产品白皮书

卡巴斯基 SIEM

kaspersky 引领未来

目录

安全信息和事件管理产品市场

各组织的网络安全领导者面临着众多挑战，包括次数不断增加的基础设施渗透企图、网络安全人员短缺以及日益复杂的攻击等等。

此外，组织必须遵守与数据保留、审核和事件调查相关的监管要求，这对全球 SIEM 市场都有一定的影响。

随着网络攻击警报的增多和复杂性的加剧，组织也面临着按优先级隔离这些警报并更有效地对其进行分类的压力。

此外，远程办公的逐渐普及促使企业开始采用 SaaS 应用程序，并允许员工自带设备 (BYOD)，突显出将网络可见性扩展到传统边界之外的必要性。

最后，在当今市场上要找到合格的信息安全专家也并非易事。企业正在想方设法优化资源并提高网络安全效率。因此，他们希望其 SOC 团队能够轻松获取可操作的情报数据。

《Kaspersky Human Factor 360》报告显示：

77%

的公司至少出现过一次网络安全漏洞，
其中许多公司在同一时期遭遇了多达六次漏洞

41%

的公司认为自己的网络安全基础架构存在不足，
计划将来在该领域加大投资

了解更多

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。

卡巴斯基统一监控和分析平台包括以下组件

一个带有集中式图形用户界面的**核心**，用于控制和监控系统组件设置。通过使用 API，可以从第三方解决方案访问该平台。

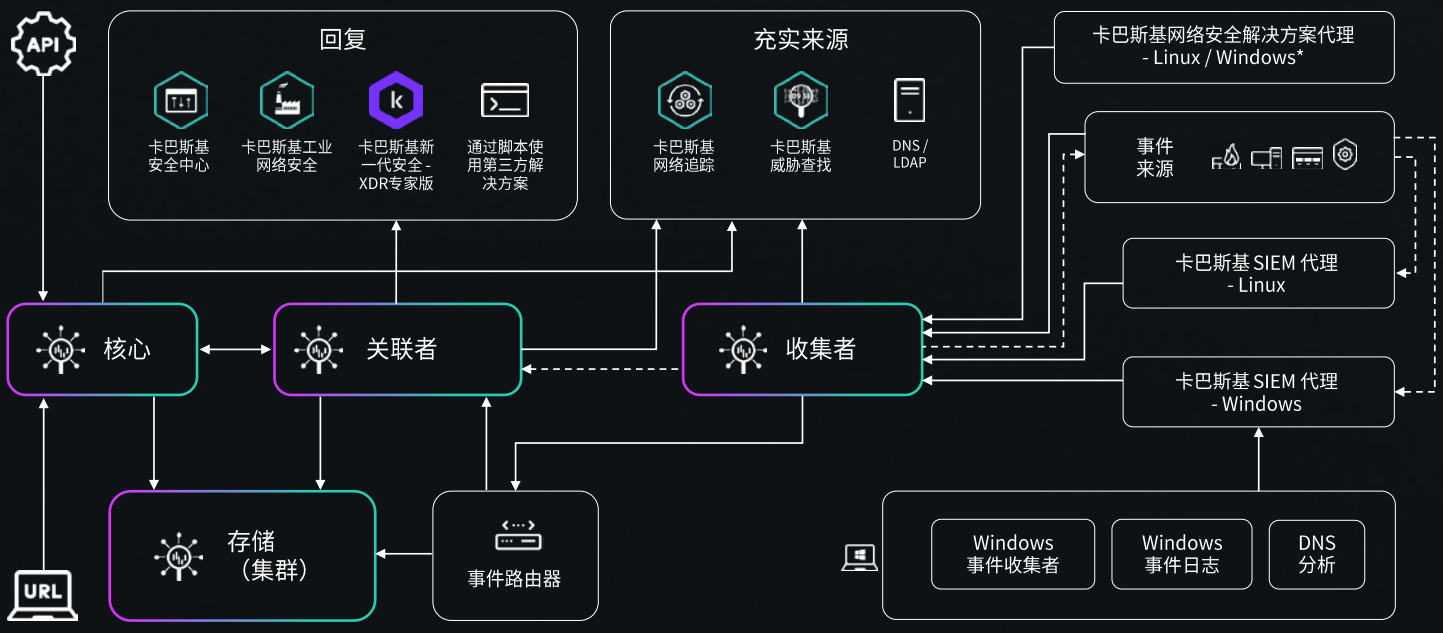
关联规则用于检测已处理事件的特定序列，并在识别后采取特定行动，例如创建关联事件/警报或与活动列表交互。**关联器**在分析从收集器接收到的规范化事件后，会使用活动列表来执行所需的操作，并根据关联标准生成警报。

一个或多个**收集器**从外部来源接收事件，并对其进行预处理：借助字典、DNS 服务调用和其他工具来规范化（更改为单一格式）、过滤、汇总并用外部来源的数据来充实这些事件。

存储系统用于存储规范化事件，以便通过 SIEM 来快速、持续地访问这些事件并提取分析数据。

代理将原始事件从工作站和服务器转发至 SIEM 收集器。在卡巴斯基网络安全解决方案 - Windows 12.6 版或 Linux 12.2 版中，现在可以将 Windows 日志事件直接发送至收集器。这大大减少了将事件来源与卡巴斯基 SIEM 系统集成的工作量。

当收集器安装在带宽较低或数据链路繁忙的远程办公室里时，事件路由器可以稳定、无延迟地接收事件，从而减少链路负载和防火墙上打开的端口数量。



卡巴斯基 SIEM 的功能

内置和自定义连接器可连接来自卡巴斯基和第三方供应商的数百个数据源，并且会定期更新和改进。

卡巴斯基专家服务团队可免费创建额外的连接器，用于整合外部事件来源。

快速搜索查询，随时报告安全事件。

在本地安全存储日志以满足监管要求和进行事件调查。

卡巴斯基 SIEM 支持跨多个存储系统的事件搜索，帮助操作人员更快、更轻松地在分布式存储集群中找到相关事件。

监控、处理和存储有关安全事件的信息

卡巴斯基统一监控和分析平台从日志中接收事件，并对来自不同事件来源的数据进行规范化处理，使其保持一致。这些信息安全事件可能包括登录尝试、数据库交互或传感器信息广播，它们是从公司整个受保护的 IT 基础设施中收集而来的。虽然单个事件可能看起来并不重要，但结合多个这样的事件就能拼凑出恶意活动的全貌，进而帮助我们找出安全问题。

数据湖是我们的集中式本地存储库，为对各种来源的日志进行收集、编制索引和分析提供了一个平台，这些来源包括安全解决方案（EPP、FW、IAM 等）、操作系统、业务应用程序（人力资源系统、办公工具）、物理安全系统（自动访问控制系统）以及其他设备。

事件经过过滤和汇总后，被传送到关联器进行分析和存储，以便保留。为了识别警报，收集器会接收不同来源的事件，对其进行处理，并将其传送至存储系统、关联器和/或第三方服务。来自工作站和服务器的原始事件被转发到 SIEM 收集器（在某些情况下通过代理进行转发），并可发送到其他系统进行进一步的分析。

解决方案在识别出某个特定事件或一系列相关事件时会产生关联事件，这些关联事件也会被分析和保留。如果某个事件或一系列事件表明存在潜在的安全威胁，卡巴斯基 SIEM 就会生成警报，其中包含有关威胁的信息以及安全专家需要考虑的任何其他相关信息。

在组件之间传输事件时，会采用可靠的传输协议，并可选择性地使用加密技术。系统可使用数据二极管从隔离部分收集数据。

卡巴斯基 SIEM 可提供包含大量服务器、工作站和网络设备的清单，从而实现集中化资产管理。该平台可从漏洞扫描器等来源收集有关资产漏洞的数据，并将其与资产类别数据关联起来，以便识别威胁。这让安全团队能够全面了解资产状况。

为了支持分析人员的工作，该平台会按规则显示 MITRE ATT&CK 矩阵的覆盖范围，以便更好地评估安全级别。

卡巴斯基服务器根据 MITRE 映射和响应建议，定期更新 650 多条用于检测攻击场景的预配置关联规则。

使用从卡巴斯基威胁情报门户（借助卡巴斯基威胁查找和卡巴斯基网络追踪）收集的分析数据来充实数据内容，提高数据相关性。

从卡巴斯基网络安全管理中心和第三方来源收集有关资产和基础设施的数据。

用户可以使用 ClickHouse 数据挖掘功能，将事件与特定时间段内的分组值、汇总值、平均值、最大值和最小值进行比较。这大大扩展了检测逻辑的能力，且无需创建大量的服务规则。

为了便于内容的创建和编辑，我们允许用户在对过滤条件进行任何更改之前，事先了解打算更改的内容将适用于哪些关联规则。

安全事件的实时和历史相关性

卡巴斯基 SIEM 按照用于识别攻击和威胁的自定义规则，以及由卡巴斯基 SOC（业内最成功、经验最丰富的主动威胁捕获团队之一）开发的数百条预定义规则，进行近乎实时的交叉关联。卡巴斯基 SOC 专家拥有多项证书，证明了他们高水平的专业技能和知识。

事件是**实时关联**的。关联器会分析规范化事件，根据关联规则创建警报，并处理所有活动列表操作。

关联器的工作原理是基于事件特征分析，即根据用户指定的关联规则处理每个事件。软件会生成关联事件，并在发现一系列符合关联规则要求的事件时将其发送到存储系统。用户可以自定义关联规则，通过将关联事件发送到关联器进行进一步分析，从而根据先前分析的结果触发这些规则。关联规则的结果可由其他关联规则使用。例如，几个较小的警报可能会触发一个较大的警报（分析几个暴力破解尝试可能会发现一个大规模暴力破解事件）。

该平台从历史数据中发现趋势，找到以前未识别的威胁，并准确检测出被某些安全要素忽略的攻击，从而提高整体威胁检测能力。

第三方解决方案或集成产品（如**卡巴斯基端点检测与响应**）可以在传感器侧进行检测。通过调整产品设置，用户可以控制这一过程，并获得这些产品通过自身的检测逻辑处理过的事件和遥测数据。

该解决方案的关联引擎包含平台侧检测功能。借助该平台强大的关联引擎，用户可以创建适应需求的关联规则。此外，该平台还提供现成的规则和规范化程序包，以支持市售的第三方产品，而且受支持的产品名单还在不断扩展和更新。

关联器的工作原理是基于事件特征分析，即根据用户指定的关联规则处理每个事件。软件会生成关联事件，并在发现一系列符合关联规则要求的事件时将其发送到存储系统。

借助威胁捕获功能，操作人员可以使用强大的面向列的数据库来分析和关联历史数据，从而发现以前未知的威胁。

通过使用基于标签的搜索功能，用户可以轻松找到由单个标签统一归类的过滤器、字典和规则。存储搜索查询历史记录可让用户轻松访问以前的查询。

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，该平台可以长期存储数据，而无需超出预算购买昂贵的存储硬件。

管理员可以借助灵活的设置来防止磁盘子系统出现空间问题：除了天数外，还能够以千兆字节为单位、按照占磁盘空间的百分比来设置事件存储深度。

安全事件数据存储

卡巴斯基 SIEM 的存储组件用于存储规范化事件，以便从**卡巴斯基统一监控和分析平台**快速、连续地访问分析数据。

ClickHouse 可确保访问的连续性和速度。存储系统通过 ClickHouse 集群连接到卡巴斯基 SIEM 存储服务。冷存储磁盘也可以添加到 ClickHouse 集群中。

用户可以在存储库中添加空间，根据特定属性对存储的事件进行分组。这样一来，管理员就可以根据事件的具体特征为其设置不同的存储时间。

卡巴斯基统一监控和分析平台还能将数据压缩，从而在不影响数据检索的情况下大幅减少对磁盘空间的占用。该卡巴斯基解决方案支持两个区域：一个用于快速检索数据，另一个用于存储大量数据。

该平台有两个不同的部分：一部分用于 Hadoop 分布式文件系统或本地磁盘上的冷存储；另一部分用于使用 ClickHouse 的操作存储。这种分离式设计对用户保持透明。

操作人员无需在压缩文件之间来回切换，就可以在单个界面中创建搜索查询，并集中全部精力进行调查工作。这既**降低了系统的拥有成本**，又确保了一流的用户体验。该平台支持跨多个存储系统的事件搜索，帮助操作人员更快、更轻松地在分布式存储集群中找到相关事件。

通过安全地收集和存储各种来源的日志，组织可以始终符合数据保留、审核和事件调查方面的监管要求。此外，集中化和结构化的存储还便于公司根据需要检索并分析日志。

卡巴斯基新一代安全 - XDR专家版

卡巴斯基新一代安全 - XDR 专家版可通过行动手册提供更广泛的响应功能。

了解更多

综合响应能力

使用卡巴斯基产品的内置响应功能可以提高安全效率。例如，为了扩展端点响应能力，可以将卡巴斯基 SIEM 与卡巴斯基端点检测与响应解决方案结合使用，以管理资产的网络隔离和预防规则，或执行应用程序和脚本。这些响应操作可以手动执行，也可以通过卡巴斯基网络安全解决方案的代理对资产自动执行。

自动收集清单信息（已安装的软件、漏洞、设备、资产所有者等）有助于了解信息安全事件的来龙去脉，并辅助事件调查。

卡巴斯基 SIEM 利用卡巴斯基网络追踪（一种功能全面的威胁情报平台，支持数十种现成的商业和公共威胁数据源），自动实时地充实事件信息，提供有关入侵指标的上下文信息。

卡巴斯基 SIEM 的人工智能组件可快速检测基础设施中的可疑活动

人工智能和机器学习工具

卡巴斯基使用预测算法、聚类技术、神经网络、统计建模技术和专业算法来提高产品的有效性，以更快地检测威胁并精准确定检测的优先级。

经过大数据和 AI 系统验证后，监控和响应团队可以划分警报的优先级，并集中精力预防潜在损害。AI 模块通过分析历史数据、对收到的警报进行优先级排序并为资产提供基于 AI 的风险评分，来帮助进行分类。这种方法有助于产生有价值的假设，这些假设可用于主动搜索。

该平台使用用户定义的关联规则来实时关联事件。其关联模块通过人工智能算法来检测异常活动（例如突然的流量激增或多个服务访问请求，这些可能是潜在安全事件的信号），从而在损害发生之前及早发现威胁。

卡巴斯基 SIEM 还整合了卡巴斯基威胁情报利用 AI 和大数据技术生成的数据。通过人工 APT 分析的结果、暗网运行数据、卡巴斯基安全网络提供的信息以及通过定期分析新恶意软件得出的见解，该数据库不断得到充实。

所有这些技术都能帮助用户最大程度地减少网络安全事件造成的潜在危害，并提高 MTTR 和 MTTD。

凭借出色的可视化控制面板和报告，数据以最具可用性的格式呈现，从而轻松识别趋势、模式和异常事件。

通过可自定义的小部件来轻松实现指标的可视化和显示，分析人员就可以对事件进行优先级排序、确定根本原因并更高效地应对威胁，而组织则可以跟踪其安全操作的有效性、识别趋势并评估其安全系统的整体运行状况。

用户可以用字典、表格、资产和账户属性的内容来充实事件字段数据，并将这些数据用于搜索和可视化。这有助于构建包含更多上下文数据的控制面板和报告。

该解决方案帮助用户根据自己的需求创建具有可调节设置的小部件，以及包含**各种小部件组的布局：**

关键警报指标

（严重程度、优先级和状态）

- 受影响的资产
- 最近的通知
- 警报最多的数据源
- 分配给特定操作人员的警报
- 受影响的用户和/或设备
- 按策略划分的警报

关键事件指标

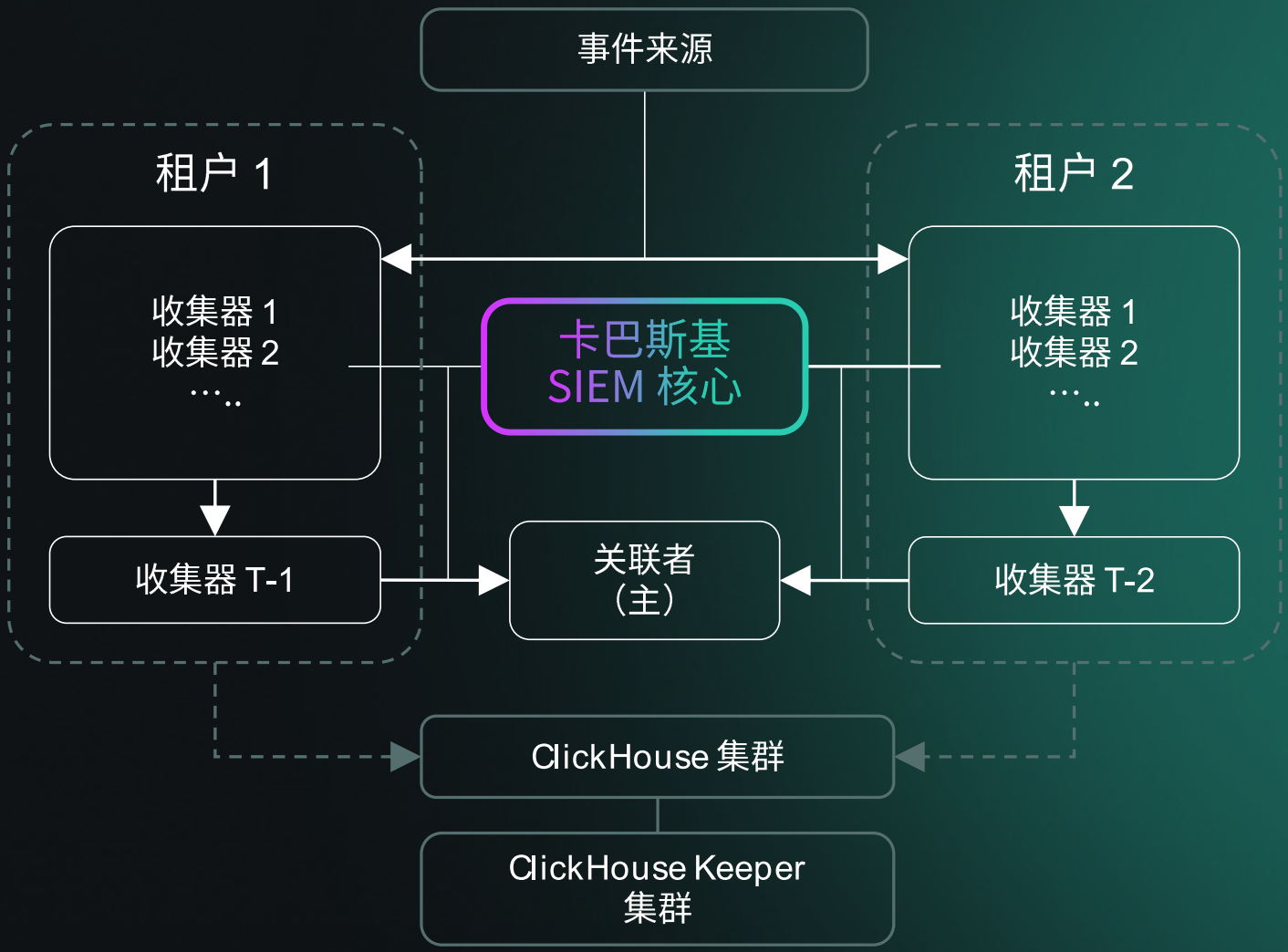
（严重程度和分配情况）

- 受影响的设备
- 按 NetFlow 流量 (BytesIn) 排名靠前的内部和外部 IP
- 用于远程管理的主要节点（端口 3389, 22）
- 内部端口的 NetFlow 字节总数
- 按事件、类别、资产和用户数量排名的主要来源

多租户架构

卡巴斯基 SIEM 提供全面的多租户支持，这意味着一个租户中的用户无法查看另一个租户的数据（事件、警报、安全事件等）。在多租户模式下，部署在主机构中的卡巴斯基 SIEM 应用程序的单个实例可以隔离分支机构，使其能够接收和处理各自的事件。

系统通过主界面集中管理，租户独立运行，只能访问自己的资源、服务和设置。与租户相关的事件单独存储。用户可以同时访问多个租户。一般管理员还可以指定在 Web 界面的不同部分显示哪些租户数据。



该平台提供了一个基于过滤的系统，用于将事件分发到不同的空间。现在，用户对事件的访问权限是在空间级别设置的。这样就能对单个租户内的事件访问进行细粒度控制。

系统通过主界面进行集中管理，而租户的运行彼此独立，只能访问各自的资源、服务和设置。租户的事件单独存储。

广泛的开箱即用集成方案

卡巴斯基统一监控和分析平台与卡巴斯基的解决方案和技术全面整合，实现了产品的协同使用并提高了效率。第三方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。

卡巴斯基
反针对性攻击

卡巴斯基
端点检测与响应 *

卡巴斯基
安全中心

卡巴斯基
安全邮件网关

卡巴斯基
网络流量安全

卡巴斯基
威胁查找

卡巴斯基
网络安全解决方案

卡巴斯基
端点安全解决方案

卡巴斯基
自动化安全感知平台

等等

与丰富的**卡巴斯基威胁情报**服务组合集成，有助于识别威胁并确定其优先级，还能快速获取有关新攻击、入侵指标以及攻击者战术和技术的上下文信息。

* 可与卡巴斯基端点检测与响应 - 专家版、卡巴斯基端点检测与响应 - 优选版、卡巴斯基新一代安全 - EDR 基础版、卡巴斯基新一代安全 - EDR 优选版、卡巴斯基新一代安全 - EDR 专家版集成

卡巴斯基 SIEM 在接收来自其他系统和设备的数据（日志）方面表现出色。为了便于快速实施，且无需在设置来源解析规则方面投入额外成本，该平台为卡巴斯基产品和第三方产品提供了多种开箱即用的集成方案：

按安全域划分

- 端点保护（EPP 和 EDR 解决方案）
- 电子邮件和 Web 流量保护（电子邮件保护、NDR、FW/NGFW、UTM、IDS）
- 安全意识
- 云工作负载（CASB、CWPP）
- 威胁情报 (CTI)
- 身份安全（IAM、PAM）
- OT/IoT 安全
- 数据丢失防护 (DLP)

按数据类型

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- 键-值
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

按传输类型

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL（SQLite、MSSQL、MySQL、PostgreSQL、Cockroach、Oracle、Firebird、ClickHouse、Elasticsearch）
- 文件
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW（DNS 分析）
- SNMP
- SNMP 陷阱
- VMware API
- MS Office 365

卡巴斯基专家服务团队或合作伙伴可以开发更多集成方案，包括使用可连接产品的 API。查看受支持事件来源的完整列表。

完整列表

按供应商分类

- 卡巴斯基
- 独立的
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- 华为
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle（甲骨文）
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- 等等。

卡巴斯基
高级支持

针对卡巴斯基 SIEM 的高级支持

针对卡巴斯基 SIEM 的高级支持包含“优选版”和“专业版”授权许可，可确保对任何问题做出快速响应并提供高质量的协助，从而保证您的卡巴斯基 SIEM 顺利运行

通信	标准支持	“优选版”授权许可	“专业版”授权许可
公司账户 (Web 门户)	●	●	●
电话		●	●
电子邮箱		●	●
服务			
卡巴斯基 SIEM 的自定义解析器		5	10
远程协助以诊断问题		●	●
支持请求优先上报		高	最高
专用补丁			●
专属技术客户经理 (TAM)			●
来自 TAM 的状态报告			季度报告
响应时间			
重大问题	无 SLA	2 小时 (24/7)	30 分钟 (24/7)
高级别问题	无 SLA	6 小时 (8/5)	4 小时 (24/7)
中等级别问题	无 SLA	8 小时 (8/5)	6 小时 (8/5)
低级别问题	无 SLA	10 小时 (8/5)	8 小时 (8/5)

快速响应

根据严格的 SLA 对请求进行优先排序，以便更快、更可靠地解决问题

自定义解析器

自定义解析器使 SIEM 能够处理来自特定数据源的独特日志格式

专用 TAM

使用“专业版”授权许可，TAM 能够更加负责地管理所有问题

专用补丁

使用“专业版”授权许可，可获得针对特定问题设计的自定义修复程序和补丁

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。

全球企业依靠卡巴斯基统一监控和分析平台来制定全面的信息安全流程，从而提高网络安全效率。

了解更多

卡巴斯基利用自身的 SIEM 发现了以前未知的针对 iOS 设备的恶意软件

在使用卡巴斯基统一监控和分析平台监控我们公司移动设备专用 Wi-Fi 网络的网络流量时，我们检测出来自多部 iOS 手机的可疑活动。

由于无法从内部检查现代 iOS 设备，我们创建了相关设备的离线备份，使用移动验证工具包的 mvt-ios 对其进行检查，发现了被入侵的痕迹。

对此，Apple 发布了安全更新，以解决卡巴斯基研究人员发现的四个零日漏洞：

CVE-2023-32434、CVE-2023-32435、CVE-2023-38606、CVE-2023-41990

这些漏洞影响到 Apple 的多种产品，包括 iPhone、iPod、iPad、macOS 设备、Apple 电视和 Apple 手表。卡巴斯基还向 Apple 报告了一项硬件功能被利用的情况，该公司随后采取了缓解措施。

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

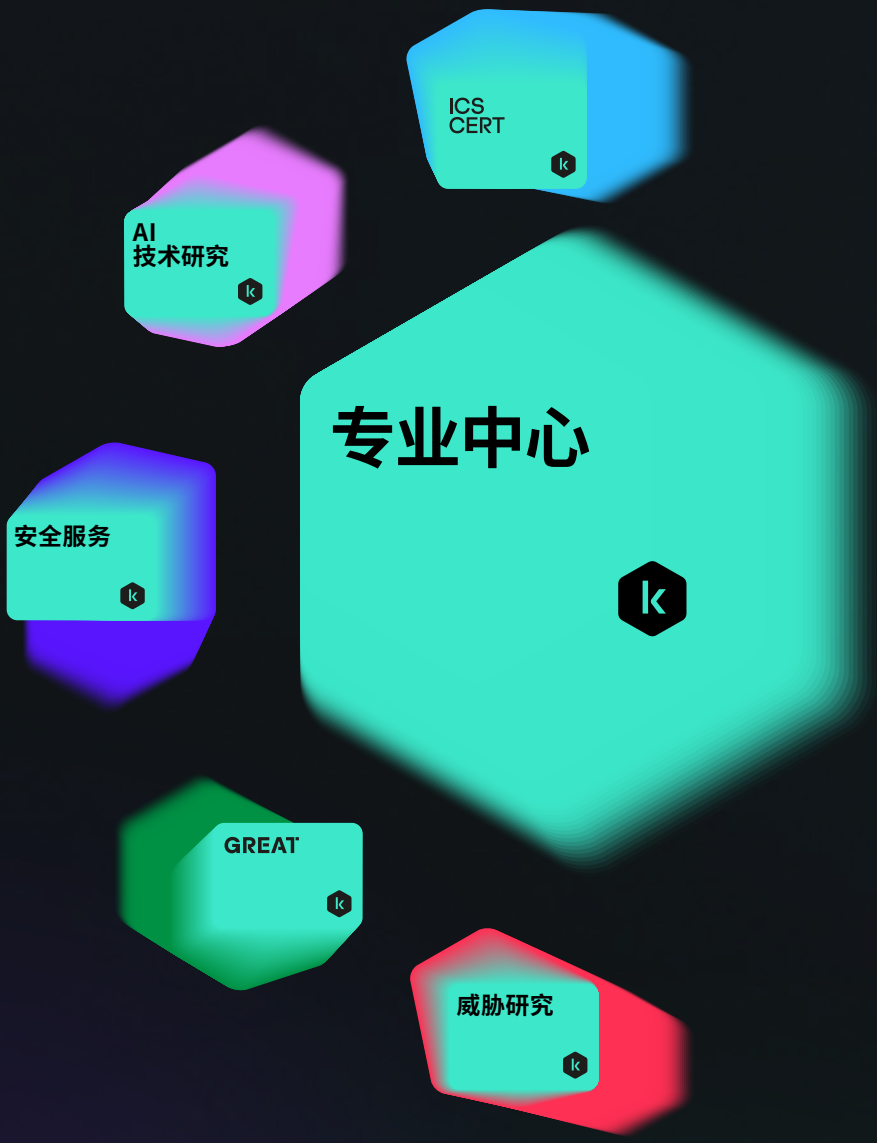
27

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

#kaspersky
#bringonthefuture