列表中的具体 IP,可以看到此攻击 IP 的告警信息, 每一条告警信息卡片中包括以下内容:告警事件、检出信息(攻击阶段、攻击类型、威 胁名称、威胁描述)、内网主机、目标地址。告警信息卡片可以通过点击展开,展开后依 次展示攻击示意图、攻击信息、原始请求日志以及 PCAP 包。这四种信息对于不同的协 议,包含的内容不同,如有缺某一项为正常现象。

点击其中的"全屏显示"按钮,用户可以全屏查看协议内容。

主机

【主机】模块展示此攻击事件涉及到的具体主机,主要信息有:内网主机 IP、资产 名称、关联域名、主机的当前威胁检出次数、最近一次检出事件,用户可以在此模块对 已经处理的主机,做"已处理"标记。

用户点击"导出"按钮,可以导出此事件相关的所有主机 IP。

外部攻击 IP

【外部攻击 IP】模块展示此攻击事件涉及到的外部攻击 IP, 主要信息有:外部攻击 IP、地理位置、IP 相关的微步情报标签、外部攻击 IP 相关的当前威胁检出次数、最近一次告警检出时间。

用户点击"导出当前表格"按钮,可以导出此事件相关的所有外部攻击 IP。

终端取证结果

展示对应威胁事件已安装的 Agent 的终端取证结果。

2.2 内网渗透

2.2.1 内网渗透列表

页面路径:

1.从导航菜单进入监控页面(登录系统默认来到此页面)

2.选择"威胁-内网渗透"子菜单项 , 来到内部攻击事件页面。

	监控	49	资产&风险 调查 报告 平台管理			٠	. .) tdp [胡出]
估量主机	■ 成协 > 成协事件 > p	1999 M						
□1 告誓主机	冒 筛选:7天-全部				主机IP/名称/域名/告警名和	1/目标地址		投釈
NURAD 章 智能聚合 成功平年 	严重性分子		1.00 - 1.	192148.100.118 192148.100.118 192148.100.118 192148.000.118 192148.000.775 192148.00.775 192148.100.775	=			1196 1177 478 471 388
🛞 失陷破坏	83(4)	严重级别	威胁事件		告誉主机	检出次数	19/7	
	2019/11/13 23:01:28	a A	建國政告:建立通信課題 展现內局傳過行为:建立通信課題:192.168.77.250		192.168.77.250(11-test1) [共11台] 未处理	40	26	i¥tA
	2019/11/13 23:03:05	n R	建國政告: 渗透改合 就现内局渗透行为:渗透改合: 192. 168. 100. 99.8080/users		10.10.51.2(幺幺零网段)[共7台] 未处理	884	20	i¥!A
	2019/11/13 20:06:32	a A	連進政告: MSSQLIE入 就说內能傳告行为; MSSQLIE入:192.168.100.175:90701sql+labs/fess-5/		192.168.100.175[共4台] 已处理	141	26	ivea.
	2019/11/13 20:06:31	<mark>е</mark> ж	建國政告: MyGQLE入 建筑均能使进行为:MyGQLE入:192.168.100.175:90701xgl-labs/fess-5/		192.168.100.116[共4台] 未处理	212	26	i¥1A
	2019/11/13 20:06:32	R R	連進改善: SQLMAP 发现內和達通行为:SQLMAP:192.168.100.175:S0701sgHabs/tess-5/		192.168.100.116[共4台] 未处理	1630	26	syna
	2019/11/13 20:06:30	a A	建造 表击: 到达SQL往入 账 到 发现内闲穿进行为完议ESQL证入账税:192.108.100.175:9070/sql-labs/tes		192.168.100.116(192)(共4台) 未处理	83	24	i¥M
	2019/11/13 23:01:23	<mark>.</mark> Ж	建造 造合:Redin未提权提到利用 发现内间穿进行为内edis未提权展到利用 192.168.88.74		192.168.88.74(192)(共1台) 未处理	4	20	i¥1A
授权给:微步在线内	2019/11/13 23:03:04	<mark>.</mark> Ф	建造改造: 扫描系帯WebhetE行 发现内局事造行为:扫描系帯WebhetE行□xphdyy.on/statiofmages/axis.jpp		192.168.100.116[共5分] 未处理	160	26	i¥tA
的职位2 内部期间	2019/11/13 20:00:34	0 4	/// 建造改造: MSSQL/接续 发现内局协选行为:MSSQL/接续:192.168.100.116		192.168.100.116(192)[共2台] 未处理	60	26	i¥1A

【严重性分布图】TDP 对所选时间范围内的所有内网渗透事件,统计事件严重程度 分布情况。

【TOP 受攻击内网主机图】TDP 将所选时间范围内,所有受到内部攻击的内网主机,根据告警次数做了排列,展示攻击最为频繁的内网主机。

【筛选功能】TDP 支持对内网渗透列表做多种筛选,包括以下条件:时间范围、严重级别、是否攻击成功。

【搜索功能】同时支持根据主机 IP、名称、域名、告警名称和目标地址进行搜索。

【内部攻击事件列表】展示了内部攻击事件的基本信息,包括:事件中最近告警的 时间、严重级别、事件名称、告警主机、检出告警次数。点击"查看详情"按钮,用户 来到内部攻击详情页面。

2.2.2 内网渗透详情页

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-内网渗透"子菜单项 , 点击威胁列表中威胁的"查看详情"按钮, 来到威胁事件详情页面。

< 返回内部攻击												
A /*=	▶								最早发现时间: 2019-0 最近发现时间: 2019-0	09-11 19:04:53 09-11 19:52:58	已处理:0台 未处理:3台	
威胁极况	威胁发现(3)	主机(3) 耳	双证结果(1)									
83(N):	/09 15:1~ 2019/0	9/16 15x	告豐主机: 所有3台主机	-	IOC: 所有0个地址	•						85 95
						h,检出和	県組 ~					
		威胁行为	内	用主机	检出次数							
- A	发现域控攻 账户非法提;	击行为:MS14068 Attac 权	k:192.168.100.141 18	2.168.100.143	2	0 2次攻击成功	[2019-09-1	1 19:52:58] 发现域控攻	击行为:MS14068 Attack	:192.168.100.141		
89(4)		못型	协议 行为描述									
2019-09-11 19	2.52.58	洗量	TCP 账户参法制	权 政告成功			1	+ 모		发出晚形请求		Δ
2019-09-11 19	0.07:09	沈嚴	TCP B/P BibB	权 取击成功			未知用户	192.168.100.143				192.168.100.141
• A	发現域控攻 取户非法提	击行为:MS14068 Attac 权	x:192.168.100.141 19	2.168.100.143	1	① 1次攻击成功	行为					
• 🔺	发现域控攻: 账户非法提	出行为:MS14068 Attac 权	k:192.168.100.141 19	2.168.100.143	1	1次攻击成功		主机名称: 源印地址:	192.168.100.143 192.168.100.143			
							тср	源端口: 目的IP地址: 目的第口: Mac地址: 请求长盘 关UIIOC:	54073 192.168.100.141 88			

在详情页开头,系统以卡片展示对应内网渗透事件的主要信息,包括:严重程度、 威胁名称、告警主机、告警最早发现时间、告警最近发现时间、已处理主机个数、未处 理主机个数。

在详情页面中,系统通过以下角度描述威胁事件:

威胁发现

在威胁发现模块,系统对所选的内网渗透事件,展示相关的告警信息,包括以下信息:

【筛选】可以根据时间、告警主机进行筛选。

【检出明细】点击"检出明细"按钮可以展示此威胁事件的告警趋势图。

【告警列表】展示了内网渗透具体告警的严重级别、威胁行为描述、内网告警主机 以及检出次数和成功次数。

【告警详情】用户点击攻击者列表进行展开,可以具体的告警信息,每一条告警展 开后依次展示攻击示意图、攻击概况、原始请求日志以及 PCAP 包。这四种信息,对于 不同的协议,包含的内容不同,如有缺某一项为正常现象。

主机

【主机】模块展示此攻击事件涉及到的具体主机,主要信息有:内网主机 IP、资产 名称、关联域名、主机的当前威胁检出次数、最近一次检出时间,用户可以在此模块对 已经处理的主机,做"已处理"标记。

用户点击"导出"按钮,可以导出此事件相关的所有主机 IP。

终端取证结果

展示对应威胁事件中,已安装的 Agent 的终端取证结果。

2.3 失陷破坏

威胁中的失陷破坏功能模块,展示了系统内部已经被病毒木马感染,导致访问恶意 地址的威胁事件,以及主机已经被攻击者攻陷并且开始向外发起攻击的威胁事件。

2.3.1 失陷破坏事件列表

使用方法:

1.从导航菜单进入威胁页面(登录系统默认来到此页面)

2.选择"威胁-失陷破坏"子菜单项 , 来到失陷破坏威胁事件详情页面。

5 1 2

2019-09-10 20:56:42 副始清史 进程法面

Ramnitus

TDP



告營主机							
严重性分布		威胁类别占比		连接的恶意地址			
	9,838 16582	 ● 「重:9751 ● 第:1027 ● 4:163 ● 低:5302 ● 低:5302 ● 低:8:376 	控整": 376 900 (1) 6 809 (1) 7 92 (1) 10 159 95 (1) 7	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		6305호 1799호 904호 772호 468호	
翌 7天-全部					主机IP/名称/城名/告警名称	/目标地址	搜索
时间	严重级别	威胁事件			告誓主机	检出次数	操作
2019/09/11 19:51:47	▲ 戸重	裁制:BiackTech团伙 连接BiackTech团伙记控地让linenews.mypicture.info.4430000/a239732446.asp			10.10.51.2共16台 未处理	508	查看详情
2019/09/12 16:20:04	▲	投制:海连花运行 连接着连花运行运动地上AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA			xtm 共16台 未处理	9213	查看详情
2019/09/11 16:54:44	▲	控制: 连接其他话控地址:btc2agc.com/			xtm 共2台 未处理	16	查看详情
2019/09/11 16:54:44	▲	控制: Biter/IE仪 连接Biter/IE仪记忆出wonsservice.dom.net/			xtm 共2台 未处理	21	查看详情
2019/09/11 19:52:58	▲ ≓∎	內國參還: MS14068 Attack 累現種腔改善行为-MS14068 Attack: 192.168.100.141			JIMR共1台 未处理	1	查看详情
2019/09/12 14:35:41	▲高	控制: Ramnit鏡虫 连接Fannit鏡虫送的地上fpet-career.com/			10.10.10.2共23台 未处理	997	查看详情
2019/09/12 18:13:08	▲高	國政利用:MyGQLE入 针对192:168.100.175590701xgl=labs/kes-5/0/MySQLE入发击行为			内部測试 共1台 未处理	25	查看详情
2019/09/11 16:54:37	<u>▲</u> ₽	控制:Bulehano控扩展负 连接Bulehano控扩展负载负达把动让fid.hognoob.se			xtm 具2台 未处理	7	查看详情
2019/09/11 16:54:37	▲ ₽	控制: Ntol進F1同時 注接Ntol進F1同時活动地にshinagov.8800.org/			xtm 共2台 未处理	12	查看详情

【严重性分布】TDP 对所选时间范围内的所有失陷破坏事件,统计事件严重程度分布情况。

【威胁类别占比】TDP 将所选时间范围内,所有失陷破坏事件的威胁类型占比, 进行统计,用户可以直观看到失陷破坏事件中的主要威胁类型。

【连接的恶意地址】TDP 将所选时间范围内,对所有失陷破坏事件向外连接的恶意地址进行统计,用户可以直观看到失陷破坏事件中的主要恶意地址。

【筛选功能】TDP 支持对失陷破坏列表做多种筛选,包括以下条件:时间范围、严重级别、近看攻击成功。

【搜索功能】TDP 支持根据主机 IP、主机名称、域名、告警名称和恶意目标地址 对失陷破坏事件进行搜索。

2.3.2 失陷破坏详情页

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-失陷破坏"子菜单项,点击威胁列表中对应威胁事件的"查看详情"按钮,来到失陷破坏威胁事件详情页面。

在详情页开头,系统以卡片展示对应失陷破坏事件的主要信息,包括:严重程度、 威胁名称、告警主机数量、告警最早发现时间、告警最近发现时间、已处理主机数、未 处理主机数。

《返回失期破坏												
	1010年 连接远控 主机: 192.166.76.126	地址:海道花日 8月17日主机	影俠						最早放现时间: 2019-11-06 11:34:37 最近批现时间: 2019-11-14 11:43:41	已处理	: Off : 17日	
就動概况 或動发	(現(221) 主机	(17) IOC	取证结果(2)									
#2ML:		合党主机:		IOC:								
2019/11/07 12:0 -	-2019/11/14 12:0	用有26份出现	• 1	所有4个地址	718 0 ±							
检出明细 🖬												
			威胁行为			内湖主机			检出次数			
• <mark>····································</mark>	W直花图仪送程地址:AA			AAAFSc.z.teriava.com		192.168.76	.126(11-test1)		600			
时间	关型	1912	行力描述				12019-11-11 16-	-36-531 (E18/8)	₩250000元均hhi->>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		AAAAFSc z teri	ava com
2019-11-11 16:35:53	沈麗	DNS意识	家主成功				[k010-11-11 10.	Sound Transi	E IVER IN REFERENCES			上一个 下一个
2019-11-11 16:35:53	沈麗	DNS 資河	攻击成功						DN5 53			CEV.
2019-11-11 16:35:53 2019-11-11 16:35:53	7.8 7.8	DNSER DNSER	发击成功 政击成功				192.188.76.126(11 -tost1)		DNS 53 重兆			
2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53	28 28 28	DNSER DNSER DNSER	友告成功 文告成功 文告成功				192.168.76.126(11 -test1)	王机名称:	DNS 53 重攻 11-est1	62	海道花活伙	
2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53	次章 沈章 沈章 沈章	DNSER DNSER DNSER	 次き成功 次き成功 次き成功 次き成功 				192.166.76.126(11 -test1)	主机名称: DNS根务提P:	DNS 53 19/8 11-6651 8.8.8.9	标签: DNS报务表演:D	海道花活休 53	
2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53	7.8 7.8 7.8 7.8	DNS登词 DNS登词 DNS登词 DNS登词	家 告成功 家 告成功 家 告成功 家 告成功				192.166.76.126(11 -test1)	主机名称: DNS报务器P: 内段主机P: MacMitti	DNS 53 2012 11-6621 182:56 75 126	632: DNS服务器構立: 内向主利法の 室の系型:	海西花出伏 53 1172 NULL	
2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53 2019-11-11 16:35:53	28 28 28 28 28 28	DNSER DNSER DNSER DNSER DNSER	 末金成功 末金成功 末金成功 末金成功 末金成功 末金成功 				192.168.76.128(11 -text1)	主机名称: DNS服务器(P) 内阁主机(P) Mac地址: 查询唱名:	DNS 33 2013 88.8.8 192 105.76 125	标签: DNS报务获储口: 内间主机建口: 室间共型: 室间结果:	用意花活伏 53 1172 NULL NXDOMAIN	
2019-11-11 16:36:53 2019-11-11 16:36:53 2019-11-11 16:36:53 2019-11-11 16:36:53 2019-11-11 16:36:53 2019-11-11 16:36:53	28 78 78 78 78 78 78 78	DNSER DNSER DNSER DNSER DNSER DNSER	 次主成で、 次主成で、 次主成で、 次主成で、 次主成で、 次主成で、 次主成で、 次主成で、 				192.168.76.128(11 -text1) DNS±39	主机系称: DNS级务器P: 内网主机P: 内码主机P: 量均可名: 关联IOC:	2048.53 257 11-641 8.8.85 192-164.76 105 204904.007 2.04904.007	标题: DNS服务器调급: 介闲主机通口: 室闲纸箱: 室内纸箱:	海底花出休 53 1172 NULL NKDOMAN	
2018-11-11 16:36:53	28 28 28 28 28 28 28 28 28	DNSER DNSER DNSER DNSER DNSER DNSER	2002 2002 2002 2002 2002 2002 2002 200				1122.168.76.126(11 -test1) DNS 9210	主机名称: DNS级务组中 内向主机中 Mac地址 室向相名 关联IOC:	2016 33 2017 8.8.6.6 102:10:17:12:10 2.001/0:12:00 2.001/0:10:00 2.001/0:10:00	标至: DNS服务器编记: 方列支机编口: 室间关型: 室间结果:	周期花譜的K 53 1172 NKL NKDOMAN	PCAPT-18
2016-11-11 16:36:33 2016-11-11 16:36:33 2016-11-11 16:36:53 2016-11-11 16:36:53 2016-11-11 16:36:53 2016-11-11 16:36:53	28 28 28 28 28 28 28 28 28	DNS분명 DNS분명 DNS분명 DNS분명 DNS분명 DNS분明 DNS분明 DNS분明 DNS분明	2002 2002 2002 2002 2002 2002 2002 200	5			192.161.76.135(11 4631) DNSER	主机系称: DNS服务器P: 内局主机P: Mac物址 查询端系 关键IOC: 3 18:07:19 TCP 192	2016 33 2017 11-0451 8.8.6 110:167/102 2.00704 000 100:102 17/102 100:102 17/102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:102 100:1	65至 DNS編表器編口: 內與主机編口: 童術典型: 童術典型: 童術紙集:	周期電話的 53 1172 NKDCMAN	PCAPTE

在详情页面中,系统通过以下角度描述失陷破坏威胁事件:

威胁发现

TDP

在威胁发现模块,系统对所选的失陷破坏事件,展示具体的告警信息,包括以下信息:

【筛选】可以根据告警主机、IOC 进行筛选。

【告警趋势】点击"检出明细"按钮可以展示此威胁事件的告警分图。

【告警列表】展示了失陷破坏的告警主机,以及具体告警的基本信息,包括:告警 主机、严重程度、威胁描述、检出次数和联通次数。

【告警详情】用户点击攻击者列表进行展开,可以具体的告警信息,每一条告警展 开后依次展示攻击示意图、攻击信息、原始请求日志以及 PCAP 包。这四种信息,不同 的协议,包含的内容不同,如有缺某一项为正常现象。

主机

【主机】模块展示此失陷破坏威胁事件涉及到的具体主机,主要信息有:内网主机 IP、资产名称、关联域名、主机的当前威胁检出次数、最近一次检出时间,用户可以在 此模块对已经处理的主机,做"已处理"标记。



用户点击"导出"按钮,可以导出此事件相关的所有主机 IP。

幺幺零网段

IOC

此模块展示此攻击事件涉及到的 IOC。主要信息有:严重级别、IOC、微步标签、 关联事件。

130

终端取证结果

10.10.221.8

展示对应威胁事件中,根据已安装的 Agent 的终端取证结果。

2.4 智能聚合

智能聚合功能会以攻击者角度,将不同的攻击者发起的攻击进行归纳和汇总,以时间线的形式呈现出来。这样用户可以清晰的看到,攻击者在什么时间,使用什么攻击方式,对哪些内网资产进行了攻击,产生了哪些危害。有利于用户对攻击者、受害主机以及失陷环节进行清晰的排查。

使用方法:

1.从导航菜单进入威胁页面(登录系统默认来到此页面)

2.选择"威胁-智能聚合"子菜单项 , 来到智能聚合页面。

威胁 > 智能聚合									2020/01/	07 00:0 ~2	020/01/13 18:0
 ⑦筛选:全部							攻击IP/普	·警主机IP/攻	击手法/攻击工具/	事件ID	搜索
事件列表(共23起) 综合排序 时间排序 【攻击成功 【夹股 】攻击未知	A	来自中国·汈 [事件ID:46e703	E苏·常州6 2b14138c70	1.160.24 eb08b3ab7c	7.70的排 333f4d8-	空制攻击 2020 1578896485]	0/01/13 14:21 - 2 別日受行为 算)	020/01/13 15:42 口初始连接成功	2 通过 phpmyadmin F	志oetshell	
(严重) 61.160.247.70攻击IP 1小时前 ■ 来自中国·江苏·常州,持续1小时21分钟	严重	b374k Webshell 猜测管理后台	连接成功 端 探测是否存在	口扫描 扫描 phpMyAdmin	黑客Webs 爆破敏感	hell后门 MySQL 文件 扫描黑客W	注入 测试SQL /ebshell后门(bas	注入漏洞 /etc/ e64传输)	passwd尝试 猜解制	效感文件	服後备份文件
abpts履道初始化成功 算刀websheli虚拟结婚执行命令 算刀websheli列目最行为 算刀初始違接成功 通过phpmyadmin日志getshell b374k Websheli连接成功	事件详 热力图 ^{立 凌晨}	情							访问 敏感行	为 📕 攻击	F 🔽 攻击成功
[严重] 70.127.242.253攻击IP 1小时前 ■ 来自美国·佛罗里达州·坦帕,持续1小时8分钟	下午	周末	工作日	周末	工作日	周末	工作日	周末	工作日	周末	▶ 工作日
菜刀webshell虛拟終端执行命令 菜刀webshell列目录行为 菜刀初始连接成功	攻击成功	2019/12/1	5 2019/12/16		2019/	12/23	2019/12/3	80	2020/01/06		2020/01/13
[严重] 61.160.247.70攻击IP 01/07 ■ 来自中国:江苏·常州,持续8小时28分钟	abptts	隧道初始化成功 [1台主机]	b374k	Webshell连接 [1台主机]	成功	菜刀webshell] [1台主	列目录行为 机]	菜刀webshe [副盧拟终端执行命令 1台主机]		
abpits隧道初始化成功 算刀webshell列目录行为 算刀初始连接成功	菜刀初 [1	始连接成功 台主机]	通过phpmy	<mark>/admin日志ge</mark> [1台主机]	tshell						
	where the star of	-									

2.4.1 攻击事件列表

智能聚合页面左侧,列出目前检测到的所有攻击事件,点击对应的攻击事件卡片,可以切换事件详情内容。

攻击事件列表支持以下功能:

【筛选功能】TDP 支持对智能聚合的列表做多种筛选,包括以下条件:时间、严重级别、攻击结果、攻击阶段、支持查看针对性攻击,同时支持对:攻击 IP、告警主机 IP、攻击手法、攻击工具以及事件 ID 的搜索。

攻击事件列表中展示以下内容:

统计事件的总数,并支持综合排序以及按照事件中最新攻击时间排序。

卡片展示包括的字段有:严重程度、攻击 IP、最新一次攻击时间、攻击来源地理位置、持续时间、攻击结果分布(攻击成功、失败、攻击未知)、以及成功的攻击手法。

2.4.2 攻击事件详情

用户可以通过点击攻击事件列表中的事件卡片,进行攻击事件详情切换。

攻击事件详情展示以下内容:

【事件详情卡片】: 展示了当前事件的攻击来源,攻击 IP,事件 ID,以及攻击的手法,红色为成功攻击。

八日日間間に DangKok 100.00.101.3守240 日が開内刊用火山 2019/11/14/09:53-2019/11/14	11:32									
▲ [事件ID:8c6b0016469ee96fabd3f34340f355f4-1573696388]	[事件ID:8c6b0016469ee96fabd3f34340f355f4-1573696388]									
SQLMAP MySQL注入 MSSQL注入 测试SQL注入漏洞 /etc/passwd尝试 尝试XSS漏洞 XSS尝试										

【热力图】根据系统检测到的本事件持续时间,在这一事件范围内绘制热力图,帮助用户判断此攻击事件的概况。

热力图						ii	前问 📃 敏感行为) 📕 攻击 📘	攻击成功
 >> 凌晨 上午 下午 C 晩上 	工作日 周末	工作日	周末	工作日	周末	工作日	周末	工作日	
	2019/10/17	2019/10/21		2019/10/28		2019/11/04		2019/11/11	

从攻击的有效性角度,热力图将事件中的告警,分为访问、敏感行为、攻击和攻击 成功四种类型,用户可以直观的查看在过去 30 天内,攻击者的持续访问时间、攻击节 奏以及成功攻击的时间点;

从攻击节奏的角度,热力绘制过去 30 天的告警,并将每天分为凌晨 (0-6 点)、上午 (6-12 点)、下午 (12-18 点) 以及晚上 (18-24 点),并且以周的维度,区分工作日以及周末,用户可以根据攻击者的活跃时间段,攻击连续性,判断攻击行为是人还是机器,攻击者自身的作息以及所处的时区等信息。

【攻击成功】展示了此事件中,攻击成功的威胁名称,以及受影响的主机个数。



【攻击来源】展示了此事件中,攻击的来源,包括攻击 IP、攻击来源的地理位置、

活跃时间段

上午6-12时

微步情报、和攻击者的活跃时间段。

攻击来源 攻击IP

攻击来源 微步情报 70.127.242.253 United States-Florida-Saint Petersburg 暂无情报

【攻击结果】展示了此事件中,攻击结果的分布比例。

攻击结果

● 攻击成功: 11102
● 攻击失败: 0
😑 攻击未知: 76989

【TOP 受攻击域名】展示了此事件中,受攻击最多的域名。

TOP受攻击域名	攻击成功	┃ 失败	攻击未知				
xtm.threadbool					-		-
F _/ 1 \ 1-				_, ,	 <u> </u>	 ~ ~ -	

【攻击过程】TDP 智能聚合模块,将每个攻击 IP 的攻击行为,经过关联分析,以时 间线的形式展示攻击过程。

攻击过程 Ⅰ//型 Ⅰ高 Ⅰ 中 Ⅱ 低 Ⅱ 信息 ● ※ トロー 11/14 11/141	□ 仅看外部攻击 〔	🗌 仅看攻击成功
首次访问:192.168.100.171/909kk.php		
● 送上年 11/14 11:31:51 (總額)		
攻击:3 <mark>成物3</mark> 70.127.242.253 → 葉刀 webshell虚 拟终端执行命令 →→ 및 192.168.217.129	1	展开 ₩
● 些上午 11/14 11:31:51 (國際利用)		
攻击:13 70.127.242.253 →→ 扫描黑客Webshell后门 →→ 및 192.168.100.171	1	展开 ₹
● 坐上午 11/14 11:31:51 [國務利用]		
攻击:13 70.127.242.253 →→ 扫描黑客Webshell后门(base64传输) →→ 및 192.168.100.171	1	展开 ₹
 		
攻击:2 <mark>成功2</mark> 70.127.242.253 →→ 葉刀 webshe ll列目录行为 →→ 및1 192.168.217.129	1	展开 ₹
 		
攻击:2 成功2 70.127.242.253 → 葉刀初始连接成功 → 및 192.168.217.129	1	展开 ₩
————————————————————————————————————		
检出:1 및Ⅲ192.168.100.171 →→ 端口扫描 →→ 192.168.100.171		展开 ₹

首次访问:展示此攻击者的首次访问页面

威胁种类聚合:系统将相同的威胁聚合在一起展示,以时间线的形式呈现。用户 可以直观的看到在这一个事件中, 攻击者使用此威胁手法对某些目标发动了多少次攻击, 先后顺序如何,其中有哪些成功了。

威胁事件卡片展示了以下元素:

攻: ●	击过程	∎严重 ■高 11/14 11:31:	i ┃中 ┃低 Ⅱ6				□ 仅看外部攻击	□ 仅看攻击成3
	首次	次访问:1 92 .1	68.100.171/90	9kk.php				
•	些 上午	11/14 11:31:	51 [控制]					
	攻击	3 成功:3	70.127.242.	253 → 菜7	Jwebshell虚拟终端执行命令 ──→ 🖵 192.168.217.129			收起 ≜
	结果		源IP	目的IP	目标地址	最近一次活动时间	操作	
	攻击	成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	送上午 11/14 11:42:39	查看日	志
	攻击	成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	送上午 11/14 11:42:39	查看日	志
	攻击	成功	70.127.242.253	192.168.217.129	192.168.100.171/909kk.php	<u> 半</u> 上午 11/14 11:31:51	查看日	志

最近一次告警时间、威胁阶段(包括:侦查、漏洞利用、敏感行为、控制、内网渗透、对外攻击)、告警总次数、成功次数、攻击源、攻击名称、受害者。

支持快速筛选:可以快速筛选"仅看外部攻击"、"仅看攻击成功"。

告警详情:用户点击威胁种类卡片中的"展开"按钮,可以看到具体的告警条目, 包括的内容有:攻击结果、源 IP、目标 IP、目标地址、最近一次活动时间以及"查看日 志"的操作。

点击"查看日志"按钮,用户可以看到告警日志的具体信息,用户可以通过告警的 具体信息作进一步的判断和调查。

020/10/22 06:51:13[]通问利用]		
攻击:1 📷 102.165.30.33 → 測意Web目录 → 🖬 192.168.177.14		收起▲
< 返回 [10/22 06:51:13] 攻击者102.165.30.33对192.168.177.14进行了敏感操作30摄Web員象 成功		
洋烟信息 原始记录		
▲ 角唇信意		
(1):3 地別時前和日野的行力, 20主者可以利用之个特性認知。web日素下的文件(52018020036)		调我注意 白名单 添加回新
日志信息		记录时间:2020-10-22 06:51:13
*	HTTP 8081	. 🔳
102.165.30.33	刘筠Web目录	192.168.177.14
чтти		意味好容
第月7月2日 2015年3月3355029 電話 電話 電話 「日本19日1日1月1日日 二日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	Image: Section 2016 Image: Section 2017 Image: Section 2017 Image: Section 2017 URL 1161812.150.8081/ Image: Section 2017 Image: Section 2017	
	HIPAENS: 200	
102 原始报文信息		● 全屏显示
诸次包		9283
0 617 / MTP/1.1 Have: 1116112.1508081 User-Agenet: NetSystem/Research studies the availability of various services across the internet. Our website is netsystemsresearch.com		
通過包		收起
HTTP/112020K Dele: Wel 21 Oct 2020 225113 GMT Enerver: Assaul 22 A41 (Mindel OpenSSU/11.1c Centent Lynge: Mindenset=UTF-8 Centent Type: UniversityITF-8		

2.5 内网渗透分析

内网渗透分析功能,方便安全运营人员直观地了解所监控区域的内网渗透攻击行为, 聚合主机之间的攻击方向和攻击手法,清晰定位攻击来源和受影响的主机,能够全面掌 握内网渗透威胁态势。

2.5.1 内网渗透分析概览

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-内网渗透分析"子菜单项,来到内网渗透分析页面。



【筛选功能】TDP 支持对内网渗透的发起方、攻击手法、以及受害主机, 做多种组合的筛选。同时支持筛选发起方、受害主机的资产类型。

【内网渗透时间卡片】TDP 将所有的内网渗透行为,按照渗透攻击名称进行聚合, 展示在左侧。用户点击对应的卡片,则会对概览图进行筛选。

【内网渗透概览】TDP 展示内网主机之间的攻击方向,以及具体的攻击手法。图中, 箭头的方向由攻击方指向受害方,箭头上会展示当前的攻击手法种类,如果只有一种, 则展示攻击手法名称。

【内网主机快速查看】用户将鼠标上移到某一台主机上, TDP 将会将与此主机无关的其他渗透行为模糊化, 高亮此主机, 以及与其相关的渗透行为, 便于用户查看单一主机的渗透行为。

ChreatBook 微步在线

【内网主机的数量限制】内网渗透概览图,默认不展示资产类型为"负载均衡"的 主机,同时会将展示的内网攻击主机控制在 30 之内。

2.5.2 内网渗透主机、事件详情

使用方法:

在内网渗透分析页面,点击希望进一步查看的主机,弹出主机详情,如果点击主机 详情中的具体事件,则会进一步展示对应的事件详情

在内网渗透分析页面,点击两主机之间的箭头,弹出内网渗透事件详情

攻击方: 192.168.7.81 服务器	1	高]Struts2远程代码执行 晶洞	受害方: 192.168 服务器	受害方: 192.168.5.225 服务器		■ 服务器 → 发起的攻击 < 遭受的攻击				
11 2020/01/15 00:0	~2020/02/13 0	01:0		检出次数:82	攻击方		攻击手法	受害方		
8			٨		<u>▲</u> 1 高 1	192.168.7.81	Struts2远程代码执行漏洞	192.168.5.22		
					高	192.168.7.84	Struts2远程代码执行漏洞	192.168.5.22		
0 2020/01/15 00:00:00	l.			2020/02/13 00:00:00	<u>▲</u> 高	192.168.7.67	使用net user命令 →	192.168.5.22		
时间	源主机	源端口	目的主机	目的端口	A	192 168 7 31	lcx端口映射	192 168 5 22		
2020/02/11 13:00:37	192.168.7.81	60126	192.168.5.225	445	高		·			
详细内容 JSON				下载JSON						
[2020-02-11 1 2.168.5.225	3:00:37] 发现	内网渗透行为:Str	ruts2远程代码打	执行漏洞:19						
		TCP 445								
모 -		TCP 445 Struts2远程代码执行漏3	a - 1	모						

【主机详情】点击任意一台主机,弹出主机详情弹层。展示主机相关的信息,包括 资产类型、主机 IP、资产名称,以及本主机发起的攻击或者遭受的攻击。如果主机被攻 击者攻击成功,或者连接恶意远控以及对外发起攻击,会将主机的颜色标红,并给出连 接,点击可以查看对应的主机详情。

【发起的攻击/遭受的攻击】系统按照攻击方向,将主机相关的内网渗透事件,分为主机发起的攻击,和主机遭受的攻击。列表中展示,攻击的攻击方 IP、攻击手法和受害方 IP。事件以严重程度进行排序。

【主机内网渗透事件详情】展示攻击方 IP、资产类型以及资产名称;攻击手法,以 及对应的严重等级;受害方 IP、资产类型以及资产名称。

【内网渗透事件趋势】展示了当前内网渗透事件的告警趋势,告警检出总次数。用 户可以自行调整时间,查看更大事件范围内的告警趋势。 【内网渗透事件具体告警】展示了对应的内网渗透事件具体告警信息。列表中展示了具体的告警时间、源主机 IP、源端口、目的主机 IP 和目的端口。点击对应的告警,可以查看告警详细内容。



2.6 告警主机

2.6.1 告警主机列表

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-告警主机"子菜单项 , 来到告警主机列表页面。

TDP

ChreatBook 微步在线

告答主机	┃ 告答主机					2020/10/16 00:00	0 ~ 2020/10/22 23:59
🚇 告警主机	全部业务组 ~	全部主机类型 🗸 🗸	主机IP/名称/	或名/告警名称/目标地址			Q
智能聚合	全部告警主机 ④ 508台	被外部攻击成) 〔11台	功 发起内 受 15g	网渗透 已失陷 会	APT 与远控踌躇立连接 WebSh 计 0台 4台 2台	II 挖矿 対外攻日 2台 31台	
② 内网渗透分析	⑦ 阶段手法:外部 告警主机(508)	咬击和投递/漏洞利用、访问	钓鱼页面、下载或传…	严重级别:全部 威胁性思	f: 全部 / 处置状态: 全部		✓ 下载主机列表
威胁事件	■ 严重级别 🜩	主机IP/资产属性	资产名称	主机威胁状态	检出威胁	最近告答时间 🔷	处置状态
■ 外部攻击 ∃ 内网渗透	▲ 严重	192.168.178.121 創 服務器	生产服务器	≫ 外部攻击或投递 受 内网渗透 膠 失陷	Cobalt Strik 连接MSSQL SQLMAP MySQL注入共24类吉蓉	10/22 14:58:29	1 未处理
5 失陷破坏		120.52.185.110 🗊 服务器	生产服务器	≫ 外部攻击或投递 ◎ 失陷	Cobalt Strik SQLMAP MySQL注入 通用SQL注入共43类告答	10/22 14:58:28	1 未处理
	□ ▲ 严重	192.168.178.116 回 服务器	生产服务器	> 医 失陷	Cobalt Strik	10/22 14:58:27	❶ 未处理
		192.168.178.54 🗐 服务器	生产服务器	> 失路	Cobalt Strik	10/22 14:58:27	😄 处理中
		192.168.178.79	生产服务器	型 内网渗透 网 生時	Cobalt Strik 木马 Trojan MySQL注入	10/22 14:58:27	1 未处理

【筛选功能】TDP 支持对告警主机做多种筛选,包括以下条件:时间范围、主机状态、资产类型和处置状态。

【搜索功能】同时支持根据主机 IP、名称、域名、告警名称以及目标地址进行搜索。

【告警主机】TDP 将所选时间范围内, 对应筛选条件的所有告警的内网主机, 根据 最近一次告警时间进行排序, 包含以下信息: 严重级别、主机 IP、域名/资产名称、主 机状态、检出威胁、最近告警时间以及处置状态。

2.6.2 告警主机详情页

使用方法:

1.从导航菜单进入威胁页面

2.选择"威胁-告警主机"子菜单项 , 点击对应的告警主机 IP , 来到告警主机详情页面。

< 返回告警主机								
A 192.168.178. ア重 服务器	54 资户	"名称 生产服务器 ළ_	所属业务组 未分组	处理状态 ○ 处理中 🖉				
威胁 威胁实体分	析 处理记录	Agent						
主机威胁状态 🕕						2020/10/16 00:00 ~	2020/10/22 23:59	
>)未適型外部攻击 该主机力速要年自互联网的攻击 ● 无角间渗透行为 来发现主机的内闭渗透行为 ● 正先期 该主机已采用。说明主机存在Webshell、或主机已振动恶雾恒乐、失用的主机会受到漂雾的控制。这 行抢矿、和素、伸展磁击、帮取数量、对外发起攻击等一系列思想行为。								
威胁事件列表 📀 已处理	!: 0 😄 处理中: 1 🚺 未3	出理:0 町 阶段手法	: 外部攻击和投递/)	電洞利用、访问钓鱼页面、下载或传 严重吸 别:::	全部 感動性质:全部	处置状态:全部 🗸 🗸	🕑 下數事件列表	
威胁事件	事件类型	事件性质		严重级别 🗢	最近发现时间 🜩	事件处理状态 🖨		
Cobalt Strike拦截清求(利 JQuery站点)	用 失陷破坏/连接远热	空地址 -		严重 1个外部地址	2020/10/22 15:07:20	⊖ 处理中 🖉	查看详情	

用户可以通过点击告警主机列表中的主机 IP,来到告警主机详情页。在详情页开 头,系统展示对应告警主机的主要信息,包括:严重程度、主机 IP、资产属性(服务器 或终端)、资产名称以及关联域名(可能无关联的域名)、所属业务组、处理状态。

在详情页面中,系统通过以下角度呈现告警主机相关信息:

威胁

TDP 在 "威胁" TAB 展示此告警主机相关的告警, 使用威胁名称进行聚合, 包含以下功能:

主机威胁状态:

主机威胁状态通过选定时间范围的威胁事件评估得出, 威胁状态分为外部攻击、 内网渗透、已失陷, 根据主机在特点的时间展示威胁的状态。

威胁事件列表:

TDP 按照威胁事件的方式,展示出每一个事件的详细信息,包括威胁事件名称、事件类型、事件性质、严重级别、管理实体、最近发现时间、事件处理状态。我们可以将 事件进行筛选来快速检索,同时也可以下载事件列表。

威胁事件详情:

操作方法:

1.从告警主机列表页面点击主机 IP 进入告警主机详情页面

2.选择一条威胁事件,点击列表中查看详情后可查看详细告警信息,详情页头部显示威胁事件名称、严重级别、事件类型、告警主机 IP、事件处理状态,下方显示威胁明细列表,展示该主机所有受到的威胁,该威胁包含时间、攻击 IP、威胁名称、严重级别、受攻击主机、协议、受攻击 URL、攻击结果,我们可以进行攻击结果及协议的筛选,也可以输入 IP 地址进行搜索,同时我们可以下载威胁明细进行内容查看。

3.点击威胁事件后,将显示该事件的详细信息,包含告警描述、示意图、行为描述 图、协议详情、PCAP 查看及下载以及原始记录,不同的协议类型,展示内容有所区别。

4.分析和处置是将威胁事件进行分析,从而进一步提升威胁用户的感知。

威胁实体分析

在威胁实体分析模块,系统对所选的告警主机遭受的外部威胁实体进行详细描述, 包括以三类:

【攻击成功的外部 IP】此模块展示了外部互联网侧攻击这一告警主机并且攻击成功的外部 IP, 展示信息包括以下内容:

外部攻击 IP:外部攻击的 IP 地址

地理位置:外部攻击 IP 的地理位置

IP 信誉标签:此外部攻击 IP 在微步情报库中的信誉标签

最近一次攻击时间:此外部 IP 攻击产生的的最近一次告警的时间

攻击手法和次数:展示了此外部 IP 攻击此告警主机的攻击手法以及次数

【攻击当前主机的内网 IP】展示内网中攻击当前主机的所有内网 IP, 展示信息包括 以下内容:

内网攻击 IP: 攻击此告警主机的内网 IP 地址

资产名称:此内网 IP 的资产名称

资产属性: 服务器或者主机

最近一次攻击时间:此内网主机攻击告警主机的最近一次告警时间

攻击手法和攻击次数:展示了此外部 IP 攻击此告警主机的攻击手法以及次数

【当前主机连接的 IOC】展示此告警主机连接的 IOC,展示信息包括以下内容:

IOC: 此告警主机的连接的 IOC 地址

严重级别: IOC 的严重级别

IOC 标签:此 IOC 在微步情报中的标签

最近一次连接时间:此内网主机攻击连接 IOC 的最近一次告警时间

连接次数:此内网主机攻击连接 IOC 的次数

操作:点击"查看详细内容"可以查看此 IOC 的详情。

处理记录

TDP 可以进行对告警主机的状态处理,进一步减少平台运营的人员的工作步骤,同时我 们也可以针对状态的修改进行主机处理的记录及查询。

处理记录将通过时间、告警主机、威胁事件、出质人、处理结果、备注及操作进行列表的展示,我们可以通过处理结果进行内容的筛选,同时我也可以选择事件,填写告警主机、威胁事件、经办人来进行内容的查询。

Agent

展示此告警主机的 Agent 的取证结果。

三、资产&风险

风险页面展示了 TDP 检测到的系统风险,包括登录风险、数据泄漏风险、API 风险和资产与服务。

3.1 登录风险

登录风险页面展示了系统检测到的登录风险,包括撞库风险和弱口令风险,具体功能如下:

3.1.1 弱口令

TDP 感動感知平台	监控 威胁	资产&风险	调查	报告 处置	平台管理	175主节点 🔻	微步在线内部测试 試用版	🔹 🌲 🙎
资产和服务	┃ 资产&风险 > 登录风险 > 弱口令					2021/	04/06 00:00 → 2021	/04/12 23:59 📋 🕯
	弱口令			登录入口弱口令类	型分布			
IPI 资产IP列表	弱口令是将相关登录入口的结果	1, 通过智能识别与弱口令			田中登号入口	關门会共计1卷 (基本)·		
🔊 域名资产	字典解析出含有關密码的内容服 方便对该内容进行查看及管理。	进行记录,通过列表展示						
登录风险								
▣ 登录入口								
合 弱口令	Q 输入用户名, 弱口令关键字查询	类型 全部	~	归属字典 全部	Ý	接口/URL 全部	Ŷ	◎ 蜀口令字典管理
								导出当前表格
数据泄漏风险	用户名 ③	弱口令	最新登录时	间	登录入口			所属字典
① 明文敏感信息	•	*****	2021/04/0	8 17:12:47	其他 192.168.100.12	1:8899/login.php 🎢		智能识别
	•		2021/04/0	8 17:09:29	其他 192.168.100.12	1:8899/login.php 🏓		智能识别
АРІ风险	•	*****	2021/04/0	8 17:07:02	其他 192.168.100.12	1:8899/login.php 🏓		智能识别
i API列表	<u>►</u>		2021/04/0	8 15:53:06	其他 192.168.100.12	1:8899/login.php 🏓		智能识别
			0004 (0.4.0		***			*

页面路径:

1.从导航菜单进入资产&风险页面

2. 选择"资产&风险-登录风险-弱口令"子菜单项,来到弱口令页面。

弱口令页面展示了 TDP 检测到的所有疑似使用弱密码登录的用户,具体展示如下 内容:

用户名、弱口令、最新登录时间、登录入口、所属字典。

弱口令页面支持以下功能:

【用户名搜索】可以根据用户用户名进行搜索。

【类型】可根据登录接口的类型进行筛选

【所属 API】默认展示所有登录 API 之下的使用弱密码的用户, 点击可以通过下拉菜单切换对应的 API, 可以根据 API 筛选所属的弱密码用户。

【弱口令字典管理】点击资产&风险>弱口令功能页面,点击弱口令管理进入该页面,进行弱口令字典的上传及管理。

3.1.2 登录入口

页面路径:

1.从导航菜单进入资产&风险页面

2. 选择"资产&风险-登录风险-登录接口"子菜单项,来到登录接口页面。

TDP 歳夢在城 威胁感知平台	监控	威胁	资产&风险	调查	报告	处置 平	P台管理	75主节点 🔻	微步在斜	讷部则试试用版	🗢 🖡 🙎
资产和服务	┃ 资产&风险 > 登录风路	会 > 登录入口	1					2	021/04/06 00:	00 2021/04	/12 23:59 📋
😂 全部服务	登录入口分类	用户行为	已忽略的登录								
IP 资产IP列表	登录入口分类		○ 登录地址/登录页面UI	RL/登录页面标题			对外开!	女 全部 是	未知 存在风险	全部 是 否	导出当前表格
👦 域名资产	▼ 🖳 WEB(4) 🚥	,	标题和登录地址		最近发现时间 ⇔	外部登录用户数 ≑	外部登录次数 ≑	内部登录用户数 ≑	内部登录次数 ≑	风险 🗘	操作
登录风险	CMS (0) 管理工具 (0)		要 ダ 192.168.100.1	121:8899/logi	2021/04/08 17:12:47	5	5	0	0	第二令	查看详情忽略 略
 □ 登录入口 □ 弱口令 	中间件 (0) 其他 (4) 🚳		要 <mark>選他</mark> & uums.xj.sgcc.	com.cn/porta	2021/04/06 13:53:52	0	0	1	1		查看详情 忽 略
数据泄漏风险	▼ 💽 远程登录(0) Telnet (0)		B 302 Moved T	其他 c.com.cn/isc	2021/04/06 13:53:39	0	0	1	1		查看详情 忽 略
 ① 明文敏感信息 ① 文件下载 	▼ 🛄 文件共享(3) FTP (3)		@ 10.218.15.30	其他 ′epm/login	2021/04/06 13:53:34	0	0	1	1		查看详情 忽 略
API风险 E API列表	▼ ● 数据库(1) MySQL (1) Redis (0) PostgreSQL (0)										
https://192.168.100.175/a	sset/serviceList ⁽¹⁾										

页面支持以下功能:

【筛选功能】可以根据登录地址、登录页面 URL、登录页面标题进行搜索

【WEB 登录配置登录规则】判断登录接口是否成功,需要用户自行配置登录成功规则。

用户点击"配置登录规则"按钮,来到登录成功规则配置页面。注意此处,用户可 以根据登录风险,状态码、内容长度、关键字以及 location 进行登录成功规则的配置, 配置完毕,点击保存即可生效。

TDP 成的感知平台 监控	成的 资产8风险 褐色	王建 报告 处望	E 平台管理 1757	18 <i>4</i> •			areinzen 🗤 🎰 🔋
< 返行登录入口							2021/04/06 00:00
王応 无标题 WEB d ⁹ 192.168.100.121:8899/fo	ginahp	最近%现时间 75 2021/04/08 17:12:47	19) 开放 豆根知道 〇 豊 (第四令)				
→ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	地理位置 金川 マ			登录风脸 全部 有风险	的登录 网络美型 全部网络		
登荣结束 金彦 成功 失敗 世社	余茂IP	用户名			R: 22		
TOP用户行为要型分析							Đ
登荣趋势 ┃ 应功 ┃ 失败 ┃ 尝试							E
5							
2021/04/06 09:00	2021/04/07 05:00		2021/04/08 18:00	202	21/04/10 03.00	2021/04/11 12:00	2021/04/12 23.00
登录用户数(5) 登录来源印地	向比(1) 其5次是委行为。查查明白						原土道新本格
登录用户名	来遵护地址	总量荣次数 ≑	量愛成功次数 ⇔	登景失败次数 ≑	做近一次量荣的问 ≑	量荣风险	操作
31323332323	19.168.60.73	1	1	0	2021/04/08 17:12:47	MD4	主 石洋信
5rWL6K+VdGV	19.168.60.73	1	1	0	2021/04/08 17:07:02	H □♦	里石洋情
6e6968616f	19.168.60.73	1	1	0	2021/04/08 15:53:06	第日や	25×6
E68588E8AF9	19.168.60.73	1	1	0	2021/04/08 17:09:29	第二令	五百冲骑
bdcadscbb	19.168.60.73	1	1	0	2021/04/08 15:51:11		医管冲器
		1	DF 3.1.1 20210409155730-013	5 Copyright 2020 微步视频, All I	Kights Reserved		

【登录详情页】用户可通过登录详情页查看该登录入口下所有登录行为及风险,支

持筛选

	近近 成功 資产を以上 荷白 ^{田田} 安告 化二 平台管理 1551万名。▼ おかついの形向は 1051万名。▼ おかついの形向は 1051万名。▼	🐟 🏨 🙁	
KIRGHITOP, SEMIST	###\$7021997/11/1313484, #5###2480.####6487#, 47#34###619##.	×	
资产和服务	1.97%A022 > 289%A2		Î
② 全部服务	登录入口分类 用户行为 己和能能要求入口		١
III 浙水中IP列北	ての理論の行う物理が影響		1
⑦ 城名窗产	10時作登記法 		l
	電磁電弧 「対応数 」 「対応数 」 「対応数 」 「対応数 」 「対応数 」 「対応 」 「対応数 」 「対応 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 」 「 」 「 」 「 」 「 」 「 」 」 「 」 「 」 』 」 」 』		1
建泉风险	12194664i i 小 1945 12194664i 小 2212 1219464i 小 2212 1219464i 小 2212 12194742目		1
① 変変入口			l
局 第□令	用小市 用量 金田同志 ション 単語 金郎 〇 ン 2021/03/14 00:00 2021/04/12 23:59 〇 55 王章		1
	用/* read 整定行为用法		l
教练把超风险	③2021/04/01 第 平年 91.1437		1
1 明文敬感信息	MAGOL 月か Port 歴史 📕 26.16.164.65 登録124.250.25.84 、登景位起27、 奥教の次 デモの役は 🗰 100	Ŧ	l
101 文件下載	© 2021/00/11 ชิดมี เปเมตร -2021/00/11 ชิดมี 5 011308		l
APINIS	MyGGL 用户 Hoot 書店 四 172.167.11	Ŧ	l
III API列表	0 201/02//7 2 - 201/02/79 3 - T+− 01.006		l
			l
	◎ 301/01/12 常作下 06239 - 3021/01/36 常 九4 011008		
	東京王高 用件 newt 義正 臣 17216711 世界17216711288680(ede.php, 世界世界5元 世界成功法, 学校3月81 (新会)	Ŧ	
	© 221,09/17 = ₹1_ 065259 - 2021/09/29 = ₹∓ 01.5008		
	MyGOL 用户 Mont 通过 [2] 192.168.42.119 登录192.168.100.177,登录创新12次, 登录成功0次, 元为12次	Ŧ	
	© 2021/03/15 ≑ €L 00.5062 - 2021/02/26 E TF 01.05.51		
	The same life of 10 101 102 101 102 102 101 104 102 102 101 104 102 101 104 102 101 104 102 101 104 102 102 102 104 104 104 104 104 104 104 104 104 104		¥

【用户行为】该页面通过用户的视角展示某个用户登录的整体行为,可查询每一个 登录详情

3.2 数据泄漏风险

TDP 可以对系统的敏感信息进行泄漏风险监测,主要包括明文敏感信息传输监测和 系统文件下载监测,具体功能介绍如下:

3.2.1 明文敏感信息

页面路径:

1.从导航菜单进入风险页面

2. 选择 "风险-数据泄漏风险-明文敏感信息" 子菜单项 , 来到明文敏感信息页面。

*&风险 > 数据泄漏风险 > 明	文敏感信息				时间 24小时 7
居接口搜索	敏感标签	▼ 输入关键字	搜索		
效感信息访问趋势			▌ 手机	, 📕 邮箱 📕 身份证 📗 银	行卡 敏感信息访问top3
222					test.threatbook.cn/article/ 访问数量 邮箱
11 -					test.threatbook.cn/article/ 访问数量 邮箱
1020/01/02 2020/01 17:00 21:00	/02 2020/01/03 0 01:00	2020/01/03 05:00	2020/01/03 2020/ 09:00 13:	01/03 2020/01/03 00 17:00	test.threatbook.cn/article/ 访问数量 身份证
test.threatbook.cn/article 邮箱	l				访问数量
▶ test.threatbook.cn/article 邮箱	1				访问数量
▶ test.threatbook.cn/article 身份证	1				访问数量
test.threatbook.cn/article	1				访问数量

明文敏感信息页面支持以下功能:

【时间切换】支持24小时和7天的时间切换。

【搜索功能】支持根据以下内容进行搜索:

根据接口搜索: 支持根据接口关键字进行搜索

敏感标签:支持搜索敏感信息类型,包括手机、邮箱、身份证号、银行卡号进行搜 索

敏感信息页面包含以下内容:

1.敏感信息访问趋势:

以柱状图的形式展示了手机、邮箱、身份证号、银行卡号在所选时间范围内的趋势, 鼠标滑动到对应的柱形图上,可以看到对应时间点手机、邮箱、身份证号、银行卡号的 访问次数。

2.敏感信息访问 TOP3:

TDP 将明文传输敏感信息的接口,统计对应的访问数量,展示访问次数最多的 TOP3 接口,并且展示接口的访问数量,以及接口泄露信息的类型。

3.敏感信息接口:

敏感信息接口列表,展示接口暴露的敏感信息类型,点击"展开"按钮,可以看到 "返回内容"和"用户列表"TAB。

•	192.168.100.99:502 邮箱	23/	访问数量 3
敏	感内容 返回内容	用户列表	
	敏感类型	敏感内容	
	邮箱	webmaster@example.com(宣看)	

"返回内容" TAB 展示对应的接口最近一次的返回内容,用户可以根据返回内容判断接口功能。其中,检测到的敏感信息会被高亮显示。

	99-50223/ 访问数量 3
敏感内容	回內容 用户列表
<pre>IDOC contex chars type= 24, 5 rgb(2 .jumb rgba(lpx s rope is wo class routi from to us src="</pre>	<pre>html PUBLIC '-//WSC//UTD XHTML 1.11/FM' "http://www.wloorg/TM/shtml11/DTD/shtml11.dtd'>chtml>chemd> cmsts http-equive*Content-type* text/html; charset=UTT-8'> <title>Apache HTTP Server Test Page powered by Cent08</title> <msts content="*text/html;<br" http-equive*content-type*="">TF-8'> <l-= boothtrap=""> <link html="/noindex/css/boothrap.ml.oss" rol="styleHoet"/> <link <br="" rel="styleHoet' html* thref='noindex/css/open-means.cs"/>t/css" > <style type="text/css"></style></l-=></msts></pre>

"用户列表" TAB 展示对应接口的访问用户,展示内容包括 IP、访问系数、QPM、访问次数、UA 和敏感数据类型。

192.168.100.99:50223						访问数量
敏感内容 返回内容	用户列表访问系数	QPM(峰值)	访问次数	Cookie	UA	敏感数据
61.160.247.70 一中国·江苏·常州 ide	1.00	1	3	hibext_instdsigdipv2=["com.mysql.cj.jdbc.admin.MiniAdm	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Geck	曲印车前

3.2.2 文件下载

TDP 将监测到的文件下载行为展示在文件下载页面,从下载 IP 角度和文件角度 进行展示。

页面路径:

1.从导航菜单进入风险页面

2. 选择"风险-数据泄漏风险-文件下载"子菜单项 , 来到文件下载页

面。

文件下载 IP 文作	ŧ											
行为分布			文件类型						文件大小			
0	 向服务器上传文件 从服务器下载文件 服务器主动下载文件 服务器主动上有文件 	₽ ₽	C	e d e d e x e t t	oc)inc ocx zip is 〕tar.gz isx 〕bak it ① myd	 mdb tar mvc ppt pptx 	 pdf 7z rar hta vbs 	ps1 dii c xmi		● 小子 ● 14回 ● 10M ● 大子	IMB - 10MB 3 - 50MB 50MB	
输入 IP 或文件	搜索									关 攻击者 IF	● 关 黒名単 IF	Ρ
源 IP	行为	目的 IP	文件	文件大小	目标地址				次数 💠	时间 🗢	操作	
192.168.77.148		111.206.239.60	wjttlpw.zip	41 Bytes	cqldk.jzpylyw	.cn/l/wjttlp	w.zip		12	2019-09-23 10:13:38	下载	
192.168.77.147	下啟→	111.206.239.60	wjttlpw.zip	41 Bytes	cqldk.jzpylyw	.cn/l/wjttlp	w.zip		4	2019-09-23 10:13:33	下载	
192.168.100.173 🔤		106.75.75.68	39604f.zip	45 KB	106.75.75.68	:8099/url_	Vtip_test_	.u	2	2019-09-23 10:12:50	下载	
											< 1 >	

"IP" TAB 内容如下:

点击 "IP" TAB, 系统以下载文件 IP 的角度, 进行了下载文件行为风险的展示。

分布概况:

【行为分布】行为分布展示了四种下载行为,分为"向服务器上传文件"、"从服务器下载文件"、"服务器主动下载文件"和"服务器主动上传文件"四种。

【文件类型】根据文件后缀类型,展示了下载文件类型的分布。

【文件大小】将文件大小按照"小于 1MB"、"1MB - 10MB"、"10MB - 50MB" 和"大于 50MB"四种类型,进行分类展示。

功能操作:用户点击对应的类型,就可以进行筛选,点击图表下方的"重置筛选" 按钮,可以清空之前选择的筛选类型。

源 IP 列表:

【搜索功能】支持根据 IP 或者文件,进行搜索。

源 IP 列表展示一下内容:

源 IP: 展示了下载文件的 IP 地址

行为:展示了源 IP 的行为类型

目的 IP: 展示了下载文件的目的 IP

文件: 展示对应下载的文件名

文件大小: 展示下载文件的大小

目标地址:展示下载文件的地址

次数:展示此文件被下载的次数,点击可以进行"升序"或者"降序"操作

时间: 展示此文件被下载最新一次时间, 点击可以按照时间的"升序"或者"降 序"排序

【操作】用户如果希望得到对应的文件,可以点击"下载"按钮进行下载,如果不能下载成功,则说明下载链接失效。

"文件" TAB 内容如下:

点击"文件"TAB,系统以下载文件的角度,进行了下载文件行为风险的展示。 分布概况:

【行为分布】行为分布展示了四种下载行为,分为"向服务器上传文件"、"从服务器下载文件"、"服务器主动下载文件"和"服务器主动上传文件"四种。

【文件类型】根据文件后缀类型,展示了下载文件类型的分布。

【文件大小】将文件大小按照"小于 1MB"、"1MB - 10MB"、"10MB - 50MB" 和 "大于 50MB" 四种类型,进行分类展示。

功能操作:用户点击对应的类型,就可以进行筛选,点击图表下方的"重置筛选"按钮,可以清空之前选择的筛选类型。

文件列表:

【搜索功能】支持输入文件,进行搜索。

文件列表展示以下内容:

文件: 文件名称

ChreatBook 微步在线

文件大小: 文件大小

下载次数: 文件被下载的次数

文件位置: 文件所处的位置

操作: 点击"下载"按钮, 可以下载该文件

3.3 API 风险

API 风险展示了 TDP 对所监控系统所有 API 的动态监控。

页面路径:

1.从导航菜单进入风险页面

2. 选择"风险-API风险-API列表"子菜单项 , 来到 API列表页面。

风险 > API风险 > API列表 全部API接口		时间 24	小时 7天 30天
搜索域名或IP	是东	搜索关键字	搜索
static-img.threatbook.cn	接口列表(5)	PV	UV
接口数量 5	/api/v1/url/report	10996	1
wwbizapi.taobao.com 接口数量 5	/api/v2/url/report	3058	1
api.bignox.com	▶ /api/v1/url/scan	712	1
接口数量 4	▶ /api/v2/url/scan	306	1
www.cnblogs.com 接口数量 3	/api/v2/sample/report	4	1

3.3.1API 列表

API 列表在左侧展示域名或者 IP, 在右侧展示所选域名或者 IP 之下的接口。

支持以下功能:

【时间搜索】支持"24小时/7天/30天"的时间范围切换

【搜索域名或 IP】在左侧搜索框,输入域名或者 IP,可以进行搜索。

【关键字搜索】在右侧搜索框,输入接口关键字,可以在当前选择的"域名和 IP" 之下进行接口的搜索。

3.4 资产与服务

资产与服务页面,展示 TDP 检测到的系统中对外提供服务的资产与服务。

3.4.1 全部服务

全部服务页面展示系统监测到的所有系统服务,包括数据库、Web 服务器、远程 登录、邮件服务、认证服务、文件传输以及其他服务。

页面路径:

1. 从导航菜单进入风险页面

2. 选择"风险-资产与服务-全部服务"子菜单项,来到全部服务页面。

TDP 威胁感知平台	监控	威胁	资产&风	<u>اور</u>	调查	报告	处置	平台管	理 175	主节点	▼ #	步在线内部测试	试用版	I		2
资产和服务	资产&风险 > 全部	资产和服务 > : 服务分类	全部服务						对外开放	8	让线					Â
📚 全部服务				•							0					
IP 资产IP列表	全部服务	数据库	Web服务 ジ	1992 1982 录	邮件服务	认证服务	文件传输	其他服务	对外开放服	服务	新上线服务					
💿 域名资产	374台	7台	310台	27台	4台	1台	17台	41台	173台		1台					
	最近7天活	跃服务(38)	近7天不活跃服	送务(11)												
登录风险	Q 请输入	服务名			Web服务	unknown	关联主机: 95							导出	当前表格	
🔋 登录入口	WebEC			<u>^</u>	资产 如震	配置资产名称信	急清前往 资产管理	页		关联端口) 关联域	8	对外开放			
🔒 弱口令	united and	2		-	Q 资产	名称/IP地址	全部	- -)版本	Q și	Q	夏索城名	全部 ▼	最近发现的	榈	
		WN l: 95	对外	开放									-			
数据泄漏风险	nginx				192.168.10	0.99	444			8088	-		音	2021/03/26		
🗍 明文敏感信息	关联主が	l: 59	对外	开放			服务器			8080	-		是	2021/03/26		
🖻 文件下载	Tengin	e					444									
	关联主が	1: 35	对外	开放	172.26.68.1	150	服务器			9080			杳	2021/03/26		
API风险	Apach #####	e 1. 29	공수상	LTT th			444									
□ API列表	Micros	off-IIS	~~~		172.16.71.1	183	服务器			1234	-		合	2021/03/31		
	关联主が	l: 25	新上线/对外	开放			555						_			

按照服务分类展示:

在全部页面,选择数据库、Web 服务器、远程登录、邮件服务、认证服务、文件传输以及其他服务的按钮,会按照对应的类型展示系统内相关的服务,选中的服务类型变为蓝色。

IP 按照对外开放、新上线服务展示:

在全部页面,选择对外开放、新上线服务按钮,会按照对应的类型展示系统内相关的服务,选中的服务类型变为蓝色。

新上线服务定义: 首次发现时间在最近三天内。

服务展示:

在全部服务页面,按照"最近7天活跃服务"以及"近7天不活跃服务"两个 TAB 进行分类。

每个服务归属对应的服务类型,点击对应服务,右侧展示该服务之下的关联主机资 产,资产信息包括 IP、资产类型、关联端口、关联域名、是否对外开放、以及主机最近 的发现时间。

【操作】支持下载当前筛选条件下的服务以及所属资产。

3.4.2 资产 IP 列表

资产 IP 列表页面展示系统监测到的所有资产,类型包括终端、服务器,支持按照 是否对外开放和近 3 天内新上线筛选。

页面路径:

1.从导航菜单进入风险页面

2. 选择"风险-资产与服务-资产 IP 列表"子菜单项 ,来到资产 IP 列表页面。

资产IP数(1284)							
🖵 修端: 33 📰 服务器: 11	197 🗍 对外开放: 629	🕤 近3天新上线:	4				导出当前表格
资产 如需配置资产名称信息请前	1往 <u>资产管理页</u>	服务	服务版本	关联域名	关联端口	对外开放	最近发现时间
172.30.150.81	服务器	Microsoft DNS	-		53	否	2019/12/24
172.30.145.33	服务器	WINS			42	否	2019/12/24
172.30.176.222	服务器	MSSQL	-		1433	否	2019/12/24
172.30.90.35	服务器	MySQL	-		3306	否	2019/12/24
172.30.91.176	服务器	Memcached	-		11211	否	2019/12/24
172.30.58.209	服务器	Postfix	-		25	否	2019/12/24
172.30.28.164	服务器	Qmail(pop3)	-	-	110	否	2019/12/24
172.30.252.101	服务器	Hmail(pop3)			110	否	2019/12/24

资产 IP 展示:

资产信息包括 IP、资产类型、服务、服务版本、关联端口、关联域名、是否对外开放、 以及主机最近的发现时间。

在列表上方,统计了资产 IP 数量,以及终端数量、服务器数量。同时统计了 对外开放的主机数量,和最近 3 天内的新上线资产数量。

支持下载当前筛选条件下的所有资产。

筛选操作:

支持对 IP 地址、资产类型、服务名称、服务版本、关联域名、关联开放端口、是 否对外开放、近 3 天新上线这些条件进行组合筛选。

3.4.3 域名资产

对于企业客户, TDP 支持对于企业内网的域名资产进行检测和展示, 支持以下功能:

梳理系统内所有二级域名以及二级域名之下的子域名,展示二级域名的注册人信息 以及最近一次的注册人变更信息;展示子域名对应的具体 IP 地址等信息。

支持查看子域名的业务属性,包括子域名之下的登录接口、API 接口(含敏感信息的 API 接口)、文件下载行为等。

能够对子域名的变更信息做监控展示,包括近3天内对外开放、近3天上线、新 增管理后台。

能够对于域名进行快速搜索和筛选。

页面路径:

选择"资产&风险"导航,选择"域名资产"子导航

即可以看到域名资产页面。

查看所有域名

在域名资产页面左侧,展示了系统内检测到的所有二级域名,点击对应的二级域名,可以查看此二级域名之下的子域名。对于每个二级域名,会统计此域名之下的子域名个数进行展示。

二级域名如果存在注册人,会展示对应的注册人信息。

TDP

ChreatBook 微步在线

是否对外开放: 😭 是否存在敏感信息接口: 全部	部是否 是否近三天内上线 部是否 是否存在管理后台	: 全部 是 否 : 全部 是 否	入域名/IP		筛选 重置		
全部域名: 2345 二級域名: 27	⑦ threatcook.com	注册人: xfh	gkgk@threatbook.c	n			导出当前表格
threatcook.com 子域名: 1234	子城名: 1234	上次变更 :注抗	册人由xfh@threatbo	gk@threatbook.cn, 变更时间:	2020/02/17 18:00	3 eff. Mito wher case	
threatcook.com 子域名: 1234	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	<u>111.206.218.124</u>	是	五求按口 1	API接口[古敏感信息按口]	12 12	近三天对外开放
threatcook.com 子域名: 1234	tzt.threatbook.cn 🛋 XXXX管理平台	111.206.218.124	是	1	<u>988</u> [<u>345</u>]	12	近期无变更
threatcook.com 子域名: 1234	tzt.threatbook.cn 📠	111.206.218.124	是	1	<u>66</u> [<u>12</u>]	12	近三天上线
	tzt.threatbook.cn 🛋	<u>111.206.218.124</u> <u>111.206.218.124</u> <u>111.206.218.124</u>	是	1	<u>988</u> [<u>345</u>]	12	近期无变更
	tzt.threatbook.cn IA XXXX管理平台	<u>111.206.218.124</u> <u>111.206.218.124</u> <u>111.206.218.124</u> …等 <u>13个</u>	是	1	<u>1000+</u> [<u>345]</u>	12	新増登录接口
						< 1 2	3 4 5 6 >

查看域名的业务属性

点击登录接口、API 接口 (含敏感信息接口)、文件下载对应的数字,可以查看此 域名之下对应的信息。

查看域名对应的变更信息

在表格变更信息列,会展示域名对应的变更信息。包括域名三天内上线,域名新增管理接口和域名三天内对外开放。

域名的快速筛选

支持对域名和对应的 IP 进行筛选。

四、调查

调查模块为用户提供高级的调查分析能力,包括日志调查,终端取证和命中情报三个功能;同时通过攻击 IP、告警主机、威胁名称视角展示相关内容。

4.1 日志调查

4.1.1 新版网络日志

TDP 新版日志调查页面,为用户提供更友好的交互方式,更全面的字段说明与提

日志清査 透露日解								时间范围:最近7天 月	副新版本: 33
网络日志							🗋 保存豐富的	件 自己保存重调	1% 历史查询
逸量方向:全部 ~ 告替主机IP:全部 ~	e e	道IP: 全部 ~	目的IP; 全部 ~	URL或域名: 全部 ~	行为类型:全部、	攻击结果	: 全部 v 西多 v	Q 高级查询	重西
攻击 📕 敏感行为	5 20	8							
fk]									
n									
120/10/14 00:00		2020/10/ 09:00	15	2020/10/16 18:00	2020/10. 05.00	18	2020/10/19 12:00		2020/10/20 21.00
原始日本 攻出	11P-TOP5	50 告罄主机-TOP50	藏胁各称-TOP50						
0 187753		详细日志 (2835)			10100000	100 D 1000		创日志下载	局下载任
晨示宁母:		東間 ×	B∎×	数×	Elé ×	\$99X ×	URLIENSXX	減齢名件 X	
1 #11		> 收主成功	2020/10/15 15:08:19	10.10.51.2:49636[P]]	198.55.121.100:443[5F]	POST 400	linenews.mypicture.info;443/0000/ a239732461.asp	BlackTech团伙	
日期 time		》 攻击威功	2020/10/15	10.10.51.2×49636(Ph)	198.55.121.100 :443[화]	HTTP	linenews.mypicture.info;443/0000/ a219712461.asp	BlackTech团伏	
目頭	ili i	Port of the	2020/10/15	102 168 102 108-100100	150 129 82 201-80184	нттр	usuu 20080 or keh is	15.10	
10-02			15:08:16	The for the the second second second	Too. Taxina a compily	GET 200	www.concertifieda		
URL脱脱名 data	th	> 校告	2020/10/15 15:08:15	172.16.27.1:63943[P]	172.16.27.141:8080(内)	HTTP POST 200	172.15.27.141:8080/jbossmq- http://HTTPServeriLServlet	JAVA 反序列化按固(Cor	mmons C
成的名称 threat.name	ıl.	• Riff	2020/10/15 15:08:15	172.16.27,1:63943[Pi]	172.16.27.141:8080[P]]	HTTP POST 200	172.16.27.141:8080/jbossmq- http://HTTPServerll.Servlet	JAVA 反序列化改善(Cor	mmonsC
可添加字段: HTTP语求方法	d.	> 收重	2020/10/15 15i08/15	172.16.27.1:63943[P]	172.16.27.141:8080(内)	HTTP POST 200	172.16.27.141:8080//bossmq- http://HTTPServerILServlet	用oss运程代码执行(C	VE-2017
net.http.method HTTP地应药 net.http.status	ıl.	▶ <u>收</u> 圭	2020/10/15 15:08:15	172.16.27.1:63943[Pi]	172.16.27.141:8080[内]	HTTP POST 200	172.16.27.141:8080/jbossmq- http://HTTPServeril.Servlet	JAVA 反序列化较贵(Cor	mmonsC
10-4-Brip			2020/10/15			нттр	172.16.27.141:8080/jbossmq-	In She was to see	UT 2017

示,以及更加灵活的告警日志展现方式。

页面路径:调查-日志调查

调查-简单筛选

用户可以通过平台日志筛选区域进行字段选择,选择后进行查询。

1) 如果字段的值为固定的值,则系统会将所有选项呈现出来,供用户选择;

2)如果字段值不固定,系统支持模糊搜索和精确匹配,同时模糊搜索与精确搜索都支持匹配多个值。

3) 如果用户希望搜索更多的字段, 而不是默认的字段, 则可以通过"更多"按钮,

获取更多支持检索的字段,进行添加;字段支持根据字段名称以及字段值进行模糊搜索;

调查-高级搜索

用户可以通过 sql 语句进行日志的检索, TDP 提供友好的提示:

- □ TDP 对于用户输入时, 会提示可搜索的字段, 并根据输入内容匹配对应的字段
- □ 用户输入或者选择字段后, TDP 会继续提示运算符
- □ 选择运算符后, TDP 会自动将匹配的值加上引号, 并将输入光标放在引号之内。
- 用户输入匹配值后,进行搜索,如果满足转换条件,高级检索可以和简单搜索切换。(当用户先进行简单查询条件筛选后,点击高级查询,则简单查询的条件将 直接展示在高级查询输入框内,多条件将默认通过 "AND" 连接,如有需要可以 自行修改,修改后不可再进行查询方式的修改。)

调查-增加日志条件记录

当用户进行日志查询时,可以通过选择不同的字段进行日志的筛选,为了方便用户 长期的使用,调查筛选增加了保存查询条件、已保存查询、历史查询功能。

- 保存查询条件:当用户选择完筛选条件后,可以点击保存查询条件,输入语句
 名称进行条件保存,我们同时也将展示检索语句及日志展示列,点击确定后可
 进行保存;
- 已保存查询:点击已保存查询,将展开通过保存查询条件后的列表,用户可以
 通过在此处选择检索条件进行日志查询;(提供搜索框、检索、删除)
- 历史查询:点击可以查看历史 7 天查询记录,同时展示检索语句。(提供检索 按钮可再次查询)

调查-告警日志展示列支持自定义

调查页面,为了便于用户查看原始告警,默认展示日志类型、日期、源、目的、协议、URL 或域名以及威胁名称六列,如果用户希望看到更多,可以自行在可展示字段中添加列;同时告警日志表格列的顺序可以自行调整。

调查-支持自动刷新

调查页面,支持根据设置的频率进行自动刷新,以便于用户了解最新的告警。刷新的告警将在日志列表中展示带有"NEW"标识,若刷新频率较为频繁,建议时间选择尽量短,以免系统开销过大。

调查-行为类型可视化

通过可视化列表展现在一定的时间范围内,受到的行为记录,通过图表展现。(目前 分为攻击行为、敏感行为、其他)

调查-日志分类展示

针对日志列表将其以不同的视角进行展示,进一步展示为用户进行内容查询及汇总。

- □ 攻击 IP-TOP50:通过攻击者视角展示其行为,在详情页中针对攻击手法、活跃
 程度及熟悉资产均进行分析描述。
- 告警主机-TOP50:通过告警主机维度展示主机被威胁的情况汇总,针对威胁次数、威胁方式、威胁事件均进行罗列。
- □ 威胁名称-TOP50:针对威胁进行列表展示,展示威胁方式整体分析威胁行为。

4.1.2 网络日志 (旧版)

旧版日志调查分为网络日志和终端日志两种,可以通过下拉选择框进行切换。

日志分析							
网络日志 🗸	1						
终端日志		快速检索:	所有告警	外部攻击	来自某IP的SQL注入攻击	内网反连某远控地址	HTTP GET访问某URL返回200

网络日志展示系统监测到的所有镜像流量的网络告警日志,包括搜索功能、检索聚 合功能、日志趋势图以及日志详情列表。

搜索功能

【时间搜索】网络日志支持时间精确搜索,以及"1小时"、"24小时"、"今天"、

"近7天"和"最近30天"的快捷选择。

【语法说明】TDP 提供快速检索语句,包括以下语句:

所有告警:检索网络日志中所有的告警

外部攻击:检索互联网对内网的攻击

来自某 IP 的 SQL 注入攻击:检索来自某 IP 的 SQL 注入攻击,用户可以自行替换 IP 以及攻击手法,进行搜索

内网反连某远控地址:检索网络日志中国,所有的对外反连地址

HTTP GET 访问某 URL 返回 200:用户可以按照需求修改返回状态码"200",以及 对应的"URL"进行检索

【语句搜索】网络日志检索支持以下语句检索:

类别	字段名称	搜索语句
实体相关	我IP 我名 我端 外IP 为端 流 网目(I)/ 资 资 资 资 资 资 资 资 资 资 资 资 资 资 资 资 资 资 资	<pre>machine = '192.168.100.175' machine_name = '' machine_port= '80' external_ip='11.11.111' external_port='12345' direction = 'in ' data= 'www.threatbook.cn'</pre>

ChreatBook 微步在线

HTTP 相关	HTTP 请求	net.http.method = "GET"					
	方法	net.http.reqs_body LIKE '%%'					
	HTTP 请求 体	net.http.resp_body LIKE '%%'					
	HTTP 响应 体	net.http.reqs_host = ' <u>www.baidu.com</u> '					
	HTTP 请求 域名	net.http.reqs_user_agent = "elastic/5.0.74 (darwin-amd64)"					
	HTTP 用户 代理	net.http.status = "200"					
		net.http.url = "/static/js/26.cde9b1f3.chunk.js"					
	HTTP 响应 码	net.http.reqs_referer = '' net.http.xff = ' '					
	url						
	http 来源 地址						
	HTTP 请 求端真实 IP						
外部攻击相关	外部 IP	external_ip = "192.168.1.168"					
	来源国家	geo_data.Country = "局域网"					
	来源省份	geo_data.Province = "局域网"					
	来源城市	geo_data.City= "局域网"					
	标签 (取威	threat.name = "查询 json 接口"					
	胁名称)	threat.msg='查询 json 接口'					
	攻击	threat.tool='SQL 注入'					

ChreatBook 微步在线

	攻击工具	
	敏感行为 名称 敏感行为 描述 ip 信誉	threat.level ='action' and threat.name='查询 json 接口' threat.level ='action' and threat.msg = "查询 json 接口" ip_reputation = "bogon"
传输层协议相 关;	传输层源 ip 6 输层目 的 标 一 输 口 输 口 输 二 目 的 端 层 目 的 令 端 同 。 令 前 。 令 前 。 令 前 。 令 前 。 令 前 。 令 前 。 令 前 。 令 前 。 令 前 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 句 。 令 令 。 令 令 。 令 令 。 令 令 。 令 令 。 令 令 。 令 令 。 令 令 令 令 令 。 令	net.src_ip = '180.120.94.175' net.dest_ip = '180.120.94.175' net.src_port = '80' net.dest_port = '80' net.proto = "TCP"

在输入框中,输入搜索语句后,鼠标失焦后,会将输入的语句标签,用户想去 掉其中一项时,点击对应标签的"X"关闭按钮以后,搜索语句会自动去掉这一条件, 点击搜索后会按照新的语句进行检索。

检索统计

TDP 在左侧展示筛选条件下的所选择的网络日志的聚合结果,包括以下内容:源 IP、目的 IP、HTTP 请求域名、传输层协议、应用层协议、攻击名称、敏感行为名称和 HTTP 返回码。 所选择的网络日志,均会统计相应的字段,按照每个项的占比暂时在左侧中,点开 后,支持搜索功能,点击下载按钮可以下载相关的内容。

日志趋势图

日志趋势图展示了所选择告警日志,在对应时间内的告警趋势,鼠标浮动在趋势图上后,浮动展示当前时间的告警次数。

时间快速选择:用户将鼠标移入趋势图的时间轴之下,可以看到鼠标变成十字选择按钮,用户可以使用此时间选择控件,快速缩小时间范围。

日志详情列表

日志详情列表展示每条告警的基本信息,点击展开后可以查看详细日志。

基本信息包含以下内容:

告警时间、源 IP 和端口(如果网络日志中存在 XFF 的 IP,并且来源于可信任 IP,

XFF 的 IP 会展示在源 IP 之下)、方向、目的 IP 和端口、协议、HTTP 方法和返回码、

URL 以及攻击标签

详细信息包含以下内容:

详细内容:展示了此告警 HTTP 以及 DNS 的请求和返回协议

JSON: 展示了这条告警在存储中的原始记录

4.1.2 终端日志 (旧版)

终端日志展示了 Agent 的所有上传日志。

在调查-日志调查页面, 切换下拉选择器, 将"网络日志"选项, 切换成终端日志,

就可以

查看系统内安装的 Agent 日志。

点击具体的日志告警,可以查看日志具体信息。

4.2 终端取证

终端取证页面展示了系统中所有已经安装的 Agent, 主要功能如下:

【时间控件】: 支持 "24 小时/7 天/30 天"的时间切换

【搜索功能】: 支持根据主机名称、网络地址、取证结果、分组、在线状态和操作状态进行搜索。

【下载 Agent】点击下拉菜单,可以下载 linux 版本的 Agent 安装包。

【终端列表】包括以下信息:主机名、分组、网络地址、取证结果、开启功能、采集模版和 Agent 版本。

【终端详情】点击列表中对应的"查看详情"按钮,系统可以查看对应 Agent 的终端取证详情页面。

4.3 自动以情报

自定义情报中,展示用户导入的情报,通知支持用户在此页面导入自定义情报。支 持以下功能:

4.3.1 自定义情报

自定义情报分为失陷检测情报、IP 信誉情报

ChreatBook 微步在线

失陷检测情报:

【搜索功能】可以根据 IOC 进行搜索

【情报标签】可根据情报标签进行筛选

【严重级别】可根据严重级别进行筛选

【新增情报】支持用户自定义上传单条情报。

【上传情报】支持用户上传自定义情报。

【失陷检测情报列表】:展示 IOC 名称、类型、情报标签、严重性、命中次数、告

警主机数。

TDP 感謝感知平台	监控	威胁 资产&	风险 调查 ^{重保}	报告	处置	平台管理	175主节点 🔻	微步在线内部测试		>	. (
调查	失陷检测情报											Î
前 重保监控	失陷检测情报	IP信苦情报										
111 日志调査	+ 新增自定义情报	十上传自定义情报	IOC	情报标签	全部情报标签	~	严重级别 全部	\sim	搜索			
前 跟踪与狩猎	自定义情报(22)											
🚔 政主委公析	юс	类型	情报标签	严重性	来源	时间	命中次数 🗢	告答主机数 🗢		操作		
	fget-career.com	DOMAIN	ramnit蠕虫	▲ 高危	custom	2021-03-29 15:45:31	214	13	白名单	编辑	删除	
◎ 自定义情报	linenews.mypicture	sinfo DOMAIN	info_idc111		custom	2021-01-04 15:57:35	207	14	白名单	编辑	删除	
	mail-csits.org	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
	mail-csg.xyz	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
	accfgov.com	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
	microsoft1.space	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
	cgbchina.xyz	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
	cgbchina.online	DOMAIN		▲ 高危	TIP-tip1111	2021-04-12 12:01:55	0	0	白名单	编辑	删除	
						2021-04-12						-

IP 信誉情报:

【搜索功能】可根据 IP 地址、情报标签进行搜索

【情报来源】可根据情报来源进行筛选

【新增 IP 信誉】支持 IP 信誉情报导入

【IP 信誉列表】: 展示 IP 地址、情报标签、情报来源、更新时间

ChreatBook 微步在线

てつP 成功を成	监控 威胁	资产&风险	調査	报告 处置	平台管理 175	主节点 🔻	微步在线内部测试 试用版	
^{調査} 1111 重保监控	关路检测情报 关路检测情报 IP(言苦情报						ĺ
目志调查	 1.录入自定义IP情报后,TDI 2.如果您同时使用了做步在 3.如果您没有开启全流量记录 	P会自动將債服际签与对应IP地 线威胁債报管理平台(TIP), 则可 製種式, 命中自定义IP信誉債报	业的告答/行为日志相关即 通过配置与TIP联动,自动 的流量日志默认不会记录	、提供更丰富的上下文展示。 以TIP同步IP信誉情报。点击都 、如果忽希望记录、可在设备都	生配置	前往配置		
登 攻击者分析 受 终端取证	十 添加IP倍誉 IP地址	按印理索	情报标签		情报来源 请选择	v	搜索 批量操作	▼ 导出当前表格
⑥ 自定义情报	IP地址 188.166.164.164	橋服标签 exploit,HW2021		情报来 TIP-tip	ag 1111		更新时间 2021-04-12 12:01:55	操作 编辑 删除
	183.141.61.119	exploit, HW2021		TIP-tip	1111		2021-04-12 12:01:55	编辑 删除
	173.208.153.34	exploit,HW2021		TIP-tip	1111		2021-04-12 12:01:55	编辑 删除
	178.62.78.40	exploit,HW2021		TIP-tip	51111		2021-04-12 12:01:55	编辑 删除
	178.62.72.12	exploit,HW2021		TIP-tip	51111		2021-04-12 12:01:55	编辑 删除
	122.190.43.149	exploit,HW2021		TIP-tip	1111		2021-04-12 12:01:55	编辑删除

4.4 攻击者分析

攻击者分析页面,列出所有 TDP 检测到的攻击 IP,通过微步情报,历史攻击/访问行为,微步云端数据等,对攻击者特征进行综合计算,为企业安全运营团队在日常安全运营和重保防御过程中提供参考。

4.4.1 攻击者分析列表

攻击者分析列表,将系统检测到以及云端共享的所有攻击者展示出来,以便于企 业安全人员了解攻击来源,明确威胁水平,提高应对能力。

TDP 蔵静感知平台	监控 威胁	资产&风险	2 调查	报告	处置 平	₽台管理	微步在线内	83%试177 📧 🕢 🌲 🔹
_{调查} 曲 日志调查	□ 调查 > 攻击者分析						自动刷新: <u>关闭</u>	2020/02/07 00:0 -2020/02/13 01:0
🧟 攻击者分析	攻击者IP					攻击者特征:重置		
🖸 终端取证	使用攻击手法		~~ 活跃度		~\~ 攻击水平	⇒÷) 针对性	掌握资产	清空
◎ 命中情报	地理位置		攻击时间	间长	手法多样 手法高级	攻击多个系统 手动攻击	与其他IP共同攻击 IP对外开放端口	搜索
	攻击访问占比 0		100			攻击过同行	IP期定了域名(可溯源)	
	系统检测 云端共	享						7548
	攻击者IP	最近攻击时间 🖨	情报标篮	攻击访问占比 ⇔	攻击者特征		攻击手法	操作
	61.160.247.70 一中国·江苏·常州	RIRI	IDC服务器	18%	手法多样 同期定了域名		b374k Webshell连接成功 扫描黑客Webshell后门 等17种	查看详情 + 关注 +阻断
	52.196.17.52 ● 日本·东京都·东京	RIRI	IDC服务器	79%	○ IP绑定了域名		利用ngrok进行内网穿透	查看 详情 + 关注 +阻断
	3.15.53.92 美国·俄亥俄州·都柏林	RIRI	-	73%	◎ IP对外开放端C	□ 🛜 IP娜定了域名	利用ngrok进行内网穿透	查看详情 + 关注 +阻断
	70.127.242.253 美国·佛罗里达州·坦帕	RIRI	Dynamic IP	71%	新发现的攻击者,正	在分析中	扫描黑客Webshell后门(base64代 菜刀webshell虚拟终端执行命令 等4种	⊭输) + 关注 → 细断
	208.51.206.168 ■ 美国·美国	RIRI	-	36%	新发现的攻击者,正	在分析中	MySQL注入 猜测管理后台 等3种	+ 关注 +阻断

页面路径:

1.从导航菜单进入调查页面

2. 选择"调查-攻击者分析"子菜单项 , 来到攻击者分析页面。

攻击者IP			攻击者特征:重置		
	N	~~~~	æ-€)		
使用攻击手法	活跃度	攻击水平	针对性	掌握资产	清空
ALL THE AT THE	攻击时间长	手法多样	攻击多个系统	与其他IP共同攻击	and the second second
地理证量		手法高级	手动攻击	IP对外开放端口	搜索
攻击访问占比	0		攻击过同行	IP绑定了域名(可溯源)	□ 已关注
0	100				

【攻击者筛选】系统支持用户使用以下字段进行攻击者筛选,包括攻击者 IP、攻击

者使用手法、攻击者所在的地理位置以及攻击者攻击/访问占比。

【攻击者特征筛选】系统定义了以下特征,同时支持用户根据进行对攻击者筛选。

攻击者特征	攻击者名称	含义
活跃度	攻击时间长	说明攻击者的攻击天数大于 3 天。
攻击水平	手法多样	攻击者使用多种手法进行攻击。

CThreatBook 微步在线

	手法高级	攻击者使用了高水平的攻击手法,体 现出了较高的能力水平。
针对性	攻击多个系统	攻击者针对多个系统进行攻击。
	手动攻击	攻击者使用非自动化等攻击手法, 说 明是针对性很强的攻击者。
	攻击过同行	攻击者近期攻击过当前客户同行业 的客户。
掌握资产	与其他 IP 共同攻 击	攻击者使用多个 IP 共同攻击。
	IP 对外开放端口	攻击者 IP 对外开放了端口。
	IP 绑定了域名 (可溯源)	攻击者 IP 绑定了域名, 可通过 whois 进行溯源。

【只查看关注的攻击者】勾选"已关注"选项,可以只查看用户关注的攻击者。

【攻击者列表自动刷新】支持攻击者列表的自动刷新,用户可以选择自动刷新的时间间隔。

【系统检测中攻击者列表】展示攻击者的攻击 IP、地理位置、最近攻击时间、情报 标签、攻击访问占比、攻击者特征、攻击手法以;

攻击者列表支持下载;

点击"查看详情",可以查看次攻击者的具体内容;

点击"关注",则用户对此 IP 进行了关注;

点击"+阻断",用户可以将这个攻击者 IP 添加至阻断列表。

系统检测 云端共調	¥					下载
攻击者IP	最近攻击时间 🖨	情报标签	攻击访问占比 ⇔	攻击者特征	攻击手法	操作
61.160.247.70 一 中国·江苏·常州	RURU	IDC服务器	18%	 手法多样 ○ IP绑定了域名 	b374k Webshell连接成功 扫描黑客Webshell后门 等17种	查看详情 + 关注 +阻断
52.196.17.52 ● 日本·东京都·东京	刚刚	IDC服务器	79%	◎ IP挪定了域名	利用ngrok进行内网穿透	查看详情 + 关注 +阻断
3.15.53.92 美国·俄亥俄州·都柏林	刷刷	-	73%	IP对外开放端口 〇 IP绑定了域名	利用ngrok进行内网穿透	查看详情 + 关注 + 组断
70.127.242.253	刚刚	Dynamic IP	71%	新发现的攻击者,正在分析中	扫描黑客Webshell后门(base64传输) 菜刀webshell虚拟终端执行命令	+ 关注 + 组断

【云端共享中攻击者列表】展示攻击者的攻击 IP、地理位置、最近攻击时间、情报标签、攻击访问占比、攻击者特征、攻击手法以;点击"+阻断",用户可以将这个攻

击者 IP 添加至阻断列表。

4.4.2 攻击者详情

《 返回攻击者分析				
52.196.17.52	攻击者特征: 该攻击 掌握资产: 1	者具备1个特征.費着所有特征		
IDC服务器	IP挪定了城名(可测	源) 攻击者IP绑定了城名,可通过whois进行溯源。		
+ 关注		ngrok.com		
攻击访问占比		邮箱: contact@ngrok.com 电话: +1.4157993439		
79% 21%		通过反查域名ns-1552.awsd关联得出		
首次发现:2020/02/04 最近活动:2020/02/12 攻击客能力模型	攻击手法:		A	-
攻击手法	 侦查手法 		温潤利用手法	● 使用WebShell
活跃度	当前选择时间段,	智未发现此类攻击手法	当前选择时间段。暂未发现此类攻击手法	当前选择时间段, 智未发现此类攻击手法
	活跃程度: 访问	🛯 皺感行为 📕 攻击 💙 攻击成功 🔿 云端情报		
掌握资产	- = =	四五六日 2020年02月12日		
	1月 14 15	16 17 18 19 利用ngrok进行内网	访问域名 家语: 13次 (成功) 52.196.17.52	 S端情报共享 无结果
	20 21 22 27 28 29	23 24 25 26 30 31		
	2月	1 2		

页面路径:

点击系统检测中某个攻击者 IP 的"查看详情"按钮,来到对应的攻击者详情页面。

【攻击者基本属性】展示攻击者的 IP、地理位置、云端情报标签;同时展示用户的 攻击访问比,首次发现时间和最近活动时间;展示攻击者的能力模型,包括攻击手法、 针对性、掌握资产和活跃度。

【攻击者特征】展示攻击者的所有特征,默认会将不具备的攻击者特征隐藏,点击 "查看所有特征"会展示全部。如果攻击者可溯源,则会展示溯源到的攻击者真实信息, 展示绑定的域名,以及注册域名时的姓名、电话和邮箱。

【攻击手法】展示攻击者的所有攻击手法,按照侦查手法、漏洞利用手法和使用 webshell 进行区分。

【活跃程度】展示了近 30 天内,攻击者的活跃程度,以及每天的具体行为。行为 主要包括:访问、敏感行为、攻击、攻击成功和云端情报。点击日历中具体的某一天, 可以查看对于天的本地攻击活动、访问的域名,以及当天此 IP 的云端共享情报。

【掌握资产】展示了此攻击者使用的攻击 IP 个数、掌握的域名个数、浏览器 User-Agent 个数和攻击使用的 cookie。Cookie 的 key 和 value 的值会以列表的形式呈现。

五、报告

5.1 报告中心

页面路径:

1.从导航菜单进入报告页面

2. 选择"报告-报告中心"子菜单项。

报告中心								
创建时间:	E 2019/09/10 00:00 - 2019/09/16 16:00			报告名	称: 按名称搜索			
报告类型:	流得极伯类型			•				8180
+ 信庫报	2							④ 管理定时任务
报告名称		报告类型	报告大小	生成状态	提交人	生成时间	10	fi .
单次_告警	消纽投表-2019-09-11_16-05-20-58	估餐明细报表	37.66MB	已生成	tdp.	2019-09-11 16:05:22	F	制体
单次_告责	退纽报表-2019-09-10_21-07-34-61	告誓胡祖报表	13.04MB	已生成	tdp	2019-09-10 21:07:36	78	BUR
单次_色管	主机报表-2019-09-10_21-07-29-80	告誓主机报表	4.55KB	C.S.M.	tdp	2019-09-10 21:07:29	TR	8018
单次_威胁	\$ 件强表-2019-09-10_21-07-26-59	威胁事件报表	32.77KB	已生成	tdp	2019-09-10 21:07:26	78	808
单次。威胁	分析报告-2019-09-10_21-07-15-88	威胁分析报告	a	生成失败	tdp			18
								4 1

报告中心, 支持用户导出以下四类报告:

告警明细报表 (.csv) :最细粒度的报表,每一行代表一次告警

威胁事件报表(.csv):每一行统计相同主机相同告警行为发生次数,和最近一次完整告警信息

告警主机报表(.csv):每台告警主机一行数据,聚合展示威胁事件,统计告警次数 威胁分析报告(.doc):综合性报告,多角度完整地描述了组织内的威胁情况 创建报告方法:

1.从导航菜单进入报告页面

2. 点击页面上"创建报告"按钮,弹出"编辑报告"弹窗,选择需要创建的报告类

型,选定时间范围、生成周期,点击确定就可以说生成。

ChreatBook 微步在线

报告列表如下:

+ 创建探告						⑥ 管理定时任务
报告名称	报告类型	报告大小	生成状态	提交人	生成时间	N/T
单次_告警明细报表-2019-09-11_16-05-20-58	告偿明细报表	37.66MB	已生成	tdp	2019-09-11 16:05:22	7741 B38
单次_告誓明细报表-2019-09-10_21-07-34-61	告誓明細报表	13.04MB	已生成	tdp	2019-09-10 21:07:38	7.42 8.03
单次_告暨主机报表-2019-09-10_21-07-29-60	告警主机报表	4.55KB	已生成	tdp	2019-09-10 21:07:29	742 803
单次_威胁事件报表-2019-09-10_21-07-28-59	威胁事件报表	32.77KB	已生成	tdp	2019-09-10 21:07:26	T-02 8038
单次_威胁分析报告-2019-09-10_21-07-15-58	藏胁分析报告		生成失敗	tdp		813
						< 1 >

包含内容有:

报告名称、报告类型、报告大小、生成状态、提交人、生成时间。用户可以点击操 作这一列,进行报告的下载和删除。

定时任务管理:

用户点击"管理定时任务"按钮,就会来到定时任务管理页面,可以对定时任务进行编辑、修改和禁用。

③ 定时报告任务									
报告名称	报告类型	状态	创建用户	创建时间	生成周期	下一次生成时间		操作	
定时_告警明细报表	告警明细报表	启用	tdp	2019-09-23 14:03:40	每周一1:00	2019-09-30 01:00:00	编辑	禁用	删除
定时_告警明细报表	告營明细报表	启用	tdp	2019-09-11 16:08:17	每周三1:00	2019-09-25 01:00:00	编辑	禁用	删除
定时_告警主机报表	告營主机报表	启用	tdp	2019-08-30 00:21:40	每周一0:00	2019-09-30 00:00:00	编辑	禁用	删除
定时_威胁事件报表	威胁事件报表	启用	dd	2019-08-29 20:16:51	每月1日1:00	2019-10-01 01:00:00	编辑	禁用	删除
定时_告警明细报表	告譬明细报表	启用	dd	2019-08-29 19:57:58	每周二3:00	2019-09-24 03:00:00	编辑	禁用	HIR
定时_告警明细报表	告營明细报表	启用	dd	2019-08-29 19:57:17	每周一2:00	2019-09-30 02:00:00	编辑	禁用	删除
定时_告警明细报表	告營明细报表	启用	dd	2019-08-29 19:48:04	每周一2:00	2019-09-30 02:00:00	编辑	禁用	删除
定时_告警明细报表	告營明细报表	启用	dd	2019-08-29 19:35:15	每周三2:00	2019-09-25 02:00:00	编辑	禁用	删除
定时_告警明细报表	告營明细报表	启用	dd	2019-08-29 19:22:12	每周四1:00	2019-09-26 01:00:00	编辑	禁用	删除
定时_威胁事件报表	威胁事件报表	启用	dd	2019-08-29 19:08:33	每周三1:00	2019-09-25 01:00:00	编辑	禁用	删除
定时_告讐明细报表	告警明細报表	启用	dd	2019-08-29 19:00:48	每周二1:00	2019-09-24 01:00:00	编辑	禁用	删除

六、处置

6.1 阻断

阻断功能是为用户提供处理外部攻击的一种方式,当前支持旁路阻断或联动阻断, 用户可自定义配置阻断方式进行阻断。

旁路阻断:



6.1.1 阻断策略

旁路阻断

通过旁路部署,向攻击方和被攻击方双向发 reset 包来实现,要实现封禁需要确保 tdp 的包能发出去,否则无效。

【阻断列表】IP、添加时间、过期时间、状态、添加来源、阻断次数、备注

【新增阻断】支持手段添加 IP、自动阻断策略配置

【筛选条件】可根据来源、状态、IP 进行筛选及搜索

自动阻断

用户可以选择自动阻断策略配置,发生外部攻击的 IP,将会被自动添加至阻断列

表。用户可以自定义这些 IP 的阻断时间,时间范围限制在 10 分钟到 30 天内。

TOP dedute				na IP		处置						Ð
REIN	处置 > 阻断	> 旁路阻断										ſ
③ 旁路阻断	旁路阻断:	HEO	CO-LEDINGAN	-				~				
联动阻断 高		 开启旁路阻断后、 开启后、用户可以 请按驾配置唱新台 	 目数加速防御1 二 添加攻击IF 季 攻击方向: 客 攻击结果: 	」 ■ ■ ● 型 小部攻击 互联网双 ■ の 取 一 型 失敗	「満足下列条件) 「内岡的攻击 ■ 芸試			×	流量研究	→ ■ 内部主机		
₩₩ □ 处理己录	阳斯列表 十 新增组和		严重级别: 地理位置: 威胁情报: 生效时间:	 ご 产重 ご 境内 ご 境内 ご 境外 ご 境外 ご 攻击IP被微步情报 阻断 100 分報 	 中 使 使 (1) <l< th=""><th>☑ 信息</th><th></th><th></th><th>2021/04/06 00:00</th><th> 2021/04/12 渡安 重置条(</th><th>23:59 👘 ŧ 🕬 🏨 Đượng</th><th></th></l<>	☑ 信息			2021/04/06 00:00	2021/04/12 渡安 重置条(23:59 👘 ŧ 🕬 🏨 Đượng	
	12 IP	.106.184.40	额外添加以下 ☑ 【里保模	(P至阻断列表 試】阻断所有情报标记	为攻击队的IP地址 ①				醫注 HW自动阻断	操作	Bile	
	42.1	193.9.231 98.40.47	2021/04/12	11:04:29 20:	21/04/13 12:41:37	唱新中	取消 HW目初	inite O	HW自动阻断 HW自动阻断	sta sta	mik Mik	
	1.15	5.228.250	2021/04/12	11:04:29 20	21/04/13 12:41:37	阻断中	HW自动	0	HW自动唱断	95	删除	
	112	.124.201.199	2021/04/12	11:04:29 20	21/04/13 12:41:37	阻断中	HW自动	0	HW自动阻断	995	1910 :	

联动阻断

通过策略生成阻断 IP List 与第三方设备联动从而达到阻断的效果

TDP 成熟感知平台	监控	威胁	资产&风险	调查重保	报告	处置	平台管理	微步在线内部测试 试用版	۰	۲
	┃ 处置 > 阻断	> 联动阻断								i i
③ 旁路阻断	联动阻断:	开启								
😼 联动阻断	• 开启第三方	联动印新后,提供1	「截錄接」供第三方设备调	用素 要阻断的入站IP。			. 🗐	田		
📙 阻断名单	• 支持该模式	的防火墙设备: PA	Fortinet(FortiOS 6.2及以	上版本), Checkpoint(R77及以上版本)	内部主机	交換机	防火墙	互联网黑IP/域:	8
	・清按案配置	阻断白名单,道免日	8時正常业务!					能 ME ME ME ME ME ME ME ME ME ME		
。 □ 处理记录							Ibr			
	阻断IP下载									
	下载链接: h	ttps://192.168.100).175:443/api/block/dow	nloadLinkageBlockL	ist 复制					
	最新生成时间	: 2021/04/12 12	51:09							
	阻断IP生成规	阙								
	☑ 添加攻击	P地址至阻断列表	(同时满足下列条件)							
	攻击方向:	☑ 外部攻击 互助	期对内网的攻击							
	攻击结果:	🖸 成功 🕑 失	敗 🖸 芸试							
	严重级别:	■ 严重 ■ 周	(治 🔽 中治 🔽 低急	☑ 信息						
	地理位置:	☑ 境内 ☑ 填	的							

【阻断策略配置】进行阻断 IP 策略配置,可进行相关配置生成阻断 IP List

【阻断 IP】通过阻断策略生成 IP List 展示该链接

阻断白名单

IP 白名单

用户可以添加阻断的白名单,支持单一IP、网段和 IP 区间。

情报、规则、模型 ID 白名单

在白名单中的情报/规则/模型 ID 关联的攻击 IP 不会被阻断

阻断黑名单

在阻断黑名单中的威胁 ID,均会被阻断。

6.2 处理

处理记录

TDP 在处置中增加了处理记录,用来记录用户在威胁中将告警主机进行过处置的内容整理,方便与处置结果的查询。

【筛选】可根据处理结果、事件范围、告警主机、威胁事件、经办人进行查询筛选 【下载】可以进行处理列表的下载

【列表展示】包含处理时间、告警主机、威胁事件、处置人、处理结果、备注

TDP 威胁感知平台	监控	威胁 资产&风险	调查报告	处置 平台管	理	金山云_公有云 就用版		
阻断	▲ 处置 > 处理 > 处理;	录						
💿 阻断	处理结果: 全部	∨ 时间范围:	<u>2020/10/16 00:00</u> ~ 2020/10/2	2 23:59 告警主机	/威胁事件/经办人	筛选 重置	🕑 下载	
	处理时间	告誓主机	威胁事件	处置人	处理结果	备注	操作	
处理	2020/10/22 13:45:2 4	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利 用JQuery站点)	tdp	处理中	则试信息	删除	
◎ 处理记录	2020/10/22 11:41:2 9	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利 用JQuery站点)	tdp	未处理		删除	
	2020/10/22 11:41:2 9	192.168.178.54(生产服务器)	Cobalt Strike拦截请求(利 用JQuery站点)	tdp	已处理/无需处理		删除	
	2020/10/20 17:41:3 8	192.168.178.121(生产服务器)	全部威胁事件	tdp	未处理		删除	
	2020/10/20 17:41:1 2	192.168.178.121(生产服务器)	利用struts2漏洞	tdp	处理中		删除	
	2020/10/20 17:41:0 3	192.168.178.121(生产服务器)	全部威胁事件	tdp	已处理/无需处理		删除	
	2020/10/20 17:40:4 6	192.168.178.121(生产服务器)	Struts2 远程代码执行漏洞 (CVE-2017-5638)	tdp	已处理/完成处理		删除	
	2020/10/20 17:40:3 5	192.168.178.121(生产服务器)	Cobalt Strike拦截请求(利 用JQuery站点)	tdp	处理中		删除	

七、误报反馈

TDP 支持用户将系统产生的误报告警反馈至云端,同时用户可以删除同类型的告警,并按照自定义规则加白。

页面路径:

在任意告警的详细内容模块,点击"误报处理"按钮,即可进行误报反馈

威胁事件详情				>
	事件类型 5億) 失陷破坏/连接远控地址	告誓主机 192.168.178.54(生产服务器)	事件处理状态 ② 处理中 🖉	
成胁明细 分析和处置			2020/10/	15 00:00 ~ 2020/10/21 23:59
与远控端建立连接 全部 是 否 分	外连地址			山 下載
时间 🔷 威胁名称	误报处理	×	目标地址	建立连接
▼ 10/21 14:54:46 Cobalt Stril 用JQuery和	对于该条报警额外进行以下处理: 同 将此告警加白, 避免后续产生同类告警		code.jquery.com/jquery- 3.4.1.min.js	K
详细信息 PCAP 原始记录	圖除最近30天相同情报/规则/模型产生的	的所有告答记录		~ ~
▲ 告警信息	✓将此误报信息反馈给微步在线安全云, 帮	B助产品优化检测质量		
严重 Cobalt Strike拦载清求(利用)Quer		取消 确定		误报处 四百名单
日志信息			记录	时间:2020-10-21 14:54:46
		HTTP 9000		
192.168.178.54 (生产服务器)		连接		code.jquery.com

选择"将此告警加白"时,用户可以选择将同类型的告警删除;同时也可以选择删除最近 30 天相同情报/规则/模型产生的所有告警记录;也可以进行将误报信息反馈给微步在线安全云,帮助产品优化检测质量。



误报反馈

 \times

对于该条报警额外进行以下处理:

🗹 针对此类告警进行加白,加白后不再产生告警

白名单策略:

匹配字段	匹配策略	匹配内容					
规则/情报/模 ▼	属于	S2019010046	$\checkmark \times$				
+ 新增条件							

- ◎ 支持对规则/情报/模型IP, url, 文件HASH加白
- 多个条件组合,则每个条件都命中时才生效
- url支持匹配字符串或者正则表达式

生效时间:

• 永久

-		
○ 延长	10	分钟

○ 生效至 📰 请选择日期

☑ 删除近30天相同规则/模型/情报产生的所有告警

取消 确定