kaspersky 引領未來

Kaspersky CyberTrace

信息安全分析师每天处理的安全警报数量呈指数级增长。要分析的数据如此之多，几乎不可能实现有效的警报优先级划分、分类和验证。不计其数的安全产品发出的警报源源不断，导致重要警报被掩埋在一片无用的噪声之中，让分析师精疲力尽。SIEM、日志管理和安全分析工具能够汇总安全数据并关联相关警报，帮助减少需要额外检查的警报数量，但安全分析师依然不堪重负。

威胁情报以不同的格式显示，并包括大量的入侵指标（IoC），导致 SIEM 或网络安全控制机制难以消化处理。

实现有效的警报分类和分析

通过将最新的可机读威胁情报整合到现有的安全控制机制（如 SIEM 系统）中，安全运营中心可以自动化初始分类流程，同时为其安全分析师提供足够的情景信息，以立即识别出哪些警报需要调查或上报给事件响应团队，以开展进一步的调查和响应。然而，威胁数据订阅源和可用威胁情报来源的数量持续增长，使得组织机构难以确定哪些信息与他们相关。威胁情报以不同的格式显示，并包括大量的入侵指标（IoC），导致 SIEM 或网络安全控制机制难以消化处理。

卡巴斯基网络威胁追踪服务是一款威胁情报平台，可实现威胁数据订阅源与 SIEM 解决方案的无缝集成，帮助分析师更有效地在现有安全运营工作流程中利用威胁情报。它能与您可能想要使用的任何 JSON、STIX、XML 和 CSV 格式的威胁情报订阅源（来自卡巴斯基、其他供应商、OSINT 的威胁情报订阅源或您的自定义情报订阅源）进行集成，并支持与众多 SIEM 解决方案和日志源的开箱即用集成。

卡巴斯基网络威胁追踪服务采用一种内化流程对传入数据进行解析和匹配，从而大大降低 SIEM 的工作负载。它会解析传入的日志和事件，迅速将所获得的数据与数据订阅源进行匹配，并在威胁检测中生成自己的警报。解决方案集成的架构概览如下图所示：

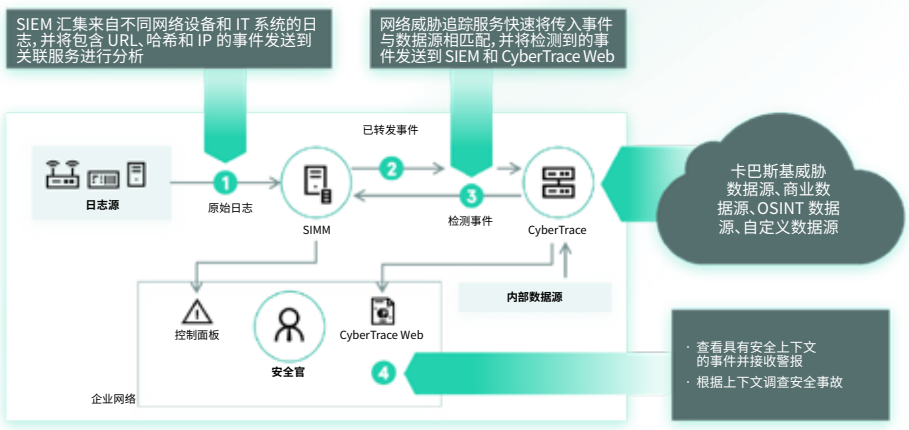

图 1.卡巴斯基网络威胁追踪服务集成架构

产品功能

卡巴斯基网络威胁追踪服务提供了一套工具，用于操控威胁情报，以进行有效的警报分类和初始响应：

- 指标数据库包含全文搜索功能，并且支持使用高级搜索查询进行搜索，从而实现跨所有指标字段（包括上下文字段）的复杂搜索。支持按情报供应商筛选结果，从而简化分析威胁情报的过程。
- 包含有关各指标详情的页面，可提供更深入的分析。每个页面都呈现了所有威胁情报提供者就某个指标提供的所有信息（删除重复数据），这让分析师可以在评论中讨论威胁，并添加关于该指标的内部威胁情报。如果检测到相应指标，则提供检测日期的信息和检测列表的链接。

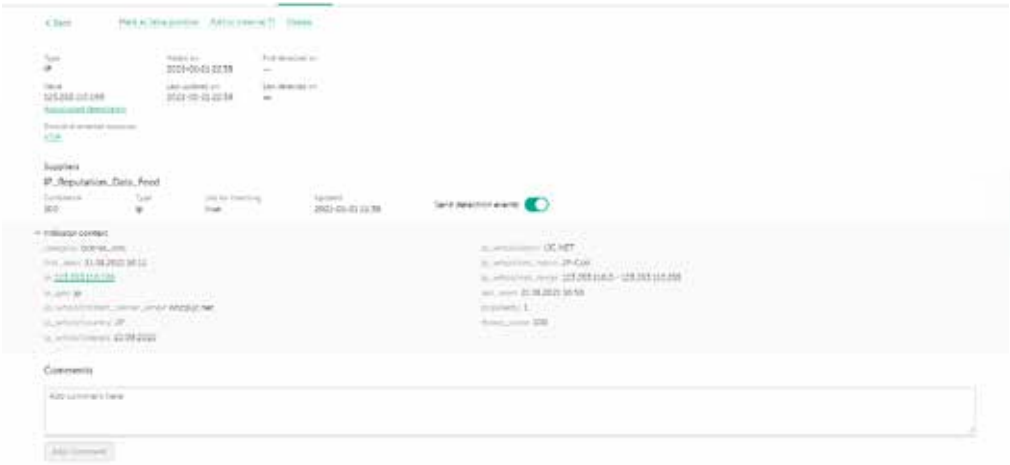

图 2.来自所有威胁情报提供者的，针对某一项指标的详细信息

- 研究图表可让您视觉化探索存储在 CyberTrace 中的数据和检测并发现威胁共性。它可通过图表视觉化网址、域、IP、文件和调查期间遇到的其它上下文之间的关系。图表包括以下功能：转换，迷你图表，分组节点，手动添加链接，添加指标和搜索图表上的节点。

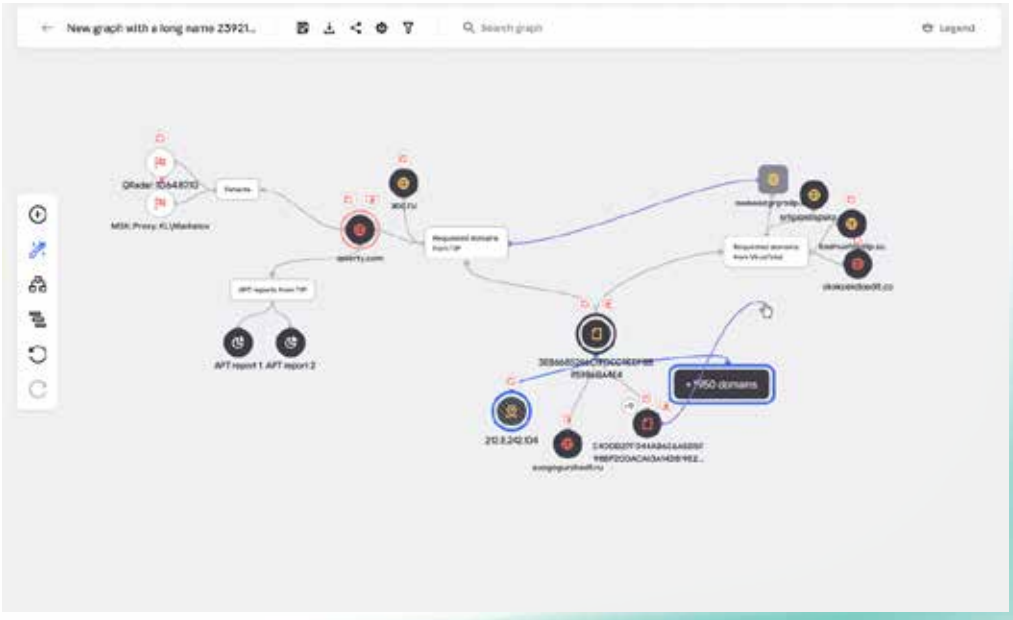

图 3.研究图表

· 指标导出功能支持将指标集导出到安全控制机制，如策略列表（阻止列表），以及在卡巴斯基网络威胁追踪服务实例之间或与其他威胁情报 (TI) 平台共享威胁数据。

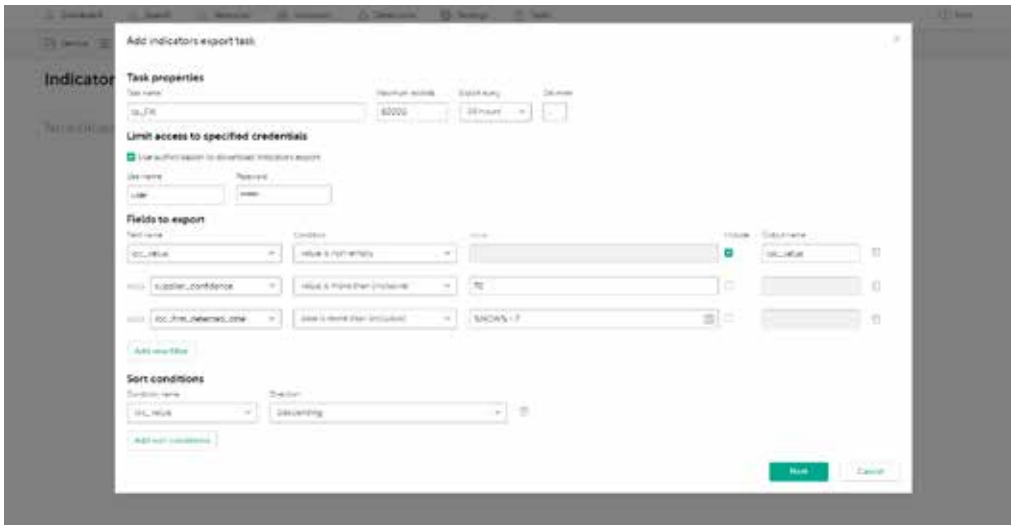

图 4.指标导出任务

· 给入侵指标做标签可简化其管理。您可以创建任何标签并指定其权重（重要性），使用它手动给入侵指标做标签。您也可以基于这些标签及其权重来排序和筛选入侵指标。

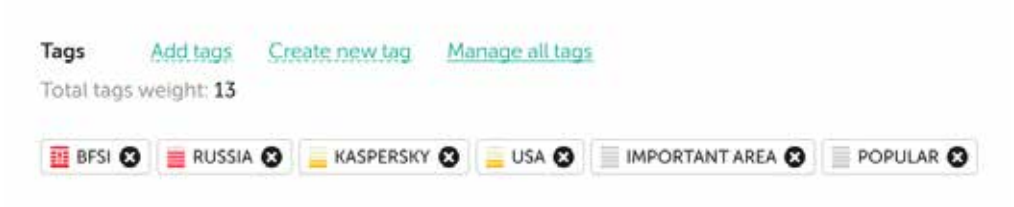

图 5.入侵指标标签

· 历史关联功能（回溯扫描）使您可以使用最新的数据订阅源来分析先前检查过的事件中的可观察信息，以发现先前未发现的威胁。报告中包含所有历史检测结果，以供将来调查时使用。

· 用于将检测事件发送到 SIEM 解决方案的筛选器可以减轻 SIEM 解决方案的负担，也为饱受警报疲劳困扰的分析师减负。它允许您只将最危险的检测结果发送到 SIEM，也就是说只发送那些必须作为事故处理的检测结果。所有其他检测结果都会被保存到内部数据库中，并可在根本原因分析或威胁搜索中使用。

· 在服务提供商（中央办公室）需要分别处理来自不同分支机构（租户）的事件时，多租户功能可以支持 MSSP 或大型企业使用系统实例。这样一来，单个卡巴斯基网络威胁追踪服务实例就可以与来自不同租户的不同 SIEM 解决方案相连接，并且您可以配置每个租户要使用哪些数据订阅源。

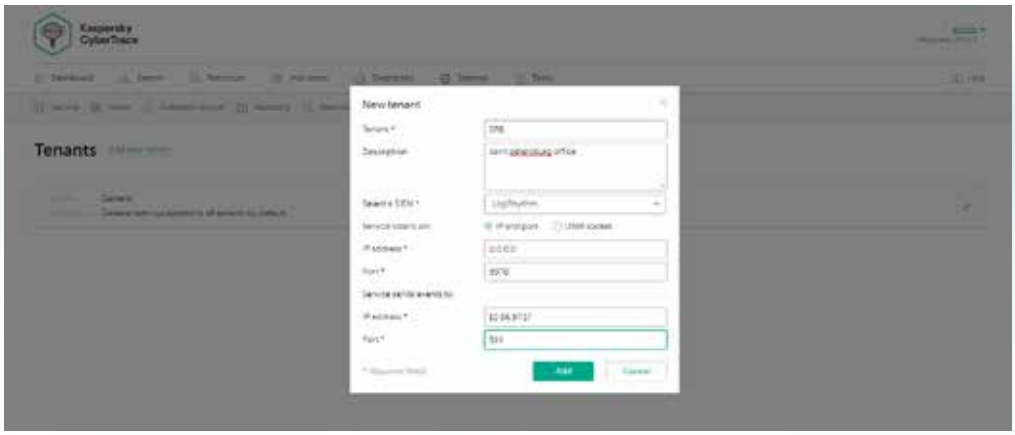

图 6.新租户创建

· 数据订阅源使用情况统计信息会衡量集成数据订阅源和数据订阅源交叉矩阵的有效性，有助于选择最有价值的威胁情报提供者。

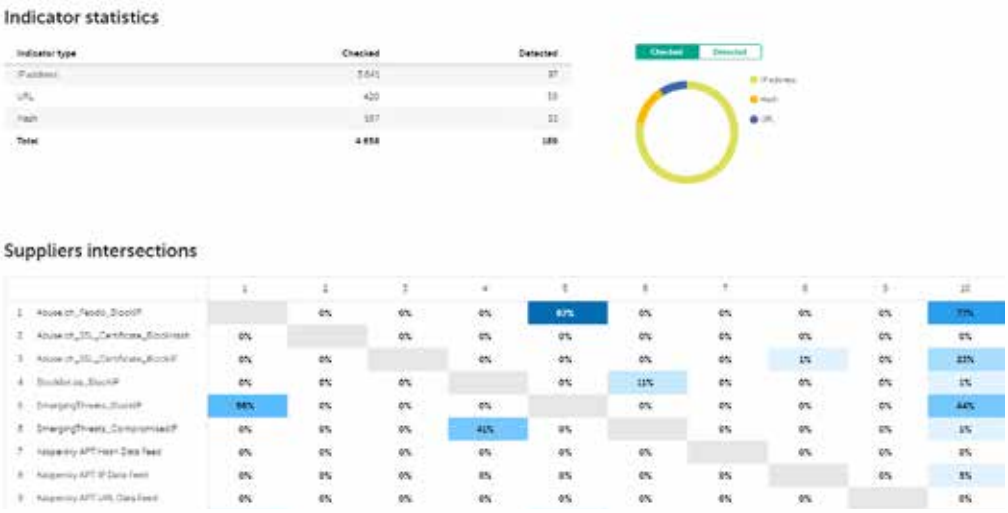

图 7.指标统计数据和数据订阅源交叉矩阵

其他产品功能：

- 用于各种 SIEM 解决方案的 SIEM 连接器，以直观显示和管理有关威胁检测的数据
- 按需查找指标（哈希、IP 地址、域、URL），以进行深入的威胁调查
- 针对数据订阅源的高级筛选
- 日志和文件批量扫描
- 适用于 Windows 和 Linux 平台的命令行界面
- 在独立模式下，卡巴斯基网络威胁追踪服务从网络设备等各种来源接收日志并加以解析
- 更多内容

· HTTP RestAPI 允许您查找和管理威胁情报。通过使用 Rest API，卡巴斯基网络威胁追踪服务可以轻松集成到复杂的环境中，以实现自动化和编排。

· 支持与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的集成，包括 Web UI 集成（单个 UI）。

尽管卡巴斯基网络威胁追踪服务和卡巴斯基威胁数据订阅源可以分别使用，但结合使用两者可以显著提升您的威胁检测能力，赋予您的安全运营团队监测网络威胁的全局能力。借助卡巴斯基网络威胁追踪服务和卡巴斯基威胁数据订阅源，您的组织能够：

· 有效地提取安全警报并确定其优先级

· 降低分析师的工作量并防止倦怠

· 立即辨别关键警报并制定更明智的决策，以决定将哪些警报上报给事故响应团队

· 建立由情报驱动的主动式防御机制。

网络威胁新闻：www.securelist.com
IT 安全新闻：business.kaspersky.com
中小企业 IT 安全：kaspersky.com/business
大型企业 IT 安全：kaspersky.com/enterprise
卡巴斯基威胁情报门户：opentip.kaspersky.com

www.kaspersky.com.cn

屡获殊荣独立自主我们价格透明。我们致力于建立更安全的世界，让技术改善我们的生活。这正是我们守护网络安全的原因，让全世界所有人都拥有无限机会。实现网络安全，创造更安全的明天。

如需了解更多信息，请访问 kaspersky.com/transparency

Proven.
Transparent.
Independent.