kaspersky 引领未来

# 卡巴斯基 SIEM

## 卡巴斯基统一监控和分析平台

产品介绍

# 关于卡巴斯基 SIEM 及其架构

**卡巴斯基统一监控和分析平台**是一款综合性的下一代 SIEM 解决方案，用于管理安全数据和事件。它在接收、处理和存储安全信息事件以及分析和关联传入数据方面表现出色。该平台还具有搜索功能，可在检测到潜在威胁时生成警报，并能够自动响应生成的警报和执行威胁捕获。

在高性能模块化架构的支持下，每个实例能够处理的每秒事件数 (EPS) 高达数十万，并通过优化系统要求来降低总体拥有成本 (TCO)。

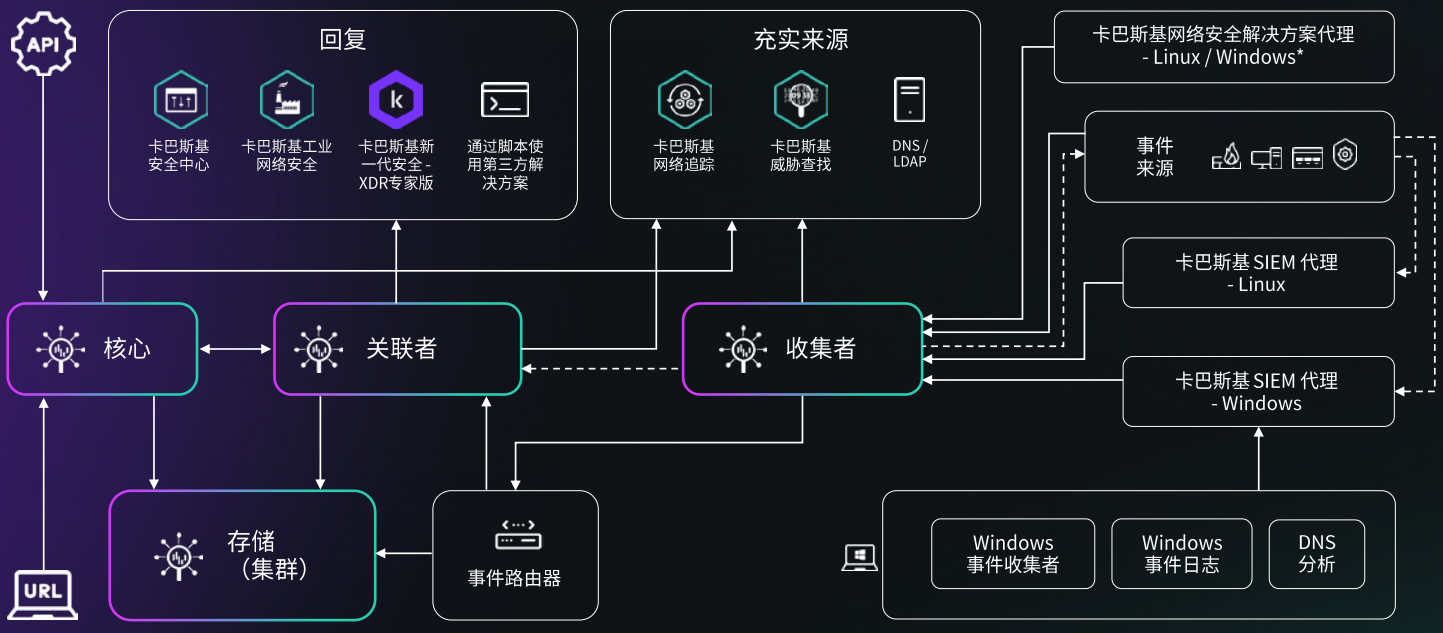
卡巴斯基 SIEM 将第三方产品和卡巴斯基产品整合到一个集中式信息安全系统中，是全面防御策略的重要组成部分，能够确保企业和工业环境的安全，并检测出在 IT 系统中发起并转移到 OT 系统的网络攻击。

得益于该解决方案的微服务架构，管理员可以创建和配置所需的微服务，从而将卡巴斯基 SIEM 用作成熟的 SIEM 系统或日志管理系统。

该解决方案可从各种来源（包括卡巴斯基产品、操作系统、第三方应用程序、安全工具和各种数据库）接收安全事件，并将事件相互关联起来，同时利用威胁情报馈送的数据来充实这些事件，从而识别出企业网络基础设施中的可疑活动，并及时发出安全事件通知。

通过收集所有安全控制的日志并实时关联数据，**卡巴斯基 SIEM 汇总并提供事件调查和响应所需的所有信息。**

此外，借助卡巴斯基 SIEM，操作人员还可以分析和关联历史数据，并建立统计基线以识别异常情况，从而使威胁捕获人员能够发现以前未知的威胁。



# 为何选择我们?

高性能模块化解决方案在成本效率方面始终优于传统 SIEM 供应商，每个实例能够处理的每秒事件数 (EPS) 高达数十万，从而节省高达 50% 的硬件或虚拟化安装需求，降低总体拥有成本。

保持灵活性 — 我们提供多种授权许可选项。我们跟踪汇总和过滤之后的日均 EPS 流量，以限制超限情况，并在出现这种情况时不限制对卡巴斯基 SIEM 的访问。

受益于各种具有内置响应选项的卡巴斯基和第三方集成方案。其他供应商无法达到我们自身产品的无缝集成水平，我们的集成方案包括用于威胁情报集成的单一界面、将我们的端点传感器用作 SIEM 代理的能力等等。

通过使用 ClickHouse 和 Hadoop 分布式文件系统(HDFS)或本地磁盘的冷热存储选项，以低成本且不影响质量的方式在本地长期存储数据，且不会超出预算，而且能够同时在这两个区域快速地进行搜索。

我们全球领先的研究人员和分析师团队通过卡巴斯基威胁情报门户网站提供战术、操作和战略威胁情报，从而提高数据相关性，加速检测和分类。

利用 MSSP 和大型企业就绪型解决方案的内置多租户功能，该解决方案提供原生多租户支持，从而在组织的主基础设施中仅需安装一个 SIEM，就能为各租户创建独立的 SIEM，用于接收和处理他们各自的事件。

# 为何选择卡巴斯基?

卡巴斯基 SIEM 融合了 5 个专业中心多年积累的深厚知识和精湛技能。

了解更多

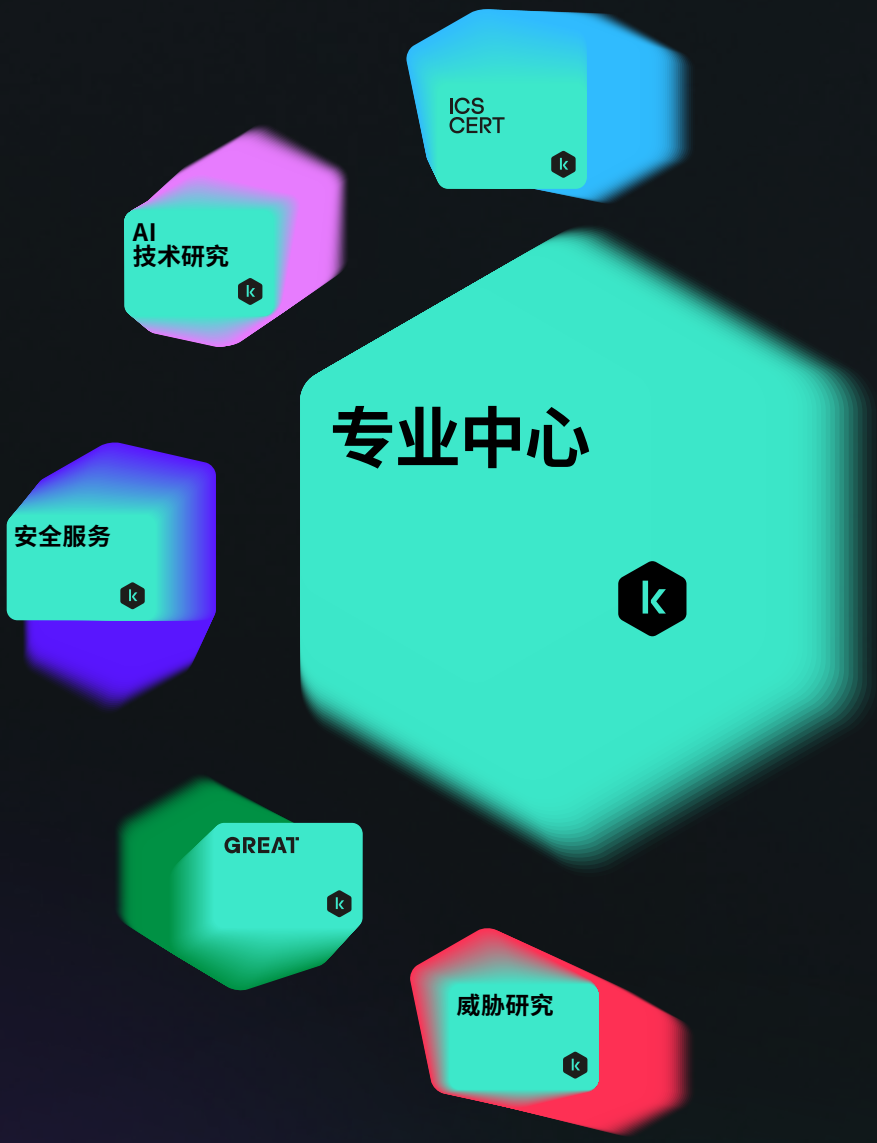
27

**27 年来**，我们一直在构建工具并提供服务，用久经测试、屡获殊荣的技术确保您的安全。

了解更多

我们是一家**全球性的私营网络安全公司**，在全球拥有成千上万名客户及合作伙伴，坚守透明度和独立性。

了解更多




## 卡巴斯基统一监控和分析平台

了解更多

www.kaspersky.com.cn

© 2024 AO Kaspersky Lab。
注册商标和服务标志归其各自所有者所有。

#kaspersky
#bringonthefuture