安全湖

产品动态

腾讯云

【版权声明】

【商标声明】

【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。

产品动态

最近更新时间：2024-11-05 15:46:42

2024年10月

动态名称	动态描述	发布时间	相关文档
检索能力优化	• 检索任务优化，新增了三种检索结果完成的方式，允许用户通过多种方式进行分析或在安全湖之外进行分析，主要的目的是为了方便用户的多种数据分析形式。 • 增加了检索的默认配置，避免用户之前的每次都要进行常用的检索配置。如结果 limit 的上限、默认习惯的查询模式、每格的展示字段等。 • 检索分析业务逻辑优化，现在用户如果在检索过程中关闭或者切换到了其他页面，检索进程会立即停止，减少计算资源损耗。	2024-10-21	-
用户体验优化	• 图表编辑/仪表盘编辑逻辑已优化，现增加了离开确认提示，以防止用户因误操作而导致数据丢失。 • 告警列表性能优化，提升查询速度。	2024-10-21	-
SPL 函数覆盖	SPL 函数扩充，常用函数覆盖率70%+。	2024-10-21	-

2024年08月

动态名称	动态描述	发布时间	相关文档
分析效率提升	• 引入中间表，现在允许用户通过检索任务直接创建中间表，提升各模块的分析效率。 • 图表现在也支持采样检索，主要目的还是为仪表盘、图表的查询加速服务，整体提升用户的可视化体验。 • 新增了仪表盘预查询机制，加速查询结果的展示。对于数据量即较大的仪表盘，不需要用户继续在页面等待结果刷新。	2024-08-23	-
数据处理能力提升	• 优化了数据处理的逻辑，数据接入支持未解析直接存储，无需配置处理任务。	2024-08-23	-

	• 优化了数据处理的操作逻辑，现在数据源为 TCP/UDP 时默认选数据源 IP 为自动识别 ，不需要用户建立多个解析任务才能够将数据接入。		
情报结果抑制	情报回溯增加了结果抑制的能力，解决用户告警疲劳。	2024-08-23	-

2024年07月

动态名称	动态描述	发布时间	相关文档
用户体验提升	• 优化了大部分模块的时间过滤器，现在允许用户通过简单的 data_math 来快速的过滤出指定时间，提升整体操作便捷性。 • 新增了富化字段引用时进行校验的逻辑，在配置安全检测规则的时候，如果用户错误的引用了或者引用了不存在的字段，系统会给予明确提示。 • 解决了之前版本一些错误问题，合入到当前版本中。	2024-07-26	-
检索加速优化	检索加速，现在支持进行结果 limit 配置以及采样检索配置。	2024-07-26	-
漏洞回溯能力增强	漏洞回溯结果丰富，新增了 url、domain 字段，并且能够通过狩猎规则进行富化。	2024-07-26	-
新增告警结果抑制能力	新增了告警抑制的业务，能够通过时间、告警字段来进行告警的抑制，并且新增了告警最大的 limit 限制，来抑制生成的告警数量。	2024-07-26	-
检索能力优化	• 检索能力优化，新增一键隐藏空白字段功能，帮助用户快速过滤空数据。 • 简易检索操作优化，现在允许将检索结果添加至检索条件中 • 新增了特别关注的业务，现在允许用户对数据库表进行特别关注的操作，这类表格将会保持在最上方展示，方便用户快速定位关键数据。	2024-07-12	-
新增高级过滤业务	支持高级条件自定义（包括 IP 白名单、情报类别白名单、复杂函数条件等过滤）在现有的固定化的配置基础上，增加高级的条件支持，用于可以输入任意合法的过滤条件。	2024-07-12	-

用户体验提升	• 新增一键隐藏空数据表的功能，帮助用户过滤一些无用数据表。 • 支持 SQL 的格式化，一键操作。	2024-07-12	-

2024年06月

动态名称	动态描述	发布时间	相关文档
情报回溯优化	• 情报回溯效率优化，整体效果优化后提升80%。 • 情报回溯任务支持 crontap，灵活配置执行间隔时间。	2024-06-29	-
用户操作体验提升	• 简易检索操作简化，新增多种快捷条件，支持在检索模块、全流量溯源分析模块调用。 • 优化了新建查找表时的错误提示，解决之前无法识别的问题。	2024-06-29	-

2024年04月

动态名称	动态描述	发布时间	相关文档
新增全流量溯源分析专题	新增全流量溯源分析专题，帮助用户检索以及管理接入后的流量数据，单独作为一个独立模块使用。	2024-04-26	-
情报回溯能力优化	情报回溯能力优化，增加了针对回溯结果的统计计算场景。	2024-04-26	-
用户体验提升	• 优化了简易检索的交互查询，降低用户的操作难度，以及学习成本。 • 加工函数能力加强。 • 可视化图表支持配置默认时间区间。 • 新增了检索的实时反馈，支持检索结果流式返回。 • 增加了标识来区分系统数据表、用户自建表。	2024-04-26	-
App 扩展以及通知	• 检索界面优化，语句输入框支持高度自适应。 • 图表优化，支持 App 间图表单独计算以及数据隔离。	2024-04-12	-

	• 数据源处理能力优化，支持历史数据以及记录清除。 • 消息通知能力新增支持腾讯云短信、企业微信等方式。 • 原生 App 支持扩展，并支持导入图表、解析策略以及安全规则等；App 扩展支持微信公众号通知。		

2024年03月

动态名称	动态描述	发布时间	相关文档
检测规则逻辑优化	安全告警检测规则优化，新增 crontab 的方式。	2024-03-15	-
底层能力优化	• ETL 函数优化，降低操作以及使用复杂程度。 • 中间件支持适配 PostgreSQL/Kafka。 • 节省优化存储空间，增加对数据源以及数据量的默认限制。 • 情报库自动更新业务优化等。	2024-03-15	-

2024年02月

动态名称	动态描述	发布时间	相关文档
新增漏洞回溯专题、情报回溯专题	• 支持全存储各类流量数据，扩展流量检测能力并支持长周期回溯分析。 • 支持针对热点 APT 组织进行攻击回溯并持续跟踪，使用威胁情报扫雷。 • 内置漏洞威胁狩猎规则，支持对0Day漏洞等进行及时响应以及风险排查。	2024-02-29	-
可视化能力增强	新增单值图、词云等图表类型，图表类型丰富以及扩充。	2024-02-29	-
数据处理能力优化	• 键值对和分隔符的抽取规则支持配置不可见字符。 • 解析规则支持批量的导入导出。	2024-02-29	-
稳定版发布	• 围绕稳定性和高可用提供故障恢复方案、监控告警等能力。 • 情报回溯和匹配支持腾讯情报 SDK。	2024-02-19	-

	• 支持异步检索，可对结果进行聚合分析。 • 增加加工函数，提升数据解析能力。		

2024年01月

动态名称	动态描述	发布时间	相关文档
产品改名为安全湖（Security Lake）	安全数据湖（ Security Data Lake ）改名为安全湖（ Security Lake ）。	2024-01-16	产品概述

2023年08月

动态名称	动态描述	发布时间	相关文档
安全数据湖（Security Data Lake）上线	安全数据湖（Security Data Lake）是一款基于云原生技术打造的高性能、低成本、纯自研、国产的安全大数据分析平台，为企业提供一体化的泛安全数据接入、加工、存储、分析、告警、可视化等服务，具备“插件化”应用开发能力，助力企业构建云原生湖仓一体安全分析平台。	2023-08-29	产品概述