卡巴斯基
反针对性攻击平台

kaspersky 引领未来

前沿网络安全，应对 APT 与复杂威胁

在当今这个网络犯罪日益猖獗的时代，犯罪分子不断设计出新颖且复杂的系统渗透与破坏手段。面对威胁的不断演变，其复杂性和破坏性日益增强，迅速检测并采取最快、最恰当的应对措施变得至关重要，这关乎着系统的安全与稳定。

卡巴斯基反针对性攻击 (KATA) 可为企业构筑网络安全防御壁垒，抵御 APT 及定向攻击，保护企业基础设施网络安全，同时助力法规合规，无需额外 IT 安全资源投入。提供高度自动化的统一管理平台，使复杂事件得以迅速识别、调查与响应，将 IT 安全团队与 SOC 团队从繁琐手动任务中释放出来，大幅提升工作效率。

卡巴斯基反针对性攻击提供多方面的反 APT 保护方案，可抵御复杂的网络威胁。无论您选择基础或高级 NDR 功能，与 EDR 解决方案结合，即可实现原生 XDR 解决方案。选择卡巴斯基反针对性攻击平台，凭借多维威胁发现能力、专业的技术应用、高效调查手段、主动威胁搜寻以及快速集中的响应机制，助您应对各类挑战。

卡巴斯基反针对性攻击平台

减少识别和响应威胁所需的时间

简化威胁分析和事件响应

帮助消除安全漏洞并减少攻击“停留时间”

在威胁检测和响应过程中自动执行手动任务

减轻 IT 安全人员负担，高效执行核心任务

全面支持合规

灵活选择

3 个级别的 APT 保护：

KATA → KATA NDR 增强版 → KATA 卓越版

版本对比

	KATA	KATA NDR 增强版	KATA 卓越版
基本 NDR 功能			
· 网络流量监控和高级检测引擎 · TLS 指纹识别 · 与 IDS 警报相关的 PCAP · URL 信誉分析 · 基于 IDS 规则的入侵检测（纵向） · 网络引导式响应 · 自动化网关级响应和具有阻止模式的 ICAP 集成	•	•	•
前沿的沙盒技术	•	•	•
卡巴斯基威胁情报和 MITRE ATT&CK 数据充实	•	•	•
增强的 NDR 功能			
· 用于协议定义的 DPI · 基于 IDS 规则的入侵检测（横向） · 网络会话表、网络映射、清查模块，可提供全面的网络可见性 · 网络遥测分析和端点监控（EPP Linux、Windows） · 防范网络安全风险（未经授权的设备、ARP 欺骗等） · 原始流量（PCAP）存储和回顾性分析 · 通过 API 连接器对网络设备做出响应 · 异常检测 · 影子 IT 检测		•	•
专家 EDR 功能			•
原生 XDR 功能			•

安全新高度

卡巴斯基反针对性攻击提供一体化 APT 防护解决方案，依托我们强大的威胁情报体系，并与 MITRE ATT&CK 框架紧密对接。该方案可覆盖所有潜在的威胁入口点，包括网络、网页、邮件、PC、笔记本电脑、服务器及虚拟机，确保一切尽在您的掌控之中。

自动化威胁发现与响应

提升安全效率，优化事件响应及 SOC 团队的成本效益，让安全体系更加智能高效。

无缝集成

与现有安全产品紧密融合，不仅提升整体安全等级，更可保护您的传统安全投资，实现价值最大化。

全面可见性

深入洞察企业 IT 基础设施的每一个角落，提供多方面安全监控。

高度灵活性

无论是物理还是虚拟环境，我们的解决方案都能灵活部署，提供管理可见性，满足多样化需求。

利用卡巴斯基威胁情报充实警报信息

卡巴斯基
威胁情报

卡巴斯基整合了遍布全球的 1 亿多个传感器、海量恶意与合法文件库以及暗网情报，结合持续的威胁狩猎与事件响应实战，为您提供多方位威胁情报支持。

通过 KATA 告警界面可直达威胁情报门户：支持分析可疑文件、关联其他监测项，并获取极具实战价值的上下文背景信息。

为何选择卡巴斯基？

- 全球影响力与国际认可
- 久经验证的技术保障
- 透明运营与合规保障
- 行业经验与专业知识
- IT 安全行业领军者
- 28 年专业客户保护

卡巴斯基
反针对性攻击平台

了解更多

www.kaspersky.com.cn

#卡巴斯基
#引领未来