卡巴斯基威胁情报

领先您的对手

kaspersky

卡巴斯基威胁情报来源

卡巴斯基威胁情报可提供由我们世界一流的分析师和研究人员收集的各种信息，帮助您的组织有效应对当今的网络威胁。

由独特的全球专业知识和经验提供支持的威胁情报

每个中心都为卡巴斯基的解决方案和服务做出贡献

威胁研究　事故调查

卡巴斯基全球研究与分析团队

- 研究最复杂的威胁：APT、网络间谍活动、全球网络流行病等
- 面向未来的技术的安全性
- 调查复杂的金融网络犯罪

卡巴斯基威胁研究

- 反恶意软件研究
- 内容过滤研究
- SSDLC 和安全设计方法

卡巴斯基 AI 技术研究

- AI 网络安全
- 生成式 AI 研究
- AI 赋能的威胁检测/解决方案

卡巴斯基安全服务

- MDR
- 事件响应
- 安全评估
- SOC 咨询服务
- 数字足迹情报

卡巴斯基 ICS CERT

- 关键基础设施威胁分析
- ICS 漏洞研究与评估
- 技术协会、分析和标准

卡巴斯基威胁情报亮点

我们在网络威胁研究方面的深厚知识、丰富经验以及对网络安全各个方面的独特洞察，使我们成为全球企业值得信赖的合作伙伴，也是包括国际刑警组织和众多 CERT 单位在内的执法机构和政府组织的重要盟友。

覆盖全球威胁，在研究大多数攻击起源地区的威胁方面拥有长期经验

卡巴斯基专家的持续贡献

面向 IT 和 OT 领域的威胁情报

卡巴斯基威胁情报亮点

我们追踪：

300+

威胁发起者

500+

场活动

200+

份私人报告/年

170000+

与报告相关的 IoC

2 500+

与报告相关的
YARA 规则

威胁情报数据级别

战术

支持安全操作和事件响应的低级别、高度易损信息。战术情报的一个例子是与新发现的攻击行为有关的 IOC。

角色：

SOC 分析师

系统：

SIEM　下一代防火墙　SOAR

IPS　入侵检测系统

进程：

威胁捕获　监控

操作

该级别通常包括有关攻击活动和更高级的 TTP 的数据。它可能包括有关具体攻击者归因以及攻击者能力和意图的信息。

角色：

SOC L3 分析师　DFIR 分析师

IR 分析师

系统：

SIEM　NTA　威胁情报平台　EDR / XDR

进程：

事件响应　威胁捕获

战略

该级别支持高管和董事会就风险评估、资源分配和组织战略做出严谨的决策。这些信息包括趋势、攻击者的动机及其分类。

角色：

首席信息安全官　CTO　CIO

首席执行官

进程：

制定 IS 策略

提高意识

威胁情报交付格式

机器可读的
威胁情报

卡巴斯基
威胁数据源

30 多个威胁数据源，侧重于 IT 和 OT 覆盖以及威胁情报平台的不同需求

可读且易理解的
威胁情报

卡巴斯基
威胁情报
门户网站

适用于 IT 和 OT 环境的核心卡巴斯基威胁情报产品组合，通过卡巴斯基威胁情报门户提供单一接入点

威胁情报
专家支持

卡巴斯基
清除服务

卡巴斯基
询问分析师

经验丰富的专业人士的专家指导

卡巴斯基威胁情报

机器可读的
威胁情报

- 卡巴斯基威胁数据源
- 卡巴斯基网络追踪

威胁情报
专家支持

- 卡巴斯基清除服务
- 卡巴斯基询问分析师

卡巴斯基
威胁情报

- 战术
- 操作
- 战略

可通过

卡巴斯基
威胁情报
门户网站

人类可读的
威胁情报

- 卡巴斯基威胁查找
- 卡巴斯基数字足迹情报
- 卡巴斯基威胁分析
  - 沙盒
  - 归因
  - 相似性
- 卡巴斯基威胁情报报告
  - APT
  - 犯罪软件
  - ICS
- 卡巴斯基威胁基础设施跟踪

卡巴斯基威胁数据源

超过 30 个开箱即用的威胁数据源可用于不同任务。还提供为您的组织量身定制的威胁数据源。

- 战术 TI
- 运营 TI

通用威胁数据源

- 恶意 URL
- 勒索软件 URL
- 网络钓鱼 URL
- 僵尸网络 C&C URL
- 移动僵尸网络 C&C URL
- 恶意散列
- 移动恶意哈希
- IP 声誉
- IoT URL
- ICS 哈希
- APT 哈希
- APT IP
- APT URL
- 犯罪软件哈希
- 犯罪软件 URL

卡巴斯基威胁数据源 → SIEM、SOAR / IRP、TIP、EDR / XDR

威胁情报平台 | 快速实施各种威胁情报源并减少 SIEM 工作负载 | 卡巴斯基网络追踪

特定威胁数据源

网络安全数据源	Suricata 规则源	Sigma 规则数据源	Yara 规则数据源	漏洞源	开源软件威胁数据源
下一代防火墙	入侵检测系统 / IPS	SIEM / EDR	YARA-扫描程序	SBOM / CMDB	OSA / CSA / ASOC

卡巴斯基威胁情报门户

统一 UI/API 内的单一卡巴斯基威胁情报接入点，各项服务在其中协同工作，相互充实和加强。将卡巴斯基的所有网络威胁专业知识和经验汇集在一起，允许使用专有的数据处理和规范化技术监控与特定组织相关的威胁，并能够检查恶意软件样本及其归属。

- 战术 TI
- 运营 TI
- 战略 TI

卡巴斯基
威胁情报门户免费版

卡巴斯基威胁情报门户上的威胁形势

地区和行业特定的威胁情报，了解您的组织面临的确切威胁

- MITRE ATT&CK 对齐
- 基于卡巴斯基持续研究的实时更新
- 自动填充对手和软件资料
- 检测规则存储库

400,000+

我们每天检测到的恶意文件数量

威胁形势 — 如何运作


筛选器：
行业
国家/地区
行为者
平台
MITRE ATT&CK 热图
详细的 TTP 描述
Top-10 统计数据
防御措施
威胁形势
攻击者
名字
描述
国家/地区
行业
TTPS
恶意软件
报告
[滋] 恶意软件
名字
描述
攻击者
TTPS
SIGMA / Suricata 规则
报告
SIGMA / Suricata 规则
TTPS
入侵指标

卡巴斯基威胁情报专家支持

卡巴斯基
询问分析师

- 运营 TI
- 战略 TI

卡巴斯基询问分析师服务延伸了我们的威胁情报产品组合，使您可以对正在面临的，或者感兴趣的具体威胁请求指引和洞彻了解。

我们会根据具体情况，让您与卡巴斯基研究人员核心小组联系。该服务可提供专家之间的全面沟通，用我们的独特知识和资源增强您的现有能力。

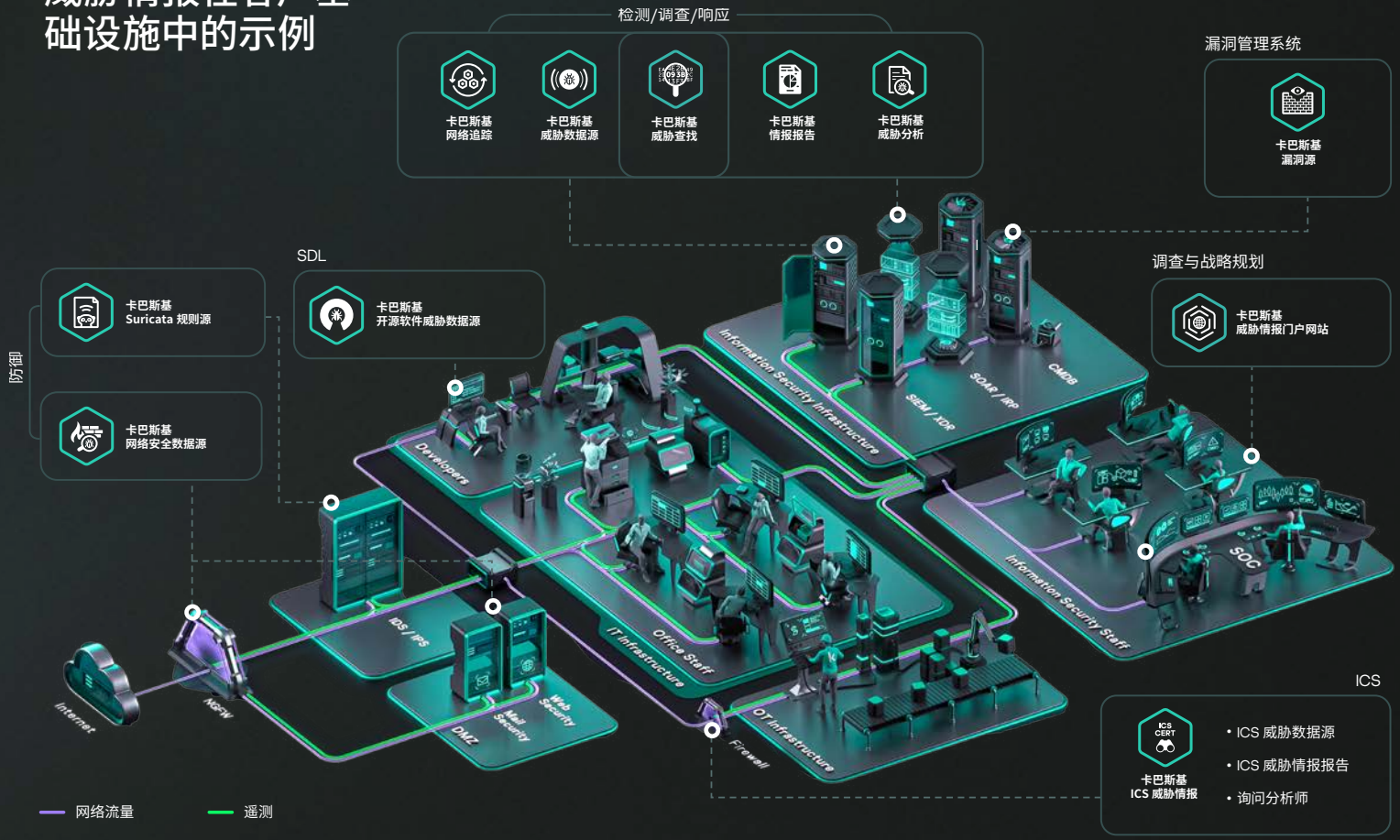
卡巴斯基
清除服务

- 运营 TI

卡巴斯基清除服务可在恶意网络钓鱼域对您的业务和品牌造成损害之前，迅速抵御它们带来的威胁。凭借丰富的域分析经验，我们知道如何收集所有必要的证据来证明它们是恶意的。我们将负责您的清除管理。

该服务在全球范围内与国际组织以及国家和地区执法机构合作提供。

卡巴斯基威胁情报在客户基础设施中的示例



卡巴斯基工业威胁情报提供

机器可读的威胁情报

卡巴斯基
威胁数据源

有关工业网络安全威胁和漏洞的机器可读数据：

卡巴斯基 ICS 哈希数据源
卡巴斯基 ICS 漏洞数据源
OVAL 格式的卡巴斯基 ICS 漏洞数据源

人类可读的威胁情报

卡巴斯基
ICS 情报
报告

访问卡巴斯基威胁情报门户上涵盖工业网络安全威胁和漏洞的定期出版物

威胁情报专家支持

卡巴斯基
询问分析师

直接咨询卡巴斯基 ICS CERT 专家，获得有关工业网络安全威胁和漏洞、威胁统计数据、威胁形势、行业标准等的个性化建议。

● 战术　● 运营 TI　● 战略 TI

为什么选择卡巴斯基威胁情报

行业分析师认可的领先 TI 产品	经过 Frost & Sullivan、Quadrant Knowledge Solutions、Forrester、IDC 等多家全球研究公司的分析师验证。
多个可信且独特的来源，提供可靠的威胁情报	我们的卡巴斯基安全网络基础设施覆盖 200 个国家/地区的 1 亿多个传感器，是最大的恶意和合法文件、暗网、持续的 TH 和 IR 活动、网络爬虫、垃圾邮件陷阱等威胁的存储库。
IT 和 OT 领域的知名专家	200 多名来自 5 个专业中心的认证专家，包括 GReAT 团队和 ICS-CERT，分布在全球各地，使用 20 多种语言。卡巴斯基的专家总是率先揭示最臭名昭著的威胁 — 从 Stuxnet 和 WannaCry 到 Operation Triangulation。
全球业务	在大多数攻击源头地区（俄罗斯/独联体、中国等）拥有强大的影响力，使我们能够为任何国家/地区的组织收集、分析和分发 100% 经过审查的威胁情报。
恶意软件检测技术方面的独特经验	作为最大的反病毒软件供应商（拥有获奖最多的产品），我们每天使用专有的威胁检测技术处理数百万个新恶意软件样本。
APT 研究方面的独特经验	我们追踪数百个 APT 行为者和活动，每年发布 200 多份深入的 TI 战略报告，并拥有业内最大的 APT 文件集，其中包括 7 万多个样本。
AI 驱动的 TI，可增强检测、响应和威胁报告	AI/ML 使我们能够提取可操作的洞察，生成自定义报告并实现自动化分析，从而节省大量时间和资源。
强大且安全的供应商	容错、透明的基础设施，具备高 SLA 和监控能力，使用 SDLC 方法构建，定期接受独立第三方评估（SOC 2 Type 2 或 ISO 27001）。

公开成功案例

这让我们能够清楚地了解客户面临的威胁。当警报发生时，拥有权威、可参考的信息，以及与之相关的所有附带数据，对于全面了解发生的情况以及我们可以从中学到什么至关重要。

Paul Colwell
CyberGuard Technologies

CyberGuard Technologies

阅读案例

新威胁出现时，卡巴斯基通常会最先发现，而软件制造商甚至还对此一无所知。

卡巴斯基具备相应的专业知识，可以帮我了解新的威胁，以及我们不熟悉的那些潜伏在黑暗之中的危险，而不是简单地发给我一大堆二手新闻，这类所谓的新闻根本无法让我们学到什么新东西。

Juan Andres Guerrero Saade
研究员，Chronicle Security

chronicle

阅读案例

卡巴斯基的功能和倾听我们需求的态度超出了我的预期。他们让我们对产品和背后的人员充满信心，并使我们拥有更安全的网络。

Rashid AlNahlawi
卡塔尔奥委会 IT 安全顾问

قطر
QATAR

阅读案例

卡巴斯基威胁情报助您……

主动识别并防范威胁

卡巴斯基威胁情报可让您始终知悉最新的威胁和漏洞，从而让您可以在攻击发生前采取主动措施，以保护您的系统。

增强威胁检测能力

卡巴斯基威胁情报使用最新的威胁情报帮助您增强现有的安全解决方案，从而提升您检测和阻止高级威胁的能力。

改善事件响应

卡巴斯基威胁情报提供关于新兴威胁和入侵指标的实时信息，以便您可以对事件做出快速、有效的相应。

了解数字足迹

卡巴斯基威胁情报提供您的数字足迹的综合视图，包括任何容易受到攻击或者泄露的资产。

丰富内部专业知识

卡巴斯基的专家团队是业界最富有经验和受人尊敬的研究人员，将为您的信息安全团队带来丰富的知识和专业经验。

符合法规和标准

所有公司都受业内的各种法规和标准制约。卡巴斯基威胁情报通过帮助您满足这些要求来支持合规性。

感谢！

卡巴斯基威胁情报门户 –
网络安全知识的汇聚地

卡巴斯基
威胁情报门户

了解更多

申请获取演示文件