卡巴斯基数字足迹情报

kaspersky 引领未来

卡巴斯基数字足迹情报

随着您的业务增长，您的 IT 环境的复杂性和分布也在增长，这带来了一项挑战：在没有直接控制或所有权的情况下，保护您广泛分布的数字业务。动态和相互连接的环境让公司受益无穷。但与此同时，不断增加的互连也扩大了攻击面。随着攻击者变得更加熟练，您不仅要对您的组织的在线业务具备准确的了解，还要跟踪它发生的变化，并对与曝光的数字资产有关的最新信息作出反应，这至关重要。

企业在安全运营中使用了广泛的安全工具，但仍有数字威胁隐现：需要拥有适当的功能来检测和抵御内部人员活动，以及位于暗网论坛上的网络犯罪分子的计划和攻击方案，等等。为了帮助安全分析师探索攻击者对其公司资源的看法，及时发现他们可用的潜在攻击媒介，并相应调整防御措施，卡巴斯基创建了卡巴斯基数字足迹情报。

对您的组织发动攻击的最佳方式是什么？用于攻击您的最具成本效益的方式是什么？将您的企业视为目标的攻击者可以获得哪些信息？您的基础架构是否已在您不知情的情况下遭到入侵？

卡巴斯基数字足迹情报可以回答这些问题及其它问题，我们的专家将针对您的攻击状态综合出来，识别容易被利用的薄弱点，并揭示过去、现在以及已经计划好的攻击的证据。

该产品提供：

- 使用非侵入式方法进行网络边界清单检查，以确定客户的网络资源和曝光的服务，这些资源和服务是攻击的潜在入口点（比如无意中留在边界上的管理接口或配置错误的服务、设备接口，等等）。
- 对现有漏洞进行定制分析，根据 CVSS 基本得分、公共漏洞的可用性、渗透测试经验和网络资源（托管/基础架构）的位置进行进一步评分和综合风险评估。
- 识别、监控和分析任何处于活动状态的定向攻击或正在计划的攻击，以及针对您的公司、行业和运营地区的 APT 活动。
- 识别将目标锁定为您的客户、合作伙伴和订阅用户的威胁，他们受感染的系统可被用于攻击您的系统。
- 谨慎监控文本存储网站、公共论坛、博客、即时消息渠道、受限制的地下在线论坛和社区，以发现遭到入侵的帐户、信息泄漏或正在计划和讨论的、针对您的组织的攻击。

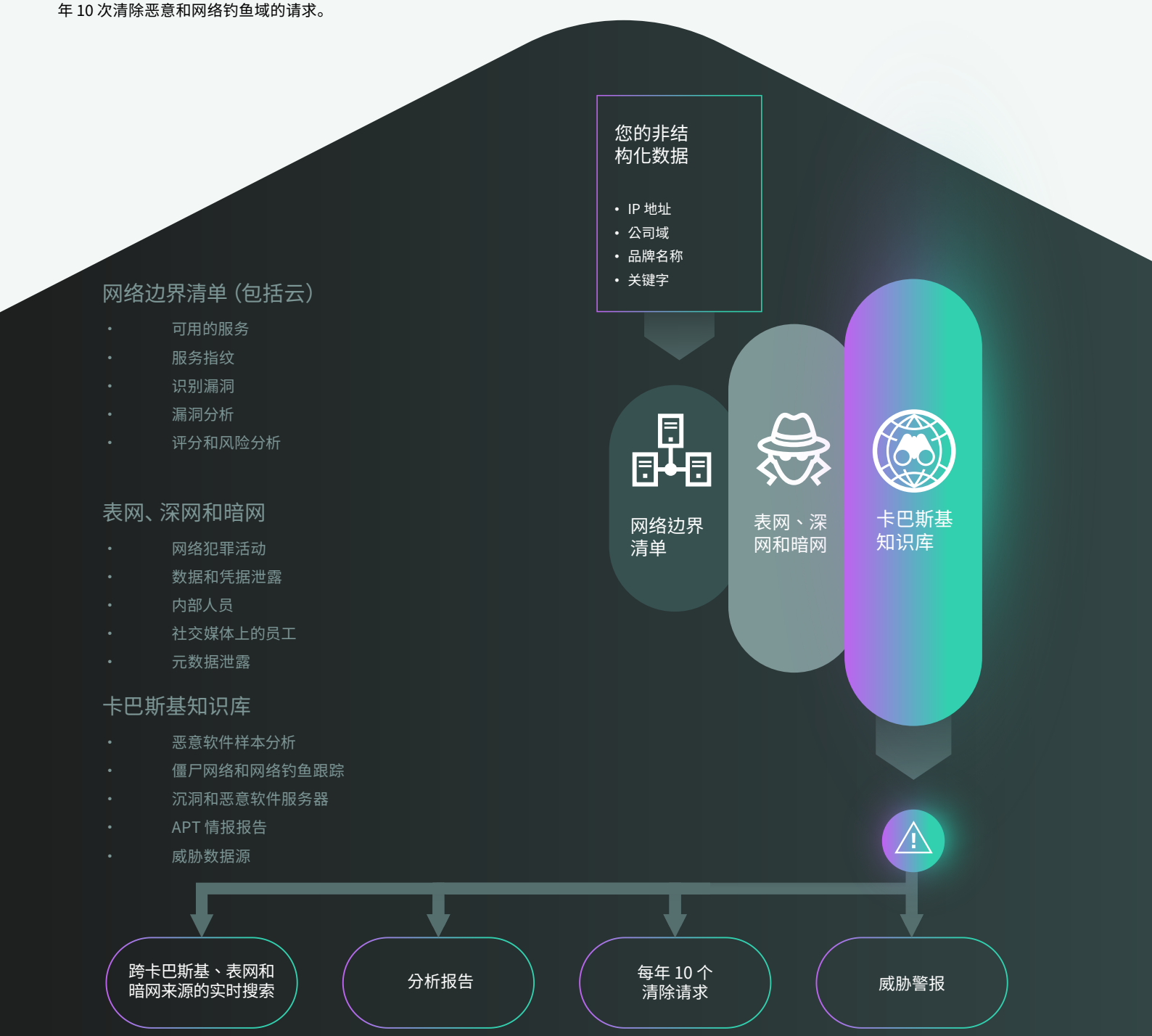
亮点

卡巴斯基数字足迹情报使用 OSINT 技术，结合对表网、深网和暗网的自动和手动分析，再加上卡巴斯基内部知识库，提供了可行的见解和建议。

可在卡巴斯基威胁情报门户上获得该产品。您可以购买四份季度报告（包含年度实时威胁警报），或者购买一份报告（激活六个月的警报）。

搜索表网和暗网，以获得与威胁您的资产的全球安全事件有关的准实时信息，以及在受限制的地下社区和论坛上搜索曝光的敏感数据。年度许可证包括每天 50 次跨外部来源和卡巴斯基知识库的搜索。

卡巴斯基数字足迹情报与卡巴斯基清除服务形成了一个单一解决方案。年度许可证包括每年 10 次清除恶意和网络钓鱼域的请求。



www.kaspersky.com.cn