持续寻找、检测以贵企业为目标的威胁并做出响应

卡巴斯基托管检测与响应

kaspersky 引领未来

公司面临的挑战

55%
的公司报告其自有设备感染过恶意软件*

20%
的公司面临 APT 威胁**

18%
的受访者报告称，其公司发生事件的原因是缺乏合格的网络安全人员***

25 亿美元
成功的网络攻击导致巨大损失****

通过全天候托管保护提高网络安全弹性

远程工作、信息交换方式的快速发展、全球技能差距的扩大以及越来越多能够绕过传统自动化预防和检测控制的网络威胁，正在给各种规模的组织带来持续不断的压力。他们能够迅速且有效地做出响应至关重要。

卡巴斯基托管检测与响应 (MDR) 是一项提供全天候托管保护的服务，可抵御传统自动化安全措施检测不到的网络威胁和复杂攻击。

该解决方案提供可快速部署的一站式服务，可提升缺乏网络安全专业知识的中小型组织的 IT 安全水平。对于拥有高级网络安全专业知识的有经验团队，它提供了额外的灵活性，使他们能够将事件检测和分类任务委托给卡巴斯基专家，或就他们自己检测到的事件获得额外的专业意见。

卡巴斯基 MDR 可增强并提高组织应对网络威胁的弹性，优化现有资源并帮助高效利用现有资源，同时优化未来对 IT 安全的投资。

关键功能

- 全天候持续监控和威胁搜寻
- 所有受保护资源及其当前状态的概览
- 自动化、引导式的响应
- 直接联系卡巴斯基的 SOC 分析师
- 用于与 IRP/SOAR 集成的 REST API
- 具有控制面板和报告的 Web 控制台
- 存储 3 个月的原始遥测数据
- 提交自定义事件
- 存储 1 年的安全事件历史记录

* 2022 年 IT 安全经济学；
** 2023 年卡巴斯基 MDR 分析报告；
*** 2023 年卡巴斯基人为因素 360 报告；
**** 全球金融稳定报告。最后一英里：金融脆弱性和风险，2024

卡巴斯基 MDR 的遥测和警报源

- **卡巴斯基端点安全 - Windows**
- **卡巴斯基端点安全 - macOS**
- **卡巴斯基端点安全 - Linux**
- **卡巴斯基虚拟化轻代理**
- **卡巴斯基反针对性攻击**

运作方式

1

卡巴斯基 SOC 分析师调查安全警报并主动分析从安装在客户网络中的卡巴斯基产品收到的遥测事件。该遥测数据与卡巴斯基的网络威胁情报相关 - 基于超过 25 年的经验，调查了一些全球最臭名昭著的网络攻击和定向攻击活动 - 以识别攻击者使用的已知、全新和新兴的战术、技术和程序。通过独特的 IoA 能够检测模拟合法活动的隐藏无恶意软件威胁。

2

作为卡巴斯基 MDR 事件处理流程的一部分，人工智能 (AI) 机制有助于减少误报数量并加快 SOC 团队的事件调查。

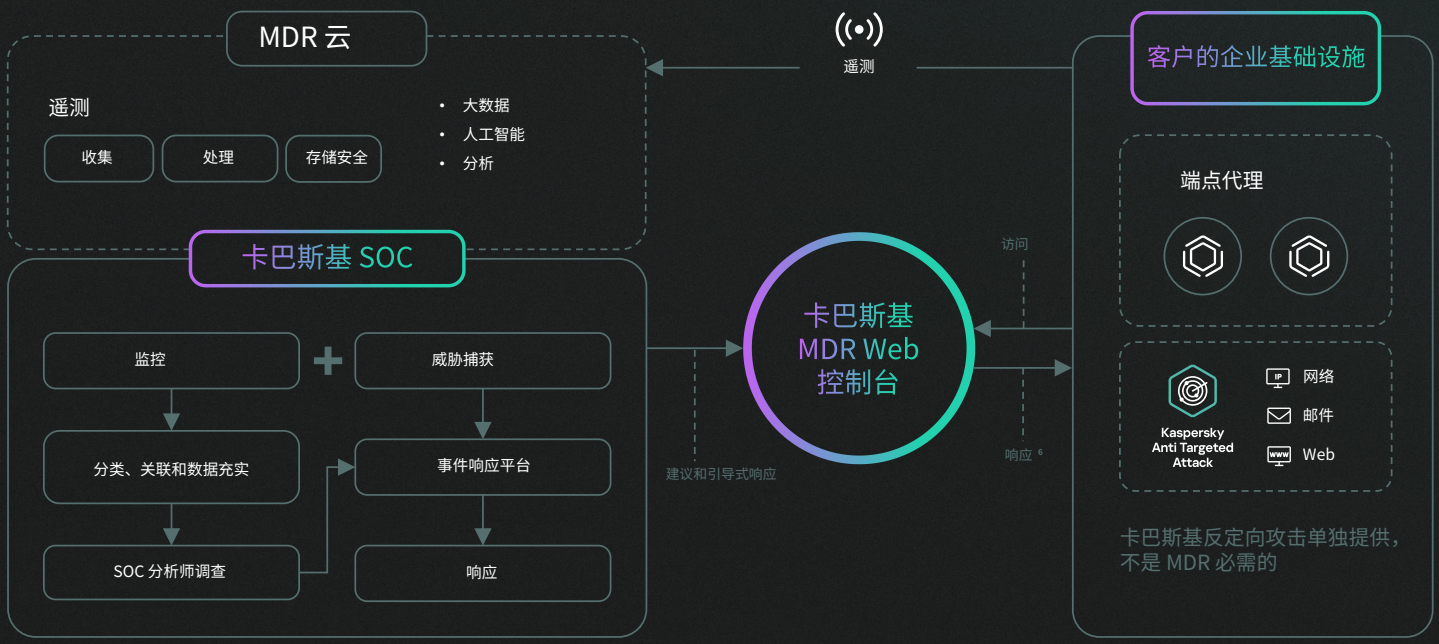
3

当检测到潜在威胁时，卡巴斯基 MDR 会按严重程度对其分类，并通过电子邮件和/或 Telegram 通知客户。在可能的情况下，根本原因分析有助于识别攻击源，并提供有关如何遏制、应对和减轻检测到的威胁的建议。

4

客户可以选择将响应* 功能部分或全部委托给卡巴斯基 SOC 团队。与事件相关的任何问题都可以在卡巴斯基 MDR Web 控制台的聊天中讨论。

卡巴斯基 MDR 架构



卡巴斯基 MDR 与第三方反病毒解决方案兼容。当客户在卡巴斯基 MDR 门户上批准后，自动响应将启动（如果客户未批准，MDR 门户将在自动响应启动前请求批准）。

* 如果需要对事件进行更深入的分析，并且您拥有卡巴斯基事件响应的有效订阅，则可以将事件移交给卡巴斯基 GERT 团队进行调查。

价值主张

持续防御最复杂、最狡猾的威胁，让您高枕无忧

无需费心费力建立自己的 SOC，即可拥有其所有主要优势

降低总体安全成本 – 无需聘用和培训多名昂贵的 IT 安全专业人员来覆盖每个方面

将内部 IT 安全资源重新集中，用于处理其他关键业务问题

全球认可，无与伦比的业绩记录

卡巴斯基参与各种独立测试，并与全球领先的分析公司密切合作。卡巴斯基是全球公认的网络安全领导者，卡巴斯基 MDR 和我们的所有产品一样，屡获殊荣。卡巴斯基 MDR 强大的检测和响应功能与高素质、经验丰富的卡巴斯基 SOC 团队享誉全球的专业知识相辅相成，该团队是业内最成功、最有经验的威胁搜寻团队之一。

Software Reviews CHAMPION 2024

Quadrant Knowledge Solutions

MITRE | ATT&CK®

GIAC CERTIFIED GCFA FORENSIC ANALYST

GIAC CERTIFIED GCIH INCIDENT HANDLER

GIAC CYBER THREAT GCTI INTELLIGENCE

GIAC NETWORK GNFA FORENSIC ANALYST

GIAC PENETRATION GPEN TESTER

GIAC EXPLOIT RESEARCHER & ADVANCED PENETRATION TESTER GXPN

GIAC REVERSE ENGINEERING GREM MALWARE

CISA

CISM

EC-Council CERTIFIED C|EH

EC-Council CERTIFIED C|HFI

OFFENSIVE SECURITY OSCP

OFFENSIVE SECURITY OSCE

CISSP®

卡巴斯基托管检测与响应

了解更多

www.kaspersky.com.cn

#kaspersky
#bringonthefuture