

安全运营中心 操作指南



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

操作指南

安全可视

安全检测

调查中心

响应中心

资产管理

漏洞管理

系统管理

操作指南

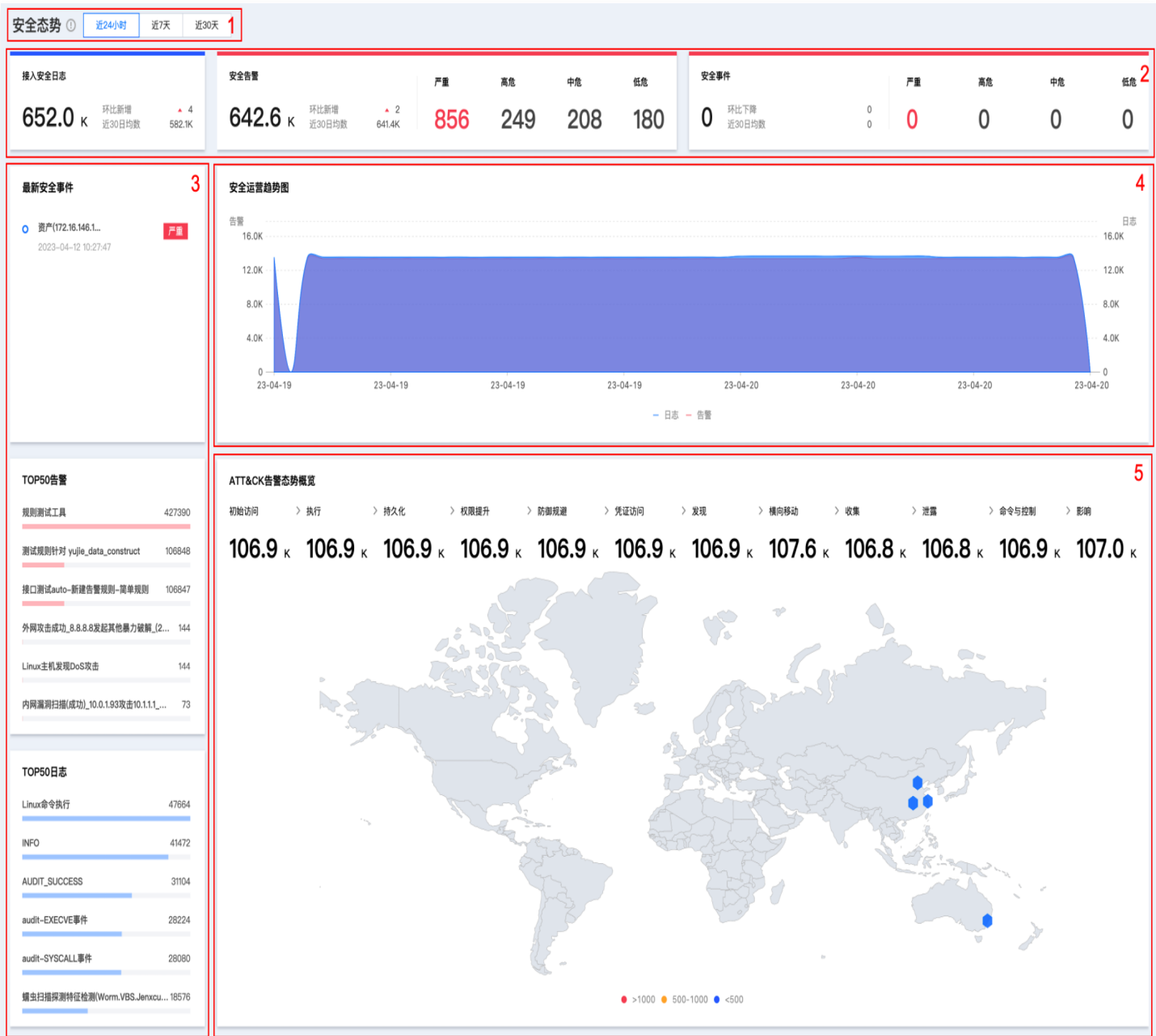
安全可视

最近更新时间：2024-12-17 18:09:02

安全态势

在**安全可视 > 安全态势**页面，数据监测能够帮助安全运维人员及时发现和处理威胁，以便于有效洞察企业面临的外部威胁和内部脆弱性风险，提高安全运维团队监测、管理、处置安全事件的效率。

在**安全可视 > 安全态势**页面，可以查看企业在全网范围内的安全日志、安全告警、安全事件数量，TOP 排行，安全运营趋势图，ATT&CK 告警态势概览。展示方式包括安全评分、趋势图、条形图和分布图等，如图所示。



态势大屏

在安全可视 > 态势大屏页面，包括七块3D大屏（漏洞分析大屏、告警态势大屏、外部攻击态势大屏、内网攻击态势大屏、系统运行态势大屏、攻防总览大屏、自适应拼接屏）。以及通过单击左下方的旧版大屏，可切换为七块2D大屏（综合态势大屏、攻击态势大屏、资产态势大屏、威胁大屏、脆弱性态势大屏、流量态势大屏、租户安全运营大屏）。

单击进入后，即可显示相应的大屏。在3D大屏中，选择大屏名称，便可切换至相应的大屏界面。

态势大屏



漏洞分析

进入 3D(Beta)

进入



告警态势

进入 3D(Beta)

进入



外部攻击态势

进入



内网攻击态势

进入



系统运行态势

进入 3D(Beta)

进入



攻防总览

进入 3D(Beta)

进入



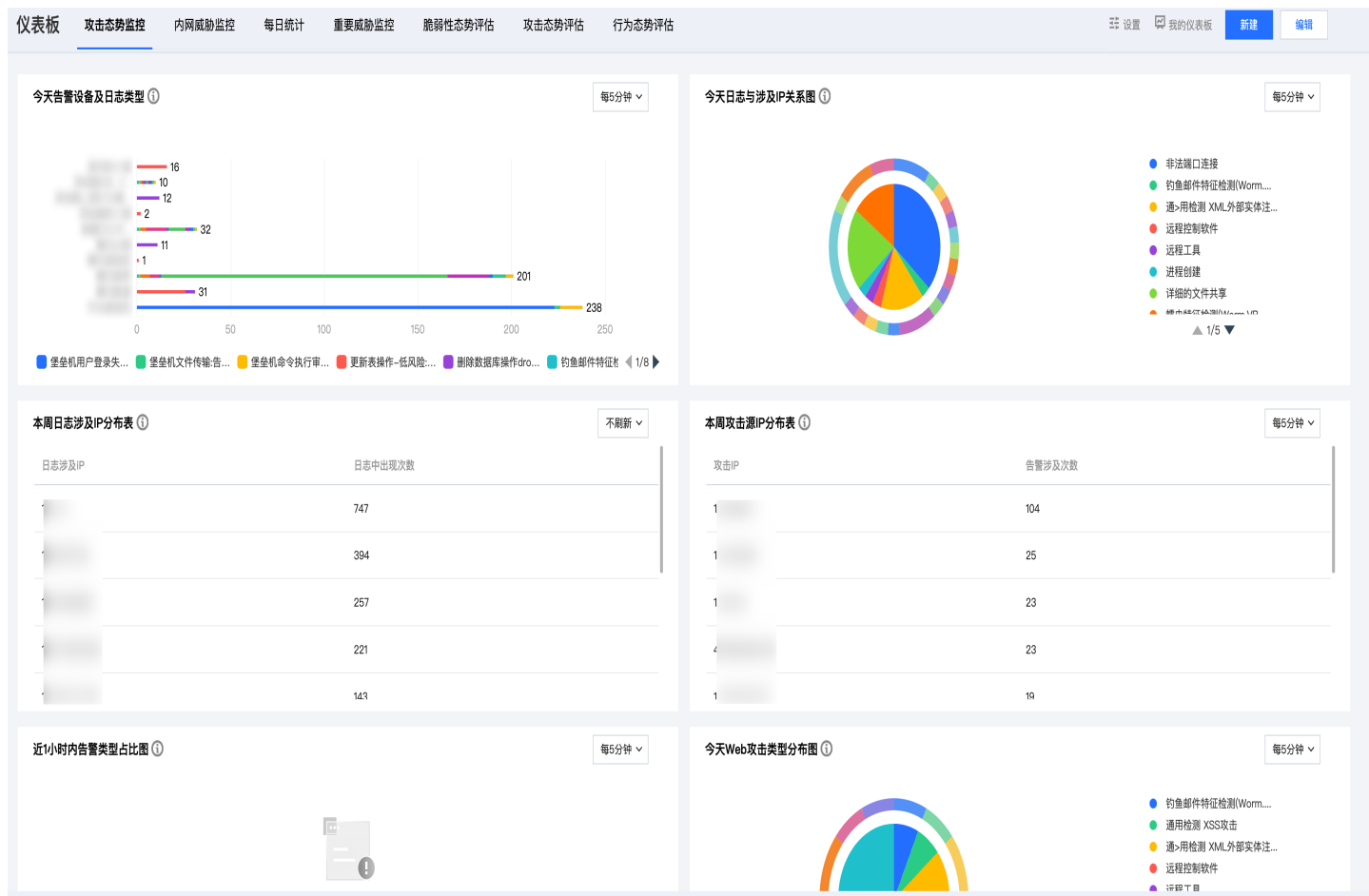
自适应拼屏

进入

旧版大屏

仪表盘

在安全可视 > 仪表盘页面，可以根据攻击态势、威胁、脆弱性态势和攻击态势等以仪表盘的形式进行监控，还可以使用本系统的组件库新建仪表盘，页面布局如图所示。



安全专题

在安全可视 > 安全专题页面，针对安全运营中常见的几种关键安全场景，SOC 将以安全专题的形式向安全运营管理人员展示，以便重点关注和分析。

报表中心

在安全可视 > 报表中心页面，内置了两种报表模板，可根据需求选择时间范围和资产范围对安全告警情况、资产风险情况及脆弱性情况等统计和呈现，并可将报表导出为 PDF 文件。

安全检测

最近更新时间：2024-12-17 18:09:02

告警列表

在安全检测 > 告警列表页面，管理员可以查看攻击事件趋势图、攻击链分布图、告警详情和告警策略，还可进行告警的导出、响应、搜索、状态变更和编辑标签等操作。

告警列表

近24小时 近7天 近30天

2024-10-19 11:14:39 ~ 2024-11-18 11:14:39

📅

与运营中心>检索 搜索语法一致

Q

条件搜索

全部展开

告警名称

威胁等级

攻击结果

状态

攻击链阶段

告警分类

告警子分类

关联规则id

ATT&CK战术

ATT&CK技术

攻击者ip

受害者ip

主机IP

告警趋势图

展开图表

导出

状态变更

标签

响应

0

实时刷新: ☐

管理

☐	生成告警时间	告警名称	状态	威胁等级	告警分类	告警子分类	攻击链阶段	攻击者ip	受害者ip
☐	2024-11-15 16:45:35	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:34	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:32	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:28	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:26	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:22	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:22	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:20	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		
☐	2024-11-15 16:45:20	测试引用集	• 新发现	信息(1)	登录操作	用户登录	环境配置		

关联分析

1. 在安全检测 > 关联分析页面，选择告警策略管理。
2. 在告警策略管理页面，管理员可以创建触发告警的策略并对其编辑和删除，也可以对全局告警归并策略和策略引用集进行管理。

告警策略管理告警策略告警白名单

规则场景

搜索规则场景

通用场景690

扫描探测54

IP扫描43

端口扫描34

服务器扫描39

爬虫33

钓鱼邮件16

钓鱼邮件13

垃圾邮件13

文件投递15

web投递7

下载恶意文件3

访问恶意网站6

DDOS9

DDOS9

账号安全74

暴力破解43

爆破成功12

异常登陆23

异常账号新增14

弱密码6

Web攻击33

Sql注入17

命令执行20

代码执行19

Webshell29

XSS17

CSRF17

SSRF17

文件包含17

文件读取17

新建删除批量启用批量停用导入导出

告警日志关注策略管理全局告警白名单策略引用集管理

输入策略ID或名称

策略名称/ID	策略更新时间	规则场景	ATTCK技术 T	ATTCK技术 T	状态	操作
测试引用集 100096	2024/11/15 11:41:23	暂无数据	暂无数据	暂无数据	☒	编辑删除复制
规则测试工具4 100094	2024/09/12 12:25:14	暂无数据	暂无数据	暂无数据	☒	编辑删除复制
规则测试工具3 100093	2024/09/12 12:25:14	暂无数据	暂无数据	暂无数据	☒	编辑删除复制
规则测试工具2 100092	2024/09/12 12:25:14	暂无数据	暂无数据	暂无数据	☒	编辑删除复制
规则测试工具1 100091	2024/09/12 12:25:14	暂无数据	暂无数据	暂无数据	☒	编辑删除复制
	2024/09/12 12:19:47	多个 (4)	多个 (5)	多个 (9)	☐	编辑删除复制
	2024/09/12 12:19:45	多个 (4)	多个 (5)	多个 (9)	☐	编辑删除复制
	2024/09/12 12:19:40	通用场景:主机安全,异常行为	多个 (2)	网络嗅探	☒	编辑删除复制
	2024/09/12 12:19:36	多个 (5)	多个 (2)	访问令牌滥用	☒	编辑删除复制
	2024/09/12 12:19:36	多个 (4)	泄露	多个 (4)	☒	编辑删除复制
	2024/09/12 12:19:35	多个 (3)	凭证访问	多个 (3)	☒	编辑删除复制
	2024/09/12 12:19:35	通用场景:扫描探测,IP扫描	多个 (4)	有效账户	☒	编辑删除复制
	2024/09/12 12:19:35	多个 (3)	影响	站点拒绝服务	☒	编辑删除复制
	2024/09/12 12:19:35	通用场景:扫描探测,IP扫描	多个 (3)	多个 (6)	☐	编辑删除复制

威胁情报

SOC 集成威胁情报本地查询功能，安全人员可以针对指定 ioc 查询情报信息，支持自定义，利用情报能力获得更快更精准的检测与响应。

1. 在安全检测 > 威胁情报页面，选择威胁情报查询。

2. SOC 平台集成本地威胁情报查询页面，可主动对 ioc 查询，支持单次和批量查询，方便研判分析。

版权所有：腾讯云计算（北京）有限责任公司

第9 共25页

情报查询

单次搜索 ▾ 请输入IP、域名、MD5、邮箱、漏洞名称、漏洞编号

搜索

单次搜索

批量搜索

行为分析

在[安全检测 > 行为分析](#)页面，可以检测组织可能面临的高级网络威胁、内部人员风险等常规安全方案难以覆盖的风险点，进而提升整个安全运营态势。

智能检测

在[安全检测 > 智能检测](#)页面，通过对流量日志进行基于深度学习的 AI 智能检测，能够进行安全检测与分析。

ATT&CK 能力矩阵

SOC 基于 ATT&CK 知识矩阵构建安全检测评价体系，提供2个维度的覆盖率展示，包括关联策略和关联告警。

SOC 平台内置 MITRE ATT&CK V10 矩阵，及相关知识库，共12个战术阶段，188个技术点。

在[安全检测 > ATT&CK 能力矩阵](#)页面，直观展示当前关联规则覆盖的 ATT&CK 矩阵，包括覆盖每个战术、技术的关联规则数及列表，并能根据 ATT&CK 技术名词、关联规则名称进行搜索。

ATT&CK能力矩阵

关联策略

关联告警

全部状态策略

输入ATT&CK技术名称、告警策略名称以搜索

初始访问 103 策略 9 / 9 技术	执行 95 策略 10 / 12 技术	持久化 154 策略 15 / 19 技术	权限提升 148 策略 13 / 13 技术	防御规避 210 策略 31 / 39 技术	凭证访问 118 策略 12 / 15 技术	发现 69 策略 25 / 27 技术	横向移动 76 策略 9 / 9 技术	收集 36 策略 13 / 17 技术	命令与控制 82 策略 14 / 16 技术	泄露 28 策略 8 / 9 技术	影响 94 策略 13 / 13 技术
网络钓鱼(38)	命令与脚本解释器(35)	创建账户(7)	计划任务/作业(6)	在主机上构建映像	中间人(4)	网络服务扫描(13)	远程服务(23)	自动收集(1)	远程访问软件(15)	通过 Web 服务泄露(7)	固件损坏(1)
硬件添加(6)	WMI Windows 管理规范(18)	浏览器扩展	创建或修改系统进程(7)	修改系统映像	操作系统凭证转值(38)	云服务发现(1)	通过可移动媒体复制(6)	来自信息库的数据(1)	Web 服务(9)	数据传输大小限制(4)	网络拒绝服务(4)
通过可移动媒体复制(6)	原生 API(5)	植入内部映像	事件触发执行(15)	混淆的文件或信息(6)	双因素身份验证拦截	网络嗅探(17)	软件部署工具(14)	电子邮件收集(5)	数据编码	通过 C2 通道进行泄露(1)	为影响而加密的数据(20)
路过式攻击(8)	计划任务/作业(6)	账户操作(8)	劫持执行流程(12)	执行护栏	窃取或伪造 Kerberos 票证(5)	系统信息发现(1)	横向工具转移(15)	中间人(4)	非标准端口(2)	通过其他网络介质进行泄露(4)	资源劫持(11)
利用面向公众的应用程序(28)	容器管理命令(1)	BITS 任务(1)	特权提升的利用(4)	直接卷访问(1)	伪造 Web 凭证(3)	系统所有者/用户发现(2)	使用替代身份验证材料(9)	视频截取	入口工具传输(3)	将数据传输到云账户(4)	磁盘擦除(2)
有效账户(56)	共享模块	攻陷客户端软件二进制文件	启动或登录初始化脚本(3)	访问令牌操纵(5)	修改认证流程(2)	云基础设施发现(1)	远程服务会话劫持(2)	来自云存储对象的数据(4)	交通信号(6)	通过物理介质进行泄露(1)	数据销毁(22)
外部远程服务(9)	进程间通信(1)	在操作系统前启动	进程注入(18)	BITS 任务(1)	强制认证(6)	账户发现(5)	利用远程服务(19)	浏览器中的人攻击	多级通道(1)	计划传输(14)	损毁(2)
供应链攻击(13)	部署容器	事件触发执行(15)	有效账户(56)	修改云计算基础设施(2)	网络嗅探(17)	远程系统发现(2)	污染共享内容(1)	屏幕截图(2)	协议隧道(4)	替代协议上的泄露(4)	系统关闭/重启(3)
信任关系(5)	利用客户端执行(13)	劫持执行流程(12)	访问令牌操纵(5)	签名二进制代理执行(15)	来自密码存储的凭据(4)	文件和目录发现(3)	内部鱼叉式网络钓鱼(1)	剪贴板数据(1)	应用层协议(12)	自动泄露	端点拒绝服务(12)
	软件部署工具	修改认证流程	滥用提升控制	在操作系统前	窃取应用程序			来自网络共享	非应用层协议		

污染共享内容 (Taint Shared Content)

子技术 0

攻击者可以通过向共享存储位置（例如网络驱动器或内部代码存储库）添加内容来向远程系统提供有效载荷。存储在网络驱动器或其他共享位置的内容可能会因向其他有效文件添加恶意程序、脚本或漏洞利用代码而受到污染。一旦用户打开共享的受污染内容，就可以执行恶意部分以在远程系统上运行对手的代码。攻击者可能会使用受污染的共享内容横向移动。目录共享数据透视是此技术的一种变体，它使用其他几种技术在用户访问共享网络目录时传播恶意软件。它使用目录.LNK 文件的快捷方式修改，使用伪装看起来像真实的目录，这些目录通过Hidden Files 和 Directories 隐藏。基于.LNK 的恶意目录具有嵌入式命令，该命令执行目录中隐藏的恶意软件文件，然后打开真正的预期目录，以便用户的预期操作仍然发生。当与经常使用的网络目录一起使用时，该技术可能会导致频繁的再感染和对系统的广泛访问，并可能导致对新的和更高特权的账户的访问。攻击者还可以通过将其代码附加或预先添加到共享网络目录上的健康二进制文件中来通过二进制感染破坏共享网络目录。恶意软件可能会修改健康二进制文件的原始入口点（OEP），以确保它在合法代码之前执行。当远程系统执行新感染收起

1 条策略已关联 前往策略列表查看

策略名称/ID	策略更新时间	规则场景	威胁等级	告警分类	告警子类	攻击结果	状态
7	0	多个 (12)	自动计算	自动计算	自动计算	自动计算	

调查中心

最近更新时间：2024-12-17 18:09:02

安全事件

在调查中心 > 安全事件页面，支持针对告警线索展开自动化调查，生成待处置分析的安全事件。支持自动将威胁告警基于影响资产、时间线、ATT&CK 技战术进行关联，自动还原攻击过程，采集战术、技术、过程和相关上下文，以及受影响资产信息，并给出安全事件的严重级别、类型、描述和处置建议等。

安全事件

近24小时

近7天

近30天

2023-03-01 16:23:18 ~ 2023-05-17 16:23:18

📅

状态变更 ▼

三管理

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

🔍

☐	事件发生时间 ↓	事件名称	事件类型 ↑	事件状态 ↑	严重性 ↑	事件描述	资产 IP	更新时间 ↕
☐	2023-04-12 10:27:47	资产	WEB攻击,主机异常等事件	多个 (2)	新发现	严重	资产可能已经失陷，详情如下：出...	2023-05-17 04:42:43
☐	2023-04-10 01:23:48	资产	主机异常事件	其他事件	新发现	高危	资产可能已经失陷，详情如下：资...	2023-05-14 06:28:04
☐	2023-04-10 01:17:04	资产	主机异常事件	其他事件	新发现	严重	资产可能已经失陷，详情如下：资...	2023-05-16 22:03:10
☐	2023-04-10 00:43:18	资产	暴力破解事件	网络攻击事件	新发现	严重	资产可能已经失陷，详情如下：对...	2023-05-14 10:13:02
☐	2023-04-10 00:23:37	资产	破解事件	网络攻击事件	新发现	严重	资产可能已经失陷，详情如下：对...	2023-04-25 18:02:03
☐	2023-04-10 00:07:44	资产	主暴力破解,账号异常等事件	网络攻击事件	新发现	严重	资产可能已经失陷，详情如下：对...	2023-05-17 04:43:35
☐	2023-04-09 23:37:45	资产	主机异常事件	其他事件	新发现	高危	资产可能已经失陷，详情如下：资...	2023-05-16 22:52:18
☐	2023-04-09 23:14:43	资产	暴力破解,主机异常等事件	多个 (2)	新发现	严重	资产已经失陷，详情如下：资产遭...	2023-05-17 04:42:43
☐	2023-04-09 23:06:57	资产	暴力破解事件	网络攻击事件	新发现	严重	资产已经失陷，详情如下：对外发...	2023-05-16 22:05:26
☐	2023-04-09 23:03:36	资产	主WEB攻击事件	网络攻击事件	新发现	高危	资产可能已经失陷，详情如下：资...	2023-05-11 21:34:08
☐	2023-04-09 22:54:03	资产	主WEB攻击,主机异常等事件	多个 (2)	新发现	高危	资产可能已经失陷，详情如下：资...	2023-05-14 10:13:46
☐	2023-04-09 22:48:06	资产	主机异常事件	其他事件	新发现	严重	资产可能已经失陷，详情如下：资...	2023-05-17 04:42:43
☐	2023-04-09 22:36:51	资产	机异常事件	其他事件	新发现	高危	资产可能已经失陷，详情如下：资...	2023-05-16 21:53:21

共 92 项

50 条 / 页

⏮

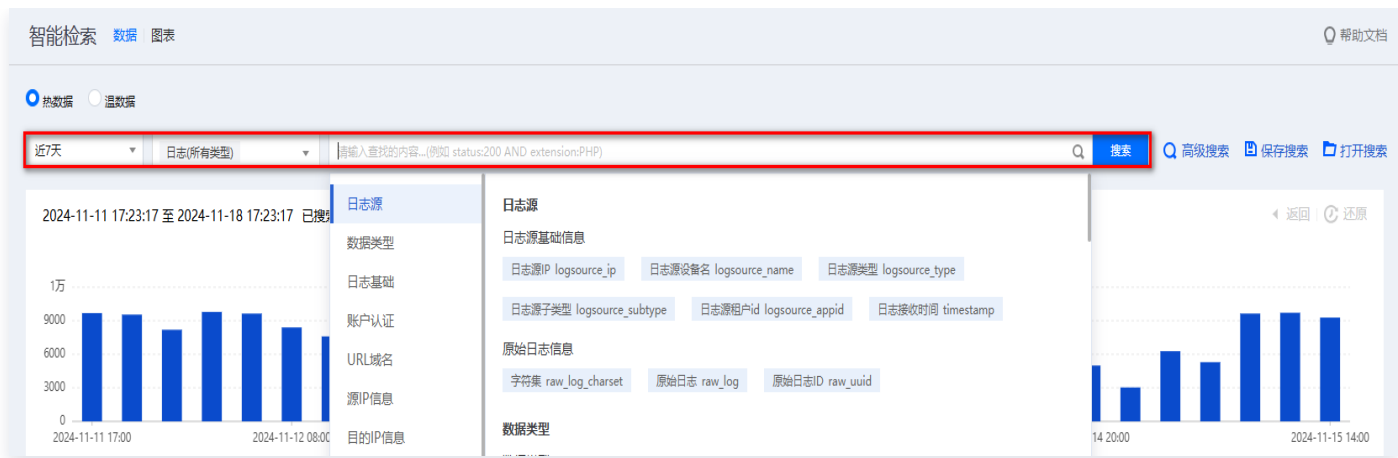
1

⏭

/ 2 页

智能检索

1. 在调查中心 > 智能检索页面，您可以根据时间、数据类型以及所需查找的内容进行搜索，单击搜索生成图表，管理员支持进行高级搜索。



2. 选择所筛选出的目标日志，单击导出，可将日志下载至本地；单击调查，可将日志添加到调查任务。

时间 timestamp	日志发生时间 event_timestamp	日志源设备名 logsource_name	日志源类型 logsource_subtype	源IP src_ip	用户ID user_id
2024-11-11 17:00	2024-11-11 17:00	app_log	其他日志分析与审计	-	-
2024-11-11 17:00	2024-11-11 17:00	app_log	其他日志分析与审计	-	-
2024-11-11 17:00	2024-11-11 17:00	app_log	其他日志分析与审计	-	-

调查任务

- 在调查中心 > 调查任务页面，支持按照时间范围、ID、调查名称、创建人进行搜索。

ID	调查名称	创建人	状态	创建时间	操作
			进行中	2024-11-18 18:54:39	详情 删除
			进行中	2024-11-18 18:54:39	详情 删除

- 在调查中心 > 调查任务页面，管理员单击新建，输入任务名称和任务说明，单击确定即可新建调查任务。

调查任务管理

任务名称 *

不超过64个字符

任务说明

不超过1024个字符

确定

取消

- 在调查中心 > 调查任务页面，选择目标 ID 并单击详情，支持对调查任务进行编辑、导出、删除和结束任务。

新建

删除

全部

近7天

近30天

近90天

选择时间

选择时间

ID/名称/创建人

Q

☐	ID	调查名称	创建人	状态 ▾	创建时间 ↓	操作
☐				进行中	2024-07-07	详情 删除
☐				进行中	2024-07-08	详情 删除
☐				进行中	2024-07-07	详情 删除
☐				结束	2024-07-06	详情 删除

日志列表

在调查中心 > 日志列表页面，管理员可以查看日志趋势和日志详情，还可进行日志的导出、响应和搜索等操作。

- 单击实时刷新开关，支持开启实时刷新事件信息功能。
- 支持根据时间范围、日志名称、类别、子类别、源 IP、目的 IP 等参考筛选所需日志，查看日志趋势和日志详情。
- 选择所需日志，支持进行日志导出、标签-添加标签/删除标签、响应操作。

日志列表

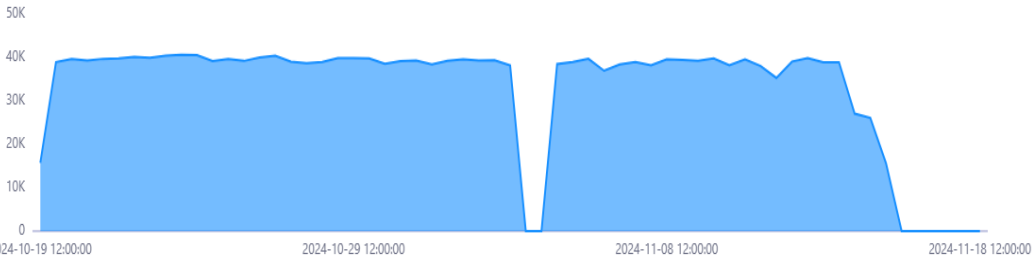
近24小时 近7天 近30天 2024-10-19 19:05:07 ~ 2024-11-18 19:05:07

与“调查中心”>“检索”搜索语法一致

条件搜索

全部展开

- 日志源类型
- 日志源子类型
- 数据类型
- 数据子类型
- 日志名称
- 类别
- 子类别
- 严重性
- 可信度
- 日志结果
- 源IP
- 目的IP
- 主机IP



收起图表

导出 标签 响应

实时刷新

已选择 2 项 选中全部 取消勾选

日志接收时间	日志发生时间	日志名称	类别	子类别	源IP	目的IP
☒	2024-03-2025:03	用户访问应用	登录操作	用户登录		
☒	2024-03-2025:03	用户访问应用	登录操作	用户登录		
☐	2024-01-2025:01	用户访问应用	登录操作	用户登录		
☐	2024-57-2025:57	用户访问应用	登录操作	用户登录		

响应中心

最近更新时间：2024-12-17 18:09:02

通过响应中心，管理员可以在发现安全日志或漏洞日志后进一步处置操作。目前支持工单通报，包括人工处置工单和联动 SOAR 的自动处置工单。

处置工单

在响应中心 > 处置工单页面，针对本系统分析出的安全告警及资产脆弱性，管理员可通过通报处置工单平台将不同的安全告警、漏洞按需下发给相关流转组或责任人进行处置，实现安全运营的分级响应与处置。

通知策略

在响应中心 > 通知策略页面，可以对本系统产生的安全告警设置通知策略，通过系统消息、邮件或短信进行通知，实现威胁信息的及时获取与感知。

通知策略									
新建 删除		ID/策略名称/创建人							
☐	ID	策略名称	分类 ▾	过滤条件	通知方式	创建人	更新时间 ▴ ▾	启停 ▾	操作
☐			告警	多个 (5)	消息		202	6 ☒	编辑 删除
☐			告警	多个 (5)	消息		202	9 ☒	编辑 删除
☐			告警	多个 (3)	消息		202	5 ☒	编辑 删除

联动响应

在响应中心 > 联动响应页面，联动阻断策略用于对已确定的威胁访问进行阻断。目前，本系统支持联动腾讯 NIPS 网络入侵防御系统进行阻断响应操作。

资产管理

最近更新时间：2024-12-17 18:09:02

在资产中心 > 资产列表页面，管理员可以查看网络环境中的资产详情和当前资产的安全事件、待处置告警和待修复漏洞，还可进行资产的新建、编辑、导入、导出、删除、搜索、编辑资产标签和添加资产组等操作。

- 支持通过时间范围、IP、资产名称、组件名称、组件版本筛选所需资产。

资产列表

近24小时近7天近30天全部2024-09-22 00:00:00 ~ 2024-11-18 00:00:00

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

聚合搜索视图搜索全部展开

资产类型

资产来源

所属系统

标签

重要性

操作系统

完整性资产权重

可用性资产权重

机密性资产权重

是否为新

是否有漏洞

是否物理机

资产负责人

资产名称

2024-09-22 00:00:00 至 2024-11-18 00:00:00 风险资产数趋势

新建删除导入导出添加到组更多操作

资产评分管理

资产名称	IP	资产分组	资产类型	资产来源	操作
	0	默认分组	服务器设备	多个(2)	编辑删除
			IOT设备	手动编辑或导入	编辑删除
		默认分组	服务器设备	手动编辑或导入	编辑删除
		默认分组	终端设备	手动编辑或导入	编辑删除
		默认分组	服务器设备	手动编辑或导入	编辑删除
		默认分组	安全设备	手动编辑或导入	编辑删除
		默认分组	网络设备	手动编辑或导入	编辑删除

- 单击新建，输入资产名称、资产类型、资产分组、网络参数、重要性等参数，单击确定即可创建资产。

新建/编辑资产

×

核心信息

资产名称

测试

资产类型

请选择

所属租户

请选择

资产分组

默认分组

组织分组

请选择分组

地理分组

请选择分组

网域分组

请选择分组

应用分组

请选择分组

资产负责人

支持多选或输入自定义词汇回车新增负责人，单个限64个字符

VPCID

- 选择目标资产，单击操作列的编辑，即可修改相关参数；单击更多操作，支持编辑标签、编辑其他字段。

新建

删除

导入

导出

添加到组

更多操作

①

资产评分管理 管理

已选择 1 项 选中全部 取消勾选

编辑标签

编辑其他

	资产名称	IP	资产分组	资产类型	资产来源	操作
☒			默认分组	服务器设备	多个(2)	编辑 删除
☐				IOT设备	手动编辑或导入	编辑 删除

- 选择目标资产，支持对资产进行删除、导入、导出、添加到组操作。

2024-09-22 00:00:00 至 2024-11-18 00:00:00风险资产数趋势

展开图表

新建

删除

导入

导出

添加到组

更多操作

①

资产评分管理 管理

已选择 2 项 选中全部 取消勾选

	资产名称	IP	资产分组	资产类型	资产来源	操作
☒		1	默认分组	服务器设备	多个(2)	编辑 删除
☒		1		IOT设备	手动编辑或导入	编辑 删除
☐		1	默认分组	服务器设备	手动编辑或导入	编辑 删除

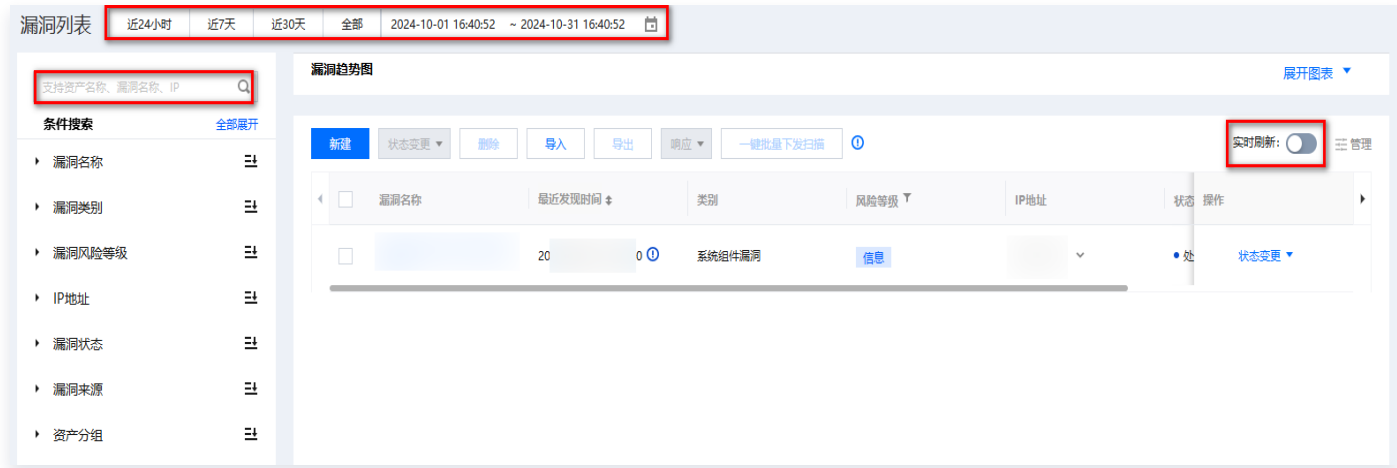
漏洞管理

最近更新时间：2024-12-17 18:09:02

漏洞列表

在漏洞管理 > 漏洞列表页面，管理员可以查看漏洞趋势和漏洞详情，还可进行漏洞的新建、导入、导出、响应、搜索、状态变更和批量下发扫描等操作。

- 支持通过时间范围、资产名称、漏洞名称、IP 筛选所需漏洞，单击实时刷新开关，支持开启实时刷新漏洞信息功能。



- 单击新建，输入漏洞名称、类别、风险等级、网络参数、重要性等参数，单击保存即可创建漏洞。

新建漏洞

×

* 漏洞名称

所属租户

请选择

▼

* 类别

请选择

▼

子类别

* 风险等级

请选择

▼

CVSS评分

—

0.0

+

漏洞CVE编号

漏洞CNNVD编号

漏洞CNVD编号

* IP地址

请输入“网段配置”中所定义范围的IP

全域名

VPC ID

—

1

+

漏洞标签

回车添加标签

* 漏洞状态

待处置

▼

取消

保存

- 选择所需漏洞，单击**状态变更**，可以选择将状态调整为待处置、处置中、已处置、忽略。

说明：

- 待处置：新发现的漏洞，还未进行处置。
- 处置中：漏洞正在处置中。
- 已处置：已完成对漏洞的处置。
- 忽略：漏洞可以不用处置。

漏洞趋势图

展开图表 ▼

新建

状态变更 ▼

删除

导入

导出

响应 ▼

一键批量下发扫描 ①

实时刷新: ☐

管理

① 已选择

待处置

处置中

已处置

忽略

最近发现时间 ⚙	类别	风险等级 ▼	IP地址	状态	操作
0 ①	系统组件漏洞	信息	▼	处	状态变更 ▼

漏洞任务

在漏洞管理 > 漏洞任务页面，支持创建单次扫描任务和周期扫描任务。

1. 在漏洞任务页面，选择所需任务类型，单击新建。

漏洞任务

单次扫描任务

周期扫描任务

新建

删除

☐	更新时间	任务名称	扫描器	待处置漏洞数
☐				0
☐				0

2. 在新建任务窗口中，配置相关参数，单击确定。

新建周期任务

×

* 任务名称

不能超过64字符

* 扫描器 ⓘ

请选择

▼

扫描IP范围 ⓘ

支持输入多个IP及网段，使用换行分隔，网段格式使用192.168.240.0/20

扫描资产组范围 ⓘ

请选择扫描的资产组范围

▼

扫描周期

每天

▼

任务启停

☒

确定

取消

参数名称	说明
------	----

任务名称	不能超过64字符。
扫描器	暂无数据时，请在 系统管理 > 安全性及其他设置 > 功能模块对接 > 漏洞扫描器对接配置 中配置。
扫描 IP 范围	支持输入多个 IP 及网段，使用换行分隔，网段格式使用192.168.240.0/20。
扫描资产组范围	仅可对不属于租户的资产组下发扫描任务。
扫描周期	仅支持周期扫描任务配置。
任务启停	仅支持周期扫描任务配置。

系统管理

最近更新时间：2024-12-17 18:09:02

数据接入

1. 在系统管理 > 数据接入 > 日志接入页面，选择安全日志接入。
2. 在安全日志接入页签，初始状态下，安全事件接入页面为空，可以进行安全事件日志源的新建、编辑、删除、控制开启/关闭和查看日志的操作。对于最近15分钟无数据上报的日志源，状态变为“不活跃”。

安全日志接入 自定义日志接入 探针管理											
新建		删除	开启	停用	快速排序	请选择接入方式		请选择活跃状态	请选择启用状态	请输入日志源名称或日志源ip的关键字进行	
☐	日志源名称	日志源	接入方式	绑定租户	创建人	日志源状态	解析策略组	解码方式	创建时间	最近流量接收时间	启用状态
☐				-		● 不活跃		UTF-8	2024	202	17
☐				-		● 不活跃		UTF-8	2024	202	10
☐				-		● 不活跃		UTF-8	2024	202	17

系统运维

在系统管理 > 系统运维页面，提供系统监控、版本管理、审计日志和消息中心的管理功能。

账号管理

本系统内置三个用户角色：超级管理员、普通管理员和审计员。只有超级管理员才能进行用户及权限管理。

知识库

ATT&CK 全称 Adversarial Tactics, Techniques, and Common Knowledge，框架由 MITRE 公司在 2013年首次提出，是用于描述攻击行为的知识库和模型，一个基于现实世界所观察到的真实攻击向量的集合，其包含了已公开报告的众多威胁组织及其使用的工具和攻击技术，可以作为红蓝对抗、安全运营人员提供良好的参考和学习指导。

在系统管理 > 知识库 > ATT&CK 页面，增加 ATT&CK 知识手册，提供战技术信息、适用平台、详细描述等信息。同时，支持通过战技术名称、技术 ID 进行搜索。

知识库

ATT&CK



▶ TA0001 初始访问 Initial Access	9
▶ TA0002 执行 Execution	12
▶ TA0003 持久化 Persistence	19
▶ TA0004 权限提升 Privilege Escalation	13
▶ TA0005 防御规避 Defense Evasion	39
▶ TA0006 凭证访问 Credential Access	15
▶ TA0007 发现 Discovery	27
▶ TA0008 横向移动 Lateral Movement	9
▶ TA0009 收集 Collection	17
▶ TA0010 泄露 Exfiltration	9
▶ TA0011 命令与控制 Command and Control	16
▶ TA0040 影响 Impact	13

安全性及其他设置

在系统管理 > 安全性及其他设置页面，包括登录安全、密码安全、自定义标题、自定义 Logo、与其他功能模块对接配置和第三方平台数据对接配置。