安全运营中心（SOC）

产品文档

腾讯云TCE

文档目录

操作指南
监测中心

最近更新时间: 2024-06-12 15:06:00

1 安全态势

安全态势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，极大提高安全运维团队监测、管理、处置安全事件的效率。 进入安全态势页面，可以查看企业在全网范围内的资产安全状况、最新待处理威胁、风险事件和安全事件趋势等，展示方式包括安全评分、趋势图、柱状图和分布图等，如图1-所示。

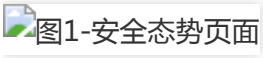

图1-安全态势页面

以查看近30天的安全态势为例，页面各区域说明如下： **1、值得关注和跟进的信息总览**

- 待处置的告警总数、待处置的漏洞数、待跟进的工单数以及与昨日的对比。
- 最近30天的告警总数、漏洞总数、事件总数以及与上个周期的对比和最近30日的日平均数。单击数字可进入告警管理页面、漏洞管理页面或事件管理页面，并过滤出对应的信息。
- 最近30天新增的工单数、调查任务数及其柱状统计图。单击数字可进入工单管理页面或调查任务管理页面，并过滤出对应的信息。

2、重点信息TOP50——告警、事件 最近30天内排名TOP50的告警和事件。单击名称可进入告警管理页面或事件管理页面，并过滤出对应的信息。

3、重点信息TOP50——风险资产、漏洞 最近30天内排名TOP50的风险资产和漏洞。单击名称可进入对应的资产详情页面或漏洞管理页面，并过滤出对应的信息。

4、告警总览/攻击者IP位置分布图

- 最近30天内产生的告警总数及其具体分类，包括资产失陷、横向渗透、权限提升、安装植入、攻击投递、扫描探测和环境配置。单击告警分类上方的数字可进入告警管理页面并过滤出对应的告警信息。
- 最近30天内产生告警的攻击者IP地理位置分布图。将鼠标悬浮在高亮点即可查看攻击者的国家/地区和IP地址，单击高亮点可进入告警管理页面并过滤出对应的告警信息。

2 态势大屏

提供针对租户安全场景的可视化大屏。展示了24小时以内、7天以内或30天以内的告警分布情况、告警趋势、告警TOP10、受害者IP TOP10、攻击者IP TOP10、安全防护漏斗图以及已处理告警数，如图2-所示。

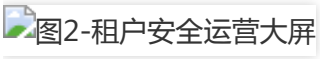

图2-租户安全运营大屏

告警与事件

最近更新时间: 2024-06-12 15:06:00

1 事件列表

进入事件列表页面，页面布局如图3-所示，与资产管理相似。管理员可以查看事件趋势和事件详情，还可进行事件的导入、导出、响应和搜索等操作。

图3-事件管理页面

图3-事件管理页面

1.1 事件搜索

在页面左侧的事件搜索栏中，除了选择详细类别，还可以直接输入lucene查询语句进行搜索。

> **说明：**
>
> 关于lucene查询语句的更多介绍，详见官方网址：
> http://imgcache.finance.cloud.tencent.com:80www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html

1.2 事件趋势图

选择时间范围查看事件的趋势，将鼠标悬浮在图中可以显示时间和事件数（与事件列表的数据实时同步）。单击【收起图表】可以将事件趋势图隐藏起来。

1.3 查看事件详情

在事件列表中，单击事件名称可以查看事件的严重性、信息概览和事件明细（对于日志源是御界的事件，还可以查看会话还原和PCAP信息），如图4-所示。

图4-事件详情

图4-事件详情

单击【编辑标签】即可为该事件添加标签。详见事件标签。

1.4 导出事件

在事件列表中，单击【导出】即可将所选事件导出为Excel文件，导出的事件内容即当前事件列表的展示列。

> **说明：**

> 导出事件之前，建议在事件列表的右上方，单击【管理】自定义事件列表的展示列。

1.5 事件标签

在事件列表上方，单击【标签】可以为所选的事件添加标签或删除已有标签，如图5-所示。

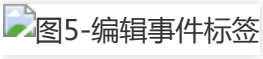

图5-编辑事件标签

1.6 事件列表快捷菜单

与告警列表的快捷菜单基本相同，详见告警列表快捷菜单。

2 告警列表

进入告警列表页面，页面布局如图6-所示，与资产管理相似。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。

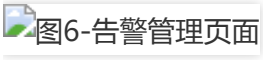

图6-告警管理页面

2.1 告警搜索

与事件搜索的操作相同，详见事件搜索。

2.2 攻击事件趋势图

选择时间范围查看攻击事件的趋势，将鼠标悬浮在图中可以显示时间和各类攻击事件数（与告警列表的数据实时同步）。单击【收起图表】可以将攻击事件趋势图隐藏起来。

2.3 攻击链分布图

选择时间范围查看攻击链的分布，将鼠标悬浮在色块上可以显示时间和对应攻击类别的事件数（与告警列表的数据实时同步）。单击【收起图表】可以将攻击链分布图隐藏起来。

2.4 查看告警详情

在告警列表中，单击告警名称可以查看告警的状态、威胁等级、可信度等级、发生次数、攻击结果、基本信息、攻击流程与信息、攻击者IP信息、攻击链阶段、告警描述、处置建议、告警明细和攻击链分析等，如图7-图9-图10-所示。 查看攻击者IP和受害者IP信息时，单击IP右侧的图标...弹出快捷菜单，可以针对该IP进一步操作，如图8-所示。

图7-告警详情（信息概述）

图8-告警详情（信息概述）-攻击者IP的快捷菜单

图9-告警详情（告警明细）

图10-告警详情（攻击链分析）

单击【变更状态】即可修改该告警的状态。

2.5 告警标签

与事件标签的操作相同，详见事件标签。

2.6 告警状态变更

如图11-所示，可以批量选择将告警的状态变更为处理中、已处理或误报。

图11-告警状态变更

2.7 导出告警

在告警列表中，单击【导出】即可将所选告警导出为Excel文件，导出的告警内容即当前告警列表的展示列。

> **说明：**
>
> 导出告警之前，建议在告警列表的右上方，单击【管理】自定义告警列表的展示列。

2.8 告警列表快捷菜单

在告警列表中，鼠标右键单击告警名称、攻击者IP、受害者IP、源IP、目的IP、关联规则ID、关联规则名、资产名称、资产组或者资产负责人，即可弹出快捷菜单，以便于一系列操作的连贯性。例如：鼠标右键单击受害者IP，弹出快捷菜单，如图12-所示。

图12-告警列表快捷菜单

> **说明：**
>
> 1）不同的告警字段和资产状态，对应的快捷菜单项也会稍有不同。
>
> 2）只有外网IP，才能进行威胁情报查询和Virus Total查询。
>
> 3）若要针对IP进行威胁情报查询，请联系售后支持人员获取安图高级威胁追溯系统的登录权限。

3 策略管理

展示目前用于判断告警的策略，支持搜索、过滤。

图13- 策略管理页面

资产中心

最近更新时间: 2024-06-12 15:06:00

1 资产列表

进入资产中心 > 资产列表，资产管理的页面布局如图14-所示。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。

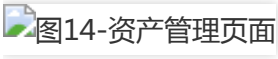

图14-资产管理页面

1、资产搜索栏

- 支持以下三种搜索模式：

  （1）简单搜索——在搜索框中输入资产IP、CIDR或资产名称进行搜索。

  （2）聚合搜索——按照资产类型、资产来源、重要性、资产IP和标签等类目，选择一个或多个条件进行搜索。

  （3）视图搜索——以树状结构展示资产的业务分组、组织分组、地理分组、网域分组和应用分组，选择一个或多个资产分组进行搜索。

  - 单击底部的即可添加或删除复合搜索模式的搜索类目。
  - 单击底部的即可将当前所选的搜索条件保存为快速搜索任务。
  - 单击底部的即可调取一个快速搜索任务，无需重新设置搜索条件。
  - 每个搜索条件都可排序显示，部分搜索条件还支持快速检索和“是非”快捷操作。
  - 不用资产搜索栏时，可将其隐藏起来。

2、新注册资产的系统提醒 显示当日新注册的资产数量，单击【查看详情】即可将新注册资产展示在资产列表中以便于进一步操作。关于资产注册的操作方法，详见注册资产。

3、险资产数量趋势图 展示近30天新发现风险资产数、已处置风险资产数与时间的关系，将鼠标悬浮在图中可显示具体日期及其对应的数量。单击【收起图表】可将风险资产数量趋势图隐藏起来。

4、资产列表 在资产列表的右上方，单击【管理】可以自定义资产列表的显示项，如图15-所示。更多介绍，详见查看资产详情至编辑资产标签。

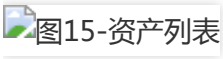

图15-资产列表

1.1 查看资产详情

如图15-所示，管理员在资产列表底部拖拽滚动条可以查看资产信息，还可以单击资产名称查看资产的完整信息：

- 资产注册信息（资产类型、资产来源、资产IP、端口、服务和域名）；
- 资产核心信息（资产名称、资产类型、资产分组、资产负责人、VPCID、网络接口、操作系统和资产发现时间等）；
- 资产安全指数（安全评分、重要性、待处置告警数、7天内事件数、待修复漏洞数），单击【一键更新】可即时更新该资产的安全评分；
- 资产拓展信息（资产所属部门、安全域、所属网段、探针名、设备ID和首次发现时间等）；
- 指定时间范围的待处置告警信息；
- 指定时间范围的安全事件；
- 待修复漏洞信息。

1.2 手动添加资产/添加到组

单击【新建】，填写资产的核心信息和拓展信息，如图16-所示。每个资产最多可配置10个IP/MAC。 若资产的业务分组尚未创建或暂不确定所属分组，可先处于"默认分组"状态；若添加资产后才确认资产组，批量选择资产并单击【添加到组】即可将其分组。

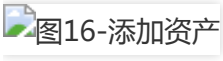

图16-添加资产

1.3 导入/导出资产

单击【导入】即可批量导入资产信息（需要从页面下载模板制作资产信息文件）。若导入时发生资产冲突，可以选择三种操作：撤销导入、仅导入新资产或者覆盖导入。 选中多个资产并单击【导出】，即可将所选资产信息导出为Excel文件。

> **说明：**
>
> 导入资产信息时，需要注意以下几点：
>
> 1）请提前在运营端中设置资产组，否则会导致导入的资产分组错乱。
>
> 2）导入的资产数量应控制在1万条以内；若填写的资产信息非常丰富，建议控制在2千条以内，避免因系统性能问题导致超时（若超过6分钟系统无响应，表示超时）。

1.4 编辑/删除资产信息

单击【编辑】，除了资产IP和APPID，其他信息均可修改；对于DHCP资产，MAC地址也不可修改。 单击【删除】或者选中多个资产并单击【删除】，即可删除所选资产。资产被删除后，历史数据（例如：事件和告警的关联资产信息）不会被清除。

1.5 编辑资产标签

选中单个或多个资产并单击更多操作> 编辑标签，即可为所选资产添加标签。资产标签可与事件联动，关联资产的事件会附带对应的资产标签。 选中单个或多个资产并单击更多操作> 编辑其他，即可批量选择字段并编辑各个字段的内容。

1.6 资产列表快捷菜单

与告警列表的快捷菜单基本相同，详见告警列表快捷菜单。

2 资产发现

资产发现页面如图17-所示，可以对自动发现的资产进行注册、导出、删除或编辑标签。

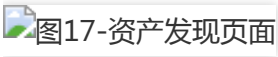

图17-资产发现页面

2.1 资产发现方式

若要监管网络环境中的资产安全，有两种方法添加资产：

- **手动资产同步**

  手动资产同步支持对接现有CMDB（配置管理数据库）、同步主机安全等系统中的资产信息、手动新建资产信息以及通过导入模板批量导入资产信息，实现资产的同步录入。

- **自动发现资产**

  对于无CMDB（配置管理数据库）及主机安全等相关系统的用户，本系统可通过流量探针自动发现网络环境中的相关资产，由自定义的资产网段筛选后，直接进入资产列表。

2.2 注册资产

对于自动发现的资产，需要进行注册才能进入资产列表接受安全监控。 **2.2.1 单个注册资产** 步骤1 在资产发现列表中单击操作栏下的【注册】。 步骤2 在弹出的注册资产页面中，填写该资产的核心信息和拓展信息。 步骤3 填写完毕，单击【完成注册】。 步骤4 进入资产列表页面，出现页面提示表示该资产注册成功，如图14-所示的区域3。 步骤5 注册后的资产，单击【编辑】定义它的资产类型和资产分组，单击【更多操作】定义它的标签或其他字段，单击资产名称查看它的告警、事件、漏洞详情和安全指数。 **2.2.2 批量注册资产** 步骤1 在资产发现列表中选中多个想要注册的资产。 步骤2 单击【批量注册】即可注册所选资产。 步骤3 批量注册资产之后，资产信息为空，建议进入资产列表通过编辑、更多操作-编辑其他或添加到组的功能继续补充。

漏洞

最近更新时间: 2024-06-12 15:06:00

聚合多种来源产生的漏洞事件，展示漏洞相关信息，为漏洞修复和资产风险管理提供支持。

1 漏洞列表

进入漏洞列表，漏洞管理的页面布局如图18-所示，与资产管理相似。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。

图18-漏洞管理页面

1.1 漏洞趋势图

选择时间范围查看漏洞的趋势，将鼠标悬浮在图中可以显示时间、修复漏洞数和发现漏洞数（与漏洞列表的数据实时同步）。单击【收起图表】可以将漏洞趋势图隐藏起来。

1.2 查看漏洞详情

在漏洞列表中，单击漏洞名称可以查看漏洞的基本信息、风险等级、状态、待修复资产数量、发现时间、漏洞编号、漏洞描述和修复建议等，如图19-所示。

图19-漏洞详情

1.3 查看漏洞状态

如图20-所示，将鼠标悬浮在漏洞状态的图标即可显示该漏洞最近10次状态修改记录。

图20-查看漏洞状态修改记录

1.4 查看漏洞发现时间

如图21-所示，将鼠标悬浮在最近发现时间的图标即可显示该漏洞最近10次发现的时间。

图21-查看漏洞发现时间

1.5 新建漏洞

在漏洞列表的上方单击【新建】，弹出新建漏洞页面填写各项信息，如图22-所示。其中，IP地址必须在“资产网段配置”定义的IP范围内。

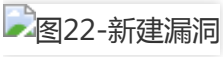

图22-新建漏洞

1.6 漏洞状态变更

如图23-所示，可以将漏洞的状态变更为待处置、处置中、已处置或忽略。既可单个操作也可以批量操作。

图23-漏洞状态变更

1.7 导入/导出漏洞

在漏洞列表中选中漏洞并单击【导出】，即可将所选漏洞导出为Excel文件。 在漏洞列表的上方单击【导入】，选择要上传的漏洞扫描报告及其对应的漏洞解析模板，即可将相关漏洞扫描系统扫描出的漏洞导入本系统，如图24-所示。

图24-导入漏洞文件

> **注意：**
>
> 导入漏洞文件时，请避免第三方平台的漏洞编号重复。

1.8 批量下发扫描任务

本功能仅适用于漏洞来源是天眼云镜的漏洞。 在漏洞列表中，选择单个或多个漏洞来源是“天眼云镜”的漏洞，单击【一键批量下发扫描】并选择与漏洞类型一致的扫描类型，如图25-所示。 下发成功后，进入漏洞任务 > 单次扫描任务，该任务状态是“进行中”，如图26-所示。

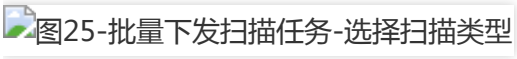

图25-批量下发扫描任务-选择扫描类型

图25-批量下发扫描任务-选择扫描类型

图26-漏洞扫描任务列表

图26-漏洞扫描任务列表

调查中心

最近更新时间: 2024-06-12 15:06:00

5.1 检索

管理员可以根据需要对本系统存储的数据进行检索，实现安全威胁的调查与分析。

5.1.1 日志

进入日志检索页面，页面布局如图27-所示。管理员可以进行高级搜索，将日志导出或生成图表，还可以添加到调查任务

图27-日志检索页面

1、帮助文档/数据源单位

- 日志检索的在线帮助文档，提供三种搜索方式的语法说明。在线查看文档时，单击【下载文档】可将PDF文档下载到本地。
- 在基础版或旗舰版的级联部署模式下，可以切换数据源单位进行日志搜索（本操作仅限超级管理员）。

2、日志搜索框

- 支持时间范围、日志类型和lucene查询语句进行日志搜索；单击【高级搜索】可以通过字段进行更精确的搜索。操作方法详见日志普通/高级检索。
- 单击【保存搜索】可以将当前搜索条件保存为搜索模板，以便于之后的搜索操作；单击【打开搜索】可以直接调用搜索模板并对其进行管理。操作方法详见日志检索模板。

3、日志统计柱状图 展示了符合搜索条件的日志在时间维度上的分布情况，包括时间范围、搜索用时和日志数量。将鼠标悬浮在柱状图上可显示具体时间及其对应的日志数量。

4、日志展示字段配置区 配置日志列表的展示字段，分为展示字段区和隐藏字段区。操作方法详见日志展示字段。

5、日志列表 以列表形式展示了符合搜索条件的日志详情，操作方法详见日志列表。

5.1.1.1 日志普通/高级检索

- **日志普通检索**

- **检索条件1：时间范围和日志类型**

日志搜索时，时间范围和日志类型不能为空，如图28-图29-所示。默认情况下，时间范围是“近24小时”，日志类型是“全部事件”。

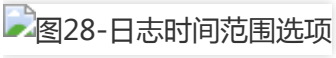

图28-日志时间范围选项

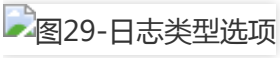

图29-日志类型选项

检索条件2：标签 通过标签可以进行更精确的日志搜索，同时支持标签的全部清空功能，如图30-图31-所示。

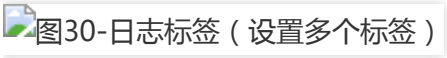

图30-日志标签（设置多个标签）

图31-日志标签（全部清空）

检索条件3：lucene查询语句 除了以上几个搜索条件，还可以直接输入lucene查询语句进行搜索，如图32-所示。

图32-日志检索（lucene查询语句）

日志高级检索 进行日志高级检索之前，系统会清空搜索框中的日志标签。 单击【高级检索】，可以设置多个搜索条件并匹配字段进行日志搜索，如图33-所示。

图33-日志高级检索

> **说明：**

> 关于lucene查询语句的更多介绍，详见官方网址：
> http://imgcache.finance.cloud.tencent.com:80www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html

5.1.1.2 日志检索模板

本系统支持检索模板的复用，可以将常用的检索场景进行保存，减少管理员重复操作。

- **保存检索模板**

  单击【保存搜索】填写搜索模板名称，即可将当前的检索条件存储为日志搜索模板，如图34-所示。

  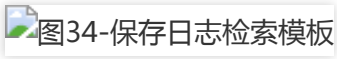

  图34-保存日志检索模板

打开检索模板 单击【打开搜索】单击某个日志搜索模板，即可快速检索，如图35-所示。

图35-打开日志检索模板列表

5.1.1.3 日志展示字段

可通过字段的展示/隐藏来控制日志列表的展示内容。

- **展示字段**

  展示字段，即日志列表的表头。若不想该字段出现在日志列表，单击字段旁边的图标即可下移到隐藏字段区域，如图36-所示。

  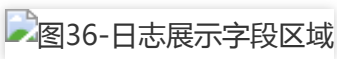

  图36-日志展示字段区域

- **隐藏字段**

单击隐藏字段旁边的图标即可上移到展示字段区域，该字段出现在日志列表的表头，操作方法与展示字段的基本相同。

- **搜索字段**

在日志展示字段配置区，可以进行字段的模糊搜索，如图37-所示。

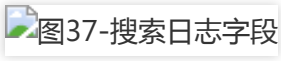

图37-搜索日志字段

查看字段值列表

单击某个展示字段名，显示该字段的日志数与占比TOP10，单击【下载】可以将当前日志字段值的全部内容导出为Excel文件，如图38-所示。

若字段值超过10个，单击【查看全部】即可查看所有字段值。对于源IP和目的IP，还可以单击图标进行字段值的过滤、排除、新建搜索和新建资产。

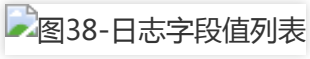

图38-日志字段值列表

5.1.1.4 日志列表

如图39-所示，符合搜索条件的日志出现在日志列表中，可以查看每个日志的Table和Json，也可以将所选日志导出、创建调查任务或添加到调查任务中。 单击))可以全屏展示日志列表；若日志字段太多导致日志列表查看不便，可单击将所有字段内容切换到列表中显示，如图40-所示。

图39-日志列表

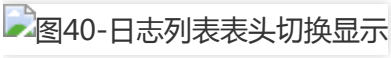

图40-日志列表表头切换显示

图40-日志列表表头切换显示

响应中心

最近更新时间: 2024-06-12 15:06:00

通过响应中心，可以在发现安全事件或漏洞事件后进一步处置操作。目前支持工单通报，包括人工处置工单和联动SOAR（自动化安全运营平台）的自动处置工单。

1 处置任务

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、事件及脆弱性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。

1.1 人工处置工单

进入响应中心 > 处置任务 > 人工处置工单，对于租户用户，只能看到自己创建和负责的工单信息；对于非租户用户，可以看到所有人工处置工单信息，如图41-所示。 对于超过2个责任人/流转组的工单，将鼠标悬浮在"多个（n）"即可显示具体的责任人或流转组名称。

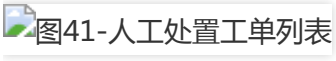

图41-人工处置工单列表

1.1.1 新建工单

在人工处置工单列表的上方，单击【新建】进入创建工单页面。创建一个完完整的工单步骤如下： 步骤1：在新建工单页面右侧填写个人信息，在页面左侧填写处置描述（支持三种模板），如图42-所示。

图42-新建工单（填写个人信息和处置描述）

步骤2：在新建工单页面左侧填写处置信息。若有告警需要处置，可以选择一个或多个告警，如图43-所示；若有漏洞需要处置，可以选择一个或多个漏洞，如图44-所示。

图43-新建工单（填写处置信息-要处置的告警）

步骤3：填写流转信息。选择下一阶段的处置动作、责任人/流转组、期望完成时间和逾期通知时间，如图45-所示。

图45-新建工单（填写流转信息）

步骤4：工单设置完毕，单击【确定】，该工单进入下一阶段，该工单下一阶段的责任人登录系统后会收到新工单的通知。

1.1.2 筛选/搜索工单

在人工处置工单列表的上方，可以通过以下条件进行人工处置工单的筛选/搜索：

- 时间范围（近24小时、近7天、近30天或自定义起止时间）
- 事件等级（极高危、高危、中危、低危或全部事件等级）
- 事件类型（有害程序事件、网络攻击事件、信息失窃密事件、信息内容安全事件、设备设施故障、灾害性事件、其他或全部事件类型）
- 工单创建人
- 工单责任人
- 工单逾期状态（是、否或全部逾期状态）
- 工单当前的处置动作（事件发现、事件研判、事件抑制、事件根除、事件溯源、事件关闭和全部处置动作）

在人工处置工单列表中，单击表头“ID”、“创建时间”或“工单处置时长”，可以按照工单ID、工单的创建时间或工单处置时长进行排序。

1.1.3 编辑工单

在人工处置工单列表中，单击工单名称即可进入人工处置工单的详情页，只有超级管理员角色的用户才有权限编辑工单。对于当前处置动作为“事件关闭”的工单，无法编辑。 如图46-所示，除了期望工单完成时间、逾期通知及通知方式，其余各项均可编辑。

图46-编辑人工处置工单

1.1.4 认领工单

在人工处置工单列表中，单击工单名称进入人工处置工单的详情页，认领工单的说明如下：

- 对于当前处置动作为“事件关闭”的工单，无法进行认领工单。

- 若当前用户是当前阶段的处置人或归属在处置组中，可以进行处置工单的操作。
- 若当前用户不是当前阶段的处置人或归属在处置组中，单击【认领工单】即可认领该工单。认领成功后，按钮变为【处置工单】，当前用户被加到当前阶段的处置人中。

1.1.5 处置工单

只有工单的当前责任人，才可进行处置工单的操作。 在人工处置工单列表中，单击工单名称进入人工处置工单的详情页，单击【处置工单】即可进行各项处置操作，如图47-所示。

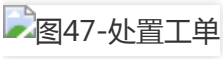

图47-处置工单

1.1.6 删除工单

在人工处置工单列表中，单击【删除】，确认后将删除对应的工单。

> **说明：**
>
> 1）工单一旦删除，将不可恢复，请谨慎操作。
>
> 2）只有工单的创建用户和超级管理员角色，才有删除工单的权限。

1.2 自动处置工单

使用自动处置工单之前，需要在运营端参考《API接口说明》进行自动工单API接口的设置。 进入响应中心> 处置任务> 自动处置工单，自动处置工单列表中显示联动 SOAR系统中自动创建的工单，如图48-所示。

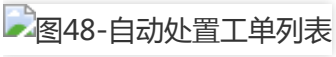

图48-自动处置工单列表

1.2.1 筛选/搜索工单

在自动处置工单列表的上方，可以通过以下条件进行自动处置工单的筛选/搜索：

- 工单优先级（严重、高危、中危、低危、信息和全部优先级）
- 工单状态（待处置、处置中、已处置、误报和全部状态）
- 事件名称的关键词

在自动处置工单列表中，单击表头“事件名称”或“时间”，可以按照触发工单的事件名称或时间进行排序。

1.2.2 查看工单详情

在自动处置工单列表中，单击事件名称或者操作栏下的【详情】，即可查看工单详情并安排工单，如图49-所示。 工单详情包括触发工单的事件名称、工单状态、事件的威胁等级/可信度等级/诊断结果、事件的基础信息和扩展信息。

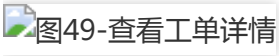

图49-查看工单详情

1.2.3 安排工单

在自动处置工单列表中，单击操作栏下的【安排】，即可将对应的工单进行流转。操作方法详见新建工单。

报表中心

最近更新时间: 2024-06-12 15:06:00

本系统内置两种报表模板，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进行统计和呈现，并可将报表导出为PDF文件。

1 报表列表

初始状态下，报表列表为空。只有在创建并生成报表任务之后，才会出现在报表列表中，并可对已生成的报表进行搜索、删除、导出和预览操作，如图50-所示。

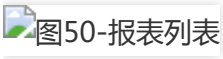

图50-报表列表

2 报表任务

报表任务分为单次报表任务和周期报表任务。

2.1 单次报表任务

进入报表中心 > 报表任务 > 单次报表任务，可以立即创建报表任务，如图51-所示。 单次报表任务创建后自动生成，并出现在单次报表任务列表中，如图52-所示。

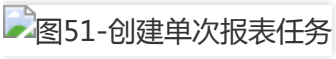

图51-创建单次报表任务

图52-单次报表任务列表

2.2 周期报表任务

进入报表中心 > 报表任务 > 周期报表任务，可以按“每日一次”、“每周一次”或“每月一次”创建周期报表任务，如图53-所示。 创建成功的任务出现在周期报表任务列表中，开启任务后，即可按指定时间生成报表，如图54-所示。

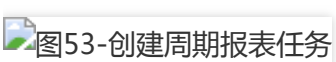

图53-创建周期报表任务

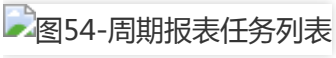

图54-周期报表任务列表

租户端日志采集接入SOC方案

最近更新时间: 2024-06-12 15:06:00

方案原理

租户侧overlay采集的日志设备ip<————物理网络服务映射————>SOC的isa1 IP，使得overlay采集的日志设备和SOC网络互通，overlay设备日志可以到达SOC。 以下接入方案以租户侧云堡垒机和数据库审计举例，其余租户侧设备均可参考。 注意事项：当前SOC可支持接入udp、tcp、syslog的端口号范围为514-550

堡垒机日志采集接入SOC

配置步骤

堡垒机信息收集

1. 登录租户端，申请overlay堡垒机实例（申请过程请自行查看堡垒机租户端用户手册），此台overlay堡垒机实例的ip为192.168.20.14；并在云服务器CVM找到这台堡垒机实例，记录VPC和subnet，此堡垒机实例分别为vpc-2at5y1pm 和waf-testt

2. 在账户中心找到APPID为1255000072.

SOC信息收集及配置

1. 登录运营端，打开安全运营中心，查看系统监控找到SOC相关的三台物理服务器IP

2. 分别ssh登录三台物理服务器IP，找到哪台是isa1，此环境中的isa1的IP为10.34.2.148.

3. 登录运营端，打开安全运营中心-系统-数据接入-日志接入-安全事件接入，填写上述获取的isa1的IP，接入方式为udp（系统内置），解析模板为腾讯堡垒机策略组，并记录使用端口为516，日志源名称为overlay_bh_1255000072.

网络映射配置

目的为了打通运营端SOC和租户测堡垒机网络连通性，将将SOC的IP映射到堡垒机网段

1. 登录运营端，产品运营-私有网络（VPC）-物理网络服务映射，填写上述获取的APPID、私有网络、子网（网络选择和堡垒机在同一个网络，是指将SOC的IP映射到堡垒机网段）、物理网络服务的isa1的IP和SOC配置的端口，此处的协议端口选择为UDP，端口号建议和SOC配置的端口保持一致为516

2. 记录自动分配的IP为192.168.20.17，此IP和堡垒机为同一子网。

堡垒机配置syslog转发

1. 登录overlay堡垒机，此环境为http://imgcache.finance.cloud.tencent.com:80192.168.20.14, 在系统管理-syslog配置端口和获取到的IP(SOC映射之后的IP)

2.使用overlay堡垒机，构建一些登录日志和运维日志。然后登录运营端，在告警和时间-事件管理查看是否有堡垒机相关日志。

多租户堡垒机syslog配置

多租户配置同样可以参考第二节步骤：

1. 堡垒机信息收集

2. SOC信息收集及配置

> **说明：**
>
> 当前无法根据日志内容识别堡垒机日志来自于哪个租户，所以在此步骤SOC创建日志源过程中，通过命名来区分租户，建议每个租户堡垒机创建一个日志接入源，命名为：overlay-bh-租户appid，如：overlay_bh_1255000072

3. 网络映射配置

4. 堡垒机配置syslog转发

数审日志采集接入SOC

配置步骤

数审信息收集

1. 登录租户端，申请数据库安全审计实例（申请过程请自行查看数据库安全审计租户端用户手册），此台overlay数据库安全审计实例的ip为172.16.0.40；并在云服务器CVM找到这台数审实例，记录VPC和subnet，此数据库安全审计实例分别为vpc-2at5y1pm 和waf-test

2. 在账户中心找到APPID为1255000068.

SOC信息收集及配置

1. 登录运营端，打开安全运营中心，查看系统监控找到SOC相关的三台物理服务器IP

2. 分别ssh登录三台物理服务器IP，找到哪台是isa1，此环境中的isa1的IP为10.34.2.148.

3. 登录运营端，打开安全运营中心-系统-数据接入-日志接入-安全事件接入，填写上述获取的isa1的IP，接入方式为tcp（系统内置），解析模板为数盾策略，并记录使用端口为518，日志源名称为overlay_数审_1255000068.

网络映射配置

目的为了打通运营端SOC和租户测数据库安全审计网络连通性，将将SOC的IP映射到数据库安全审计网段

1. 登录运营端，产品运营-私有网络（VPC）-物理网络服务映射，填写上述获取的APPID、私有网络、子网（网络选择和数据安全审计实例在同一个网络，是指将SOC的IP映射到数据库安全审计网段）、物理网络服务的isa1的IP和SOC配置的端口，此处的协议端口选择为TCP(数审只支持tcp外发syslog)，端口号建议和SOC配置的端口保持一致为518

2. 记录自动分配的IP为172.16.0.22，此IP和数据安全审计实例为同一子网。

数审配置syslog转发

1. 登录overlay数据安全审计实例，此环境为http://imgcache.finance.cloud.tencent.com:80172.16.0.40 在系统管理-syslog配置端口和获取到的IP(SOC映射之后的IP)

2. 告警开关打开syslog告警及相关告警内容

3. 使用overlay数据库安全审计，构建一些登录日志和运维日志。然后登录运营端，在告警和时间-事件管理查看是否有数据安全审计相关日志。

多租户数审syslog配置

多租户配置同样可以参考第二节步骤：

1. 数审信息收集

2. SOC信息收集及配置

> **说明：**
>
> 当前无法根据日志内容识别数据库安全审计日志来自于哪个租户，所以在此步骤SOC创建日志源过程中，通过命名来区分租户，建议每个租户数据库安全审计创建一个日志接入源，命名为：overlay-数审-租户appid，如：overlay_数审_1255000068

3. 网络映射配置

4. 数审配置syslog转发

产品简介
产品概述

最近更新时间: 2024-06-12 15:06:00

什么是安全运营中心

安全运营中心(SOC)（以下简称SOC），是面向政府以及金融、制造业、医疗、教育等大型企事业单位推出的一款以安全大数据分析和可视化为基础的智能化安全运营平台。SOC围绕安全运营和风险管理，构建了以安全检测为核心、以事件分析和威胁情报为重点、以可视化为特色、以可靠服务为保障，可针对企业面临的外部攻击和内部潜在风险进行深度检测，为企业提供及时的安全告警。通过对海量数据进行多维度分析、及时预警，并且对威胁及时做出智能处置，实现企业全网安全态势可知、可见、可控的闭环。

主要功能

监控检测、事件分析、取证调查和处置响应是安全运营过程中的核心任务。

监测中心

通过仪表板或态势大屏，总览全企业范围内的资产安全状况、最新待处理威胁、风险事件、安全事件趋势等值得关注的安全信息。

资产中心

为用户提供资产可视功能，从资产角度了解安全态势，盘点现有资产，对资产进行编辑管理，同时方便运维人员对企业内网资产进行管理。可对用户环境中的各个资产实现列表管理，包含列表呈现各个资产基本信息，例如资产名称、资产IP、资产来源、资产分组等。用户可选取资产列表中的相关资产以Excel表格的形式进行导出。针对单个资产的详细信息，御见提供详细直观的可视化展示，包含该资产的详细信息、安全告警、安全事件及脆弱性的展示。

漏洞管理

实时收集互联网最新安全漏洞情报，扫描内网资产安全状况，发现并生成漏洞事件，方便运维跟踪处理。

告警与事件管理

将接收的日志归一化为事件，经关联引擎匹配告警策略，生成安全告警，帮助用户调查分析、溯源事件、联动处置问题。

调查中心

供用户对日志进行查询、检索。通过接收并保存企业内部各种设备日志及流量日志，提供给安全运维人员进行关键字段筛选搜索。

响应中心

通过响应中心，可以在发现安全事件或漏洞事件后进一步处置操作。目前支持工单通报与流转。

报表中心

可根据用户实际需求制定并输出安全报表，方便安全运维人员总结一段时间内的安全工作成果，提供向上汇报，内部总结分析的材料支撑。

订购管理

提供用户对安全运营中心(SOC)的订阅、取消订阅、查看订阅信息的功能

产品优势

最近更新时间: 2024-06-12 15:06:00

1. 大数据平台支撑技术

云平台多年的大数据分析处理能力赋能到 SOC 平台中，使得本产品在以下几个方面优势明显：

- 海量数据处理能力：SOC 支持 PB 级别的数据分析与存储。
- 数据处理性能：流量处理能力达到10Gbps，并可支持平行扩展。

SOC 具备支持不同来源、不同类型、不同格式的数据聚合能力。具体数据源包括以下几方面：

- 网络流量：通过将核心交换或其他网络节点上的流量旁路到智能态势感知平台的流量探针。
- 设备、主机和系统日志：支持主流网络设备日志、Windows 系统日志、Linux 系统日志等。
- 业务及应用的日志：Web 服务器日志（IIS 日志、nginx 等常见Web日志）、代理服务器日志、FTP 日志、VPN 日志、RDP 日志、主流数据库日志等。
- 安全设备事件日志（告警日志）：支持安全设备、安全软件的安全事件日志（例如：哈勃沙箱的分析日志）、防火墙、WAF 的拦截日志以及终端安全软件日志。

2. 无代码扩展安全检测能力

SOC 的 AI 引擎运用了基于 AI 的分析和检测技术，将 AI 方面的探索应用于网络安全，使用传统规则引擎与机器学习智能算法相结合的分析技术，配合丰富的业务场景与安全场景，最终实现风险发现和威胁检测的能力，即安全感知。 安全监测手段包括以下几方面：

- 基于特征、统计及关联规则的威胁感知；
- 基于威胁情报匹配的威胁感知；
- 基于机器学习的流量异常感知。

能够覆盖的部分典型场景如下：

- 内部威胁：能够有效识别异常的主机行为、用户行为（例如：发现对关键资产的异常访问、敏感数据的外发等），进而识别口令失窃、越权访问、内鬼等企业内部的安全威胁。

- 横向移动：黑客在攻陷某一主机后，为扩大控制范围会尝试横向移动（例如：扫描、爆破、文件感染、流量代理等）。SOC能够检测到攻击者的这类横向移动行为。

- 黑客牟利：能够检测到典型的黑客牟利手段和对应恶意行为（例如：外发垃圾邮件、对外扫描、爆破、刷广告、挖矿等）。

- 隐蔽通道检测：能够检测 DGA 等较为隐蔽的C2方法，能够检测 DNS 隧道、文件类型伪造等用于隐蔽数据传输的方法。

- 恶意流量识别：能够使用不基于特征的智能检测模型从网络流量中识别到恶意软件的通信流量，进而识别出疑似失陷主机和C2服务器。

- APT 攻击：能够对来路不明的对象（例如：邮件附件、可疑链接等），结合沙箱进行深度分析，判定其恶意性，进而提升APT 攻击的对抗能力。

3. 威胁情报能力

百亿级恶意文件样本库、数亿级 IP 信誉库、域名信誉库、木马病毒样本、日均新增100W+、数千万级恶意网址、高质量情报云查、数十万级漏洞情报……SOC 内置的威胁情报关联能力，在关联分析中能够将系统采集到的流量、各种安全日志和事件与威胁情报进行碰撞比对。

应用场景

最近更新时间: 2024-06-12 15:06:00

安全管理合规运营

需要对安全事件、漏洞、资产等安全要素进行全方面运营，感知整体安全态势，满足等保2.0关于日志审计、安全管理等合规需求。

- 网络流量和安全设备日志都是安全运营中心（私有云）的数据来源。
- 网络流量会先经过高级威胁检测系统探针处理。

  高级威胁检测系统(以下简称NTA)，是基于腾讯云金融专区 的安全能力、依托腾讯云金融专区 在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统。凭借基于行为的防护和智能模型两大核心能力，NTA可高效检测未知威胁，并通过对企业内外网边界处网络流量的分析，感知漏洞的利用和攻击。

多级安全管理

用于安全运营情况监管场景，例如，上级单位需要对下级的安全情况有统一了解。

- 单网络出口和多网络出口部署情形相类似，通常多出口的情况下需要有多套探针来分别采集对应的出口流量。

多租户场景

支持租户数据隔离与账号分发，借助平台可实现租户安全托管服务与租户自服务。

常见问题

最近更新时间: 2024-06-12 15:06:00

软件化部署时，如何计算存储资源？

安全运营中心（私有云）将对网络流量进行解析并存储全流量日志，会占用较大的存储资源，按经验值，1G流量每三个月需要消耗40T存储空间。

- 收集第三方日志时，存储空间需要另行计算。

安全运营中心（私有云）可以管控安全设备吗？

安全运营中心（私有云）定位为感知分析，将流量、日志等数据汇聚后，进一步关联分析与展现。安全运营中心 (私有云）不对其他设备进行管理与控制。

安全运营中心（私有云）的大屏可以定制吗？

安全运营中心（私有云）提供两块标准 2D 大屏（资产安全态势和威胁态势），同时可对接 3D 态势大屏。通常情况下，用户可根据业务需要进行 3D 大屏定制，但会收取定制费用。

安全运营中心（私有云）支持哪些部署模式？

安全运营中心（私有云）采用软件化部署模式，但对部署的机器性能有一定的要求。主要要求如下：

方案组件	系统组件	组件功能	1G流量	5G流量	备注
高级威胁检测系统探针	流量分析引擎	流量分析	CPU：E5-2630v4（10核 2.2G主频）* 1 内存：64G DDR4 硬盘：2T 网卡：1G * 2电口 文件分析量：1w - 1.5w/天	【CPU：E5-2670v4（12核 2.3G主频） * 2 内存：128G DDR4 硬盘：4T 网卡：10G * 2电口】* 2套 文件分析量：4w - 6w/天	-
		哈勃沙箱			

方案组件	系统组件	组件功能	1G流量	5G流量	备注
安全运营中心（私有云）平台	大数据存储平台	HIVE + HDFS	【CPU：E5-2630v4（10核2.2G主频）* 1 内存：64G DDR4 硬盘：10T 网卡：1G * 2电口】* 3套	【CPU：E5-2670v3（12核2.3G主频）* 2 内存：256G DDR4 硬盘：20T 网卡：10G * 2电口】* 3套	1. 大数据平台按分布式部署，最少需要3台服务器；且支持平行扩容。 2. 离线存储可按用户实际的需求确定，平台支持存储资源平行扩容。
	日志解析引擎	TCE3100安全日志			
		第三方日志			
	安全分析引擎	智能安全检测			
	溯源分析引擎	全文索引			

如何购买安全运营中心（私有云）？

安全运营中心（私有云）处于产品内测期间，如需使用，请提交内测申请，申请通过的用户将收到站内信和短信通知，详情请参见购买指南。